HOSPITAL UNIVERSITARIO
DEPARTAMENTAL DE NARIÑO E.S.E

AUDITORÍA AL MODULO DE HISTORIA CLINICA

JENNY NAYIBI BURGOS GARCÍA
MARÍA CAROLINA DOMÍNGUEZ GÓMEZ

DINAMICA GERENCIAL

AUDITORÍA DEL MÓDULO DE HISTORIA CLÍNICA ELECTRÓNICA DEL SISTEMA DE INFORMACIÓN EN EL HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO

JENNY NAYIBI BURGOS GARCÍA
MARÍA CAROLINA DOMÍNGUEZ GÓMEZ

UNIVERSIDAD DE NARIÑO
FACULTAD DE INGENIERÍA
PROGRAMA DE INGENIERÍA DE SISTEMAS
SAN JUAN DE PASTO
2008

AUDITORÍA DEL MÓDULO DE HISTORIA CLÍNICA ELECTRÓNICA DEL SISTEMA DE INFORMACIÓN EN EL HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO

JENNY NAYIBI BURGOS GARCÍA
MARÍA CAROLINA DOMÍNGUEZ GÓMEZ

Trabajo de grado presentado como requisito para optar al título de Ingeniera de Sistemas

Director
Especialista FRANCISCO NICOLAS SOLARTE SOLARTE

UNIVERSIDAD DE NARIÑO
FACULTAD DE INGENIERÍA
PROGRAMA DE INGENIERÍA DE SISTEMAS
SAN JUAN DE PASTO
2008

NOTA DE RESPONSABILIDAD

Las ideas y conclusiones expuestas en el presente trabajo de grado es responsabilidad exclusiva de los autores.

Artículo 1° del acuerdo 324 de octubre 11 de 1966, emanado del honorable Consejo Directivo de la Universidad de Nariño.

NOTA DE ACEPTACION

_____

_____

_____

_____

JURADO

_____

JURADO

San Juan de Pasto, Diciembre 05 de 2008

A mis hijos: Luisa Fernanda, Hugo Sebastián, Laura Carolina.

A mis padres y hermana por su apoyo incondicional y por su cariño, y a Dios porque siempre está presente en mi vida y la llena de maravillosos motivos para alcanzar las metas que me he propuesto.

Mª Carolina Domínguez.

A Dios, por brindarme esta hermosa oportunidad de luchar por mis ideales y por rodearme de grandes personas, que han hecho de mi vida la más linda experiencia.

A mi Madre y mi Padre por guiarme durante la vida, por darme su comprensión y ayuda.

A Luís Alberto, Alex y David por apoyarme incondicionalmente, y brindarme su cariño y su comprensión.

Jenny Nayibi Burgos García.

AGRADECIMIENTOS

Ante todo, muchas gracias a nuestras familias, su compresión y su apoyo fue de gran importancia para la realización de este proyecto, y culminar con éxito nuestra carrera.

En segundo lugar agradecemos la formación al interior de La Universidad de Nariño, que no solo ha sido nuestra Alma Mater durante estos 5 años de carrera, si no que además nos ha proporcionado las herramientas necesarias y la prospectiva de la importancia del trabajo en grupo, de la ética profesional, del compañerismo y del trabajo bien hecho así como muchas experiencias más, que sin lugar a duda nos enriquece para enfrentar el mundo exterior, la competencia laboral y el entorno de la región y el mundo.

Es de gran importancia para nosotros terminar nuestra carrera, nos espera mucho camino por recorrer y mucha experiencia por adquirir, durante este estudio hemos procurado alcanzar una madurez de conocimientos que nos permitan ser buenos profesionales, hoy en día gracias al desarrollo de este proyecto, hemos podido experimentar y conocer como es entorno laboral lo difícil de la competencia que existe en la actualidad en la región, la falta de trabajo y oportunidades nos exige mayor dedicación y preparación, igualmente hemos observado la realidad del mundo laboral y de esto se ha concluido que las personas y entorno son egoístas y difíciles de sobrellevar, que si queremos mantener una buena imagen y salvar la ética de nuestras profesiones, debemos realizar nuestro trabajo con el buen criterio que se nos ha formado, con honestidad y dedicación.

Durante el desarrollo de este trabajo se ha pasado por dificultades, como la inexperiencia, la convivencia con diferentes personas y sus propios intereses, el entorno mismo del Hospital Departamental de Nariño, pero hoy deseamos agradecer a todas aquellas personas que nos colaboraron y nos brindaron su

apoyo, todo esto no hubiera sido posible si no contáramos con profesores y compañeros de la institución que nos afirmaron en la realización de algunas actividades, ellos nos ayudaron en la realización de nuestros objetivos, agradecemos a todas aquella personas que brindaron su conocimiento su experiencia y su tiempo, sin esa colaboración no hubiera sido posible la realización de este proyecto, y por ello ofrecemos nuestro agradecimiento perpetuo.

TABLA DE CONTENIDO

Pág.

GLOSARIO

BUZÓN DE CORREO ELECTRÓNICO: área de almacenamiento para los correos electrónicos entrantes y salientes de los usuarios, ubicado en el servidor de correo

CONFIDENCIALIDAD: proteger la información de ser leída y/o copiada por cualquier persona que no este explícitamente autorizada para esto.

CONTRASEÑA (PASSWORD): conjunto de caracteres alfanuméricos que le permite a un usuario el acceso a un determinado recurso o la utilización de un servicio dado en la red. Se destaca que la contraseña no es visible en la pantalla al momento de ser tecleada con el propósito de que sólo pueda ser conocida por el usuario.

COPIA DE RESPALDO O SEGURIDAD (BACKUP): acción de copiar archivos o datos de forma que estén disponibles en caso de que un fallo produzca la pérdida de los originales. Esta sencilla acción evita numerosos, y a veces irremediables, problemas si se realiza de forma habitual y periódica.

DISPONIBILIDAD: proteger los servicios para que no se degraden o se encuentren inaccesibles sin autorización.

HACKING: el acto de aprender los detalles de otros sistemas computarizados. Acceder a un sistema informático sin autorización.

HARDWARE: todos los componentes físicos de la computadora y sus periféricos.

INFRAESTRUCTURA DE COMUNICACIONES: toda la base tecnológica que soporta la transmisión de voz y datos por la red del ICBF y que permite el uso de Internet, intranet, videoconferencia y correo electrónico entre otros.

INFRAESTRUCTURA DE CÓMPUTO: todos los equipos de computadoras, servidores, impresoras, pantallas y demás periféricos que contribuyen al desarrollo laboral de los servidores públicos y contratistas del ICBF.

INTEGRIDAD: Proteger la información y los programas de ser borrados o alterados sin el permiso del dueño.

INTERNET: internet se define generalmente como la red de redes mundial, las redes que son parte de esta red se pueden comunicar entre sí a través de un protocolo denominado TCP/IP (Transmission Control Protocol / Internet Protocol). Fue concebida a fines de la década de 1960 por el Departamento de Defensa de los Estados Unidos, más precisamente por la ARPA.

INTRANET: las intranets son redes corporativas que utilizan los protocolos y herramientas de Internet. Su aspecto es similar al de las páginas de Internet. Si esta red se encuentra a su vez conectada a Internet, generalmente se la protege mediante firewalls.

MICROSOFT TREND: antivirus utilizado por parte de SIMA para prevenir y eliminar virus en la red de Cómputo del ICBF.

OUTSOURCING: subcontratación de servicios y productos en una alianza tal con los proveedores elegidos, que éstos prácticamente se convierten en una extensión de los negocios de la organización, pero siguen ocupándose de su propia administración.

PAQUETIZACIÓN: la parte de un mensaje que se transmite por una red. Antes de ser enviada a través de Internet, la información se divide en paquetes.

PROTOCOLO DE INTERNET: conjunto de comandos que permite que dos computadores se comuniquen entre sí a través de Internet.

SERVICIO DE RED INTERNA: servicio que provee Teledifusión a la red de comunicaciones del ICBF y que se basa en la administración y mantenimiento de la misma para que la transferencia de información se presente sin errores y en tiempo mínimo de transmisión.

SIMA: grupo llamado Servicio Informático y Mesa de Ayuda encargado del soporte y mantenimiento de la red de comunicaciones y de cómputo del ICBF.

SOFTWARE: término general que designa los diversos tipos de programas usados en computación.

SPAM: son mensajes no solicitados, habitualmente de tipo publicitario, enviados en cantidades masivas.

SPAMMING: acto de enviar correo electrónico no solicitado.

USUARIO: cualquier funcionario, usuario y/o trabajador con acceso autorizado, que hace uso de alguno de los recursos de cómputo con los que cuenta el Instituto Colombiano de Bienestar Familiar.

VIRUS: programa que se duplica a sí mismo en un sistema informático incorporándose a otros programas que son utilizados por varios sistemas. Este tipo de programas pueden actuar de diversas maneras como son:

- Solamente advertir al usuario de su presencia, sin causar daño aparente.
- Tratar de pasar desapercibidos para causar el mayor daño posible.
- Adueñarse de las funciones principales (infectar los archivos de sistema).

RESUMEN

LA AUDITORÍA AL SISTEMA DE INFORMACIÓN DEL HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO EN EL MÓDULO DE HISTORIA CLÍNICA ELECTRÓNICA, SE ENFOCA BÁSICAMENTE A IDENTIFICAR ALGUNAS FALENCIAS AL INTERIOR DE LA ORGANIZACIÓN, TENIENDO EN CUENTA LA MISIÓN Y LA VISIÓN DEL HOSPITAL Y GENERANDO UNA ACTITUD DE CAMBIO EN DONDE SE CONTRIBUYA A LA COMPETITIVIDAD ORGANIZACIONAL. EL HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO SE ENCUENTRA EN EL PROCESO DE IMPLANTACIÓN DEL MÓDULO DE HISTORIA CLÍNICA, UNA HERRAMIENTA VALIOSA PARA LA GESTIÓN DE SU INFORMACIÓN Y EN ARAS DE CONVERTIRSE EN LA MEJOR UNIDAD COMPLEMENTARIA DE SALUD DEL DEPARTAMENTO, SE HAN GENERADO GRANDES ESFUERZOS PARA CUMPLIR CON LOS ESTÁNDARES DE ACREDITACIÓN Y CALIDAD. EN ESE MISMO SENTIDO Y TENIENDO EN CUENTA LOS ESTÁNDARES DE LA ISO 27001, SE HA INTEGRADO EL PROCESO DE AUDITORÍA AL MÓDULO PARA QUE SIRVA DE ANTECEDENTE A LA GESTIÓN INMEJORABLE POR CONVERTIR AL HOSPITAL UNIVERSITARIO EN EL MEJOR DE LA REGIÓN.

ABSTRACT

THE AUDIT TO THE INFORMATION SYSTEM OF THE DEPARTMENTAL UNIVERSITY HOSPITAL OF NARIÑO IN MÓDULO DE ELECTRONIC CLINICAL HISTORIA, BASICALLY FOCUSES TO IDENTIFY SOME FALENCIAS TO THE INTERIOR OF THE ORGANIZATION, CONSIDERING THE MISSION AND THE VISION OF THE HOSPITAL AND GENERATING A CHANGE ATTITUDE IN WHERE IT IS CONTRIBUTED TO THE ORGANIZACIONAL COMPETITIVENESS. THE DEPARTMENTAL UNIVERSITY HOSPITAL OF NARIÑO IS IN THE PROCESS OF IMPLANTATION OF I MODULATE OF CLINICAL HISTORIES, A VALUABLE TOOL FOR THE MANAGEMENT OF ITS INFORMATION AND FOR THE SAKE OF BECOMING THE BEST COMPLEMENTARY UNIT OF HEALTH OF THE DEPARTMENT HAS GENERATED GREAT EFFORTS TO FULFILL THE STANDARDS OF ACCREDITATION AND QUALITY. IN THAT SAME SENSE AND CONSIDERING THE STANDARDS OF ISO 27001, THE PROCESS OF AUDIT HAS BEEN INTEGRATED TO I MODULATE SO THAT IT SERVES AS ANTECENDENTE THE SUPERB MANAGEMENT TO TURN TO THE UNIVERSITY HOSPITAL THE BEST ONE OF THE REGION.

INTRODUCCION

El hospital universitario departamental de Nariño es una entidad de tercer nivel de salud, dentro de las políticas que proyecta a la población del municipio, esta la del suministro del servicio de salud y la búsqueda de una mejora continua en el desenvolvimiento de las áreas administrativas y asistenciales.

En la actualidad la informática ocupa uno de los lugares principales dentro de las instituciones y organizaciones empresariales, es así como en las instituciones de salud se hace necesario prestar un mejor servicio a los usuarios, y se busquen herramientas que mejoren el trabajo del personal administrativo cumpliendo con los requerimientos de la acreditación para entidades de salud, teniendo en cuenta la necesidad de sistematizar los procedimientos. El hospital departamental de Nariño ha venido trabajando para implementar en las diferentes áreas administrativas como asistenciales, procesos y herramientas que permitan la optimización de las actividades, en pro de brindar cada día un servicio más competitivo acorde con la exigencia de la competencia y la sociedad.

En cuanto a la administración de la información el hospital universitario departamental de Nariño es una de las instituciones del departamento, que se preocupa por estar a la vanguardia en el uso de tecnología para el manejo de información, en ella muchos de los procesos se han sistematizado logrando mejorar la atención al público, disminuyendo los tiempos de búsqueda de información, garantizando mayor integridad y confiabilidad de los datos, contribuyendo a la prestación de servicios de calidad.

La importancia de realizar la auditoría al módulo de historia clínica del aplicativo WINDG de dinámica gerencial dentro del hospital universitario departamental de Nariño, radica en verificar el correcto funcionamiento de todos los procesos

del módulo, así como también el cumplimiento de los requerimientos de entradas y salidas de datos para el módulo de historia clínica y evaluar que todos ellos suplan las necesidades de los diferentes usuarios tanto administrativos como asistenciales (médicos, enfermeras), igualmente permitirá verificar como a sido el proceso del implantación del módulo de historia clínica dentro del contrato outsourcing con SYAC, la empresa contratada, y el área de información y sistemas del hospital encargada de este proyecto, finalmente se debe destacar que la auditoría permitirá verificar el correcto funcionamiento de la infraestructura física y lógica (base de datos) destacando dentro de este componente, la evaluación de la seguridad de acuerdo al estándar ISO 27001, con el fin primordial de garantizar que el módulo tenga un nivel de desempeño efectivo y eficaz para sus usuarios.

Los beneficios que traerá la presente auditoría al módulo de historia clínica digital del hospital universitario departamental de Nariño, es la revisión de los controles existentes en cuanto al cumplimiento de los diferentes requerimientos de los usuarios del módulo de historia clínica, como también la seguridad lógica del sistema operativo y acceso a la base de datos para comprobar su eficiencia y eficacia, recomendando la implementación de planes, herramientas, políticas, controles y mejoras para la protección de uno de los principales activos de la institución, su información, garantizando que el funcionamiento del módulo sea optimo y que permita una gestión transparente por parte de sus usuarios.

El título del proyecto de grado que se desarrolla en este trabajo es auditoria del módulo de historia clínica electrónica, del sistema de información en el hospital universitario departamental de Nariño, y responde a la categorización dentro su modalidad i***nvestigación científica o aplicada,*** ya que “es un proceso reflexivo, sistemático controlado y critico” acorde con la capacidad analítica y de síntesis para la resolución de un problema, que aplica una serie de operaciones lógicas tomando como punto de partida datos y objetivos, para

resolver problemas y descubrir hechos o datos, relaciones o leyes en los campos del conocimiento humano.[1]

Se ha desarrollado dentro del área de investigación ***gestión y desarrollo de sistemas****,* puesto que a través de su estudio, se logran obtener la conceptualización necesaria sobre los sistemas de información de una organización, en relación a sus procesos, el manejo que debe tener la información mediante su sistematización, la estructura y gestión de los sistemas implementados, el papel que cumple el recursos humano frente a todos ellos, brindando las herramientas necesarias para su evaluación y análisis.[2]

Según las líneas de Investigación aprobadas y definidas en el programa de ingeniería de sistemas de la universidad de Nariño, la línea de investigación para el proyecto planteado corresponde a s*istemas computacionales* debido a que esta línea tiene como objetivo planificar, diseñar, implantar, administrar y evaluar sistemas computacionales y servicios basados en estos sistemas complejos de información, la cual soporta la temática de auditoría de sistemas.

Evidentemente la temática referenciada al proyecto es ***auditoria a sistemas de información,*** puesto que a través de su estudio e investigación, se conocerán todas las bases necesarias para desarrollar este proyecto, en relación a todos los aspectos de software y hardware como: revisión y evaluación de los controles del sistema, procedimientos de informática, infraestructura física y equipos de cómputo, seguridad física y lógica, administración de la información, papel del recurso humano, a fin de establecer las pautas que determinarán el estado en el que se encuentra la organización, y cuales serian los controles y recomendaciones a seguir para mejorar la administración y apoye la toma de decisiones.

---

[1] Guerrero, José. Guía Para el Desarrollo del Proyecto de Grado. Bogota: UNAD,1999.p.30
http://www.monografias.com/trabajos15/invest-cientifica/invest-cientifica.shtml

[2]

En el planteamiento inicial de este proyecto se ha realizado la siguiente pregunta : ¿Cómo evaluar el proceso y el módulo de historia clínica electrónica, que garantice la confiabilidad, integridad y seguridad permitiendo adelantar actividades de mejoramiento del sistema y la acreditación del hospital universitario departamental de Nariño?, y al mismo tiempo se plantea la sistematización del problema en donde se pueda obtener toda la información necesaria y pertinente para los procesos que mantiene el hospital y así evaluar el módulo de historia clínica electrónica.

Cuando se generalizó el uso de las nuevas tecnologías, surgió también la necesidad de realizar auditorías sobre los sistemas de información. En este sentido se podría decir que la auditoría informática comprende el conjunto de actividades encaminadas a la validación y verificación de los sistemas, procesos y resultados en los que se utilicen tecnologías automatizadas, ya sea en cumplimiento de la legislación, como garantía de la integridad y rectitud de la información aportada por un sistema o por alineamiento con determinados estándares relacionados con el buen uso o buenas prácticas de los sistemas.

Actualmente el campo de la salud a ido evolucionando y creciendo, dando como resultado el origen de diversas entidades de carácter público y privado, dedicadas a la prestación del servicio de salud, convirtiéndose en competencia en aspectos como: talento humano, recursos físicos, manejo administrativo, y herramientas informáticas entre otros. De igual manera las entidades reguladoras de salud se han visto en la necesidad de establecer requerimientos y normas mínimas, para el normal desenvolvimiento de estas instituciones, como también se han establecido normas ISO, y procedimientos que permiten definir cuales de estas instituciones cumplen con los estándares de calidad. El hospital universitario departamental como eje central del departamento se encuentra en ese proceso de acreditación, con el fin de brindar a sus usuarios el mejor de los servicios.

El desarrollo de este proyecto de tesis está sustentado primordialmente en la práctica en el área de auditoría de sistemas, aplicando una metodología adecuada para las entidades públicas teniendo en cuenta los estándares de calidad que se sustentan en la norma ISO y que actualmente regulan y tipifican la excelencia dentro de la empresa.

1. DELIMITACIÒN Y ALCANCE

Se realizará un análisis de riesgos al módulo de historia clínica electrónica, evaluar los riesgos en cada una de las secciones, y posteriormente realizar el proceso de auditoría a las que evidencien riesgos más altos, ella comprende: un análisis integral de los procesos, aplicación de la norma ISO para la calidad y seguridad del software, evaluación de controles , técnicas y procedimientos de seguridad, uso de software para evidenciar pruebas de fallas, con el fin de establecer controles óptimos sobre los procesos y el módulo de historia clínica electrónica, que garanticen la confiabilidad, integridad y seguridad de la información.

1.1. FACTIBILIDAD DE LA INVESTIGACIÒN

Para el desarrollo del proyecto de auditoría del módulo de historia clínica electrónica, del sistema de información en el hospital universitario departamental de Nariño, se cuenta con los recursos necesarios y la disponibilidad sobre aspectos como: presupuesto, recurso humano y los elementos como hardware y software necesarios entre otros.

1.1.1. Factibilidad técnica

Para el desarrollo del proyecto se cuenta con los recursos que brinda la institución en cuanto a: infraestructura física como el aula virtual, que es el sitio asignado para el proceso del implantación del módulo de historia clínica electrónica, equipos de cómputo, impresora, escáner, cámaras fotográficas, grabadoras, filmadora, multimetro digital y certificaciones de red.

1.1.2. Factibilidad operativa

El personal administrativo, los interventores y el líder del proyecto, son concientes de que esta auditoría informática contribuirá de manera significativa a mejorar e implementar las condiciones de calidad y los controles adecuados, sobre la gestión del módulo y el recurso humano involucrado con su dirección,

manejo y soporte, permitiendo brindar un servicio de calidad a los pacientes de la región. De manera conjunta se cuenta con el personal calificado para el desarrollo del proyecto de auditoría informática.

En el hospital universitario departamental de Nariño, y en especial el área de sistemas, existe un ambiente de colaboración tanto para el desarrollo como para la implementación de la auditoría, contando con el recurso humano necesario, el cual brinda asistencia en el desarrollo de soluciones para el cumplimiento de las tareas de competencia de la auditoría.

1.1.3. Factibilidad económica

El presente trabajo de auditoría informática, estará plasmado en un documento, con el cual tanto el coordinador de sistemas, personal administrativo y demás usuarios, puedan guiarse en la toma de decisiones sobre las mejoras que hayan de realizarse en el área de información y sistemas del hospital, la investigación no presenta gastos elevados, por tal razón será financiado por el grupo investigador.

2. MARCO REFERENCIAL

2.1. MARCO CONTEXTUAL

2.1.1. Información general y ubicación

El hospital universitario departamental de Nariño es una institución de carácter social del estado, ubicado en la ciudad de Pasto en el departamento de Nariño (Colombia) sus datos son los siguientes:

- Dirección: Calle 22 No 7-93 Parque Bolívar.
- Teléfono: 7214525 - 7214526
- e-mail: www.hosdenar.gov.co

La finalidad de la institución es prestar el servicio de salud en mediana y alta complejidad, cuenta con una trayectoria de 33 años lo que lo acredita como uno de los mejores hospitales de la zona.

Actualmente cuenta con un sistema de información conformado por 16 módulos, que de manera general se dividen en dos grandes subsistemas que son:

Administrativos: Conformado por los siguientes módulos:

- Pagos
- Contabilidad
- Inventarios hospitalarios
- Nomina
- Facturación
- Cartera
- Presupuesto

- Costos hospitalarios
- Tesorería
- Activos fijos

Asistenciales: Conformados por los siguientes módulos:

- Admisiones
- Hospitalización citas médicas
- Consulta externa
- Contratos
- Administrativo de recursos
- Historia clínica electrónica, (en proceso de actualización).

El hospital universitario departamental de Nariño es una institución de amplia trayectoria que con el avance tecnológico, la confrontación de una amplia competencia y la exigencia de estándares de calidad, está comprometida a trabajar por la implementación de planes estratégicos que permitan no solo la correcta gestión del hospital, sino también la exigencia de implementación de nuevas herramientas que permitan mejorar los procesos y funciones de la institución, para poder prestar el mejor de los servicios a los usuarios.

De la mano de estas normas y políticas se encuentran las herramientas informáticas, actualmente se cuenta con un sistema de información conformado por 16 módulos y dividido en dos grandes columnas *administrativo y asistencial,* de donde algunos de sus módulos ya han sido sometidos a procesos de auditorías logrando discernir aquellas irregularidades, para lograr optimizar el sistema.

Con la aplicación del sistema de gestión estratégica, se esta buscando conseguir un modelo de gestión integral por calidad, y en mira al proceso de acreditación se han acogido metodologías establecidas por la ISO para lograr contribuir a los objetivos estratégicos y lograr la acreditación en un mediano plazo.

2.1.2. Misión: El hospital universitario departamental de Nariño, es una empresa social del estado, que complementa la red departamental de prestadores de servicios de salud en mediana y alta complejidad. Propicia el crecimiento integral de talento humano, lo cual permite proyectarse e incidir en el mejoramiento de la salud y calidad de vida de la comunidad del sur occidente colombiano.[3]

2.1.3. Visión: El hospital universitario departamental de Nariño, dirigirá sus esfuerzos al mejoramiento continuo, se convertirá en una organización centrada en el usuario y fortalecerá la implementación de tecnología de tal manera que complemente de manera armónica la red de prestadores de servicios de salud en los niveles de media y alta complejidad. Obtener la acreditación en los próximos tres años, es el sueño del futuro, ya que de esta manera se dará cumplimiento a la misión.[4]

2.1.3. Objetivos

- Implementar una cultura de excelencia empresarial
- Estandarización de procesos administrativos y de apoyo – estandarización de procesos asistenciales.
- Administración efectiva de los recursos físicos y financieros.
- Disminuir el impacto ambiental generado por el desarrollo de los procesos de la cadena productiva y de apoyo.
- Adquisición de tecnología y modernización de infraestructura.
- Promover el desarrollo integral del personal.
- Aumentar la participación en los diferentes segmentos del mercado.
- Excelencia operacional.[5]

[3] Documento de HUDN Direccionamiento estratégico
[4]
[5]

2.1.4. Servicios que ofrece[6]

Portafolio de servicios del HUDN

El hospital universitario departamental de Nariño empresa social de estado, es la única organización de la red publica de nivel lll de la región , funciona desde el 15 de diciembre de 1975 y en octubre de 1990 mediante resolución del ministerio de salud No. 14676, es clasificado como organismo para atención de nivel lll. A partir del 10 de diciembre de 1994, se constituye en una empresa social del estado E.S.E. por ordenanza 067 expedida en la asamblea departamental de Nariño, y el 17 de diciembre de 2004 por ordenanza No. 023 se reorganiza como hospital universitario proyectándose con los avances de la ciencia, la tecnología y la gerencia moderna a la comunidad del sur occidente del país, dentro de las áreas de servicios que ofrece se encuentra:

A. Cirugía y subespecialidades quirúrgicas

Quirófanos sala de partos:

- Cirugía general
- Traumatología y ortopedia
- Oftalmología
- Ginecología y obstetricia
- Urología
- Cirugía maxilofacial
- Otorrinolaringología
- Neurocirugía
- Cirugía plástica
- Cirugía dermatológica

[6] Procesos Hospitalarios

- Cirugía laparoscopia diagnostica

Cirugía ambulatoria:

- Cirugía general
- Ortopedia
- Ginecología y obstetricia
- Oftalmología
- Otorrinolaringología
- Cirugía plástica
- Cirugía maxilofacial
- Urología
- Dermatología
- Cirugía de ortopedia y traumatología

Cirugía corta estancia:

- Cirugía general
- Urología
- Otorrinolaringología
- Oftalmología
- Dermatología

Cirugía estética a bajo costo:

- Liposucción
- Septo rinoplastia

- Resección de masas en la piel

B. Consulta externa

El servicio de consulta externa cuenta con amplias instalaciones para brindar una mejor atención a los usuarios, además de especialistas, garantizando una consulta personalizada y la tranquilidad de los pacientes.

- Cirugía general
- Traumatología y ortopedia
- Oftalmología
- Ginecología y obstetricia
- Urología
- Cirugía maxilofacial
- Otorrinolaringología
- Neurocirugía
- Cirugía plástica
- Cirugía dermatológica
- Cirugía laparoscopia diagnostica
- Medicina familiar integral

C. Rehabilitación - fisioterapia

Fonoaudiología y audiologia básica

- Audiometría tonal y vocal (Logo audiometría)
- Impedanciometria (Inmitancia acústica)

Terapia del lenguaje para pacientes que presentan:

- Trastornos en la articulación de los fonemas (dislalias)
- Alteración en la comprensión auditiva y expresión verbal (disfasias - afasias)
- Trastornos en el proceso de adquisición del lenguaje lecto-escrito acompañados de trastornos en la articulación de los fonemas (persistencia de procesos fonológicos - dislalias).

- Terapia para pacientes que han recibido tratamiento quirúrgico o radioterapia y presentan alteración en la expresión verbal por ausencia parcial o total de los órganos fono articuladores (labios, lengua)
- Retardo en el desarrollo del lenguaje
- Alteración en los procesos motores del habla (disartria)

Terapia de voz: alteración en la voz (disfonías - afonías) de origen funcional, o secundario a tratamiento con radioterapia o quirúrgico, en caso de Incomunicación oral post laringectomía total.

Terapia de deglución: Para pacientes que presentan alteración en el mecanismo de la deglución (disfagias), de origen neurológico, o secundaria a tratamientos por cáncer en la cavidad oral, en la laringe y en la faringe.

Terapia miofuncional orofacial:

- Para pacientes que presentan imbalance muscular orofacial debido a patrones incorrectos de deglución y persistencia de hábitos orales.
- (respiración oral – succión digital)

Estimulación motora – oral: Para neonatos de alto riesgo (prematurez, daño neurológico, labio paladar hendido), con dificultades para iniciar y desarrollar succión y deglución.

Terapia Física:

- Terapia individualizada
- Terapia respiratoria
- Ejercicio terapéutico
- Hidroterapia
- Mecanoterapia

- Electroterapia
- Rehabilitación funcional
- Gimnasio

Unidad de rehabilitación y fisiatría:

- Consulta de fisiatría
- Estudios de electrodiagnóstico
- Electromiografía y neuroconducción
- Potenciales evocados somato sensoriales
- Bloqueo nervio periférico
- Potenciales evocados auditivos
- Test de estimulación repetitiva (test de lambert)
- Estudios de fibra única.

D. Hospitalización: el servicio de hospitalización dispone de talento humano comprometido a prestar servicio de calidad que permitan al paciente su pronta recuperación.

- Unidad de cuidado intensivo
- Unidad de cuidado intensivo e intermedio neonatal
- Servicio de cirugía general
- Servicio de cirugía especializada
- Servicio de neonatología
- Servicio de gineco - obstetricia
- Servicio de medicina interna

- Servicio de ortopedia y traumatología
- Servicio de hospitalización unidad de cuidados intensivos
- Servicio de especializaciones medicas

E. Laboratorio clínico:

- Química Clínica
- Hematológica y coagulación
- Uro análisis
- Microbiología
- Parasitología medica y coproanalisis
- Marcadores tumorales y hormonas
- Inmunohematología
- Programa de control de calidad nacional e internacional
- Laboratorio de urgencias 24 horas

F. Banco de sangre tipo A y medicina transfusional

- Preparación y selección de componentes
- Transfusión sanguínea

G. Programas especiales

- Transfusión antóloga
- Hemaferesis

H. Laboratorio, patología y citología

- Citología por aspiración (Bacaf)
- Citología cervico-vaginal oncológica

- Citología de líquidos corporales (líquido cefalorraquídeo orina, liquido pleural peritonal, cito centrífuga)
- Lavado y cepillado bronco alveolar y bronquial
- Citología de vías biliares
- Coloraciones especiales
- ZN - PAS - PAS con diastasa - Hierro - Retículo

I. Medicina interna: En esta área se encuentran médicos internistas, de urgencias y hospitalización, las 24 horas, prestando un servicio con la excelencia y la calidez humana.

- Medicina interna general
- Cardiología
- Neumología
- Fisiatría
- Gastroenterología
- Dermatología
- Hematológica
- Endocrinología

J. Materno infantil

Ginecología y obstetricia

- Ginecología
- Ginecología oncológica
- Obstetricia
- Obstetricia de alto riesgo

- Inserción de dispositivo intrauterino
- Post-parto y post-legrado
- Monitoreo fetal
- Ecografía obstétrica
- Colposcopia
- Biopsia cervical y endometrial
- Salas de cirugía
- Sala de atención al recién nacido
- Unidad de recuperación (pacientes simultáneos)
- Vídeo endoscopia
- Monitoreo paciente obstétrica de alto riesgo

Iniciativa Instituciones amigas de la mujer y la infancia (Iami):

- Ofrece atención integral a la unidad materno – infantil.
- Brinda a las mujeres gestantes, educación atención oportuna.
- Garantiza la atención del parto con calidad y calidez.
- Brinda ayuda efectiva a las mujeres y sus familias para que puedan poner en práctica la lactancia materna.
- Favorece el alojamiento conjunto.
- Conserjería en lactancia materna y planificación familiar.
- Atención, programa mama – canguro.
- Facilita el registro civil.

- Atención integral de las enfermedades prevalecientes de la infancia (recién nacidos).
- Favorece el acompañamiento permanente al recién nacido hospitalizado.
- Atención programa de estimulación adecuada para niños de alto riesgo neurológico.
- Contacto con grupos de apoyo a la lactancia.

Neonatología: Todo recién nacido ingresa a la unidad de neonatología por presentar diagnósticos de:

- Prematurez
- Sufrimiento fetal
- Malformaciones congénitas
- Trastornos metabólicos
- Ruptura previa de membrana
- Infecciones virales y bacterianas
- Síndrome ictérico del neonato
- Síndrome de dificultad respiratoria: en quirófano se dispone de equipos de alta tecnología que garantizan el adecuado servicio: Incubadoras, monitores, lampas de calor radiante, ventiladores neonatales, bombas de Infusión, pulsioscimetros.

Programa ampliado de inmunización a recién nacido entre estos se encuentran: la vacuna anti poliomielítica, B.C.G, hepatitis B, vacunación a mujeres en post-parto y post-legrado, vacunación de triple viral y el programa de seguimiento neurológico y estimulación adecuada.

K. Plan de servicios y servicios especiales

- POS plan obligatorio de salud
- POS-S plan obligatorio de salud subsidiado
- PAC-S planes de atención complementario
- ECAT accidentes de transito y enfermedades catastróficas
- ATEP accidentes de trabajo y enfermedades profesionales
- SOAT seguro obligatorio por accidentes de transito
- Régimen contributivo

L. Otros servicios a pacientes particulares

- Servicio a población vinculada
- Servicio a población desplazada
- Servicio a patologías de IVA social
- Servicio a población indígena
- Atención trauma mayor
- Atención por enfermedades de alto costo, los que contemple la ley 100 de 1993

M. Servicios especiales

- Vigilancia epidemiológica y de salud publica
- Salud ocupacional
- Servicio de cirugía laparoscopia diagnostica
- Servicio de neumología y terapia respiratoria
- Servicio de nutrición dietética

- Clínica especializada en enfermedades mamarias
- Asesoría en planificación familiar
- Prevención y manejo cáncer de cuello uterino
- Programa manejo integral de la menopausia
- Colposcopia
- Programa de asesoría en lactancia materna
- Alojamiento conjunto con la madre
- Consejería en lactancia exclusiva
- Orientación en problemas durante la lactancia
- Asesoría en la lactancia de niños con labio leporino y paladar hendido y otras patologías
- Consejería a través de comité de apoyo comunitario
- Unidad de servicio farmacéutico - dosis unitaria
- Medicina familiar integral

N. Traslado asistencial básico en ambulancia: Este servicio se presta a los pacientes del hospital, y a otras personas que lo soliciten las 24 horas, cubriendo así toda la red publica departamental de salud, cumpliendo con la norma ISO de calidad en manufacturas de vehículos asistenciales básicos. El hospital cuenta con personal calificado y suficiente para la asistencia remota, durante el traslado a través de un ágil sistema de comunicaciones.

- Urbano
- Rural
- Intermunicipal
- Interdepartamental

O. Imaginología

Tomografía computarizada (escanografia):

- TAC helicoidal
- Reconstrucción tridimensional y multiplanar
- TAC trifásico ,estudio de nódulo pulmonar y estudios diagnósticos en cabeza y cuerpo
- Biopsias y drenajes
- Procedimientos intervencionistas
- Estudios especiales del tracto gastrointestinal y genitourinario
- Radiología general
- Radiología convencional

Mamografía: mamografía de tamizaje y diagnostica

Ecografía:

- Convencional
- Intraoperatoria
- Intracavitaria (transvaginal, transrectal)
- Pequeñas partes y mamaria
- Doppler color
- Biopsias y drenajes

P. Servicio farmacéutico

Unidad de servicio farmacéutico: El servicio cuenta con el sistema de distribución de medicamento por dosis unitaria, parentérales totales y

medicamentos en “y”. Considerado como el más seguro para el paciente. Prestando así la calidad y disponibilidad de los medicamentos, a los usuarios del hospital en forma oportuna y segura, para lo cual se han implementado controles técnicos y científicos, garantizando los procesos de recepción, almacenamiento, distribución y producción de los servicios ofrecidos.

- Farmacia hospitalaria convencional
- Farmacia externa
- Medicamentos especiales
- Otros que contemple la ley 100 de 1993.

Q. Unidad de cuidados intensivos: En la unidad de cuidados intensivos (UCI), el hospital universitario departamental de Nariño E.S.E, brida atención apacientes en estado critico, que requiere de la atención continua de profesionales especializados además del monitoreo permanente de los equipos con tecnología de ultima generación, garantizando al paciente eficiencia en la atención.

- Ventilación mecánica asistida
- Soporte vital avanzado
- Monitoreo permanente
- Ínter consultas por especialidades monitoria
- Monitoria invasiva
- Colocación catéter swan gantz
- Colocación marcapasos transitorio
- Colocación marcapasos definitivo
- Terapia respiratoria
- Terapia física

- Fisiatría y rehabilitación
- Terapia del lenguaje
- Problemas de voz
- Problemas de aprendizaje
- Fonoaudiologia
- Procedimientos diagnósticos
- Procedimientos terapéuticos
- Analizador de gases arteriales
- Hiperalimentacion parenteral
- Soporte ventilatorio

R. Unidad de oncología

Radioterapia:

- Consulta de radioterapia – oncológica
- Cobaltoterapia
- Quimioterapia
- Consulta de oncológica Clínica
- Sala de quimioterapia

Odontología:

- Odontología oncológica
- Soporte Oncológico
- Psicoterapia individual y grupal
- Asesoria familiar

Otros servicios: Albergue "fundación esperanza de vida"
Programas:

- Atención interdisciplinaria del paciente con cáncer
- Tratamiento del paciente con cáncer, basado en protocolos actualizados.

S. Urgencias: Este servicio trabaja de manera integral las urgencias de adultos las 24 horas al día, 365 días al año, con disponibilidad permanente del personal en todas las especialidades básicas y de alta complejidad.

- Atención de urgencias por medico general
- Atención de urgencias por médicos especialistas
- Atención por otros profesionales de la salud
- Procedimientos y diagnósticos terapéuticos
- Estancia de observación

T. Triage: El paciente es evaluado por médicos generales, encargados de priorizar su atención con el fin de brindar mayor seguridad al usuario de acuerdo al grado de su situación.

2.1.6. Competencia

El hospital universitario departamental de Nariño y sus estamentos tienen competencia en el departamento de Nariño, por ser catalogada como una entidad prestadora de servicios de salud en el tercer nivel de complejidad.

2.2. ANTECEDENTES[7]

Inicialmente el enfoque de la auditoría en la institución se centro en la verificación interna y externa de los registros contables de la organización, posteriormente y de acuerdo al sistema establecido de gestión de la calidad de manera integral se evidencio que se hacia necesario ampliar las verificaciones

[7] http://www.hosdenar.gov.co

a todos los procesos claves del hospital en el campo asistencial y administrativo.

Dentro de los antecedentes en procesos de auditoría en el hospital universitario departamental de Nariño, que es una entidad de carácter público, se a encontrado que posee revisoría fiscal, entidad encargada de auditar todos los procesos al nivel administrativo y asistencial, año tras año se realizan dos auditorías, en las épocas de junio y diciembre por parte de la empresa GMS asesores Ltda.

El sistema de información del hospital ha sido auditado únicamente en los módulos administrativos en las fechas señaladas.

Por otra parte en relación a la universidad de Nariño, en el programa de ingeniería de sistemas se han realizado diferentes proyectos de auditorías dirigidos a los componentes internos de la institución, como lo es el caso del centro de informática, secciones administrativas entre otras, de igual manera también se conocen referencias de investigaciones y auditorías que se a realizado en el entorno del departamento y sus entidades públicas.

2.3. MARCO HISTORICO

2.3.1. Antecedentes históricos de la auditoría[8]

Es interesante estudiar cuales fueron los primeros antecedentes de la auditoría, remontándose con este concepto en el tiempo hacia la antigüedad, se encuentra que el termino de auditoría ya aparece en las sociedades egipcia y romana, en relación a las negociaciones entre terratenientes y aparceros; cuando llegaba el momento de pagar las rentas por las tierras los aparceros liquidaban las cuentas verbalmente con los “auditores” que eran los que les oían o auditaban, de esta forma se evidencia que la auditoría existe desde

8 http://www.google.com.co/search?hl=es&q=antecedentes+historicos+sobre+auditoría+informatica&meta=

tiempos inmemoriales, prácticamente desde que un propietario entregó la administración de sus bienes a otra persona, lo que hacía que la auditoría primitiva fuera en esencia un control contra el desfalco y el incumplimiento de las normas establecidas por el propietario.

Otro antecedente se enmarca aproximadamente hacia el siglo XVIII, cuando surge el concepto de sociedad anónima en el ámbito empresarial, en aquel entonces con esta nueva idea de administración se empiezan a confundir los términos de propiedad y gerencia principalmente en el área de comercialización, por tal razón se pensó que para reducir el riesgo económico se fletara los barcos mercantes y se hicieran pequeños títulos, ayudando a diferenciar los conceptos de propiedad y gerencia, esta figura se generalizo y se extendió especialmente en el área contable, donde empezaron a surgir muchos fraudes y quiebras, con esto surgió la necesidad de contar con un experto que controle estos temas, que sea independiente del la empresa, de confianza de los socios y sujeto a la ética profesional.

La auditoria en su concepción moderna nació en Inglaterra o al menos en ese país se encuentra el primer antecedente, la fecha exacta se desconoce, pero se han hallado datos y documentos que permiten asegurar que a fines del siglo XIII y principios del siglo XIV ya se auditaban las operaciones de algunas actividades privadas y las gestiones de algunos funcionarios públicos que tenían a su cargo los fondos del estado.

Como elemento de análisis, control financiero y operacional la auditoría surge como consecuencia del desarrollo producido por la revolución industrial del siglo XIX, en efecto, la primera asociación de auditores se crea en Venecia en el año 1851 y posteriormente en ese mismo siglo se produjeron eventos que propiciaron el desarrollo de la profesión, así en 1862 se reconoció en Inglaterra la auditoría como profesión independiente, en 1867 se aprobó en Francia la ley de sociedades que reconocía al comisario de cuentas o auditor, en 1879 en Inglaterra se estableció la obligación de realizar auditorías independientes a los

bancos, en 1880 se legalizó en Inglaterra el título de charretera accountants o contadores autorizados o certificados, en 1882 se incluyó en Italia en el código de comercio la función de los auditores y en 1896 el estado de New York había designado como contadores públicos certificados, a aquellas personas que habían cumplido las regulaciones estatales en cuanto a la educación, entrenamiento y experiencia adecuados para ejecutar las funciones del auditor.

Debido al mayor desarrollo de la auditoría en Inglaterra, a fines del siglo XIX e inicios del siglo XX se trasladaron hacia los estados unidos de norte América muchos auditores ingleses que venían a auditar y revisar los diferentes intereses en este país de las compañías inglesas, dando así lugar al desarrollo de la profesión en Norte América, creándose en los primeros años de ese siglo el american Institute of accountants (instituto americano de contadores).

Es conveniente considerar que la contabilidad y la auditoría que se realizaban en el siglo XIX y a principios del siglo XX no estaban sujetas a normas de auditoría o principios de contabilidad generalmente aceptados, por lo que la dificultad para ejecutarlos e interpretarlos generó en el primer cuarto del siglo XX una tendencia hacia la unificación o estandarización de los procedimientos contables y de auditoría, un ejemplo de esta aspiración son los folletos mencionados anteriormente que emitió el instituto americano de contadores, así como el sistema uniforme de contabilidad hotelera emitido por la asociación hotelera del estado de New York.

En 1917 el ya creado instituto americano de contadores preparó a solicitud de la comisión federal de comercio de USA un "Memorándum sobre las auditorías de balance general" que fue aprobado por la comisión, publicado en el boletín de la reserva federal y distribuido en forma de folleto a los intereses bancarios, de negocios y a los contadores de ese país bajo el nombre de: "contabilidad uniforme, propuesta presentada por el comité de la reserva federal". Este folleto fue reeditado en 1918 bajo un nuevo título, "Métodos Aprobados para la

preparación de estados de balance general", indicando tal vez el cambio de nombre a una realización del enfoque utópico de la "contabilidad uniforme".

En 1929, el folleto fue revisado a la luz de la experiencia de la década transcurrida, en adición a un cambio del título, (que se convirtió en "verificación de estados financieros" como evidencia de la creciente toma de conciencia acerca de la importancia del estado de resultado), la revisión contenía la significativa declaración de que "la responsabilidad por la extensión del trabajo requerido debe ser asumida por el auditor".

En 1936, el instituto como vocero de una profesión que ya en esa fecha estaba bien establecida, revisó los folletos previos y emitió de forma independiente bajo su propia responsabilidad un folleto titulado: "examen de estados financieros por contadores públicos independientes", aparecieron dos interesantes desarrollos de la profesión:

- Primero, que la palabra "verificación" utilizada en el título del folleto anterior, no es una representación exacta de la función del auditor independiente en el examen de los estados financieros de una entidad.

- Segundo, la aceptación por el instituto de la responsabilidad de la determinación y publicación de las normas y procedimientos de contabilidad y auditoría.

El aprovechamiento del trabajo de los auditores internos como parte del proceso de revisión de las auditorías de estados financieros a sido específicamente normado por el instituto americano de contadores públicos certificados, y poco a poco se ha ido difundiendo a diferentes área, campos y actividades, de esta forma se observa que día a día, esta profesión sigue aumentado su cobertura y requiere que las personas involucradas con su desarrollo, investigue y creen nuevas herramientas para garantizar el cumplimientos de los objetivos generales de la auditoría.

2.3.2. Antecedentes históricos de la auditoría informática[9]

La auditoría informática, nace desde el momento que se empieza a ver la necesidad de gestionar la información, como ayuda para el proceso de toma de decisiones de los directivos. En 1938 se señalo en el libro *las funciones del ejecutivo* que la proliferación rápida y creciente de datos exigiría una mayor atención a la calidad de las decisiones, a su vez la calidad en la toma de decisiones depende de la capacidad del directivo para transformar los datos en la información que se ajuste a la perspectiva del mismo para decidir.

En 1.947 algunos investigadores trataron de determinar los procesos que permitieran a los directivos estructurar la información necesaria para la toma de decisiones, estos trabajos junto a la irrupción de los computadores, llevaron en 1.958 a la publicación de un artículo que proporcionó una base conceptual inicial para el análisis del proceso de datos (utilización de los ordenadores para el tratamiento de los datos) y de su influencia en las organizaciones y toma de decisiones, los autores predijeron que la tecnología de la información tendría una importante repercusión organizativa.

De forma progresiva en los años 60 y 70, las empresas trataban de utilizar la tecnología de la información para contrarrestar el aumento del número de datos e información dentro de la empresa, como también las fuertes alzas de costes en personal, energía y materias primas, así se empezó a denotar todas las ventajas que tenia la implementación de tecnología en las empresas.

A finales del siglo XX, los sistemas informáticos se constituyeron en las herramientas más poderosas para materializar uno de los conceptos más vitales y necesarios para cualquier organización empresarial, los sistemas de información de la empresa.

Hoy en día la informática esta sumergida en la gestión integral de la empresa, y por eso las normas y estándares propiamente informáticos deben contribuir

[9] http://www.escet.urjc.es/~ai/T1Apuntes.pdf
http://espanol.geocities.com/audiconsystem/auditori.htm

con el cumplimiento de los objetivos de la empresa, en consecuencia las organizaciones informáticas forman parte de lo que se a denominado el “management” o gestión de la empresa, cabe aclarar que la informática no gestiona propiamente la empresa, ayuda a la toma de decisiones, pero no decide por si misma, por esta razón surge la necesidad de realizar el trabajo de auditoría en las operaciones propias de los ambientes sistematizados.

Aproximadamente hacia el año de 1960, nace la auditoría informática y con ella se busca verificar el uso correcto de los recursos de la empresa y disponer de un eficiente y eficaz sistema de información, es por esto que es necesario entender la empresa en su mas amplio sentido, en la actualidad la mayoría de empresas utilizan la informática para gestionar sus negocios de forma rápida y eficiente, con el fin de obtener beneficios económicos y reducción de costos.

2.3.3. Evolución y cultura de control

La necesidad de planificar a mediano y largo plazo en virtud de la complejidad creciente y de adoptar decisiones racionales en condiciones de mayor incertidumbre, impulsa a las organizaciones a incrementar sus esfuerzos en desarrollar sistemas de información que les permita minimizar esas incertidumbres para la de toma de decisiones.

El nacimiento de estructuras organizacionales cada vez más complejas producto de la creciente especialización o división del trabajo, la proliferación de funciones, la especialización de las personas y la mayor necesidad de coordinación entre ellas, hacen necesario un control de toda la actividad de la organización, que implique la evaluación de la gestión en todos sus niveles y funciones, y les permita operar con eficiencia dentro de las restricciones, minimizar la incertidumbre, responder a las exigencias y aprovechar las oportunidades del ambiente.

Estos factores hacen que a partir de la década del los 60, se fuera incorporando la expresión “Control” al lenguaje propio de la administración, el

cual era conocido como una técnica de seguimiento de las operaciones en las organizaciones a fin de verificar que se actúa ajustándose a lo planificado.

El explosivo desarrollo de las comunicaciones y el avance de la tecnología en general, introdujeron nuevos procesos e instrumentos que afectan la estructura y comportamiento de las organizaciones, disminuyen el costo de acumular información y tener acceso a ella (creación eficiente de bases de datos, la recopilación de información y rápido tratamiento), en ese contexto, el control de gestión se presenta como un proceso, dinámico y permanente, que posibilita reunir, cruzar, relacionar e involucrar elementos componentes del caudal informativo generando así otra información más valiosa y compleja, los indicadores, cuya evolución define el resultado de la gestión.[10]

Hoy en día se entiende por control como un proceso continuo realizado por la dirección, gerencia y otros empleados de la entidad, para proporcionar seguridad razonable, respecto a sí están lográndose los objetivos como: promover la efectividad y eficiencia de la operaciones, proteger y conservar todos los recursos de la organización, cumplir la leyes y reglamentos internos y externos relacionados con la empresa, contar con información confiable en cualquier momento.

La cultura de control define al conjunto de circunstancias que enmarcan el accionar de una entidad desde la perspectiva del control interno, y muestran su importancia sobre la conducta y la administración de una organización.

En toda organización es de vital importancia que haya una persona idónea para gestión e implementación de controles sobre las demás dependencias, en relación a sus funciones, imponiendo disciplina a través de la influencia que ejerce sobre el comportamiento del personal de la organización.

El control interno dentro de una organización constituye el andamiaje para el

[10] http://admindeempresas.blogspot.com/2008/05/evolucion-del-control-de-gestion.html

desarrollo de las acciones y de allí deviene su trascendencia, y como conjunción de medios, operadores y reglas previamente definidas, traduce la influencia colectiva de varios factores en el establecimiento, fortalecimiento o debilitamiento de políticas y procedimientos efectivos en una organización. Los principales factores de la cultura del control son:

- La filosofía y estilo de la dirección y la gerencia.
- La estructura, el plan organizacional, los reglamentos y los manuales de procedimiento.
- La integridad, los valores éticos, la competencia profesional y el compromiso de todos los componentes de la organización, así como su adhesión a las políticas y objetivos establecidos.
- Las formas de asignación de responsabilidades, de administración y desarrollo del personal.
- El grado de documentación de políticas, decisiones, y de formulación de programas que contengan metas, objetivos e indicadores de rendimiento.
- En las organizaciones que lo justifiquen, la existencia de consejos de administración y comités de auditorías con suficiente grado de independencia y calificación profesional.
- El ambiente de control reinante será tan bueno, regular o malo como lo sean los factores que lo determinan. El mayor o menor grado de desarrollo y excelencia de éstos hará, en ese mismo orden, a la fortaleza o debilidad del ambiente que generan y consecuentemente al tono de la organización.

2.3.4. Auditoría informática a entidades de salud[11]

El entorno y los componentes de una entidad de salud generalmente son muy amplios, de acuerdo al nivel al que pertenezca y la variedad de servicios que preste, se hace necesario la implementación de herramientas tecnológicas que le permitan manejar su información de una manera adecuada, igualmente se

[11] Documento HUDN Direccionamiento Estratégico.

requiere de la correcta estructuración y organización de las dependencias, en este tipo de organización generalmente se encuentra en un área denominada auditoría medica, que se encarga de manejar todos los procesos relacionados con la atención de pacientes, y la cual tiene un papel importante en relación a la implementación de módulos asistenciales como lo es el caso de historia clínica, auditoría medica también se encarga se suministrar los informes requeridos por el estado y varían de acuerdo a la región y el país, igualmente es necesario que exista un área encargada del control interno, para regular el funcionamiento de las actividades de la organización.

La auditoría en entidades de salud está dirigida a mejorar los aspectos relacionados con: la prestación de un servicio de salud de calidad, excelencia clínica, equidad, transparencia, buen desenvolvimiento de recurso humano, con el propósito de mejorar la atención a los clientes.

En la actualidad la mayoría de las entidades de salud se encuentran en el proceso de implementación de tecnologías de información en aspectos como:

Sanidad en línea:

- Garantizar la identificación inequívoca de los ciudadanos, mediante un registro único, a través de un código de identificación personal para uso en todo el sistema.
- Impulsar la historia clínica electrónica, y posibilitar el intercambio de información clínica entre diferentes profesionales, dispositivos asistenciales y dependencias de la organización.
- Ofrecer nuevos servicios a los ciudadanos, como cita por Internet, telemedicina y teleformación.

Mayor transparencia:

- Diseñar un sistema de información fiable, oportuno y accesible.
- Seleccionar y definir los indicadores de evaluación sobre: nivel de salud, oferta de recursos, accesibilidad, calidad de la atención y resultados.

- Mejorar e integrar los subsistemas de información existentes.
- Establecer un plan de acceso a los datos y de difusión de la información obtenida, así como la puesta en marcha de foros de comunicación y discusión para profesionales y para ciudadanos.

Para el desarrollo adecuado de estos procesos y el soporte de los mismos, en la actualidad las entidades de salud tienen claro el papel que juega la auditoría no solo en el área de sistemas si no también en sus demás dependencias, ya que permite realizar un proceso de retroalimentación que ayudará a mejorar las actividades de la organización sobre todo cuando existen criterios de acreditación.

2.4. MARCO LEGAL

2.4.1. Aspectos legales sobre la gestión de historia clínica

A. LEY 23 DE 1981 (febrero 18):

Diario Oficial No. 35.711, del 27 de febrero de 1981, por la cual se dictan normas en materia de ética médica, esta norma esta conformada por 94 artículos que hacen referencia a los fines principales de la medicina, la posición del médico en relación a aspectos relacionados con la vida humana, aspectos relacionados con la practica de la profesión y la relación entre médico y paciente, igualmente establece como deben ser las relaciones entre colegas, el capitulo III es muy importante para el objeto de estudio puesto que habla sobre las disposiciones de la prescripción médica, la historia clínica, el secreto profesional y algunas conductas, el capitulo IV trata de las relaciones del médico con las instituciones, trata también de las relaciones entre el médico, sociedad y estado, aspectos sobre la publicidad y la propiedad intelectual y el proceso disciplinario ético profesional.

B. Resolución 1995 de 1999 (julio 8), dada por el ministerio de salud:

Por la cual se establecen normas para el manejo de la historia clínica y considera:

Que conforme al artículo 8 de la Ley 10 de 1990, al Ministerio de Salud le corresponde formular las políticas y dictar todas las normas científico-administrativas, de obligatorio cumplimiento por las entidades que integran el sistema de salud.

Que la ley 100 de 1993, en su Artículo 173 numeral 2, faculta al Ministerio de Salud para dictar las normas científicas que regulan la calidad de los servicios, de obligatorio cumplimiento por parte de todas las entidades promotoras de salud, los prestadores de servicios de salud del sistema general de seguridad social en salud y las direcciones seccionales, distritales y locales de salud. Que el decreto 2174 de 1996, mediante el cual se organizó el sistema obligatorio de garantía de calidad del sistema general de seguridad social en salud, en el numeral 4 del artículo 5, estableció como uno de los objetivos del mismo, estimular el desarrollo de un sistema de información sobre la calidad, que facilitara la realización de las labores de auditoría, vigilancia y control y contribuyera a una mayor información de los usuarios.

Que la historia clínica es un documento de vital importancia para la prestación de los servicios de atención en salud y para el desarrollo científico y cultural del sector.

Que de conformidad con el artículo 35 de la Ley 23 de 1981, corresponde al ministerio de salud implantar modelos relacionados con el diligenciamiento de la historia clínica en el sistema nacional de salud.

Que se hace necesario expedir las normas correspondientes al diligenciamiento, administración, conservación, custodia y confidencialidad de las historias clínicas, conforme a los parámetros del ministerio de salud y del archivo general de la nación en lo concerniente a los aspectos archivísticos contemplados en la ley 80 de 1989.

De manera general se encuentra que la ley establece:

Articulo 1. Definiciones: La historia clínica es un documento privado, obligatorio y sometido a reserva, en el cual se registran cronológicamente las condiciones de salud del paciente, los actos médicos y los demás procedimientos ejecutados por el equipo de salud que interviene en su atención.

Articulo 2. Ámbito de aplicación: Estas disposiciones incluye todos los prestadores de servicios de salud y demás personas naturales o jurídicas que se relacionen con la atención en salud.

Articulo 3. Características de la historia clínica:

- Integralidad: La historia clínica de un usuario debe reunir la información de los aspectos científicos, técnicos y administrativos relativos a la atención en salud.

- Secuencialidad: Los registros de la prestación de los servicios en salud deben consignarse en la secuencia cronológica en que ocurrió la atención.

- Racionalidad científica: El diligenciamiento y registro de las acciones en salud brindadas a un usuario, deben ser en forma lógica, clara y completa, el procedimiento que se realizó en la investigación de las condiciones de salud del paciente, diagnóstico y plan de manejo.

- Disponibilidad: Es la posibilidad de utilizar la historia clínica en el momento en que se necesita, con las limitaciones que impone la ley.

- Oportunidad: Es el diligenciamiento de los registros de atención de la historia clínica, simultánea o inmediatamente después de que ocurre la prestación del servicio.

Articulo 4. Obligatoriedad del registro: Los profesionales, que atienden un usuario, tienen la obligación de registrar sus observaciones, conceptos, decisiones y resultados de las acciones en salud desarrolladas.

Articulo 5. Generalidades: La historia clínica debe diligenciarse en forma clara, legible, sin tachones, enmendaduras, intercalaciones, sin dejar espacios en blanco y sin utilizar siglas.

*Articulo 6. Apertura e identificación de la historia clínica: T*odo prestador de servicios de salud que atiende por primera vez a un usuario debe realizar el proceso de apertura de historia clínica, a partir del primero de enero del año 2000, la identificación de la historia clínica se hará con el número de la cédula de ciudadanía para los mayores de edad; el número de la tarjeta de identidad para los menores de edad mayores de siete años, y el número del registro civil para los menores de siete años. Para los extranjeros con el número de pasaporte o cédula de extranjería. En el caso en que no exista documento de identidad de los menores de edad, se utilizará el número de la cédula de ciudadanía de la madre, o el del padre en ausencia de ésta, seguido de un número consecutivo de acuerdo al número de orden del menor en el grupo familiar.

Articulo 7. Numeración consecutiva de la historia clínica: Todos los folios que componen la historia clínica deben numerarse en forma consecutiva.

Articulo 8. Componentes Son componentes de la historia clínica, la identificación del usuario, los registros específicos y los anexos.

Articulo 9. Identificación del Usuario: Los contenidos mínimos de este componente son: datos personales de identificación del usuario, apellidos y nombres completos, estado civil, documento de identidad, fecha de nacimiento, edad, sexo, ocupación, dirección y teléfono del domicilio y lugar de residencia, nombre y teléfono del acompañante; nombre, teléfono y parentesco de la

persona responsable del usuario, según el caso; aseguradora y tipo de vinculación.

Articulo 10. Registros específicos: Registro específico es el documento en el que se consignan los datos e informes de un tipo determinado de atención. El prestador de servicios de salud debe seleccionar para consignar la información de la atención en salud brindada al usuario, los registros específicos que correspondan a la naturaleza del servicio que presta.

Articulo 11. Anexos: Son todos aquellos documentos que sirven como sustento legal, técnico, científico y/o administrativo de las acciones realizadas al usuario en los procesos de atención, tales como: autorizaciones para intervenciones quirúrgicas (consentimiento informado), procedimientos, autorización para necropsia, declaración de retiro voluntario y demás documentos que las instituciones prestadoras consideren pertinentes.

Articulo 12. Obligatoriedad del archivo: Todos los prestadores de servicios de salud, deben tener un archivo único de historias clínicas en las etapas de archivo de gestión, central e histórico, el cual será organizado y prestará los servicios pertinentes guardando los principios generales establecidos en el acuerdo 07 de 1994, referente al reglamento general de archivos, expedido por el archivo general de la nación y demás normas que lo modifiquen o adicionen.

Articulo 13. Custodia de la historia clínica: La custodia de la historia clínica estará a cargo del prestador de servicios de salud que la generó en el curso de la atención, cumpliendo los procedimientos de archivo señalados en la presente resolución, sin perjuicio de los señalados en otras normas legales vigentes.

Articulo 14. Acceso a la historia clínica: Podrán acceder a la información contenida en la historia clínica, en los términos previstos en la ley:

- El usuario.

- El Equipo de salud.
- Las autoridades judiciales y de salud en los casos previstos en la ley.
- Las demás personas determinadas en la ley.

Articulo 15. Retención y tiempo de conservación: La historia clínica debe conservarse por un periodo mínimo de 20 años contados a partir de la fecha de la última atención. Mínimo cinco (5) años en el archivo de gestión del prestador de servicios de salud, y mínimo quince (15) años en el archivo central, una vez transcurrido el término de conservación, la historia clínica podrá destruirse.

Articulo 16. Seguridad del archivo de historias clínicas: El prestador de servicios de salud, debe archivar la historia clínica en un área restringida, con acceso limitado al personal de salud autorizado, conservando las historias clínicas en condiciones que garanticen la integridad física y técnica, sin adulteración o alteración de la información.

Articulo 17. Condiciones físicas de conservación de la historia clínica: Los archivos de historias clínicas deben conservarse en condiciones locativas, procedimentales, medio ambientales y materiales, propias para tal fin, de acuerdo con los parámetros establecidos por el archivo general de la nación en los acuerdos 07 de 1994, 11 de 1996 y 05 de 1997, o las normas que los deroguen, modifiquen o adicionen.

Articulo 18. De los medios técnicos de registro y conservación de la historia clínica. Los prestadores de servicios de salud pueden utilizar medios físicos o técnicos como computadoras y medios magneto-ópticos, cuando así lo consideren conveniente, atendiendo lo establecido en la circular 2 de 1997 expedida por el archivo general de la nación, o las normas que la modifiquen o adicionen.

Articulo 19. Definición: Defínase el comité de historias clínicas como el conjunto de personas que al interior de una institución prestadora de servicios de salud,

se encarga de velar por el cumplimiento de las normas establecidas para el correcto diligenciamiento y adecuado manejo de la historia clínica.

Articulo 20. Funciones del comité de historias clínicas: Promover en la institución la adopción de las normas nacionales sobre historia clínica y velar porque estas se cumplan, elaborar, sugerir y vigilar el cumplimiento del manual de normas y procedimientos de los registros clínicos del prestador, incluida la historia clínica.

Articulo 21. Sanciones: Los prestadores de servicios de salud que incumplan lo establecido en la presente resolución, incurrirán en las sanciones aplicables de conformidad con las disposiciones legales vigentes.

C. Resolución 3881 de 1982 por la cual se reglamenta parcialmente el decreto 526 de 1975:

Esta norma hace referencia a aspectos como:

- Necesidad de la creación de un comité de historia clínica.
- Registro obligatorio de las condiciones del paciente.
- Diligenciamiento de historia clínica con claridad.
- Implantación de formularios y manual de normas y procedimientos y prestar sus servicios en base a este manual.
- Normas del diligenciamiento de historia clínica.
- Capacitación del personal.

2.4.2. Aspectos Legales de contratación y seguridad informática

A. Ley 527 de 1999 El principal problema al que se ve enfrentada la humanidad ante la nueva realidad que se le presenta es la carencia de un marco regulatorio adecuado y homogéneo que comprenda todas las dificultades que el tráfico comercial genera entre los distintos países, ya que tal vez el mayor obstáculo para la expansión de las diversas operaciones electrónicas es la

sensación de inseguridad que experimentan los consumidores, empresarios y usuarios a la hora de transmitir sus datos confidenciales.

Mecanismos de seguridad para las transacciones a través de internet: Encriptación de documentos: una de las formas de conseguir que los datos transferidos solamente puedan ser interpretados correctamente por el emisor del mismo y por el receptor al que va dirigido, de forma tal que el mensaje viaje seguro desde la fuente al destino, siendo imposible la interceptación por terceros del mensaje, o que si se produce ésta, el mensaje capturado sea incomprensible para quien tenga acceso al mismo.

Firma digital: “el conjunto de datos, en forma electrónica, anexos a otros datos electrónicos o asociados funcionalmente con ellos, utilizados como medios para identificar formalmente al autor o autores del documento que la recoge”.

Autoridades de certificación: realizan la comprobación de que la clave pública de un usuario, cuyo conocimiento es imprescindible para autenticar su firma electrónica,, y que pertenece realmente a este, haciéndolo constar y dando fe pública de ello en el certificado digital que para el efecto expiden.

- *Tratamiento legal de los dispositivos de seguridad.*
- Estándares internacionales.
- Ley modelo de la firma electrónica: UNCITRAL.
- Cámara de comercio internacional.
- Legislación vigente:
  - Unión europea: Directiva 99/93 del consejo de Europa.
  - Estados unidos: Electronic signature in global and national commerce
- Colombia: Ley 527 de 1999.

Problemática y desafío:

- Confianza y seguridad de la web como mayor activo.
- La diversidad de los sistemas normativos en un mundo globalizado.

- Desafío: adaptación de sistemas jurídicos y reducción del derecho a un único sistema legal: Importancia de los procesos comunitarios.

La subsistencia de la red depende de la creación de una estructura subyacente de seguridad, cuyos fundamentos estén dados tanto por los avances tecnológicos, como por la normatividad jurídica. En este sentido, y como se expuso a lo largo de este trabajo, la regulación de instrumentos de seguridad como los sistemas de encriptación, la firma digital y las autoridades de certificación, proporciona y garantiza la confiabilidad de las transacciones, piedra angular del nuevo modelo económico implantado. Es así como se deduce que la creación de un sistema confiable que brinde niveles de seguridad apropiados, debe incorporar la tecnología a través de equivalentes funcionales jurídicos en único ordenamiento jurídico global con validez y aplicabilidad universal.

B. Ley 80:

Dictada en (octubre 28) por la cual se expide el estatuto general de contratación de la administración pública el congreso de Colombia, decreta:

Articulo 1º

La presente ley tiene por objeto disponer las reglas y principios que rigen los contratos de las entidades estatales.

Articulo 2º De la definición de entidades, servidores y servicios públicos, para los efectos de esta ley: Se denominan entidades estatales: La nación, las regiones, los departamentos, las provincias, el distrito capital y los distritos especiales, las áreas metropolitanas, las asociaciones de municipios, los territorios indígenas y los municipios; los establecimientos públicos, las empresas industriales y comerciales del estado, las sociedades de economía mixta en las que el estado tenga participación superior al cincuenta por ciento (50%), así como las entidades descentralizadas indirectas y las demás personas jurídicas en las que exista dicha participación pública mayoritaria, cualquiera sea la denominación que ellas adopten, en todos los órdenes y niveles.

C. Cecua: Confederación de asociaciones europeas de usuarios de tecnologías de la información, esta es una herramienta que brinda algunos criterios a tener en cuenta en relación a la contratación informática y aspectos de contratantes, la parte expositiva, las cláusulas o pactos que se convengan en donde se deben incluir la mayor parte de de situaciones que se puedan originar dentro del convenio, deberes y aseguramiento, plazos de cumplimientos, formación del usuario, prohibición de sub arrendar, sustitución del equipo, definición de términos o conceptos oscuros, mantenimiento y garantías.

D. Ley 1150: La ley 1150 de 2007 fue expedida el 16 de julio, por medio de la cual se introducen medidas para la eficiencia y la transparencia en la ley 80 de 1993 y se dictan otras disposiciones generales sobre la contratación con recursos públicos.

De manera general se decreta en su articulo 1, que la presente ley tiene por objeto introducir modificaciones en la ley 80 de 1993, así como dictar otras disposiciones generales aplicables a toda contratación con recursos públicos, en su articulo 2 no habla sobre reglas relacionadas para las modalidades de selección en relación a la escogencia del contratista.

2.5. MARCO TEORICO

2.5.1. Aspectos generales sobre auditoría[12]

De manera general se podría decir que la auditoría se define como «un proceso sistemático para obtener y evaluar de manera objetiva las evidencias relacionadas con informes sobre actividades económicas y otros acontecimientos relacionados, cuyo fin consiste en determinar el grado de correspondencia del contenido informativo con las evidencias que le dieron origen, así como establecer si dichos informes se han elaborado observando los principios establecidos para el caso».

[12] ARENS,Alvin A.Auditoría Un Enfoque Integral.6 ed.México: Prentice Hall,1996

Con la auditoría se busca encontrar y evaluar evidencias, es realizado por una persona independendiente y competente acerca de la información cuantificable de una entidad especifica, con el propósito de determinar e informar sobre el grado de correspondencia existente entre la información cuantificable y los criterios establecidos. De igual manera detecta todos los puntos de control en las diferentes dependencias que son críticas.

Objetivos generales de una auditoría de sistemas:

- Buscar una mejor relación costo-beneficio de los sistemas automáticos o computarizados diseñados e implantados.
- Incrementar la satisfacción de los usuarios de los sistemas computarizados.
- Asegurar una mayor integridad, confidencialidad y confiabilidad de la información mediante la recolección de seguridades y controles.
- Conocer la situación actual del área de sistemas y las actividades y esfuerzos necesarios para lograr los objetivos propuestos.
- Seguridad del personal, datos, hardware, software, e instalaciones.
- Apoyo de función información a las metas y objetivos de la institución.
- Seguridad, utilidad, confianza, privacidad, y disponibilidad en el ambiente informático.
- Minimizar existencias de riesgos en el uso de tecnologías de información.
- Decisiones de inversión y gastos innecesarios.
- Capacitación y educación sobre controles en los sistemas.

2.5.2. Tipos de auditoria

Existe una amplia clasificación de las auditorías entre ellas se encuentra:[13]

[13] http://www.mitecnologico.com/Main/TiposDeAuditoría
http://www.galeon.com/anaranjo/tipos_audi.htm

Según los objetivos que persiguen las auditorías se clasifican en:

Auditoría financiera: Consiste en la revisión, critica de los controles y la determinación de veracidad de los estados financieros de una empresa, es realizada generalmente por un contador publico, donde se concluye un concepto sobre estos registros.

Auditoría operacional: Es la valoración independiente de todas las operaciones de una empresa, en forma analítica objetiva y sistemática, para determinar si se lleva a cabo políticas y procedimientos aceptables, si se siguen las normas establecidas y si se utilizan los recursos de manera eficaz y económica, la evaluación se enfoca a aspectos como: eficiencia, eficacia, economía, de los métodos y procedimientos que rigen los procesos de la empresa.

Auditoría de sistemas de información: Con el avance y comercialización de las tecnologías, surgió también la necesidad de realizar auditorías sobre los sistemas de tratamiento de información. En este sentido se podría decir que la auditoría informática comprende el conjunto de actividades encaminadas a la validación y verificación de los sistemas, procesos y resultados en los que se utilicen tecnologías automatizadas, ya sea en cumplimiento de la legislación, como garantía de la integridad de la información aportada por un sistema o por alineamiento con determinados estándares relacionados con el buen uso de los sistemas.

Auditoría fiscal: Se dedica a observar y verificar el cumplimiento de las leyes fiscales como el pago de impuestos, obligaciones fiscales, o estudia entidades como: tesorerías de hacienda estatales o tesorerías municipales.

Auditoría administrativa: Realiza una evaluación completa y constructiva de la estructura organizativa de una entidad social, es realizada por un profesional de la administración, con el fin de evaluar la eficiencia de sus resultados, sus

metas fijadas con base en la organización, los recursos humanos, financieros, materiales, como también los métodos y controles en sus operaciones.[14]

De acuerdo a las personas que la realizan: [15]

Auditoría externa: Es una examen crítico, sistemático y detallado de un sistema de información de una empresa, realizado por una persona sin vínculos laborales con la misma, utilizando técnicas determinadas y con el objeto de emitir una opinión independiente sobre la forma como opera el sistema, el control interno del mismo y formular sugerencias para su mejoramiento. El dictamen u opinión independiente tiene trascendencia a los terceros, ya que da plena validez a la información generada por el sistema, emitiendo recomendaciones y sugerencias para el mejoramiento del sistema.

Auditoría interna: De manera similar es una evaluación sistemática y detallada sobre el sistema de una empresa, la cual es realizada por una persona que posee vínculos laborales con la misma, utilizando técnicas y herramientas, que permitirán emitir sugerencias para el mejoramiento de los diferentes procesos de la entidad auditada y la toma de decisiones.

2.5.3. Auditoría informática[16]

La auditoría informática es el proceso de recoger, agrupar y evaluar evidencias para determinar si el sistema realiza una correcta gestión de la información, mediante esta evaluación se busca mantener la integridad de los datos, utilizar eficientemente los recursos del sistema y cumplir eficazmente con los fines de la organización.

Auditar consiste principalmente en estudiar los mecanismos de control que están implantados en una empresa u organización, determinando si los mismos

[14] http://www.galeon.com/anaranjo/tipos_audi.htm,

[15] http://html.rincondelvago.com/auditoría_3.html

[16] http://www.monografias.com/trabajos39/la-auditoría/la-auditoría.shtm

son adecuados y cumplen unos determinados objetivos o estrategias, estableciendo los cambios que se deberían realizar para la consecución de los mismos, los mecanismos de control pueden ser directivos, preventivos, de detección, correctivos o de recuperación ante una contingencia.

Los objetivos que persigue la auditoría informática son:

- El control de la función informática
- El análisis de la eficiencia de los sistemas informáticos
- La verificación del cumplimiento de la normativa en este ámbito
- La revisión de la eficaz gestión de los recursos informáticos.
- Mejorar la eficacia de la organización informática y proteger sus activos y recursos (seguridad, políticas, normas)
- Garantizar resultados fiables en tiempo, coste y utilidad de los sistemas de información.
- Mejorar los procedimientos, estándares y planificación, colaborando en su diseño y en la actualización de sus normas.

Partiendo de las diversas actividades que se llevan a cabo en las oficinas de sistemas o informática de las empresas, se han establecido las principales divisiones de la auditoría informática como:

Auditoría informática de producción o explotación: Auditar la producción, operación o explotación consiste en revisar las secciones que la componen y sus interrelaciones, las cuales generalmente son: planificación, producción y soporte técnico, igualmente se encarga de realizar listados, ordenes automatizadas, resultados informáticos para incluir o modificar procesos, la producción o explotación informática dispones de elementos importantes como los datos, los cuales serán transformados y serán sometidos a controles para verificar su integridad y calidad, una ves se encuentren las vulnerabilidades deben ser dadas a conocer al personal administrativo encargado de la implementación de controles y la toma de decisiones.

Auditoría informática de desarrollo de proyectos: La auditoría en este campo se debe aplicar a sus diferentes etapas como: recolección de los requerimientos, análisis, diseño, desarrollo (programación), implantación y pruebas entre otros, con el fin de detectar aquellos riesgos y vulnerabilidades para establecer los juicios y recomendaciones necesarias a seguir en el desarrollo de cada etapa, permitiendo realizar una entrega oportuna y la satisfacción del usuario.

Auditoría informática de sistemas: Se ocupa de analizar y revisar los controles, la efectividad y eficacia del entorno general de sistemas, el cual incluye sistemas operativos, software básico, aplicaciones, administración de base de datos, infraestructura física, lógica y sistemas de seguridad.

Auditoría informática de comunicaciones y redes: Este tipo de revisión se enfoca en las redes tanto computacionales como telefónicas, líneas, concentradores, multiplexores, etc, generalmente se requiere de personal especializado en el área de redes y comunicaciones, donde se estudiaran los casos de: topologías de red, uso, cantidad y ubicación de los puntos existentes, con el fin de encontrar las debilidades y establecer lo controles necesarios.

Auditoría de la seguridad informática: La auditoría de la seguridad en la informática abarca los conceptos de seguridad física y lógica. La seguridad física se refiere a la protección del hardware, protección de la red física y la seguridad de los edificios e instalaciones que los albergan. La seguridad lógica se refiere a la seguridad en el uso de software, la protección de la información, procesos y aplicaciones, control y gestión de usuarios.

Auditoría informática para aplicaciones en internet: Esta auditoría se realiza con el fin de detectar cuales son los riesgos de internet en relación a aspectos operativos, tecnológicos y su probabilidad de ocurrencia, igualmente detectar las vulnerabilidades en relaciona la arquitectura de seguridad implementada, y para verificar la confidencialidad de las aplicaciones y la publicidad negativa como consecuencia de ataques exitosos por parte de hackers.

2.5.4. Aspectos que evalúa la auditoría informática

Dentro del trabajo de auditoría de sistemas es importante que auditor analice y evalué aspectos relacionados con la seguridad tanto física como lógica, el control interno, la efectividad, la gestión de campo, la integridad de la información, la infraestructura física, la gestión de riesgos y la continuidad de las operaciones.

Igualmente pueden existir otros factores a evaluar, esto dependerá de las necesidades de la Institución, de su sistema de información y su entorno, de manera general existen una serie de elemento importante para evaluar como:

- Verificación de control interno, tanto de las aplicaciones como de los sistemas de información.
- Análisis de la gestión de los sistemas de información desde un punto de vista de riesgo de seguridad, de gestión y de efectividad de gestión e infraestructura física.
- Análisis de la gestión de los riesgos de la información y de la seguridad implícita.
- Análisis de la integridad, fiabilidad y certeza de la información a través del análisis de las aplicaciones. Esta función que la vienen desempeñando los auditores informáticos, están empezando a desarrollarla los auditores financieros.

2.5.4.1. Auditoría de la seguridad informática

La seguridad sigue siendo el área principal a auditar, o por la que se debe auditar una empresa, la importancia de la información especialmente relacionada con sistemas basados en el uso de tecnologías de la información y comunicaciones, por el impacto en los fallos, los accesos no autorizados, la revelación de la información y otras incidencias. Si no existen suficientes y adecuadas medidas de protección se puede perder información vital, o al

menos no esta disponible en el momento requerido. Generando una toma de decisiones erróneas.[17]

Al hablar de seguridad siempre se habla de sus tres dimensiones, confidencialidad, integridad, y disponibilidad de la información, y algunos controles van mas dirigidos a tratar de garantizar alguna de estas características:

La confidencialidad: Solo se cumple cuando las personas autorizadas (en un sentido amplio se puede referir tan bien a sistemas) pueden conocer los datos o la información correspondiente.

La integridad: Consiste en que solo los usuarios autorizados puedan variar (modificar, borrar) los datos. Deben quedar pistas para control posterior y para auditoría.

La disponibilidad: Se alcanza si las personas autorizadas pueden acceder a tiempo a la información a la que están autorizadas.

2.5.4.2. Auditoría de la seguridad física

Se evalúa las protecciones físicas de los datos, instalaciones, equipos, redes, soportes, considerando también a las personas, que estén protegidas y existan medidas de evacuación, alarmas, salidas alternativas, así como que no existen expuestas a riesgos superiores a los considerados admisibles en la entidad e incluso en el sector.[18]

Las amenazas pueden ser muy diversas: sabotaje, vandalismo, terrorismo, accidentes de distinto tipo, incendios, inundaciones, averías importantes, derrumbamientos, explosiones, así como otros que afectan a las personas y pueden impactar el funcionamiento de los centros, tales como errores,

[17] http://www.delitosinformaticos.com/propiedadindustrial/auditoría.shtml
[18] http://web.bemarnet.es/seguridad.html

negligencias, huelgas, desde las perspectivas de las protecciones físicas algunos aspectos a considerar son:

- Estructura, diseño construcción y distribución de los edificios y de sus plantas.
- Amenazas de fuego (materiales empleados), riesgos por agua, accidentes atmosféricos o por averías en las conducciones, problemas en el suministro eléctrico, tanto por caídas como por perturbaciones.
- Controles tanto preventivos como de detección, relacionados con los puntos anteriores, así como de acceso basándose en la clasificación de áreas según usuarios.
- Control de los soportes magnéticos en cuanto a acceso, almacenamiento y posible transporte, además de otras protecciones no fiscal, todo bajo un sistema de inventario, así como protección de documentos impresos y de cualquier tipo de documentación clasificada.

2.5.4.3 Auditoría de la seguridad lógica

La seguridad lógica se refiere a la seguridad de uso de software, a la protección de los datos, procesos y programas, así como la del ordenado y autorizado acceso de los usuarios a la información.[19]

Es necesario verificar que cada usuario solo pueda acceder a los recursos a los que le autoricé el propietario, aunque sea de forma genérica, según su función, y con las posibilidades que el propietario haya fijado: lectura, modificación, borrado, ejecución. Desde el punto de vista de la ejecución, es necesario revisar como se identifican y sobre todo autentican los usuarios, como han sido autorizados y por quien, y que ocurre cuando se producen transgresiones o intentos: quien se entera y cuando se hace.

Algunos aspectos a evaluar con respecto a las contraseñas pueden ser:

- Quien asigna la contraseña inicial y las sucesivas.

[19] http://www.monografias.com/trabajos/auditoinfo/auditoinfo.shtml

- Protección o cambio de las contraseñas iniciales que llegan en los sistemas, y que a menudo aparecen en los propios manuales.
- Si las contraseñas están cifradas y bajo que sistema, y sobre todo que no aparezcan en claro en las pantallas, listados, mensajes de comunicaciones o corrientes de trabajos.
- Vigencia, incluso puede haberlas de un solo uso o dependencias de una función tiempo.

Con el incremento de agresiones a instalaciones informáticas en los últimos años, se han ido originando acciones para mejorar la seguridad informática a nivel físico. Los accesos y conexiones indebidos a través de las redes de comunicaciones, han acelerado el desarrollo de productos de seguridad lógica y la utilización de sofisticados medios criptográficos.

El sistema integral de seguridad debe comprender:

- Elementos administrativos.
- Definición de una política de seguridad.
- Organización y división de responsabilidades.
- Seguridad física y contra catástrofes (incendios, terremotos, catástrofes).
- Practicas de seguridad del personal.
- Elementos técnicos y procedimientos.
- Sistemas de seguridad (equipos y de sistemas, incluyendo todos los elementos tanto redes como terminales).
- Aplicación de los sistemas de seguridad, incluyendo datos y archivos.
- El papel de los auditores, tanto internos como externos.

La decisión de abordar una auditoría informática de seguridad global en una empresa o institución, se fundamenta en el estudio cuidadoso de los riesgos potenciales a los que esta sometida. Se fundamenta en el estudio cuidadoso de los riesgos potenciales a los que esta sometida. Se elaboran “matrices de riesgo”, en donde se consideran los factores de las “amenazas” a las que esta sometida una instalación y los “impactos” que aquellas puedan causar cuando

se presentan, las matrices de riesgo se representan en cuadros de doble entrada <<amenaza _ impacto>> en donde se evalúan las probabilidades de ocurrencia de los elementos de la matriz.

Los grandes grupos de controles son los siguientes, además de poderlos dividir en manuales y automáticos, o en generales y de aplicación.

Directivos: Son los que establecen las bases, como las políticas, o la creación de comités relacionados o de funciones de administración de seguridad o auditoría de sistemas de información interna.

Preventivos: Antes del hecho, como la identificación de visitas (seguridad física), o las contraseñas (seguridad lógica).

De detención: Como determinadas revisiones de accesos producidos a la detección de incendios.

Correctivos: Para rectificar errores, negligencias o acciones intencionadas, como la recuperación de un archivo dañado a partir de una copia.

Recuperación: Que facilitan la vuelta a la normalidad después de accidentes o contingencias, como puede ser un plan de continuidad adecuado.

2.5.5. Metodología de trabajo de auditoría informática

Se requieren de varias etapas para realizar la auditoría, cada una de ellas cumple un papel importante, por tal razón cada una de ellas debe realizarse con profundidad e integridad

De manera general una vez identificado el objeto de investigación, el auditor de sistemas debe realizar un estudio preliminar que le permita evaluar los riesgos globales para poder desarrollar y establecer un programa de auditoría, el cual

constara de objetivos de control y procedimientos de auditoría que deben satisfacer esos objetivos.

El proceso de auditoría exige que el auditor de sistemas reúna evidencia, evalúe a través de herramientas apropiadas las fortalezas y debilidades de los controles existentes basado en la evidencia recopilada, y de acuerdo a criterios o estándares se concluya cual es la situación de cada elemento auditado identificando los riesgos y vulnerabilidades, dando como resultado las recomendaciones necesarias, donde se indique cual es la situación actual, y cuales serian los controles necesarios a seguir para evitar o disminuir el riesgo, una ves terminado este proceso es necesario preparar un informe de auditoría, que presente estos temas en forma objetiva a la gerencia, igualmente la gerencia de auditoría debe garantizar una disponibilidad y asignación adecuada de recursos para realizar el trabajo de auditoría además de las revisiones de seguimiento sobre las acciones correctivas emprendidas por la gerencia.
Se han identificado las siguientes etapas para la realización de la auditoría:[20]

- Identificación del objeto de estudio.
- Definición de alcances y objetivos.
- Estudio inicial del entorno auditable.
- Determinación de los recursos necesarios para realizar la auditoría.
- Elaboración del programa de auditoría.
- Ejecución de la auditoría (realización de actividades propiamente dichas de la auditoría).
- Determinación de hallazgos y realización de recomendaciones.
- Elaboración del informe final.
- Elaboración de carta de presentación del informe final.

2.5.5.1. Identificación del objeto de estudio

Toda empresa u organización dentro de su estructura administrativa y jerárquica se encuentra conformada por áreas o dependencias, las cuales

[20] http://www.monografias.com/trabajos39/la-auditoría/la-auditoría.shtml

tienen unas actividades y funciones establecidas, dentro de estas áreas se encuentra la oficina encargada de la gestión de información y sistemas, generalmente esta área involucra la realización de diferentes actividades y procesos que requieren de un alto grado de organización como el establecimiento de políticas, planes, definición de procesos, correcta delimitación de funciones de su recurso humano, definición de elementos de entorno entre otros, por tal razón y por la complejidad de su cobertura es de gran importancia que las empresas públicas y privadas y más aun las empresas prestadoras de salud, definan dentro de sus políticas administrativas la elaboración periódica de auditoría de sistemas, con el fin de contribuir en la mejora continua de la gestión de los mismos y su impacto en relación a las áreas con las que se relaciona, contribuyendo con el cumplimiento de la misión y visión de la organización.

De esta forma se hace necesario que la administración o gerencia de una determinada empresa puntualicen continuamente el entorno a auditar en relación a las dependencia que la conforman, de acuerdo a la actividad a la que se dedica y objetivos que persigue, teniendo en cuenta que con las exigencias del avance tecnológico, día a día son más las empresas que se tecnifican y sistematizan, la administración y gerencia de las mismas tienen que ser concientes de la definición constantes de auditorías para el buen funcionamiento de este entorno, que esta sujeto a los continuos cambios y avances tecnológicos y científicos.

2.5.5.2. Definición de alcances y objetivos[21]

Una vez definido el objeto a auditar, en el caso de esta investigación el área de sistemas de información, se planteara la realización de una auditoría de tipo interno o externo, en donde el auditor de sistemas pasa a establecer la cobertura de la auditoría y la definir los limites de la misma, es de gran importancia resaltar de que se debe generar una buena comunicación entre auditor de sistemas y los clientes, ya que esto permitirá que exista un mutuo

[21] http://www.monografias.com/trabajos39/la-auditoría/la-auditoría.shtml

acuerdo sobre las funciones, los elementos, las áreas y las organizaciones a auditar, permitiendo ser concretos en la realización de la auditoría tomando un correcto enfoqué, en donde se administre bien el tiempo del desarrollo del trabajo, evitando la dilatación de las actividades de evaluación en temas que no tienen importancia, relación e impacto.

Es necesario conformar una documentación completa desde el inicio de las actividades, por tal razón dentro del informe final, se deben definir los alcances y las excepciones de la auditoría, permitiendo así documentar de forma integral el proceso de auditoría.

De forma paralela el auditor de sistemas debe encargarse de apropiarse del entorno a auditar para poder definir claramente los objetivos de la auditoría, debe preocuparse por comprender los deseos y sugerencias del cliente, de forma que los objetivos planteados puedan ser alcanzados, permitiendo así definir el objetivo global y los objetivos específicos, que de igual forma se incluirán en el informe final de la auditoría.

2.5.5.3. Estudio inicial del entorno auditable[22]

Esta es una de las etapas más complejas de la auditoría, ya que el auditor se debe encargar de conocer todo el entorno del sistema de información, en relación a software de aplicación y la base de datos, el hardware e infraestructura física, las funciones administrativas del recurso humano de la oficina de sistemas, el papel de los usuarios frente al sistema de información, la seguridad física y lógica entre otros. De esta forma se establece que el auditor debe encargarse del estudio pleno de:

Organización:

En donde el auditor de sistemas debe investigar y conocer sobre aspectos como:

[22] http://www.monografias.com/trabajos39/la-auditoría/la-auditoría.shtml

Organigrama: El organigrama expresa la estructura oficial de la organización a auditar, que permite determinar la organización jerárquica, las dependencias y direcciones entre áreas.

Departamentos: Se entiende como departamento a los órganos que siguen inmediatamente a la dirección, el equipo auditor describirá brevemente las funciones de cada uno de ellos en relación con el objeto de estudio.

Relaciones jerárquicas y funcionales entre órganos de la organización: El equipo auditor verificará si se cumplen las relaciones funcionales y jerárquicas previstas por el organigrama, o por el contrario detectará, si existe una mala dependencia de cargos en relación a jefes y niveles, a través de las jerarquías se evidencia la correspondiente subordinación y las funciones que indican las relaciones no estrictamente subordinables.

Flujos de información: Además de las corrientes verticales intradepartamentales, la estructura organizativa cualquiera que sea, produce corrientes de información horizontales y oblicuas extra departamentales, los flujos de información entre los grupos de una organización son necesarios para su eficiente gestión, siempre y cuando tales corrientes no distorsionen el propio organigrama. En ocasiones, las organizaciones crean espontáneamente canales alternativos de información, sin los cuales las funciones no podrían ejercerse con eficacia; estos canales alternativos se producen porque hay pequeños o grandes fallos en la estructura y en el organigrama que los representa, otras veces, la aparición de flujos de información no previstos obedece a afinidades personales o simple comodidad. Estos flujos de información son indeseables y producen graves perturbaciones en la organización.

Número de puestos de trabajo: El equipo auditor comprobará que los nombres y los puestos de trabajo de la organización corresponden a las funciones reales distintas, es frecuente que bajo nombres diferentes se realicen funciones

idénticas, lo cual indica la existencia de funciones operativas redundantes, esta situación pone de manifiesto deficiencias estructurales; los auditores darán a conocer tal circunstancia y expresarán el número de puestos de trabajo verdaderamente diferentes.

Número de personas por puesto de trabajo: Es un parámetro que los auditores informáticos deben considerar, la inadecuación del personal determina que el número de personas que realizan las mismas funciones rara vez coincida con la estructura oficial de la organización.

Entorno operacional:

El equipo de auditoría informática debe poseer una adecuada referencia del entorno en el que va a desenvolverse, esto a través del conocimiento previo de:

Situación geográfica de los sistemas: En el caso que la empresa funcione con oficinas alternas o sucursales, se hace necesario la ubicación geográfica de los centros de procesos de datos en la empresa, la ubicación de los responsables o encargados, y la verificación de los mismos estándares de trabajo.

Arquitectura y configuración de hardware y software: En el caso de existir redes y el uso de varios equipos de cómputo, los auditores deben tener en su poder la distribución e interconexión de los equipos, igualmente es fundamental la configuración elegida para cada uno de ellos, ya que los mismos deben constituir un sistema compatible e intercomunicado, y se debe encontrar ligada a las políticas de seguridad lógica de las compañías.

Inventario de hardware y software: El grupo auditor debe revisar toda la información escrita, en donde figuren todos los elementos físicos y lógicos de la instalación, en relación a hardware figurarán las CPUs, unidades de control locales y remotas, periféricos de todo tipo, etc. El inventario de software debe contener todos los productos lógicos del Sistema, desde el software básico

hasta los programas de utilidad adquiridos o desarrollados internamente generalmente clasificados en facturables y no facturables.

Comunicación y redes de comunicación: En el estudio inicial los auditores dispondrán del número, situación y características principales de las líneas, así como de los accesos a la red pública de comunicaciones, Igualmente, poseerán información de los diferentes tipos de redes con los que cuente la empresa.

Aplicaciones, bases de datos y ficheros

El estudio inicial que han de realizar los auditores se cierra y culmina con una idea general de los procesos informáticos realizados en la empresa auditada. Para ello deberán conocer lo siguiente:

Volumen, antigüedad y complejidad de las aplicaciones: Con el fin de determinar cual es arquitectura del sistema de información, su evolución y los cambios que a sufrido, su manejo y funcionamiento lógico.

Metodología del diseño: En donde es necesario determinar la existencia total o parcial del tipo de metodología usada en el desarrollo de las aplicaciones o verificar si existen el uso de más de 1 metodología.

Documentación: La existencia de una adecuada documentación de las aplicaciones, procesos y funciones, proporciona beneficios tangibles e inmediatos muy importantes, la documentación de programas disminuye gravemente el mantenimiento de los mismos.

Cantidad y complejidad de bases de datos y ficheros: El auditor deberá investigar información relacionada con las características de las bases de datos, clasificándolas en relación y jerarquías, determinara un promedio de número de accesos a ellas por hora o días, como también en los archivos

verificando la frecuencia de actualizaciones de los mismos, con estos datos se generara una visión aceptable de las características de la carga informática.

2.5.5.4. Determinación de los recursos necesarios para realizar la auditoría[23]

Mediante los resultados del estudio inicial realizado se procede a determinar los recursos humanos y materiales que han de emplearse en la auditoría.

Recursos materiales

Es muy importante su determinación, por cuanto la mayoría de ellos son proporcionados por el cliente, las herramientas software propias del equipo van a utilizarse igualmente en el sistema auditado, por lo que han de convenirse en lo posible las fechas y horas de uso entre el auditor y cliente. Los recursos materiales del auditor son de dos tipos:

Recursos materiales Software: Se encuentran encaminados en dos herramientas:

Programas Propios de la Auditoría: son muy potentes y flexibles y generalmente son usados para la realización de las pruebas de ejecución de los procesos del sistema para verificar que se desempeñan correctamente y cumplen con las políticas de la organización y los estándares de calidad.

Monitores: Se utilizan en función del grado de desarrollo observado en la actividad de Técnica de Sistemas del auditado y de la cantidad y calidad de los datos ya existentes.

Recursos materiales hardware: Los recursos hardware que el auditor necesita son proporcionados por el cliente, puesto que la revisión de los controles y la realización de las pruebas deben efectuarse necesariamente en las computadoras del auditado, igualmente estas herramientas serán usadas para efectuar las investigaciones y realizar la documentación pertinente, este tema

[23] http://www.monografias.com/trabajos39/la-auditoría/la-auditoría.shtml

debe ser convenido entre el grupo auditor y el cliente, donde se debe especificar el tiempo de uso de la maquina, elementos disponibles como: espacio en disco, uso de otros elementos como impresoras, escáner entre otros que se estimen necesarios.

Recursos humanos

La cantidad de recursos depende del volumen auditable, igualmente las características y perfiles del personal seleccionado depende de la materia auditable. Es igualmente reseñable que la auditoría en general suele ser ejercida por profesionales universitarios y por otras personas de probada experiencia multidisciplinaria.

2.5.5.5. Elaboración del programa de auditoría[24]

Un programa de auditoría es un conjunto documentado de procedimientos diseñados para alcanzar los objetivos de auditoría planificados. El esquema típico de un programa tiene en cuenta los siguientes criterios:

- Si la revisión debe realizarse por áreas generales o áreas específicas, en el primer caso, la elaboración es más compleja y costosa.
- Si la auditoría es global, de toda la informática, o parcial, el volumen determina no solamente el número de auditores necesarios, sino las especialidades necesarias del personal.

Como primera instancia para la realización de programa de auditoría es necesario definir la estrategia y las herramientas, que se debe seguir para la realización de la auditoría, con los lineamientos de la herramienta utilizada se conlleva a planear los temas que se deben evaluar, de manera que aseguren la realización de una auditoría de alta calidad con una cobertura conveniente y que se logre con economía, eficiencia, eficacia y prontitud.

[24] http://www.monografias.com/trabajos39/la-auditoría/la-auditoría.shtml
http://www.eici.ucm.cl/Academicos/ygomez/descargas/Auditoría.../AUDITORÍA%20Y%20SEGURIDAD%20DE%20SISTEM

Se debe tener muy en claro los objetivos y alcance previstos para la auditoría y considerando toda la información obtenida y conocimientos adquiridos sobre la entidad en la etapa de exploración, el grupo auditor hace la planeacion de las tareas a desarrollar y las comprobaciones necesarias para alcanzar los objetivos de la auditoría, Igualmente se debe determinar la importancia relativa de los temas que se van a auditar y reevaluar la necesidad de personal requerido para el desarrollo de las actividades, de acuerdo con los elementos de que dispone, también se debe determinar el tiempo a emplear en la ejecución de cada comprobación o verificación, y todos estos aspectos deben ser documentados para ser incluidos en el informe final.

De manera general se concluye que dentro el programa de auditoría se debe incluir:

- Identificación y selección del enfoque del trabajo
- Definición de los temas y las tareas a ejecutar.
- Identificación de lista de personas a entrevistar.
- Identificación y obtención de políticas, normas y directivas.
- Desarrollo de herramientas y metodología para probar y verificar los controles existentes.
- Nombre del o los especialistas que intervendrán en cada una de ellas.
- Fecha prevista de inicio y terminación de cada tarea.
- Extensión de cada prueba.
- Papeles de trabajo que se utilizarán.
- Procedimientos para evaluar los resultados de las pruebas y revisiones.
- Procedimientos de comunicación con la gerencia.
- Procedimientos de seguimiento.
- Vista global en el informe final.

2.5.5.6. Ejecución de la auditoría (realización de actividades propiamente dichas de la auditoría)

El propósito fundamental de esta etapa es recopilar las pruebas que sustenten las opiniones del auditor en cuanto al trabajo realizado, es la fase comparada con del trabajo de campo, esta depende en gran medida del grado de profundidad con que se hayan realizado las dos etapas anteriores, en ella se elaboran los papeles de trabajo y las hojas de nota, instrumentos que respaldan excepcionalmente la opinión del auditor.

En la etapa de ejecución se pone en práctica el plan de auditoría y los procedimientos planificados a fin de obtener suficiente evidencia que respalde la elaboración del informe.

Existen unas actividades de auditoría que constituyen métodos prácticos de investigación y prueba, que el auditor emplea de acuerdo a su criterio o juicio según las circunstancias, unas son utilizadas con mayor frecuencia que otras, a fin de obtener la evidencia o información adecuada y suficiente para fundamentar sus opiniones y conclusiones contenidas en el informe.

Técnicas de trabajo

- Análisis de la información proporcionada por el auditado.
- Análisis de la información propia.
- Cruzamiento de las informaciones anteriores.

Técnicas de verificación ocular:

- Comparación.
- Observación.
- Revisión selectiva.
- Rastreo.

Técnica de verificación verbal:

- Indagación.

Técnica de verificación escrita:

- Análisis.
- Conciliación.
- Confirmación.

Técnicas de verificación documental:

- Comprobación.
- Computación.

Técnica de verificación física:

- Inspección.

2.5.5.7. Determinación de hallazgos y realización de recomendaciones

El hallazgo en la auditoría tiene el sentido de obtención y síntesis de información específica sobre una operación, actividad, proyecto, unidad administrativa u otro asunto evaluado, los resultados sean de interés para los funcionarios de la entidad auditada.

Una vez que se cuenta con la evidencia real obtenida durante la ejecución de la auditoría, los hallazgos deben ser evaluados en función de cada procedimiento, de cada componente y de la auditoría en su conjunto, considerando si la evidencia obtenida es importante y confiable, en base en esta evaluación se deberán obtener conclusiones a fin de comprobar si los objetivos determinados para cada componente han sido alcanzados.

La evidencia de los hallazgos de auditoría deberá ser evaluada en términos de suficiencia, importancia, confiabilidad y eficacia, una vez aplicados y completados los programas específicos de auditoría se evaluará si la evidencia obtenida satisface las expectativas establecidas en la planificación, la evidencia será evaluada en términos de la suficiencia, competencia y confiabilidad, así como de la naturaleza e importancia de las observaciones identificadas.

Cuando se evalúen los hallazgos de auditoría debe considerarse si la información y las condiciones sobre las cuales se preparó el plan de auditoría continúan siendo apropiadas y por consiguiente, si se a obtenido suficiente información. En especial debe considerarse que:

- La evidencia obtenida es suficiente, competente, confiable y eficaz.
- La naturaleza y el nivel de las observaciones están de acuerdo con lo previsto en la planificación.

Al evaluar los resultados de auditoría en su conjunto, se obtienen una serie de conclusiones, basadas en el trabajo desarrollado para cada componente.

En general este proceso incluye:

- Revaluar la efectividad de la planificación específica de la auditoría, particularmente la relevancia del riesgo, a base de la información obtenida durante la etapa de ejecución.
- Analizar si existen inconsistencias en la evidencia de auditoría obtenida o en las conclusiones determinadas para los componentes individuales, si se detectan deben ser investigadas y resueltas.
- Comparar los errores acumulados con los criterios de importancia y la propuesta de corrección o ajustes, cuando fuere apropiado.
- Formular una conclusión sobre la auditoría global y su consideración para el informe.
- Plantear los controles respectivos para cada hallazgo.

2.5.5.8. Elaboración del informe final[25]

La función de la auditoría se materializa principalmente por escrito, por lo tanto es de gran importancia elaborar un documento de calidad que presente de forma objetiva todas las actividades desarrolladas en la auditoría, generalmente dentro del encabezado del informe general se incluye la fecha de elaboración

[25] http://www.monografias.com/trabajos39/la-auditoría/la-auditoría.shtml
http://www.eici.ucm.cl/Academicos/ygomez/descargas/Auditoría.../AUDITORÍA%20Y%20SEGURIDAD%20DE%20SISTEM

de la auditoría, fecha de redacción del informe, nombres del equipo auditor, registro de las personas entrevistadas y se sigue la siguiente estructura:

1. Definición de objetivos y alcance de la auditoría.
2. Enumeración de temas considerados: Antes de tratarlos con profundidad, se enumerarán lo más exhaustivamente posible todos los temas objeto de la auditoría.
3. Cuerpo expositivo: Para cada tema, se seguirá el siguiente orden a saber:
a) Situación actual: Cuando se trate de una revisión periódica, en la que se analiza no solamente una situación sino además su evolución en el tiempo, se expondrá la situación prevista y la situación real.
b) Tendencias: Se tratarán de hallar parámetros que permitan establecer tendencias futuras.
c) Puntos débiles y amenazas.
d) Recomendaciones y planes de acción: Constituyen junto con la exposición de puntos débiles, el verdadero objetivo de la auditoría informática.

Modelo conceptual de la exposición del informe final:

- El informe debe incluir solamente hechos importantes.
- La inclusión de hechos poco relevantes o accesorios desvía la atención del lector.
- El Informe debe consolidar los hechos que se describen en el mismo.
- El término de "hechos consolidados" adquiere un especial significado de verificación objetiva y deben estar documentalmente probados y soportados. La consolidación de los hechos debe satisfacer, al menos los siguientes criterios:
    1. El hecho debe poder ser sometido a cambios.
    2. Las ventajas del cambio deben superar los inconvenientes derivados de mantener la situación.
    3. No deben existir alternativas viables que superen al cambio propuesto.

4. La recomendación del auditor sobre el hecho debe mantener o mejorar las normas y estándares existentes en la instalación.

2.5.5.9. Elaboración de carta de presentación del informe final[26]

La realización de la carta de introducción o presentación del proyecto, es de vital importancia, puesto que en ella se expone un resumen sobre el proyecto de auditoría realizado, la cual se dispone al máximo responsable de la empresa o la persona que contrato la auditoría, de esta carta no existirá ninguna copia, mientras que del informe final si se pueden disponer varios documentos.

La carta de introducción poseerá los siguientes atributos:

- Carta de presentación del informe final.
- Resumen en 3 ó 4 folios del contenido del informe final.
- Incluye fecha, naturaleza, objetivos y alcance de la auditoría.
- Cuantifica la importancia de las áreas analizadas.
- Proporciona una conclusión general, concretando las áreas de gran debilidad.
- Presentar las debilidades en orden de importancia.

2.5.6. Estándares internacionales de auditoría de sistemas

La función de auditoría continúa proporcionando servicios de aseguramiento tanto a clientes internos como externos, dado que la tecnología impacta la forma de hacer negocios, deben haber formas efectivas y sencillas para llevar a cabo la evaluación de los controles que deben existir para garantizar dicho servicio.

Bajo la premisa anterior, existe un gran interés en el medio por identificar los estándares internacionales que son utilizados comúnmente por empresas tanto públicas como privadas, con el fin de determinar si la organización ha implementado proyectos de tecnología de información, cubriendo

[26] http://www.monografias.com/trabajos39/la-auditoría/la-auditoría.shtml
http_//www.eici.ucm.cl/Academicos/ygomez/descargas/Auditoría.../AUDITORÍA%20Y%20SEGURIDAD%20DE%20SISTEM

adecuadamente las necesidades de los clientes en forma eficiente y dentro del presupuesto contemplado.

Entre estos estándares se encuentra:

A. Directrices gerenciales de COBIT, desarrollado por la Information systems audit and control association (ISACA): Las directrices gerenciales son un marco internacional de referencias que abordan las mejores prácticas de auditoría y control de sistemas de información, permiten que la gerencia incluya, comprenda y administre los riesgos relacionados con la tecnología de información y establezca el enlace entre los procesos de administración, aspectos técnicos, la necesidad de controles y los riesgos asociados.

B. The management of the control of data Information technology, desarrollado por el instituto canadiense de contadores certificados (CICA): Este modelo está basado en el concepto de roles y establece responsabilidades relacionadas con seguridad y los controles correspondientes, dichos roles están clasificados con base en siete grupos: administración general, gerentes de sistemas, dueños, agentes, usuarios de sistemas de información, así como proveedores de servicios, desarrollo y operaciones de servicios y soporte de sistemas, además hace distinción entre los conceptos de autoridad, responsabilidad respecto a control y riesgo previo al establecimiento del control, en términos de objetivos, estándares y técnicas mínimas a considerar.

C. Administración de la inversión de tecnología de Inversión: un marco para la evaluación y mejora del proceso de madurez, desarrollado por la oficina de contabilidad general de los Estados Unidos (GAO): Este modelo identifica los procesos críticos, asegurando el éxito de las inversiones en tecnología de información y comunicación electrónicas, además los organiza en cinco niveles de madurez, similar al modelo CMM.

D. Estándares de administración de calidad y aseguramiento de calidad ISO 9000, desarrollados por la organización internacional de estándares (ISO): La

colección ISO 9000 es un conjunto de estándares y directrices que apoyan a las organizaciones a implementar sistemas de calidad efectivos, para el tipo de trabajo que ellos realizan.

E. SysTrust – Principios y criterios de confiabilidad de sistemas, desarrollados por la asociación de contadores públicos (AICPA) y el CICA: Este servicio pretende incrementar la confianza de la alta gerencia, clientes y socios, con respecto a la confiabilidad en los sistemas por una empresa o actividad en particular. Este modelo incluye elementos como: infraestructura, software de cualquier naturaleza, personal especializado y usuarios, procesos manuales y automatizados, y datos, el modelo persigue determinar si un sistema de información es confiable, (i.e. si un sistema funciona sin errores significativos, o fallas durante un periodo de tiempo determinado bajo un ambiente dado).

F. Modelo de evolución de capacidades de software (CMM), desarrollado por el instituto de ingeniería de software (SEI): Este modelo hace posible evaluar las capacidades o habilidades para ejecutar, de una organización, con respecto al desarrollo y mantenimiento de sistemas de información. Consiste en 18 sectores clave, agrupados alrededor de cinco niveles de madurez. Se puede considerar que CMM es la base de los principios de evaluación recomendados por COBIT, así como para algunos de los procesos de administración de COBIT.

G. Administración de sistemas de información: Una herramienta de evaluación práctica, desarrollado por la directiva de recursos de tecnología de información (ITRB): Este es una herramienta de evaluación que permite a entidades gubernamentales, comprender la implementación estratégica de tecnología de información y comunicación electrónica, que puede apoyar su misión e incrementar sus productos y servicios.

H. Guía para el cuerpo de conocimientos de administración de proyectos, desarrollado por el comité de estándares del instituto de administración de

proyectos: Esta guía esta enfocada en las mejores prácticas sobre administración de proyectos, se refiere a aspectos sobre los diferentes elementos necesarios para una administración exitosa de proyectos de cualquier naturaleza, en forma precisa, este documento identifica y describe las prácticas generalmente aceptadas de administración de proyectos que pueden ser implementadas en las organizaciones.

I. Ingeniería de seguridad de sistemas – modelo de madurez de capacidades (SSE – CMM), desarrollado por la agencia de seguridad nacional (NSA) con el apoyo de la universidad de carnegie mellon: Este modelo describe las características esenciales de una arquitectura de seguridad organizacional para tecnología de información y comunicación electrónica, de acuerdo con las prácticas generalmente aceptadas observadas en las organizaciones.

J. Administración de seguridad de información: aprendiendo de organizaciones líderes, desarrollado por la oficina de contabilidad general de los Estados Unidos (GAO): Este modelo considera ocho organizaciones privadas reconocidas como líderes respecto a seguridad en cómputo, este trabajo hace posible la identificación de 16 prácticas necesarias para asegurar una adecuada administración de la seguridad de cómputo, las cuáles deben ser suficientes para incrementar significativamente el nivel de administración de seguridad en tecnología de información y comunicación electrónica.

2.5.7. Herramientas y técnicas para la auditoría de sistemas[27]

2.5.7.1. Entrevista

Sirve como instrumento para que el auditor pueda conocer las funciones del personal auditado y como se están llevando a cabo los procesos dentro de la organización, existen varias formas de realizar esta estrategia:

[27] http://www.monografias.com/trabajos39/la-auditoría/la-auditoría.shtml

1. Mediante la petición de documentación concreta sobre alguna materia de su responsabilidad.

2. Mediante "entrevistas" en las que no se sigue un plan predeterminado ni un método estricto de sometimiento a un cuestionario.

3. Por medio de entrevistas en las que el auditor sigue un método preestablecido de antemano y busca unas finalidades concretas.

La entrevista es una de las actividades personales más importante del auditor; en ellas, éste recoge gran cantidad de información de forma clara, a través de de las respuestas que el entrevistado brinda y la observación por parte del auditor en el momento de entrevistar a un determinado funcionario.

El proceso de entrevista se basa fundamentalmente en el concepto interrogatorio, el auditor se encarga de realizar las preguntas necesarias que lleven a la determinación de conclusiones necesarias en un determinado objetivo de control.

El auditor informático experto entrevista al auditado siguiendo un cuidadoso sistema previamente establecido, consistente en que bajo la forma de una conversación correcta y lo menos tensa posible, el auditado conteste sencillamente y con pulcritud a una serie de preguntas variadas, también sencillas. Sin embargo, esta sencillez es solo aparente. Tras ella debe existir una preparación muy elaborada y sistematizada, y que es diferente para cada caso particular.

2.5.7.2. Cuestionarios

El auditor profesional y experto es aquél que reelabora muchas veces sus cuestionarios en función de los escenarios auditados, tiene claro lo que necesita saber, y por qué, sus cuestionarios son vitales para el trabajo de

análisis, cruzamiento y síntesis posterior, lo cual no quiere decir que haya de someter al auditado a unas preguntas estereotipadas que no conducen a nada.

Muy por el contrario, el auditor conversará y hará preguntas "normales", que en realidad servirán para el cumplimiento sistemático de sus Cuestionarios.

Hay opiniones que descalifican el uso de las checklists, ya que consideran que leerle una pila de preguntas recitadas de memoria o leídas en voz alta descalifica al auditor informático.

El profesionalismo pasa por un procesamiento interno de información a fin de obtener respuestas coherentes que permitan una correcta descripción de puntos débiles y fuertes, el profesionalismo pasa por poseer preguntas muy estudiadas que han de formularse flexiblemente.

El conjunto de estas preguntas recibe el nombre de checklist, salvo excepciones, las checklists deben ser contestadas oralmente, ya que superan en riqueza y generalización a cualquier otra forma.

Según la claridad de las preguntas y el talante del auditor, el auditado responderá desde posiciones muy distintas y con disposición muy variable. El auditado, habitualmente informático de profesión, percibe con cierta facilidad el perfil técnico y los conocimientos del auditor, precisamente a través de las preguntas que éste le formula, esta percepción configura el principio de autoridad y prestigio que el auditor debe poseer. Por ello, aun siendo importante tener elaboradas listas de preguntas muy sistematizadas, coherentes y clasificadas por materias, todavía lo es más el modo y el orden de su formulación. Las empresas externas de auditoría informática guardan sus checklists, pero de poco sirven si el auditor no las utiliza adecuada y oportunamente.

El auditor deberá aplicar la checklist de modo que el auditado responda clara y escuetamente. Se deberá interrumpir lo menos posible a éste, y solamente en los casos en que las respuestas se aparten sustancialmente de la pregunta, en algunas ocasiones, se hará necesario invitar a aquél a que exponga con mayor amplitud un tema concreto, y en cualquier caso, se deberá evitar absolutamente la presión sobre el mismo.

Algunas de las preguntas de las checklists utilizadas para cada sector, deben ser repetida, bajo apariencia distinta, el auditor formulará preguntas equivalentes a las mismas o a distintas personas, en las mismas fechas, o en fechas diferentes, de este modo, se podrán descubrir con mayor facilidad los puntos contradictorios; el auditor deberá analizar los matices de las respuestas y reelaborar preguntas complementarias cuando hayan existido contradicciones, hasta conseguir la homogeneidad. El entrevistado no debe percibir un excesivo formalismo en las preguntas, el auditor, por su parte, tomará las notas imprescindibles en presencia del auditado, y nunca escribirá cruces ni marcará cuestionarios en su presencia.

Los cuestionarios responden fundamentalmente a dos tipos de "filosofía" de calificación o evaluación:

a. Checklist de rango: Contiene preguntas que el auditor debe calificar dentro de un rango preestablecido (por ejemplo, de 1 a 5, siendo 1 la respuesta más negativa y el 5 el valor más positivo). Ejemplo de checklist de rango: Se supone que se está realizando una auditoría sobre la seguridad física de una instalación y, dentro de ella, se analiza el control de los accesos de personas y cosas al centro de cálculo, podrían formularse las preguntas en donde las respuestas tienen los siguientes significados:

- 1: Muy deficiente.
- 2: Deficiente.
- 3: Mejorable.
- 4: Aceptable.

- 5: Correcto.

Las checklists de rango son adecuadas si el equipo auditor no es muy grande y mantiene criterios uniformes y equivalentes en las valoraciones, permiten una mayor precisión en la evaluación que en la checklist binaria, sin embargo, la bondad del método depende excesivamente de la formación y competencia del equipo auditor.

b. Checklist binaria: Es la constituida por preguntas con respuesta única y excluyente: Si o No. aritméticamente, equivalen a 1(uno) o 0(cero), respectivamente.

Las checklists binarias siguen una elaboración inicial mucho más ardua y compleja, deben ser de gran precisión, como corresponde a la suma precisión de la respuesta, una vez construidas, tienen la ventaja de exigir menos uniformidad del equipo auditor y el inconveniente genérico del <si o no> frente a la mayor riqueza del intervalo.

No existen checklists estándar para todas y cada una de las instalaciones informáticas a auditar, cada una de ellas posee peculiaridades que hacen necesarios los retoques de adaptación correspondientes en las preguntas a realizar.

2.5.7.3. Trazas y/o huellas

Con frecuencia, el auditor informático debe verificar que los programas, tanto de los sistemas como de usuario, realizan exactamente las funciones previstas y no otras, para ello se apoya en productos software muy potentes y modulares que permiten rastrear los caminos que siguen los datos a través del programa, muy especialmente, estas "trazas" se utilizan para comprobar la ejecución de las validaciones de datos previstas, estas herramientas no deben modificar en absoluto el sistema.

Por lo que se refiere al análisis del sistema, los auditores informáticos emplean productos que comprueban los valores asignados por técnica de sistemas a cada uno de los parámetros variables de las librerías más importantes del mismo, estos parámetros variables deben estar dentro de un intervalo marcado por el fabricante, por ejemplo algunas instalaciones descompensan el número de iniciadores de trabajos de determinados entornos o toman criterios especialmente restrictivos o permisivos en la asignación de unidades de servicio, estas actuaciones son útiles en principio, pero pueden resultar contraproducentes si se traspasan los límites, no obstante la utilidad de las trazas, a de repetirse lo expuesto en la descripción de la auditoría informática de sistemas: el auditor informático emplea preferentemente la amplia información que proporciona el propio sistema: así los ficheros de <accounting> o de <contabilidad>, en donde se encuentra la producción completa de aquél, y los <log*> de dicho sistema, en donde se recogen las modificaciones de datos y se pormenoriza la actividad general.

2.5.7.4. Software de interrogación

Hasta hace ya algunos años se han utilizado productos software llamados genéricamente <paquetes de auditoría>, capaces de generar programas para auditores escasamente cualificados desde el punto de vista informático.

Más tarde, dichos productos evolucionaron hacia la obtención de muestreos estadísticos que permitieran la obtención de consecuencias e hipótesis de la situación real de una instalación.

En la actualidad, los productos software especiales para la auditoría informática se orientan principalmente hacia lenguajes que permiten la interrogación de ficheros y bases de datos de la empresa auditada, estos productos son utilizados solamente por los auditores externos, por cuanto los internos disponen del software nativo propio de la instalación.

Del mismo modo, la proliferación de las redes locales y de la filosofía "cliente-servidor", han llevado a las firmas de software a desarrollar interfaces de transporte de datos entre computadoras personales y mainframe, de modo que el auditor informático copia en su propia PC la información más relevante para su trabajo.

Cabe recordar, que en la actualidad casi todos los usuarios finales poseen datos e información parcial generada por la organización informática de la compañía, efectivamente, conectados como terminales al "host", almacenan los datos proporcionados por este, que son tratados posteriormente en modo pc. El auditor se ve obligado (naturalmente, dependiendo del alcance de la auditoría) a recabar información de los mencionados usuarios finales, lo cual puede realizar con suma facilidad con los polivalentes productos descritos, las opiniones más autorizadas indican que el trabajo de campo del auditor informático debe realizarse principalmente con los productos del cliente. Finalmente, a de indicarse la conveniencia de que el auditor confeccione personalmente determinadas partes del Informe, para ello, resulta casi imprescindible una cierta soltura en el manejo de procesadores de texto, paquetes de gráficos, hojas de cálculo, etc.

2.5.7.5. Software especializado para la realización de pruebas de ejecución a la infraestructura lógica

Igualmente es de gran importancia contar con herramientas que permitan verificar la infraestructura física y lógica, enfocada principalmente a la seguridad, donde se debe analizar si existen huecos de seguridad en el sistema operativo o los servicios implementados en la organización, defectos en el software que permiten la intrusión o generan fallas graves en el funcionamiento.

Existen varias herramientas que permiten analizar los aspectos mencionados anteriormente por ejemplo:[28]

[28] http://www.oxid.it/cain.html

El escaneo de puertos: Es una herramienta que aunque apoya la seguridad, puede ser utilizada en contra de ella, permite conocer el estado de los puertos asociados con los servicios disponibles en la instalación.

Sniffer: Es un programa que intercepta la información que transita por una red, sniffing significa espiar y obtener la información que circula por la red, coloca la interfaz en modo promiscuo y captura el tráfico, su misión para los ataques es fisgonear la red en busca de claves o puertos abiertos.

Troyanos: Programas que simulan ser otros para así atacar el sistema.

Ataque de Fuerza bruta sobre claves: Forma poco sutil de entrar en un sistema que consiste en probar distintas contraseñas hasta encontrar la adecuada.

Ingeniería Social: Es una técnica por la cual se convence a alguien por diversos medios, de que proporcione información útil para hackear o para beneficiarnos, requiere grandes dosis de psicología, explota la tendencia de la gente a confiar en sus semejantes.

Basureo o Trashing: Se trata de buscar en la basura (física o informática) información que pueda ser útil para hackear.

Ping: Ubicar equipos conectados.

Traceroute: Ver la ruta de paquetes y enrutadores en la red.

Spams: No es un código dañino, pero si bastante molesto, es un programa que ejecuta una orden varias veces, y es ampliamente utilizado por empresas de marketing usando el correo electrónico para enviar sus mensajes en forma exagerada.

NMAP 4.65: Nmap esta orientado a la identificación de puertos abiertos en los equipos de una red, determinando que servicios se están ejecutando, y el sistema operativo que utiliza.

Ha llegado a ser uno de las herramientas imprescindibles para todo administrador de sistema, y es usado para pruebas de penetración y tareas de seguridad informática en general. Como muchas herramientas usadas en el campo de la seguridad informática, nmap puede ser utilizado tanto por los administradores de sistema como por personas menos éticas.

Los administradores de sistema pueden utilizarlo para verificar la presencia de posibles aplicaciones no autorizadas ejecutándose en el servidor, así como los crakers pueden usarlo para descubrir objetivos potenciales.

Nmap es a menudo confundido con herramienta para verificación de vulnerabilidades como nessus, nmap es difícilmente detectable, ha sido creado para evadir los detectores de intrusos (IDS - intruder detection systems) e interfiere lo menos posible con las operaciones normales de las redes y de las computadoras que son analizadas.

Para poder utilizarlo en sistemas windows es necesario que la tarjeta de red este en modo promiscuo, para ello necesitaras el winpcap.

Las características principales de NMAP son:

- Descubrimiento de servidores: Identifica computadoras en una red.
- Identifica puertos abiertos en una computadora objetivo.
- Determina qué servicios está ejecutando la misma.
- Determinar qué sistema operativo y versión utiliza dicha computadora, (esta técnica es también conocida como fingerprinting)
- Obtiene algunas características del hardware de red de la máquina objeto de la prueba.

Entornos de trabajo:
Nmap es una herramienta usada principalmente en Microsoft Windows pero puede funcionar en otros sistemas operativos como: unix, solaris, mac OS X, y BSD, GNU/Linux.

CAIN Y ABEL:[29] Cain y abel es una herramienta de recuperación de contraseñas para los sistemas operativos de microsoft que se suele utilizar para hachear redes, permite la recuperación fácil de las variadas clases de contraseñas que se difunden a través de una Lan, rompiendo contraseñas cifradas usando los ataques del diccionario, de fuerza bruta y de criptoanálisis, conversaciones de registración de voip, contraseñas web, destapando contraseñas depositadas y analizando protocolos de encaminamiento, este programa aprovecha una cierta inseguridad presente en los estándares de protocolo y métodos de autentificación; su propósito principal es la recuperación simplificada de contraseñas y de credenciales de varias fuentes, no obstante también tiene algunas utilidades "no estándares" para los usuarios de microsoft windows.

La última versión es más rápida y contiene nuevas características como abril (encaminamiento del veneno arp) que permite esnifar en lans (engañando las tablas de los switch) y ataques de Hombre en el Medio, el succionador en esta versión puede también analizar protocolos cifrados tales como ssh-1 y https, y contiene los filtros para capturar las credenciales de una amplia gama de mecanismos de autentificación, la nueva versión también envía protocolos de encaminamiento que la autentificación supervisa y encamina los extractores, las cookies del diccionario y la fuerza bruta para todos los algoritmos de cálculo comunes y para varias autentificaciones específicas, las calculadoras de password/hash, los ataques del criptoanálisis, los decodificadores de la contraseña y algunas utilidades no tan comunes relacionados con la seguridad de la red y del sistema.

[29] http://vtroger.blogspot.com/2005/11/cain-y-abel.html

2.5.8. Estándares utilizados para La auditoría de sistemas en el HUDN

2.5.8.1. COBIT (Control objectives for Information and related technology): De la information systems audit and control asociation (ISACA)[30], COBIT fue lanzado en el año de 1996, es una herramienta de gobierno de TI que ha cambiado la forma en que trabajan los profesionales de TI. Vinculando tecnología informática y prácticas de control, COBIT consolida y armoniza estándares de fuentes globales prominentes en un recurso crítico para la gerencia, los profesionales de control y los auditores.

COBIT se aplica a los sistemas de información de toda la empresa, incluyendo las computadoras personales, mini computadoras y ambientes distribuidos, esta basado en la filosofía de que los recursos de TI necesitan ser administrados por un conjunto de procesos naturalmente agrupados para proveer la información pertinente y confiable que requiere una organización para lograr sus objetivos.

El fin primordial del COBIT es Investigar, desarrollar, publicar y promover un conjunto internacional y actualizado de objetivos de control para tecnología de información que sea de uso cotidiano para gerentes y auditores

El COBIT esta orientado a los siguientes usuarios:

- La gerencia: para apoyar sus decisiones de inversión en TI y control sobre el rendimiento de las mismas, analizar el costo beneficio del control.
- Los usuarios finales: quienes obtienen una garantía sobre la seguridad y el control de los productos que adquieren interna y externamente.
- Los auditores: para soportar sus opiniones sobre los controles de los proyectos de TI, su impacto en la organización y determinar el control mínimo requerido.

[30] Comité Directivo de COBIT y El IT Governance Institute TMCOBIT. Directrices De Auditoría.3 Edición, Julio 2000,pag229

- Los responsables de TI: para identificar los controles que requieren en sus áreas.

Dentro de sus características principales se encuentra:

- Esta orientado al negocio.
- Alineado con estándares y regulaciones "de facto".
- Basado en una revisión crítica y analítica de las tareas y actividades en TI.
- Alineado con estándares de control y auditoría (coso, ifac, iia, isaca, aicpa).

El enfoque del control en TI se lleva a cabo visualizando la información necesaria para dar soporte a los procesos de negocio y considerando a la información como el resultado de la aplicación combinada de recursos relacionados con las TI que deben ser administrados por procesos de TI.

Requerimientos de la información del negocio: Para alcanzar los requerimientos de negocio, la información necesita satisfacer ciertos criterios:

- Requerimientos de calidad: Calidad, costo y entrega.
- Requerimientos fiduciarios: Efectividad y eficiencia operacional, confiabilidad de los reportes financieros y cumplimiento le leyes y regulaciones.

Definiciones de trabajo de COBIT: Se han tenido en cuenta varias definiciones entre ellas están:

- Efectividad: Se refiere a que la información relevante sea pertinente para el proceso del negocio, así como a que su entrega sea oportuna, correcta, consistente y de manera utilizable.
- Eficiencia: Se refiere a la provisión de información a través de la utilización óptima (más productiva y económica) de recursos.

- Confidencialidad: Se refiere a la protección de información sensible contra divulgación no autorizada.
- Integridad: Se refiere a la precisión y suficiencia de la información, así como a su validez de acuerdo con los valores y expectativas del negocio.
- Disponibilidad: Se refiere a la disponibilidad de la información cuando ésta es requerida por el proceso de negocio ahora y en el futuro. También se refiere a la salvaguarda de los recursos necesarios y capacidades asociadas.
- Cumplimiento: Se refiere al cumplimiento de aquellas leyes, regulaciones y acuerdos contractuales a los que el proceso de negocios está sujeto, por ejemplo, criterios de negocio impuestos externamente.
- Confiabilidad de la información: Se refiere a la provisión de información apropiada para la administración con el fin de operar la entidad y para ejercer sus responsabilidades de reportes financieros y de cumplimiento.

Requerimientos de seguridad:

Confidencialidad: Protección de la información sensible contra divulgación no autorizada

- Integridad: Refiere a lo exacto y completo de la información así como a su validez de acuerdo con las expectativas de la empresa.
- Disponibilidad: accesibilidad a la información cuando sea requerida por los procesos del negocio y la salvaguarda de los recursos y capacidades asociadas a la misma.
- Recursos de TI

Los recursos de TI identificados en COBIT pueden identificarse/definirse como se muestra a continuación:

- Datos: Los elementos de datos en su más amplio sentido, (por ejemplo, externos e internos), estructurados y no estructurados, gráficos, sonido, etc.

- Aplicaciones: Se entiende como sistemas de aplicación la suma de procedimientos manuales y programados.
- Tecnología: La tecnología cubre hardware, software, sistemas operativos, sistemas de administración de bases de datos, redes, multimedia, etc.
- Instalaciones: Recursos para alojar y dar soporte a los sistemas de información.
- Personal: Habilidades del personal, conocimiento, conciencia y productividad para planear, organizar, adquirir, entregar, soportar y monitorear servicios y sistemas de información.

Estructura del COBIT: Se define a partir de una premisa simple y pragmática: "Los recursos de las tecnologías de la información (TI) se han de gestionar mediante un conjunto de procesos agrupados de forma natural para que proporcionen la información que la empresa necesita para alcanzar sus objetivos".

COBIT se divide en tres niveles:

- Dominios: Agrupación natural de procesos, normalmente corresponden a un dominio o una responsabilidad organizacional.
- Procesos: Conjuntos o series de actividades unidas con delimitación o cortes de control.
- Actividades: Acciones requeridas para lograr un resultado medible, se definen 34 objetivos de control generales, uno para cada uno de los procesos de las TI, estos procesos están agrupados en cuatro grandes dominios.

Las definiciones para los dominios mencionados son las siguientes:

- Planeación y organización: Este dominio cubre la estrategia y las tácticas y se refiere a la identificación de la forma en que la tecnología

de información puede contribuir de la mejor manera al logro de los objetivos del negocio. Además, la consecución de la visión estratégica necesita ser planeada, comunicada y administrada desde diferentes perspectivas. Finalmente, deberán establecerse una organización y una infraestructura tecnológica apropiadas.

- Adquisición e implementación: Para llevar a cabo la estrategia de TI, las soluciones de TI deben ser identificadas, desarrolladas o adquiridas, así como implementadas e integradas dentro del proceso del negocio. Además, este dominio cubre los cambios y el mantenimiento realizados a sistemas existentes.
- Entrega y soporte: En este dominio se hace referencia a la entrega de los servicios requeridos, que abarca desde las operaciones tradicionales hasta el entrenamiento, pasando por seguridad y aspectos de continuidad. Con el fin de proveer servicios, deberán establecerse los procesos de soporte necesarios. Este dominio incluye el procesamiento de los datos por sistemas de aplicación, frecuentemente clasificados como controles de aplicación.
- Monitoreo: Todos los procesos necesitan ser evaluados regularmente a través del tiempo para verificar su calidad y suficiencia en cuanto a los requerimientos de control.

Se lleva a cabo una clasificación dentro del marco referencial COBIT basada en rigurosos informes y observaciones de procesos por parte de investigadores, expertos y revisores con las estrictas definiciones determinadas previamente.

- Primario: Es el grado al cual el objetivo de control definido impacta directamente el requerimiento de información de interés.
- Secundario: Es el grado al cual el objetivo de control definido satisface únicamente de forma indirecta o en menor medida el requerimiento de información de interés.

- Blanco (vacío): Podría aplicarse; sin embargo, los requerimientos son satisfechos más apropiadamente por otro criterio en este proceso y/o por otro proceso.

Tabla Resumen

Dominio	Proceso	Criterios de Información						Recursos de TI				
		Efectividad	Eficiencia	Confidencialidad	Integridad	Disponibilidad	Cumplimiento	Confiabilidad	Humanos	Sistemas / Inf	Tecnología	Instalaciones	Datos
Planeación y Organización													
PO1	Definir un Plan Estratégico de TI	P	S						✓	✓	✓	✓	✓
PO2	Definir la Arquitectura de Información	P	S	S	S					✓			✓
PO3	Determinar la dirección tecnológica	P	S								✓	✓	
PO4	Definir la Organización y Relaciones de TI	P	S						✓				
PO5	Manejar la Inversión en TI	P	P					S	✓	✓	✓	✓	
PO6	Comunicar las directrices gerenciales	P					S		✓				
PO7	Administrar Recursos Humanos	P	P						✓				
PO8	Asegurar el cumplir Requerimientos Externos	P					P	S	✓	✓			✓
PO9	Evaluar Riesgos	S	S	P	P	P	S	S	✓	✓	✓	✓	✓
PO10	Administrar proyectos	P	P						✓	✓	✓	✓	
PO11	Administrar Calidad	P	P		P			S	✓	✓			

Adquisición e Implementación

AI1	Identificar Soluciones	P	S							✓	✓	✓	
AI2	Adquisición y Mantener Software de Aplicación	P	P		S		S	S		✓			
AI3	Adquirir y Mantener Arquitectura de TI	P	P		S						✓		
AI4	Desarrollar y Mantener Procedimientos relacionados con TI	P	P		S		S	S	✓	✓	✓	✓	
AI5	Instalar y Acreditar Sistemas	P			S	S			✓	✓	✓	✓	✓
AI6	Administrar Cambios	P	P		P	P		S	✓	✓	✓	✓	✓

Servicios y Soporte

DS1	Definir niveles de servicio	P	P	S	S	S	S	S	✓	✓	✓	✓	✓
DS2	Administrar Servicios de Terceros	P	P	S	S	S	S	S	✓	✓	✓	✓	✓
DS3	Administrar Desempeño y Capacidad	P	P			S				✓	✓	✓	
DS4	Asegurar Servicio Continuo	P	S			P			✓	✓	✓	✓	✓
DS5	Garantizar la Seguridad de Sistemas			P	P	S	S	S	✓	✓	✓	✓	✓
DS6	Identificar y Asignar Costos		P					P	✓	✓	✓	✓	✓
DS7	Capacitar Usuarios	P	S						✓				
DS8	Asistir a los Clientes de TI	P							✓	✓			
DS9	Administrar la Configuración	P				S		S		✓	✓	✓	
DS10	Administrar Problemas e Incidentes	P	P			S			✓	✓	✓	✓	✓
DS11	Administrar Datos				P			P					✓
DS12	Administrar Instalaciones				P	P						✓	
DS13	Administrar Operaciones	P	P		S	S			✓	✓	✓	✓	✓

Monitoreo

M1	Monitorear los procesos	P	S	S	S	S	S	S	✓	✓	✓	✓	✓
M2	Evaluar lo adecuado del control Interno	P	P	S	S	S	S	S	✓	✓	✓	✓	✓
M3	Obtener aseguramiento independiente	P	P	S	S	S	S	S	✓	✓	✓	✓	✓
M4	Proveer auditoría independiente	P	P	S	S	S	S	S	✓	✓	✓	✓	✓

2.5.8.2. ISO 27001[31]

Para referirse a la norma ISO 27001, es importante denotar sus antecedes, inicialmente la norma BS7799 fue originalmente el resultado de una iniciativa conjunta de DTI (deparment of trade and industry) en el reino unido y empresas británicas del sector privado, la primera versión de la norma BS7799 apareció en febrero de 1995, y consistía en un código de practica para la gestión de la seguridad de las tecnologías de información, en el año de 1998 se hizo una revisión a esta norma y en 1999 se publico una norma actualizada, nombrada como “el código de practica original”, este se conservo como la primera parte de una norma británica (BS 7799-1), la segunda parte fue titulada como “specification for information security management system” (BS 7799-2), la cual proporcionaba la especificación contra la cual podría evaluarse y certificarse un sistema de gestión de la seguridad de una organización.

Como código de práctica, la norma BS7799-1 era un documento de orientación y recomendaciones el cual se internacionalizó como ISO/IEC 17799 en diciembre del año 2000, la segunda parte conocida como BS7799-2 se internacionalizó como ISO/27001 en noviembre de 2005 y contó con más de 1700 empresas certificadas en BS7799-2, este esquema se publicó por ISO como estándar ISO 27001, al tiempo que se revisó y actualizó ISO17799, esta última norma se renombra como ISO 27002:2005 el 1 de julio de 2007, manteniendo el contenido así como el año de publicación formal de la revisión.

[31] Calder Alan. Nueve Claves Para el Éxito Una visión general de la implementación de la norma NTC-ISO/IEC 27001,Icontec 2006, pag125

La serie 27000: A semejanza de otras normas ISO, la 27000 es realmente una serie de estándares, los rangos de numeración reservados por ISO van de 27000 a 27019 y de 27030 a 27044.

ISO 27000: En fase de desarrollo; su fecha prevista de publicación es Noviembre de 2008, contendrá términos y definiciones que se emplean en toda la serie 27000, la aplicación de cualquier estándar necesita de un vocabulario claramente definido, que evite distintas interpretaciones de conceptos técnicos y de gestión, esta norma está previsto que sea gratuita, a diferencia de las demás de la serie, que tendrán un coste.

ISO 27001: Publicada el 15 de Octubre de 2005. es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información, tiene su origen en la BS 7799-2:2002 y es la norma con arreglo a la cual se certifican por auditores externos los SGSI de las organizaciones, sustituye a la BS 7799-2, habiéndose establecido unas condiciones de transición para aquellas empresas certificadas en esta última, en su anexo a, enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002:2005 (nueva numeración de ISO 17799:2005 desde el 1 de Julio de 2007), para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI; a pesar de no ser obligatoria la implementación de todos los controles enumerados en dicho anexo, la organización deberá argumentar sólidamente la no aplicabilidad de los controles no implementados, desde el 28 de noviembre de 2007.

La norma ISO 27001 contempla diez dominós que son:

- Política de seguridad de la información.
- Organización de la seguridad de la información.
- Gestión de activos.
- Seguridad de los recursos humanos.
- Seguridad física y del entorno.
- Gestión de comunicaciones y operaciones.

- Control de acceso.
- Adquisición, desarrollo y mantenimiento de sistemas de información.
- Gestión de incidentes de la seguridad de la información.
- Cumplimiento.

Estos dominios están compuestos por un conjunto de subdominios y sus correspondientes controles, los cuales han de ser abordados adoptando un modelo de phva (planificar, hacer, verificar, actuar).

2.5.9. Riesgo informático

Se define el riesgo informático como la probabilidad de que se de un error, falle un proceso, o tenga lugar un hecho negativo para la empresa u organización, incluyendo la posibilidad de fraudes, el riesgo se puede evaluar mediante un modelo.

Modelo de riesgo

Se puede establecer un modelo de riesgo informático como una función de los siguientes componentes:

- Activos
- Amenazas
- Impacto
- Vulnerabilidades

Estos componentes se pueden evaluar como factores de análisis del riesgo existente.

Tipos de riesgos informáticos: Existen diferentes tipos de riesgos en entornos informáticos, se clasifican de la siguiente manera:

- Riesgo de fraude.
- Riesgo de confidencialidad.
- Riesgo de pérdida de imagen.
- Riesgos de inexactitud de los datos.

- Riesgos de integridad de la información.
- Riesgos de la protección de activos.
- Riesgos de incumplimiento de normas legales.
- Riesgos en la eficiencia y eficacia de los procesos y utilización de los recursos.

2.5.10. Control interno informático

El control interno informático controla diariamente que todas las actividades de sistemas de Información sean realizadas cumpliendo procedimientos, estándares y normas fijados por la dirección de la organización o del área de informática, así como los requerimientos legales.[32]

Los controles informáticos se encuentran clasificados de la siguiente manera:

Controles preventivos: Son aquellos que reducen la frecuencia con que ocurren las causas del riesgo, permitiendo cierto margen de violaciones.

Controles detectivos: Son aquellos que no evitan que ocurran las causas del riesgo, sino que los detecta luego de ocurridos, son los más importantes para el auditor, puesto que le sirven para evaluar la eficiencia de los controles preventivos.

Controles correctivos: Ayudan a la investigación y corrección de las causas del riesgo, la corrección adecuada puede resultar difícil e ineficiente, siendo necesaria la implantación de controles detectivos sobre los controles correctivos, debido a que la corrección de errores es en si una actividad altamente propensa a errores.

Grupos de procedimientos de control interno:

[32] http://espanol.geocities.com/audiconsystem/auditori.htm

A. *Controles de la operatividad del sistema:* Para conseguir la operatividad de los sistemas se debe acudir a la realización de controles técnicos generales de operatividad y controles técnicos específicos.

B. *Controles de la gestión Informática:* Una vez conseguida la operatividad de los sistemas, el segundo objetivo de control es la verificación de que se cumplen las normas teóricamente existentes en el departamento de Informática y que son coherentes con las del resto de la empresa, para lograr este objetivo se deben seguir los siguientes controles:

- Control de las normas generales de la instalación informática: Donde se realizara una revisión inicial sin estudiar a fondo las contraindicaciones que pudieran existir, pero registrando las áreas que carezcan de normativa y sobre todo verificando que esta norma no este en contradicción con alguna norma general no informática de la organización.

- Control de procedimientos generales informáticos: Se verificara su existencia, al menos en los sectores más importantes como:

* Controles de operación y organización.
* Controles de desarrollo de sistemas y documentación.
* Controles de hardware y software de sistemas.
* Controles de acceso.
* Controles de seguridad.

C. Control de procedimientos específicos informáticos: Se revisara su existencia en las áreas fundamentales, donde se deberá comprobar que los procedimientos específicos no se oponen a los procedimientos generales, es decir que los procedimientos generales y de informática deben ser coherentes, consistentes, compatibles y subordinados a los procedimientos y áreas de la empresa.

2.6. MARCO CONCEPTUAL

2.6.1. Auditoría

Se considera que la auditoría son los ojos y oídos de la dirección, que generalmente no puede, no sabe o no debe realizar las verificaciones y evaluaciones.

La palabra auditoría viene del latín auditorius y de esta proviene auditor, que tiene la virtud de oír y revisar cuentas, pero debe estar encaminado a un objetivo especifico que es el de evaluar la eficiencia y eficacia con que se esta operando para que, por medio del señalamiento de cursos alternativos de acción, se tomen decisiones que permitan corregir los errores, en caso de que existan, o bien mejorar la forma de actuación. La auditoría es contar con los mecanismos para poder determinar que es lo que sucede en el sistema, que es lo que hace cada uno y cuando lo hace.

2.6.1.1. Concepto de auditar

Auditar, en su acepción más amplia significa verificar si la información financiera, operacional y administrativa que se presenta es confiable, veras y oportuna.

Es revisar que los hechos, fenómenos y operaciones se den en la forma como fueron planeados; que las políticas y lineamientos establecidos han sido observados y respetados; que se cumplen con obligaciones fiscales, jurídicas y reglamentarias en general.

Es evaluar la forma como se administra y opera teniendo al máximo el aprovechamiento de los recursos.

2.6.1.2. Técnicas de auditoría

Las técnicas de auditoría a tratar en el presente están orientadas fundamentalmente hacia la auditoría de estados financieros; sin embargo, es de observar que son de aplicación general a cualquier tipo de auditoría.

Técnicas de auditoría, son los métodos prácticos de investigación y prueba que el contador público utiliza para lograr la información y comprobación necesaria para poder emitir su opinión profesional, su objetivo consiste en proporcionar elementos técnicos que pueden utilizar el auditor para obtener la información necesaria que fundamente su opinión profesional sobre la entidad sujeta a su examen, las técnicas de auditoría son las siguientes:

Estudio general: Apreciación sobre la fisonomía o características generales de la empresa, de sus estados financieros y de las partes importantes, significativas o extraordinarias. Esta apreciación se hace aplicando el juicio profesional del contador publico que, basado en su preparación y experiencia, podrá obtener de los datos o informaciones originales de la empresa que se va a examinar, situaciones importantes o extraordinarias que pudieran requerir atención especial, esta técnica sirve de orientación para la aplicación de otras técnicas por lo que, generalmente deberá aplicarse antes de cualquier cosa.

2.6.2. Sistema

Un sistema es un grupo de elementos interdependientes que interactúan regularmente formando un todo organizado, el concepto tiene dos usos muy diferenciados, que se refieren respectivamente a los sistemas de conceptos y a los objetos reales más o menos complejos y dotados de organización.

2.6.2.1. Sistema de información

Es un conjunto de elementos interrelacionados que permite capturar, procesar datos, para generar salidas, se encarga de administrar y organizar adecuadamente la información en una entidad, apoyando la toma de decisiones.

Dentro de las actividades principales de un sistema de información se encuentra:

Capturar datos: Existen dos formar de capturar los datos, de manera manual en el caso de facturas, a través de listados entre otros documentos, y de manera automatizada, cuando se utilizan dispositivos especiales como sensores, o láser que permiten capturar el moviendo, el calor, la presión etc.

Procesar los datos: En este proceso el sistema toma las entradas y las transforma a través de cálculos, estadísticas, validaciones, búsquedas etc.

Almacenamiento de datos o información. Se puede generar:

- Listados: secuencia no excluyentes de datos.
- Reportes: Información seleccionada, especialización de los datos.
- Medios magnéticos.
- Otros sistemas.
- Feek back o retroalimentación.
- Señales de salida que se convierten en entrada.

La arquitectura de un sistema de información consiste en identificar las entradas, procesos y sitios de almacenamiento (base de datos).

2.6.2.2. Auditoría a sistemas de información

Es el examen y evaluación de los procesos del área de procesamiento automático de datos (PAD) y de la utilización de los recursos que en ellos intervienen, para llegar a establecer el grado de eficiencia, efectividad y economía de los sistemas computarizados en una empresa y presentar conclusiones y recomendaciones encaminadas a corregir las deficiencias existentes y mejorarlas. Los aspectos que generalmente evalúa la auditoría a un sistema de información es:

1. Eficiencia en el uso de los recursos informáticos.

2. Validez de la información.
3. Efectividad de los controles establecidos.
4. seguridad física y lógica.

2.6.3. Aspectos que se tienen en cuenta en el análisis de la calidad de un sistema de información

2.6.3.1. Efectividad

Congruencia entre lo planificado y los logros obtenidos en el tiempo, se refiere a que la información relevante sea pertinente para el proceso del negocio, así como a que su entrega sea oportuna, correcta, consistente y de manera utilizable.

2.6.3.2. Eficiencia

Es la capacidad administrativa de producir, acción, fuerza, producción, el máximo de resultados con el mínimo de recursos, el mínimo de energía y en el mínimo de tiempo posible, se refiere a la provisión de información a través de la utilización óptima (más productiva y económica) de recursos.

2.6.3.3. Confiabilidad

La confiabilidad de la información hace referencia a la provisión de información apropiada para la administración con el fin de operar la entidad y para ejercer sus responsabilidades de reportes financieros y de cumplimiento.

2.6.3.4. Cumplimiento

Se refiere a la disponibilidad de la información cuando ésta es requerida por el proceso de negocio ahora y en el futuro. También se refiere a la salvaguarda de los recursos necesarios y capacidades asociadas.

2.6.4. Requerimientos de seguridad

2.6.4.1. Confidencialidad

Se refiere a la protección de información sensible contra divulgación no autorizada.

2.6.4.2. Integridad

La integridad se refiere a la seguridad de que una información no a sido alterada, borrada, reordenada, copiada, etc., bien durante el proceso de transmisión o en su propio equipo de origen. Es un riesgo común que el atacante al no poder descifrar un paquete de información y, sabiendo que es importante, simplemente lo intercepte y lo borre.

2.6.4.3. Disponibilidad

Al hablar de disponibilidad se refiere a la disponibilidad de la información cuando ésta es requerida por el proceso de negocio ahora y en el futuro. También se refiere a la salvaguarda de los recursos necesarios y capacidades asociadas.

2.6.5. Estructura organizacional de una empresa

2.6.5.1. Planeacion estratégica informática

Es un proceso en el cual los administradores de la organización obtienen, procesan, analizan información interna y externa de la organización para determinar el estado de la misma, mediante este proceso se busca anticipar, es decir anticipar el futuro para poder definir: donde nos encontramos?, a donde podemos ir?, a donde debemos ir?, como estamos llegando a nuestras metas?.

La planeacion estratégica informática tiene 6 elementos que son:

a) Estrategias: Son las estrategias para que los funcionarios de la empresa consigan sus objetivos.

b) El direccionamiento: Permite definir un plan marco de desarrollo institucional, donde se enmarcan los principios corporativos, la visión y la misión de la entidad.
c) El diagnostico: Es un referente para estudiar la situación interna y externa de la organización, responde a las preguntas: donde estamos?, donde nos encontramos ahora?
d) Las opciones: Son la opciones estratégicas que se deben llevar a cabo, dentro de ellas encontramos: el análisis DOFA, análisis de vulnerabilidades de la empresa, entre otros.
e) La formulación: Se hace a través de proyectos, planes de acción con responsables y permite generar proyectos tangibles.
f) La auditoría, evaluación: Presenta índices de gestión sobre la evaluación critica de los objetivos, planes acción, procesos, infraestructura, software, entre otros.

2.6.5.2. Política

Es el proceso y actividad, orientada ideológicamente, de toma de decisión de un grupo para la consecución de unos objetivos.

2.6.5.3. Responsabilidad

La responsabilidad es la virtud o disposición habitual de asumir las consecuencias de las propias decisiones, respondiendo de ellas ante alguien. Responsabilidad es la capacidad de dar respuesta de los propios actos.

2.6.5.4. Plan de contingencias

Pese a todas las medidas de seguridad puede ocurrir un desastre, de hecho los expertos en seguridad afirman “sutilmente” que hay que definir un plan de recuperación de desastres “para cuando falle el sistema”, no por “si falla el sistema”.

Por lo tanto, es necesario que el plan de contingencias que incluya un plan de recuperación de desastres, el cual tendrá como objetivo, restaurar el servicio de cómputo en forma rápida, eficiente y con el menor costo y pérdidas posibles. Si bien es cierto que se pueden presentar diferentes niveles de daños, también se hace necesario presuponer que el daño a sido total, con la finalidad de tener un plan de contingencias lo mas completo y global posible.

Un plan de contingencias de seguridad informática consiste los pasos que deben seguir, luego de un desastre, para recuperar, aunque sea parte, la capacidad funcional del sistema aunque, y por lo general, constan de reemplazos de dichos sistemas. Se entiende por recuperación. “tanto la capacidad de seguir trabajando en un plazo mínimo después de que se haya producido el problema, como la posibilidad de volver a la situación anterior al mismo, habiendo reemplazado o recuperado el máximo posible de los recursos e información”.

Se dice que el plan de contingencias es el encargado de sostener el modelo de seguridad informática planteado y de levantarlo cuando se vea afectado, La recuperación de la información se basa en el uso de una política de copias de seguridad (backup) adecuada.

3. METODOLOGÍA

3.1. TIPO DE ESTUDIO

Partiendo de que el contexto para el desarrollo este proyecto, es una entidad prestadora del servicio de salud, de carácter publico y catalogada en tercer nivel, a la cual se le exige la acreditación en sus diferentes procesos y dependencias; el área de información y sistemas a encontrado la necesidad de realizar una auditoría a los nuevos módulos que se están incorporando al sistema dinámica gerencial, especialmente en relación a historia clínica electrónica,, puesto que es un proceso que cambiara de manera significativa la atención de los pacientes.

De manera general la metodología a utilizar para el desarrollo de este proyecto, esta enfocada como primera instancia en la realización del análisis preliminar donde se identificara los objetivos y el alcance del proyecto, como también se conocerá todo el entorno del hospital universitario departamental de Nariño, en relación a sus funcionarios, la infraestructura física, el sistema de información, las dependencias y sus diferentes procesos, para luego continuar con la asignación de los recursos lo cual se planificara con el coordinador del área de sistemas, una vez conocido el entorno se proseguirá con la realización del programa de auditoría, donde se determinaran los aspectos a evaluar, las actividades y las pruebas a desarrollar, esto con el fin de recolectar las evidencias, identificar cuales son los riesgos relacionados con el módulo de historia clínica, y determinar si los diferentes procesos han sido llevados a cabo de forma correcta; finalmente en base al desarrollo de las actividades anteriores, se podrá obtener una visión critica que permitirá denotar los hallazgos y las recomendaciones necesarias, las cuales serán documentadas en un informe final que será socializado con el coordinador del área de información y sistemas.

Para el desarrollo de la auditoría al módulo de historia clínica electrónica, se seguirán los siguientes patrones:

1. Análisis preliminar de la entidad para visualizar el objeto de investigación que es el módulo de historia clínica.

2. Definir los alcances del proyecto, teniendo en cuenta que solo se auditara al módulo de historia clínica de dinámica gerencial, determinando los dominios referenciales a los que se enfocara la auditoría en relación a aspectos de seguridad, administración, configuración y calidad.

3. Recolección de la información del entorno relacionado con la gestión de historia clínica como: políticas de la institución, aspectos legales, requerimientos de los usuarios finales (médicos y enfermeras), requerimientos de la administración del hospital y del área de información y sistemas, todo esto se realizara mediante el uso de herramientas como la observación, entrevistas, encuestas a los funcionarios y usuarios, confirmación y revisión de documentos, manuales y normas, con el fin de identificar las vulnerabilidades, riesgos, amenazas y fallas dentro del HUDN.

4. Elaboración del programa de auditoría, para lo cual se utilizara como herramienta el COBIT (Control Objectives for Information and related Technology); el cual permite definir los procesos y las actividades a auditar, brindando unos criterios de información y los recursos sobre los cuales se realizara el análisis, teniendo en cuenta el nivel de clasificación establecido con fin de priorizar ciertas actividades.

5. Elaboración de los cuestionarios en base a cada uno de los objetivos de control planteados en el programa de auditoría.

6. Aplicación de los cuestionarios al personal correspondiente, con el fin de evidenciar, las fallas e inconsistencias encontradas en los procesos evaluados.

7. En base a los resultados de los cuestionarios, realizar las pruebas pertinentes en relación a: revisión de documentos, verificación de procesos entrevistas al personal involucrado con el proceso, utilizar diversos medios para aporte de pruebas a las fallas existentes (cámara digital, filmadora, grabadora), realización de las pruebas de ejecución en relación al aplicativo, la base de datos, la seguridad física y lógica, todo esto con el fin de contar con el fundamento necesario para hacer el análisis y conclusión de cada proceso a auditar.

8. En base a las actividades anteriores, a las fallas y evidencias encontradas, determinar los hallazgos, mostrar cuales son las posibles causas y el impacto que ocasionan en el desenvolvimiento de la institución, con el fin principal de elaborar la recomendaciones necesarias que establezcan los controles a implementar para mejorar el desempeño del módulo de historia clínica su gestión y manejo.

9. Presentación del informe final de auditoría al personal administrativo y de sistemas involucrados con el manejo de historia clínica electrónica,

3.2. INSTRUMENTO DE RECOLECCION DE DATOS

3.2.1. Fuentes primarias

Dentro de las fuentes primarias de información que se utilizaran para el desarrollo de este proyecto se encuentran:

- Entrevistas, que se realizaran al personal del área de información y sistemas, los usuarios finales del módulo (médicos y enfermeras), representante de SYAC, auditoría medica entre otros.
- Aplicación de cuestionarios a todo el recurso humano involucrado con el manejo del módulo de historia clínica.
- Manuales, políticas, planes y toda documentación relacionada con las actividades planteadas en el programa de auditoría, que tengan relación con el manejo de las tecnologías de información del hospital.

- Módulo de historia clínica del sistema dinámica gerencial.
- Base de datos relacionada con el módulo de historia clínica.

3.2.2. Fuentes secundarias

Dentro de las herramientas secundarias usadas para el desarrollo de este proyecto se encuentran los libros referenciales e internet, de donde se podrá consultar diferentes temas relacionados con la auditoría a sistemas de información, aspectos propios de las entidades de salud y la gestión de historia clínica entre otros.

4. DESARROLLO DEL PROYECTO

4.1. LEGAJO PERMANENTE

4.1.1. Ambiente general de la empresa

4.1.1.1. Nombre de la empresa

Hospital universitario departamental de Nariño E.S.E.

4.1.1.2. Reseña histórica del hospital universitario departamental De Nariño E.S.E.

El hospital se encuentra en el municipio de Pasto, dentro del departamento de Nariño el cual representa cerca del 3.48% del total de la población del país, con una población de aproximadamente 1.541.956 habitantes, de los cuales el 45.5% esta ubicado en las zona urbanas.

La institución mantiene cautivo el segmento de los servicios del III nivel de complejidad dentro de la región, al ser la única entidad con la capacidad técnica para atender este tipo de casos. Sin embargo, cuenta con la competencia de varias instituciones privadas que también ofrecen la prestación de servicios de salud de segundo nivel de complejidad, estas trabajan en su mayoría con los segmentos de mayor poder adquisitivo de la región, donde se encuentra la atención a particulares y al régimen contributivo, al igual que la mayor parte de los hospitales de referencia departamentales, el hospital de

Nariño atiende una cantidad importante de pacientes, especialmente de los segmentos más vulnerables de la sociedad, es decir los regímenes subsidiado y vinculado, los cuales componen el 87% de los usuarios de la institución.

En el mes de Marzo de 1967, el entonces presidente de la república, Dr. Carlos Lleras Restrepo, visita la ciudad y es enterado de las precarias condiciones funcionales del entonces hospital civil de pasto, y se compromete a facilitar las gestiones conducentes a la creación del hospital departamental de Nariño, en el mes de enero de 1970, se inicia el proceso de construcción y el 15 de diciembre de 1975, inició la prestación de servicios de salud, con la inauguración del servicio de consulta externa, en 1977, se dio apertura a los servicios de hospitalización, con medicina interna, cirugía, gineco obstetricia, pediatría y las unidades de apoyo como radiología, laboratorio, patología, rehabilitación, farmacia y nutrición, en 1976, y por las políticas imperantes a la fecha, el hospital se convierte en la sede de la regional central No 1 y se coloca bajo su cuidado, al hospital infantil los ángeles y 18 organismos de salud de baja complejidad. En el año de 1987, el gobierno del Japón se vincula a la región y al hospital, a través de un proyecto de cooperación internacional, realizando una importante donación en equipos médicos que colocaron al hospital en ésa época, a la vanguardia de la tecnología biomédica.

Con el advenimiento de la ley de seguridad social, el hospital, inicia los caminos tendientes a adaptarse, al nuevo modelo, y se transforma en empresa social del estado; sin embargo la ausencia de modelos de gestión, la injerencia política, y fenómenos de corrupción, sumieron al hospital en profundas crisis, que comprometieron el logro de los objetivos institucionales y condujeron a una pérdida de confianza por parte de la sociedad en la organización, durante 1999, y sumido en una gran crisis institucional, el estado colombiano interviene y se produce la reestructuración de la organización con el apoyo, con una nueva estructura, el hospital enfrenta el nuevo siglo, sin embargo al no corregirse las verdaderas causas de la crisis (ausencia de modelos de gestión e injerencia política), la inestabilidad institucional continua.

En el año de 2003, se convoca un concurso de méritos para la selección de un nuevo gerente y el gobernador del departamento de Nariño de la época respeta los resultados del mismo y nombra al ganador de la convocatoria a Bernardo Ocampo Martínez, quien presenta a la junta directiva un plan de desarrollo, que se convierte en el norte a seguir. En el año 2004, la honorable asamblea del departamento, modifica los estatutos, establece una nueva estructura, que está de acuerdo con el desarrollo de la estrategia y que se debe adaptar a la cultura de calidad que se pretende construir y lo convierte en hospital universitario departamental de Nariño empresa social del estado.

En el período 2003-2006, (período para el cual fue nombrado el actual gerente), se subsidia al estado colombiano en un suma superior a los 9 mil millones de pesos correspondientes a excedentes de facturación de pacientes vinculados, y se programan inversiones superiores a los 10 mil millones de pesos en modernización de la infraestructura y adquisición de tecnología.

En el año 2006, el gobernador del departamento nombra a Bernardo Ocampo Martínez para un nuevo período de tres años, entendiendo la importancia de la continuidad de la gestión.

En éste año, es publicado el ranking de instituciones prestadoras de servicios de salud, y el hospital universitario departamental de Nariño, es clasificado como el primero en la categoría de mediana complejidad, simultáneamente la presidencia de la república a través del departamento administrativo de la función pública, considera que en el hospital existe una experiencia exitosa de gestión y recomienda la inscripción en el banco de éxitos de la función pública la experiencia del hospital: “el direccionamiento estratégico con enfoque prospectivo para el éxito y la competitividad en las empresas sociales del estado”.

4.1.1.3. Situación antes de la creación del hospital universitario departamental de Nariño

La más antigua referencia que al respecto se encuentra en el departamento de Nariño, es la fundación del hospital San Pedro, uno de los hospitales más antiguos del sur occidente colombiano, fundado en 1886 por don Pedro Vela y Figueroa, esta institución a prestado servicios ininterrumpidos a la comunidad nariñense, por esto es considerado como un verdadero patrimonio social. Este hospital de caridad se pone en manos y bajo la dirección de las hermanas de la caridad, las religiosas Vicentinas se hicieron cargo del hospital San Pedro, actualmente se encuentra en reestructuración y se describe como una entidad de II nivel de complejidad en el departamento de Nariño, se encuentra ubicado en el inmediaciones del barrio san juan de dios. En segunda instancia se tiene como centros hospitalarios del departamento, al hospital civil de pasto que fue creado como institución oficial de carácter departamental, mediante decreto 259 de abril 20 de 1939 del ejecutivo departamental, con personería jurídica No. 985 de diciembre de 1972 en las instalaciones donde actualmente funciona el centro de salud del calvario. Actualmente se encuentra ubicado en el barrio corazón de Jesús del municipio de pasto y a iniciado el proceso de modernización de su plata física y de gran parte de su información, catalogándose como una entidad de salud de II nivel que acoge a la población de régimen subsidiado, y vinculado por excelencia, quedando el hospital civil como dependencia directa desde 1976 del hospital departamental de Nariño.

El 31 de mayo de 1952 se fundó el hospital infantil los ángeles, gracias a un grupo de damas y ciudadanos deseosos de dar respuesta a las necesidades de salud de la niñez de la comunidad. En 1953 se reconoce personería jurídica al hospital infantil mediante resolución No 24 del mes de febrero del mismo año, actualmente cuenta con instalaciones dotadas de implementos modernos que atienden a la población de menores de la capital nariñense, se encuentra ubicado en la avenida de los estudiantes y se perfila como uno de los organismos mejor dotados del departamento para la atención infantil.

4.1.1.4. Creación del hospital universitario departamental de Nariño E.S.E

El hospital universitario departamental de Nariño, entró en operación desde el 15 de diciembre de 1975 en la ciudad de Pasto, como la única organización de la red pública de atención de la región. En octubre de 1990, es clasificado como un organismo para prestación del servicio de salud en un III nivel de complejidad. En 1994, se convirtió en empresa social del estado del orden departamental, con patrimonio propio y autonomía administrativa, según la ley 100 de 1993, conforme a esta norma y en concordancia con el plan nacional de desarrollo está obligado a mantener su auto sostenibilidad financiera, implementando procesos eficientes que le permitan ser competitivo en el mercado del área de influencia. A partir del 17 de Diciembre de 2004, se reestructuró la entidad como un hospital universitario, proyectándose como un eje de referencia en los avances científicos, tecnológicos y administrativos del Sur Occidente del País. La administración actual se encuentra enfocada hacia una idea de calidad, respaldada por la obtención de las certificaciones correspondientes. En estos momentos el hospital cuenta con la totalidad de sus servicios habilitados por parte del ministerio de protección social, pero la gerencia está buscando la obtención de la acreditación de la institución en servicios de salud, para la cual se ha venido preparando mediante la revisión y optimización de los procesos.

4.1.1.5. Al presente

El hospital universitario departamental de Nariño, es una entidad prestadora de servicios de salud de tercer nivel, que atiende a usuarios de régimen como: vinculado, contributivo, subsidiado, y otros.

Actualmente el hospital cuenta con 310 empleados de planta, de los cuales el 71% está compuesto por personal asistencial y el restante es de carácter administrativo, adicionalmente, a través de la contratación externa por cooperativas cuenta con 286 empleados más, que buscan garantizar la adecuada prestación del servicio de salud.

Al igual que la mayor parte de los hospitales de referencia departamentales, el hospital de Nariño atiende una cantidad importante de pacientes, especialmente de los segmentos más vulnerables de la sociedad, es decir los regímenes subsidiado y vinculado, los cuales componen el 87% de los usuarios de la institución.

El hospital universitario de Nariño ha presentado un plan ambicioso de inversiones para desarrollar en los próximos cuatro años, el valor de los proyectos equivale a $26.301 millones, dentro de los cuales se destaca la construcción de la unidad complementaria de servicios la cual busca que el hospital se convierta en una alternativa para atraer nuevos tipos de clientes y a su vez generar nuevos ingresos. Con esta edificación se espera renovar la sección de urgencias, sala de cirugías y la unidad de cuidados intensivos, entre otros.

4.1.1.6. Sistema de gestión estratégica del HUDN

En la búsqueda de un desarrollo integral y armónico del hospital universitario departamental de Nariño, se implementa un sistema de gestión Integral por calidad, para realizar las diferentes actividades de cada área, las cuales están organizados y definidos mediante un organigrama que representa el orden jerárquico de la institución.

En la búsqueda de un desarrollo integral y armónico del hospital universitario departamental de Nariño, se implementa un sistema de gestión Integral por calidad, con elementos como: el direccionamiento o gestión estratégica, la gestión por procesos y la gestión de la cultura.

La organización ha desarrollado un sistema de gestión estratégica (SGE), **(Fig.1.1)** cuya finalidad es agregar valor a los diferentes grupos de interés, a través de la definición de los objetivos estratégicos que los diferentes sistemas de gestión y grupos internos de trabajo que se deberán cumplir para alcanzar la visión.

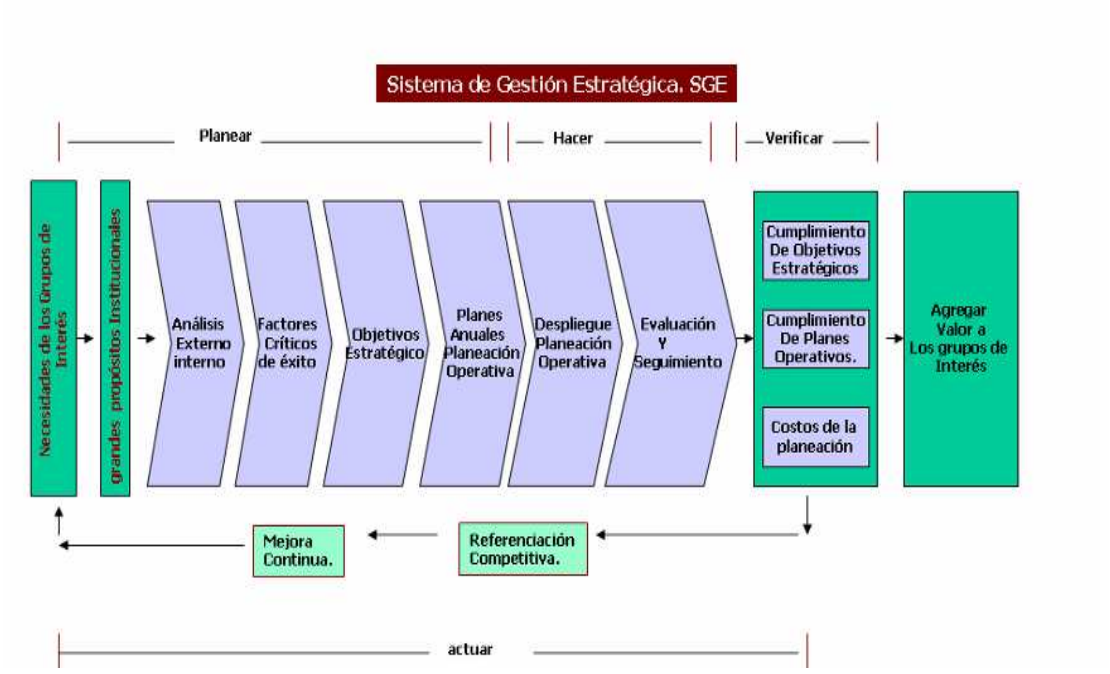


Figura 1.1

El sistema de gestión estratégica (SGE), se fundamenta en la declaración de la misión, visión, valores y políticas declaradas por la organización.

Es importante destacar que el espacio de trabajo para la auditoría del módulo de historia clínica electrónica, dentro del hospital universitario departamental de Nariño, será el área de información y sistemas y las áreas asistenciales en donde el módulo de historia clínica será implantando para el uso de personal propio de la sección y usuarios del hospital, estas áreas incluyen: triage, urgencias, hospitalización, y consulta externa.

4.1.1.7. Marco legal del módulo de historia clínica en el HUDN

El desarrollo de la interventoría esta enmarcado en el cumplimiento de las directrices de la gerencia del hospital universitario departamental de Nariño E.S.E, específicamente en las funciones del módulo de historia clínica, los interventores a cargo dentro del contrato OJ006-2008 que hace referencia a la adquisición, implementación y actualización del aplicativo dinámica gerencial hospitalaria dentro de la organización son:

- Ing. Roberto Yánez C. Coordinador del área de sistemas
- Dr. Javier Andrés Ruano Asesor de planeación
- Dr. Vicente López Juelpaz Coordinador de recursos financieros
- Dr. Héctor Fabio Quiroz O Asesor de control interno del HUDN

4.1.1.8. Recursos técnicos del módulo de historia clínica electrónica,

El hospital universitario departamental de Nariño, dispone de más de 249 equipos distribuidos entre las diferentes dependencias de la institución, utilizados para la realización de sus actividades en las distintas áreas; y durante el desarrollo de procesos de sistema, los equipos de cómputo se irán actualizando a nivel de software y de hardware paralelamente a la asignación del presupuesto asignado.

Dentro del proceso de implementación e implantación del módulo de historia clínicas se han dispuesto un total de 19 portátiles, 46 equipos PC y 15 impresoras, entregados por convenio con la universidad mariana.

La relación y el inventario de los equipos nuevos para la implementación del módulo de historia clínica, se adjunta en este legajo, no viéndose conveniente anexar el inventario correspondiente a todo el hardware de la organización, que no ha sido sometido a un proceso de actualización desde el año 2006. Dentro de la institución se han detallado los siguientes sistemas operativos, por inspección de los equipos y las áreas donde se encuentran ubicados respectivamente: windows 98, windows xp, windows vista, y windows 2003 server, se maneja antivirus cliente – servidor symantec y las bases de datos están implementadas bajo sql server y oracle.

4.1.2. Organización administrativa

4.1.2.1. Área de información y sistemas

El hospital departamental de Nariño es una entidad social del estado, cuyo propósito es brindar y prestar servicios salud, particularmente para la atención

del régimen subsidiado y vinculado de la región, de acuerdo con el articulo 51 de la ley 715 de 2001.

La institución se encuentra ubicada en el parque bolívar, al sur oriente de la ciudad de pasto, cuenta con su propia planta física, y está en remodelación de su espacio y la construcción de una unidad complementaria de servicios de salud.

Dentro de sus políticas cabe destacar:

De calidad: El compromiso es superar las necesidades y expectativas de los clientes internos y externos, contribuyendo positivamente al mejoramiento de la calidad de vida de los habitantes de la región, para lo cual el hospital a decidido establecer y mejorar continuamente el sistema de gestión Integral para la calidad, garantizando una atención humanizada, dentro del marco legal existente, con competencia técnica y científica, oportunidad e información clara y real a los usuarios y sus familias, involucrando en este propósito el desarrollo integral y participativo tanto en de los trabajadores como de proveedores, logrando con ello el crecimiento de la organización.

Ambiental: Los esfuerzos de la organización están dirigidos a la preservación del medio ambiente, y la creación de una cultura de coeficiente que estandarice las acciones, bajo la aplicación de un sistema integral de administración ambiental.

Salud ocupacional: El hospital universitario departamental de nariño ese declara su especial interés, por la protección de la integridad de sus trabajadores, usuarios y comunidad que directa o indirectamente están involucrados en los procesos, a través de la identificación de los factores de riesgo en los puestos de trabajo, su evaluación y el control de estos, asignando recursos necesarios e implementando procesos de mejoramiento continuo

orientados a la prevención de accidentes de trabajo y enfermedades profesionales dentro del marco legal.

De equidad: Es compromiso de la organización, impulsar la equidad entre hombres y mujeres, asegurando la igualdad de oportunidades, favoreciendo la equidad de género, así como el cumplimiento de la ley en cuanto fortalecer ambientes de trabajo en donde se respete la dignidad de la personas.

Administrativa: Modernizar sistemas y procesos acorde con la normatividad, alienando la estructura a la estrategia y a la cultura deseada.

Laboral: Proporcionar condiciones adecuadas de trabajo para mejorar la calidad de vida de sus trabajadores y propiciar su desarrollo.

Social: Promover la activa participación de comunidad en los procesos de desarrollo organizacional y coadyuvar a la creación de estilos de vida saludables con actividades de promoción en el nivel de complejidad.

Económica-Financiera: Administrar correctamente los bienes y recursos para el óptimo beneficio empresarial y lograr la eficiencia operativa al menor costo.

Las políticas descritas, están articuladas y propenden por el cumplimiento de la política nacional de prestación de servicios de salud, que pretende garantizar el acceso, optimizar el uso de los recursos y mejorar la calidad de los servicios que se prestan a la población.

4.1.2.2. Organización jerárquica de la institución

El organigrama del hospital universitario departamental de Nariño E.S.E. representa el orden jerárquico de la institución, este se ha diseñado para especificar el nivel y las funciones de las diferentes áreas.

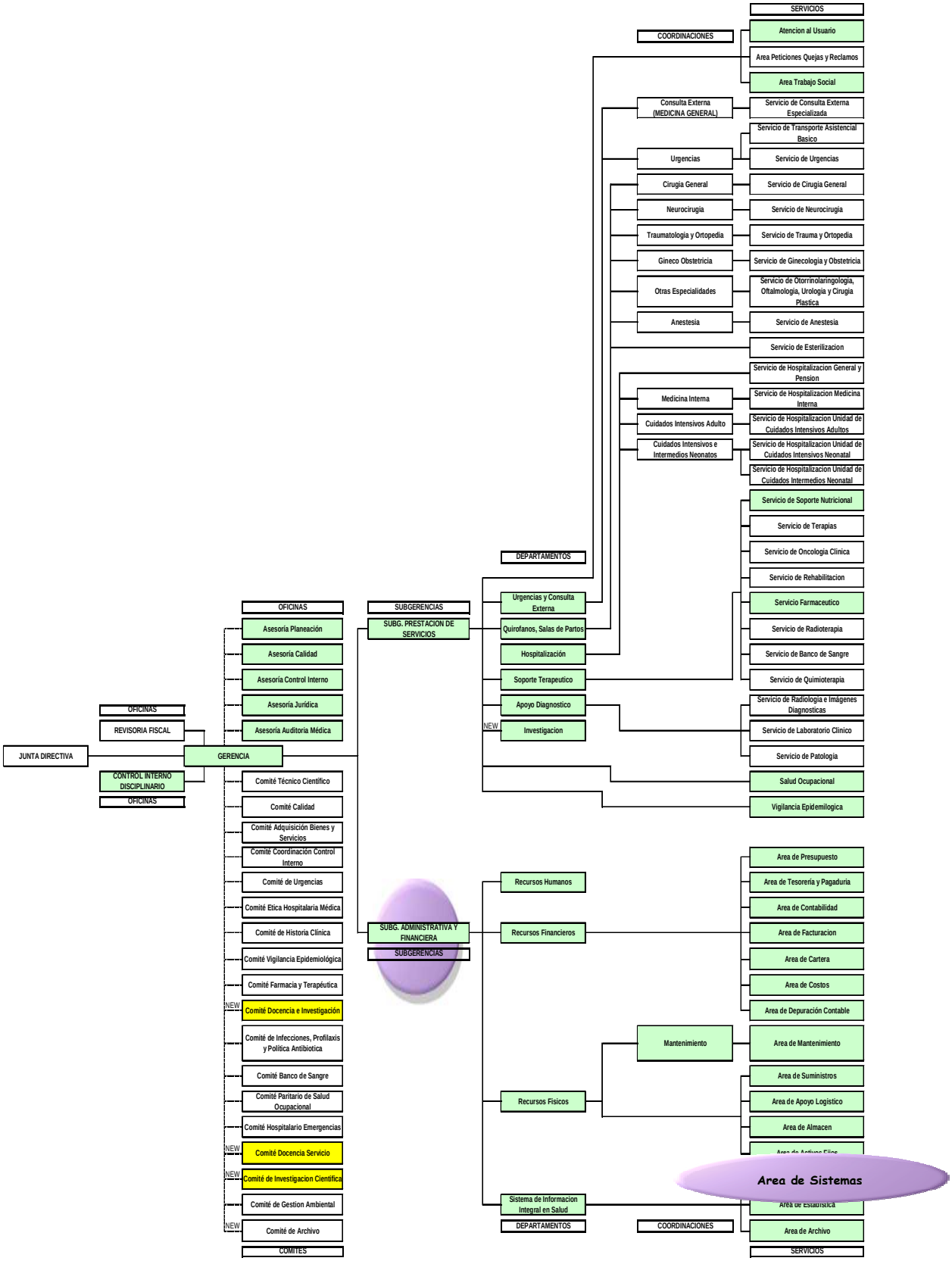

JUNTA DIRECTIVA
OFICINAS
REVISORIA FISCAL
CONTROL INTERNO DISCIPLINARIO
OFICINAS
GERENCIA
OFICINAS
Asesoría Planeación
Asesoría Calidad
Asesoría Control Interno
Asesoría Jurídica
Asesoría Auditoria Médica
COMITES
Comité Técnico Científico
Comité Calidad
Comité Adquisición Bienes y Servicios
Comité Coordinación Control Interno
Comité de Urgencias
Comité Etica Hospitalaria Médica
Comité de Historia Clínica
Comité Vigilancia Epidemiológica
Comité Farmacia y Terapéutica
NEW
Comité Docencia e Investigación
Comité de Infecciones, Profilaxis y Política Antibiotica
Comité Banco de Sangre
Comité Paritario de Salud Ocupacional
Comité Hospitalario Emergencias
NEW
Comité Docencia Servicio
NEW
Comité de Investigacion Cientifica
Comité de Gestion Ambiental
NEW
Comité de Archivo
SUBGERENCIAS
SUBG. PRESTACION DE SERVICIOS
SUBG. ADMINISTRATIVA Y FINANCIERA
SUBGERENCIAS
DEPARTAMENTOS
Urgencias y Consulta Externa
Quirofanos, Salas de Partos
Hospitalización
Soporte Terapeutico
Apoyo Diagnostico
NEW
Investigacion
Recursos Humanos
Recursos Financieros
Recursos Fisicos
Sistema de Informacion Integral en Salud
DEPARTAMENTOS
COORDINACIONES
Consulta Externa (MEDICINA GENERAL)
Urgencias
Cirugia General
Neurocirugia
Traumatologia y Ortopedia
Gineco Obstetricia
Otras Especialidades
Anestesia
Medicina Interna
Cuidados Intensivos Adulto
Cuidados Intensivos e Intermedios Neonatos
COORDINACIONES
Mantenimiento
SERVICIOS
Atencion al Usuario
Area Peticiones Quejas y Reclamos
Area Trabajo Social
Servicio de Consulta Externa Especializada
Servicio de Transporte Asistencial Basico
Servicio de Urgencias
Servicio de Cirugia General
Servicio de Neurocirugia
Servicio de Trauma y Ortopedia
Servicio de Ginecologia y Obstetricia
Servicio de Otorrinolaringologia, Oftalmologia, Urologia y Cirugia Plastica
Servicio de Anestesia
Servicio de Esterilizacion
Servicio de Hospitalizacion General y Pension
Servicio de Hospitalizacion Medicina Interna
Servicio de Hospitalizacion Unidad de Cuidados Intensivos Adultos
Servicio de Hospitalizacion Unidad de Cuidados Intensivos Neonatal
Servicio de Hospitalizacion Unidad de Cuidados Intermedios Neonatal
Servicio de Soporte Nutricional
Servicio de Terapias
Servicio de Oncologia Clinica
Servicio de Rehabilitacion
Servicio Farmaceutico
Servicio de Radioterapia
Servicio de Banco de Sangre
Servicio de Quimioterapia
Servicio de Radiologia e Imágenes Diagnosticas
Servicio de Laboratorio Clinico
Servicio de Patologia
Salud Ocupacional
Vigilancia Epidemilogica
Area de Presupuesto
Area de Tesorería y Pagaduria
Area de Contabilidad
Area de Facturacion
Area de Cartera
Area de Costos
Area de Depuración Contable
Area de Mantenimiento
Area de Suministros
Area de Apoyo Logistico
Area de Almacen
Area de Sistemas
Area de Estadistica
Area de Archivo
SERVICIOS

Figura No. 1 Organigrama del hospital universitario departamental de Nariño.

4.1.2.3. Organigrama del área de información y sistemas

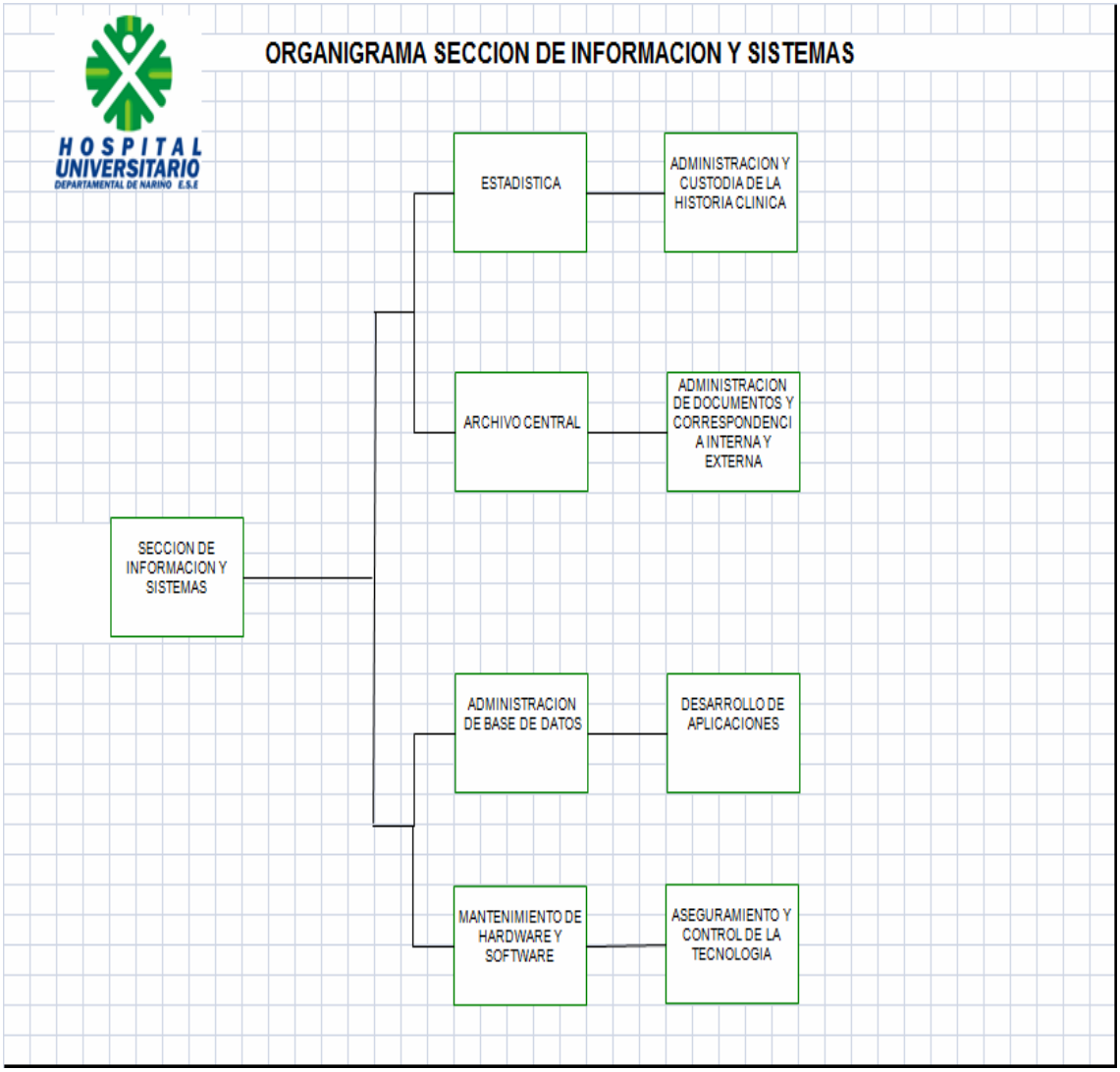


Figura No. 2 (Organigrama de la sección)

Enfoque:

La experiencia y conocimiento de los procesos que se realizaron teniendo en cuenta los requerimientos del sistema de información nos permite obtener

información detallada de todos los informes solicitados por entidades, es decir de los clientes internos como externos de la institución.

Cada área funcional realiza un análisis de las necesidades de información como también su priorización y periodicidad que permiten en conjunto con los ingenieros de soporte establecer cuales son las variables que tienen que trabajar con el fin de obtener una información que servirán como entradas a los diferentes procesos y su posterior procesamiento y entrega de información a los clientes internos como externos.

Estos requerimientos de información y el análisis de la misma permiten realizar planes de acción que posibiliten cumplir con los estándares de acreditación dentro del estándar de gerencia de información, de igual manera los análisis determinan las fortalezas y oportunidades de mejoramiento que llevaran a desarrollar productos como aplicaciones a la medida para las áreas que lo requieran, con el fin de satisfacer las necesidades de los clientes.

Los diagnósticos que se realizan periódicamente a los módulos administrativos y asistenciales del sistema de información, permite determinar el porcentaje de funcionalidad y la confiabilidad de la información, como también las oportunidades de mejoramiento que son necesarios corregirlos y procesos que están sin implementar que se hace necesario sistematizarlos.

Estas oportunidades de mejoramiento se convierten en proyectos que son trasladados a los planes operativos anuales de la sección de información y sistemas para poder ser implementados en metodologías como ciclos de vida clásicos o creación y desarrollo de prototipos que implícitamente interactúan con el ciclo **p.h.v.a** (planear, hacer, verificar y actuar), para su posterior implantación.

4.1.2.4. Metodologías empleadas en el hospital universitario departamental de Nariño

Metodología ciclo de vida clásico:

Se utiliza esta metodología para la implementación de los proceso en cualquiera de las dependencias de la institución.

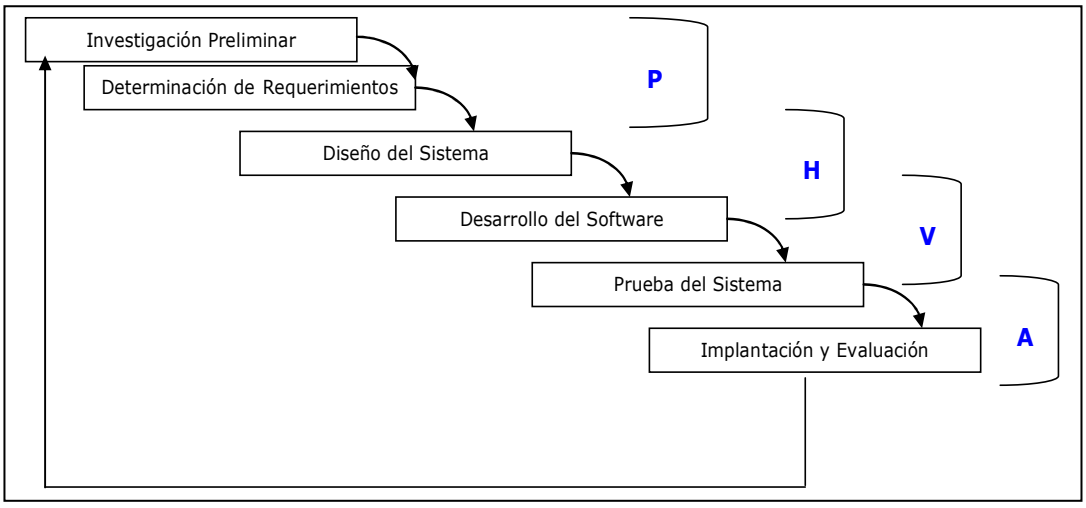


Figura No. 3 (Metodología ciclo de vida clásico)

*Implementación: E*l hospital tiene como soporte fundamental la información soportada en las historias clínicas y la información recolectada en el sistema de información que es alimentado por el personal asistencial y administrativo de la organización, esta historia clínica a sido el principal registro para la trazabilidad del servicio y el único soporte valido para justificar los servicios prestados por la organización; por lo tanto se enfocan importantes esfuerzos al diseño y desarrollo de un sistema de información especializado e integrado en donde uno de los ejes principales de este es la historia clínica del paciente que permita el flujo de información en los módulos relacionados con este como lo es facturación, inventarios, tesorería, etc. Logrando así efectividad en la gestión de procesos asistenciales y administrativos.

Dentro del plan estratégico se realizo un proyecto para implementar e implantar algunos módulos administrativos que se encontraban en muy baja producción como son los módulos de presupuesto, cartera, nomina y activos fijos, con el fin de dar solución a la demanda de soportes informáticos en las distintas áreas del negocio, satisfaciendo las necesidades de el cliente interno. Se han implementado aplicativos a la medida utilizando una base de datos relacional SQL server y una red de área local nivel cinco y seis que abarca toda la estructura de la organización tanto en cable como en fibra óptica lo que a permitido:

- Digitalización de los procesos de imágenes diagnosticas como es el caso del TAC, ecografía y radiología que son de disponibilidad inmediata desde cualquier lugar de la organización o de la red mundial internet.
- Confiabilidad y seguridad en la información, mediante los procesos de creación de perfiles de acceso y asignación de usuarios de acuerdo con los perfiles y las directrices de las coordinaciones de área.
- Sistema de información amigable bajo ambiente windows con opciones de ayudas y búsquedas con teclas especiales o de funciones.
- Integración entre los procesos asistenciales y administrativos lo que permite en tiempo real obtener información para la atención a los pacientes, proveedores, clientes y la alta gerencia.
- Manejo flexible de la información mediante la generación de reportes personalizados en cada uno de los módulos del sistema de información logrando así satisfacer los requerimientos internos de los usuarios, para que a su vez ello puedan prestar un mejor servicio a sus clientes.

El hospital ha dispuesto de un grupo de ingenieros, los cuales ponen en práctica procesos y procedimientos para mantener la continuidad del servicio las 24 horas del día y también evitar la perdida de información realizando actividades de copia de seguridad diarias internas y externas.

Metodología creación de prototipos

Esta es la metodología empleada en el área e información y sistemas para el desarrollo de sistemas.

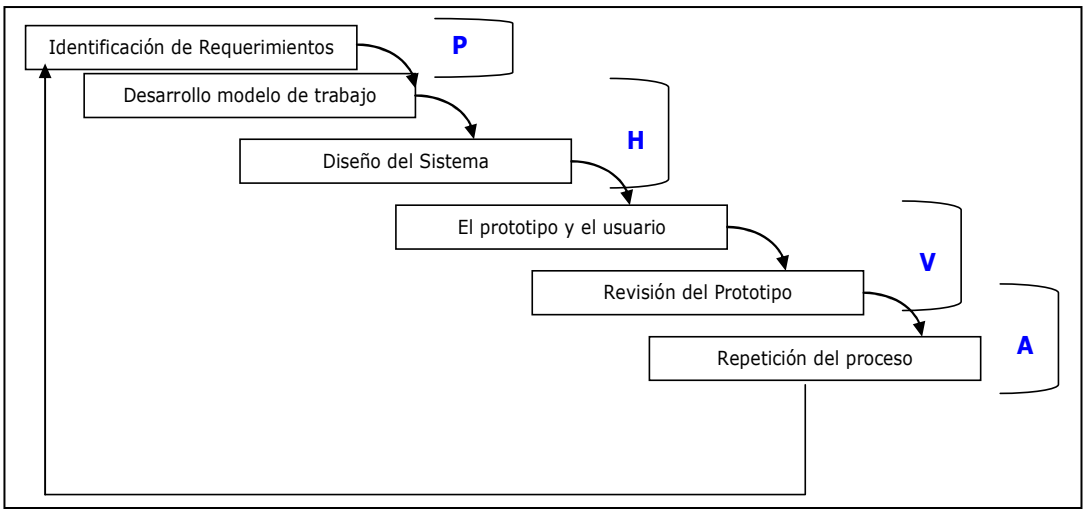


Figura No. 4 (Metodología creación de prototipos)

Evaluación y seguimiento: Teniendo en cuenta que la gestión de la información es la clave para dirigir y mejorar el desempeño organizacional y su competitividad se priorizan los criterios de confiabilidad, consistencia, seguridad, integridad y actualización de la información de la siguiente manera:

Confiabilidad y consistencia: Se basa en procesos mensuales rutinarios que realizan las áreas funcionales de la organización, de la información generada en línea y por lotes, con el fin de conciliar entre las mismas y determinar una información confiable que este acorde con la producción y venta de los servicios y en directa relación con la información contable y financiera de la institución.

Integridad y seguridad: Se aplican procedimientos establecidos en los estándares de acreditación que se encuentran definidos en la sección de información y sistemas procedimientos de custodia, backup, realizados en

áreas destinadas para tal fin como el área de estadística y sistemas de igual manera con backups que reposan en áreas externas de la institución.

Existen tres niveles de seguridad como son los del sistema operativo multiusuario, el sistema de información, y por ultimo el nivel de acceso a cada uno de los módulos.

Disponibilidad: Se asegura el almacenamiento de datos en base de datos de cada uno de los módulos, donde los clientes podrán tener acceso a información desde el año 2000, información que se entrega en tiempo real mediante el montaje de backus de periodos anuales en el sistema de información.

Oportunidad: Garantizar para los clientes externos e internos operaciones y registros en tiempo real y en línea mediante una tecnología de punta, con una red de área local de categoría 5 y 6 certificada y la reposición de equipos de cómputo actualizados con un alto rendimiento de procesamiento, ubicados en toda la infraestructura de la institución.

El diagnostico de el sistema de información se realiza mediante el manejo de no conformidades establecidos en la norma ISO 9001 y los planes de acción para su posterior corrección.

Los planes de acción son trasladados al plan operativo anual los cuales son controlados por las áreas administrativas y gerenciales de la institución revisando periódicamente su ejecución y se determina si se realizaron en el tiempo contemplado en un cronograma de actividades (5 W 1 H), o requieren su replanteamiento y requerimientos para su puesta en funcionamiento.

Las acciones incluyen desde mejorar procedimientos de índole administrativo y/o asistencial hasta la selección de una nueva solución Informática que apoye el sistema de información o el cambio o migración del mismo, que permita estar acorde con el crecimiento de la institución.

4.1.2.5. Análisis de la información

Enfoque: La generación y análisis de información de manera rutinaria o permanente han permitido obtener y desarrollar planes operativos anuales, planes de compras anuales que son controlados mensualmente con el fin de que se analicen los desfases presentados y poder realizar planes de mejoras. Como resultado se han obtenido una disminución de costos en las diferentes áreas asistenciales y/o administrativas de la organización como también invertir en aquellas áreas que presentan mayor productividad y que permitan apoyar las mayores necesidades de los clientes.

La información financiera ha sido pilar fundamental para lograr invertir en proyectos de infraestructura y adquisición de tecnología de punta todo esto gracias a tener una información confiable y veraz pilar fundamental de la alta gerencia para la toma de decisiones en estos grandes proyectos de inversión.

La implementación e implantación del sistema de información con sus 16 módulos administrativos y asistenciales han permitido un significativo mejoramiento en las áreas como archivo, facturación, almacén e inventarios, servicio farmacéutico, compras, contabilidad.

Implementación: Los funcionarios de las áreas administrativas y asistenciales, los lideres de los diferentes módulos, los ingenieros de soporte han desarrollado una cultura de conciliar la información generada como un proceso de auditoría previa con el fin de obtener una información confiable que permita la toma de decisiones, los módulos administrativos y asistenciales están totalmente adaptado a la legislación colombiana y gracias a que interactúa en

línea con los demás módulos, permite obtener información actualizada a nivel administrativo y, el estado de las cuentas por cobrar, las cuentas por pagar y la contabilidad general, y a su vez obtener los requerimientos legales y tributarios e informes para decisiones financieras. Lógicamente con aplicativos realizados a la medida que interactúan con las bases de datos del sistema de información. Los cuales fueron desarrollados como resultado del análisis de necesidades de información.

De igual manera se tiene aplicaciones de los grandes proveedores que han permitido sistematizar áreas como laboratorio, banco de sangre, nomina en la dispersión de fondos, radiología y tomografía mediante un proceso de digitalización de imágenes, servicio farmacéutico en su dosis unitaria mediante un proceso de benchmarking como punto de referencia de la mejor practica y en el año 2006 la digitalización de imágenes diagnosticas.

Como una empresa interesada en el proceso de actualización, capacitación e investigación en todas las áreas del conocimiento y especialmente en el área de la salud se cuenta con un acceso a Internet con un canal dedicado de 256 kb, que nos permite tener cobertura a conectar los 116 equipos de cómputo a la red mundial.

Se lleva un proceso de mantenimiento preventivo, detectivo y correctivo de todo el software y hardware de la institución con procesos establecidos y hojas de control que nos permite la recolección de hechos y datos logrando disminuir el porcentaje de daños en hardware o software mediante planes de acción rutinarios.

Una etapa de este proyecto de análisis de información precisa la construcción de un nuevo modelo de sistema de información, basado en el aprendizaje colectivo y la recopilación de las mejores prácticas. Como producto de esta etapa, se obtiene un mejoramiento sustancial de los sistemas de información, acorde a las necesidades del negocio y de los clientes internos y externos, en donde está contemplada la actualización de nuestras herramientas y uso de nuestras tecnologías de información.

De igual manera se contempla la implantación de la red estructurada de categoría 6 en la nueva unidad de servicios con equipos de cómputo de tecnología de punta y un software licenciado que permita la implementación del sistema de información.

Siguiendo el modelo de gestión integral por calidad, y en mira al proceso de acreditación se han acogido metodologías establecidas en ISO 9001, en el premio calidad en salud Colombia, premio colombiano a la calidad de la gestión y específicamente al estándar de gerencia de la información del proceso de acreditación para lograr contribuir a los 8 grandes objetivos estratégicos o de calidad y lograr así acreditarnos en un mediano plazo.

4.1.2.6. Cargos y funciones dentro del área de sistemas

Cargo: Técnico en estadística

1. Revisión cualitativa de historia clínica de pacientes hospitalizados.
2. Codificación de historias clínicas de hospitalización y consulta de observación.
3. Generación de informes estadísticos.
4. Manejo, revisión y registro de certificados de defunción.
5. Adiestramiento del personal nuevo en el área.
6. Supervisión de actividades realizadas por los auxiliares.
7. Elaboración informe mensual de egresos hospitalarios.
8. Elaboración informe mensual de procedimientos quirúrgicos.
9. Elaboración informe mensual de exámenes especiales de consulta externa.
10. Consolidación de informes periódicos (Producción y Calidad, Indicadores ministerio de protección social, plan de evaluación y seguimiento, red publica hospitalaria).
11. Participación en la generación y entrega de información esporádica.
12. Apoyar los procesos de referencia y contra referencia.
13. Participar en el comité de historias clínicas.
14. Integrar y apoyar al comité de estadísticas vitales.

15 Elaborar el informe de gestión de su cargo.

Cargo: Técnicos en sistemas (3)

1- Soporte de los módulos
    a. Facturación
    b. Admisiones
    c. Hospitalización
    d. Nomina
    e. Presupuesto

2- Soporte de las aplicaciones desarrolladas internamente
    a. Despacho facturación
    b. Conciliación facturación – contabilidad
    c. Verificador de derechos y Ley 387
    d. Registro de historias clínicas

3- Prestar soporte a las diferentes secciones en lo relacionado con informes acordes a sus módulos.

4- Análisis - diseño – desarrollo e implementación de herramientas que contribuyan a la administración de información, a nivel de toda la institución, según el plan de trabajo (POA), establecido para cada año.

5- Tener una semana de turno administrativo, durante la cual se da respuesta inmediata a todas las necesidades tanto de software o hardware que demande la institución, además de la verificación de la estabilidad y respaldo del sistema de información (DG), esta semana comprende un jornada semanal de 7:00 a.m. – 3:00 p.m., y los fines de semana o festivos de 10:00 a.m. – 12:00 m., y en horario no contemplado en este turno se tendrá disponibilidad inmediata según demanda.

6- Generar informes según demanda de los clientes internos y externos de la institución, de lo relacionado con la atención al paciente.

7- Trabajar en la identificación de problemas cuando la información generada presenta inconsistencias, y colaborar en la corrección de las mismas y en la búsqueda de acciones preventivas y correctivas que prevean este tipo de anomalías.

8- Contribuir en el proceso de recepción de facturas, que busca controlar la generación y despacho de facturación.

9- Colaborar en procesos específicos del manejo de información que sean requeridos de la parte administrativa.

10- Colaborar en el diseño e implementación de procesos sistematizados que permitan generar nuevos niveles de control, para facilitar la toma de decisión.

11- Contribuir con la implementación e implantación del portar empresarial e intranet en la institución.

12- Realizar jornadas de capacitación de ofimática, a los diferentes funcionarios de la institución.

13- Realizar actualizaciones a nuevas versiones del sistema de información DINAMICA GERENCIAL.

14- Participar en el proceso de acreditación del estándar de la información.

15- Acoger las nuevas funciones relacionadas con el cargo que sean asignadas por el jefe inmediato.

4.1.2.7. Descripción del personal encargado del módulo de historia clínica

Administrador de la red

Denominación Del Empleo**:**	Técnico en mantenimiento de sistemas y redes
Código:	4010

Funciones:

1. Instalar y/o distribuir los recursos de software y hardware a los usuarios según las disposiciones y necesidades.

2. Dar buena utilización a los elementos y equipos de trabajo y velar por el buen uso de los equipos de cómputo, en el sentido de orientar a los diferentes usuarios en las técnicas de su manejo.

3. Ejercer mantenimiento preventivo, detectivo y correctivo de hardware y software.

4. Realizar cotizaciones y procedimientos necesarios para la adquisición de equipos de cómputo y dispositivos de hardware requeridos por los diferentes usuarios.

5. Tener una semana de turno administrativo, durante la cual se da respuesta inmediata a todas las necesidades tanto de Software o Hardware que demande la institución, además de la verificación de la estabilidad y respaldo del sistema de información (DG), esta semana comprende un jornada semanal de 7:00 a.m. – 3:00 p.m., y los fines de semana o festivos de 10:00 a.m. – 12:00 m., y en horario no contemplado en este turno se tendrá disponibilidad inmediata según demanda.

6. Contribuir en el proceso de recepción de facturas, que busca controlar la generación y despacho de facturación.

7. Realizar jornadas de capacitación de ofimática, a los diferentes funcionarios de la institución.

8. Acoger las nuevas funciones relacionadas con el cargo que sean asignadas por el jefe inmediato.

Naturaleza de las funciones del cargo: Prestar servicios técnicos a la empresa, realizando acciones de mantenimiento preventivo y correctivo de la empresa física y/o de los equipos hospitalarios.

- Administrar la red de computadores.
- Servir de soporte técnico a las diferentes áreas.
- Garantizar la eficiencia, eficacia y buen desempeño de los equipos de cómputo en las actividades que realiza cada área.
- Analizar nuevas soluciones de implementación de software que permitan un óptimo desempeño del sistema.
- Control de virus en la red.

Coordinador Del Área De Sistemas

Denominación del cargo:	Jefe de sección recursos de información
Código:	2900

Naturaleza de Las funciones del cargo: Prestar servicios gerenciales en la sección de información, que garanticen el desarrollo de las políticas, normas, órganos, procedimientos e instrumentos que aplicados racional y coordinadamente permitan llevar a cabo los procesos de registro, manejo, archivo, clasificación de la información e indicadores.

Funciones:

- Analizar periódicamente el funcionamiento y efectuar las modificaciones necesarias buscando la adaptación a circunstancias de cambio en la concepción de la prestación de salud.
- Planear el número y clase de personal que la sección requiera.
- Entrevistar al personal en relación con las características del empleo.
- Orientar a los funcionarios nuevos en sus labores, en la organización del hospital, en sus relaciones con otras áreas y en la confidencialidad de la historia clínica.
- Supervisar el trabajo de los funcionarios.
- Dirigir las reuniones del personal para discusión de las actividades, explicaciones de nuevos principios e instrucción sobre nuevos procedimientos.
- Seleccionar y gestionar equipos y materiales.
- Colaborar con los diferentes comités en la preparación de los temarios de reuniones, cuando estos lo soliciten.
- Colaborar con el personal médico en el desarrollo de criterios y métodos para la evaluación de la calidad de atención.
- Estimular la investigación llamando la atención del personal científico sobre hallazgos insólitos en el análisis técnico de las historias clínicas.
- Colaboración en el establecimiento de normas con respecto al contenido de la historia clínica completa.
- Desarrollar procedimientos para establecer el curso que deben seguir los documentos hasta llegar a la historia clínica.
- Determinar con el personal médico las normas que rijan el registro de diagnósticos exactos y completos.
- Colaborar en el establecimiento de normas con respecto al contenido de las historias clínicas completas.
- Desarrollar procedimientos para establecer el curso que deben seguir los documentos hasta llegar a la historia clínica.
- Determinar con el personal médico las normas que rijan el registro de diagnósticos definitivos exactos y completos.

- Establecer con el nivel directivo, jefes de unidades y secciones, las necesidades de información médica y administrativa.
- Establecer el tipo de informes periódicos, contenido, indicadores, etc., que permitan satisfacer sus necesidades.
- Desarrollar instrumentos que permitan la recolección de los datos en las distintas unidades y secciones.
- Planear y desarrollar métodos sistematizados que permitan guardar oportunamente la información.
- Planear el sistema de archivo de historias clínicas de tal manera que satisfaga las necesidades del hospital.
- Recomendar el método más conveniente para la conservación de las historias clínicas, así como la conveniencia de la destrucción de algunas de ellas.
- Controlar el cumplimiento de las normas para la producción de información,
- indicadores, plazos, etc.
- Velar por el buen manejo de la historia clínica de acuerdo a las normas vigentes.
- Velar por el buen uso de los equipos y materiales de la sección.
- Organizar y mantener actualizada la sección de información de acuerdo al marco legal vigente de tal manera que sea capaz de presentar respuestas no solo a las necesidades de información para la atención del paciente, si no para la dinámica de los procesos de decisión y acción administrativa y científica.
- Identificar y definir el tipo de información a captarse, los indicadores mínimos necesarios, los flujos entre los diversos componentes del sistema de información para apoyar los procesos de evaluación, programación e investigación.
- Identificar los requerimientos de información de las demás secciones del hospital, del instituto departamental de salud y del ministerio de salud.
- Planear, desarrollar, dirigir y mantener actualizado el sistema de información de la entidad.

- Analizar periódicamente el funcionamiento del sistema de información del hospital, efectuando las modificaciones necesarias para adoptarlo a los requerimientos y cambios que imponga la normatividad del sistema de seguridad social en salud.
- Presentar informes estadísticos que sean requeridos por gerencia, subgerencias, jefes de sección y autoridades competentes.
- Colaborar en el establecimiento de parámetros para el desarrollo, revisión y evaluación técnica de las historias clínicas estableciendo parámetros con respecto a su contenido.
- Levantar procedimientos para establecer el curso que deben seguir los documentos hasta llegar a la historia clínica.
- Determinar con el personal médico las normas que rigen el registro de diagnósticos definitivos exactos y completos.
- Velar por el correcto archivo, conservación, custodia y reserva de las historias clínicas.

Técnicos en sistemas a cargo del soporte (3)

Control y administración de los registros paramétricos de la base de datos del sistema con respecto al módulo de historia clínica.

1) Análisis de los datos registrados en el módulo de historia clínica.
2) Análisis de los nuevos requerimientos para desarrollo en el sistema Dinámica gerencial.
3) Diagnostico de cada uno de los procesos involucrados en el módulo.
4) Y las demás funciones que demande su cargo.

Personal de soporte del módulo de historia clínica

De acuerdo a la resolución 0101 del 28 de febrero de 2008, por medio de la cual se conforman el equipo de liderazgo de implantación para llevar a cabo la sistematización del sistema de información de la organización, y se designan funciones de los miembros del equipo de trabajo así:

Conformación del equipo de liderazgo de implantación para el módulo de historia clínica

LIDER PRINCIPAL	INGENIERO DE SOPORTE
Dr. Héctor Fabio Sánchez (UCI)	Ing. Orlando García P (Quirófanos)
Ing. Adrian Gallego (Calidad)	Ing. Harold Ortega (Apoyo e imagenologia)
Jefe María Elena Erazo (Apoyo -diag)	Ing. Harold Ortega (Apoyo e imagenologia)
Dr. Germán Cadena (Auditoría)	Ing. Roberto Yánez C (Hospitalización)
Jefe Nubia Jurado (Hospitalización)	Ing. Roberto Yánez C (Hospitalización)
Dr. Miguel Guerrero (Apoyo Terapéutico)	Ing. Alexander Acosta (Apoyo - Terapéutico)
Jefe Gloria Córdoba (Urgencias)	Ing. William Solarte (Consulta Externa –Urgencias)
Edgar Acosta Santander (estadística)	Ing. William Solarte (Consulta Externa –Urgencias)

En su artículo primero se resuelve: de las funciones: las funciones que desempeñará el equipo líder serán:

- Cumplir a cabalidad con las directrices del comité técnico del hospital
- Verificar y reportar las novedades de todo cuanto suceda en cuanto hace referencia a las actualizaciones de los diferentes módulos en los cuales haya sido designado.
- Realizar el acompañamiento a las actualizaciones que realice el proveedor en los tiempos y métodos establecidos con el ánimo de realizar sugerencias en los aplicativos de acuerdo a lo contemplado en el contrato OJ 006-2008.

- Realizar las sugerencias pertinentes al proveedor en cuanto hace referencia a la inclusión en los diferentes módulos aplicativos de la legislación pertinente y actualizada.
- Asistir a las diferentes capacitaciones y/o reuniones que sean necesarias con el ánimo de posibilitar la efectividad tanto en el montaje como en el desarrollo de la implantación de los diferentes módulos aplicativos en los cuales a sido designado.
- Certificar los avances y/o alcances del proveedor a los supervisores del contrato, en cuanto se refiere al "recibido a satisfacción" del los módulos aplicativos a los que ha sido designado. Los parámetros que se evaluarán serán la actualización, estabilización, diagnóstico, respuesta a requerimientos por concepto de mejoramientos nuevos, suficiencia y amplitud de la capacitación, implementación, soporte técnico.

4.1.3. Planos de la infraestructura física y del cableado estructurado del hospital universitario departamental de Nariño

Los relacionados con la planta física del hospital universitario departamental de Nariño, como también los planos del cableado estructurado se encuentran relacionados al final del documento, remitirse a los anexos: 14 y 15 que se anexan de forma digital.

4.1.4. Equipos de cómputo y otros dispositivos utilizados para la implantación del módulo de historia clínica electrónica

Hardware

El recurso tecnológico de equipos de cómputo se encuentra distribuido en las diferentes áreas de atención al usuario las cuales comprenden triage, urgencias, hospitalización, y consulta externa.

Hospital universitario departamental de Nariño relación de hardware para historia clínica electrónica

Existe un total de 46 equipos fijos y 19 portátiles que se relacionan a continuación:

AREA	CANTIDAD	**MARCA**	TIPO/serial	PROCESO
Cirugía General	4	Dell Optiplex 755	PC /6ZRV6l	Historia clínica Digital
Oftalmología	NA	Dell Optiplex 755	PC /6DBX6G	Historia clínica Digital
Ginecoobstetricia	3	Dell Optiplex 755	PC /1ZRV6G	Historia clínica Digital
Medicina Interna	3	Dell Optiplex 755	PC /2ZRV661	Historia clínica Digital
Neurocirugía	3	Dell Optiplex 755	PC /8YRV6G	Historia clínica Digital
Urología	4	Dell Optiplex 755	PC /7YRV6C	Historia clínica Digital
Otorrinolaringología	2	Dell Optiplex 755	PC /BDBX6G	Historia clínica Digital
Dermatología	4	Dell Optiplex 755	PC /9LVT6G	Historia clínica Digital
Cirugía plástica	3	Dell Optiplex	PC /JYRV6G	Historia clínica

		755		Digital
Gastroenterología	NA	Dell Optiplex 755	PC /FDBX6G	Historia clínica Digital
Neumología	NA	Dell Optiplex 755	PC /3MVT6G	Historia clínica Digital
Pediatría	NA	Dell Optiplex 755	PC /CLVT6G	Historia clínica Digital
Fisiatría	3	Dell Optiplex 755	PC /4KVT6G	Historia clínica Digital
Cardiología	3	Dell optiplex 755	PC /6YRV6G	Historia clínica Digital
Endocrinología	4	Dell optiplex 755	PC /B9RVZZ	Historia clínica Digital
Hematología	4	Dell Optiplex 755	PC /2FBY6G	Historia clínica Digital
Anestesiología	3	Dell Optiplex 755	PC /DZRV6G	Historia clínica Digital
Neurología	1	Dell Optiplex 755	PC /1KVT6G	Historia clínica Digital
Psicología	1	Dell Optiplex 755	PC /1KVT1G	Historia clínica Digital

Siquiatria	1	Dell optiplex 755	PC /DDBX6G	Historia clínica Digital
Nutrición	1	Dell optiplex 755	PC /9KVT6G	Historia clínica Digital
Rehabilitación	1	Dell Optiplex 755	PC /FJVT6B1	Historia clínica Digital
Consulta externa	2	KYOCERA FS200D	IMPRESORA LASER	Historia clínica Digital
Oncología	1	KYOCERA FS200D	IMPRESORA BURBUJA	Historia clínica Digital
Rehabilitación	1	HP-5940	IMPRESORA BURBUJA	Historia clínica Digital
Gastroenterología	1	HP-5940	IMPRESORA BURBUJA	Historia clínica Digital

Descripción de Los equipos relacionados anteriormente

Área de urgencias

SECCION: TRIAGE

MARCA CPU: DELL OPTIPLEX 755

PROCESADOR Y VELOCIDAD: INTEL PENTIUM 4 DUAL

TARJETA DE RED: REALTEK RTL8187B WIRELESS 802.11

RAM: 1.0 G

CAPACIDAD DISCO DURO: 160 G (1)

MARCA MONITOR:	DELL 17”
SISTEMA OPERATIVO:	WINDOWS XP PROFESSIONAL V2002 SERVICE PACK
LICENCIA:	76460-OEM-0011903-00102
OFFICE:	NO TIENE
ANTIVIRUS:	AVG 7.5
DIRECCION IP:	192.168.21.159
OTRAS APLICACIONES:	ADOBE READER 8.0 WINDOWS MESSENGER INTERNET EXPLORER

Consultorio 1 urgencias

MARCA CPU:	DELL OPTIPLEX 755
PROCESADOR Y VELOCIDAD:	INTEL PENTIUM 4 DUAL
TARJETA DE RED:	REALTEK RTL8187B WIRELESS 802.11
RAM:	1.0 G
CAPACIDAD DISCO DURO:	160 G (1)
MARCA MONITOR:	DELL 17”
SISTEMA OPERATIVO:	WINDOWS XP PROFESSIONAL V2002 SERVICE PACK
LICENCIA:	76460-OEM-0011903-00102
OFFICE:	
ANTIVIRUS:	AVG 7.5
DIRECCION IP:	192.168.21.78
OTRAS APLICACIONES:	ADOBE READER 8.0 WINDOWS MESSENGER INTERNET EXPLORER SKIPE YAHOO MESSENGER

Consultorio 2

MARCA CPU:	DELL OPTIPLEX 755
PROCESADOR Y VELOCIDAD:	INTEL PENTIUM 4 DUAL
TARJETA DE RED:	REALTEK RTL8187B WIRELESS 802.11
RAM:	1.0 G
CAPACIDAD DISCO DURO:	160 G (1)
MARCA MONITOR:	DELL 17”
SISTEMA OPERATIVO:	WINDOWS XP PROFESSIONAL 2002 SERVICE PACK
LICENCIA:	76460-OEM-0011903-00102
OFFICE:	
ANTIVIRUS:	AVG 7.5
DIRECCION IP:	192.168.21.65
OTRAS APLICACIONES:	ADOBE READER 8.0 WINDOWS MESSENGER INTERNET EXPLORER

Área de oncología (numero de equipos 3)

Consultorio de odontología oncológica

MARCA CPU:	DELL OPTIPLEX 755
PROCESADOR Y VELOCIDAD:	INTEL PENTIUM 4 DUAL
TARJETA DE RED:	REALTEK RTL8187B WIRELESS 802.11
RAM:	1.0 G
CAPACIDAD DISCO DURO:	160 G (1)
MARCA MONITOR:	DELL 17”

SISTEMA OPERATIVO:	WINDOWS XP PROFESSIONAL V2002 SERVICE PACK
LICENCIA:	76460-OEM-0011903-00102
OFFICE:	OFICCE 2003
ANTIVIRUS:	SYMANTEC CLIENTE SERVIDOR
DIRECCION IP:	192.168.21.197
OTRAS APLICACIONES:	WINDOWS MESSENGER INTERNET EXPLORER POWER DVD

Consultorio No. 1 oncología

MARCA CPU:	DELL OPTIPLEX 755
PROCESADOR Y VELOCIDAD:	INTEL PENTIUM 4 DUAL
TARJETA DE RED:	REALTEK RTL8187B WIRELESS 802.11 INTEL 82566DM 2GB
RAM:	1.0 G
CAPACIDAD DISCO DURO:	160 G (1)
MARCA MONITOR:	DELL 17”
SISTEMA OPERATIVO:	WINDOWS XP PROFESSIONAL V2002 SERVICE PACK
LICENCIA:	76460-OEM-0011903-00102
OFFICE:	NO TIENE
ANTIVIRUS:	SYMANTEC CLIENTE SERVIDOR
DIRECCION IP.	192.168.21.128
OTRAS APLICACIONES:	WINDOWS MESSENGER INTERNET EXPLORER POWER DVD

Consultorio No. 2 oncología

MARCA CPU:	DELL OPTIPLEX 755

PROCESADOR Y VELOCIDAD:	INTEL PENTIUM 4 DUAL
TARJETA DE RED:	REALTEK RTL8187B WIRELESS 802.11
RAM:	1.0 G
CAPACIDAD DISCO DURO:	160 G (1)
MARCA MONITOR:	DELL 17”
SISTEMA OPERATIVO:	WINDOWS XP PROFESSIONAL V2002 SERVICE PACK
LICENCIA:	76460-OEM-0011903-00102
OFFICE:	OFICCE 2003
ANTIVIRUS:	SYMANTEC CLIENTE SERVIDOR
DIRECCION IP:	192.168.21.187
OTRAS APLICACIONES:	WINDOWS MESSENGER INTERNET EXPLORER POWER DVD

Servidor

- Computador hp DL380G5 (QUAD CORE)
- Procesador: (1) Quad core E5345 DI 360 Kit (2.30 Ghz Watts, 1333 FSB) Intel Xeon Processor: Crece a dos Procesadores, memoria caché de 8MB (2x 4MB) level 2 cache – Intel Xeon processor 5300 sequence
- Memoria RAM de 4GB PC2-5300 Fully Buffered DIMMs (DDR2-667) with Advanced ECC, mirrored an online spare memory capabilities.
- Tarjeta de RED Embedded Dual Port NC373i Multifunction Gigabit NIC Controladora de discos: Smart Array P400/256MB Controller (RAID 0/1/1+0/5) Almacenamiento: soporta 8 discos SFF SAS de 2.5;
- Total almacenamiento hasta 8 discos duros 576GB MAX.
- No contiene Unidad de diskette ni CD-Rom slots PCI Express: Four avaible PCI-Express slots, optional mixed PCI-X/PCI-Express configurations avaible. Fuente de Poder: Hot plug power supply with optional redundancy
- Ventiladores: Fully redundant hot plug fans, Forma: RACK 2U

- Garantía: 3-3-3

Componentes de la red y cableado del hospital universitario departamental

DESCRIPCION	UNIDAD DE MEDIDA	PISO	TOTAL PUNTOS
Número de puntos dobles	UND	1	74
Numero de Puntos Sencillos	UND		0
Cuarto de Telecomunicaciones	UND	1, 3,5	3
CABLEADO			
CABLE CATEGORIA 6 CMR	METROS		20.690
RACKS PARA LOS CUARTOS DE TELECOMUNICAICONES			
RACK EN ALUMINIO COLOR NEGRO, CERTIFICADO POR UL. 19X84 PULGADAS	UND	3	3
ORGANIZADORES VERTICALES DELANTERO CON CAPACIDAD DE ALBERGAR 240 CABLES COLOR NEGRO	UND		6
PUERTA FRONTAL MOVIL PARA ADMINISTRACIÓN DE CABLES	UND		6
TAPA LATERAL FINAL	UND		6
ANILLOS PLASTICOS PARA ORGANIZACIÓN DE CABLES	PAQUETE		6
MULTITOMA DE 20 AMPERIOS	UND		6
SOLUCION DE FIBRA			
FIBRA OPTICA DE DISTRIBUCION INTERNA MULTIMODO 50/125 Um, 10Gbps/SEG DE	MF		290

SEIS HILOS			
HERRAJE DE 24 PUERTOS PARA BANDEJA DE FIBRA: DEBE SER UL LISTADO Y CSA Capacidad de alojar Conectores de Fibra óptica SC, ST, Small Form factor (TIA/EIA 568B.3), conectores Categoría 6, conectores de Categoría 5E, Categoría 3, , conectores para Audio tipo RCA, Conectores coaxiales (Aplicaciones de video), Conectores coaxiales tipo F, sistemas blindados FTP y ScTP. O una mezcla de cualquiera de ellos, dependiendo de las necesidades que se le puedan presentar a través del tiempo.	UND		3
BANDEJA DE FIBRA OPTICA MODULAR: Capacidad de alojar Conectores de Fibra óptica SC, ST, Small Form factor (TIA/EIA 568B.3), conectores Categoría 6, conectores de Categoría 5E, Categoría 3, , conectores para Audio tipo RCA, Conectores coaxiales (Aplicaciones de video), Conectores coaxiales tipo F, sistemas blindados FTP y ScTP. O una mezcla de cualquiera de ellos, dependiendo de las necesidades que se le puedan presentar a través del tiempo.	UND		3
ORGANIZADOR HORIZONTAL DELANTERO CON MANEJO D ERADIOS DE CURVATURA DE UNA UNIDAD DE RACK CON TAPAS.	UND		3
ACOPLADOR LC DUPLEX , DEBE CUMPLIR CON LOS FOCIS-3 TIA/EIA-568-B.3, DEBE SOPORTAR CONECTORES Y	UND		9

PATCH CORDS DE FIBRA OPTICA MULTIMODO Y MONOMODO			
MÓDULO CIEGO PARA PATCH PANEL DEBE SER UL LISTADO Y CSA	UND		63
CONECTOR DE FIBRA OPTICA LC SIMPLEX, DEBE CUMPLIR CON LOS FOCIS-3 TIA/EIA-568-B.3, MULTIMODO QUE SOPORTE 62.5/15 Y 50/125, LAS PERDIDAS POR INSERCIÓN DEBEN SER DE .10 dB O INFERIORES, Y PERDIDAS DE RETORNO MENORES A 20dB, DEBE TRAER LAS DOS BOTAS TANTO PARA FIBRAS TIGHT BUFFERED DE 900 um COMO PARA FIBRAS CON JACKETED DE 3.0 mm, TIPO DE FERRLE 2.5 MM ZIRCONIA CERAMIC. TERMINACIÓN DEL CONECTOR FIELD POLISH, NO SE ACEPTAN CONECTORES DE TERMINACIÓN MECANICA.	UND		18
PATCH CORD DE FIBRA LC-LC OPTICA DUPLEX MULTIMODO 50/125 Um DE DOS METROS DE LONGITUD, CERTIFICADOS PARA SOPORTAR VELOCIDADES DE TRANSMISIÓN HASTA DE 10 Gbps PARA ENLACES DE LONGITUDES HASTA DE 300 METROS EN LONGITUDES DE ONDA DE 850 NM DE ACUERDO AL ESTANDAR: IEEE 802.3ae 10GbE, DEBE REUNIR TODOS LOS REQUERIMIENTOS DE LA EIA/TIA-568-B.3, CON UNA PERDIDA POR INSERCIÓN POR CONECTOR DE .1 dB; MÁXIMA EN EL PATCH CORD DE .3dB, EL PATCH CORD	UND		6

DUPLEX DEBE NCLUIR EL CLIP DE SUJECION PARA MANTENER LA POLARIDAD.			
CUARTO DE TELECOMUNICACIONES			
PATCH PANEL MODULAR 48 PUERTOS, DEBE SER UL LISTADO Y CSA. Capacidad de alojar Conectores de Fibra óptica SC, ST, Small Form factor (TIA/EIA 568B.3), conectores Categoría 6, conectores de Categoría 5E, Categoría 3, , conectores para Audio tipo RCA, Conectores coaxiales (Aplicaciones de video), Conectores coaxiales tipo F, sistemas blindados FTP y ScTP. O una mezcla de cualquiera de ellos, dependiendo de las necesidades que se le puedan presentar a través del tiempo.	UND		15
JACK CAT 6 ROJO DEBE SER UL LISTADO Y CSA, DEBE CUMPLIR CON EL ESTANDAR TIA/EIA-568-B.2-1 PARA CATEGORIA 6, SE DEBE ANEXAR LAS PRUEBAS DE ETL PARA CANAL A 100 metros. Terminación tipo IDC (ANSI/TIA/EIA 568B.2). El conector debe garantizar el mínimo destrenzado por parte del instalador en el momento de su montaje. El estándar exige destrenzado mínimo de 1/2". El conector debe tener la capacidad de recibir cables (conductores) con calibres 22AWG, 23 AWG y 24 AWB, El conector deb poderse terminar	UND		74

sin herramienta de impacto especializada para su terminación (Ponchado). El proceso debe permitir hacer la terminación de los ocho hilos al mismo tiempo y tener un "click" de verificación que le indique al instalador que el ponchado se finalizó con éxito. El conector debe ser Re-utilizable sin perder sus características eléctricas exigidas por la Categoría 6 y TIA/EIA 568B. Cada conector debe poseer la característica de re-terminado un mínimo de 10 veces avalada por el fabricante del producto. Cada conector soportará ciclos de conexión y reconexión superiores a 10.000 veces por su orificio RJ45.			
JACK CAT 6 AZUL DEBE SER UL LISTADO Y CSA, DEBE CUMPLIR CON EL ESTANDAR TIA/EIA-568-B.2-1 PARA CATEGORIA 6, SE DEBE ANEXAR LAS PRUEBAS DE ETL PARA CANAL A 100 metros. Terminación tipo IDC (ANSI/TIA/EIA 568B.2). El conector debe garantizar el mínimo destrenzado por parte del instalador en el momento de su montaje. El estándar exige destrenzado mínimo de 1/2". El conector debe tener la capacidad de recibir cables (conductores) con calibres 22AWG, 23 AWG y 24 AWB, El conector deb poderse terminar sin herramienta de impacto especializada para su terminación (Ponchado). El proceso debe permitir hacer la terminación de los ocho hilos al mismo tiempo y tener un "click" de	UND		74

verificación que le indique al instalador que el ponchado se finalizó con éxito. El conector debe ser Re-utilizable sin perder sus características eléctricas exigidas por la Categoría 6 y TIA/EIA 568B. Cada conector debe poseer la característica de re-terminado un mínimo de 10 veces avalada por el fabricante del producto. Cada conector soportará ciclos de conexión			
y reconexión superiores a 10.000 veces por su orificio RJ45.			
JACK CAT 5E NEGRO DEBE SER UL LISTADO Y CSA, DEBE CUMPLIR CON EL ESTANDAR TIA/EIA-568-B.2 PARA CATEGORIA 5E, SE DEBE ANEXAR LAS PRUEBAS DE ETL PARA CANAL A 100 metros. Terminación tipo IDC (ANSI/TIA/EIA 568B.2). El conector debe garantizar el mínimo destrenzado por parte del instalador en el momento de su montaje. El estándar exige destrenzado mínimo de 1/2". El conector debe tener la capacidad de recibir cables (conductores) con calibres 22AWG, 23 AWG y 24 AWB, El conector debe poderse terminar sin herramienta de impacto especializada para su terminación (Ponchado). El proceso debe permitir hacer la terminación de los ocho hilos al mismo tiempo y tener un "click" de verificación que le indique al instalador que el ponchado se finalizó con éxito. El conector debe ser Re-utilizable sin perder sus	UND		74

características eléctricas exigidas por la Categoría 6 y TIA/EIA 568B. Cada conector debe poseer la característica de re-terminado un mínimo de 10 veces avalada por el fabricante del producto. Cada conector soportará ciclos de conexión y reconexión superiores a 10.000 veces por su orificio RJ45.			
MÓDULO CIEGO PARA PATCH PANEL DEBE SER UL LISTADO Y CSA	UND		120
LABELS PARA PATCH PANEL autoadhesivos con las siguientes dimensiones: .61´´x0.33´´	HOJAS		3
VELCRO TAKTY	PAQUETE		6
ICONOS DE VOZ color rojo Estos deben ser elaborados por el mismo fabricante de la conectividad y precertificados por el fabricante como lo estipula la TIA/EIA.	PAQUETE		148
ICONOS DE DATOS color azul Estos deben ser elaborados por el mismo fabricante de la conectividad y precertificados por el fabricante como lo estipula la TIA/EIA.	PAQUETE		74
ORGANIZADOR HORIZONTAL DELANTERO TRASERO DE DOS UNIDADES DE RACK CON TAPAS.	UND		30
ORGANIZADOR HORIZONTAL DELANTERO TRASERO DE UNA UNIDAD DE RACK CON TAPAS.	UND		6

PATCH CORD CATEGORIA 6 DE FABRICA DE 3 PIES AZUL DEBE SER UL LISTADO Y CSA, DEBE CUMPLIR CON EL ESTANDAR TIA/EIA-568-B.2-1 PARA CATEGORIA 6, SE DEBE ANEXAR LAS PRUEBAS DE ETL PARA CANAL A 100 metros. Construido con cable categoría 6 24 AWG stranded, deben tener un recubrimiento de 50 um de oro para maximizar su durabilidad, · Deben tener una impedancia de entrada sin promediar de: 100 Ω + 32% y con respuesta en frecuencia superior a 250Mhz (verificado por prueba ETL).· Los plugs usados para los patch cords deben venir diseñados para que estos eviten trabarse al momento de conexión o desconexión de los equipos activos (Tarjetas de Red). Todo lo anterior, con el fin de permitir un crecimiento económico, ordenado y evitar daños. Estos deben ser elaborados por el mismo fabricante de la conectividad y precertificados por el fabricante como lo estipula la TIA/EIA.	UND		74
PATCH CORD CATEGORIA 6 DE FABRICA DE 3 PIES ROJO DEBE SER UL LISTADO Y CSA, DEBE CUMPLIR CON EL ESTANDAR TIA/EIA-568-B.2-1 PARA CATEGORIA 6, SE DEBE ANEXAR LAS PRUEBAS DE ETL PARA CANAL A 100 metros. Construido con cable categoría 6 24 AWG stranded, deben tener un recubrimiento de 50 um de oro para maximisar su durabilidad, · Deben tener una impedancia de entrada sin promediar de: 100	UND		74

Ω + 32% y con respuesta en frecuencia superior a 250Mhz (verificado por prueba ETL).· Los plugs usados para los patch cords deben venir diseñados para que estos eviten trabarse al momento de conexión o desconexión de los equipos activos (Tarjetas de Red). Todo lo anterior, con el fin de permitir un crecimiento económico, ordenado y evitar daños. Estos deben ser elaborados por el mismo fabricante de la conectividad y precertificados por el fabricante como lo estipula la TIA/EIA.			
LABELS PARA CABLES autoadhesivos con protección de la marcación (indoor/outdoor), para imprimir en impresora laser, con las siguientes dimensiones: 2´´x1.5´´.	HOJAS		25
PUNTOS DE CONSOLIDACION			
CAJA PARA PUNTO DE CONSOLIDACION DEBE SER UL LISTADO, debe cumplir la UL2043 aprobada para ser usadas en techos falsos o paredes	UND		17
LABELS PARA CABLES autoadhesivos con protección de la marcación (indoor/outdoor), para imprimir en impresora laser, con las siguientes dimensiones: 2´´x1.5´´.	HOJAS		17
AREAS DE TRABAJO			
ICONOS DE VOZ color rojo Estos deben ser elaborados por el mismo fabricante de la conectividad y precertificados por el fabricante como lo estipula la TIA/EIA.	PAQUETE		74

ICONOS DE DATOS color azul Estos deben ser elaborados por el mismo fabricante de la conectividad y precertificados por el fabricante como lo estipula la TIA/EIA.	PAQUETE		74
FACEPLATE EJECUTIVO PARA DUCTO T70 DE DOS POSICIONES CON PROTECCIÓN DE LA MARCACIÓN DEBE SER UL LISTADO Y CSA, DEBE SER UL LISTADO Y CSA Capacidad de alojar Conectores de Fibra óptica SC, ST, Small Form factor (TIA/EIA 568B.3), conectores Categoría 6, conectores de Categoría 5E, Categoría 3, , conectores para Audio tipo RCA, Conectores coaxiales (Aplicaciones de video), Conectores coaxiales tipo F, sistemas blindados FTP y ScTP. O una mezcla de cualquiera de ellos, dependiendo de las necesidades que se le puedan presentar a través del tiempo.	UND		74
JACK CAT 6 ROJO DEBE SER UL LISTADO Y CSA, DEBE CUMPLIR CON EL ESTANDAR TIA/EIA-568-B.2-1 PARA CATEGORIA 6, SE DEBE ANEXAR LAS PRUEBAS DE ETL PARA CANAL A 100 metros. Terminación tipo IDC (ANSI/TIA/EIA 568B.2). El conector debe garantizar el mínimo destrenzado por parte del instalador en el momento de su montaje. El estándar exige destrenzado mínimo de 1/2". El conector debe tener la capacidad de recibir cables (conductores) con calibres 22AWG, 23 AWG y 24 AWB, El conector deb poderse terminar sin herramienta de impacto especializada para	UND		74

su terminación (Ponchado). El proceso debe permitir hacer la terminación de los ocho hilos al mismo tiempo y tener un "click" de verificación que le indique al instalador que el ponchado se finalizó con éxito. El conector debe ser Re-utilizable sin perder sus características eléctricas exigidas por la Categoría 6 y TIA/EIA 568B. Cada conector debe poseer la característica de re-terminado un mínimo de 10 veces avalada por el fabricante del producto. Cada conector soportará ciclos de conexión y reconexión superiores a 10.000 veces por su orificio RJ45.			
JACK CAT 6 AZUL DEBE SER UL LISTADO Y CSA, DEBE CUMPLIR CON EL ESTANDAR TIA/EIA-568-B.2-1 PARA CATEGORIA 6, SE DEBE ANEXAR LAS PRUEBAS DE ETL PARA CANAL A 100 metros. Terminación tipo IDC (ANSI/TIA/EIA 568B.2). El conector debe garantizar el mínimo destrenzado por parte del instalador en el momento de su montaje. El estándar exige destrenzado mínimo de 1/2". El conector debe tener la capacidad de recibir cables (conductores) con calibres 22AWG, 23 AWG y 24 AWB, El conector debe poderse terminar sin herramienta de impacto especializada para su terminación (Ponchado). El proceso debe permitir hacer la terminación de los ocho hilos al mismo tiempo y tener un "click" de verificación que le indique al instalador que el	UND		74

ponchado se finalizó con éxito. El conector debe ser Re-utilizable sin perder sus características eléctricas exigidas por la Categoría 6 y TIA/EIA 568B. Cada conector debe poseer la característica de re-terminado un mínimo de 10 veces avalada por el fabricante del producto. Cada conector soportará ciclos de conexión y reconexión superiores a 10.000 veces por su orificio RJ45.			
PATCH CORD CATEGORIA 6 DE FABRICA DE 10 PIES AZUL DEBE SER UL LISTADO Y CSA, DEBE CUMPLIR CON EL ESTANDAR TIA/EIA-568-B.2-1 PARA CATEGORIA 6, SE DEBE ANEXAR LAS PRUEBAS DE ETL PARA CANAL A 100 metros. Construido con cable categoría 6 24 AWG stranded, deben tener un recubrimiento de 50 um de oro para maximizar su durabilidad, · Deben tener una impedancia de entrada sin promediar de: 100 Ω + 32% y con respuesta en frecuencia superior a 250Mhz (verificado por prueba ETL).· Los plugs usados para los patch cords deben venir diseñados para que estos eviten trabarse al momento de conexión o desconexión de los equipos activos (Tarjetas de Red). Todo lo anterior, con el fin de permitir un crecimiento económico, ordenado y evitar daños. Estos deben ser elaborados por el mismo fabricante de la conectividad y precertificados por el fabricante como lo estipula la TIA/EIA.	UND		74

MÓDULO CIEGO PARA FACEPLATE DEBE SER UL LISTADO Y CSA	UND		0
LABELS PARA CABLES autoadhesivos con protección de la marcación (indoor/outdoor), para imprimir en impresora laser, con las siguientes dimensiones: 2´´x1.5´´.	HOJAS		36
LABELS PARA FACEPLATES autoadhesivos con las siguientes dimensiones: 1.8´´x0.38´´	HOJAS		6
DUCTERIA Y CANALIZACION			
BASE DUCTO T70 Los ductos y canalizaciones deben ser construidas con ductos profesionales plásticos, que cumplan con todos los requerimientos de TIA/EIA 569A y con énfasis en que los radios de curvatura mínimos a cumplir para estos ductos deben ser de 4 veces el diámetro del cable a utilizar (UTP Cat. 6 de 4 pares). Nunca se deben cruzar los cables eléctricos y los de comunicaciones en ningún lugar, el sistema de canalizaciones debe tener todos los accesorios adecuados para cumplir con estas especificaciones. debe cumplir con la UL y la CSA requerida a 600 V, de acuerdo a los estándares UL5A y CSA 22.2 No 62-93, debe ser compatible con NEMA, y debe ser tamper resistant. Los sistemas de canalización deben tener una garantía mínima de 10 años otorgada por el fabricante de estos y preferiblemente para este efecto se seleccionarán canalizaciones de la misma marca de la conectividad instalada para	METROS		1.565

integrar las garantías.			
TAPA DUCTO T70 Los ductos y canalizaciones deben ser construidas con ductos profesionales plásticos, que cumplan con todos los requerimientos de TIA/EIA 569A y con énfasis en que los radios de curvatura mínimos a cumplir para estos ductos deben ser de 4 veces el diámetro del cable a utilizar (UTP Cat. 6 de 4 pares). Nunca se deben cruzar los cables eléctricos y los de comunicaciones en ningún lugar, el sistema de canalizaciones debe tener todos los accesorios adecuados para cumplir con estas especificaciones. Debe cumplir con la UL y la CSA requerida a 600 V, de acuerdo a los estándares UL5A y CSA 22.2 No 62-93, debe ser compatible con NEMA, y debe ser tamper resistant. Los sistemas de canalización deben tener una garantía mínima de 10 años otorgada por el fabricante de estos y preferiblemente para este efecto se seleccionarán canalizaciones de la misma marca de la conectividad instalada para integrar las garantías.	METROS		1.565
DIVISOR DUCTO T70 Los ductos y canalizaciones deben ser construidas con ductos profesionales plásticos, que cumplan con todos los requerimientos de TIA/EIA 569A y con énfasis en que los radios de curvatura mínimos a cumplir para estos ductos deben ser de 4 veces el diámetro del cable a utilizar (UTP Cat. 6 de 4 pares). Nunca se deben	METROS		1.565

cruzar los cables eléctricos y los de comunicaciones en ningún lugar, el sistema de canalizaciones debe tener todos los accesorios adecuados para cumplir con estas especificaciones. Debe cumplir con la UL y la CSA requerida a 600 V, de acuerdo a los estándares UL5A y CSA 22.2 No 62-93, debe ser compatible con NEMA, y debe ser tamper resistant. Los sistemas de canalización deben tener una garantía mínima de 10 años otorgada por el fabricante de estos y preferiblemente para este efecto se seleccionarán canalizaciones de la misma marca de la conectividad instalada para integrar las garantías.			
UNION BASE DUCTO T70 Los ductos y canalizaciones deben ser construidas con ductos profesionales plásticos, que cumplan con todos los requerimientos de TIA/EIA 569A y con énfasis en que los radios de curvatura mínimos a cumplir para estos ductos deben ser de 4 veces el diámetro del cable a utilizar (UTP Cat. 6 de 4 pares). Nunca se deben cruzar los cables eléctricos y los de comunicaciones en ningún lugar, el sistema de canalizaciones debe tener todos los accesorios adecuados para cumplir con estas especificaciones. Debe cumplir con la UL y la CSA requerida a 600 V, de acuerdo a los estándares UL5A y CSA 22.2 No 62-93, debe ser compatible con NEMA, y debe ser tamper resistant. Los sistemas de canalización deben	UND		783

tener una garantía mínima de 10 años otorgada por el fabricante de estos y preferiblemente para este efecto se seleccionarán canalizaciones de la misma marca de la conectividad instalada para integrar las garantías.			
UNION TAPA DUCTO T70 Los ductos y canalizaciones deben ser construidas con ductos profesionales plásticos, que cumplan con todos los requerimientos de TIA/EIA 569A y con énfasis en que los radios de curvatura mínimos a cumplir para estos ductos deben ser de 4 veces el diámetro del cable a utilizar (UTP Cat. 6 de 4 pares). Nunca se deben cruzar los cables eléctricos y los de comunicaciones en ningún lugar, el sistema de canalizaciones debe tener todos los accesorios adecuados para cumplir con estas especificaciones. Debe cumplir con la UL y la CSA requerida a 600 V, de acuerdo a los estándares UL5A y CSA 22.2 No 62-93, debe ser compatible con NEMA, y debe ser tamper resistant. Los sistemas de canalización deben tener una garantía mínima de 10 años otorgada por el fabricante de estos y preferiblemente para este efecto se seleccionarán canalizaciones de la misma marca de la conectividad instalada para integrar las garantías.	UND		783

ANGULO RECTO T70 Los ductos y canalizaciones deben ser construidas con ductos profesionales plásticos, que cumplan con todos los requerimientos de TIA/EIA 569A y con énfasis en que los radios de curvatura mínimos a cumplir para estos ductos deben ser de 4 veces el diámetro del cable a utilizar (UTP Cat. 6 de 4 pares). Nunca se deben cruzar los cables eléctricos y los de comunicaciones en ningún lugar, el sistema de canalizaciones debe tener todos los accesorios adecuados para cumplir con estas especificaciones. debe cumplir con la UL y la CSA requerida a 600 V, de acuerdo a los estándares UL5A y CSA 22.2 No 62-93, debe ser compatible con NEMA, y debe ser tamper resistant. Los sistemas de canalización deben tener una garantía mínima de 10 años otorgada por el fabricante de estos y preferiblemente para este efecto se seleccionarán canalizaciones de la misma marca de la conectividad instalada para integrar las garantías.	UND		78
ANGULO ENTRANTE 90 T70 Los ductos y canalizaciones deben ser construidas con ductos profesionales plásticos, que cumplan con todos los requerimientos de TIA/EIA 569A y con énfasis en que los radios de curvatura mínimos a cumplir para estos ductos deben ser de 4 veces el diámetro del cable a utilizar (UTP Cat. 6 de 4 pares). Nunca se deben cruzar los cables eléctricos y los de	UND		157

comunicaciones en ningún lugar, el sistema de canalizaciones debe tener todos los accesorios adecuados para cumplir con estas especificaciones. Debe cumplir con la UL y la CSA requerida a 600 V, de acuerdo a los estándares UL5A y CSA 22.2 No 62-93, debe ser compatible con NEMA, y debe ser tamper resistant. Los sistemas de canalización deben tener una garantía mínima de 10 años otorgada por el fabricante de estos y preferiblemente para este efecto se seleccionarán canalizaciones de la misma marca de la conectividad instalada para integrar las garantías.			
ANGULO SALIENTE DE 90 T70 Los ductos y canalizaciones deben ser construidas con ductos profesionales plásticos, que cumplan con todos los requerimientos de TIA/EIA 569A y con énfasis en que los radios de curvatura mínimos a cumplir para estos ductos deben ser de 4 veces el diámetro del cable a utilizar (UTP Cat. 6 de 4 pares). Nunca se deben cruzar los cables eléctricos y los de comunicaciones en ningún lugar, el sistema de canalizaciones debe tener todos los accesorios adecuados para cumplir con estas especificaciones. debe cumplir con la UL y la CSA requerida a 600 V, de acuerdo a los estándares UL5A y CSA 22.2 No 62-93, debe ser compatible con NEMA, y debe ser tamper resistant. Los sistemas de canalización deben tener una garantía mínima de 10 años	UND		78

otorgada por el fabricante de estos y preferiblemente para este efecto se seleccionarán canalizaciones de la misma marca de la conectividad instalada para integrar las garantías.			
TEE PARA DUCTO T70 Los ductos y canalizaciones deben ser construidas con ductos profesionales plásticos, que cumplan con todos los requerimientos de TIA/EIA 569A y con énfasis en que los radios de curvatura mínimos a cumplir para estos ductos deben ser de 4 veces el diámetro del cable a utilizar (UTP Cat. 6 de 4 pares). Nunca se deben cruzar los cables eléctricos y los de comunicaciones en ningún lugar, el sistema de canalizaciones debe tener todos los accesorios adecuados para cumplir con estas especificaciones. Debe cumplir con la UL y la CSA requerida a 600 V, de acuerdo a los estándares UL5A y CSA 22.2 No 62-93, debe ser compatible con NEMA, y debe ser tamper resistant. Los sistemas de canalización deben tener una garantía mínima de 10 años otorgada por el fabricante de estos y preferiblemente para este efecto se seleccionarán canalizaciones de la misma marca de la conectividad instalada para integrar las garantías.	UND		78

SEPARADOR DE VIAS PARA TEE EN DUCTO T70 Los ductos y canalizaciones deben ser construidas con ductos profesionales plásticos, que cumplan con todos los requerimientos de TIA/EIA 569A y con énfasis en que los radios de curvatura mínimos a cumplir para estos ductos deben ser de 4 veces el diámetro del cable a utilizar (UTP Cat. 6 de 4 pares). Nunca se deben cruzar los cables eléctricos y los de comunicaciones en ningún lugar, el sistema de canalizaciones debe tener todos los accesorios adecuados para cumplir con estas especificaciones. Debe cumplir con la UL y la CSA requerida a 600 V, de acuerdo a los estándares UL5A y CSA 22.2 No 62-93, debe ser compatible con NEMA, y debe ser tamper resistant. Los sistemas de canalización deben tener una garantía mínima de 10 años otorgada por el fabricante de estos y preferiblemente para este efecto se seleccionarán canalizaciones de la misma marca de la conectividad instalada para integrar las garantías.	UND		78
BAJANTE PARA DUCTO T70 Los ductos y canalizaciones deben ser construidas con ductos profesionales plásticos, que cumplan con todos los requerimientos de TIA/EIA 569A y con énfasis en que los radios de curvatura mínimos a cumplir para estos ductos deben ser de 4 veces el diámetro del cable a utilizar (UTP Cat. 6 de 4 pares). Nunca se deben	UND		78

cruzar los cables eléctricos y los de comunicaciones en ningún lugar, el sistema de canalizaciones debe tener todos los accesorios adecuados para cumplir con estas especificaciones. Debe cumplir con la UL y la CSA requerida a 600 V, de acuerdo a los estándares UL5A y CSA 22.2 No 62-93, debe ser compatible con NEMA, y debe ser tamper resistant. Los sistemas de canalización deben tener una garantía mínima de 10 años otorgada por el fabricante de estos y preferiblemente para este efecto se seleccionarán canalizaciones de la misma marca de la conectividad instalada para integrar las garantías.			
CAJAS PARA SALIDAS DE DATOS Y POTENCIA Los ductos y canalizaciones deben ser construidas con ductos profesionales plásticos, que cumplan con todos los requerimientos de TIA/EIA 569A y con énfasis en que los radios de curvatura mínimos a cumplir para estos ductos deben ser de 4 veces el diámetro del cable a utilizar (UTP Cat. 6 de 4 pares). Nunca se deben cruzar los cables eléctricos y los de comunicaciones en ningún lugar, el sistema de canalizaciones debe tener todos los accesorios adecuados para cumplir con estas especificaciones. Debe cumplir con la UL y la CSA requerida a 600 V, de acuerdo a los estándares UL5A y CSA 22.2 No 62-93, debe ser compatible con NEMA, y debe ser tamper	UND		74

resistant. Los sistemas de canalización deben tener una garantía mínima de 10 años otorgada por el fabricante de estos y preferiblemente para este efecto se seleccionarán canalizaciones de la misma marca de la conectividad instalada para integrar las garantías.			
FACEPLATE DE POTENCIA Los ductos y canalizaciones deben ser construidas con ductos profesionales plásticos, que cumplan con todos los requerimientos de TIA/EIA 569A y con énfasis en que los radios de curvatura mínimos a cumplir para estos ductos deben ser de 4 veces el diámetro del cable a utilizar (UTP Cat. 6 de 4 pares). Nunca se deben cruzar los cables eléctricos y los de comunicaciones en ningún lugar, el sistema de canalizaciones debe tener todos los accesorios adecuados para cumplir con estas especificaciones. Debe cumplir con la UL y la CSA requerida a 600 V, de acuerdo a los estándares UL5A y CSA 22.2 No 62-93, debe ser compatible con NEMA, y debe ser tamper resistant. Los sistemas de canalización deben tener una garantía mínima de 10 años otorgada por el fabricante de estos y preferiblemente para este efecto se seleccionarán canalizaciones de la misma marca de la conectividad instalada para integrar las garantías.	UND		74

Salida de potencia regulada			
Cable de potencia triplex thhn	METROS		2.601
Tomas de potencia eléctrica regulada con polo a tierra aislado grado hospitalario	UND		74
Tablero eléctrico de 12 circuitos con totalizador, barraje de tierra, barraje de tierra aislada, puerta chapa y breakers de 20ª	UND		1
Tablero eléctrico de 18 circuitos con totalizador, barraje de tierra, barraje de tierra aislada, puerta chapa y breakers de 20ª	UND		1
Tablero eléctrico de 24 circuitos con totalizador, barraje de tierra, barraje de tierra aislada, puerta chapa y breakers de 20ª	UND		1
LABELS PARA TOMAS DE POTENCIA térmica de 3/8 de pulgada autolaminable, adhesiva	UND		1
Bandejas y tuberia emt			
Bandeja metalica tipo escalera de 30x8 cms.	METROS		664
Bandeja metalica tipo escalera de 15x8 cms.	METROS		200
Tuberia emt de 3/4"	METROS		0
Accesorios para tuberia emt de 3/4" (terminales, uniones)	UND		0
Tuberia emt de 1"	METROS		0
Accesorios para tuberia emt de 1" (terminales, uniones)	UND		0
Tuberia emt de 1 1/2"	METROS		120
Accesorios para tuberia emt de 1 1/2" (terminales, uniones)	METROS		120
Cajas de paso de 30x30x20	UND		0

Solucion de ducto profesional fiber runner			
Fiberrunner 12X4 canal.	FT		54
Fiberrunner tapa para canal 12x4	FT		54
Fiberrunner retenedor de cable	PAQUETE		25
Fiberrunner acoplador de partes	und		27
Fiberrunner bajante vertical	Und		12
Tapa para bajante vertical	Und		12
Ducto ranurado 4x4	FT		24
Tapa ducto ranurado 4x4	FT		24
Acoplador para bajante 4x4	Und		8
Curva vertical externa	Und		12
Tapa para Curva vertical externa	Und		12
Soporte de la canastilla al canal	Und		10
Brackek para sujetar la canastilla al canal	Und		10
Suministro e instalación de tornillo sin fin de 5/8 pulgada CON LONGITUD DE 12".	Und		10
Servicios adicionales			
Certificación por punto	Und		148
Documentación	Und		0
Planos en autocad	Und		0
Instalación	Und		0
equipos activos			
Switch 48 puertos layer 3. 48x10/1000 mbps and 2x1000 mbps networking switch.	Und		4

4.1.5. Diagrama general de procesos del área de información y sistemas del hospital universitario departamental de Nariño

Caracterización de procesos

Nombre del Proceso: Copia de seguridad del software de la organización.

Responsable: Técnico en sistemas

Objetivo: Garantizar el respaldo de la información registrada en los equipos de cómputo de la institución con el fin de obtener seguridad y continuidad en los procesos que requieran de la misma.

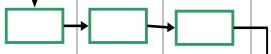
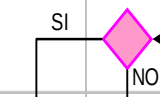
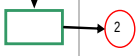
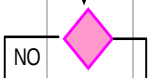
HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO E.S.E	PROCESO: ADMINISTRACION DEL SISTEMA DE INFORMACION	CODIGO:	FECHA DE ELABORACIÓN:
			8 DE MAYO DEL 2006
	SUBPROCESO: COPIA DE SEGURIDAD DEL SOFTWARE DE LA ORGANIZACION		FECHA DE ACTUALIZACIÓN:
		VERSIÓN:	8 DE MAYO DEL 2006
		OO	HOJA: 1 DE: 2

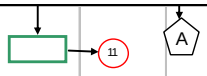
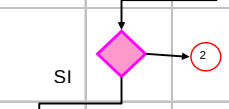
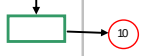
OBJETIVO: Garantizar el respaldo de la informacion registrada en los equipos de computo de la institucion con el fin de obtener seguridad y continuidad en los procesos que requieran de la misma.

ALCANCE: Toda la organización

RESPONSABLE: Coordinador de Informacion y sistemas - Tecnicos en Sistemas

	RESPONSABLES / DESCRIPCION	TECNICO EN SISTEMAS	COORDINADOR DE INFORMACION Y SISTEMAS		REGISTROS	PUNTOS DE CONTROL			
1	INICIO								
2	REALIZAR INVENTARIO ACTUALIZADO DE EQUIPOS DE COMPUTO				SIS-PMI-001				
3	ESTABLECER PRIORIDADES DE TODAS LAS AREAS DE LA ORGANIZACIÓN Y PERIORICIDAD DE LAS COPIAS				SIS-PPA-001				
4	CON BASE EN EL INVENTARIO DE SOFTWARE LICENCIADO SE SACARA TIPO DE ARCHIVOS CON SUS EXTENSIONES								
5	ELABORACION DE UN CRONOGRAMA 5W1H PARA DETERMINAR LA COPIA DE SEGURIDAD DE LAS DIFERENTES AREAS DE LA ORGANIZACIÓN				SIS-FCA-001				

6	Registrar no conformidad y aplicar plan de mejora		SIS-FNC-001					
7	Realizar diagnostico de cada uno de los modulos y-o aplicativos del sistema de informacion							
8	Se presentaron no conformidades en el dianostico y-o actualizacion del sistema de informacion y aplicativos desarrollados por la organización			calidad	Numero de no conformidades/Numero de modulos diagnosticados			
9	Presentar informe de auditoria		SIS-MAS-001					
10	Registrar no conformidad y aplicar plan de mejora, informar al proveedor del SI o aplicativo		SIS-FNC-001					
11	Recepcion de Medio magnetico empresa proveedora o el aplicativo actualizado		SIS-FRI-001					
12	Realizar verificacion de condiciones tecnicas de los medios magneticos (FISICA Y TECNICA)		SIS-FRI-001					
13	Se realizo la recepcion y se determino el estado del medio magnetico		SIS-FRI-001	si/no	confiabilidad			
14	n de insumos e informar al proveedor		SIS-FRI-001					

15	los datos obtenidos en la lista de chequeo		SIS-FRI-001					
16	de los modulos del sistema de informacion							
17	cada uno de los lideres de los modulos							
18	Se presentaron no conformidades en el dianostico del sistema de informacion y aplicativos desarrollados por la organización			calidad	Numero de no conformidades/Numero de modulos diagnosticados			
19	Registrar no conformidad y aplicar plan de mejora, informar al proveedor del SI o aplicativo		SIS-FNC-001					
20	Presentar informe de auditoria		SIS-MAS-001					

ELABORADO POR:	REVISADO POR:	APROBADO POR:
COORDINACION INFORMACION Y SISTEMAS	GESTIÓN DE CALIDAD / SUBGERENCIA ADMINISTRATIVA	GERENCIA

Nombre del proceso: Mantenimiento preventivo de hardware y software.

Responsable: Técnico en sistemas.

Objetivo: Obtener tecnología en correcto funcionamiento y acorde a las necesidades de cada área logrando así la atención oportuna y eficiente de los clientes de la organización.

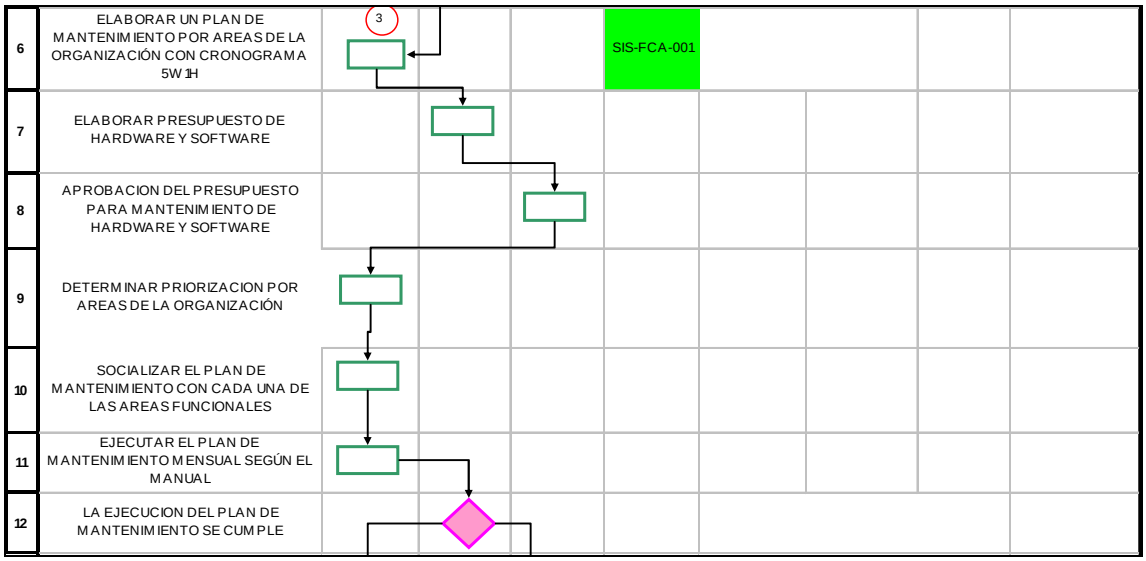
HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO E.S.E	PROCESO: ADMINISTRACION DEL SISTEMA DE INFORMACION	CODIGO:	FECHA DE ELABORACIÓN:
			2 DE MAYO DEL 2006
	SUBPROCESO: MANTENIMIENTO PREVENTIVO DE HARDWARE Y SOFTWARE		FECHA DE ACTUALIZACIÓN:
		VERSIÓN:	2 DE MAYO DEL 2006
		OO	HOJA: 1 DE: 2

OBJETIVO: Obtener tecnologia en correcto funcionamiento y acorde a las necesidades de cada area logrando asi la atencion oportuna y efciente de los clientes de la organización.

ALCANCE: Toda la organización

RESPONSABLE: Coordinador de Informacion y sistemas - Tecnicos en Sistemas

	RESPONSABLES / DESCRIPCION	TECNICO EN SISTEMAS	COORDINADOR DE INFORMACION Y SISTEMAS	COMITÉ DE COMPRAS	REGISTROS	PUNTOS DE CONTROL			
1	INICIO								
2	REALIZAR PROGRAMA DE MANTENIMIENTO PREVENTIVO				SIS-INM -001				
3	INVENTARIO DE EQUIPOS DE COMPUTO E IMPRESORAS INCLUYENDO SOFTWARE				SIS-PMI-001				
4	LOS INVENTARIOS DE EQUIPOS E IMPRESORAS ESTAN ACORDE CON EL LISTADO DE ACTIVOS FIJOS	NO			Numero de equipos del inventario /Numero de equipos de Activos Fijos				
5	ACTUALIZAR LISTADO DE ACTIVOS O INVENTARIOS-HOJA DE VIDA		SI		SIS-FHV-001				



Nombre del Proceso: Mantenimiento correctivo hardware y software.

Responsable: Técnico en sistemas.

Objetivo: Obtener tecnología en correcto funcionamiento y acorde a las necesidades de cada área logrando así la atención oportuna y eficiente de los clientes de la organización.

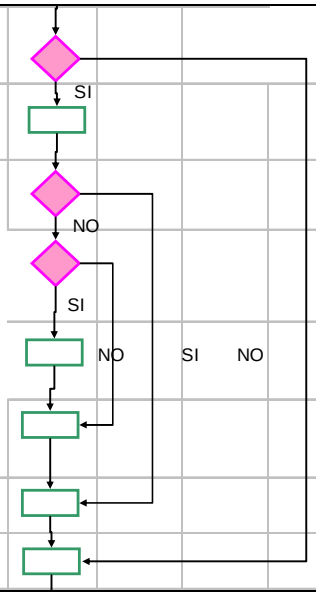
HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO E.S.E	PROCESO: ADMINISTRACION DEL SISTEMA DE INFORMACION	CODIGO:	FECHA DE ELABORACIÓN:
			2 DE MAYO DEL 2006
	SUBPROCESO: MANTENIMIENTO CORRECTIVO DE HARDWARE Y SOFTWARE		FECHA DE ACTUALIZACIÓN:
		VERSIÓN:	2 DE MAYO DEL 2006
		OO	HOJA: 1 DE: 2

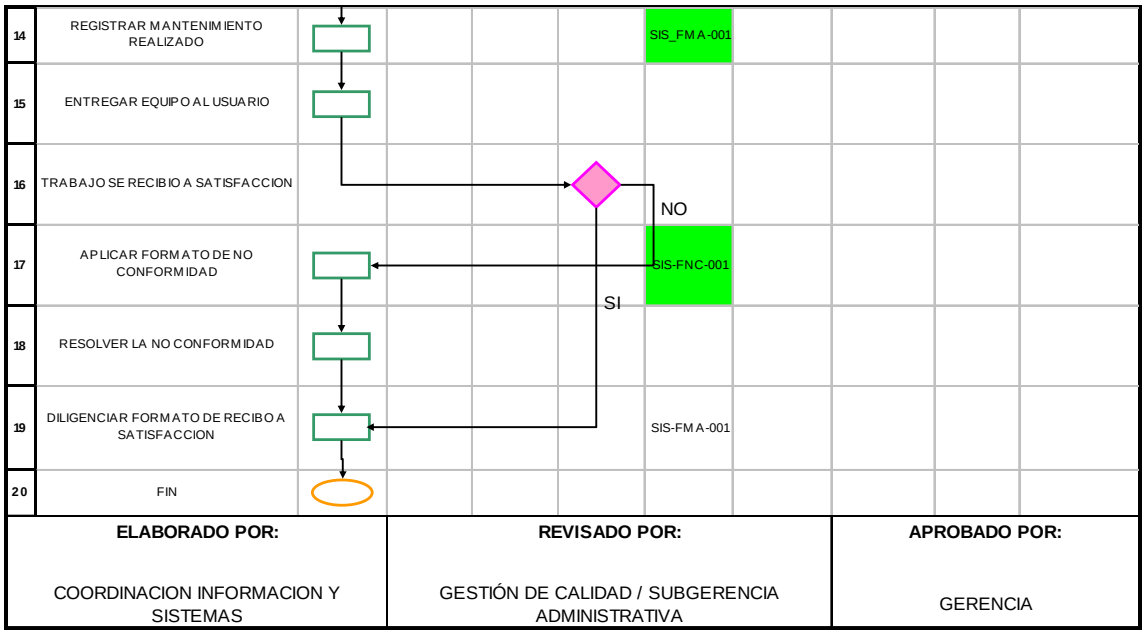
OBJETIVO: Obtener tecnologia en correcto funcionamiento y acorde a las necesidades de cada area logrando asi la atencion oportuna y eficiente de los clientes de la organización.

ALCANCE: Toda la organización

RESPONSABLE: Coordinador de Informacion y sistemas - Tecnicos en Sistemas

	DESCRIPCION / RESPONSABLES	TECNICO EN SISTEMAS	COORDINADOR DE INFORMACION Y SISTEMAS	COMITÉ DE COMPRAS	USUARIO	REGISTROS	PUNTOS DE CONTROL			
1	INICIO									
2	RECEPCIONAR FORMATO DE MANTENIMIENTO DE HARDWARE O SOFTWARE					SIS_FMA-001				
3	RADICAR FORMATO ASIGNARLE CONSECUTIVO Y ASIGNACION DE RESPONSABLE					SIS_FMA-001				
4	RETIRAR EL EQUIPO DEL AREA PARA SER LLEVADO A MANTENIMIENTO									
5	REALIZAR DIAGNOSTICO DE HARDWARE Y SOFTWARE									
6	EL EQUIPO NECESITA RESPUESTOS									
7	DILIGENCIAR FORMATO DE SOLICITUD DE REPUESTOS					SIS-FSR-001				
8	HAY STOCK EN EXISTENCIAS									
9	EL REPUESTO SE PUEDE COMPRAR POR CAJA MENOR									
10	APLIQUE SUBPROCESO DE CAJA MENOR									
11	APLICAR SUBPROCESO DE ADQUISICION DE BIENES									
12	RECEPCIONAR REPUESTOS									
13	REALIZAR MANTENIMIENTO CORRECTIVO									





Nombre del Proceso: Producción y entrega de información.

Responsable: Técnico en sistemas.

Objetivo: Brindar información confiable, oportuna a los clientes externos e internos de la organización que la requieran.

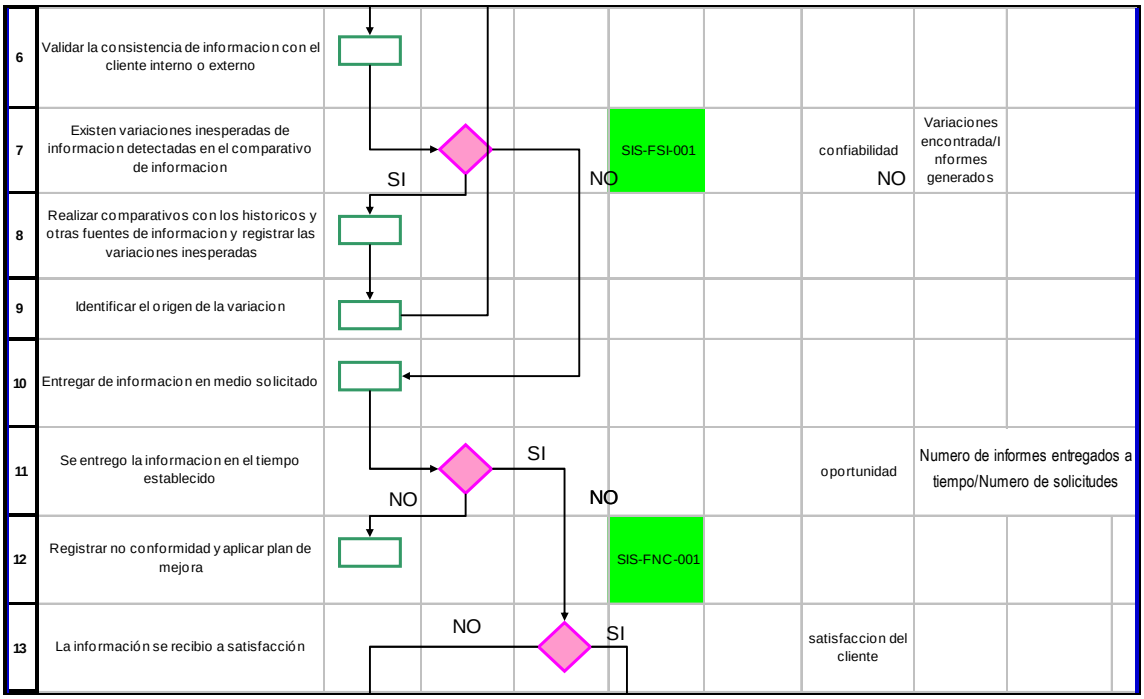
HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO E.S.E	PROCESO: ADMINISTRACION DEL SISTEMA DE INFORMACION	CODIGO:	FECHA DE ELABORACIÓN:
			2 DE MAYO DEL 2006
	SUBPROCESO: Produccion y entrega de Informacion		FECHA DE ACTUALIZACIÓN:
		VERSIÓN:	2 DE MAYO DEL 2006
		OO	HOJA: 1 DE: 2

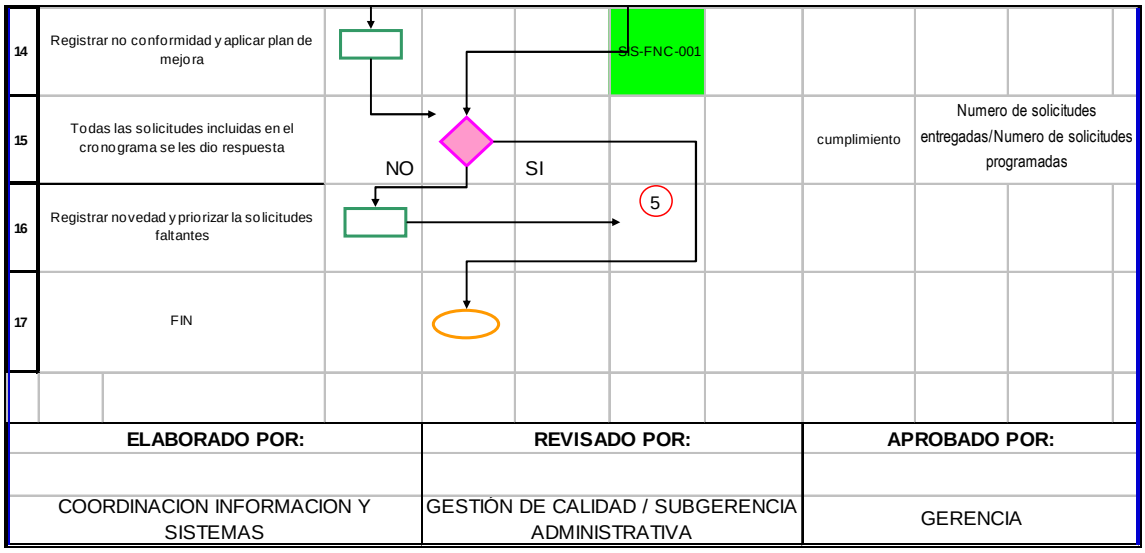
OBJETIVO: Brindar informacion confiable, oportuna a los clientes externos e internos de la organización que la requieran.

ALCANCE: Toda la organización y clientes externos

RESPONSABLE: Coordinador de Informacion y sistemas - Tecnicos en Sistemas

	DESCRIPCION / RESPONSABLES	TECNICO EN SISTEMAS	COORDINADOR DE INFORMACION Y SISTEMAS	CLIENTE	REGISTROS	PUNTOS DE CONTROL			
1	INICIO								
2	Determinar las necesidades de informacion de los clientes internos y externos de la organización				SIS-FSI-001				
3	Priorizar las necesidades de informacion de acuerdo a normatividad, cliente y tipo de informacion solicitada								
4	Establecer un cronograma con base en la solicitud de informacion 5w 1h de los clientes internos-Externo				SIS-FCA-001				
5	Generar informacion con base en el cronograma 5w 1h tanto del cliente interno como externo								
6	Validar la consistencia de informacion con el cliente interno o externo								
7	Existen variaciones inesperadas de informacion detectadas en el comparativo de informacion				SIS-FSI-001		confiabilidad	Variaciones encontrada/Informes generados	
8	Realizar comparativos con los historicos y otras fuentes de informacion y registrar las variaciones inesperadas								
9	Identificar el origen de la variacion								
10	Entregar de informacion en medio solicitado								
11	Se entrego la informacion en el tiempo establecido						oportunidad	Numero de informes entregados a tiempo/Numero de solicitudes	
12	Registrar no conformidad y aplicar plan de mejora				SIS-FNC-001				
13	La información se recibio a satisfacción						satisfaccion del cliente		





Nombre del Proceso: Actualización, implementación e implantación de módulos y aplicativos.

Responsable: Técnico en sistemas.

Objetivo: Dar soluciones informáticas a las áreas de la organización que las requieran, con base en los requerimientos de información de cada área, con el fin de lograr sistematizar sus procesos obteniendo un adecuado tiempo de respuesta en la atención de sus clientes.

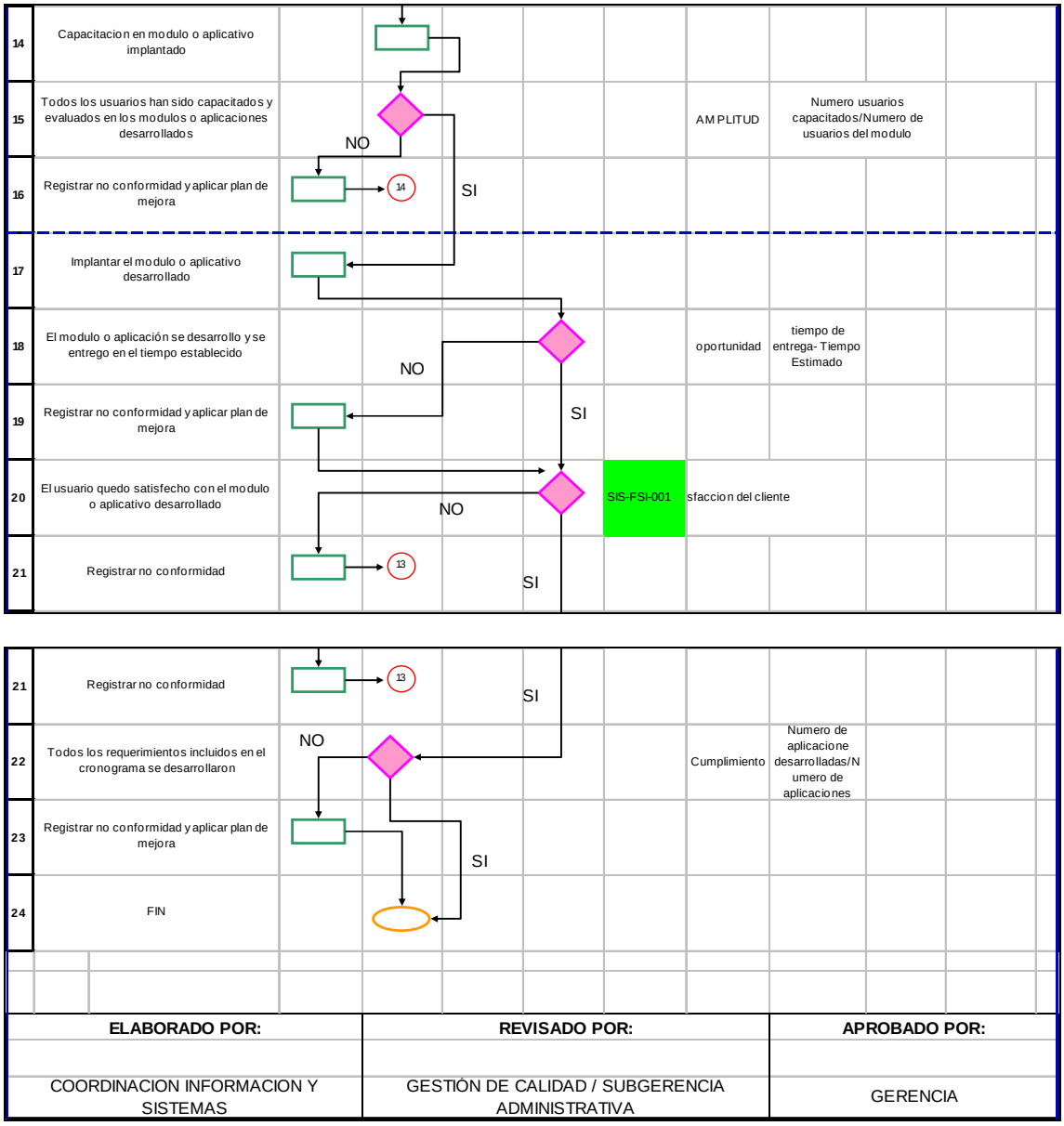
HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO E.S.E	PROCESO: ADMINISTRACION DEL SISTEMA DE INFORMACION	CODIGO:	FECHA DE ELABORACIÓN:
			2 DE MAYO DEL 2006
	SUBPROCESO: Actualizacion, Implementacion e Implantacion de Modulos y Aplicativos		FECHA DE ACTUALIZACIÓN:
		VERSIÓN:	2 DE MAYO DEL 2006
		OO	HOJA: 1 DE: 2

OBJETIVO: Dar soluciones informaticas a las areas de la organización que las requieran, con base en los requerimientos de informacion de cada area, con el fin de lograr sistematizar sus procesos obteniendo un adecuado tiempo de respuesta en la atencion de sus clientes.

ALCANCE: Toda la organización

RESPONSABLE: Coordinador de Informacion y sistemas - Tecnicos en Sistemas

	RESPONSABLES / DESCRIPCION	TECNICO EN SISTEMAS	COORDINADOR DE INFORMACION Y SISTEMAS	COMITÉ DE COMPRAS	CLIENTE INTERNO	REGISTROS	PUNTOS DE CONTROL
1	INICIO						
2	Es una actualizacion del sistema de informacion o aplicativo desarrollado por la organización		NO				
3	Ir al paso 2 del proceso de auditoria						
4	Paso satisfactoriamente el proceso de auditoria		14 SI / 24 NO				
5	Identificar necesidades de sistematizacion de procesos de la organización.					SIS-FSI-001	
6	Priorizar las necesidades de informacion de acuerdo a: normatividad y al cliente interno.						
7	Realizar un estudio de factibilidad (costo / beneficio) o comparacion con otra institucion						
8	El desarrollo de la aplicación es factible		NO / SI			FACTIBILIDAD Costo/Beneficio	
9	Registrar no conformidad		24			SIS-FNC-001	
10	Establecer un cronograma con base en la solicitud de requerimientos 5w 1h de los clientes internos					SIS-FCA-001	
11	Determinar requerimientos y presupuesto de hardware, software y talento humano						
12	Existe aprobación del Presupuesto		SI / NO 24				
13	Desarrollo de la aplicación con base en la metodologia 5w 1h teniendo en cuenta instructivo creacion de prototipos					SIS-MCP-001	



Nombre del Proceso: Auditoría de sistemas.

Responsable: Coordinador de información y sistemas.

Objetivo: Garantizar un sistema de información confiable mediante un proceso de auditoría que permita, administrar y controlar por medio de una evaluación, al proveedor del sistema de Información y aplicativos desarrollados por el mismo y los implantados por la organización.

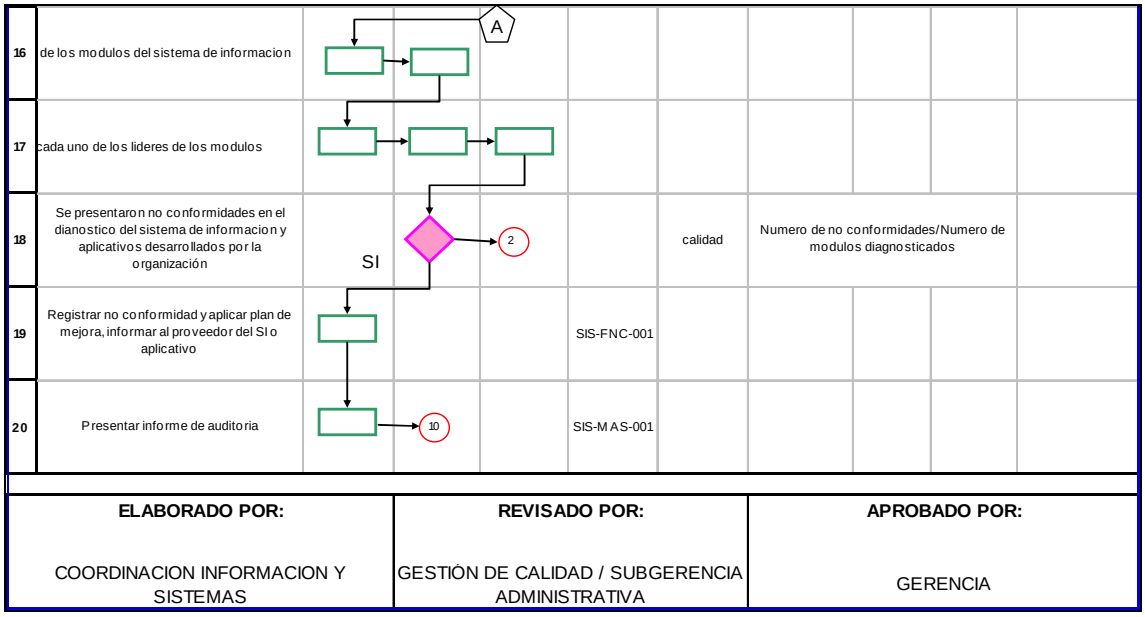
HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO E.S.E	PROCESO: ADMINISTRACION DEL SISTEMA DE INFORMACION	CODIGO:		FECHA DE ELABORACIÓN:
				2 DE MAYO DEL 2006
				FECHA DE ACTUALIZACIÓN:
	SUBPROCESO: Auditoria de Sistemas	VERSIÓN:		2 DE MAYO DEL 2006
		OO		HOJA: 1 DE: 2

OBJETIVO: Garantizar un sistema de información confiable mediante un proceso de auditoria que permita, administrar y controlar por medio de una evaluacion, al proveedor del Sistema de Información y aplicativos desarrollados por el mismo y los implantados por la organizacion.

ALCANCE: Toda la organización

RESPONSABLE: Coordinador de Informacion y sistemas - Tecnicos en Sistemas

	DESCRIPCION / RESPONSABLES	TECNICO EN SISTEMAS	COORDINADOR DE INFORMACION Y	LIDERES DE LOS MODULOS	REGISTROS	PUNTOS DE CONTROL				
1	INICIO									
2	Elaboracion de un cronograma de diagnostico y-o actualizacion trimestral con cada uno de los lideres de los modulos del sistema de informacion 5w 1h				SIS-FCA-001					
3	Socializar con cada lider de los modulos el cronograma para coordinar actividades para el diagnostico y-o actualizacion									
4	Entregar mediante oficio a cada lider del modulo las fechas de actualizacion y-o diagnostico y-o actualizacion									
5	Todos los lideres de los modulos han sido incluidos en el cronograma e informados sobre fechas de diagnostico y-o actualizacion del SI	NO				amplitud	Numero de lideres socializados/Numero de Modulos o aplicativos			
6	Registrar no conformidad y aplicar plan de mejora		3	SI	SIS-FNC-001					
7	Realizar diagnostico de cada uno de los modulos y-o aplicativos del sistema de informacion									
8	Se presentaron no conformidades en el dianostico y-o actualizacion del sistema de informacion y aplicativos desarrollados por la organización	SI		NO		calidad	Numero de no conformidades/Numero de modulos diagnosticados			
9	Presentar informe de auditoria		2		SIS-MAS-001					
10	Registrar no conformidad y aplicar plan de mejora, informar al proveedor del SI o aplicativo				SIS-FNC-001					
11	Recepcion de Medio magnetico empresa proveedora o el aplicativo actualizado				SIS-FRI-001					
12	Realizar verificacion de condiciones tecnicas de los medios magneticos (FISICA Y TECNICA)				SIS-FRI-001					
13	Se realizo la recepcion y se determino el estado del medio magnetico	NO			SIS-FRI-001	si/no	confiabilidad			
14	n de insumos e informar al proveedor			SI	SIS-FRI-001					
15	los datos obtenidos en la lista de chequeo		11	A	SIS-FRI-001					



4.1.6. Descripción de los procesos asistenciales de historia clínica

4.1.6.1. Triage

Proceso de categorización de lesionados basado en la urgencia de sus lesiones y la posibilidad de supervivencia", diferente al criterio de atención en condiciones normales, en las que el lesionado más grave tiene prioridad sin tener en cuenta el pronóstico inmediato o a largo plazo.

La aplicación de los diferentes conceptos sobre el triage de los lesionados comprende una serie de acciones que se complementan entre sí, como son:

- La evaluación de los lesionados según su gravedad.
- La asignación de prioridades según la posibilidad de sobrevivencia.
- La identificación.
- La estabilización.
- La asignación de su destino inmediato y final.

Todas estas acciones deben estar enmarcadas dentro de esquemas estandarizados de atención de emergencias.

La selección se basa en un procedimiento asistencial de carácter diagnóstico, que luego debe ser complementado con cuidados iniciales de urgencia, estabilización del lesionado, supervivencia y transporte hacia los demás niveles de atención en salud.

Prioridad tipo I ó ROJA: Se aplica a los lesionados de CUIDADOS INMEDIATOS, quienes requieren una atención médica urgente, ya que por la gravedad de sus lesiones pueden perder su vida y con los recursos disponibles tienen probabilidad de sobrevivir.

Prioridad tipo II ó AMARILLA: Se aplica a los lesionados de CUIDADOS INTERMEDIOS O DIFERIBLES, quienes requieren una atención médica que da lugar a espera.

Prioridad tipo III ó NEGRA: Se aplica a los lesionados de CUIDADOS MINIMOS, es decir, a aquellos cuyas lesiones son de tal gravedad, que existen pocas o ninguna probabilidad de sobrevivir, pero que merecen algún grado de atención médica.

Prioridad tipo IV ó VERDE: Se reserva para aquellos lesionados de CUIDADOS MENORES, o sea los que presentan lesiones leves o que su atención puede dejarse para el final sin que por ello se vea comprometida su vida.

Prioridad tipo V ó BLANCA Este color se utiliza para las personas fallecidas, todos estos criterios para la clasificación de los lesionados por colores, implican una elección, la cual se ve complementada por un diagnóstico preliminar, cuidados iníciales, estabilización, medidas de supervivencia y transporte, los cuales se realizan siguiendo una serie de etapas de triage, como son:

- Etapa diagnóstica: Que conduce a la categorización por colores en cada nivel.
- de triage, según el orden de atención.
- Etapa terapéutica: Que permite adoptar los primeros pasos en el manejo de las lesiones según su gravedad.
- Etapa de preparación: En la que se prepara y organiza la evacuación de los lesionados hacia el siguiente nivel de triage.

Entidades que participan en el proceso

- Vigilante que entrega turno
- Usuario – Paciente.
- Medico

Procedimiento

- El usuario ingresa.
- Solicita el servicio.
- El operario de servicios generales realiza la recepción y observación del usuario de que se deriva el medio de transporte y la activación del circuito de emergencias.
- Se realiza el registro del usuario en el libro control de ingreso y entrega la boleta de oportunidad de la atención.

4.1.6.2. Urgencias

Se garantiza al usuario que asiste a la consulta médica de urgencias, una atención oportuna de acuerdo a su condición, con el fin de satisfacer sus necesidades de salud en el tiempo requerido.

Entidades que participan en el proceso

- Medico hospitalario de urgencias
- Enfermera jefe
- Auxiliar de enfermería.

Procedimiento

El paciente ingresa al consultorio de Triage en donde se asigna el nivel de complejidad de la patología asociada a la atención y en consulta médica de urgencias se registra la historia clínica de urgencias del paciente según instructivo.

Dentro de la consulta médica de urgencias se pueden tomar acciones para el paciente detalladas así:

- Observación
- Remitir a otra entidad de salud de menor nivel
- Remitir a otra entidad de salud de mayor nivel
- Atención por consulta externa

Ingreso a observación

Este subproceso se define por ingresar al usuario al proceso de observación brindando una adecuada información y orientación a él y su familia, el paciente ingresa al área de observación proveniente de consulta inicial de urgencias y consulta externa.

Entidades que participan en el proceso

- Equipo multidisciplinario.
- Medico especialista
- Enfermera jefe
- Auxiliar de enfermería

Procedimiento

Se recepciona el paciente por parte de la enfermera y la documentación que trae de consultorio de urgencias.

Se realiza el ingreso del paciente al área de observación y se le brinda la atención diaria intrahospitalaria que requiera la patología asociada a la atención.

Otros subprocesos relacionados a urgencias:

- Atención diaria intrahospitalaria.
- Egreso y seguimiento al usuario.
- Preparación pre-operatoria.
- Interconsulta.
- Preparación de ayudas diagnosticas y terapéuticas a pacientes hospitalizados.
- Administración de medicamentos a usuarios hospitalizados.
- Procedimientos asistenciales especiales.
- Junta medica.
- Custodia de pertenencia al usuario.

4.1.6.3. Consulta Externa

El paciente puede proceder del servicio de:

- Triage
- Urgencias
- Hospitalización
- Remitido de un servicio de salud de menor complejidad

El paciente ingresa a la especialidad que amerite el tipo de enfermedad que presenta, se realizan los procedimientos respectivos para el ingreso del paciente al proceso de consulta externa.

Se realiza el registro de historia clínica de consulta externa en el consultorio del medico tratante. A continuación se relacionan un ejemplo de proceso a*sistencial en el área de urgencias* que se manejan al interior del hospital universitario departamental de Nariño, y que son tomados en cuenta por la oficina de coordinación y sistemas para el proceso de implantación del módulo de historia clínica electrónica.

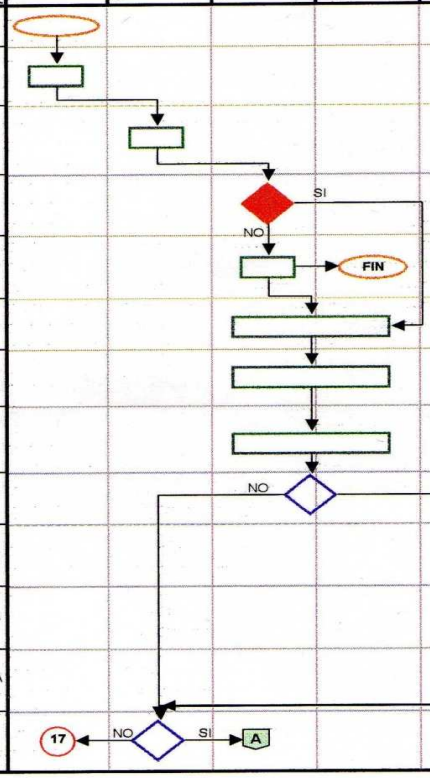
HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO E.S.E	PROCESO: URGENCIAS	CODIGO:	FECHA DE ELABORACIÓN:
		PRURG - 08	31 de Marzo de 2008
	SUBPROCESO: PREPARACIÓN DE AYUDAS DIAGNOSTICAS Y TERAPEUTICAS A PACIENTES HOSPITALIZADOS		FECHA DE ACTUALIZACIÓN:
		VERSIÓN:	31 de Marzo de 2008
		OO	HOJA: 1 DE: 2

OBJETIVO: Garantizar una oportuna preparación al usuario e información a los procesos correspondientes de ayudas diagnósticas y terapeúticas para apoyar efectivamente el diagnostico y/o tratamiento del usuario

ALCANCE: Servicio de Urgencias

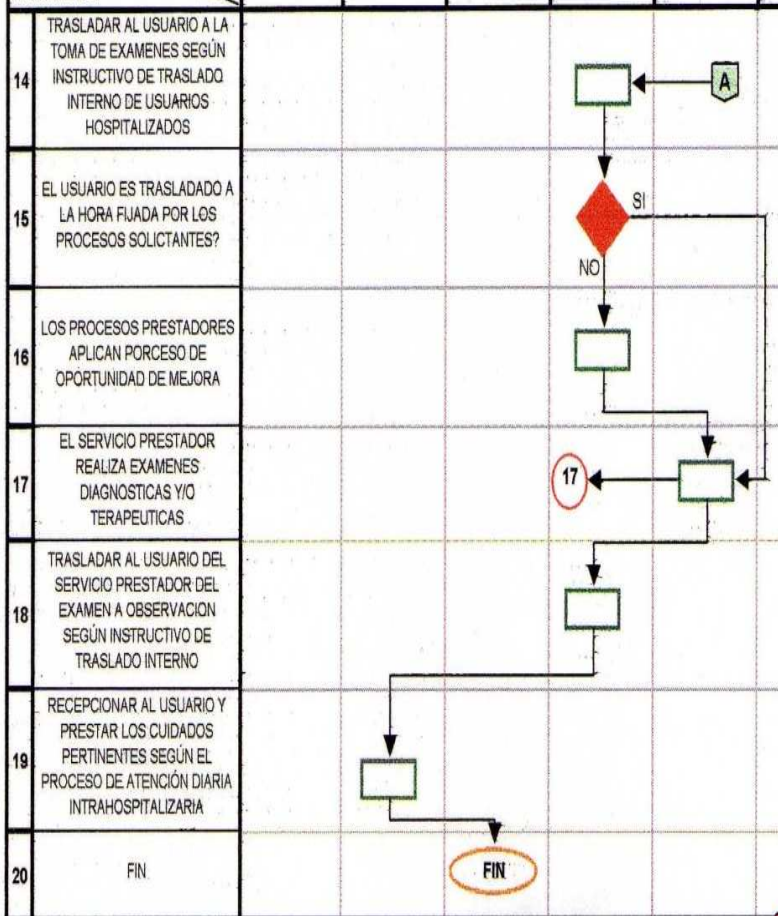
RESPONSABLE: Enfermera - Auxiliar de Enfermería - Auxiliar administrativa - Operario de servicios Generales

	DESCRIPCION / RESPONSABLES	MEDICO TRATANTE	ENFERMERA	AUXILIAR ADMINISTRATIVA	OPERARIO DE SERVICIOS GENERALES	PROCESOS PRESTADORES DE SERVICIOS	AUXILIAR DE ENFERMERIA	REGISTROS	PUNTO DE CONTROL
1	INICIO								
2	REGISTRAR LA ORDEN MEDICA EN LA HISTORIA CLINICA Y ELABORAR EL FORMATO CORRESPONDIENTE							SOLICITUD DE AYUDAS DIAGNOSTICAS	
3	RECEPCIONAR ORDEN Y ENTREGAR EL FORMATO A LA AUXILIAR ADMINISTRATIVA Y/O CAMILLERO PARA EL TRAMITE CORRESPONDIENTE								
4	LA AYUDA DIAGNOSTICA Y/O TERAPEUTICA SE PRESTA EN LAS INSTALACIONES DEL HOSPITAL								CAPACIDAD
5	VER PROCESO DE TRAMITE Y TRASLADO EXTERNO DE USUARIOS HOSPITALIZADOS								
6	REGISTRAR ORDEN EN RADICADOR DE AYUDAS DIAGNOSTICAS								
7	LLEVAR AL SERVICIO PRESTADOR LA ORDEN DILIGENCIADA CON EL RADICADOR								
8	HACE FIRMAR EN EL LIBRO LA HORA DE ENTREGA DE LA SOLICITUD EN EL SERVICIO DONDE SE REALIZA EL PROCEDIMIENTO								
9	EL USUARIO REQUIERE PREPARACIÓN PARA LA TOMA DE AYUDAS								
10	PREPARAR AL USUARIO TENIENDO EN CUENTA LAS INDICACIONES BRINDADAS POR EL SERVICIO PRESTADOR								
11	SE PREPARO AL USUARIO SEGÚN INDICACIONES DE CADA SERVICIO?								RACIONALIDAD
12	APLICA PROCESO DE OPORTUNIDAD DE MEJORA Y DA RESPUESTA AL MISMO								
13	EL USUARIO REQUIERE SER TRASLADADO INTERNAMENTE								



HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO E.S.E	PROCESO: URGENCIAS	CODIGO:	FECHA DE ELABORACIÓN:
		PRURG -08	31 de Marzo de 2008
	SUBPROCESO: PREPARACION DE TOMA DE AYUDAS DIAGNOSTICAS Y TERAPEUTICAS A PACIENTES HOSPITALIZADOS	VERSIÓN:	FECHA DE ACTUALIZACIÓN:
		00	31 de Marzo de 2008
			HOJA: 2 DE: 2

	DESCRIPCION / RESPONSABLES	MEDICO TRATANTE	ENFERMERA	AUXILIAR ADMINISTRATIVA	OPERARIO DE SERVICIOS GENERALES	PROCESOS PRESTADORES DE SERVICIOS	AUXILIAR DE ENFERMERIA	REGISTROS	PUNTO DE CONTROL
14	TRASLADAR AL USUARIO A LA TOMA DE EXAMENES SEGÚN INSTRUCTIVO DE TRASLADO INTERNO DE USUARIOS HOSPITALIZADOS								
15	EL USUARIO ES TRASLADADO A LA HORA FIJADA POR LOS PROCESOS SOLICTANTES?							RADICADOR	OPORTUNIDAD
16	LOS PROCESOS PRESTADORES APLICAN PORCESO DE OPORTUNIDAD DE MEJORA								
17	EL SERVICIO PRESTADOR REALIZA EXAMENES DIAGNOSTICAS Y/O TERAPEUTICAS								
18	TRASLADAR AL USUARIO DEL SERVICIO PRESTADOR DEL EXAMEN A OBSERVACION SEGÚN INSTRUCTIVO DE TRASLADO INTERNO								
19	RECEPCIONAR AL USUARIO Y PRESTAR LOS CUIDADOS PERTINENTES SEGÚN EL PROCESO DE ATENCIÓN DIARIA INTRAHOSPITALIZARIA								
20	FIN								



CONTROLADO

ELABORADO POR:	REVISADO POR:	APROBADO POR:
Grupo de Urgencias	Gestión de Calidad	Gerencia

4.1.6.4. Hospitalización

El proceso de hospitalización trata del ingreso del paciente a observación, se tienen en cuenta las siguientes etapas:

- Inicio.
- Se recepciona al usuario y la documentación que trae del consultorio de urgencias.
- Se solicita información pertinente referente a la condición clínica del paciente.
- Se realizan los procedimientos asistenciales pertinentes.
- Se hace el ingreso del paciente al servicio de observación.
- Se elabora el registro en la aplicación de historia clínica y se realiza el registro de enfermería correspondiente.

4.1.7. Descripción del aplicativo WINDG

El proceso de instalación y configuración para el aplicativo de dinámica Gerencial.Net, está diseñado por sistemas y asesorías de colombia SYAC, bajo plataforma .net.

- SISTEMA DE INFORMACION WINGDG: Aplicativo para el manejo asistencial y administrativo del hospital universitario departamental de Nariño puede ser implantada en ambientes para Internet o intranet.
- Para instalar la aplicación este tipo de arquitectura, se hace necesario contar con los elementos tales como firewall a nivel físico y/o a nivel de software, con el fin de ofrecer los más altos niveles de seguridad para evitar el acceso no autorizado a la red interna (lan). De igual manera el proveedor de Internet o ISP debe suministrar una dirección IP pública que permita publicar el sitio web.
- La instalación del servidor se debe realizar en un equipo con sistemas operacionales Windows 2000 o superior en sus diferentes versiones,

incluyendo también windows 2000 y xp profesional service pack 2 (únicamente para efecto de pruebas). es importante tener en cuenta que los servidores deben estar completamente actualizados con las ultimas versiones de service pack tanto para el sistema operacional como para el motor de base de datos con el fin de evitar problemas de ejecución.

Instalación de la base de datos

SQL SERVER

Al instalar en sql solo se crean dos contenedores *dgempres01***,** el cual reemplaza todos los contenedores dat para la versión anterior de dinámica y *dggeneral* en el cual se deben importar las estructuras y los datos de generales y seguridad.

Para la nueva versión cada usuario con ingreso a la aplicación debe tener su propia cuenta.

ORACLE

Con este tipo de motor se utiliza la misma estructura que para la anterior versión, cada usuario dentro del motor de base de datos corresponde a un usuario dentro de la aplicación y solo se deben actualizar las estructuras (tablas y campos) con los script correspondientes.

El aplicativo cuenta con manual de capacitación y soporte para el ingreso a la aplicación, a los usuarios finales (Personal asistencial) así como el manual de configuración e instalación de Dinámica.Net, en donde se referencia la instalación del módulo de historias clínicas bajo plataforma .net .

4.1.8. Descripción de la Base De Datos

1. HCACTENFER: Se almacena los datos relacionados con las actividades de enfermería.

dbo_HCACTENFER

HCFECREG	GASCODIGO	GPACODIGO	AINCONSEC	HCHORACTIV	HCACTIVIDAD	HCOBSERVACION	USUCODIGO	HCHORASEG	HCHORATER
Fecha/Hora	Texto	Texto	Texto	Fecha/Hora	Texto	Memo	Texto	Fecha/Hora	Fecha/Hora

2. HCACTPREQ: En esta tabla se relaciona la información perteneciente a las actividades pre- quirúrgicas como fecha de registro, área del servicio, paciente, consecutivo de ingreso, actividad etc.

dbo_HCACTPREQ

HCFECREG	GASCODIGO	GPACODIGO	AINCONSEC	HCACTIVIDAD	HCOBSERVACION	USUCODIGO
Fecha/Hora	*Texto*	*Texto*	*Texto*	*Texto*	*Memo*	*Texto*

3. HCACTRENAL: Se almacena los datos relacionados con la actividad renal.

dbo_HCACTRENAL

OID	HCDESCRIP	HCDESHAB	GCRecord
Autonumérico	*Texto*	*Sí/No*	*Número*

4. HCANEXOD: Esta tabla contiene la información relacionada con los datos del anexo de diagnostico, los cuales se encuentran en el botón anexo diagnostico de historia.

dbo_HCANEXOD

GPACEDULA	GPACODIGO	AINCONSEC	HCCONFOLIO	ANOBSERVA	HCCONFOLI
Texto	*Texto*	*Texto*	*Número*	*Texto*	*Número*

5. HCANTECE: Se almacena la información relacionada con los antecedentes del paciente.

dbo_HCANTECE					
GPACODIG	**AINCONSEC**	**HCCONFOLI**	**HCCTIPOHC**	**HCAOPGPAT**	**HCACUALPA**
Texto	*Texto*	*Número*	*Texto*	*Número*	*Texto*
HCAOPGQUI	**HCACUALQU**	**HCAOPGFAR**	**HCACUALFA**	**HCAOPGTOX**	**HCALCOHOL**
Número	*Texto*	*Número*	*Texto*	*Número*	*Número*
HCACIGARR	**HCAESTIMU**	**HCACAOTOXIC**	**HCACUALTX**	**HCAFRETOX**	**HCAOPGALE**
Número	*Número*	*Número*	*Texto*	*Texto*	*Número*
HCAALERGI	**HCAOPGAME**	**HCASULFAS**	**HCAMAINES**	**HCAPENICI**	**HCATETRAC**
Texto	*Número*	*Número*	*Número*	*Número*	*Número*
HCAOTROAL	**HCACUALAL**	**HCAGINECG**	**HCAGINECP**	**HCAGINECA**	**HCAGINFUR**
Número	*Texto*	*Número*	*Número*	*Número*	*Texto*
HCACICLO1	**HCACICLO2**	**HCACICREG**	**HCAACTSEX**	**HCAPLANIF**	**HCAMETODO**
Texto	*Texto*	*Número*	*Número*	*Número*	*Número*
HCACUALME	**HCAOPGETS**	**HCACUAETS**	**HCAOPGTRA**	**HCACUATRA**	**HCAFAMILI**
Texto	*Número*	*Texto*	*Número*	*Texto*	*Texto*
HCACODIGO	**HCAFECREG**	**HCACESARE**	**HCAFECPPA**	**HCAEDAGES**	**HCAOBSGIN**
Texto	*Fecha/Hora*	*Número*	*Fecha/Hora*	*Número*	*Texto*
HCAOPGFUS	**HCACUAFUS**	**HCMENARQUI**	**HCMENOPAU**	**HCANTEHOSP**	**HCEMBARAZ**
Número	*Texto*	*Número*	*Número*	*Memo*	*Número*
HCPARTO	**HCCAUCESA**	**HCPN**	**HCTN**	**HCAPGAR**	**HCPATPER**
Número	*Memo*	*Número*	*Número*	*Número*	*Número*
HCUALPAT					
Texto					

6. HCANTECED: Se almacena la información relacionada con los antecedentes del paciente.

dbo_HCANTECED									
GPACODIGO	**ANTMEDICO**	**ANTQUIRUR**	**ANTTRANSF**	**ANTTOXICO**	**ANTINMUNO**	**ANTALERGI**	**ANTTRAUMA**	**ANTPSIQUI**	**ANTGINECO**
Texto	*Memo*	*Memo*	*Memo*	*Memo*	*Memo*	*Memo*	*Memo*	*Memo*	*Memo*
ANTGINECG	**ANTGINECP**	**ANTGINECA**	**ANTGINECC**	**ANTGINECV**	**ANTPLANIF**	**ANTMETODO**	**ANTFARMAC**	**ANTFAMILI**	**ANTOTROS**
Número	*Número*	*Número*	*Número*	*Número*	*Número*	*Memo*	*Memo*	*Memo*	*Memo*

7. HCANTENCEN: Se almacena la información relacionada con los antecedentes del paciente.

dbo_HCANTENCEN							
GPACODIGO	**ANTFECHA**	**GMECODIGO**	**ANTTIPO**	**ANTDETALLE**	**ANTGINECG**	**ANTGINECP**	**ANTGINECA**
Texto	*Fecha/Hora*	*Texto*	*Número*	*Memo*	*Número*	*Número*	*Número*
ANTGINECC	**ANTGINECV**	**ANTPLANIF**	**ANTMETODO**	**ANTNUMERO**	**ANTRESALTA**	**ANTGINECE**	**ANTGINECM**

Número	*Número*	*Número*	*Memo*	*Número*	*Número*	*Número*	*Número*
ANTGINFUP	**ANTOPCION**	**ANTFUMADO**	**ANTFUMTIE**	**ANTFUMMED**	**ANTEXFTIE**	**ANTEXFMED**	**ANTFUMCAS**
Fecha/Hora	*Texto*	*Texto*	*Número*	*Número*	*Número*	*Número*	*Número*
ANTMASCAS	**ANTEXPTIE**	**ANTEXPMED**	**ANTSUSTAN**	**ANTSUSTIE**	**ANTSUSMED**		
Número	*Número*	*Número*	*Memo*	*Número*	*Número*		

8. HCAUDENF: En esta tabla se relaciona la información perteneciente a la auditoría de registro de enfermería como fecha, código de área y paciente, etc.

dbo_HCAUDENF

HCFECREG	GASCODIGO	GPACODIGO	AINCONSEC	HCCODTURNO	HCHORARIO	HCNOMMOD	HCFECMOD
Fecha/Hora	*Texto*	*Texto*	*Texto*	*Texto*	*Texto*	*Texto*	*Fecha/Hora*

9. HCAUTMED: Esta tabla contiene la información relacionada con la autorización médica como: documento, paciente, ingreso, folio, medicamentos y justificaciones.

dbo_HCAUTMED

GPACEDULA	GPACODIGO	AINCONSEC	HCCONFOLI	HCMNUEVOP	HCAJUSTI1	HCAJUSTI2	HCAJUSTI3	HCAJUSTI4	HCAJUSTI5
Texto	*Texto*	*Texto*	*Número*	*Texto*	*Texto*	*Texto*	*Texto*	*Texto*	*Texto*

10. HCAUTOTUR: En esta tabla se almacena la información sobre las autorizaciones de turno de médicos y enfermeras.

dbo_HCAUTOTUR

HCUSUARIO	HCTURNO	HCHORINIM	HCHORFINM	HCHORINIT	HCHORFINT	HCHORININ	HCHORFINN
Texto	*Número*	*Fecha/Hora*	*Fecha/Hora*	*Fecha/Hora*	*Fecha/Hora*	*Fecha/Hora*	*Fecha/Hora*

11. HCAUTPRO: Se almacena la información perteneciente a los consentimientos informados en relación a procedimientos con pacientes.

dbo_HCAUTPRO

HCUCONSEC	HCUFECDOC	GPACODIGO	AINCONSEC	HCCONFOLI	GMECODIGO	HCUTEXTO1	HCUTEXTO2	HCUUSUCRE
Texto	*Fecha/Hora*	*Texto*	*Texto*	*Número*	*Texto*	*Memo*	*Memo*	*Texto*

12. HCBLOQREGENF: En este registro se almacena el bloqueo de registro de enfermería.

dbo_HCBLOQREGENF							
GCRecord	**OID**	**HCFECREG**	**GASCODIGO**	**GPACODIGO**	**AINCONSEC**	**HCBLOQUEO**	**USUCODIGO**
Número	*Autonumérico*	*Fecha/Hora*	*Texto*	*Texto*	*Texto*	*Sí/No*	*Texto*

13. HCCAMPOS: En esta tabla se relaciona la información perteneciente a la configuración básica de campos.

dbo_HCCAMPOS							
HCCTIPOHC	**HCCSECCIO**	**HCCNUAREA**	**HCCTIPCAM**	**HCCNCAMPO**	**HCCLONGIT**	**HCCDECIMA**	**HCCINDIME**
Texto	*Número*	*Número*	*Número*	*Texto*	*Número*	*Número*	*Número*
HCCMEDIDA	**HCCTITIND**	**HCCTITULO**	**HCCINDIRE**	**HCCTIPRES**	**HCCINDIRA**	**HCCRANINI**	**HCCRANFIN**
Texto	*Número*	*Texto*	*Número*	*Número*	*Número*	*Número*	*Número*
HCCINCREM	**HCCNUMOPC**	**HCCDESOPC**	**HCCTOPCAM**	**HCCLEFCAM**	**HCCWIDCAM**	**HCCHEICAM**	**HCCWIDTIT**
Número	*Número*	*Memo*	*Número*	*Número*	*Número*	*Número*	*Número*
HCCTABIDX	**HCCDESCRI**	**HCCGUIANT**	**HCCTEXINI**	**HCCEPICRI**	**HCCSALTOS**	**HCCIMTITU**	**HCINFORMU**
Número	*Memo*	*Número*	*Texto*	*Número*	*Número*	*Número*	*Número*
HCFCODIGO	**HCTIPOIMP**	**HCCDIAGNO**	**HCSEPARAC**				
Memo	*Número*	*Número*	*Número*				

14. HCCAMPOSN: En esta tabla se almacena la información relacionada con la configuración avanzada de campos como: tipo de historia, sección, área, nombre del campo, características de controles, titulo de epicrisis, parámetros de condiciones, referencia, contrareferencia entre otros.

dbo_HCCAMPOSN							
HCCTIPOHC	**HCCSECCIO**	**HCCNUAREA**	**HCCNCAMPO**	**HCCPOSXTIT**	**HCCPOSYTIT**	**HCCCOLORFC**	**HCCCOLORLC**
Texto	*Número*	*Número*	*Texto*	*Número*	*Número*	*Texto*	*Texto*
HCCLETRACO	**HCCCOLORFT**	**HCCCOLORLT**	**HCCLETRATI**	**HCCPADRE**	**HCCCONDI**	**HCCINDEX**	**HCCIMAGE**
Memo	*Texto*	*Texto*	*Memo*	*Texto*	*Memo*	*Número*	*Objeto OLE*
HCCEXECON	**HCCEXEFOR**	**HCCSOLLEC**	**HCCTITEPI**	**HCCPARCON**	**HCCPARFOR**	**HCCCOLWIDTH**	**HCCSYSDATE**
Número	*Número*	*Número*	*Texto*	*Memo*	*Memo*	*Número*	*Número*
HCCREFERE	**HCCCONREF**	**HCCTITREF**	**HCCTITCRE**	**HCCHORMIL**	**HCCGETHIS**	**HCCSELIND**	
Número	*Número*	*Texto*	*Texto*	*Número*	*Número*	*Número*	

15. HCCARGOS: Se almacena la información perteneciente a los diferentes cargos del personal asistencial.

dbo_HCCARGOS		
HCCCODIGO	**HCCNOMBRE**	**HCCFUNCIO**
Texto	*Texto*	*Número*

16. HCCDEVMED: En esta tabla se almacena la información relacionada con la cabecera de devolución de medicamentos como fecha, área, paciente, ingreso, numero de devolución, medico, estado, devolución generada.

dbo_HCCDEVMED							
HCFECREG	**GASCODIGO**	**GPACODIGO**	**AINCONSEC**	**HCNUMDEV**	**GMECODIGO**	**HCESTADO**	**IDSNUMERO**
Fecha/Hora	*Texto*	*Texto*	*Texto*	*Número*	*Texto*	*Texto*	*Texto*

17. HCCODONTO: Se almacena los datos relacionados con la cabecera de datos odontológicos.

dbo_HCCODONTO							
GCRecord	**OID**	**GPACODIGO**	**AINCONSEC**	**HCCTIPOHC**	**HCCONFOLI**	**GMECODIGO**	**REGISTRADO**
Número	*Autonumérico*	*Texto*	*Texto*	*Texto*	*Número*	*Texto*	*Fecha/Hora*

18. HCCONANE: Esta tabla almacena los datos relacionados con la contrareferencia anexa.

dbo_HCCONANE						
GCRecord	**OID**	**GPACODIGO**	**AINCONSEC**	**HCCONFOLI**	**HCRCONSEC**	**CONRELANE**
Número	*Autonumérico*	*Texto*	*Texto*	*Número*	*Texto*	*Memo*
CONCONREF	**CONCONDES**	**PRECODIGO**	**CONFECCON**	**CONFECSAL**	**CONCONDUC**	**OptimisticLockField**
Número	*Memo*	*Texto*	*Fecha/Hora*	*Fecha/Hora*	*Texto*	*Número*

19. HCCONCEP: Se almacena los datos relacionados con los conceptos médicos sobre los pacientes.

dbo_HCCONCEP										
HCOCONSEC	HCOFECDOC	HCOCONCDE	HCODIRIGA	GPACODIGO	HCOPESOKG	HCOTALLAP	GEMCODIGO	AINCONSEC	HCCONFOLI	GMECODIGO
Texto	*Fecha/Hora*	*Texto*	*Texto*	*Texto*	*Número*	*Número*	*Texto*	*Texto*	*Número*	*Texto*
HCOMOTIVO	HCOCIRCUN	HCOSINTOM	DIACODIGO	HCOETIOLO	HCOTRATAM	HCOESTACT	HCOPRONOS	HCOCONDUC	HCODOCCER	
Número	*Texto*	*Texto*	*Texto*	*Texto*	*Texto*	*Texto*	*Texto*	*Texto*	*Número*	

20. HCCONING: Se almacena la información perteneciente al control de ingesta de pacientes.

dbo_HCCONING							
HCFECREG	GASCODIGO	GPACODIGO	AINCONSEC	HCHORREG	HCHORAING	HCVIAING	HCESTADO
Fecha/Hora	*Texto*	*Texto*	*Texto*	*Fecha/Hora*	*Fecha/Hora*	*Texto*	*Texto*
HCDESCRIP	USUCODIGO						
Memo	*Texto*						

21. HCCONLIQ: Esta tabla recopila toda la información relacionada con el control de líquidos de pacientes.

dbo_HCCONLIQ						
GPACODIGO	AINCONSEC	HCCFECCON	HCLCODIGO	HCLTIPEVE	HCCCANTID	GMECODIGO
Texto	*Texto*	*Fecha/Hora*	*Texto*	*Número*	*Número*	*Texto*

22. HCCONMED: Se almacena los datos relacionados con el control de medicamentos suministrados a pacientes.

Dbo_HCCONMED							
HCFECREG	GASCODIGO	GPACODIGO	AINCONSEC	HCHORREG	HCHORAMED	IPRCODIGO	
Fecha/Hora	*Texto*	*Texto*	*Texto*	*Fecha/Hora*	*Fecha/Hora*	*Texto*	
HCCANTID	HCDOSIS	HCOBSERV	HCRESPON	HCRESPUES	HCCONFOLI	HCMNUEVOP	USUCODIGO
Número	*Texto*	*Memo*	*Texto*	*Texto*	*Número*	*Texto*	*Texto*

23. HCCONPRE: Se almacena la información sobre los registros bloqueados para préstamo de historias clínicas.

dbo_HCCONPRE	
GPACODIGO	**USUCODIGO**
Texto	*Texto*

24. HCCONREF: Se almacena información perteneciente a las referencias y contrareferencias asignadas a pacientes.

dbo_HCCONREF								
HCRCONSEC	**GPACODIGO**	**HCRFECHRE**	**AINCONSEC**	**HCRREMITE**	**HCRORIGEN**	**GERCODENT**	**GMECODIGO**	**HCRREFERE**
Texto	*Texto*	*Fecha/Hora*	*Texto*	*Número*	*Número*	*Texto*	*Texto*	*Texto*
HCRMOTIRE	**HCTCODIGO**	**HCDCODIGO**	**HCCONFOLI**	**GMECODIG1**	**HCRFECRES**	**HCRANAMNE**	**HCRSIGNTA**	**HCRSIGNTO**
Memo	*Texto*	*Texto*	*Número*	*Texto*	*Fecha/Hora*	*Memo*	*Texto*	*Número*
HCRSIGNFC	**HCRSIGNFR**	**HCRSIGNPS**	**HCRSIGNTL**	**HCREXAFIS**	**HCRRESPRU**	**HCRTRAINS**	**HCRDIAPRE**	**HCRTIPDOC**
Número	*Número*	*Número*	*Número*	*Memo*	*Memo*	*Memo*	*Texto*	*Texto*
HCRTIPSER	**GESECODSE**	**HCRNOMSER**	**HCRCANTID**	**HCRDETREF**	**HCRFOLORI**	**HCRCONFIN**		
Texto	*Texto*	*Texto*	*Número*	*Memo*	*Número*	*Texto*		

25. HCCONSTAN: Se almacena información relacionada con constancias para pacientes emitidas por los médicos.

dbo_HCCONSTAN					
HCTCONCON	**GPACODIGO**	**GMECODIGO**	**HCTDESCRI**	**HCTFECCON**	**HCTDOCCER**
Texto	*Texto*	*Texto*	*Texto*	*Fecha/Hora*	*Número*

26. HCCPLANTI: Se almacena datos relacionados con las diferentes plantillas usadas para la configuración de historia clínica.

dbo_HCCPLANTI			
HCPCCODIGO	**HCPCNOMBRE**	**HCPCTIPO**	**GASCODIGO**
Texto	*Texto*	*Número*	*Texto*

27. HCCSOLMED: Se almacena la información sobre la cabecera de solicitud de suministros.

dbo_HCCSOLMED							
HCFECREG	**GASCODIGO**	**GPACODIGO**	**AINCONSEC**	**HCNUMSOL**	**GMECODIGO**	**HCESTADO**	**ISCNUMERO**
Fecha/Hora	*Texto*	*Texto*	*Texto*	*Número*	*Texto*	*Texto*	*Texto*

28. HCDATOSEV: En esta tabla se almacena la información relacionada con los datos de evolución del paciente, desde epicrisis como: consecutivo de epicrisis, fecha, descripción y número de ítems.

dbo_HCDATOSEV			
HCEPICRI	**HCFECHA**	**HCDESCRI**	**HCNUMITEM**
Texto	*Fecha/Hora*	*Memo*	*Número*

29. HCDCHARDES: Tablas de configuración de historia clínica

dbo_HCDCHARDES					
HCCTIPOHC	**HCCNCAMPO**	**HCSERNAME**	**DCPOINTID**	**DCPOINTARG**	**DCPOINTVAL**
Texto	*Texto*	*Texto*	*Número*	*Texto*	*Texto*

30. HCDIACRI: Se almacena la información relacionada con la contrareferencia de ingreso y el diagnostico del paciente.

dbo_HCDIACRI			
DIAGNOSI	**CONTRAREFI**	**OID**	**OptimisticLockField**
Texto	*Número*	*Autonumérico*	*Número*

31. HCDIACRS: Se almacena la información relacionada con la contrareferencia de salida y el diagnostico del paciente.

dbo_HCDIACRS			
DIAGNOSS	**CONTRAREFS**	**OID**	**OptimisticLockField**
Texto	*Número*	*Autonumérico*	*Número*

32. HCDIAPAC: Se almacena relacionada con el diagnostico el paciente.

Dbo_HCDIAPAC							
GPACODIGO	**AINCONSEC**	**HCCONFOLI**	**HCDCODIGO**	**HCDITEMDI**	**HCDTIPODI**	**HCDNUEVOI**	**HCDNUEVOP**
Texto	*Texto*	*Número*	*Texto*	*Número*	*Número*	*Número*	*Número*
HCDDIAPRI	**HCDCLASDI**	**HCDNUMUES**	**SITCODIGO**	**HCDOBSERV**	**HCLABORAT**	**HCINGRESO**	**HCEGRESO**
Número	*Número*	*Número*	*Texto*	*Texto*	*Texto*	*Número*	*Número*
HCNOTIFICA	**HCCLASEDI**						
Memo	*Texto*						

33. HCDIAREF: En esta tabla se relaciona la información perteneciente a los diagnósticos de referencia.

dbo_HCDIAREF			
DIAGNOSTICO	**REFERENCIA**	**OID**	**OptimisticLockField**
Texto	*Número*	*Autonumérico*	*Número*

34. HCDIEPAC: Tabla que relaciona la dieta del paciente en FOX.

dbo_HCDIEPAC						
GCRecord	**OID**	**GEPACIEN**	**HCCONFOLI**	**NUDIETAS**	**HCDRESTRIC**	**HCDOBSERV**
Número	*Autonumérico*	*Texto*	*Número*	*Texto*	*Memo*	*Memo*

35. HCDIETPA: Esta tabla relaciona la información sobre la solicitud de dietas de pacientes, para .net

dbo_HCDIETPA							
GPACODIGO	**AINCONSEC**	**HCCONFOLI**	**NUDCODIGO**	**HCDIOBSER**	**HCDIFECHA**	**HCDIPERIO**	**HCDIUNITI**
Texto	*Texto*	*Número*	*Texto*	*Texto*	*Fecha/Hora*	*Número*	*Número*

36. HCDINDSA: Esta tabla relaciona la información sobre detalle de la indicación de salida de pacientes.

dbo_HCDINDSA					
GPACODIGO	**AINCONSEC**	**HCCONFOLI**	**DETCONSEC**	**HCMCODMED**	**DETDOSISS**
Texto	*Texto*	*Número*	*Texto*	*Texto*	*Memo*

37. HCDOCAYU: En esta tabla se maneja la información perteneciente a la ayuda en línea para usuarios finales del módulo.

dbo_HCDOCAYU			
GCRecord	**OID**	**HCYNOMBRE**	**optimisticlockfield**
Número	*Autonumérico*	*Texto*	*Número*

38. HCDODONTO: En esta tabla se relaciona la información sobre los detalles de odontograma.

dbo_HCDODONTO					
GCRecord	**OID**	**HCCODONTO**	**ODOFECHA**	**HCTRATAMI**	**ODOOBSERV**
Número	*Autonumérico*	*Número*	*Fecha/Hora*	*Número*	*Memo*

39. HCENTIPOVACUNA: Esta tabla relaciona la información perteneciente a los tipos de vacunas para pacientes.

dbo_HCENTIPOVACUNA	
GCRecord	**OID**
Número	*Autonumérico*

40. HCENTPLA: Se almacena la información perteneciente a los estudios radiológicos para pacientes.

dbo_HCENTPLA							
GPACEDULA	**HCEFECDOC**	**SIPCODIGO1**	**SIPCODIGO2**	**SIPCODIGO3**	**HCPROCED1**	**HCPROCED2**	**HCPROCED3**
Texto	*Fecha/Hora*	*Texto*	*Texto*	*Texto*	*Texto*	*Texto*	*Texto*
HCEFECHA1	**HCEFECHA2**	**HCEFECHA3**	**HCEOBSER1**	**HCEOBSER2**			
Fecha/Hora	*Fecha/Hora*	*Fecha/Hora*	*Texto*	*Texto*			

41. HCEPICRI: Se maneja la información relacionada con epicrisis.

dbo_HCEPICRI							
HCECONSEC	**HCEFECDOC**	**GPACODIGO**	**AINCONSEC**	**ADEEGRSER**	**HCEFECEGR**	**HCEMOTSOL**	**HCEESTING**
Texto	*Fecha/Hora*	*Texto*	*Texto*	*Número*	*Fecha/Hora*	*Memo*	*Memo*
HCEENFACT	**HCEANTECE**	**HCEREVSIS**	**HCEEXAFIS**	**DIACODIIN**	**HCECONDUC**	**DIACODIR1**	**DIACODIR2**

Memo	*Memo*	*Memo*	*Memo*	*Texto*	*Memo*	*Texto*	*Texto*
DIACODIR3	**DIACODICO**	**HCERESPRO**	**HCEJUSTIF**	**DIACODIEG**	**HCECONSAL**	**HCEPLANMA**	**GMECODIGO**
Texto	*Texto*	*Memo*	*Memo*	*Texto*	*Memo*	*Memo*	*Texto*
HCEDOCCER	**DIACODIR4**	**HCEAPACHE**	**HCEESTADO**	**HCEHORASU**	**DIACODIEG1**	**DIACODIEG2**	**DIACODIEG3**
Texto	*Texto*	*Número*	*Texto*	*Número*	*Texto*	*Texto*	*Texto*
DIACODIEG4	**DIACODIEG5**	**DIACODIEG6**	**DIACODIEG7**	**HCDATOSEV**	**HCJUSMUE**	**HCEMEDICA**	**HCEEXAMEN**
Texto	*Texto*	*Texto*	*Texto*	*Memo*	*Memo*	*Memo*	*Memo*
EPIRESEXA	**EPIMEDADI**	**EPIEXAADI**	**GMEMEDMOD**	**GMEMEDCRE**			
Memo	*Memo*	*Memo*	*Texto*	*Texto*			

42. HCESPMEDN: En esta tabla se maneja los datos pertenecientes a las especialidades y los medicamentos para pacientes.

dbo_HCESPMEDN

ESPECIALI	MEDICAMENIPRCLAPRO	MEDICAMENIPRCODIGO	OID	OptimisticLockField	MEDICAMEN
Texto	*Texto*	*Texto*	*Autonumérico*	*Número*	*Texto*

43. HCESTAME: Se almacena los datos relacionados con el estado mental en la valoración neurológica de los pacientes.

dbo_HCESTAME

GPACODIGO	HCFFECREG	AINCONSEC	HCRALERTA	HCRSOMNOL	HCRESTUPO
Texto	*Texto*	*Texto*	*Texto*	*Texto*	*Texto*
HCRCOMA	**HCRESTAME**	**HCRORARE**	**GASCODIGO**		
Texto	*Texto*	*Texto*	*Texto*		

44. HCEVENTADV: Tabla que relacional los eventos adversos del paciente

dbo_HCEVENTADV

OID	EVTDESCRIP	GCRecord
Autonumérico	*Memo*	*Número*

45. HCEVENTADV: Tabla que relaciona los eventos adversos al examen físico.

dbo_HCEXAFISIC

HCFECREG	GASCODIGO	GPACODIGO	AINCONSEC	HCEXAMEN	HCHORAEXA	HCRESULT	USUCODIGO
Fecha/Hora	*Texto*	*Texto*	*Texto*	*Texto*	*Fecha/Hora*	*Texto*	*Texto*

46. HCEXAPAC: Se almacena los datos relacionados con los exámenes dados al paciente.

dbo_HCEXAPAC							
GPACODIGO	**AINCONSEC**	**HCCONFOLI**	**HCPCODIGO**	**HCPITEMPR**	**HCENUEVOE**	**HCECANTID**	**HCEDESCRI**
Texto	*Texto*	*Número*	*Texto*	*Texto*	*Texto*	*Número*	*Texto*
HCEOBSERV	**SOSORDSER**	**GASCODIGO**	**PRECODIGO**	**HCERESPUE**	**HCESTADO**	**HCFECSOL**	**HCEPROVIE**
Texto	*Texto*	*Texto*	*Texto*	*Número*	*Número*	*Fecha/Hora*	*Número*
HCECONSEC							
Texto							

47. HCEXPCON: Tabla de configuración de historia clínica, expresiones condicionadotas de campo.

dbo_HCEXPCON			
HCCTIPOHC	**HCXTARGET**	**HCXTRIGGE**	**HCXEXPRES**
Texto	*Texto*	*Texto*	*Texto*

48. HCFOLIOS: Se almacena registro de folios de historia clínica.

dbo_HCFOLIOS	
GPACODIGO	**HCCONFOLI**
Texto	*Número*

49. HCFORMED: Se almacena la formula medica del paciente

dbo_HCFORMED								
GPACODIGO	**AINCONSEC**	**HCCONFOLI**	**HCMCODMED**	**HCMNUEVOP**	**HCMCLAPRO**	**HCMCANTID**	**HCMDESCRI**	**HCMOBSERV**
Texto	*Texto*	*Número*	*Texto*	*Texto*	*Número*	*Número*	*Texto*	*Memo*
HCMEXISTE	**HCMTIPORD**	**ISCNUMERO**	**GASCODIGO**	**PRECODIGO**	**HCMRESPUE**	**CCCCODCEN**	**HCMTIPO**	**HCMFECPRE**
Número	*Número*	*Texto*	*Texto*	*Texto*	*Número*	*Texto*	*Número*	*Fecha/Hora*
IALCODIGO	**HCDOSIS**	**HCFRECUEN**	**HCTIEMTRA**	**HCVIADMIS**				
Texto	*Texto*	*Texto*	*Texto*	*Número*				

50. HCFORMULA: Se almacena formulación de paciente.

dbo_HCFORMULA				
HCCTIPOHC	**HCCNUAREA**	**HCFCODIGO**	**HCFNOMBRE**	**HCFDETALLE**
Texto	*Número*	*Texto*	*Texto*	*Texto*

51. HCFUNCIO: Se almacena registro de funcionarios de enfermería.

dbo_HCFUNCIO			
FUNCODIGO	**FUNNOMBRE**	**FUNTELEFO**	**HCCODIGO**
Texto	*Texto*	*Texto*	*Texto*

52. HCGENERI: Se almacena registro de medicamentos genéricos.

dbo_HCGENERI	
HCGCODGEN	**HCGNOMGEN**
Texto	*Texto*

53. HCGLUCOM: Se almacena el registro de glucometrías.

dbo_HCGLUCOM							
HCFECREG	**GASCODIGO**	**GPACODIGO**	**AINCONSEC**	**HCHORREG**	**HCHORGLUC**	**HCRESGLUC**	**HCCANGLUC**
Fecha/Hora	*Texto*	*Texto*	*Texto*	*Fecha/Hora*	*Fecha/Hora*	*Número*	*Número*
HCINSULINA	**HCINSUUNI**	**HCINSUTIP**	**HCVIAINGE**	**HCOBSERV**	**HCRESPON**	**USUCODIGO**	
Texto	*Número*	*Texto*	*Texto*	*Texto*	*Texto*	*Texto*	

54. HCGRAFICO: Tabla de configuración de gráficos.

dbo_HCGRAFICO
GRAFICA
Objeto OLE

55. HCGRAFICOP: Tabla de configuración de gráficos.

dbo_HCGRAFICOP
GRAFICA
Objeto OLE

56. HCGRAFICOXY: Tabla de configuración de gráficos.

dbo_HCGRAFICOXY
GRAFICA
Objeto OLE

57. HCGUIEXA: Tabla de registro de guía de exámenes.

dbo_HCGUIEXA						
DIACODIGO	**EXACODIGO**	**HCGITEMPR**	**HCGCANTID**	**HCGDESCRI**	**HCGOBSERV**	**GASCODIGO**
Texto	*Texto*	*Número*	*Número*	*Texto*	*Texto*	*Texto*

58. HCGUIPNQ: Guía de procedimientos no quirúrgicos.

dbo_HCGUIPNQ						
DIACODIGO	**HCGCODIGO**	**HCGDESCRI**	**HCGITEMPR**	**HCGCANTID**	**HCGOBSERV**	**GASCODIGO**
Texto	*Texto*	*Texto*	*Número*	*Número*	*Texto*	*Texto*

59. HCGUIPQX: Guía de procedimientos quirúrgicos.

dbo_HCGUIPQX						
DIACODIGO	**HCGCODIGO**	**HCGITEMPR**	**HCGDESCRI**	**HCGCANTID**	**HCGOBSERV**	**GASCODIGO**
Texto	*Texto*	*Número*	*Texto*	*Número*	*Memo*	*Texto*

60. HCGUISUM: Guía de suministro a pacientes.

dbo_HCGUISUM						
DIACODIGO	**HCGCODMED**	**HCGCANTID**	**HCGDESCRI**	**HCGOBSERV**	**GASCODIGO**	**HCGTIPOS**
Texto	*Texto*	*Número*	*Texto*	*Texto*	*Texto*	*Número*
HCGTIPORD	**HCGFECPRE**	**HCGVIAAPL**	**CCCCODCEN**	**HCGTERMIN**	**HCGFECTER**	**IALCODIGO**

Número	*Fecha/Hora*	*Texto*	*Texto*	*Texto*	*Fecha/Hora*	*Texto*

61. HCHCHARDES: Tabla de configuración de historia clínica.

dbo_HCHCHARDES

HCCTIPOHC	HCCNCAMPO	HCSERNAME	HCSERTITLE	HCSERTYPEA	HCSERTYPEV	HCSERTYPE
Texto	*Texto*	*Texto*	*Texto*	*Número*	*Número*	*Número*

62. HCHISUSU: Tabla de gestión de historias de usuarios.

dbo_HCHISUSU

GCRecord	OID	HCTIPHIS	USUCODIGO	OptimisticLockField
Número	*Autonumérico*	*Texto*	*Texto*	*Número*

63. HCHORTUR: Tabla de gestión de horarios de turnos.

dbo_HCHORTUR

HHTINIMAN	HHTFINMAN	HHTINITAR	HHTFINTAR	HHTININOC	HHTFINNOC
Fecha/Hora	*Fecha/Hora*	*Fecha/Hora*	*Fecha/Hora*	*Fecha/Hora*	*Fecha/Hora*

64. HCIMADIA: Tabla donde se almacena información de imágenes diagnosticas.

dbo_HCIMADIA

GPACODIGO	AINCONSEC	HCCONFOLI	HCIFECHAT	HCIESTADO	SIPCODIGO	HCITIPEXA	HCIFECHAE	HCINOMRES
Texto	*Texto*	*Número*	*Fecha/Hora*	*Texto*	*Texto*	*Número*	*Fecha/Hora*	*Texto*
HCIDESRES	**HCIANALIS**	**HCIIMAGE1**	**HCIIMAGE2**	**HCIIMAGE3**	**GMECODIGO**	**HCCONTROL**		
Texto	*Texto*	*Texto*	*Texto*	*Texto*	*Texto*	*Texto*		

65. HCIMGSDIS: Tabla donde se almacena imágenes asociadas a diseños de historias clínicas.

dbo_HCIMGSDIS

HCCTIPOHC	HCCNCAMPO	HCINUMIMG	HCITITULO	HCICOMENT	HCIFECCRE	HCIRUTA
Texto	*Texto*	*Número*	*Memo*	*Memo*	*Fecha/Hora*	*Memo*

66. HCIMGSHCS: Tabla donde se almacena imágenes de historias clínicas.

dbo_HCIMGSHCS					
GPACODIGO	**AINCONSEC**	**HCCTIPOHC**	**HCCONFOLI**	**GMECODIGO**	**HMFECHARE**
Texto	*Texto*	*Texto*	*Número*	*Texto*	*Fecha/Hora*
HCCNCAMPO	**HCINUMIMG**	**HCITITULO**	**HCICOMENT**	**HCIRUTA**	
Texto	*Número*	*Memo*	*Memo*	*Memo*	

67. HCINCAPA: Se almacena la información de las incapacidades de pacientes.

dbo_HCINCAPA							
HCNCONINC	**GPACODIGO**	**HCNFECINI**	**HCNDIAINC**	**HCNFECFIN**	**HCNDESCRI**	**GMECODIGO**	**HCNDOCCER**
Texto	*Texto*	*Fecha/Hora*	*Número*	*Fecha/Hora*	*Texto*	*Texto*	*Número*
AINCONSEC	**HCCONFOLI**	**HCNFECDOC**	**HCNCAUINC**	**DIACODIGO**	**HCNTIPO**	**HCNGRADO**	**HCABSRLT**
Texto	*Número*	*Fecha/Hora*	*Número*	*Texto*	*Número*	*Número*	*Número*
HCGRDINC	**HCTIPPROC**	**HCTIPINCA**	**HCDIASPRO**	**HCFECACT**	**HCMOTIVO**	**GESEDEDUCA**	
Número	*Número*	*Número*	*Número*	*Fecha/Hora*	*Número*	*Número*	

68. HCINDMEDIC: Se almacena las indicaciones médicas.

dbo_HCINDMEDIC			
GPACODIGO	**AINCONSEC**	**HCCONFOLI**	**HCINDMEDIC**
Texto	*Texto*	*Número*	*Memo*
HCINDTIPO	**HCISUSMED**		
Texto	*Memo*		

69. HCINDSAL: Se almacena las indicaciones de salida de paciente.

dbo_HCINDSAL							
GPACODIGO	**AINCONSEC**	**HCCONFOLI**	**GASCODIGO**	**INDFECHAS**	**ENTCODIGO**	**INDDIETAS**	**INDACTFIS**
Texto	*Texto*	*Número*	*Texto*	*Fecha/Hora*	*Texto*	*Memo*	*Memo*
DIACODIGO	**INDRECOME**	**INDPEDICI**	**INDCITCON**	**GMECODIGO**	**INDSITIOS**	**INDENTIMA**	
Texto	*Memo*	*Número*	*Texto*	*Texto*	*Memo*	*Texto*	

70. HCINGRES: Se almacena la información de ingreso de paciente de historia clínica.

dbo_HCINGRES							
GPACODIGO	**HCICONSEC**	**HCCTIPOHC**	**HCCONFOLI**	**HCIFECING**	**HCIVIAING**	**HCIFECNAM**	**HCIPESOKG**
Texto	*Texto*	*Texto*	*Número*	*Fecha/Hora*	*Texto*	*Fecha/Hora*	*Número*
HCIDOCCER	**HCIFINCON**	**HCICAUEXT**	**HCIFECATE**	**GMECODIGO**	**HCOCODIGO**	**HCIPROCDE**	**HCIPESOGR**
Número	*Número*	*Número*	*Fecha/Hora*	*Texto*	*Texto*	*Texto*	*Número*
HCICORFOL	**HCIFOLASO**	**HCDIAGPA**	**HCUDIAGPA**	**GASCODIGO**	**HCIREEXME**	**HCIREPREM**	
Texto	*Número*	*Texto*	*Número*	*Texto*	*Número*	*Número*	

71. HCINTERC: Tabla que guarda la información de interconsultas de pacientes.

dbo_HCINTERC								
HCUCONSEC	**HCUFECDOC**	**GPACODIGO**	**AINCONSEC**	**HCCONFOLI**	**GMECODIGO**	**DIACODIGO**	**HCUTIPDIA**	
Texto	*Texto*	*Texto*	*Texto*	*Número*	*Texto*	*Texto*	*Número*	
GASCODIGO	**HCUMOTIVO**	**HCUOBSERV**	**SOSORDSER**	**GASCODIGO1**	**HCRESESP**	**GMECODMED**	**DIAGRESP**	**SIPCODIGO**
Texto	*Memo*	*Memo*	*Texto*	*Texto*	*Memo*	*Texto*	*Texto*	*Texto*

72. HCINTERR: Tabla que almacena las respuestas a solicitud de interconsultas.

dbo_HCINTERR							
HCRCONSEC	**HCRFECDOC**	**GPACODIGO**	**AINCONSEC**	**HCCONFOLI**	**GMECODIGO**	**DIACODIGO**	**GASCODIGO**
Texto	*Fecha/Hora*	*Texto*	*Texto*	*Número*	*Texto*	*Texto*	*Texto*
HCROBSERV	**HCUCONSEC**	**HCUAINCON**	**HCUHCCONF**	**HCUANAOBJ**	**HCUANASUB**	**HCUPLASEG**	
Memo	*Texto*	*Texto*	*Número*	*Memo*	*Memo*	*Memo*	

73. HCINTLAB: Se almacena los datos de muestras a laboratorios.

dbo_HCINTLAB								
GPACODIGO	**AINCONSEC**	**HCCONFOLI**	**HCGCODIGO**	**HCGITEMPR**	**SIPCODIGO**	**HCDCODI11**	**HCDCODI12**	**HCDCODI13**
Texto	*Texto*	*Número*	*Texto*	*Número*	*Texto*	*Texto*	*Texto*	*Texto*
HCDCODI21	**HCDCODI22**	**HCDCODI23**	**HCDCODI31**	**HCDCODI32**	**HCDCODI33**	**HCDCODI41**	**HCDCODI42**	**HCDCODI43**
Texto	*Texto*	*Texto*	*Texto*	*Texto*	*Texto*	*Texto*	*Texto*	*Texto*
HCDCODI51	**HCDCODI52**	**HCDCODI53**	**HCIDESEXA**	**GMECODIGO**	**SITCODIG1**	**SITCODIG2**	**SITCODIG3**	**SITCODIG4**
Texto	*Texto*	*Texto*	*Memo*	*Memo*	*Memo*	*Memo*	*Memo*	*Memo*

SITCODIG5								
Memo								

74. HCINYACC: Se almacena la información e los registro de eventos adversos, incidentes y accidentes.

dbo_HCINYACC

GCRecord	OID	IYAFECDOC	IYAESTDOC	GPACODIGO	AINCONSEC	IYAINFINI	IYAAUXENF
Número	*Autonumérico*	*Fecha/Hora*	*Número*	*Texto*	*Texto*	*Memo*	*Texto*
IYATIIADM	**IYATIICUI**	**IYATIIAME**	**IYATIISNE**	**IYATIIPAR**	**IYATIISAN**	**IYATIIOTR**	**IYATIIOTD**
Texto	*Texto*	*Texto*	*Texto*	*Texto*	*Texto*	*Texto*	*Memo*
IYACAUSAS	**IYAAPOVAL**	**IYAAPODES**	**IYAVMEVAL**	**GMECODIGO**	**IYAVMEDIA**	**IYAVMETRA**	**IYAVMEREN**
Memo	*Texto*	*Memo*	*Texto*	*Texto*	*Memo*	*Memo*	*Texto*
IYAVMENEN	**IYAMCONET**	**IYAMCONEN**	**IYAMCOOBJ**	**IYAMCORES**	**IYAMCOPRO**	**IYASEGDES**	**IYASEGRES**
Texto	*Texto*	*Texto*	*Memo*	*Memo*	*Memo*	*Memo*	*Texto*
IYASEGPEN	**IYAFECCRE**	**IYAUSUCRE**	**IYAFECCON**	**IYAUSUCON**	**IYAFECANU**	**IYAUSUANU**	**GradoSeveridad**
Texto	*Fecha/Hora*	*Texto*	*Fecha/Hora*	*Texto*	*Fecha/Hora*	*Texto*	*Número*

75. HCIODONTO: tabla que relaciona los ítems odontológicos.

dbo_HCIODONTO

GCRecord	OID	HCCODONTO	ODDIENTE	ODTAAMALGA	ODTARESINA	ODTACONDUC
Número	*Autonumérico*	*Número*	*Número*	*Sí/No*	*Sí/No*	*Sí/No*
ODTACORONA	**ODTAINCRUS**	**ODTAPULPOT**	**ODTASELLAN**	**ODTAPUENTE**	**ODEDGIROVE**	**ODEDRETENI**
Sí/No	*Sí/No*	*Sí/No*	*Sí/No*	*Sí/No*	*Sí/No*	*Sí/No*
ODEDCARIE	**ODEDSURPRO**	**ODEDFRACTU**	**ODEDAUSENT**	**ODEDMOVDEN**	**ODEDSUPNUM**	**ODEDAGENEC**
Número	*Sí/No*	*Sí/No*	*Sí/No*	*Sí/No*	*Sí/No*	*Sí/No*
ODOBSERVA	**OptimisticLockField**	**ODDEFINIT**	**DOTAPUENTE**			
Memo	*Número*	*Sí/No*	*Sí/No*			

76. HCISOFAR: Se almacena la información de isótopos y fármacos.

dbo_HCISOFAR

HCICODELE	HCITIPELE	HCINOMELE	HCIVALOR
Texto	*Número*	*Texto*	*Número*

77. HCIYAEVTS: tabla complemento de eventos adversos.

dbo_HCIYAEVTS			
EventosAdversos	**InsidentesAccidentes**	**OID**	**OptimisticLockField**
Número	*Número*	*Autonumérico*	*Número*

78. HCJUNMED: Se almacena el registro de Junta Medica.

dbo_HCJUNMED						
HCOCONSEC	**HCOFECDOC**	**GPACODIGO**	**HCOPESOKG**	**HCOTALLAP**	**AINCONSEC**	**HCCONFOLI**
Texto	*Fecha/Hora*	*Texto*	*Número*	*Número*	*Texto*	*Número*
HCOMOTIVO	**HCOCIRCUN**	**HCOSINTOM**	**HCOTRATAM**	**HCOESTACT**	**HCOETIOLO**	
Número	*Texto*	*Texto*	*Texto*	*Texto*	*Texto*	

79. HCLACPAC: Se almacena la información de laboratorios de pacientes.

dbo_HCLACPAC					
GCRecord	**OID**	**LACFECHAL**	**GPACODIGO**	**AINCONSEC**	**HCCONFOLI**
Número	*Autonumérico*	*Fecha/Hora*	*Texto*	*Texto*	*Número*

80. HCLECEXAM: Se almacena la información de lectura de exámenes.

dbo_HCLECEXAM				
HCCONFOLI	**AINCONSEC**	**HCPCODIGO**	**GEMEDICO**	**HCFECHALEC**
Número	*Texto*	*Texto*	*Texto*	*Fecha/Hora*

81. HCLIQADM: Se almacena líquidos administrados al paciente.

dbo_HCLIQADM					
HCFECREG	**GASCODIGO**	**GPACODIGO**	**AINCONSEC**	**HCHORREG**	**HCVIALIQ**
Fecha/Hora	*Texto*	*Texto*	*Texto*	*Fecha/Hora*	*Texto*
HCLIQUIA	**HCCANTID**	**HCHORAINI**	**HCHORAFIN**	**USUCODIGO**	
Texto	*Número*	*Fecha/Hora*	*Fecha/Hora*	*Texto*	

82. HCLIQELIM: Se almacena los líquidos eliminados del paciente.

dbo_HCLIQELIM					
HCFECREG	**GASCODIGO**	**GPACODIGO**	**AINCONSEC**	**HCHORREG**	**HCVIAELIM**
Fecha/Hora	*Texto*	*Texto*	*Texto*	*Fecha/Hora*	*Texto*
HCCODLIQ	**HCCANTID**	**HCHORAELM**	**HCCOMENT**	**USUCODIGO**	
Texto	*Número*	*Fecha/Hora*	*Memo*	*Texto*	

83. HCLIQUIA: Se almacena la información líquidos administrados en fox.

dbo_HCLIQUIA							
GPACODIGO	**HCFFECREG**	**HCFHORARE**	**AINCONSEC**	**HCLLIQUI1**	**HCLLIQUI2**	**HCLLIQUI3**	**HCLLIQUI4**
Texto	*Texto*	*Texto*	*Texto*	*Número*	*Número*	*Número*	*Número*
HCLLIQUI5	**HCLLIQUI6**	**HCLSNG**	**HCLVO**	**HCLTIPO**	**HCHORAFIN**	**GASCODIGO**	
Número	*Número*	*Número*	*Número*	*Número*	*Texto*	*Texto*	

84. HCLIQUID: Se almacena la información de registro de líquidos.

dbo_HCLIQUID		
HCLCODIGO	**HCLNOMBRE**	**HCLDESCRI**
Texto	*Texto*	*Texto*

85. HCLIQUIE: Se almacena la información de líquidos eliminados en fox.

dbo_HCLIQUIE							
GPACODIGO	**HCFFECREG**	**HCFHORARE**	**AINCONSEC**	**HCLDIUR**	**HCLSNG**	**HCLTT**	**HCLDEP**
Texto	*Texto*	*Número*	*Texto*	*Número*	*Número*	*Número*	*Número*
HCLDREN	**HCLVOMITO**	**HCLOTRO**	**HCLTUBMED**	**HCHORAFIN**	**GASCODIGO**		
Número	*Número*	*Número*	*Número*	*Número*	*Texto*		

86. HCMANAYU: Se almacena la información sobre la configuración para archivos de ayuda.

dbo_HCMANAYU			
HCYCODIGO	**HCYNOMBRE**	**HCYRUTARC**	**HCYFORMAT**
Texto	*Texto*	*Texto*	*Número*

87. HCMARCAPA: Se almacena la información de marcapasos del paciente.

dbo_HCMARCAPA									
HCFECREG	**GASCODIGO**	**GPACODIGO**	**AINCONSEC**	**HCHORREG**	**HCVIA**	**HCFRECUEN**	**HCSENSIV**	**HCSALIDA**	**HCFECBAT**
Fecha/Hora	*Texto*	*Texto*	*Texto*	*Fecha/Hora*	*Texto*	*Texto*	*Texto*	*Texto*	*Fecha/Hora*

88. HCMAUTPRO: Tabla que almacena los movimientos de autorización de procedimientos.

dbo_HCMAUTPRO					
HCUCONSEC	**HCFECDOC**	**HCNOMESPEC**	**HCNOMPAC**	**HCNUMHCLIN**	**HCCEDPAC**
Texto	*Fecha/Hora*	*Texto*	*Texto*	*Texto*	*Texto*
HCTIPAUTOR	**HCNOMAUT**	**HCDIAGNOS**	**HCTIPPROC**	**HCPROCED**	**HCASPPROC**
Texto	*Texto*	*Memo*	*Texto*	*Memo*	*Memo*
HCRIESPROC	**HCTIPANEST**	**HCTIEMQX**	**HCTIPPRE**	**HCREQESP**	
Memo	*Texto*	*Memo*	*Memo*	*Memo*	

89. HCMDEVMED: Se almacena la información de movimientos de devolución de medicamentos.

dbo_HCMDEVMED				
HCFECREG	**GASCODIGO**	**GPACODIGO**	**AINCONSEC**	**HCNUMDEV**
Fecha/Hora	*Texto*	*Texto*	*Texto*	*Número*
HCNUMITEM	**IPRCODIGO**	**HCCANTID**	**ISCNUMER1**	**HCMOTIVO**
Número	*Texto*	*Número*	*Texto*	*Texto*

90. HCMEDADM: Se almacena la información de medicamentos administrados.

dbo_HCMEDADM						
GPACODIGO	**HCFFECREG**	**AINCONSEC**	**HCNOMBRE**	**HCDOSISS**	**HCVIASUM**	**HCFHORAS**
Texto	*Fecha/Hora*	*Texto*	*Texto*	*Texto*	*Texto*	*Número*

91. HCMEDESP: Contiene la información de medicamentos por especialidad.

dbo_HCMEDESP	
GEECODIGO	**IPRCODIGO**
Texto	*Texto*

92. HCMEDICA: Se almacena la información de medicamentos fox.

dbo_HCMEDICA						
HCMCODMED	**HCMNOMMED**	**HCMCLAPRO**	**HCMPRESEN**	**HCMVADEME**	**HCMMEDPOS**	**HCMPOSSUB**
Texto	*Texto*	*Número*	*Texto*	*Número*	*Número*	*Número*
HCGCODGEN	**HCMINDICA**	**HCMCONTRA**	**HCMDOCIFI**	**HCMINTERA**	**HCMEFESEC**	
Texto	*Texto*	*Texto*	*Texto*	*Texto*	*Texto*	

93. HCMEDPAC: Se almacena la información de registro de medicamentos de productos para paciente.

dbo_HCMEDPAC							
GPACODIGO	**AINCONSEC**	**HCCONFOLI**	**HCMCODMED**	**HCMNUEVOP**	**HCMCLAPRO**	**HCMCANTID**	**HCMDESCRI**
Texto	*Texto*	*Número*	*Texto*	*Texto*	*Número*	*Número*	*Texto*
HCMOBSERV	**HCMEXISTE**	**HCMTIPORD**	**ISCNUMERO**	**GASCODIGO**	**PRECODIGO**	**HCMRESPUE**	**CCCCODCEN**
Nemo	*Número*	*Número*	*Texto*	*Texto*	*Texto*	*Número*	*Texto*
HCMTIPO	**HCMFECPRE**	**IALCODIGO**	**HCCTIPOHC**	**HCMVIAAPL**	**GMECODIGO**	**HCMESTADO**	**HCMFECSUS**
Número	*Fecha/Hora*	*Texto*	*Texto*	*Texto*	*Texto*	*Texto*	*Fecha/Hora*
GMECODSUS	**HCMTERMIN**	**HCMFECTER**	**HCMCANRES**	**HCMPROVIE**	**HCMCANDIA**	**HCMCONSEC**	**HCINVENTA**
Texto	*Texto*	*Fecha/Hora*	*Número*	*Número*	*Número*	*Texto*	*Número*

94. HCMEDSUM: Se almacena la información de medicamentos suministrados.

dbo_HCMEDSUM						
GPACODIGO	**AINCONSEC**	**HCMFECREG**	**GMECODIGO**	**HCMNOMMED**	**HCMFECINI**	**HCMFECFIN**
Texto	*Texto*	*Fecha/Hora*	*Texto*	*Texto*	*Fecha/Hora*	*v*
HCMFRECUE	**HCMDOSIS**	**HCMVIAMED**	**HCMHORA1**	**HCMNOMBR1**	**HCMHORA2**	**HCMNOMBR2**
Texto	*Texto*	*Texto*	*Texto*	*Texto*	*Texto*	*Texto*
HCMHORA3	**HCMNOMBR3**	**HCMHORA4**	**HCMNOMBR4**	**HCMHORA5**	**HCMNOMBR5**	**HCMHORA6**
Texto	*Texto*	*Texto*	*Texto*	*Texto*	*Texto*	*Texto*
HCMNOMBR6						
Texto						

95. HCMNOPOS: Se almacena la información de medicamentos no pos.

dbo_HCMNOPOS						
HCMNFECHA	**GPACEDULA**	**GPACODIGO**	**AINCONSEC**	**HCMCODIGO**	**HCMDURACI**	**HCMMEDHOM**
Fecha/Hora	*Texto*	*Texto*	*Texto*	*Texto*	*Texto*	*Texto*
HCMBIBLIO	**HCMMEDICO**	**HCMNFOLIO**	**HCJUSTIFM**	**HCMNUEVOP**	**HCMDOSISD**	**HCMHCN**
Texto	*Texto*	*Número*	*Memo*	*Texto*	*Texto*	*Texto*
HCMCAMA	**HCMDIAGPR**	**HCMEFADME**	**HCMMEAPPA**	**HCMGARANT**		
Texto	*Memo*	*Memo*	*Memo*	*Texto*		

96. HCMONRENAL: Se almacena la información de medicamento renal.

dbo_HCMONRENAL					
HCFECREG	**GASCODIGO**	**GPACODIGO**	**AINCONSEC**	**HCHORREG**	**HCHORRENAL**
Fecha/Hora	*Texto*	*Texto*	*Texto*	*Fecha/Hora*	*Fecha/Hora*
HCFLUJO	**HCPRESIONV**	**HCPRESIONART**	**HCPTM**	**HCOBSERV**	**USUCODIGO**
Número	*Número*	*Número*	*Fecha/Hora*	*Texto*	*Texto*

97. HCMOVINT: Se almacena la información de movimientos de la interconsulta.

dbo_HCMOVINT						
HCUCONSEC	**SIPCODIGO**	**HCMICANTI**	**HCMINUMIT**	**GPACODIGO**	**AINCONSEC**	**HCCONFOLI**
Texto	*Texto*	*Número*	*Texto*	*Texto*	*Texto*	*Número*

98. HCMOVIRE: Se almacena la información de movimientos de referencia y contrareferencia.

dbo_HCMOVIRE					
HCRCONSEC	**HCMTIPSER**	**GESECODSE**	**HCMCANTID**	**HCMDETREF**	**HCMDETCON**
Texto	*Número*	*Texto*	*Número*	*Memo*	*Memo*
HCMNUMITE	**HCMNOMSER**	**GPACODIGO**	**AINCONSEC**	**HCCONFOLI**	**HCRTIPDOC**
Texto	*Texto*	*Texto*	*Texto*	*Número*	*Número*

99. HCMPLANTI: Se almacena la información de movimientos de plantillas.

dbo_HCMPLANTI					
HCPCCODIGO	**HCPMCODIGO**	**HCPMCANTID**	**HCPMOBSERV**	**HCPMTIPO**	**HCPMPRIN**
Texto	*Texto*	*Número*	*Memo*	*Número*	*Número*
HCPMINST	**HCPMPROG**	**HCPMCLASE**	**HCPMITEMID**		
Número	*Número*	*Número*	*Número*		

100. HCMSOLMED: Se almacena la información de movimientos de solicitud médica.

dbo_HCMSOLMED								
HCFECREG	**GASCODIGO**	**GPACODIGO**	**AINCONSEC**	**HCNUMSOL**	**HCNUMITEM**	**IPRCODIGO**	**HCCANTID**	**GASCODSUM**
Fecha/Hora	*Texto*	*Texto*	*Texto*	*Número*	*Número*	*Texto*	*Número*	*Texto*

101. HCNOTASE: Se almacena notas enfermería

dbo_HCNOTASE								
GPACODIGO	**HCFFECREG**	**HCFHORARE**	**AINCONSEC**	**HCRITEMSE**	**HCROBSERV**	**HCRENFERM**	**HCRESTPIE**	**GASCODIGO**
Texto	*Texto*	*Número*	*Texto*	*Número*	*Texto*	*Texto*	*Texto*	*Texto*

102. HCNOTASENF: Se almacena la información de notas de enfermería.

dbo_HCNOTASENF					
HCFECREG	**GASCODIGO**	**GPACODIGO**	**AINCONSEC**	**HCHORREG**	**HCREGISTRA**
Fecha/Hora	*Texto*	*Texto*	*Texto*	*Fecha/Hora*	*Texto*
HCTITULO	**HCSUBOBJ**	**HCANAPLAN**	**HCIMPORT**	**USUCODIGO**	
Texto	*Texto*	*Texto*	*Número*	*Texto*	

103. HCNUCLEA: Se almacena la información de medicina nuclear.

dbo_HCNUCLEA							
HCUNUMERO	**GPACODIGO**	**HCCONFOLI**	**AINCONSEC**	**AINFECING**	**SIPCODIGO**	**HCUTIPEST**	**HCUURGENT**
Texto	*Texto*	*Número*	*Texto*	*Fecha/Hora*	*Texto*	*Número*	*Número*
HCUISOTOP	**HCUDOSIS**	**HCUFARMAC**	**HCUFECHAR**	**GMECODIGO**	**HCUFECHAE**	**HCUNOMRES**	**HCUDATCLI**
Texto	*Texto*	*Texto*	*Fecha/Hora*	*Texto*	*Fecha/Hora*	*Texto*	*Texto*
HCUPROCED	**HCURESULT**	**HCUINTERP**	**HCUFECINY**	**HCUPORCIO**	**HCUFABISO**	**HCULOTISO**	**HCUACTISO**
Texto	*Texto*	*Texto*	*Fecha/Hora*	*Número*	*Texto*	*Texto*	*Número*

HCUVOLISO	HCUFABKIT	HCULOTKIT	HCUTIPKIT	HCUVOLKIT	HCUFABSAL	HCULOTSAL	HCUPCVSAL
Número	*Texto*	*Texto*	*Texto*	*Número*	*Texto*	*Texto*	*Texto*
HCUVOLTOT	**HCUPORM**	**HCUPORPRQ**	**HCUPREPAR**	**HCUCONTRO**	**GMECODIG1**	**HCUIMAGE1**	**HCUIMAGE2**
Número	*Número*	*Número*	*Texto*	*Texto*	*Texto*	*Texto*	*Texto*
HCUIMAGE3	**HCUESTADO**	**GEECODIGO**	**DIACODIGO**	**DIACODIG2**	**HCUTIPDIA**	**HCUCAMARA**	**GMECODIG2**
Texto	*Texto*	*Texto*	*Texto*	*Texto*	*Número*	*Número*	*Texto*
GASCODIGO	**HCUCONCOR**	**HCPCODIPR**	**HCUDIAING**	**HCUDIANUC**	**HCUISOCAN**	**HCUFARCAN**	**HCIVALOR1**
Texto	*Número*	*Texto*	*Texto*	*Texto*	*Número*	*Número*	*Número*
HCIVALOR2	**GMECODIG3**	**HCNORIGEN**	**HCNRUTA1**	**HCNRUTA2**	**HCNRUTA3**	**HCNNUMINT**	**HCIVALOR3**
Número	*Texto*	*Número*	*Texto*	*Texto*	*Texto*	*Texto*	*Número*
HCIVALOR4	**HCUOTFARCAN**	**HCUEQVCAN**	**HCUOTFAR**	**HCUEQVEN**	**HCUOTFARCA**		
Número	*Número*	*Número*	*Texto*	*Texto*	*Número*		

104. HCOCUPAC: Se almacena la información de ocupaciones Homologadas.

dbo_HCOCUPAC

HCOCODIGO	HCONOMBRE	HCODGCODI
Texto	*Texto*	*Texto*

105. HCORDENC: Tabla de configuración de gráficos y ordenamiento de campos.

dbo_HCORDENC

HCCTIPOHC	HCCNCAMPO	HCNUMCAM	HCCTIPCAM	HCCNUAREA
Texto	*Texto*	*Número*	*Número*	*Número*

106. HCORDHOS: Se almacena la información de orden de hospitalización.

dbo_HCORDHOS

HOHNUMERO	HOHFECORD	GMECODIGO	GPACODIGO	HOHFECHOS	HOHMOTIVO	HOHOBSERV
Texto	*Fecha/Hora*	*Texto*	*Texto*	*Fecha/Hora*	*Texto*	*Texto*
HOHESTADO	**PRECODIGO**	**DIACODIGO**	**GASCODIG1**	**GASCODIG2**	**HOHDETANU**	**HOHUSUANU**
Texto	*Texto*	*Texto*	*Texto*	*Texto*	*Texto*	*Texto*

107. HCPAGHIS: Se almacena la información de paginación de historias.

dbo_HCPAGHIS		
HCCTIPOHC	**HCPNUMERA**	**HCPTITARE**
Texto	*Número*	*Nemo*

108. HCPARAME: Se almacena la información de parámetros de historias clínicas.

dbo_HCPARAME							
HCPINVF26	**HCPNAPROD**	**HCPNAINAL**	**HCPPACF26**	**HCPSALUPA**	**HCPMANCON**	**HCPHABMEN**	**HCPCOMEN1**
Número	*Texto*	*Texto*	*Número*	*Texto*	*Número*	*Número*	*Memo*
HCPCOMEN2	**HCPORSAUT**	**HCPSUMAUT**	**GASCODIGO**	**IALCODIGO**	**HCPMANGRA**	**HCPRUTGRA**	**HCPTIPGRA**
Memo	*Número*	*Número*	*Texto*	*Texto*	*Número*	*Texto*	*Número*
HCPREGEXI	**HCPBUSFAC**	**GECCODIGO**	**PLACODIGO**	**HCPCAMMED**	**HCPCONMEDNUC**	**HCPTA1**	**HCPTA2**
Número	*Número*	*Texto*	*Texto*	*Número*	*Número*	*Número*	*Número*
HCPFRECA1	**HCPFRECA2**	**HCPFRERE1**	**HCPFRERE2**	**HCPPVC1**	**HCPPVC2**	**HCPSAT1**	**HCPSAT2**
Número	*Número*	*Número*	*Número*	*Número*	*Número*	*Número*	*Número*
HCPPULD1	**HCPPULD2**	**HCPPULI1**	**HCPPULI2**	**HCPPAM1**	**HCPPAM2**	**HCPCUNA1**	**HCPCUNA2**
Número	*Número*	*Número*	*Número*	*Número*	*Número*	*Número*	*Número*
HCPPPS1	**HCPPPS2**	**HCPPPM1**	**HCPPPM2**	**HCPPPD1**	**HCPPPD2**	**HCPGC1**	**HCPGC2**
Número	*Número*	*Número*	*Número*	*Número*	*Número*	*Número*	*Número*
HCPIC1	**HCPIC2**	**HCPIRVS1**	**HCPIRVS2**	**HCPIRVP1**	**HCPIRVP2**	**HCPITVI1**	**HCPITVI2**
Número	*Número*	*Número*	*Número*	*Número*	*Número*	*Número*	*Número*
HCPITVD1	**HCPITVD2**	**HCPTEMPE1**	**HCPTEMPE2**	**SIPCODIGO**	**HCTIPBUS**	**HCANTEPI**	**HCPIMPCON**
Número	*Número*	*Número*	*Número*	*Texto*	*Número*	*Número*	*Número*
HCHORAMIL	**HCPPROCUB**	**OID**	**HCPCIERRE1**	**HCPCIERRE2**	**HCPCIERRE3**	**HCPCIERRE4**	**HCPDIASCIE**
Texto	*Número*	*Autonumérico*	*Sí/No*	*Sí/No*	*Sí/No*	*Sí/No*	*Número*
GCRecord							
Número							

109. HCPARTICI: Se almacena la información de participantes.

dbo_HCPARTICI							
HCCEDULA	**HCNOMBRES**	**HCENTIDAD**	**HCTELEFON**	**HCDIRECCI**	**HCUBICACI**	**HCCODIGO**	**HCTIPEVEN**
Texto	*Texto*	*Texto*	*Texto*	*Texto*	*Texto*	*Texto*	*Número*

110. HCPATPAC: Se almacena la información patologías de paciente.

dbo_HCPATPAC					
GPACODIGO	**AINCONSEC**	**HCCONFOLI**	**HCGCODIGO**	**HCGITEMPR**	**HCGNUEVOE**
Texto	*Texto*	*Número*	*Texto*	*Texto*	*Texto*
HCGCANTID	**HCGDESCRI**	**HCGOBSERV**	**SOSORDSER**	**GASCODIGO**	**PRECODIGO**
Número	*Texto*	*Texto*	*Texto*	*Texto*	*Texto*
HCGRESPUE	**HCGORIMUE**	**HCESTADO**	**HCFECSOL**		
Número	*Texto*	*Número*	*Fecha/Hora*		

111. HCPATROC: Se almacena la infamación sobre patrocinadores de la institución.

dbo_HCPATROC				
PATCODIGO	**PATNOMBRE**	**PATEMPRES**	**PATDIRECC**	**PATTELEFO**
Texto	*Texto*	*Texto*	*Texto*	*Texto*

112. HCPLAIMG: Se almacena la información de plantillas de imágenes.

dbo_HCPLAIMG		
PICODIGO	**PIDESCRI**	**PIIMAGEN**
Texto	*Texto*	*Texto*

113. HCPLANAE: Se almacena la información e planeacion de actividades de enfermería en fox.

dbo_HCPLANAE						
GPACODIGO	**AINCONSEC**	**GMECODIGO**	**HCLALERGI**	**GASCODIGO**	**HCLTIPACT**	**HCLDESCRI**
Texto	*Texto*	*Texto*	*Texto*	*Texto*	*Número*	*Texto*
HCLFECHA1	**HCLFECHA2**	**HCLCANULA**	**HCLVENTUR**	**HCLHOOD**	**HCLMNB**	**USUCODIGO**
Fecha/Hora	*Fecha/Hora*	*Texto*	*Texto*	*Texto*	*Número*	*Texto*

114. HCPLAPMA: Se almacena la información de plantillas de medicamentos.

dbo_HCPLAPMA					
HCPCCODIGO	**HCMITEMID**	**HCMCODMED**	**HCMCLAPRO**	**HCMCANTID**	**HCMOBSERV**
Texto	*Número*	*Texto*	*Número*	*Número*	*Nemo*
HCMTIPORD	**GASCODIGO**	**CCCCODCEN**	**HCMTIPO**	**IALCODIGO**	**HCMVIAAPL**
Número	*Texto*	*Texto*	*Número*	*Texto*	*Texto*

115. HCPPLAPMA: Se almacena la información de plantillas de medicamentos.

dbo_HCPPLAPMA					
HCPCCODIGO	**HCMITEMID**	**HCMCODMED**	**HCMCLAPRO**	**HCMCANTID**	**HCMOBSERV**
Texto	*Número*	*Texto*	*Número*	*Número*	*Nemo*
HCMTIPORD	**GASCODIGO**	**CCCCODCEN**	**HCMTIPO**	**IALCODIGO**	**HCMVIAAPL**
Número	*Texto*	*Texto*	*Número*	*Texto*	*Texto*

116. HCPPLASER: Se almacena la información de plantillas de servicios.

dbo_HCPPLASER					
HCPCCODIGO	**HCPCODIGO**	**HCPCANTID**	**HCPOBSERV**	**HCPORIMUE**	**HCPESTADO**
Texto	*Texto*	*Número*	*Texto*	*Texto*	*Número*
HCPLUGARP	**HCPAYUDAN**	**HCPANESTE**	**HCPTIPINT**	**HCPEVENT**	**HCPUSAREN**
Número	*Número*	*Texto*	*Número*	*Texto*	*Número*

117. HCPRESTA: Se almacena la información relacionada con prestamos de historia clínica.

dbo_HCPRESTA						
HCPNUMERO	**GPACODIGO**	**HCPFECSOL**	**HCPFECPRE**	**HCPNOMRES**	**GASCODIGO**	**HCPFECDEV**
Texto	*Texto*	*Fecha/Hora*	*Fecha/Hora*	*Texto*	*Texto*	*Fecha/Hora*
USUCODIG1	**USUCODIG2**	**USUCODIG3**	**USUCODIG4**	**HCPFECANU**	**HCPESTADO**	
Texto	*Texto*	*Texto*	*Texto*	*Fecha/Hora*	*Texto*	

118. HCPRETRI: Se almacena la información de pre-triage y control de triage.

dbo_HCPRETRI						
GCRecord	**OID**	**GPACEDULA**	**GPANOMBRE**	**GPASEGNOM**	**GPAAPELLI**	**GPASEGAPE**
Número	*Autonumérico*	*Texto*	*Texto*	*Texto*	*Texto*	*Texto*
ENTCODIGO	**ENTNOMBRE**	**PREFECLLE**	**PRETRIAGE**	**OptimisticLockField**	**ADCENATE**	
Texto	*Texto*	*Fecha/Hora*	*Sí/No*	*Número*	*Texto*	

119. HCPROCED: Se almacena la información de procedimientos y exámenes.

dbo_HCPROCED						
HCPCONSEC	**HCPMANASO**	**HCPCODIGO**	**HCPITEMPR**	**HCPNOMBRE**	**HCPTIPOPR**	**HCPOBSERV**
Texto	*Número*	*Texto*	*Número*	*Texto*	*Número*	*Texto*

120. HCPROEDUC: Se almacena la información de programación para educación.

dbo_HCPROEDUC				
HCFECINSC	**HCTCODIGO**	**HCCODIGO**	**HCCANPER**	**HCCANHORA**
Fecha/Hora	*Texto*	*Texto*	*Número*	*Número*
HCFECINCU	**HCFECFICU**	**HCRESPON**	**HCAENTREN**	**HCTEVENTO**
Fecha/Hora	*Fecha/Hora*	*Texto*	*Texto*	*Número*

121. HCPROFAR: Se almacena la información e productos farmacéuticos.

dbo_HCPROFAR							
HCFCONSEC	**HCFDESPRO**	**HCFASOCIO**	**HCFCODPRO**	**HCFCLAPRO**	**HCFCODGEN**	**HCFPRESEN**	**HCFVADEME**
Texto	*Memo*	*Número*	*Texto*	*Número*	*Texto*	*Nemo*	*Número*
HCFMEDPOS	**HCFPOSSUB**	**HCFINDICA**	**HCFCONTRA**	**HCFDOCIFI**	**HCFINTERA**	**HCFEFESEC**	
Número	*Número*	*Memo*	*Memo*	*Memo*	*Memo*	*Memo*	

122. HCPROMEN: Se almacena la información e procedimientos de medicina nuclear.

dbo_HCPROMEN	
HCPCODIPR	**HCPDESCPR**
Texto	*Texto*

123. HCPROMYP: Se almacena la información de promoción y prevención.

dbo_HCPROMYP				
HCSCODIGO	**HCSNOMBRE**	**HCSINDICA**	**HCSCUIDAD**	**HCSOBSERV**
Texto	*Texto*	*Texto*	*Texto*	*Texto*

124. HCQUIPAC: Se almacena la información de procedimientos quirúrgicos.

dbo_HCQUIPAC							
GPACODIGO	**AINCONSEC**	**HCCONFOLI**	**HCQCODIGO**	**HCQITEMPR**	**HCQNUEVOE**	**HCQCANTID**	**HCQLUGARP**
Texto	*Texto*	*Número*	*Texto*	*Número*	*Texto*	*Número*	*Número*
HCQAYUDAN	**HCQANESTE**	**HCQDESCRI**	**HCQOBSERV**	**HCQTIPINT**	**HCQSEGCIR**	**SOSORDSER**	**GASCODIGO**
Número	*Texto*	*Texto*	*Texto*	*Número*	*Texto*	*Texto*	*Texto*
PRECODIGO	**HCQRESPUE**	**HCESTADO**	**HCQEVENTO**	**HCQPROVIE**	**HCQDESCRI**		
Texto	*Número*	*Número*	*Texto*	*Número*	*Texto*		

125. HCRACTREN: Se almacena la información e actividades renales.

dbo_HCRACTREN						
OID	**HCFECREG**	**GASCODIGO**	**GPACODIGO**	**AINCONSEC**	**HCACTRENAL**	**GCRecord**
Autonumérico	*Fecha/Hora*	*Texto*	*Texto*	*Texto*	*Número*	*Número*

126. HCRECUPE: Se almacena la información sobre recuperación de pacientes en quirófanos en fox.

dbo_HCRECUPE									
HCFECREG	**GASCODIGO**	**GPACODIGO**	**AINCONSEC**	**HCHORREG**	**HCDORMIDO**	**HCSOMNOLI**	**HCEXITADO**	**HCCONCIEN**	**HCROSADO**
Fecha/Hora	*Texto*	*Texto*	*Texto*	*Fecha/Hora*	*Texto*	*Texto*	*Texto*	*Texto*	*Texto*
HCPALIDO	**HCCIANOTI**	**HCICTERICO**	**HCAMPLIA**	**HCSUPERF**	**HCDISNEA**	**HCESPON**	**HCCANULA**	**HCVENTURY**	**HCENTUBA**
Texto	*Texto*	*Texto*	*Texto*	*Texto*	*Texto*	*Texto*	*Texto*	*Texto*	*Texto*
HCTRAQUE	**HCSANGRA**	**HCTUBOGA**	**HCTUBOTO**	**HCSONDA**	**HCHEMOVAC**	**HCIRRIGA**	**HCOTROSD**	**HCBATA**	**HCRAYOS**
Texto	*Texto*	*Texto*	*Texto*	*Texto*	*Texto*	*Texto*	*Texto*	*Texto*	*Texto*
HCHCANT	**HCVEST**	**HCFICHA**	**HCOTROSV**	**HCCATETER**					
Texto	*Texto*	*Texto*	*Texto*	*Texto*					

127. HCRECUPERA: Se almacena la información sobre recuperación de pacientes en quirófanos.

dbo_HCRECUPERA						
GPACODIGO	**HCFFECREG**	**AINCONSEC**	**DATO1**	**DATO2**	**DATO3**	**DATO4**
Texto	*Texto*	*Texto*	*Número*	*Número*	*Número*	*Número*
DATO5	**DATO6**	**DATO7**	**DATO8**	**DATO9**	**DATO10**	**DATO11**
Número	*Número*	*Número*	*Número*	*Número*	*Número*	*Número*
DATO12	**DATO13**	**DATO14**	**HCDORMIDO**	**HCSOMNOLI**	**HCEXITADA**	**HCCONCIEN**
Número	*Número*	*Número*	*Texto*	*Texto*	*Texto*	*Texto*

HCROSADO	HCPALIDO	HCCIANOTI	HCICTERIC	HCAMPLIA	HCSUPERFI	HCDISNEA
Texto	*Texto*	*Texto*	*Texto*	*Texto*	*Texto*	*Texto*
HCTOS	**HCFLEMAS**	**HCENLABUD**	**HCCANUMA**	**HCTRASQUE**	**HCOTROS**	**HCSANGRA**
Texto	*Texto*	*Texto*	*Texto*	*Texto*	*Texto*	*Texto*
HCTUBOGAS	**HCTUBOTOR**	**HCSUNDVES**	**HCHEMOVAC**	**HCIRRIGAC**	**HCOTRODR**	**HCSHOCK**
Texto	*Texto*	*Texto*	*Texto*	*Texto*	*Texto*	*Texto*
HCBATAQU	**HCRAYOSX**	**HCANTIGUAC**	**HCVESTAMB**	**HCFICHA**	**HCOTROSS**	**HCCATETER**
Texto	*Texto*	*Texto*	*Texto*	*Texto*	*Texto*	*Texto*
GASCODIGO						
Texto						

128. HCREFANE: Se almacena la información e anexos de referencia.

dbo_HCREFANE

GCRecord	OID	GPACODIGO	AINCONSEC	HCCONFOLI	HCRCONSEC	REANIVSOC1	REANIVSOC2
Número	*Autonumérico*	*Texto*	*Texto*	*Número*	*Texto*	*Texto*	*Texto*
REAGLAGOW1	**REAGLAGOW2**	**REAGLAGOWTC**	**REAEMBARA**	**REAGINECG**	**REAGINECP**	**REAGINECA**	**REAGINECC**
Número	*Número*	*Número*	*Sí/No*	*Número*	*Número*	*Número*	*Número*
REAGIFUR1	**REAGIFUR2**	**REAGIFUR3**	**REAEDAGES**	**REAGINFCF**	**REAALTUTE**	**REAACTUTE**	**REAACUTIR**
Número	*Número*	*Número*	*Número*	*Número*	*Número*	*Sí/No*	*Texto*
REAAMINOR	**REARUPMEM**	**REATIEEVO**	**READILATA**	**REABORRAM**	**REAESTACI**	**REACEFALI**	**REAMOTREM1**
Sí/No	*Sí/No*	*Número*	*Número*	*Número*	*Número*	*Sí/No*	*Número*
REAMOTREMD	**REAIPSARE**	**REANIVIPS**	**REAFECCON**	**REAFECSAL**	**REAFECSAL**	**REASERREM**	**REASERREMD**
Memo	*Texto*	*Texto*	*Fecha/Hora*	*Fecha/Hora*	*Texto*	*Número*	*Nemo*
REASERARE	**REASERARED**	**OptimisticLockField**	**HCRFECRE**	**HCRORIGEN**	**GERCODENT**	**HCRMOTIRE**	**HCTCODIGO**
Número	*Nemo*	*Número*	*Fecha/Hora*	*Texto*	*Texto*	*Texto*	*Texto*
HCDCODIGO	**HCDNOMBRE**	**HCRANAMNE**	**HCRSIGNTA**	**HCRSIGNFR**	**HCRSIGNPS**	**HCRSIGNTO**	**HCRSIGNFC**
Texto	*Texto*	*Texto*	*Texto*	*Texto*	*Texto*	*Texto*	*Texto*
HCRSIGNTL	**HCREXAFIS**	**HCRRESPRU**	**HCRTRAINS**	**HCRDIAPRE**	**HCRDIANOM**	**HCRTIPSER**	**GESECODSE**
Texto	*Texto*	*Texto*	*Texto*	*Texto*	*Texto*	*Texto*	*Texto*
HCRNOMSER	**HCRDETREF**	**HCRREMITE**	**REAFICSIS**	**REAFECFUR**	**REARESHIS**		
Texto	*Texto*	*Texto*	*Texto*	*Fecha/Hora*	*Nemo*		

129. HCREGACT: Se almacena la información de registró e actividades y procedimientos.

dbo_HCREGACT

GPACODIGO	AINCONSEC	SIPCODIGO	HCRFECPRO	HCRTURMAN	HCRTURTAR
Texto	*Texto*	*Texto*	*Fecha/Hora*	*Número*	*Número*
HCRTURNOC	**HCRMARES**	**HCRTARRES**	**HCRNORESP**	**HCRCANTID**	
Número	*Texto*	*Texto*	*Texto*	*Número*	

130. HCREGENF: Se almacena registro de enfermería

dbo_HCREGENF							
HCFECREG	**GASCODIGO**	**GPACODIGO**	**AINCONSEC**	**GPAPESO**	**GPATALLA**	**HCACTPREQPRE**	**HCACTPREQENV**
Fecha/Hora	*Texto*	*Texto*	*Texto*	*Número*	*Número*	*Texto*	*Texto*

131. HCREGEXA: Se almacena la información sobre control de laboratorios y exámenes.

dbo_HCREGEXA					
GPACODIGO	**HCFFECREG**	**HCFHORARE**	**AINCONSEC**	**HCRDESEXA**	**HCRTOMADO**
Texto	*Texto*	*Número*	*Texto*	*Texto*	*Número*
HCRREPORT	**HCRITEMSE**	**HCRFECTOM**	**HCRFECREP**	**GASCODIGO**	
Número	*Número*	*Fecha/Hora*	*Fecha/Hora*	*Número*	

132. HCRENAL: Se almacena la información de registro renal.

dbo_HCRENAL						
GPACODIGO	**HCFFECREG**	**AINCONSEC**	**DATO1**	**DATO2**	**DATO3**	**DATO4**
Texto	*Texto*	*Texto*	*Texto*	*Número*	*Número*	*Número*
DATO5	**DATO6**	**HCTIATENH**	**HCTIATENA**	**HCCRONICO**	**HCAGUDO**	**HCMAQUINA**
Número	*Texto*	*Texto*	*Texto*	*Texto*	*Texto*	*Texto*
HCTIEMPO	**HCDUALIZA**	**HCINICIO**	**HCTERMINA**	**HCPESOSE**	**HCFAV**	**HCCATETER**
Texto	*Texto*	*Texto*	*Texto*	*Texto*	*Texto*	*Texto*
HCCATETER	**HCP**	**HCT**	**HCINJERTO**	**HCPESOPRE**	**HCPESOPOS**	**HCTAPRE**
Texto	*Texto*	*Texto*	*Texto*	*Número*	*Número*	*Texto*
HCTAPOS	**HCPULPRE**	**HCPULPOS**	**HCCANULA**	**HCDESOBVE**	**HCSIN**	**HCFH**
Texto	*Texto*	*Texto*	*Texto*	*Texto*	*Texto*	*Texto*
HCTOTAL	**HCVST**	**HCVUF**	**GASCODIGO**			
Número	*Texto*	*Texto*	*Texto*			

133. HCRESEPIMG: Se almacena la información sobre recepción de imágenes.

dbo_HCRESEPIMG				
GPACODIGO	**AINCONSEC**	**HCCONFOLI**	**HCPCODIGO**	**HCPITEMPR**
Texto	*Texto*	*Número*	*Texto*	*Texto*
HCPTIPREG	**HCCODIMG**	**HCITITULO**	**HCICOMENT**	**HCIRUTA**
Número	*Número*	*Texto*	*Nemo*	*Nemo*

134. HCRESEXAPAT: Se almacena la información de resultados de exámenes de patología.

dbo_HCRESEXAPAT							
GPACODIGO	**AINCONSEC**	**HCCONFOLI**	**HCPCODIGO**	**HCPITEMPR**	**HCPTIPREG**	**HCIFECATE**	**HCLFECRES**
Texto	*Texto*	*Número*	*Texto*	*Texto*	*Número*	*Fecha/Hora*	*Fecha/Hora*
HCRFECEXA	**HCLDESRES**	**HCLANALIS**	**HCLDOCCER**	**GMECODIGO**	**HCINTERPRE**	**HCFECINTER**	
Fecha/Hora	*Memo*	*Memo*	*Número*	*Texto*	*Texto*	*Fecha/Hora*	

135. HCRESLAP: Se almacena la información de resultados de exámenes de patología.

dbo_HCRESLAP						
GPACODIGO	**AINCONSEC**	**HCCONFOLI**	**HCPCODIGO**	**HCPITEMPR**	**HCIFECATE**	**HCLFECRES**
Texto	*Texto*	*Número*	*Texto*	*Número*	*Fecha/Hora*	*Fecha/Hora*
HCLDESRES	**HCLANALI1**	**HCLANALI2**	**HCLGEMCOD**	**HCLDOCCER**	**HCRFECEXA**	**HCLGRAFI1**
Texto	*Texto*	*Texto*	*Texto*	*Número*	*Fecha/Hora*	*Texto*
HCLGRAFI2	**HCLGRAFI3**	**HCENUEVOE**	**GMECODIGO**			
Texto	*Texto*	*Texto*	*Texto*			

136. HCRESNOQ: Se almacena la información de resultados no quirúrgicos.

dbo_HCRESNOQ						
GPACODIGO	**AINCONSEC**	**HCCONFOLI**	**HCTCODIGO**	**HCTITEMPR**	**HCIFECATE**	**HCNFECRES**
Texto	*Texto*	*Número*	*Texto*	*Número*	*Fecha/Hora*	*Fecha/Hora*
HCNDESRES	**HCNANALI1**	**HCNANALI2**	**HCNGEMCOD**	**HCNDOCCER**	**HCRFECEXA**	**HCNGRAFI1**
Texto	*Texto*	*Texto*	*Texto*	*Número*	*Fecha/Hora*	*Texto*
HCNGRAFI2	**HCNGRAFI3**	**HCTNUEVOE**	**GMECODIGO**			
Texto	*Texto*	*Texto*	*Texto*			

137. HCRESQUI: Se almacena la información de resultados quirúrgicos.

dbo_HCRESQUI						
GPACODIGO	**AINCONSEC**	**HCCONFOLI**	**HCQCODIGO**	**HCQITEMPR**	**HCIFECATE**	**HCQFECRES**
Texto	*Texto*	*Número*	*Texto*	*Número*	*Fecha/Hora*	*Fecha/Hora*
HCQDESRES	**HCQANALI1**	**HCQANALI2**	**HCQGEMCOD**	**HCQDOCCER**	**HCRFECEXA**	**HCQGRAFI1**
Texto	*Texto*	*Texto*	*Texto*	*Número*	*Fecha/Hora*	*Texto*
HCQGRAFI2	**HCQGRAFI3**	**HCQNUEVOE**	**GMECODIGO**			
Texto	*Texto*	*Texto*	*Texto*			

138. HCRESTRI: Se almacena de resultados de triage.

dbo_HCRESTRI	
USUCODIGO	**HCCTIPOHC**
Texto	*Texto*

139. HCRESUQX: Se almacena de resultados de quirófanos.

dbo_HCRESUQX						
GCRecord	**OID**	**GPACODIGO**	**AINCONSEC**	**HCCONFOLI**	**SIPCODIGO**	**SERNUMERO**
Número	*Autonumérico*	*Texto*	*Texto*	*Número*	*Texto*	*Texto*
SERCONHOJ	**RESLUGINT**	**RESTIPINT**	**RESTIOANE**	**SIPNOMBRE**	**OptimisticLockField**	**SOSORDSER**
Texto	*Número*	*Número*	*Texto*	*Texto*	*Número*	*Texto*

140. HCSEMINA: Se almacena la información de programación de seminarios.

dbo_HCSEMINA							
HCCEDULA	**HCCANTIHO**	**HCFECINSC**	**HCNOCONSI**	**HCTALLERE**	**HCVACONSI**	**HCCUPOSOT**	**TCACODIGO**
Texto	*Número*	*Fecha/Hora*	*Texto*	*Número*	*Número*	*Texto*	*Texto*

141. HCSERINT: Se almacena la información de servicios de interconsultas.

dbo_HCSERINT
SIPCODIGO
Texto

142. HCSERREF: Se almacena la información de servicios de referencia.

dbo_HCSERREF			
SERVICIOIPS	**REFERENCIA**	**OID**	**OptimisticLockField**
Texto	*Número*	*Autonumérico*	*Número*

143. HCSIGVIT: Se almacena la información de signos vitales.

dbo_HCSIGVIT								
HCFECREG	**GASCODIGO**	**GPACODIGO**	**AINCONSEC**	**HCHORREG**	**HCHORSIGV**	**HCCODSIGV**	**HCVALSIGV**	**USUCODIGO**
Fecha/Hora	*Texto*	*Texto*	*Texto*	*Fecha/Hora*	*Fecha/Hora*	*Texto*	*Texto*	*Texto*

144. HCSOLANE: Se almacena la información de anexo de solicitud.

dbo_HCSOLANE			
HCCTIPOHC	**HCXFORMAT**	**HCCNCAMPO**	**HCXORDEN**
Texto	*Número*	*Texto*	*Número*

145. HCSOLCYF: Se almacena la información de solicitud de anexos.

dbo_HCSOLCYF					
HCSNUMERO	**GPACEDULA**	**HCSFECHOS**	**HCSFECURG**	**HCSDETALLE**	**HCSNOMSOL**
Texto	*Texto*	*Fecha/Hora*	*Fecha/Hora*	*Texto*	*Texto*
HCSIDESOL	**HCSDIRSOL**	**HCSTELSOL**	**HCSENTREGA**	**HCSFECHA**	**HCSTIPO**
Texto	*Texto*	*Texto*	*Texto*	*Fecha/Hora*	*Número*

146. HCSOLIHC: Se almacena la información de solicitud de historia clínica.

dbo_HCSOLIHC					
HCSCONSHC	**HCSFECSHC**	**GPACODIGO**	**AINCONSEC**	**HCSOBSERV**	**HCSTIPO**
Texto	*Fecha/Hora*	*Texto*	*Texto*	*Texto*	*Número*

147. HCTCARGOS: Se almacena la información de los diferentes cargos.

dbo_HCTCARGOS		
HCCODIGO	**HCCNOMBRE**	**HCCANFUN**
Texto	*Texto*	*Número*

148. HCTEMCAP: Se almacena la información de capacitaciones.

dbo_HCTEMCAP			
TCACODIGO	**TCANOMBRE**	**TCAINTENS**	**TCAINTMIN**
Texto	*Texto*	*Número*	*Número*

149. HCTEMTEX: Se almacena de datos de texto temporales.

dbo_HCTEMTEX						
HCECONSEC	**CAMPO1**	**CAMPO2**	**CAMPO3**	**CAMPO4**	**CAMPO5**	**CAMPO6**
Texto	*Memo*	*Memo*	*Memo*	*Memo*	*Memo*	*Memo*
CAMPO7	**CAMPO8**	**CAMPO9**	**CAMPO10**	**CAMPO11**	**CAMPO12**	**CAMPO13**
Memo	*Memo*	*Memo*	*Memo*	*Memo*	*Memo*	*Memo*
CAMPO14	**CAMPO15**	**CAMPO16**	**CAMPO17**	**CAMPO18**	**CAMPO19**	**CAMPO20**
Memo	*Memo*	*Memo*	*Memo*	*Memo*	*Memo*	*Memo*
CAMPO21	**CAMPO22**	**CAMPO23**	**CAMPO24**	**CAMPO25**		
Memo	*Memo*	*Memo*	*Memo*	*Memo*		

150. HCTERPAC: Se almacena la información de terapia de paciente.

dbo_HCTERPAC							
GPACODIGO	**AINCONSEC**	**HCCONFOLI**	**HCTCODIGO**	**HCTITEMPR**	**HCTNUEVOE**	**HCTCANTID**	**HCTDESCRI**
Texto	*Texto*	*Número*	*Texto*	*Número*	*Texto*	*Número*	*Texto*
HCTOBSERV	**SOSORDSER**	**GASCODIGO**	**PRECODIGO**	**HCTRESPUE**	**HCESTADO**	**HCTPROVIE**	
Texto	*Texto*	*Texto*	*Texto*	*Número*	*Número*	*Número*	

151. HCTESTALD: Se almacena la información de

dbo_HCTESTALD						
HCFECREG	**GASCODIGO**	**GPACODIGO**	**AINCONSEC**	**HCCATEGORIA**	**HCNUMITEM**	**HCVALOR**
Fecha/Hora	*Texto*	*Texto*	*Texto*	*Texto*	*Texto*	*Texto*

152. HCTIPCON: Se almacena la información de tipo de consulta.

dbo_HCTIPCON	
HCTCODIGO	**HCTNOMBRE**
Texto	*Texto*

153. HCTIPHIS: Se almacena la información de tipo de historia.

dbo_HCTIPHIS							
HCCTIPOHC	**GEECODIGO**	**HCDETALLE**	**HCNUAREAS**	**HCNOMBARC**	**HCALTURAM**	**HCCODINT**	**HCEXIDIA**
Texto	*Texto*	*Texto*	*Número*	*Texto*	*Número*	*Texto*	*Número*
HCPERFOL	**HCODONTO**	**GASCODIGO**	**HCEXIDIE**	**HCARESER**	**HCCAUEXT**	**HCFINCON**	
Número	*Número*	*Texto*	*Número*	*Texto*	*Número*	*Número*	

154. HCTIPLIQEL: Se almacena la información de tipo de líquido eliminado.

dbo_HCTIPLIQEL			
HCCODLIQ	**HCNOMLIQ**	**HCDESLIQ**	**HCRESGAS**
Texto	*Texto*	*Texto*	*Texto*

155. HCTIPSIGV: Se almacena la información de tipo de signo vital.

dbo_HCTIPSIGV					
HCCODSIGV	**HCDESCRIP**	**HCVALMIN**	**HCVALMAX**	**HCMASCARA**	**HCNOMSIGV**
Texto	*Texto*	*Texto*	*Texto*	*Texto*	*Texto*

156. HCTIPVAC: Se almacena la información de tipo de vacuna.

dbo_HCTIPVAC					
GCRecord	**OID**	**TVACODIGO**	**TVANOMBRE**	**TVAANOMIN**	**TVAMESMIN**
Número	*Autonumérico*	*Texto*	*Texto*	*Número*	*Número*
TVAANOMAX	**TVAMESMAX**	**TVAUNIDAD**	**OptimisticLockField**	**AGREGAR**	
Número	*Número*	*Texto*	*Número*	*Sí/No*	

157. HCTODONTO: Se almacena la información sobre tratamiento odontológico.

dbo_HCTODONTO					
GCRecord	**OID**	**HCIODONTO**	**ODTRAFECHA**	**HCTRATAMI**	**ODTRACADI**
Número	*Autonumérico*	*Número*	*Fecha/Hora*	*Número*	*Sí/No*
ODTRACAPA	**ODTRACAOC**	**ODTRACAME**	**ODTRACAVE**	**ODTRACAIN**	**ODTRAESTAD**
Sí/No	*Sí/No*	*Sí/No*	*Sí/No*	*Sí/No*	*Número*
OptimisticLockField	**ODTOBSERV**	**ODTRACALI**			

Número	*Texto*	*Sí/No*			

158. HCTRAPAC: Se almacena la información sobre tratamiento de paciente.

dbo_HCTRAPAC

HCTCONSEC	GPACODIGO	AINCONSEC	HCCONFOLI	HCTFECTRA	GASCODIG1	GASCODIG2	HCTREQCAM	GMECODIGO	HCTMOTRAS
Texto	*Texto*	*Texto*	*Número*	*Fecha/Hora*	*Texto*	*Texto*	*Número*	*Texto*	*Memo*

159. HCTRATAMI: Se almacena la información sobre tratamiento de paciente.

dbo_HCTRATAMI

GCRecord	OID	TRANOMBRE	TRACONVEN	TRACOLOR	OptimisticLockField
Número	*Autonumérico*	*Memo*	*Número*	*Objeto OLE*	*Número*
TRASUPERF	**TRACONVE1**	**TRACODCUPS**	**TRACEPCOP**	**TRACEPVAL**	**TRACOPVAL**
Sí/No	*Memo*	*Texto*	*Número*	*Número*	*Número*

160. HCTRIAGE: Se almacena la información sobre historia clínica de triage.

dbo_HCTRIAGE

HCTNUMERO	HCTFECTRI	GPACEDULA	HCTEDAD	HCTUNEDAD	ENTCODIGO	GEMCODIGO	GPANOMBRE
Texto	*Fecha/Hora*	*Texto*	*Número*	*Número*	*Texto*	*Texto*	*Texto*
GPASEGNOM	**GPAAPELLI**	**GPASEGAPE**	**HCTMOTCON**	**HCTTENART**	**HCTFRECAR**	**HCTFRERES**	**HCTTEMPER**
Texto	*Texto*	*Texto*	*Memo*	*Texto*	*Texto*	*Texto*	*Texto*
HCTSO2	**HCTOBSERV**	**HCTCLASIF**	**USUCODIGO**	**GPACODIGO**	**HCTDIABET**	**HCTCORONA**	**HCTACV**
Texto	*Nemo*	*Numero*	*Texto*	*Texto*	*Texto*	*Texto*	*Texto*
HCTCONVUL	**HCTHIPERT**	**HCTPULMON**	**HCTOTROAN**	**HCTCUALOT**	**HCTCIRUGI**	**HCTALERGI**	**HCTDROGAS**
Texto	*Texto*	*Texto*	*Texto*	*Nemo*	*Texto*	*Texto*	*Texto*
HCTCONESP	**HCTREMISI**	**HCTCONFIR**	**HCTSINCON**	**HCTCAMINA**	**HCTVEHICU**	**HCTAMBULA**	**HCTPOLICI**
Texto	*Texto*	*Texto*	*Texto*	*Texto*	*Texto*	*Texto*	*Texto*
HCTCOLLAR	**HCTTABLAE**	**HCTFERULA**	**HCTOXIGEN**	**HCTLEV**	**HCTINTUBA**	**HCTSNG**	**HCTVESICA**
Texto	*Texto*	*Texto*	*Texto*	*Texto*	*Texto*	*Texto*	*Texto*
HCTTUBTOR	**GMECODIGO**	**HCTHELI**	**HCTACCI**	**HCTSOAT**	**HCTENFE**	**HCCAUING**	**HCFMODTRI**
Texto	*Texto*	*Texto*	*Texto*	*Texto*	*Texto*	*Numero*	*Fecha/Hora*
HCHOSREC	**HCPACANT**	**HCPAREC**	**HCINFREC**	**HCONEXTHU**	**HCLINPAG**	**HCTDOCCER**	**HCTESTCON**
Texto	*Texto*	*Texto*	*Texto*	*Texto*	*Número*	*Texto*	*Texto*
HCTPESO	**HCTHALPOS**	**HCTALIALC**	**HCTPLANIF**	**HCTALTERN**	**HCTFEULRE**	**HCTDIAGNO**	**HCTOBSDIA**
Número	*Nemo*	*Texto*	*Texto*	*Texto*	*Fecha/Hora*	*Texto*	*Nemo*
HCTRECOME	**HCAUSENT**	**ACACODIGO**	**TRIIDENTI**	**HCTDIAGN2**	**HCTDIAGN3**	**HCTBOMBER**	**HCTTAXI**
Nemo	*Texto*	*Texto*	*Texto*	*Texto*	*Texto*	*Texto*	*Texto*

161. HCTTEMA: Se almacena la información de terapias.

dbo_HCTTEMA

HCTCODIGO	HCTNOMBRE	HCINTHORA
Texto	*Texto*	*Número*

162. HCTURNOENF: Se almacena la información turnos de enfermería.

dbo_HCTURNOENF

CODTURNO	DESCRIPCION	HORAINICIO	HORAFINAL	TIPOTURNO
Texto	*Texto*	*Fecha/Hora*	*Fecha/Hora*	*Texto*

163. HCTURNTENF: Se almacena la información de turnos de enfermería.

dbo_HCTURNTENF

GCRecord	OID	SEUSUARIO	HCFECTURN	HCHORINI	HCHORFIN
Número	*Autonumérico*	*Texto*	*Fecha/Hora*	*Fecha/Hora*	*Fecha/Hora*

164. HCTURUSU: Se almacena la información de turnos de usuarios.

dbo_HCTURUSU

USUCODIGO	HTUPERMAN	HTUPERTAR	HTUPERNOC
Texto	*Número*	*Número*	*Número*

165. HCUNIRENAL: Se almacena la información de unidad renal.

dbo_HCUNIRENAL

HCFECREG	GASCODIGO	GPACODIGO	AINCONSEC	HCHORREG	HCATEHOSP	HCATEAMB
Fecha/Hora	*Texto*	*Texto*	*Texto*	*Fecha/Hora*	*Texto*	*Texto*
HCCRONICO	**HCAGUDO**	**HCMAQUINA**	**HCTIEMPO**	**HCDIALIZA**	**HCHORAINI**	**HCHORAFIN**
Texto	*Texto*	*Texto*	*Texto*	*Texto*	*Fecha/Hora*	*Fecha/Hora*
HCPESOSEC	**HCFAV**	**HCCATETER**	**HCP**	**HCT**	**HCINJERTO**	**HCPESOPRE**
Texto	*Texto*	*Texto*	*Texto*	*Texto*	*Texto*	*Texto*
HCPESOPOS	**HCTAPRE**	**HCTAPOS**	**HCPULPRE**	**HCPULPOS**	**HCCANULA**	**HCDESCON**
Texto	*Texto*	*Texto*	*Texto*	*Texto*	*Texto*	*Texto*
HCSIN	**HCFH**	**HCTOTAL**	**HCVST**	**HCVUF**		
Número	*Número*	*Número*	*Texto*	*Texto*		

166. HCUSUTURNO: Se almacena la información de turnos de usuarios.

dbo_HCUSUTURNO		
USUCODIGO	**CODTURNO**	**CODDIA**
Texto	*Texto*	*Texto*

167. HCVACPAC: Se almacena la información de vacunas de pacientes.

dbo_HCVACPAC				
GCRecord	**OID**	**GPACODIGO**	**TIPOVACUNA**	**VAPFECREA**
Número	*Autonumérico*	*Texto*	*Número*	*Fecha/Hora*
VAPANOEDAD	**VAPMESEDAD**	**OptimisticLockField**	**FECHAREAL**	
Número	*Número*	*Número*	*Fecha/Hora*	

168. HCVALNEURO: Se almacena la información de valoración neurológica.

dbo_HCVALNEURO						
HCFECREG	**GASCODIGO**	**GPACODIGO**	**AINCONSEC**	**HCHORAVAL**	**AOESPONTANEA**	**AOVOZ**
Fecha/Hora	*Texto*	*Texto*	*Texto*	*Número*	*Texto*	*Texto*
AODOLOR	**AONINGUNA**	**RVORIENTADA**	**RVCONFUSA**	**RVINAPROPIADA**	**RVINCOMPRENSIBLE**	**RVNINGUNA**
Texto	*Texto*	*Texto*	*Texto*	*Texto*	*Texto*	*Texto*
RMOBEDORDEN	**RMLOCDOLOR**	**RMRESDOLOR**	**RMFLEXION**	**RMEXTENSION**	**RMFLACIDO**	**GLASGOW**
Texto	*Texto*	*Texto*	*Texto*	*Texto*	*Texto*	*Texto*
PDTAMANO	**PDREACCION**	**PITAMANO**	**PIREACCION**	**MSNORMAL**	**MSDEBIL**	**MSAUSENTE**
Texto	*Texto*	*Texto*	*Texto*	*Texto*	*Texto*	*Texto*
MINORMAL	**MIDEBIL**	**MIAUSENTE**	**EMALERTA**	**EMSOMNOLIENTO**	**EMESTUPOR**	**EMCOMA**
Texto	*Texto*	*Texto*	*Texto*	*Texto*	*Texto*	*Texto*
OBSERVACION	**RFNORMAL**	**RFAUMENT**	**RFDISMIN**	**RFBABYN**	**RSNORMAL**	**RSCHEYNES**
Nemo	*Texto*	*Texto*	*Texto*	*Texto*	*Texto*	*Texto*
RSKUSS	**RSBIOT**	**RSAPNEUS**	**RSPARO**	**RSASISTEN**		
Texto	*Texto*	*Texto*	*Texto*	*Texto*		

169. HCVENOPU: Se almacena la información de venopunciones.

dbo_HCVENOPU						
HCFECREG	**GASCODIGO**	**GPACODIGO**	**AINCONSEC**	**HCHORREG**	**HCFECTRAS**	**HCFECSUSP**
Fecha/Hora	*Texto*	*Texto*	*Texto*	*Fecha/Hora*	*Fecha/Hora*	*Fecha/Hora*
HCFECCANAL	**HCFECSEGUI**	**HCSITIO**	**HCFECCURA**	**HCFECCAMBIO**	**HCINDICACION**	**HCGRADOFLE**
Fecha/Hora	*Fecha/Hora*	*Texto*	*Fecha/Hora*	*Fecha/Hora*	*Texto*	*Texto*

HCDESCRIP	HCOTRACAU	HCRESPON	HCOBSERV	HCCATETER	HCCLASCAT	HCMOTRETIR
Texto	*Texto*	*Texto*	*Nemo*	*Número*	*Texto*	*Texto*
USUCODIGO						
Texto						

170. HCVENTIL: Se almacena la información de ventilación (UCI).

dbo_HCVENTIL

GPACODIGO	HCFFECREG	HCFHORARE	AINCONSEC	HCRITEMSE	HCVMODOVE	HCVFL02VE
Texto	*Texto*	*Número*	*Texto*	*Número*	*Texto*	*Texto*
HCVVOLCOR	**HCVFLUJUV**	**HCVFRVENT**	**HCVPEEPVE**	**HCVPLATEA**	**HCVGASIME**	**GASCODIGO**
Texto	*Texto*	*Texto*	*Texto*	*Texto*	*Texto*	*Texto*

171. HCVENTILA: Se almacena la información de ventilación.

dbo_HCVENTILA

HCFECREG	GASCODIGO	GPACODIGO	AINCONSEC	HCHORREG	HCHORAVEN	HCMODOVEN
Fecha/Hora	*Texto*	*Texto*	*Texto*	*Fecha/Hora*	*Fecha/Hora*	*Texto*
HCFI02	**HCVOLCOR**	**HCFORVEN**	**HCPEEP**	**HCPLATEAU**	**HCGASIMETRIA**	**USUCODIGO**
Texto	*Texto*	*Texto*	*Texto*	*Texto*	*Texto*	*Texto*
HCIMV	**HCFR**	**HCVMIN**	**HCIE**	**HCINSP**	**HCCURVA**	**HCSAT**
Texto	*Texto*	*Texto*	*Texto*	*Texto*	*Número*	*Texto*
HCPIM	**HCPEUA**					
Texto	*Texto*					

172. HMOMGE1: Se almacena la información de parámetros de seguridad.

dbo_HMOMGE1

GPACODIGO	AINCONSEC	HCCTIPOHC	HCCONFOLI	GMECODIGO	HMFECHARE	mge01mdc	mge01neu
Texto	*Texto*	*Texto*	*Número*	*Texto*	*Fecha/Hora*	*Memo*	*Número*
mg01fc	**mge01dis**	**mge01ena**	**mge01etn**	**mge01ext**	**mge01fr**	**mge01gen**	
Número	*Número*	*Nemo*	*Número*	*Número*	*Número*	*Número*	
mge01gra	**mge01par**	**mge01pie**	**mge01rmo**	**mge01roc**	**mge01rve**	**mge01tea**	**mge01tem**
Número	*Nemo*	*Número*	*Número*	*Número*	*Número*	*Texto*	*Número*
mge01tgl	**mge01tip**	**mge01abd**	**mge01ano**	**mge01cab**	**mge01can**	**mge01cor**	**mge01cue**
Número	*Número*	*Número*	*Nemo*	*Número*	*Número*	*Número*	*Número*
mge01cus	**mge01dev**	**mge01ot1**	**mge01int**	**mge01efh**	**mge01lol**	**mge01mec**	**mge01oac**
Número	*Texto*	*Texto*	*Número*	*Fecha/Hora*	*Número*	*Número*	*Texto*
mge01oin	**mge01por**	**mge01pqu**	**mge01ual**	**mge01udr**	**mge01act**	**mge01cau**	**mge01cau**

Texto	*Número*	*Número*	*Número*	*Número*	*Número*	*Número*	*Texto*
mge01eds	**mge01fap**	**mge01ipr**	**mge01atm**	**mge01ttr**	**mge01usu**	**mge01con**	**mge01o01**
Número	*Número*	*Número*	*Número*	*Número*	*Número*	*Número*	*Texto*
mge01o02	**mge01o03**	**mge01o04**	**mge01o05**	**mge01o06**	**mge01ot3**	**mge01sea**	**mge01rav**
Texto	*Texto*	*Texto*	*Texto*	*Texto*	*Número*	*Número*	*Número*
mge01apa	**mge014cbi**	**mge01cha**	**mge01cin**	**mge01cmo**	**mge01ctx**	**mge01cra**	**mge01dpa**
Número	*Número*	*Número*	*Número*	*Número*	*Número*	*Número*	*Número*
mge01inf	**mge01mno**	**mge01msu**	**mge01**	**mge01elu**	**mge01fra**	**mge01lal**	**mge01los**
Número	*Número*	*Número*	*Número*	*Número*	*Número*	*Número*	*Número*
mge01lpp	**mge01nss**	**mge01ota**	**mge01que**	**mge01tcr**	**mge01cmh**	**mge01o08**	**mge01o09**
Número	*Número*	*Número*	*Número*	*Número*	*Número*	*Texto*	*Texto*
mge01ode	**mge01ojo**	**mge01oro**	**mge01pge**	**mge01sis**	**mge01tor**	**mge01tag**	**mge01tim**
Texto	*Número*	*Número*	*Número*	*Número*	*Número*	*Número*	*Número*
mgeo07	**mge01ado**	**mge01cll**	**mge01clm**	**mge01rsi**	**mge01obs**		
Texto	*Número*	*Número*	*Número*	*Nemo*	*Nemo*		

173. HMANE001: Se almacena parámetros de seguridad.

dbo_HMANE001

GPACODIGO	AINCONSEC	HCCTIPOHC	HCCONFOLI	GMECODIGO	HMFECHARE
Texto	*Texto*	*Texto*	*Número*	*Texto*	*Fecha/Hora*
aneana	**anefc**	**anefr**	**aneplan**	**anesub**	**aneta**
Memo	*Número*	*Número*	*Nemo*	*Nemo*	*Número*
aneta1	**anetem**				
Número	*Número*				

174. HMMGE002: Se almacena la información de parámetros de seguridad.

dbo_HMMGE002

GPACODIGO	AINCONSEC	HCCTIPOHC	HCCONFOLI	GMECODIGO	HMFECHARE	mge02pla
Texto	*Texto*	*Texto*	*Número*	*Texto*	*Fecha/Hora*	*Memo*
mge02ana	**mg2fr**	**mge02tar**	**mge02exa**	**mge02sub**	**mg2fc**	**mge02tem**
Memo	*Número*	*Texto*	*Memo*	*Memo*	*Número*	*Número*

175. HMONC002: Se almacena la información de parámetros de seguridad.

dbo_HMONC002					
GPACODIGO	**AINCONSEC**	**HCCTIPOHC**	**HCCONFOLI**	**GMECODIGO**	**HMFECHARE**
Texto	*Texto*	*Texto*	*Número*	*Texto*	*Fecha/Hora*
onc2ost	**onc2geni**	**onc2adb**	**onc2cora**	**onc2cue**	**onc2piel**
Número	*Número*	*Número*	*Número*	*Número*	*Número*
onc2anor	**onc2cab**	**onc2fc**	**onc2fr**	**onc2neu**	**onc2para**
Texto	*Número*	*Número*	*Número*	*Número*	*Nemo*
onc2ta	**onc2tem**	**oncenf**	**oncmov**	**oncpe**	**oncsc**
Texto	*Número*	*Texto*	*Texto*	*Número*	*Número*
oncsis	**onctal**				
Texto	*Número*				

176. HMPRUEB1: Se almacena la información de parámetros de seguridad.

dbo_HMPRUEB1						
GPACODIGO	**AINCONSEC**	**HCCTIPOHC**	**HCCONFOLI**	**GMECODIGO**	**HMFECHARE**	**datos**
Texto	*Texto*	*Texto*	*Número*	*Texto*	*Fecha/Hora*	*Texto*

177. HMPRUEBA: Se almacena la información de parámetros de seguridad.

dbo_HMPRUEBA						
GPACODIGO	**AINCONSEC**	**HCCTIPOHC**	**HCCONFOLI**	**GMECODIGO**	**HMFECHARE**	**preuba2**
Texto	*Texto*	*Texto*	*Número*	*Texto*	*Fecha/Hora*	*Texto*
prueba	**prueba1**	**datos**	**muestra**	**mostrar**	**muestra2**	**texto**
Texto	*Texto*	*Número*	*Texto*	*Número*	*Texto*	*Texto*
uno	**dos**	**tres**	**cinco**	**cuatro**	**opcion**	
Número	*Número*	*Número*	*Número*	*Número*	*Número*	

4.1.9. Importancia del módulo de historia clínica para la institución

Es la más importante herramienta de consulta y registro de la historia clínica de pacientes para los profesionales de la salud de la institución, ya que pone a su disposición un completo y ágil modelo de diagnostico, seguimiento y toma de decisiones asistenciales, disminuyendo al máximo la tareas manuales ya que es completamente integrado a todas las áreas asistenciales.

Su principal característica es que permite generar directamente desde el consultorio o desde cualquiera de las áreas medicas de la institución, las ordenes de los diferentes servicios que se prestan, logrando así la disminución de pasos en procesos administrativos ya que las registra en línea, ofreciendo así facilidad de registro al medico y oportunidad de acceso a la información al personal de apoyo. Todo lo anterior soportado en la reglamentación ordenada en la resolución de 1995 del ministerio de salud y al manejo de confidencialidad que este documento exige.

Contiene:

- Configurable para todas las especialidades
- Resolución 412/2000
- Odontología
- Triage
- Resultados de procedimientos quirúrgicos
- Epicrisis
- Interconsultas
- UCI
- Referencia y contra referencia
- Imágenes diagnósticas
- Ayudas diagnósticas
- Cuadros de enfermería
- Planeación actividades de enfermería
- Vacunación
- Incapacidades/Constancias/Solicitudes
- Medicina Nuclear.

El producto **Dinámica Gerencial** se ajusta de acuerdo con la dinámica del mercado y la tecnología de punta.

Las actualizaciones del producto se sustentan en:

1. Cambios de Ley.

2. Modificaciones del producto y los procesos.
3. Mejoras en el producto.

MANUALES Y DOCUMENTOS SOPORTES

4.1.10. Manuales y documentos soportes

Manuales:

1. Manual de soporte documental sección de información y sistemas.

2. Manual de historia clínicas .net (manual de usuario).

3. Manual de instalación y configuración de dynamica .net

4. Manual de referencia de administración de los datos de dinámica gerencial en oracle.

5. Manual de funciones.

Estándares organizacionales:

1. Guía de administración del riesgo (MECCI).

2. Sistema de direccionamiento estratégico.

3. Direccionamiento estratégico y liderazgo.

4. Documento maestro de creación de prototipos (ciclo de vida de sistemas).

5. Procesos.

Normas, leyes, resoluciones y acuerdos:

1. Resolución 3881 de 1982. (historia clínica)

2. Circular externa 12 de 1993. (historia clínica)

3. Ley 23 e 1981. (ética médica)

4. Circular No 014 del 23 de Julio e 2008 5. (certificación de modelos de historias clínicas con base en especialidades).

5. Resolución 0101 del 28 de febrero de 2008 (conformación del equipo líder de implantación de historia clínica.net).

6. Ley 527 de 1999

Otros documentos:

1. Instructivos de manejo de no conformidades y administración del riesgos (de control interno).

2. Contrato con SYAC.

3. Formato de registro de actualización.

4. Reporte de diferencia para la actualización empresa 01.

5. Requerimientos de historia clínica.

6. Documentación sobre capacitación a técnicos del hospital.

7. Documentación sobre capacitación a usuarios finales (médicos y enfermeras).

8. Diccionario de datos de dinámica gerencial.

9. Reportes del módulo de historia clínica.net.

10. Plataforma para el registro de solicitud de cambios con SYAC.

11. Pantallas del módulo de historia clínica.net.

12. Resolución 0101.

13. Documentos servidor.

14. Planos de cableado estructurado.

15. Planos arquitectónicos. (1, 2, 3, 4 y 5 piso).

16. (Videos de capacitación en la aplicación).

17. Archivo fotográfico, imágenes 3d del hospital.

18. Video revisión infraestructura física.

19. Videos sobre módulo de historia clínica

20. Contrato de Mantenimiento

ANEXOS

DEL LEGAJO PERMANENTE

SE ANEXA DIGITALMENTE

ENTREVISTAS

4.2. LEGAJO CORRIENTE

4.2.1. Memorando de planeación

4.2.1.1. Objetivo general

Evaluar el proceso y el módulo de historia clínica electrónica, que garanticen la confiabilidad, integridad y seguridad permitiendo adelantar actividades de mejoramiento del sistema del hospital universitario departamental de Nariño.

4.2.1.2. Objetivos específicos

1. Recolectar toda la información perteneciente al el módulo de historia clínica y conocer los procesos que se llevan a cabo.
2. Verificar y evaluar el proceso de entrada de datos al módulo de historia clínica para identificar los riesgos de falla en la captura.
3. Verificar y evaluar el procesamiento de datos en el módulo de historia clínica, para verificar del correcto funcionamiento de los procesos implementados en el módulo.
4. Verificar y evaluar las salidas de datos del módulo de historia clínica, para confrontar los reportes generados con las necesidades de los usuarios del sistema.
5. Verificar y evaluar la seguridad e integridad de la información, en el módulo de historia clínica electrónica. Así mismo los controles de acceso que posee cada uno de los usuarios del sistema.
6. Verificar y evaluar el correcto funcionamiento de la red de datos, en relación a la conexión y equipos de la misma, las normas de seguridad y las Políticas que se aplican en la institución.
7. Realizar un informe preliminar con los riesgos encontrados y los posibles controles a los mismos.
8. Realizar una comparación entre las normas ISO y el módulo de historia clínica electrónica, para verificación del cumplimiento de las mismas.

9. Presentar el informe final de auditoría y las recomendaciones, ante el personal de sistemas y administrativo del hospital, que estén vinculados con el manejo de este proceso.

4.2.1.3. Justificación

Teniendo en cuenta que las tecnologías de información han evolucionando y han creciendo especialmente en el campo de la salud, se hace necesario que día a día las entidades de salud tanto públicas como privadas, enfocadas en brindar la prestación de un servicio de salud de calidad, sistematicen sus procesos y cuenten con buenas herramientas en infraestructura física, talento humano, tecnología, entre otros, implementando nuevos procesos que requieren ser monitoreados y evaluados, por tal razón es de gran importancia que estas entidades implementen Auditorías en los procesos asistenciales, administrativos e informáticos, puesto que se desarrollan paralelamente y requieren de un análisis integral y critico.

La importancia de realizar la auditoría a cada uno de los procesos del módulo de historia clínica del aplicativo WINDG, de dinámica gerencial dentro del hospital universitario departamental de Nariño, radica en verificar el correcto funcionamiento de todos los procesos del módulo, y evaluar que todos ellos correspondan a los diferentes requerimientos de sus usuarios (médicos, personal asistencial).

Los beneficios que traerá la presente auditoría al módulo de historia clínica digital del hospital universitario departamental de Nariño, es la revisión de los controles existentes en cuanto a la seguridad lógica del sistema operativo y acceso a la base de datos para comprobar su eficiencia y eficacia, recomendando mejoras para la protección de uno de los principales activos de la empresa, su información. Durante el proceso de auditoría se tratará de encontrar las fallas o riesgos de falla a los cuales se enfrenta el hospital departamental de Nariño, detectar las causas y consecuencias y recomendar controles para su optimización.

4.2.1.4. Alcance

Dentro del alcance de la auditoría que se pretende realizar, se incluye únicamente el módulo de historia clínica electrónica, en el hospital universitario departamental de Nariño, en ella se evaluara los riesgos en cada una de las secciones, y posteriormente se realizara el proceso de auditoría a las que evidencien riesgos más críticos para identificar las causas, dentro de la auditoría se incluye: un análisis integral de los procesos, entrada y salida de datos, aplicación de la norma ISO para la calidad y seguridad del software, evaluación de los controles existentes, técnicas y procedimientos de seguridad, evaluar el correcto funcionamiento de red en relación a conexiones, equipos de cómputo, normas y políticas de seguridad dentro de la institución.

El proceso de auditoría se realiza con el fin de establecer controles óptimos sobre los procesos y el software que gestiona las historias clínicas, con el objetivo primordial de garantizar: confiabilidad, integridad y seguridad de la información, de igual manera se busca establecer controles en relación a la red y el hardware relacionado con el módulo de historia clínica, para que los usuarios (médicos y enfermeras), puedan desempeñar correctamente sus actividades.

4.2.1.5. Metodología empleada

- Recolectar la información perteneciente al módulo de historia clínica electrónica, lo cual se realizara a través de encuestas aplicadas a los usuarios como lo son: médicos y enfermeras de las áreas de triage, urgencias, hospitalización y consulta externa. De igual manera se entrevistara al personal del área de sistemas, al personal de SYAC, que es la empresa con la que se contrato el outsoursing del programa dinámica gerencial, y la implantación del módulo de historia clínica que es el que nos compete, y se utilizara la observación directa para conocer el manejo del módulo, las funciones del personal de sistemas entre otros.

- Evaluar el proceso de entrada de datos, para ello se encuestara a los médicos y enfermeras de las diferentes áreas, para determinar cuales son los requerimientos, se revisara la documentación como los manuales de usuario, los formularios del módulo, las aprobaciones de diseño de historias clínicas, las normas y políticas de la institución, para poder determinar si el proceso del ingreso de datos al módulo, se ajusta y suple las necesidades de los usuarios.
- Verificar y evaluar el procesamiento de datos en el módulo de historia clínica, esto se llevara a cabo mediante encuestas, recogiendo los requerimientos de los usuarios (médicos y enfermeras), se revisara la información y normas de la institución referentes a los procesos que se llevan a cabo y se comparara con los procesamientos realizados por el módulo de historia clínica electrónica.
- Verificar y evaluar las salidas de datos del módulo de historia clínica, esto mediante la realización de encuestas a sus usuarios, para la recolección de requerimientos de salida, se analizara la documentación de los reportes exigidos por la institución y se compara con los reportes del módulo, igualmente se revisara las políticas y normas de la institución (auditoría medica) en relación a los reportes exigidos para la entrega a terceros como la alcaldía y entidades gubernamentales.
- Evaluar la seguridad e integridad de la información en el módulo de historia clínica, esto se realizara mediante el análisis de la documentación de la políticas y normas de la institución referente a la seguridad de los datos, los accesos de los usuarios, se entrevistara al personal del área de sistemas para verificar que modelos de seguridad se utilizan referente al módulo y la base de datos, se analizara la documentación de contratación con la empresa SYAC, para verificar el modelo y estándares de seguridad frente a la otra empresa en los casos de implementación, actualización y mantenimiento del módulo, verificar mediante encuestas y observación directa si los usuarios tienen un referente se seguridad, si se realiza un continuo monitoreo sobre su

disponibilidad de software en cada equipo, igualmente analizar como es su desenvolvimiento, en relación los aspectos de seguridad.

- Evaluar el correcto funcionamiento de la red en relación a la conexión y el hardware utilizado, esto se realizara mediante la toma de fotos y de videos de los cuartos de equipos, de la disposición de la red, de los equipos asignados a médicos y enfermeras, los cuales serán comparados con los estándares de cableado estructurado, el inventario del hardware, igualmente se revisara la documentación sobre la topología de red, certificaciones entre otros, para compararse con los estándares de red y las políticas y requerimientos de la institución. También se realizaran encuestas a los ingenieros del área de sistemas y mediante observación directa se revisara aspectos de seguridad, en relación al modelo de seguridad y firewall instalados.
- Elección de datos de prueba para realizar las pruebas del módulo de historia clínica, tendientes a la revisión de cada uno de los procesos, entrada y salida de datos, validaciones y controles existentes actualmente.
- Realizar una comparación entre la norma ISO y el módulo de historia clínica, para verificar el cumplimiento de las mismas.

4.2.1.6. Recursos

Infraestructura física y hardware: Se asignaron los siguientes recursos de infraestructura física y hardware:

- Espacio físico dentro del aula virtual, que fue el lugar asignado por la institución para la implantación del módulo de historia clínica.
- Dos equipos de cómputo.
- 2 puntos de acceso a la red e Internet.
- 1 impresora.
- 1 Scanner.
- Papelería.

Software:

- Aplicativo WINDG de dinámica gerencial.
- Módulo de historia clínica electrónica.

Talento humano:

- Auditores a cargo de este trabajo: Jenny Nayibi Burgos García.
  María Carolina Domínguez.

Otros recursos

- Cámara de video.
- Grabadora periodista.
- Cámara digital.
- Escáner.

4.2.2. Programa de auditoría

PROGRAMA DE AUDITORÍA

A continuación se relaciona el programa de auditoría a seguir, para evaluar el módulo de historia clínica electrónica, del hospital departamental de Nariño, donde se aplica la metodología denominada COBIT (Control Objectives for Information and related Technology) de la information systems audit and control asociation (ISACA), que está ampliamente aceptado por la comunidad internacional de auditores de sistemas de información como una norma estándar.

Dentro de las características importantes del COBIT, se tendrá muy en cuenta los recursos de la TI (datos, aplicaciones, tecnologías, instalaciones, recurso humano).

De igual manera se tendrán en cuenta los siguientes dominios, procesos y actividades:

4.2.2.1. Dominio 1 - Planeacion y organización (PO)

Este dominio se refiere a la identificación de la forma en que la tecnología de información puede contribuir de la mejor manera al logro de los objetivos de negocio e incluye los siguientes procesos.

4.2.2.1.1. PO2 - Definición de la arquitectura de información

Objetivo: Satisfacer los requerimientos de la institución, organizando de la mejor manera posible los sistemas de información, a través de la creación y mantenimiento de un modelo de información de negocio.

- 2.1. Modelo de la arquitectura de información: Se refiere a que la información debe conservar consistencia con las necesidades y debe ser identificada, capturada y comuni8cada para llevar a cabo las tareas eficientemente.
- 2.2. Diccionario de datos y reglas de sintaxis de datos de la corporación: Es necesario que exista en la institución un diccionario de datos, que este continuamente actualizado y que muestre como es la sintaxis de los datos del hospital.
- 2.3. Esquema de clasificación de datos: En la institución se debe establecer un marco de referencia de los datos, clasificándolos por categorías, y con la definición de normas y políticas de acceso a dichos datos.
- 2.4. Niveles de Seguridad: La gerencia del hospital debe definir niveles de seguridad para cada clasificación de datos que exista.

4.2.2.1.2. PO8 - Asegurar el cumplimiento de los requerimientos externos

Objetivo: Cumplir con obligaciones legales, regulatorias y contractuales, donde es necesario identificar y analizar los requerimientos externos de las TI.

- 8.1. Revisión de requerimientos externos:
  La institución debe establecer los requerimientos externos de acuerdo a los marcos legales establecidos por entidades gubernamentales.
- 8.2. Prácticas y procedimientos para el cumplimiento de requerimientos externos: Se debe garantizar el cumplimiento de las prácticas y procedimientos de los requerimientos externos.
- 8.3. Cumplimiento de seguridad y ergonomía: En la institución debe existir el cumplimiento de estándares ergonómicos y de seguridad en el ambiente de trabajo.
- 8.4. Privacidad, propiedad intelectual y flujos de datos y flujo de datos:
  La gerencia de la institución debe garantizar el cumplimiento de la privacidad, la confidencialidad, y propiedad intelectual.
- 8.5. Comercio Electrónico: En caso de que se realicen operaciones de intercambio en Internet, la institución debe garantizar la integridad a través de la implementación de políticas de seguridad en este aspecto.
- 8.6. Cumplimiento con los contratos de seguros: Para el hospital es de gran importancia que existan políticas de aseguramiento de software.

4.2.2.1.3. PO9 - Evaluación de riesgos

Objetivo: Asegurar el logro de los objetivos de TI y responder a las amenazas hacia la provisión de servicios de TI.

- 9.1. Evaluación de riesgos del negocio: Establecer una marco de referencia, de evaluación sistemática de riesgos, es necesario hacer un seguimiento a los riesgos utilizando los resultados de auditorías, inspecciones e incidentes identificados.
- 9.2. Enfoque de evaluación de riesgos: Escoger una metodología adoptada para la evaluación de riesgos.
- 9.3. Identificación de Riesgos: El análisis se debe enfocar a los elementos esenciales de riesgo.
- 9.4. Medición de Riesgos: Determinar cualitativamente y cuantitativamente, que tan alto es el riesgo.

- 9.5. Plan de acción contra riesgos: Definir un plan de acción contra riesgos para asegurar que existan controles, y establecer medidas económicas.
- 9.6. Aceptación de riesgos: Asegurar la aceptación formal del riesgo residual, y comunicarlo para que se acepte formalmente.

4.2.2.1.4. PO11- Administración de calidad

Objetivo: Satisfacer los requerimientos del cliente, a través de planeación, implementación y mantenimiento de estándares y sistemas de calidad.

- 11.1. Plan general de calidad: Debe existir un plan general de calidad (norma o política dentro del hospital).
- 11.2. Enfoque de aseguramiento de calidad: Se debe establecer en la institución un enfoque estándar de aseguramiento de calidad, donde se certifique que se hacen auditorías y revisiones.
- 11.3. Planeación del aseguramiento de calidad: Implementar un proceso de planeación, que indique el alcance y la duración de las actividades, para que garanticen la calidad.
- 11.4. Revisión del aseguramiento de la calidad sobre el cumplimiento de estándares y procedimientos de la función de servicios de información, dentro de la funciones del personal encargado de revisar la calidad, estará la revisión de los estándares de calidad.
- 11.5. Metodología del ciclo de vida de desarrollo de sistemas: La organización debe definir estándares de sistemas, y una metodología del ciclo de vida para el software en las diferentes fases como implementación e implantación entre otras.
- 11.6. Metodología del ciclo de vida de desarrollo de sistemas para cambios mayores a la tecnología actual: La gerencia de la institución, debe asegurar que se cumpla la metodología del ciclo de vida escogido, en caso de que surjan cambios.

- 11.7. Actualización de la metodología del ciclo de vida de desarrollo de sistemas: Se deben hacer revisiones de las metodologías, para garantizar que estén actualizadas.
- 11.8. Coordinación y comunicación: Se debe garantizar una buena comunicación entre los clientes o usuarios y los implementadotes del sistema.
- 11.9. Marco de referencia de adquisición y mantenimiento para la infraestructura de tecnología.
- 11.10. Relaciones con terceras partes como implementadores: Dentro de la institución deben existir políticas que garanticen las buenas relaciones con terceros y debe existir buena comunicación.
- 11.11. Estándares para la documentación de programas: Dentro del ciclo de vida de desarrollo de sistemas se deben incluir estándares, que hayan sido comunicados anteriormente.
- 11.12. Estándares para pruebas de programas: Dentro del ciclo de vida de desarrollo de sistemas se deben incluir estándares de prueba, verificación de software entre otros.
- 11.14. Pruebas piloto/en paralelo: Se debe especificar las condiciones con las que se realizaran las pruebas en paralelo y piloto.
- 11.15. Documentación de las pruebas del sistema: Dentro el proyecto de desarrollo del módulo de historia clínica se deberá disponer d la documentación de los resultados de pruebas.
- 11.16. Evaluación del aseguramiento de la calidad sobre el cumplimiento de estándares de desarrollo: Dentro del proceso de calidad para el hospital se debe incluir pruebas de post-implementación del módulo.
- 11.17. Revisión del aseguramiento de calidad sobre el logro de los objetivos de la función de servicios de información: Revisión del cumplimiento e los objetivos de los servicios de información.
- 11.18. Métricas de calidad: La gerencia del hospital y dentro de su proceso de acreditación, debe evaluar si los objetivos de calidad para el módulo, han sido cumplidos.

- 11.19. Reportes de revisiones de aseguramiento de calidad: Se deben enviar los reportes de revisión de calidad a la de gerencia y usuarios.

4.2.2.2. Dominio 2 - Adquisición e implementación (AI)

Para llevar a cabo la estrategia de TI, las soluciones de TI deben ser identificadas, desarrolladas o adquiridas, así como implementadas e integradas dentro del proceso de la institución, además este dominio cubre los cambios y el mantenimiento realizados al módulo, este dominio incluye los siguientes procesos:

4.2.2.2.1. AI2 - Adquisición y mantenimiento de software de aplicación

Objetivo: Asegurar el mejor enfoque para cumplir con los requerimientos del usuario, a través del análisis de las oportunidades alternativas, comparadas contra los requerimientos de los usuarios.

- 2.3. Aprobación del diseño: Se requiere que las especificaciones de diseño para el módulo de historia clínica, sean revisadas y aprobadas por el departamento encargado.
- 2.4. Definición y documentación de requerimientos de archivos: Asegurar la aplicación de un procedimiento apropiado para la documentación de los archivos y que se garantice el respeto a las reglas de diccionario de datos.
- 2.6. Diseño para la recopilación de datos fuente: Debe existir un mecanismo para la recopilación y entrada de datos.
- 2.7. Definición y documentación de requerimientos de entrada de datos: Garantizar que existan mecanismos adecuados para documentar los requerimientos de entrada.
- 2.8. Definición de interfaces: En el proceso de implantación del módulo se debe garantizar que se especifiquen, diseñen y documenten apropiadamente todas las interfases internas y externas del módulo de historia clínica.

- 2.9. Interfase usuario-máquina: El módulo de historia clínica debe presentar de una interfase entre el usuario y la máquina fácil de utilizar y que sea capaz de autodocumentarse (por medio de funciones de ayuda).
- 2.10. Definición y documentación de requerimientos de procesamiento: Dentro de los requerimientos de los usuarios del módulo de historia clínica, deben existir mecanismos adecuados para definir y documentar los requerimientos de procesamiento.
- 2.11. Definición y documentación de requerimientos de salida de datos: Deben existir mecanismos adecuados para definir y documentar los requerimientos de salida de datos en el caso de los reportes del módulo.
- 2.12. Controlabilidad: Garantizar mecanismos adecuados, para identificar los requerimientos de seguridad y control internos para el módulo de historia clínica, y que el aplicativo de igual manera refleje esos mecanismos de seguridad y control de los procesos.
- 2.13. Disponibilidad como factor clave de diseño: El módulo debe garantizar la disponibilidad y confiabilidad de funcionamiento, para sus usuarios.
- 2.14. Consideraciones de integridad de tecnología para software de programas de aplicación: La aplicación deberá garantizar medios para verificar tareas realizadas por los usuarios (médicos y enfermeras), con el fin de apoyar el aseguramiento de la integridad de los datos y se permita la restauración de la integridad a través de procedimientos de recuperación en reversa u otros medios.
- 2.15. Pruebas de software de aplicación: En el momento de la implantación del módulo, deberán aplicarse pruebas necesarios (unitarias, aplicación, integración y pruebas de carga y estrés, de acuerdo con el plan de prueba y los estándares de pruebas, antes de ser aprobado por el usuario. Igualmente aplicar pruebas de seguridad.

4.2.2.2.2. AI5 - Instalación y acreditación de sistemas

Objetivo: Verificar y confirmar que la solución sea adecuada para el propósito deseado. Para ello se realiza una migración de instalación, conversión y plan de aceptaciones adecuadamente formalizadas.

- 5.1. Entrenamiento: El personal encargado de administrar el módulo de historia clínica dentro del área de sistemas, deberán estar entrenados de acuerdo al plan de entrenamiento definido y los materiales relacionados, dentro del proceso de implementación o modificación de sistemas de información.
- 5.2. Adecuación del desempeño del software de aplicación: Debe existir una medición (optimización) del desempeño del software de aplicación, lo cual debe ser tenido en cuenta para cambios futuros dentro del módulo de historia clínica, para hacer los requerimientos a la empresa que presta el soporte al hospital.
- 5.4. Pruebas de Cambios: Se debe asegurar que los cambios sean probados por un grupo de prueba independiente (distinto al de los desarrolladores), antes de ponerse al servicio de lo usuarios, y se deben tener en cuenta las condiciones de seguridad y controles internos o políticas del Hospital.
- 5.5. Criterios y desempeño de pruebas en paralelo/ piloto: Deben establecerse procedimientos de pruebas de acuerdo a una metodología usada por el área encargada, y establecer tiempo y fechas de ejecución y terminación de los procesos.
- 5.6. Prueba de aceptación final: Debe existir una evaluación y aprobación formal de los resultados de las pruebas, abarcando todos los componentes del sistema de información.
- 5.8. Prueba operacional: Antes de poner en operación el módulo de historia clínica, deberá ser operado y validado por sus usuarios finales, en iguales condiciones a las que ellos operan.

- 5.9. Paso a producción: Se debe definir procesos para controlar la entrega del sistema en el momento de pruebas y en el momento de operación, ambos ambientes deben separarse y protegerse.
- 5.10. Evaluación de la satisfacción de los requerimientos del usuario: Terminado el proceso de implantación, deben realizarse una revisión post - implementación de los requerimientos del módulo, teniendo en cuenta: capacidad, desempeño de procesamiento, entre otros, con el fin de evaluar si las necesidades del usuario están siendo satisfechas por el mismo.
- 5.11. Revisión gerencial post – implementación: Se debe realizar una revisión post - implementación del sistema de información, donde se evalué y se reporte si el sistema proporcionó los beneficios esperados de la manera más económica.

4.2.2.2.3. AI6 - Administración de cambios

Objetivo: Minimizar la probabilidad de interrupciones, alteraciones no autorizadas y errores. Esto se hace posible a través de un sistema de administración que permita el análisis, implementación y seguimiento de todos los cambios requeridos y llevados a cabo a la infraestructura de TI actual.

- 6.2. Evaluación del impacto: En el caso de surgir un cambio este debe ser analizado y autorizado.
- 6.3. Control de cambios: La administración de cambios y el control del software deben ser integrados, supliendo las necesidades de administración y configuración.
- 6.4. Documentación y procedimientos: Cada vez que se realice un cambio o actualización en el módulo, debe quedar documentado de manera correspondiente.
- 6.5. Mantenimiento autorizado: La institución debe asegurar que el personal que presta soporte y mantenimiento al módulo, sea

monitoreado apropiadamente, en relación a sus derechos de acceso al sistema, para evitar riesgos de accesos no autorizados.

4.2.2.3. Dominio 3 - Entrega de servicios y soporte (DS)

En este dominio se hace referencia a la entrega de los servicios requeridos, que abarca desde las operaciones tradicionales hasta el entrenamiento, pasando por seguridad y aspectos de continuidad. Con el fin de proveer servicios, deberán establecerse los procesos de soporte necesarios. Este dominio incluye el procesamiento de los datos por sistemas de aplicación, frecuentemente clasificados como controles de aplicación, de este dominio se han tomado los siguientes procesos:

4.2.2.3.1. DS2 - Administración De Servicios Prestados Por Terceros

Objetivo: Asegurar que las tareas y responsabilidades de las terceras partes estén claramente definidas, que cumplan y continúen satisfaciendo los requerimientos.

Para ello se establecen medidas de control dirigidas a la revisión y monitoreo de contratos y procedimientos existentes, en cuanto a su efectividad y suficiencia, con respecto a las políticas de la organización.

- 2.1. Interfases con proveedores: Se debe asegurar que todos los servicios prestados por terceros sean propiamente identificados y que las interfaces técnicas y organizacionales con los proveedores sean documentadas.
- 2.2. Relaciones de dueños: Se debe establecer o designar un dueño del software, que sea responsable de asegurar la calidad de las relaciones con terceros.
- 2.3. Contratos con terceros: Se deben definir procedimientos específicos para asegurar que un contrato formal sea definido y acordado para cada relación de servicio con SYAC que es el proveedor del software.

- 2.4. Calificación de terceros: Se debe asegurar que la empresa proveedora del software, cumpla con los estándares requeridos para la prestación del servicio.
- 2.6. Continuidad de servicios: Con respecto al aseguramiento de la continuidad de los servicios, se debe considerar el riesgo de incertidumbre legal, y el interés de continuidad de los procesos del módulo de historia clínica.
- 2.7. Relaciones de seguridad: Con respecto a las relaciones con el proveedor del software de servicios, se deberá asegurar que los acuerdos de seguridad (por ejemplo, los acuerdos de no-revelación) sean identificados, declarados explícitamente y acordados, que éstos concuerden con los estándares de negocios universales y estén en línea con los requerimientos legales y regulatorios, incluyendo obligaciones.
- 2.8. Monitoreo: Establecer un proceso continuo de monitoreo sobre la prestación de servicio de terceros, con el fin de asegurar el cumplimiento de los acuerdos del contrato.

4.2.2.3.2. DS3 - Administración de desempeño y capacidad

Objetivo: Asegurar que la capacidad adecuada está disponible y que se esté haciendo el mejor uso de ella para alcanzar el desempeño deseado. Para ello se realizan controles de manejo de capacidad y desempeño que recopilen datos y reporten acerca del manejo de cargas de trabajo, tamaño de aplicaciones, manejo y demanda de recursos.

- 3.1. Requerimientos de disponibilidad y desempeño: Identificar las necesidades para ser convertidas en requerimientos, en términos de disponibilidad.
- 3.2. Plan de disponibilidad: Establecer un plan de disponibilidad para alcanzar, monitorear y controlar la disponibilidad de los servicios de información.
- 3.3. Monitoreo y reporte: Implementación de un proceso que asegure que el desempeño de los recursos de tecnología de información sea

continuamente monitoreado y que las excepciones sean reportadas de manera oportuna y completa.

- 3.4. Herramientas de modelado: Asegurar que se utilicen las herramientas de modelado apropiadas para producir un modelo del sistema actual, calibrado y ajustado según la carga de trabajo real. Las herramientas de modelado deberán utilizarse para apoyar el pronóstico de los requerimientos de capacidad, confiabilidad de la configuración, desempeño y disponibilidad. Deberán llevarse a cabo investigaciones técnicas profundas sobre el hardware de los sistemas y deberán incluirse pronósticos acerca de futuras tecnologías.
- 3.5. Manejo proactivo del desempeño: El proceso de administración del desempeño deberá incluir la capacidad de pronóstico para permitir que los problemas sean solucionados antes de que éstos afecten el desempeño del sistema. Deberán llevarse a cabo análisis de las fallas e irregularidades del sistema en cuanto a frecuencia, grado del impacto y magnitud del daño.
- 3.6. Pronóstico de carga de trabajo: Deberán establecerse controles para asegurar que se preparen pronósticos de carga de trabajo con el fin de identificar tendencias y proporcionar la información necesaria para el plan de capacidad.
- 3.8. Disponibilidad de recursos: Prevenir que se pierda la disponibilidad de los recursos, mediante la implementación de mecanismos de tolerancia de fallas, mecanismos de asignación equitativa de recursos y la definición de prioridades de tareas.

4.2.2.3.3. DS5 - Garantizar la seguridad de sistemas

Objetivo: salvaguardar la información contra uso no autorizados, divulgación, modificación, daño o pérdida. Para ello se realizan controles de acceso lógico que aseguren que el acceso a sistemas, datos y programas está restringido a usuarios autorizados.

- 5.1. Administrar medidas de seguridad: Administrar medidas de seguridad de acuerdo a los requerimientos de la institución, esto incluye:

    - Traducir información sobre evaluación de riesgos a los planes de seguridad de tecnología;
    - Implementar el plan de seguridad de tecnología de información.
    - Actualizar el plan de seguridad de tecnología de información.
    - Evaluar el impacto de solicitudes de cambio en la seguridad de tecnología de información;
    - Monitorear la implementación del plan de seguridad de tecnología de información.
- 5.2. Identificación, autenticación y acceso: Implementación de mecanismos de seguridad, para el acceso de lógico de los usuarios al módulo y sus recursos, usar mecanismos de autenticación de usuarios, en relación a conexiones telefónicas, redes, entre otros accesos, de igual manera garantizar el mantenimiento de esto mecanismos, (cambios de periódicos de contraseñas).
- 5.3. Seguridad de acceso a datos en línea: En caso de operaciones en línea en el módulo de historia clínica, se deberá implementar procedimiento según las normas de seguridad de acceso de la institución.
- 5.4. Administración de cuentas de usuario: Dentro del módulo de historia clínica, debe existir un procedimiento que administre las cuentas de usuarios en caso de: requisición, establecimiento, emisión, y suspensión de cuentas de usuario.
- 5.5. Revisión gerencial de cuentas de usuario: Garantizar revisiones periódicas sobre las cuentas y derechos de acceso.
- 5.6. Control de usuarios sobre cuentas de usuario: Garantizar que los usuarios controlen sus propias cuentas de acceso, igualmente supervisarlo y alertarlos sobre el manejo de sus cuentas.

- 5.7. Vigilancia de seguridad: Asegurar que las actividades de seguridad sean llevadas en un registro y en caso de violación, verificar que han sido notificadas al personal correspondiente.
- 5.8. Clasificación de datos: Clasificar los datos, mediante decisión formal de su dueño o responsable.
- 5.9. Clasificación de datos: Deben existir controles para asegurar que el acceso de los usuarios y los derechos de acceso, son administrados de forma única y global.
- 5.10. Reportes de violación y de actividades de seguridad: Las violaciones de los mecanismos de seguridad deben ser registradas, reportadas, revisadas y escaladas constantemente.
- 5.11. Manejo de incidentes: Implementar procedimientos para atender casos de incidentes, mediante el uso de una plataforma centralizada con suficiente experiencia y equipada con instalaciones de comunicación rápidas y seguras. Igualmente establecer las responsabilidades y procedimientos, para el manejo de incidentes.
- 5.14. Autorización de transacciones: Existan políticas que aseguren que existan controles en donde sea necesario, para proporcionar autenticidad de transacciones a través de criptografía para “firmar” y verificar transacciones.
- 5.16. Sendero seguro: Asegurar que la información de transacciones (datos, password, llaves criptográficas) es enviada y recibida por canales confiables (trusted paths), mediante encriptamiento de sistemas y usuarios.
- 5.17. Protección de funciones de seguridad: El software y hardware relacionado con el módulo de historia clínica, debe estar protegido contra cualquier intromisión.
- 5.19. Prevención, detección y corrección de software “malicioso”: Garantizar procedimientos para el manejo y corrección de problemas ocasionados por software malicioso generalmente en el caso de virus.

- 5.20. Arquitectura de firewalls y conexión a redes públicas: En la institución al existir conexión a la red de Internet, se deben implementar firewalls, para proteger los recursos informáticos.
- 5.21. Protección de valores electrónicos: Garantizar la protección de las tarjetas o dispositivos físicos similares, que son utilizados para autenticación o almacenamiento de información financiera u otra información sensitiva.

4.2.2.3.4. DS7 - Educación y entrenamiento de usuarios

Objetivo: Asegurar que los usuarios estén haciendo un uso efectivo de la tecnología y estén conscientes de los riesgos y responsabilidades involucrados Para ello se realiza un plan completo de entrenamiento y desarrollo.

- 7.1. Identificación de necesidades de entrenamiento: Implementar procedimientos junto con el plan a largo plazo, para entrenar al personal de la Institución, frente a las necesidades que surjan sobre el manejo del módulo de historia clínica.
- 7.2. Organización del entrenamiento: De acuerdo a las necesidades identificadas en el personal, se deben asignar entrenadores y sesiones de entrenamiento, para capacitar al recurso humano.
- 7.3. Entrenamiento sobre principios y conciencia de seguridad: Se deben brindar capacitaciones de conducta ética de la función de servicios de información y principios de seguridad de sistemas, para que todo el personal este debidamente entrenado, y sepan que hacer en situaciones propias de estas temáticas.

3.2.2.3.5. DS9 - Administración de la configuración

Objetivo: Dar cuenta de todos los componentes de TI, prevenir alteraciones no autorizadas, verificar la existencia física y proporcionar una base para el sano manejo de cambios. Para ello se realizan controles que identifiquen y registren todos los activos de TI así como su localización física y un programa regular de verificación que confirme su existencia.

- 9.1. Registro de la configuración: Deben existir procedimientos para hacer seguimiento a los cambios realizados en la configuración, se llevara un registro en bitácoras y el control deberá ser una parte integrada del sistema de registro de la configuración y sus modificaciones.
- 9.2. Configuración base: Debe existir una configuración base para regresar, en el momento de cambios.
- 9.3. Registro de estatus: Asegurar que los registros de las configuraciones reflejen el estatus real de los elementos de la configuración y sus cambios.
- 9.4. Control de la configuración: Garantizar que existan revisiones periódicas de registro de configuraciones.
- 9.5. Software no autorizado: Realizar revisiones constantes a todos los equipos de la Institución, con el fin de verificar que no exista software no autorizado instalado en los PC del personal del hospital.
- 9.6. Almacenamiento de software: Debe existir un área de almacenamiento de archivos (biblioteca), estas áreas deberán estar separadas unas de otras y de las áreas de almacenamiento de archivos de desarrollo, pruebas y producción.

4.2.2.4. Dominio 4 – monitoreo (M)

Los procesos del hospital universitario departamental de Nariño necesitan ser evaluados regularmente a través del tiempo para verificar su calidad y suficiencia en cuanto a los requerimientos de control, integridad y confidencialidad, de este dominio se incluido el siguiente proceso:

4.2.2.4.1. M2 - Evaluar lo adecuado del control interno

Objetivo: Incrementar los niveles de confianza entre el hospital, usuarios y proveedores externos. Este proceso se lleva a cabo a intervalos regulares de tiempo.

- 2.1. Monitoreo de control interno: Monitorear que tan efectivos son los controles internos, aplicados las actividades relacionadas al módulo, con el fin de tomar correctivos.
- 2.2. Operación oportuna de controles internos: Verificar si los resultados de los controles, son reportados y analizados rápidamente, para evitar errores e inconsistencias y que estos son corregidos a tiempo.
- 2.4. Seguridad de operación y aseguramiento de control interno: La seguridad operacional y los controle internos, deben ser señalados por una auditoría independiente para examinar si están operando de forma adecuada y se identifiquen puntos vulnerables y problemas de seguridad.

4.2.3. Proceso de recolección de información y planteamiento de actividades

Para iniciar con el desarrollo de la auditoría es necesario partir del planteamiento de los c*uadros de definición de fuente de conocimiento*, mediante este planteamiento se logra establecer las fuentes de conocimientos, es decir cual es la documentación, política, manual, entrevista o procedimiento requerido para poder evaluar un determinado proceso, una vez establecido el medio de estudio, se plantea las pruebas de análisis y de ejecución que se debe realizar con el material sugerido.

A continuación se muestra un ejemplo para el dominio de planeación y organización (PO), en el proceso definición de la arquitectura de información (PO2).

Tipo de Registro: Cuadro de Definición de Fuentes de Conocimiento, Pruebas de Análisis y Pruebas de Auditoría.

ENTIDAD AUDITADA:	Hospital Universitario Departamental de Nariño		
AREA AUDITADA:	Módulo de Historia clínica	**SISTEMA:**	Dinámica Gerencial
RESPONSABLES:	Jenny Burgos García y Maria Carolina Domínguez		

Descripción de Actividad/Prueba: Satisfacer los requerimientos de la institución, organizando de la mejor manera posible los sistemas de información, a través de la creación y mantenimiento de un modelo de información de negocio.

MATERIAL DE SOPORTE: COBIT

DOMINIO:	PLANEACIÓN Y ORGANIZACIÓN (PO)	**PROCESO:**	Definición de la Arquitectura de Información: (PO2)

FUENTES DE CONOCIMIENTO	**REPOSITORIO DE PRUEBAS APLICABLES**	
	DE ANÁLISIS	**DE EJECUCIÓN**
• Entrevista al Coordinador del área de sistemas. • Entrevista a Ingenieros de soporte empresa SYAC. • Entrevista a Interventores. • Entrevista a Ingenieros Área de Sistemas. • Manual de Sistemas. • Políticas y procedimientos sobre la arquitectura de información. • Modelo de arquitectura de información (incluyendo documentación de soporte del Modelo de datos corporativos). • Verificar los objetivos y planes (hardware disponible y la arquitectura del módulo). • Diccionario de Datos de la Institución • Políticas o procedimientos especificando la propiedad de datos y su clasificación de acuerdo a la seguridad e importancia de los mismos. • Archivo físico del soporte prestado por SYAC. • Reporte de status y minutas (actas de reunión y reportes) • Contrato con SYAC.	• Análisis del Manual del Sistema Módulo de Historia clínica electrónica,. • Analizar el modelo de arquitectura de información. • Análisis del Modelo y Diccionario de Datos del Módulo de Historia clínica Electrónica,. • Análisis de las políticas de propiedad de los datos de Historia clínica: Clasificación (Públicos, privados, secretos), Niveles Acceso (controles de Protección). • Analizar los objetivos y planes de la institución a corto y largo plazo, verificando su correspondencia en el modelo de Arquitectura de Información. • Análisis de Roles y Responsabilidades de la Información. en Historia clínica Electrónica, (Quien tiene acceso, quien determina el nivel de acceso, requerimientos especiales de acceso?) • Análisis de las políticas y procedimientos para garantizar la integridad y consistencia de los datos.	• Benchmarking entre el modelo de datos de Historia clínica Electrónica, y Otros Similares de la industria. • Revisión detallada del diccionario de datos, comparado con la base de datos en producción. • Revisión detallada del modelo de Arquitectura. • Revisión detallada de los niveles de seguridad en producción contra los definidos en las políticas y procedimientos. • Obtención de Inconsistencias del modelo de datos. • Obtención de datos obsoletos e inapropiados. • Obtención de datos cuya propiedad no este clara y apropiadamente determinada. • Niveles de Seguridad de datos inconsistentes o inapropiados.

Como se puede analizar en la figura anterior, en el recuadro de Fuentes de Conocimiento se plantea cuales son los documentos que se deben recolectar, y las entrevistas que se deben efectuar, conjuntamente se especifican las pruebas de análisis y de ejecución a realizarse con el material recolectado.

Una vez establecida la estructura a seguir para el estudio del proceso, se continúa con el planteamiento del *cuestionario cuantitativo*, el cual nos muestra una serie de preguntas realizadas en base al planteamiento del Cuadro de definición de fuente de conocimiento, y nos especifica la persona a la cual va dirigida cada pregunta, existen tres opciones de respuestas: SI, NO o NA (no aplica).

El cuestionario nos permite medir o calificar el proceso, para ello es necesario dar un puntaje máximo entre 1 y 5 a cada pregunta, de acuerdo a su nivel de importancia según criterio, la sumatoria del puntaje de todas las preguntas nos da el total de la encuesta, luego se prosigue a calificar la columna del SI, sumando el puntaje de sus preguntas, y las columnas del NO Y NA.

Después de cuantificar la encuesta, se analiza la columna del NO, se verifica si su resultado es alto, medio o bajo y con esto se formula las conclusiones respectivas, es necesario que conjuntamente se trabaje en la obtención de pruebas que permitan ratificar los resultados de la encuesta, para esto es necesario diseñar un p*lan de pruebas,* que nos indique el tipo de prueba a realizar en cada uno de los objetivos de control planteados en el programa de auditoría, y no brinde los mecanismos y herramientas que se utilizaran para su desarrollo. Una vez terminado el seguimiento a cada pregunta se determinan los hallazgos encontrados, para proseguir al planteamiento de las recomendaciones respectivas, a continuación se muestra el cuestionario cuantitativo para el ejemplo a seguir.

Tipo de Registro: Cuestionario cuantitativo.			
ENTIDAD AUDITADA:	Hospital universitario departamental de Nariño		
AREA AUDITADA:	Módulo de Historia clínica	**SISTEMA:**	Dinámica Gerencial
RESPONSABLES:	Jenny Burgos García y Maria Carolina Domínguez		
MATERIAL DE SOPORTE: COBIT			
DOMINIO:	Planeación y Organización (PO)	**PROCESO:**	Definición de la Arquitectura de Información: (PO2)

PREGUNTA	SI	NO	NA	FUENTE
1. ¿Existe un manual de sistema (técnico) para el módulo de historia clínica electrónica?		4		Entrevista al Representante de SYAC Entrevistas a ingenieros/ área de sistemas
2. El manual de sistema contiene:				Revisión del manual de sistema de historia clínica.
• Requerimientos de software y hardware para su funcionamiento.		4		
• Descripción de la configuración.	4			
• Descripción y catalogo de formas.	4			
• Descripción de operación de cada botón y elementos del módulo.	4			
• Diagramas de flujo de datos o pseudocódigo o diagramas de flujo de las partes del módulo.		4		
• Descripción y catalogo de reportes.	4			
• Lista de archivos y especificaciones.		4		
• Escalabilidad e interacción con otros módulos.		4		
3. ¿El manual de sistema (técnico) de soporte del módulo es actualizado cada vez que se realizan cambios o actualizaciones?		4		Revisión del manual de historia clínica, ultimas versiones
4. ¿Existe algún procedimiento establecido para mantener actualizado el manual técnico de soporte del módulo?		4		Entrevista a representante de SYAC

5. ¿Existe el diccionario de datos?	5			Entrevista a representante de SYAC
6. El diccionario de datos contiene:				Revisión del Diccionario de datos.
• Modelo entidad relación.	5			
-Tablas.	5			
- Relaciones.	5			
- Llaves.	5			

PREGUNTA	SI	NO	NA	FUENTE
▪ El modelo lógico de la base de datos (descripción de los elementos de la base de datos, como tabla: descripción, campos, longitud, descripción del campo, valores por defecto, condiciones entre otros)	**5**			Revisión del Diccionario de datos.
▪ Descripción del personal encargado de la función de dar mantenimiento del diccionario de datos.		5		
▪ Clasificación de usuarios, niveles de acceso y restricciones.		5		
▪ Roles y privilegios.		5		
7. ¿Le ha sido entregado al personal del área de sistemas encargado del manejo del módulo de historia clínica, el diccionario de datos relacionado con el módulo de historia clínica?		5		Entrevistas Ingenieros del área de sistemas.
8. ¿El diccionario de datos se actualiza cada vez que se realizan cambios o actualizaciones al módulo de historia clínica?	**5**			Entrevista al representante de SYAC. Diccionario de datos, verificación de fecha de actualización.
9. ¿Se ha establecido un procedimiento para mantener actualizado el diccionario de datos?		**5**		Entrevista al representante de SYAC.
10 ¿Existe un modelo de arquitectura de información?		4		Entrevista al representante de SYAC.
11. ¿Existen políticas y procedimiento en relación al modelo de arquitectura de información?		4		Entrevista al representante de SYAC.
12. El modelo de arquitectura de información tiene en cuenta: ▪ Identificación de entradas.		4		Revisión de la documentación del modelo de arquitectura de Información del módulo de historia clínica.
▪ Identificación de procesos.		4		
▪ Identificación de sitios de almacenamiento (base de datos).		4		
▪ Identificación de reportes.		4		
▪ Identificación de la interacción con otros sistemas.		4		
▪ Diseño de interacción de los elementos e identidades del módulo.		4		
▪ Definición de usuarios finales.		4		
▪ Requerimientos de las diferentes Instituciones.		4		
▪ Los planes de la gerencia a corto y largo plazo.		4		
▪ Costos, riesgos y aprobaciones para hacer modificaciones al modelo.		4		
13. ¿El modelo de arquitectura de información del módulo de historia clínica, ha sido dado a conocer al personal del área de sistemas del Hospital Universitario departamental de Nariño?		4		Entrevista al representante de SYAC. Entrevista a Ingenieros del área de sistemas a cargo del módulo de historia clínica.
14. ¿Existe la definición de políticas de auditoría y control?	4			Entrevista al Coordinador del área de sistemas. Revisión del documento de definición de políticas de auditoría y control.

PREGUNTA	SI	NO	NA	FUENTE
15. Las definición de las políticas de auditoría y control están establecidas para:				Documento de definición de políticas de auditoría y control. Comprobación del contenido del documento de la definición de políticas de auditoría y control.
▪ Accesos a la información.		4		
▪ Accesos al sistema de información.		4		
▪ Cambios a los datos.		4		
▪ Cambios a la configuración.		4		
▪ Comprobación de la aplicación de la normatividad.		4		
▪ Comprobación de procedimientos automatizados (formulación).		4		
16. ¿Se ha realizado una clasificación formal de los datos, de acuerdo a criterios de propiedad y niveles de importancia?	3			Entrevista al Coordinador del área de sistemas
17. ¿Existen políticas y procedimientos para la clasificación de los datos?		3		Entrevista al Coordinador del área de sistemas
18. Dentro de las políticas y procedimientos que permiten la clasificación de los datos se incluye:				Revisión de las políticas y procedimientos para la clasificación de los datos.
▪ Categorías de seguridad.		3		
▪ Propiedad de los datos.		3		
- Datos públicos.		3		
- Datos Privados.		3		
- Datos Secretos.		3		
▪ Estándares de clasificación “Default”, para los activos de datos que no contienen un identificador de clasificación.		3		
19. ¿Existe una oficina encargada de definir e implementar las políticas y procedimientos de la función de los servicios informáticos?	4			Entrevista al Coordinador del área Revisión del documento que contiene las funciones, procesos y procedimientos del area de sistemas
20. Las políticas y procedimientos de la función de los servicios informáticos incluye:				Verificación del contenido de las funciones, procesos y procedimientos de la oficina de sistemas
▪ Niveles de seguridad definidos para cada clasificación de datos.		3		
▪ Niveles de acceso definidos y apropiados para la clasificación de los datos.		3		
21. ¿Existen informes del soporte prestado por SYAC?	3			Entrevista Ingenieros a cargo del módulo. Revisión de los informes del soporte prestado por SYAC.
22. Los informes del soporte prestado por SYAC se encuentran clasificados en:				Reportes de requerimientos solucionados por SYAC Revisión de la clasificación de los requerimientos solucionados por SYAC
▪ Requerimientos de usuarios finales.	3			
▪ Requerimientos de capacitaciones.	3			

PREGUNTA	SI	NO	NA	*FUENTE*
23.Los soportes físicos del soporte prestado por SYAC contiene:				*Comprobación del contenido de los reportes de requerimientos solucionados solicitados a SYAC*
▪ Fecha, hora, persona que hace la solicitud.	3			
▪ Descripción del problema o inconveniente presentado.	3			
▪ Fecha, hora, persona que atiende el requerimiento.	3			
▪ Descripción de la solución del problema o inconveniente presentado.	3			
▪ Espacio para anotación de pruebas.	3			
▪ Espacio para inclusión de anexos.	3			
24. ¿El soporte que presta SYAC está contenido dentro del contrato y se planifica al inicio de la ejecución del mismo indicadores que permitan demostrar su cumplimiento?	3			*Verificación del contrato de outsourcing entre SYAC y el Hospital Departamental Revisión de los requerimientos negados o solucionados por SYAC determinar si se encuentran o no contemplados en lo contratado*
TOTALES	***89***	***156***		
	89/245	**156/245**		
TOTAL ENCUESTA	***245***			

Dentro del cuestionario cuantitativo se busca analizar el porcentaje de riesgo es cual es equivalente a:

% de Riesgo = $\frac{\text{Puntaje casilla SI} * 100}{\text{Total Encuesta – Puntaje casilla NA}}$ para el ejercicio tenemos: $\frac{89*100}{245-0} = 36\%$

De acuerdo al MECCI la categorización asignada para determinar el nivel de riesgo es:

1% -30% = Riesgo Bajo

31% - 70% = Riesgo Medio

71% - 100% = Riesgo Alto

Es así que el riesgo asignado para el proceso es medio.

A continuación se anexa los cuadros de definición de fuentes de conocimiento y los cuestionarios de cuantitativos realizados para el programa de auditoria de este proyecto.

Cuadros de definición de fuentes de conocimiento

Tipo de Registro: Cuadro de definición de fuentes de conocimiento, pruebas de análisis y pruebas de auditoría.			
ENTIDAD AUDITADA:	Hospital Universitario Departamental de Nariño		
AREA AUDITADA:	Módulo de Historia Clínica	**SISTEMA:**	Dinámica Gerencial
RESPONSABLES:	Jenny Burgos García y Maria Carolina Domínguez		
Descripción de Actividad/Prueba: Satisfacer los requerimientos de la institución, organizando de la mejor manera posible los sistemas de información, a través de la creación y mantenimiento de un modelo de información de negocio.			
MATERIAL DE SOPORTE: COBIT			
DOMINIO:	PLANEACIÓN Y ORGANIZACIÓN (PO)	**PROCESO:**	Definición de la Arquitectura de Información: (PO2)

FUENTES DE CONOCIMIENTO	**REPOSITORIO DE PRUEBAS APLICABLES**	
	DE ANÁLISIS	**DE EJECUCIÓN**
• Entrevista al Coordinador del área de sistemas. • Entrevista a Ingenieros de soporte de la empresa SYAC. • Entrevista a Interventores. • Entrevista a Ingenieros del área de Sistemas. • Manual de Sistemas. • Políticas y procedimientos sobre la arquitectura de información. • Modelo de arquitectura de información (incluyendo documentación de soporte del Modelo de datos corporativo). • Verificar los objetivos y planes (hardware disponible y la arquitectura del módulo). • Diccionario de datos de la Institución • Políticas o procedimientos especificando la propiedad de datos y su clasificación de acuerdo a la seguridad e importancia de los mismos.	• Análisis del manual del sistema del módulo de Historia Clínica electrónica. • Analizar el modelo de arquitectura de información. • Análisis del modelo y diccionario de datos del módulo de historia clínica electrónica. • Análisis de las políticas de propiedad de los datos de historia clínica: clasificación (públicos, privados, secretos), niveles acceso (controles de protección). • Analizar los objetivos y planes de la institución a corto y largo plazo, verificando su correspondencia en el modelo de arquitectura de Información.	• Benchmarking entre el modelo de datos de historia clínica electrónica y otros similares de la industria. • Revisión detallada del diccionario de datos, comparado con la base de datos en producción. • Revisión detallada del modelo de arquitectura. • Revisión detallada de los niveles de seguridad en producción contra los definidos en las políticas y procedimientos. • Obtención de Inconsistencias del modelo de datos. • Obtención de datos obsoletos e inapropiados.

FUENTES DE CONOCIMIENTO	REPOSITORIO DE PRUEBAS APLICABLES	
	DE ANÁLISIS	DE EJECUCIÓN
• Archivo físico del soporte prestado por SYAC. • Reporte de status y minutas (actas de reunión y reportes) • Contrato con SYAC.	• Análisis de roles y responsabilidades de la Información, en el diligenciamiento de historia clínica electrónica (quien tiene acceso, quien determina el nivel de acceso, requerimientos especiales de acceso). • Análisis de las políticas y procedimientos para garantizar la integridad y consistencia de los datos.	• Obtención de datos cuya propiedad no este clara y apropiadamente determinada. • Niveles de seguridad de datos inconsistentes o inapropiados.

Tipo de Registro: Cuadro de definición de fuentes de conocimiento, pruebas de análisis y pruebas de auditoría.

ENTIDAD AUDITADA:	Hospital Universitario Departamental de Nariño		
AREA AUDITADA:	Módulo de Historia Clínica	**SISTEMA:**	Dinámica Gerencial
RESPONSABLES:	Jenny Burgos García y Maria Carolina Domínguez		
MATERIAL DE SOPORTE: COBIT			
DOMINIO:	PLANEACIÓN Y ORGANIZACIÓN (PO)	**PROCESO:**	Asegurar el Cumplimiento de los Requerimientos Externos: (PO8)
Descripción de Actividad/Prueba: Cumplir con obligaciones legales, regulatorias y contractuales, donde es necesario identificar y analizar los requerimientos externos de las TI.			

FUENTES DE CONOCIMIENTO	**REPOSITORIO DE PRUEBAS APLICABLES**	
	DE ANÁLISIS	**DE EJECUCIÓN**
• Entrevista al Consejero legal. (Abogado del Hospital) • Entrevista a Funcionario de Recursos Humanos del Hospital. • Entrevista a coordinador del área de sistemas del Hospital (gerencia de los servicios de información). • Requerimientos externos: gubernamentales, leyes y normas en el campo de la salud, y con relaciones externas que tenga el hospital, para el módulo de historia clínica. • Normas de Privacidad. • Normas seguridad y salud (incluyendo ergonomía). • Clasificación de sensibilidad de datos ingresados, procesados, almacenados, producidos y transmitidos. • Seguros y copias de todos los contratos de seguros relacionados con la función de servicios de información. • Reportes de auditoría de auditores externos, en relación al módulo de Historia Clínica.	• Análisis de requerimientos externos, gubernamentales y con relaciones externas, los cuales deben estar acuatizados. • Análisis de las normas de seguridad, salud y ergonomía, en relación a módulo y sus usuarios. • Análisis de documentación de Auditorías externas. • Analizar si los procedimientos de seguridad van de acuerdo con todos los requerimientos legales. • Análisis de los contratos de seguros existentes en relación al software. • Análisis de normas y políticas de seguridad y salud en el hospital en relación al módulo de historia clínica.	• Benchmarking del cumplimiento de requerimientos externos, actividades y requerimientos de los contratos de seguros contra organizaciones similares. • Hacer una revisión detallada de los archivos de requerimientos externos, para garantizar su cumplimiento o que se están realizando acciones correctivas para implementarse. • Hacer una revisión detallada de los reportes de seguridad para evaluar si la información sensible/privada, está siendo protegida.

Tipo de Registro: Cuadro de definición de fuentes de conocimiento, pruebas de análisis y pruebas de auditoría.

ENTIDAD AUDITADA:	Hospital Universitario Departamental de Nariño		
AREA AUDITADA:	Módulo de Historia Clínica	**SISTEMA:**	Dinámica Gerencial
RESPONSABLES:	Jenny Burgos García y Maria Carolina Domínguez		
Descripción de Actividad/Prueba: Asegurar el logro de los objetivos de TI y responder a las amenazas hacia la provisión de servicios de TI.			
MATERIAL DE SOPORTE: COBIT			
DOMINIO:	PLANEACIÓN Y ORGANIZACIÓN (PO)	**PROCESO:**	Evaluación De Riesgos: (PO9)

FUENTES DE CONOCIMIENTO	**REPOSITORIO DE PRUEBAS APLICABLES**	
	DE ANÁLISIS	**DE EJECUCIÓN**
• Entrevista al coordinador del área de sistemas. • Entrevista a Ingenieros del área de sistemas. • Personal relacionado con la administración de riesgos (Interventores). • Usuarios claves (médicos-enfermeras). • Políticas y procedimientos de evaluación de riesgos en el módulo de historia clínica. • Documentos de evaluación de riesgos del negocio. • Documentos de evaluación de riesgos. • Detalles de la base sobre la cual se miden los riesgos y la exposición a los riesgos • Expedientes de personal escogido para la evaluación de riesgos. • Políticas de seguros que cubren el riesgo residual • Consulta de las bases de datos de administración de riesgos.	• Análisis de la documentación de la metodología de evaluación de riesgos. • Análisis de la documentación sobre la identificación de riesgos. • Análisis de plan de acción contra los riesgos identificados • Análisis de la cobertura de los seguros contra riesgos residuales.	• Benchmarking del marco referencial de evaluaciones de riesgos contra organizaciones similares o estándares internacionales. • Una revisión detallada del enfoque de evaluación de riesgos utilizado para identificar, medir y mitigar los riesgos a un nivel aceptable de riesgo residual.

Tipo de Registro: Cuadro de definición de fuentes de conocimiento, pruebas de análisis y pruebas de auditoría.

ENTIDAD AUDITADA:	Hospital Universitario Departamental de Nariño		
AREA AUDITADA:	Módulo de Historia Clínica	**SISTEMA:**	Dinámica Gerencial
RESPONSABLES:	Jenny Burgos García y Maria Carolina Domínguez		
Descripción de Actividad/Prueba: Satisfacer los requerimientos del cliente, a través de planeación, implementación y mantenimiento de estándares y sistemas de calidad.			
MATERIAL DE SOPORTE: COBIT			
DOMINIO:	PLANEACIÓN Y ORGANIZACIÓN (PO)	**PROCESO:**	Administración De Calidad: (PO11)

FUENTES DE CONOCIMIENTO	**REPOSITORIO DE PRUEBAS APLICABLES**	
	DE ANÁLISIS	**DE EJECUCIÓN**
• Entrevista al Coordinador del área de sistemas. • Entrevista a Ingenieros del área de sistemas encargados del manejo de seguridad del módulo. • Entrevista a Ingenieros de SYAC. • Políticas y procedimientos globales del hospital para el módulo, relacionados con el aseguramiento de la calidad. • Plan estratégico de la organización, política de calidad, manual de calidad y plan de calidad. • Organigramas de todas las funciones de aseguramiento de la calidad. • Minutas de las reuniones de planeación de la calidad. • Minutas de las reuniones para la revisión de la metodología del ciclo de vida del desarrollo de sistemas. • Copias de las revisiones a la metodología del ciclo de vida del desarrollo de sistemas.	• Análisis de las políticas de calidad del hospital. • Analizar si existe un enfoque estándar de aseguramiento de la calidad, y prescribe los tipos de actividades de aseguramiento de la calidad, como: revisiones, auditorías, inspecciones. • Analizar el plan de calidad de Hospital. • Analizar si se hacen revisiones de aseguramiento de la calidad, y evalúan el cumplimiento general de los estándares, políticas y procedimientos del hospital. • Analizar si existe una metodología del ciclo de vida de desarrollo de sistemas, y esta completo y actualizado.	• Benchmarking de la metodología del ciclo de vida del módulo de Historia Clínica con otros similares o estándares internacionales • Revisar en el plan de calidad, las medidas de desempeño, para probar si son alcanzables, satisfacen las expectativas y los requerimientos del hospital. • Revisar la documentación de la implementación del módulo para saber si cumple con: - Metodología del ciclo de vida de desarrollo de sistemas. - El módulo es escalable. - El módulo ha sido aprobado por los usuarios finales, personal de revisión de calidad entre otros, verificar si existen reportes de calidad.

FUENTES DE CONOCIMIENTO	REPOSITORIO DE PRUEBAS APLICABLES	
	DE ANÁLISIS	DE EJECUCIÓN
	• Analizar si la documentación de las especificaciones de entrada de datos concuerda con el diseño del formulario del módulo en cada área. • Analizar si existe documentación de interfaces internas y externas. • Analizar los requerimientos de control de aplicación para que garanticen: precisión, suficiencia, oportunidad, autorización de entradas y salidas de los médicos y enfermeras. • Analizar si existe un plan de pruebas del proyecto y un proceso de aprobación de usuario. • Analizar los manuales de soporte y referencia para usuarios. • Analizar si la metodología de ciclo de vida requiere hacer una evaluación de sensibilidad, y una evaluación de aspectos de seguridad.	Usuarios finales. - verificar la integridad de los datos. • Hacer una revisión detallada de la efectividad de: especificaciones de diseño, de entrada, de interfase usuario-maquina, de salida. • Hacer una revisión detallada de los estándares y la implementación de pruebas para el módulo. • Hacer una revisión detallada de la satisfacción del usuario con el módulo, sus reportes, manuales, etc. • Revisar en el módulo si las especificaciones usuario-maquina son fáciles de usar y puede autodocumentarse.

Tipo de Registro: Cuadro de Definición de Fuentes de Conocimiento, Pruebas de Análisis y Pruebas de Auditoría.

ENTIDAD AUDITADA:	Hospital Universitario Departamental de Nariño		
AREA AUDITADA:	Módulo de Historia Clínica	**SISTEMA:**	Dinámica Gerencial
RESPONSABLES:	Jenny Burgos García y Maria Carolina Domínguez		

Descripción de Actividad/Prueba: Asegurar el mejor enfoque para cumplir con los requerimientos del usuario, a través del análisis de las oportunidades alternativas, comparadas contra los requerimientos de los usuarios.

MATERIAL DE SOPORTE: COBIT

DOMINIO:	ADQUISICION E IMPLEMENTACION: AI	**PROCESO:**	Adquisición Y Mantenimiento De Software De Aplicación: (AI2)

FUENTES DE CONOCIMIENTO	**REPOSITORIO DE PRUEBAS APLICABLES**	
	DE ANÁLISIS	**DE EJECUCIÓN**
• Entrevista al Director del área de sistemas. • Entrevista a la presidencia de TI (Gerente). • Políticas y procedimientos relacionados con el ciclo de vida para el diseño de historias clínicas. • Objetivos y planes de la tecnología a corto y largo plazo. • Documentación de aprobaciones de diseños. • Documentos de requerimientos. • Documentos de especificaciones del programa. • Diseño de especificaciones de datos fuentes. • Definiciones de requerimientos de entrada. • Definiciones de requerimientos de salida. • Definiciones de requerimientos de procesamiento. • Interfaz de usuario – maquina. • Requerimientos de control interno y de seguridad • Requerimientos de disponibilidad para la integridad de la TI. • Plan de pruebas.	• Análisis si la participación del usuario en el ciclo de vida de desarrollo de sistemas es significativa. • Analizar si la metodología del ciclo de vida del desarrollo de historia clínica, involucra un proceso apropiado para el diseño del sistema, teniendo en cuenta: entrada, procesamiento, salida, controles internos, seguridad, control de cambios. • Analizar la metodología usada frente a cambios, que se hagan al módulo. • Analizar si los diseños de historia clínica fueron aprobados. • Analizar si la documentación del módulo y el diccionario de datos van de acuerdo a los estándares.	• Benchmarking de los costos de adquirir y desarrollar software de aplicación contra organizaciones similares o estándares. • Hacer una revisión detallada de: - Documentación del diseño del módulo, para verificar el cumplimiento de los requerimientos. - Documentación del software para asegurar que los requerimientos de archivo, son claros para los implementadores, en relación a: tablas, reportes, transacciones, controles, entre otros. • Analizar proyectos de desarrollo para: - Asegurar instrumentos de recopilación de datos fuente. - Identificar discrepancias técnicas, lógicas o de diseño. - Adecuación de acciones de seguridad y

FUENTES DE CONOCIMIENTO	REPOSITORIO DE PRUEBAS APLICABLES	
	DE ANÁLISIS	DE EJECUCIÓN
	• Analizar si la documentación de las especificaciones de entrada de datos concuerda con el diseño del formulario del módulo en cada área. • Analizar si existe documentación de interfaces internas y externas. • Analizar los requerimientos de control de aplicación para que garanticen: precisión, suficiencia, oportunidad, autorización de entradas y salidas de los médicos y enfermeras. • Analizar si existe un plan de pruebas del proyecto y un proceso de aprobación de usuario. • Analizar los manuales de soporte y referencia para usuarios. • Analizar si la metodología de ciclo de vida requiere hacer una evaluación de sensibilidad, y una evaluación de aspectos de seguridad.	Usuarios finales. - verificar la integridad de los datos. • Hacer una revisión detallada de la efectividad de: especificaciones de diseño, de entrada, de interfase usuario-maquina, de salida. • Hacer una revisión detallada de los estándares y la implementación de pruebas para el módulo. • Hacer una revisión detallada de la satisfacción del usuario con el módulo, sus reportes, manuales, etc. • Revisar en el módulo si las especificaciones usuario-maquina son fáciles de usar y puede autodocumentarse.

Tipo de Registro: Cuadro de definición de fuentes de conocimiento, pruebas de análisis y pruebas de auditoría.

ENTIDAD AUDITADA:	Hospital Universitario Departamental de Nariño		
AREA AUDITADA:	Módulo de Historia Clínica	**SISTEMA:**	Dinámica Gerencial
RESPONSABLES:	Jenny Burgos García y Maria Carolina Domínguez		
Descripción de Actividad/Prueba: Verificar y confirmar que la solución sea adecuada para el propósito deseado. Para ello se realiza una migración de instalación, conversión y plan de aceptaciones adecuadamente formalizadas.			
MATERIAL DE SOPORTE: COBIT			
DOMINIO:	ADQUISICION E IMPLEMENTACION: (AI)	**PROCESO:**	Instalación Y Acreditación De Sistemas: (AI5)

FUENTES DE CONOCIMIENTO	**REPOSITORIO DE PRUEBAS APLICABLES**	
	DE ANÁLISIS	**DE EJECUCIÓN**
• Entrevista al coordinador del área de sistemas. • Administración de TI (Ingenieros a cargo del módulo). • Entrevista a SYAC en relación a: entrenamiento, desarrollo de aplicaciones, seguridad, aseguramiento de la calidad y administración de TI. • Entrevista a Director proyecto o gerencia, en relación a contratos con proveedores para recursos de desarrollo de sistemas. • Políticas y procedimientos relacionados con el proceso del ciclo de vida de desarrollo de sistemas. • Políticas y procedimientos de TI relacionados con: políticas, comités de seguridad, plantación del ciclo de vida, procedimiento para pruebas, planes de calidad, entrenamiento de usuarios, migración de sistemas, aseguramiento de calidad. • Plan y programación de recursos para el ciclo de vida de desarrollo de sistemas. • Muestras de reportes de estatus de las actividades realizadas durante el desarrollo de sistemas.	• Analizar si existen políticas relacionadas con el ciclo de vida de desarrollo de sistemas. • Analizar si existe una metodología formal de ciclo de vida de desarrollo de sistemas para la acreditación de sistemas, donde se tenga en cuenta: entrenamiento, pruebas de programas, grupos de programas, plan de pruebas prototipo y en paralelo, prueba de aceptación, de acreditación, de seguridad, pruebas operativas, controles de cambio y post-implementación. • Analizar si los controles del módulo corresponden con los estándares de seguridad y las políticas de la institución. • Analizar si existen criterios para probar el acierto y las fallas en el módulo.	• "Benchmarking" de la instalación y acreditación de sistemas contra organizaciones similares o estándares internacionales. • Hacer una revisión detallada de: - El cumplimiento de cronogramas (fechas limites de grupo de desarrollo o diseño de las historias clínica para el usuario). - El material de entrenamiento asociado. - Revisión de migraciones, sistemas ambiente de prueba al estatus y las librerías de producción, en el aseguramiento de calidad. - Revisión de las herramientas y monitoreo de redes y los recursos para el mantenimiento y optimización del aplicativo. - Registro de: Entrenamiento de usuarios, seguridad, desempeño de software, documentación y resultados de pruebas.

FUENTES DE CONOCIMIENTO	REPOSITORIO DE PRUEBAS APLICABLES	
	DE ANÁLISIS	DE EJECUCIÓN
• Archivo físico del soporte prestado por SYAC.	• Analizar si dentro del proceso de aseguramiento de calidad se incluye la migración independiente de desarrollo a las librerías de producción y la suficiencia de la aceptación requerida. • Analizar el programa de entrenamiento asociado con una muestra de varias tentativas en relación a las interfaces con otros sistemas, errores y corrección de errores. • Analizar si existen herramientas automatizadas para optimizar el funcionamiento del sistema.	Plan de conversión, migración a producción, control de cambios, satisfacción de las necesidades de usuario, prueba piloto o en paralelo, revisión post-implementación. • Revisar los resultados de las pruebas para confirmar que satisfacen los criterios establecidos. • Verificar como ha sido la participación del usuario en el proceso. • Revisar la participación del proveedor. • Revisar los manuales de operación, para verificar el cronograma de actividades. • Revisar en el contrato la formalidad de las relaciones con los proveedores • Revisar la metodología del ciclo de vida, usada por el proveedor. • Revisar la documentación del proveedor en cuanto al cumplimiento de las actividades programadas.

Tipo de Registro: Cuadro de definición de fuentes de conocimiento, pruebas de análisis y pruebas de auditoría.

ENTIDAD AUDITADA:	Hospital Universitario Departamental de Nariño		
AREA AUDITADA:	Módulo de Historia Clínica	**SISTEMA:**	Dinámica Gerencial
RESPONSABLES:	Jenny Burgos García y Maria Carolina Domínguez		
Descripción de Actividad/Prueba: Minimizar la probabilidad de interrupciones, alteraciones no autorizadas y errores. Esto se hace posible a través de un sistema de administración que permita el análisis, implementación y seguimiento de todos los cambios requeridos y llevados a cabo a la infraestructura de TI actual.			
MATERIAL DE SOPORTE: COBIT			
DOMINIO:	ADQUISICION E IMPLEMENTACION: (AI)	**PROCESO:**	Administración De Cambios: (AI6)

FUENTES DE CONOCIMIENTO	**REPOSITORIO DE PRUEBAS APLICABLES**	
	DE ANÁLISIS	**DE EJECUCIÓN**
• Entrevista a Director de TI, (coordinador del área de sistemas). • Entrevista a ingenieros del área de sistemas a cargo del módulo. • Entrevista a Ingeniero representante de SYAC. • Entrevista a usuarios del módulo de historia clínica. • Políticas y procedimientos relacionados con: planeación de sistemas de información, control de cambios, seguridad. • Políticas y procedimientos de: la metodología formal del ciclo de vida, estándares de seguridad, aseguramiento independiente, implementación, distribución, mantenimiento, control de versiones. • Plan de desarrollo de aplicaciones. • Formato y bitácora de requisiciones del control de cambios. • Contratos con los proveedores (SYAC).	• Análisis de la metodología que permite priorizar los requerimientos de los usuarios. • Analizar si se realizan los cambios necesarios en los manuales de operaciones. • Analizar si el control de cambios es un procedimiento formal para los usuarios y para SYAC. • Analizar si el proceso de cambios es monitoreado. • Analizar si Existen procedimientos para verificar el código sin modificar y el código modificado, para establecer cambios realizados. • Analizar si los usuarios tienen conciencia y conocimiento de la necesidad de establecer procedimientos formales para el control de cambios.	• Benchmarking de la administración de control de cambios contra organizaciones similares o estándares. • Revisar la bitácora de control de cambios, para verificar si se asegura que los cambios mostrados fueron resueltos. • Inspeccionar si los usuarios están satisfechos con el resultado de los cambios solicitados. • Revisar la adecuación de los sistemas y los planes de prueba de los usuarios y sus resultados. • Revisar la migración formal de prueba a producción vía grupo de aseguramiento de la calidad. • Revisión de la actualización de los manuales de usuario y de operación para

FUENTES DE CONOCIMIENTO	REPOSITORIO DE PRUEBAS APLICABLES	
	DE ANÁLISIS	DE EJECUCIÓN
		Reflejar el cambio. • Revisar si se hace la distribución de la nueva versión a los usuarios.

Tipo de Registro: Cuadro de definición de fuentes de conocimiento, pruebas de análisis y pruebas de auditoría.

ENTIDAD AUDITADA:	Hospital Universitario Departamental de Nariño		
AREA AUDITADA:	Módulo de Historia Clínica	**SISTEMA:**	Dinámica Gerencial
RESPONSABLES:	Jenny Burgos García y Maria Carolina Domínguez		
Descripción de Actividad/Prueba: Asegurar que las tareas y responsabilidades de las terceras partes estén claramente definidas, que cumplan y continúen satisfaciendo los requerimientos.			
MATERIAL DE SOPORTE: COBIT			
DOMINIO:	ENTREGA DE SERVICIOS Y SOPORTE: (DS)	**PROCESO:**	Administración De Servicios Prestados Por Tercero: (DS2)

FUENTES DE CONOCIMIENTO	**REPOSITORIO DE PRUEBAS APLICABLES**	
	DE ANÁLISIS	**DE EJECUCIÓN**
• Entrevista al Director de información (representante de SYAC). • Presidencia de la función de servicios de información (Coordinador del área de sistemas). • Administrador de contrato/nivel de servicio de servicios de información (Interventores). • Políticas y procedimientos de la Institución frente a los servicios adquiridos con terceros. • Procedimientos de selección de proveedores. • Contrato realizado con la empresa SYAC en relación a la implantación del módulo de Historia Clínica. • Políticas de manejo se seguridad lógica y física, con la empresa SYAC. • Normas de mantenimiento de la calidad, planeación de contingencias y outsourcing. • Minutas de reuniones sobre revisión de contratos.	• Analizar si existen políticas y procedimientos de TI sobre relaciones con terceras partes. • Analizar si existen políticas que consideren la necesidad realizar subcontratación. • Las interfaces están definidas para agentes independientes involucrados en la conducción del proyecto y demás partes como los subcontratados. • Análisis de los contratos para verificar que estén establecidos con el fin de dar continuidad a los servicios. • Analizar si dentro de los contratos se incluye: un plan de contingencia para garantizar la continuidad del proyecto. • Analizar si los acuerdos escritos han sido negociados apropiadamente.	• Benchmarking de los servicios de terceras partes contra otras instituciones o estándares. • Hacer una revisión de los contratos y verificar que incluya los aspectos básicos para su buen desarrollo. • Hacer una revisión detallada de cada uno de los contratos de terceras partes para determinar provisiones cualitativas y cuantitativas que confirmen la definición de las obligaciones.

FUENTES DE CONOCIMIENTO	REPOSITORIO DE PRUEBAS APLICABLES	
	DE ANÁLISIS	DE EJECUCIÓN
• Acuerdo de confidencialidad para relaciones con terceras partes. • Listas de seguridad de acceso con los perfiles y recursos disponibles para los proveedores.	• Analizar la existencia de evaluaciones o criterios que permitieron escoger al proveedor del módulo	• Obtención de datos cuya propiedad no este clara y apropiadamente determinada. • Niveles de Seguridad de datos inconsistentes o inapropiados.

Tipo de Registro: Cuadro de definición de fuentes de conocimiento, pruebas de análisis y pruebas de auditoría.

ENTIDAD AUDITADA:	Hospital Universitario Departamental de Nariño		
AREA AUDITADA:	Módulo de Historia Clínica	**SISTEMA:**	Dinámica Gerencial
RESPONSABLES:	Jenny Burgos García y Maria Carolina Domínguez		
Descripción de Actividad/Prueba: Asegurar que la capacidad adecuada está disponible y que se esté haciendo el mejor uso de ella para alcanzar el desempeño deseado.			
MATERIAL DE SOPORTE: COBIT			
DOMINIO:	ENTREGA DE SERVICIOS Y SOPORTE: (DS)	**PROCESO:**	Administración de Desempeño y Capacidad : (DS3)

FUENTES DE CONOCIMIENTO	**REPOSITORIO DE PRUEBAS APLICABLES**	
	DE ANÁLISIS	**DE EJECUCIÓN**
• Entrevista a la Presidencia de la función de servicios de información. • Entrevista a la administración de operaciones de la función de servicios de información. • Entrevista a la administración de la capacidad de la función de servicios de información. • Administración de redes de la función de servicios de información. • Políticas y procedimientos del Hospital en relación al reporte del desempeño del módulo, carga de trabajo, administración de la capacidad y programación de actividades.	• Analizar si los períodos de tiempo y el nivel de servicio están definidos para todos los servicios que presta el módulo de historia clínica. • Analizar si los períodos de tiempo y los niveles de servicio reflejan los requerimientos del usuario. • Analizar si los períodos de tiempo y los niveles de servicio son consistentes con las expectativas de desempeño. • Analizar si existe un plan de disponibilidad, si está actualizado y refleja los requerimientos del usuario. • Analizar si se lleva a cabo y se reporta un monitoreo continuo del desempeño de todo el equipo y de la capacidad.	• Benchmarking de la administración del desempeño y la capacidad contra organizaciones similares o estándares internacionales. • Realizar pruebas de las necesidades continuas del negocio. • Hacer una revisión del proceso de plantación de capacidad y los recursos para asegurar la modificación oportuna de planes. • Hacer verificaciones para asegurar que las expectativas de desempeño están siendo alcanzadas. • Hacer una comparación de los requerimientos de desempeño desde una perspectiva de análisis costo/beneficio, para verificar el uso de los recursos.

FUENTES DE CONOCIMIENTO	REPOSITORIO DE PRUEBAS APLICABLES	
	DE ANÁLISIS	DE EJECUCIÓN
• Políticas y procedimientos para el módulo de historia clínica en relación a la disponibilidad de la organización, la planeación y el monitoreo. • Representaciones del producto por parte del proveedor con respecto a las normas de capacidad y desempeño. • Una lista de todos los productos actuales de software de SYAC. • Reportes de monitoreo de redes de comunicación. • Minutas de las reuniones en las que se discuten la planeación de la capacidad, las expectativas de desempeño y la "afinación" del desempeño. • Documentos de disponibilidad, capacidad, carga de trabajo y planeación de recursos. • Reportes relacionados con el desempeño operativo dentro de la función de servicios de información, incluyendo el reporte y la historia de la solución de problemas.	• Analizar si se monitorea el desempeño óptimo de configuración utilizando herramientas de modelado. • Analizar si los usuarios revisan proactivamente la capacidad y desempeño del módulo. • Análisis de Las estadísticas sobre reportes de desempeño y disponibilidad son precisas. • Analizar si los reportes de flujo de trabajo, consideran las oportunidades de eficiencia de procesos adicionales. • Analizar los reportes de información de desempeño para los usuarios y la disponibilidad del módulo. • Analizar si existen procedimientos de escalonamiento para la solución de problemas. • Análisis de los niveles de soporte proporcionados, para determinar si son suficientes para apoyar los objetivos del Hospital.	

Tipo de Registro: Cuadro de definición de fuentes de conocimiento, pruebas de análisis y pruebas de auditoría.

ENTIDAD AUDITADA:	Hospital Universitario Departamental de Nariño		
AREA AUDITADA:	Módulo de Historia Clínica	**SISTEMA:**	Dinámica Gerencial
RESPONSABLES:	Jenny Burgos García y Maria Carolina Domínguez		
Descripción de Actividad/Prueba: Salvaguardar la información contra uso no autorizados, divulgación, modificación, daño o pérdida. Para ello se realizan controles de acceso lógico que aseguren que el acceso a sistemas, datos y programas está restringido a usuarios autorizados.			
MATERIAL DE SOPORTE: COBIT			
DOMINIO:	ENTREGA DE SERVICIOS Y SOPORTE: (DS)	**PROCESO:**	Garantizar La Seguridad De Sistemas : (DS5)

FUENTES DE CONOCIMIENTO	**REPOSITORIO DE PRUEBAS APLICABLES**	
	DE ANÁLISIS	**DE EJECUCIÓN**
• Entrevista al Ingeniero coordinador del área de sistemas. • Entrevistas a ingenieros del área de sistemas responsables de la seguridad. • Políticas y procedimientos globales de la Institución referentes a la seguridad y el acceso de los sistemas de información. • Políticas y procedimientos de TI relacionadas con: seguridad y acceso al módulo de historia clínica. • Políticas de seguridad que son exigidas legalmente al Hospital para temas servicios de salud en historias clínica, incluyendo: - Administración de cuentas de usuarios. - política de seguridad del usuario o de protección de la información.	• Analizar si se cuenta con un plan de seguridad que brinde control sobre el módulo. • Se cuenta con una organización de seguridad que asegurare el correcto acceso al módulo. • Analizar si existe un esquema de clasificación de datos que indique los recursos del sistema y sus propietarios responsables. • Analizar si se cuenta con perfiles de seguridad de usuarios y si se revisan continuamente. • Analizar si las capacitaciones realizadas a los usuarios incluye aspectos de seguridad. • Analizar si hacen reportes de fallas a aspectos de seguridad, y si estos reportes incluyen: - intentos no autorizados al módulo y sus recursos y accesos autorizados.	• Benchmarking de la seguridad de los sistemas de información contra organizaciones similares o estándares. • Una revisión detallada de la seguridad de los sistemas de información. • Entrevistas a los nuevos empleados para asegurar el conocimiento y la conciencia en cuanto a seguridad. • Entrevista a los usuarios para asegurar el acceso tomando como base los requerimientos. • Entrevistar a los usuarios para determinar si tienen instrucciones para la detección y reportes de virus.

FUENTES DE CONOCIMIENTO	REPOSITORIO DE PRUEBAS APLICABLES	
	DE ANÁLISIS	DE EJECUCIÓN
- estándares relacionados con el comercio electrónico. - plano de los edificios y cuartos de equipos del hospital, que contienen recursos de sistemas de información - inventario o esquema de los puntos de acceso físico, (por ejemplo, módems, líneas telefónicas y terminales remotas). - procedimientos de control de cambios de software de seguridad. - reportes de violaciones a la seguridad y procedimientos de revisión administrativa. - inventario de dispositivos de encriptación de datos y de estándares de encriptación. - lista de los proveedores y clientes con acceso a los recursos del módulo de Historia Clínica. - Proveedor de servicios de transmisión de datos al hospital, (proveedor de Internet). - Practicas de administración de redes relacionadas con pruebas contiguas de seguridad. - copias de los contratos de los proveedores de servicios de transmisión de datos. - copias de documentos firmados por los usuarios relacionados con seguridad y concientización. - contenido del material de entrenamiento de seguridad para los usuarios del módulo.	- Privilegios de acceso por ID de Usuario. • Analizar si existen módulos criptográficos, procedimientos de mantenimiento, estándares de administración de llaves criptográficas. • Analizar si los mecanismos de autenticidad proveen de: - Número de sesiones concurrentes de usuario están limitadas y cada una tiene password. - Analizar si antes de ingresar al módulo se muestra un mensaje de advertencia, de los problemas legales de accesos no autorizados. - Analizar si al ingresar a la sesión, se muestra un historial de intentos de ingresos. • Analizar si en cambios o ausencia de personal, se controlan las cuentas de estos usuarios. • Analizar si se utilizan rutas confiables para transmitir la información. • Analizar si existen la implementación de medidas de control para prevenir y detectar virus en los computadores. • Analizar si existe un botón que forcé salida del módulo, al dejar la sesión inactiva por un periodo de tiempo. • Analizar si existen procedimientos para el mantenimiento de acceso de usuarios al sistema. • Analizar si los parámetros de seguridad del SO tienen como base estándares locales. • Se emiten reportes de seguridad en cuanto a incidentes. • Analizar si existen llaves secretas para la transmisión de datos. • Analizar si existen políticas de descarga de archivos y de revisión del software antes de una instalación. • Analizar las propiedades de los firewalls.	

Tipo de Registro: Cuadro de definición de fuentes de conocimiento, pruebas de análisis y pruebas de auditoría.

ENTIDAD AUDITADA:	Hospital Universitario Departamental de Nariño		
AREA AUDITADA:	Módulo de Historia Clínica	**SISTEMA:**	Dinámica Gerencial
RESPONSABLES:	Jenny Burgos García y Maria Carolina Domínguez		
Descripción de Actividad/Prueba: Asegurar que los usuarios estén haciendo un uso efectivo de la tecnología y estén conscientes de los riesgos y responsabilidades involucrados, para ello se realiza un plan completo de entrenamiento y desarrollo.			
MATERIAL DE SOPORTE: COBIT			
DOMINIO:	ENTREGA DE SERVICIOS Y SOPORTE: (DS)	**PROCESO:**	Educación Y Entrenamiento De Usuarios: (DS7)

FUENTES DE CONOCIMIENTO	**REPOSITORIO DE PRUEBAS APLICABLES**	
	DE ANÁLISIS	**DE EJECUCIÓN**
• Entrevista a Ingenieros del área de sistemas e Ingeniero de SYAC responsable de las capacitaciones del módulo. • Entrevista a Administrador y usuarios del módulo de Historia Clínica. • Políticas y procedimientos generales del hospital, relacionados con la capacitación de médicos y enfermeras, en controles y seguridad. • Programas de entrenamiento para los usuarios en relación a l módulo de historia clínica y sus recursos. • Programas, y procedimientos de entrenamiento y de educación de TI relacionados con la concientización en controles y seguridad, controles y seguridad técnica.	• Analizar si existen políticas y procedimientos para concientizar a los usuarios sobre seguridad y controles. • Analizar si se cuenta con un programa de entrenamiento enfocado a los principios de seguridad. • Analizar si los nuevos empleados tienen conocimiento y conciencia de la responsabilidad de seguridad y los recursos del módulo. • Analizar si se cuenta con políticas y procedimientos relacionados con capacitaciones y estos van acordes al módulo de historia clínica.	• Hacer una revisión detallada de los manuales usados para las capacitaciones, verificando que se traten los temas de controles de seguridad, confidencialidad, disponibilidad e integridad • Realizar entrevistas a los usuarios del módulo (médicos y enfermeras), para determinar sus requerimientos en relación al manejo del módulo y sus recursos, verificando la satisfacción del entrenamiento recibido.

FUENTES DE CONOCIMIENTO	REPOSITORIO DE PRUEBAS APLICABLES	
	DE ANÁLISIS	DE EJECUCIÓN
	• Analizar si hay disponibilidad de hacer entrenamiento interno, y entrenamiento técnico externo, considerando también la asistencia de los médicos y enfermeras. • Analizar si las capacitaciones son planeadas con base en las necesidades del personal, y con base a los aspectos de seguridad y controles. • Analizar si se exige a los usuarios del módulo, asistir a entrenamientos de conciencia sobre seguridad y controles a las TI.	

Tipo de Registro: Cuadro de definición de fuentes de conocimiento, pruebas de análisis y pruebas de auditoría.

ENTIDAD AUDITADA:	Hospital Universitario Departamental de Nariño		
AREA AUDITADA:	Módulo de Historia Clínica	**SISTEMA:**	Dinámica Gerencial
RESPONSABLES:	Jenny Burgos García y Maria Carolina Domínguez		
Descripción de Actividad/Prueba: Dar cuenta de todos los componentes de TI, prevenir alteraciones no autorizadas, verificar la existencia física y proporcionar una base para el sano manejo de cambios.			
MATERIAL DE SOPORTE: COBIT			
DOMINIO:	ENTREGA DE SERVICIOS Y SOPORTE: (DS)	**PROCESO:**	Administración De La Configuración: (DS9)

FUENTES DE CONOCIMIENTO	**REPOSITORIO DE PRUEBAS APLICABLES**	
	DE ANÁLISIS	**DE EJECUCIÓN**
• Entrevista a la Administración de operaciones del módulo de Historia Clínica. • Entrevista a la Administración de desarrollo de aplicaciones, (Ingenieros a cargo del diseño de los formularios de historia clínica). • Entrevista al Ingeniero de SYAC encargado de soporte del módulo. • Manual de Sistema y de Usuario. • Manual o procedimiento de instalación del módulo en los usuarios. • Documentación de la arquitectura del módulo. • Reporte detallado de accesos de los usuarios al sistema operativo y la base de datos. • Archivo físico del soporte prestado por SYAC.	• Análisis de la arquitectura del módulo. • Analizar la documentación de los cambios, en la configuración y en las versiones del módulo. • Analizar si se hace una revisión periódica de la configuración sobre los equipos terminales. • Análisis de los manuales o procedimientos de instalación del módulo en los usuarios. • Análisis si el proceso para crear y controlar las líneas bases de la configuración es apropiado. • Analizar si existen funciones para mantener la base de la configuración. • Analizar si existe un proceso para controlar la contabilización y registro de los recursos adquiridos.	• Ejecución de programas que permitan conexión con el sistema operativo y la base de datos, para verificar la seguridad y acceso de otros medios. • Revisión de los reportes de instalación y configuración del módulo en los usuarios, verificando el plan de instalación. • Revisión de la última versión del módulo de historia clínica instalada, para verificar su actualización. • Observar la frecuencia de las revisiones administrativas de los registros de la configuración, los cambios a estos registros. • Revisión de la instalaciones físicas y los cuartos de equipos verificado que se cumplan las normas de cableado.

FUENTES DE CONOCIMIENTO	REPOSITORIO DE PRUEBAS APLICABLES	
	DE ANÁLISIS	DE EJECUCIÓN
• Registro de configuración y modificación de los parámetros de la base de datos. • Inventario de la configuración: hardware, software de sistema operativo, software de aplicativo, instalaciones y archivos de datos –dentro y fuera de las instalaciones. • Políticas y procedimientos del Hospital en relación con la adquisición, inventario y disposición de software y equipo computacional adquirido. • Documentación de los cambios realizados en cada versión realizada. • Reportes de los cambios realizados en la configuración del módulo. • Información de la línea base/estándar de la configuración. • Manual de procedimiento de instalación y configuración del servidor. (Sistema operativo, motor de base de datos, red, servicios, seguridad). • Documentación de la red de datos (mapas de red, normas, topologías aplicadas).	• Analizar si los procesos de migración de aplicaciones de desarrollo al ambiente de pruebas y finalmente al estatus de producción, interactúan con el reporte de la configuración. • Analizar si existe una coordinación entre el desarrollo de aplicaciones, el aseguramiento de la calidad y las operaciones con respecto a los cambios sobre la línea base de la configuración, en su actualización. • El software en los equipos de los usuarios es rotulado e inventariado.	• Hacer una revisión sobre duplicaciones, eliminación de archivos de datos, programas y registro de configuración. • Verificar que los procedimientos de control de la configuración incluyan: - Integridad en la línea base de la configuración - Controles de autorización de acceso al sistema. - La recuperación de la configuración. - Evaluaciones periódicas del registro de configuración. - La existencia de procedimientos para revisar el acceso a las bases del software. - Los resultados de las revisiones sean proporcionados a la administración para llevar a cabo acciones correctivas.

Tipo de Registro: Cuadro de definición de fuentes de conocimiento, pruebas de análisis y pruebas de auditoría.

ENTIDAD AUDITADA:	Hospital Universitario Departamental de Nariño		
AREA AUDITADA:	Módulo de Historia Clínica	**SISTEMA:**	Dinámica Gerencial
RESPONSABLES:	Jenny Burgos García y Maria Carolina Domínguez		
Descripción de Actividad/Prueba: Incrementar los niveles de confianza entre el Hospital, Usuarios y proveedores externos.			
MATERIAL DE SOPORTE: COBIT			
DOMINIO:	MONITOREO: (M2)	**PROCESO:**	Evaluar Lo Adecuado Del Control Interno: (M2)

FUENTES DE CONOCIMIENTO	REPOSITORIO DE PRUEBAS APLICABLES	
	DE ANÁLISIS	**DE EJECUCIÓN**
• Entrevista al Director Ejecutivo. • Entrevista al Director de Información. • Entrevista al Director de auditoría interna y externa. • Entrevista al Director de servicios de información y administración de control de calidad. • Entrevista a los Usuarios del módulo de historia clínica. • Entrevista a los Miembros del comité de auditoría, si aplica. • Políticas y procedimientos organizacionales relacionadas con la planeación, administración, monitoreo y reporte de los controles internos. • Políticas y procedimientos de la función de servicios de información relacionadas con el monitoreo y el reporte de los controles internos y la frecuencia de las revisiones. • Reportes de las actividades.	• Analizar si los datos identificados para monitorear los controles internos del módulo son apropiados. • Analizar si los reportes internos de los datos de control interno del módulo son adecuados. • Analizar si existe una revisión administrativa de los controles internos sobre el módulo. • Analizar si existen controles de monitoreo para proporcionar una retroalimentación oportuna. • Analizar las respuestas del hospital frente a las recomendaciones de mejoramiento. • Analizar si existen iniciativas y resultados de mejoramiento del control interno. • Analizar la información de errores, inconsistencias y excepciones del control interno. • Analizar si la entrega oportuna de reportes permite una respuesta rápida frente a errores.	• Benchmarking de la evaluación del control interno respecto a organizaciones similares o estándares internacionales. • Hacer una revisión de la relevancia de los datos dentro de los procesos que se están monitoreando y en el reporte de los controles internos. • Hacer una revisión de los controles internos del hospital, tomando un marco de referencia. • Revisar los grados de cumplimientos de las metas de control interno y propuestas de mejoramiento. • Hacer una revisión de la satisfacción de los encargados de supervisar el desempeño del módulo. • Revisar si las recomendaciones han sido implementadas.

Cuestionarios Cuantitativos

Tipo de Registro: Cuestionario Cuantitativo.			
RESPONSABLES:	Jenny Burgos García y Maria Carolina Domínguez		
MATERIAL DE SOPORTE: COBIT			
DOMINIO:	Planeación y Organización (PO)	**PROCESO:**	Definición de la Arquitectura de Información: (PO2)

PREGUNTA	SI	NO	NA	*FUENTE*
1. ¿Existe un manual de sistema (técnico) para el módulo de historia clínica electrónica?		4		*Entrevista al Representante de SYAC* *Entrevistas a ingenieros/ área de sistemas*
2. El manual de sistema contiene:				*Revisión del manual de sistema de historia clínica.*
• Requerimientos de software y hardware para su funcionamiento.		4		
• Descripción de la configuración.	4			
• Descripción y catalogo de formas.	4			
• Descripción de operación de cada botón y elementos del módulo.	4			
• Diagramas de flujo de datos o pseudocódigo o diagramas de flujo de las partes del módulo.		4		
• Descripción y catalogo de reportes.	4			
• Lista de archivos y especificaciones.		4		
• Escalabilidad e interacción con otros módulos.		4		
3. ¿El manual de sistema (técnico) de soporte del módulo es actualizado cada vez que se realizan cambios o actualizaciones?		4		*Revisión del manual de historia clínica, ultimas versiones*
4. ¿Existe algún procedimiento establecido para mantener actualizado el manual técnico de soporte del módulo?		4		*Entrevista a representante de SYAC*
5. ¿Existe el diccionario de datos?	5			*Entrevista a representante de SYAC*
6. El diccionario de datos contiene:				*Revisión del Diccionario de datos.*
• Modelo entidad relación.	5			
-Tablas.	5			
- Relaciones.	5			
- Llaves.	*5*			

PREGUNTA	SI	NO	NA	FUENTE
▪ El modelo lógico de la base de datos (descripción de los elementos de la base de datos, como tabla: descripción, campos, longitud, descripción del campo, valores por defecto, condiciones entre otros)	5			Revisión del Diccionario de datos.
▪ Descripción del personal encargado de la función de dar mantenimiento del diccionario de datos.		5		
▪ Clasificación de usuarios, niveles de acceso y restricciones.		5		
▪ Roles y privilegios.		5		
7. ¿Le ha sido entregado al personal del área de sistemas encargado del manejo del módulo de historia clínica, el diccionario de datos relacionado con el módulo de historia clínica?		5		Entrevistas Ingenieros del área de sistemas.
8. ¿El diccionario de datos se actualiza cada vez que se realizan cambios o actualizaciones al módulo de historia clínica?	5			Entrevista al representante de SYAC. Diccionario de datos, verificación de fecha de actualización.
9. ¿Se ha establecido un procedimiento para mantener actualizado el diccionario de datos?		5		Entrevista al representante de SYAC.
10 ¿Existe un modelo de arquitectura de información?		4		Entrevista al representante de SYAC.
11. ¿Existen políticas y procedimiento en relación al modelo de arquitectura de información?		4		Entrevista al representante de SYAC.
12. El modelo de arquitectura de información tiene en cuenta:				Revisión de la documentación del modelo de arquitectura de Información del módulo de historia clínica.
▪ Identificación de entradas.		4		
▪ Identificación de procesos.		4		
▪ Identificación de sitios de almacenamiento (base de datos).		4		
▪ Identificación de reportes.		4		
▪ Identificación de la interacción con otros sistemas.		4		
▪ Diseño de interacción de los elementos e identidades del módulo.		4		
▪ Definición de usuarios finales.		4		
▪ Requerimientos de las diferentes Instituciones.		4		
▪ Los planes de la gerencia a corto y largo plazo.		4		
▪ Costos, riesgos y aprobaciones para hacer modificaciones al modelo.		4		
13. ¿El modelo de arquitectura de información del módulo de historia clínica, ha sido dado a conocer al personal del área de sistemas del Hospital Universitario departamental de Nariño?		4		Entrevista al representante de SYAC. Entrevista a Ingenieros del área de sistemas a cargo del módulo de historia clínica.
14. ¿Existe la definición de políticas de auditoría y control?	4			Entrevista al Coordinador del área. Revisión del documento de definición de políticas de auditoría y control.
15. Las definición de las políticas de auditoría y control están establecidas para:				Documento de definición de políticas de auditoría y control. Comprobación del contenido del documento de la definición de políticas de auditoría y control.
▪ Accesos a la información.		4		
▪ Accesos al sistema de información.		4		
▪ Cambios a los datos.		4		
▪ Cambios a la configuración.		4		
▪ Comprobación de la aplicación de la normatividad.		4		
▪ Comprobación de procedimientos automatizados (formulación).		4		

PREGUNTA	SI	NO	NA	FUENTE
16. ¿Se ha realizado una clasificación formal de los datos, de acuerdo a criterios de propiedad y niveles de importancia?	3			Entrevista al Coordinador del área de sistemas
17. ¿Existen políticas y procedimientos para la clasificación de los datos?		3		Entrevista al Coordinador del área de sistemas
18. Dentro de las políticas y procedimientos que permiten la clasificación de los datos se incluye:				Revisión de las políticas y procedimientos para la clasificación de los datos.
▪ Categorías de seguridad.		3		
▪ Propiedad de los datos.		3		
- Datos públicos.		3		
- Datos Privados.		3		
- Datos Secretos.		3		
▪ Estándares de clasificación “Default”, para los activos de datos que no contienen un identificador de clasificación.		3		
19. ¿Existe una oficina encargada de definir e implementar las políticas y procedimientos de la función de los servicios informáticos?	4			Entrevista al Coordinador del área de sistemas Revisión del documento que contiene las funciones, procesos y procedimientos de la oficina de sistemas
20. Las políticas y procedimientos de la función de los servicios informáticos incluye:				Verificación del contenido de las funciones, procesos y procedimientos de la oficina de sistemas
▪ Niveles de seguridad definidos para cada clasificación de datos.		3		
▪ Niveles de acceso definidos y apropiados para la clasificación de los datos.		3		
21. ¿Existen informes del soporte prestado por SYAC?	3			Entrevista Ingenieros a cargo del módulo. Revisión de los informes del soporte prestado por SYAC.
22. Los informes del soporte prestado por SYAC se encuentran clasificados en: ▪ Requerimientos de usuarios finales. ▪ Requerimientos de capacitaciones.	3			Reportes de requerimientos solucionados por SYAC Revisión de la clasificación de los requerimientos solucionados por SYAC
23.Los soportes físicos del soporte prestado por SYAC contiene:				Comprobación del contenido de los reportes de requerimientos solucionados solicitados a SYAC
▪ Fecha, hora, persona que hace la solicitud.	3			
▪ Descripción del problema o inconveniente presentado.	3			
▪ Fecha, hora, persona que atiende el requerimiento.	3			
▪ Descripción de la solución del problema o inconveniente presentado.	3			
▪ Espacio para anotación de pruebas.	3			
▪ Espacio para inclusión de anexos.	3			
▪ Firma de usuario de recibo a satisfacción.	3			
▪ Firma de la persona que atendió el requerimiento.	3			

PREGUNTA	SI	NO	NA	*FUENTE*
24. ¿El soporte que presta SYAC está contenido dentro del contrato y se planifica al inicio de la ejecución del mismo indicadores que permitan demostrar su cumplimiento?	3			*Verificación del contrato de outsourcing entre SYAC y el Hospital Departamental Revisión de los requerimientos negados o solucionados por SYAC determinar si se encuentran o no contemplados en lo contratado*
TOTALES	***89***	***156***		
	89/245	***156/245***		
TOTAL ENCUESTA	***245***			

% Riesgo = $\frac{89 * 100}{245-0}$ = 36% (Medio)

Tipo de Registro: Cuestionario Cuantitativo.			
ENTIDAD AUDITADA:	Hospital Universitario Departamental de Nariño		
AREA AUDITADA:	Módulo de Historia Clínica	**SISTEMA:**	Dinámica Gerencial
RESPONSABLES:	Jenny Burgos García y Maria Carolina Domínguez		
MATERIAL DE SOPORTE: COBIT			
DOMINIO:	Planeación y Organización (PO)	**PROCESO:**	Asegurar el Cumplimiento de los Requerimientos Externos: (PO8)

PREGUNTA	SI	NO	NA	*FUENTE*
1. ¿Existen normas gubernamentales que le son exigidas al Hospital Universitario Departamental de Nariño, en relación a los procedimientos llevados en la gestión de Historias Clínicas?	5			*Entrevista al Auditor Medico*
2. ¿Dentro de diferentes procesos del Módulo y los diseños de Historia Clínica, se han tenido en cuenta las políticas o normas gubernamentales para las entidades prestadoras del servicio de salud?	5			*Entrevista a Ing. de SYAC, Entrevista a ingeniero Coordinador del área de sistemas.*
3. Dentro de los procesos y diseños del módulo de Historia Clínica se ha tenido en cuenta:				*Entrevista a representante de SYAC, Entrevista a ingeniero Coordinador del área de sistemas. Entrevista a Ingenieros a cargo del módulo de historia clínica.*
▪ La norma para lesión de causa externa, que se aplica generalmente a las áreas de triage o urgencias para el HUDN?	5			
▪ Dentro de los diseños de historia clínica se incluye el decreto 526 de 1975, que obliga a llevar los diseños de historia clínica a las entidades gubernamentales.	5			
▪ Se incluye dentro del módulo la resolución 3881 del 21/04/1982, de la circular externa 12 de 1993.	5			
▪ Se usa el numero de cedula, tarjeta de identidad, numero de registro civil, para la identificación de la historia clínica del ciudadano, como estándar aplicado en Colombia desde enero del año 2000.	5			
▪ La integridad: Contenga la información de aspectos científicos, técnicos y administrativos relativos a la atención en salud.	5			
▪ Secuencialidad: Secuencia cronológica de la atención del paciente.	5			
▪ Racionalidad: Se evidencia de forma lógica y clara las condiciones del paciente.	5			
▪ Disponibilidad: Posibilidad de usar la Historia clínica en el momento en que se necesite.	5			
▪ *Oportunidad: Diligenciamiento de los registros inmediatamente después de que ocurre la prestación del servicio.*	*5*			

PREGUNTA	SI	NO	NA	*FUENTE*
4. ¿Existen normas o políticas de seguridad y salud en el Hospital, relacionadas con el desenvolvimiento e interacción de los usuarios y las tecnologías de Información?	3			*Entrevista a enfermera jefe responsable del área de Salud Ocupacional*
5. las normas ergonomía y seguridad incluyen:				*Entrevista a enfermera jefe responsable del área de Salud Ocupacional, Entrevista a Ingeniero coordinador del área de sistemas. Entrevista A ingenieros del área de sistemas. Entrevista a responsable de la adquisición e instalación de los equipos de computo, y demás elementos para el módulo de historia clínica. Entrevista a Auditor Medico. Entrevista a usuarios finales*
▪ Definición de políticas y normas de ergonomía relacionadas con las tecnologías de Información, donde se defina las actividades de riesgo para el personal que interactúa con tecnologías de información.	3			
▪ Definición de un programa de seguridad y ergonomía, donde se traten todos los temas que garanticen la seguridad del personal del área de sistemas y el personal asistencial encargado del manejo del módulo de historia clínica.	3			
▪ ¿Se ha dado ha conocer a los usuarios (médicos y enfermeras) y demás personal (ingenieros del área de sistemas) relacionados con el módulo, el programa de seguridad y ergonomía, donde se describen las normas de ergonomía y seguridad relacionadas con las tecnologías de información?		3		
▪ ¿Se le ha explicado a los usuarios y recurso humano del área de sistemas, cuales son las situaciones correctas de ergonomía y seguridad?		3		
▪ ¿Se le ha entregado al usuario y personal de sistemas, elementos que cumplen con las normas de ergonomía y seguridad, en relación a implementos de trabajo como: sillas, escritorio, pantalla del computador, infraestructura física entre otros?		3		
▪ ¿Se realizan periódicamente capacitaciones para la prevención de riesgos, explicando los manuales y normas de seguridad y ergonomía?		3		
▪ ¿Se han explicado las causas de accidentes de trabajo?		3		
▪ ¿Se ha capacitado a la persona responsable de la infraestructura física y de cómputo del área de sistemas, para que realice una Instalación de equipos basándose en las normas y recomendaciones de seguridad y ergonomía?		3		
6. ¿Existen políticas o normas relacionadas con la seguridad y privacidad de la Información del Hospital?	5			*Entrevista a Coordinador del área de sistemas*
7. Dentro de estas políticas se incluye:				*Revisión de las normas o políticas de seguridad y privacidad de la información.*
▪ ¿Normas relacionadas con el flujo de datos entre las áreas que interactúan con el módulo?		5		
▪ ¿En caso de usar correo electrónico, existen normas relacionadas con el uso de correo electrónico por parte de los usuarios para el envió de información de historias clínicas a otras entidades de salud o EPS?		5		
▪ ¿Los datos son clasificados de acuerdo a niveles de Importancia y confidencialidad en el módulo de historia clínica?		5		
• ¿Dentro de las políticas para garantizar la seguridad de la información, se han incluido procedimientos que indiquen cual es el correcto manejo de las tecnologías de información, por parte de los médicos y enfermeras?		5		
8. ¿Existen normas o políticas del hospital en relación al aseguramiento del software?	*3*			*Entrevista al Coordinador de área, Revisión de normas y políticas del hospital en relación al las tecnologías de información.*

PREGUNTA	SI	NO	NA	*FUENTE*
9. ¿Existen contratos con Aseguradoras para el cubrimiento de las tecnologías de información de Hospital?	3			*Entrevista Ingeniero Coordinador del área de sistemas*
10. Los contratos con seguros que tiene el hospital incluyen:	3			*Revisión de los contratos con aseguradoras*
▪ Cobertura en casos de catástrofes naturales, como incendios.	3			
▪ Violación de la Información por parte de personas externas.	3			
11. ¿Se han realizado auditorías externas al módulo?		2		*Entrevista a Ingeniero Coordinador del área de sistemas. Entrevista a representante de SYAC.*
	84	***40***		
TOTALES				
	84/124	***40/124***		
TOTAL ENCUESTA	***124***			

% Riesgo = $\frac{84 * 100}{124 - 0}$ = 67% (Medio)

Tipo de Registro: Cuestionario Cuantitativo.			
ENTIDAD AUDITADA:	Hospital Universitario Departamental de Nariño		
AREA AUDITADA:	Módulo de Historia Clínica	**SISTEMA:**	Dinámica Gerencial
RESPONSABLES:	Jenny Burgos García y Maria Carolina Domínguez		
MATERIAL DE SOPORTE: COBIT			
DOMINIO:	Planeación y Organización (PO)	**PROCESO:**	Evaluación de Riesgos: (PO9)

PREGUNTA	SI	NO	NA	FUENTE
1. ¿Existen políticas y procedimientos en relación a la evaluación de riesgos en el módulo de historia clínica?		4		Entrevista al Coordinador de sistemas, Ingeniero SYAC y Control Interno.
2. ¿Existe un marco referencial y procedimientos para la evaluación de riesgos?		4		Entrevista al Coordinador, ingenieros del área de sistemas, Ingeniero de SYAC y Control Interno
3. Dentro del marco referencial y los procedimientos para la evaluación de riesgos se incluyen:				Entrevista a Ingeniero representante de SYAC. Entrevista a Ingeniero Coordinador del área de sistemas. Entrevista a Control Interno. Revisión del marco referencial para la evaluación de riesgos.
▪ Aspectos relacionados con la actualización o mantenimiento del hardware e infraestructura de red.	4			
▪ El manejo que le da el usuario a su equipo de trabajo, sus recursos de Software, e instalación de otros programas que quitan rendimiento al hardware, o pueden ser causantes de adquisición de virus.		4		
▪ Cambios en los requerimientos de los usuarios.		4		
▪ Cambios en los requerimientos externos, del entorno del módulo o gubernamentales.		4		
▪ Revisión del manejo del módulo por parte de los usuarios en aspectos de seguridad.		4		
▪ Auditorías, inspecciones, o incidentes anteriores ocurridos en relación a las tecnologías de información del Hospital.		4		
4. ¿Se realiza periódicamente una evaluación de riesgos en el módulo de historia clínica, y se cumple en base al marco de referencia para la evaluación de riesgos?		4		Entrevista al Coordinador del área del área de sistemas e ingeniero de SYAC.
5. ¿Se lleva un reporte o documentación relacionada con el seguimiento a la identificación de riesgos?		4		Entrevista al Coordinador de sistemas, Ingeniero SYAC y Control Interno.
6. La información de la documentación de riesgos contiene:				Revisión de la documentación de evaluación de Riesgos.
▪ ¿Descripción de la metodología de evaluación de riesgos?		4		
▪ ¿La identificación de exposiciones significativas y los riesgos correspondientes?		4		
▪ ¿Los riesgos y exposiciones correspondientes considerados?		4		

PREGUNTA	SI	NO	NA	FUENTE
7. ¿Existe un enfoque cuantitativo y/o cualitativo (o combinado) formal, para la identificación y medición de riesgos, amenazas y exposiciones?		4		Entrevista al Coordinador de sistemas, Ingeniero SYAC y Control Interno.
8. ¿Se han categorizado los riesgos del módulo de acuerdo a su nivel de importancia e impacto?		4		Entrevista al Coordinador de sistemas, Ingeniero SYAC y Control Interno.
9. ¿Existe un plan de acción contra riesgos?		4		Entrevista al Coordinador de sistemas, Ingeniero SYAC y Control Interno.
10. El plan de acción incluye:				Revisión del plan de acción
▪ ¿Controles económicos?		4		
▪ ¿Medidas de seguridad para evitar que vuelva a ocurrir el riesgo?		4		
▪ ¿Seguimiento o monitoreo realizado al proceso?		4		
11. ¿Se ha realizado un proceso informativo y de toma de conciencia de la evaluación de riesgos, al personal del área de sistemas, sobre el desempeño y funcionamiento de las tecnologías de información?		4		Entrevista al Coordinador de sistemas. Entrevista a Control Interno. Entrevista a Ingenieros del área de sistemas encargados de la evaluación y monitoreo de riesgos en el módulo de historia clínica.
12. ¿Se envía periódicamente reportes sobre la evaluación de riesgos a la Gerencia del Hospital?		4		Entrevista al Coordinador sistemas. Entrevista a Control Interno. Revisión de los reportes sobre la evaluación de riesgos.
13. ¿Existe un seguro que cubra los riesgos de las tecnologías de información del Hospital?	3			Entrevista al Coordinador de sistemas. Entrevista a Control Interno.
14. El seguro contra riesgos incluye casos de:				Entrevista al Coordinador de sistemas. Entrevista a Control Interno. Revisión del contrato con la Aseguradora de las tecnologías de información.
▪ Incendio, inundaciones, terremotos, tornados, terrorismo y otros desastres naturales no predecibles.		3		
▪ Violaciones a las responsabilidades fiduciarias del empleado.		3		
▪ Interrupción del negocio, pérdidas de ingresos, perdida de pacientes, etc.		3		
▪ Otros riesgos no cubiertos generalmente por la tecnología de información y planes de riesgo/continuidad del negocio.		3		
TOTALES	***7***	***92***		
	7/99	***92/99***		
TOTAL ENCUESTA	**99**			

$$\% \text{ Riesgo} = \frac{7 * 100}{99 - 0} = 7\% \text{ (Bajo)}$$

Tipo de Registro: Cuestionario Cuantitativo.			
ENTIDAD AUDITADA:	Hospital Universitario Departamental de Nariño		
AREA AUDITADA:	Módulo de Historia Clínica	**SISTEMA:**	Dinámica Gerencial
RESPONSABLES:	Jenny Burgos García y Maria Carolina Domínguez		
MATERIAL DE SOPORTE: COBIT			
DOMINIO:	Planeación y Organización (PO)	**PROCESO:**	Administración De Calidad: (PO11)

PREGUNTA	SI	NO	NA	FUENTE
1. ¿Existen políticas y procedimientos para el aseguramiento de la calidad en el módulo de historia clínica?	4			Entrevista a Ingeniero Coordinador del área de sistemas e Ingeniero de SYAC.
2. ¿Existe un plan de calidad de aplicación a las tecnologías de información?	4			Entrevista a Ingeniero Coordinador del área de sistemas e Ingeniero de SYAC. Entrevista a ingenieros del área de sistemas
3. Dentro del plan de calida se incluyen:				Revisión del plan de calidad de Hospital relacionados con las tecnologías de información.
▪ ¿Una planeación y organización de los planes del hospital a corto y largo plazo?	4			
▪ ¿Esta Actualizado?	4			
▪ ¿La infraestructura de información requerida para soportar los sistemas e interfases?		4		
▪ ¿El entrenamiento requerido para desarrollar y soportar el ambiente de TI escogido como objetivo?		4		
▪ ¿Los recursos tanto financieros como humanos?	4			
▪ ¿Fomenta la filosofía de mejora continua?	4			
4. ¿Existe un enfoque de aseguramiento de calidad en el hospital para las tecnologías de información?	4			Entrevista Ingeniero Coordinador del área del área de sistemas.
6. El enfoque de aseguramiento de calidad incluye:				Revisión de la documentación del enfoque de aseguramiento de calidad para las tecnologías de información del Hospital.
▪ ¿Especificaciones sobre las revisiones o auditorías?	4			
▪ ¿Revisiones de post-implementación de las versiones del módulo, para verificar si va de acuerdo al ciclo de vida usado en versiones anteriores?		4		
▪ ¿Revisión del cumplimiento de los requerimientos nuevos del hospital para historias clínicas?		4		
▪ ¿Recomendaciones a las que se les hace seguimiento periódicamente y que son reportadas al personal administrativo encargado de la toma de decisiones del Hospital?		4		

PREGUNTA	SI	NO	NA	*FUENTE*
7. ¿Se hacen revisiones de aseguramiento de calidad, y son evaluadas de acuerdo al cumplimiento de estándares de calidad?	3			*Entrevista Ingeniero Coordinador del área del área de sistemas.*
8. ¿Existe un modelo de ciclo de vida de desarrollo de sistemas en el Hospital y esta documentado?	4			*Entrevista Ingeniero Coordinador del área del área de sistemas. Entrevista a Ingenieros del área de sistemas.*
9. El ciclo de vida de desarrollo de sistemas permite:				*Revisión del ciclo de vida usado en el módulo, y ciclo de vida del sistemas del hospital*
▪ ¿Rige el proceso de desarrollar, adquirir, implementar y mantener sistemas de información computarizados y tecnologías relacionadas?	4			
▪ ¿Soporta y fomenta los esfuerzos de desarrollo/modificación que cumplen con los planes a corto y largo plazo de TI y de la organización?	4			
▪ ¿Requiere un proceso de desarrollo o modificación estructurado que contenga puntos de revisión en momentos clave de decisión, así como la autorización para proceder con el proyecto en cada punto de revisión?	4			
▪ ¿Es escalable?	4			
▪ ¿Esta Documentado y en la diferentes versiones del módulo?		4		
▪ ¿Lleva orden secuencial de las fases como: adquisición documentación y pruebas entre otros?	4			
▪ ¿cuenta con diagramas de flujo de la programación del módulo?		4		
10. ¿El módulo de historia clínica se ha desarrollado de acuerdo al ciclo de desarrollo de sistemas que usa el software del Hospital?		4		*Entrevista a Ingeniero Coordinador del área de sistemas.*
11. ¿Los diseños de historias clínicas de las diferentes áreas se han desarrollado de acuerdo al ciclo de vida de sistemas definido para el Hospital?	4			*Entrevista a Ingenieros del área de sistemas.*
12. ¿La administración encargada del manejo de la tecnología de información hace revisiones periódicas al ciclo de vida de desarrollo de sistemas y lo mantiene actualizado?	4			*Entrevista a Ingeniero Coordinador del área de sistemas*
TOTALES	***67***	***32***		
	67/99	***32/99***		
		99		

% Riesgo = $\frac{67 * 100}{99 - 0}$ = 67% (Medio).

Tipo de Registro: Cuestionario Cuantitativo.			
ENTIDAD AUDITADA:	Hospital Universitario Departamental de Nariño		
AREA AUDITADA:	Módulo de Historia Clínica	**SISTEMA:**	Dinámica Gerencial
RESPONSABLES:	Jenny Burgos García y Maria Carolina Domínguez		
MATERIAL DE SOPORTE: COBIT			
DOMINIO:	ADQUISICION E IMPLEMENTACION : (AI)	**PROCESO:**	Adquisición y Mantenimiento De Software De Aplicación: (AI2)

PREGUNTA	SI	NO	NA	*FUENTE*
1. ¿Existe documentación del los requerimientos de diseño de historia clínica para las diferentes áreas y se especifican claramente: datos de entrada proceso y salidas?	4			*Entrevista a Ingeniero Coordinador e ingenieros del área de sistemas.*
2. ¿Los diseños de historia clínica fueron aprobados por el personal encargado (Auditoría medica y usuarios como médicos y enfermeras)?	4			*Entrevista a Ingeniero Coordinador e ingenieros del área de sistemas. Revisión de las aprobaciones de los diseños. Entrevista a Auditor Medico.*
3. ¿Existe un desarrollo de entrada de datos al módulo, de acuerdo a los requerimientos de entrada del HUDN?	4			*Entrevista al representante de SYAC. Revisión de requerimientos de entrada*
4. ¿Existe un desarrollo de procesamiento de datos del módulo, de acuerdo a los requerimientos de procesamiento del HUDN?	4			*Entrevista al representante de SYAC. Revisión de requerimientos de procesamiento*
5. ¿Los reportes generados por el módulo se desarrollaron de acuerdo a los requerimientos de salida del HUDN?	4			*Entrevista al representante de SYAC. Revisión de los reportes requeridos por el Hospital*
6. ¿Se implemento en el módulo controles internos y seguridad, de acuerdo a los requerimientos del Hospital?	4			*Entrevista al representante de SYAC. Revisión de requerimientos de control y seguridad del Hospital.*
7. Existe el desarrollo de interfases del módulo y diseño de Historia clínicas entre usuario y maquina que incluya:				*Entrevista al representante de SYAC. Entrevista a usuarios del módulo.*
▪ Que sea Amigable para el usuario.	5			
▪ Interfases fácil de usar y cumplan con los requerimientos de los médicos y enfermeras.	5			
▪ *Herramienta de ayudas y pueda autodocumentarse.*		*5*		

PREGUNTA	SI	NO	NA	*FUENTE*
8. Dentro de las diferentes opciones del módulo y los diseños de historia clínica se hayan realizado las validaciones necesarias según el tipo de información que se maneja.		5		*Revisión de las diferentes interfases del Módulo de Historia Clínica.*
9. ¿Dentro de la metodología del ciclo de desarrollo de sistema se incluye:				*Revisión de la metodología del ciclo de vida de desarrollo de sistemas*
▪ Continua comunicación entre los usuarios del módulo: médicos y enfermeras y los diseñadores de las historias clínicas.		4		
▪ Existen mecanismos adecuados para la recopilación de requerimientos de entrada procesamiento y salida de datos.	4			
▪ Existen mecanismos adecuados para la recopilación de requerimientos de control interno y seguridad.		4		
10. ¿Existen manuales de referencia para los usuarios del módulo de historia clínica?	4			*Entrevista a Representante de SYAC Entrevista a usuarios, revisión de los manuales de usuario.*
11. ¿Existen políticas y procedimientos para mantener actualizado el manual de usuario?	4			*Entrevista a Ingeniero de SYAC*
12 ¿Los manuales de referencia para usuarios se encuentran actualizados?	4			*Revisión de la fecha de los manuales de usuarios*
13. Los manuales de referencia a usuarios contiene:				*Revisión del manual de usuarios*
▪ Especificaciones de todos lo botones del módulo.	4			
▪ Manejo de módulo de forma secuencial.	4			
▪ Especificaciones de las diferentes interfases del módulo.	4			
▪ Se encuentra en formato digital para facilitar su consulta.	4			
14. ¿Existe un plan de pruebas para el módulo y la aprobación del usuario?		3		*Entrevista a representante de SYAC. Entrevista a Ingenieros del área de sistemas, y usuarios finales*
15. El plan de pruebas incluye:				*Revisión del plan de pruebas.*
▪ Reevaluación de las interfases de historia clínicas, verificando que cumplan con los diseños aprobados por Auditoría médica y usuarios.		3		
▪ Evaluación de los aspectos de seguridad del módulo, verificando que cumple con los requerimientos del hospital.		3		
▪ Pruebas de usuarios para aceptación del módulo.		3		
▪ Prueba a los procesos de entrada, salida y procesamiento de datos.		3		
▪		3		
TOTALES	***66***	***36***		
TOTAL ENCUESTA	***102***			

% Riesgo = $\frac{66 * 100}{102 - 0}$ = 64% (Medio)

Tipo de Registro: Cuestionario Cuantitativo.			
ENTIDAD AUDITADA:	Hospital Universitario Departamental de Nariño		
AREA AUDITADA:	Módulo de Historia Clínica	**SISTEMA:**	Dinámica Gerencial
RESPONSABLES:	Jenny Burgos García y Maria Carolina Domínguez		
MATERIAL DE SOPORTE: COBIT			
DOMINIO:	ADQUISICION E IMPLEMENTACION : (AI)	**PROCESO:**	Instalación Y Acreditación De Sistemas: (AI5)

PREGUNTA	SI	NO	NA	*FUENTE*
1. ¿Existen políticas y procedimientos en relación al ciclo de vida de desarrollo de sistemas para la acreditación de los mismos?	4			*Entrevista a Ingeniero Coordinador del área de sistemas.*
2. ¿Existe una metodología formal de ciclo de vida de desarrollo de sistemas para la instalación y acreditación de sistemas?	4			*Entrevista a Ingeniero Coordinador del área de sistemas.* *Entrevista Al representante de SYAC.*
3. La metodología formal de ciclo de vida de desarrollo incluye:				*Revisión de la documentación relacionada con la metodología del ciclo de vida.* *Entrevista a Ingeniero Coordinador del área de sistemas, entrevista al representante de SYAC.*
▪ Entrenamiento a Ingenieros a cargo del módulo de historia clínica.		4		
▪ Adecuación de desempeño.	4			
▪ Pruebas del módulo.		4		
▪ Pruebas prototipo y paralelo.		4		
▪ Pruebas de aceptación de usuarios.	4			
▪ Pruebas y acreditación de seguridad.		4		
▪ Pruebas operativas.	4			
▪ Controles de cambio.		4		
▪ Revisiones de modificaciones e implementaciones.	4			
▪ Pruebas de post-implementación.		4		
4. ¿Existe un programa de entrenamiento para los ingenieros a cargo del desarrollo de los diseños de historias clínicas, mediante la herramienta de WINDG?	*3*			*Entrevista a representante de SYAC* *Entrevista a ingenieros del área de sistemas a cargo del módulo de historia clínica*

PREGUNTA	SI	NO	NA	*FUENTE*
5. El programa de entrenamiento contiene:				*Revisión del programa de entrenamiento. Entrevistas a Ingenieros a cargo el módulo de historia clínica.*
▪ Diferencias con respectos a otros módulos de Dinámica gerencial.		3		
▪ Cambios que afecten las entradas procesamientos y salidas de datos.	3			
▪ Programación de actividades.	3			
▪ Interacción con otros módulos del sistema dinámica gerencial.	3			
▪ Errores y corrección de errores.		3		
▪ Concientización de los usuarios sobre sus responsabilidades en el diseño, aprobación, pruebas del módulo de historia clínica.	3			
6. ¿Existe un plan de pruebas para todas las áreas de los recursos del sistema?		3		*Entrevista a ingeniero representante de SYAC Entrevista a ingeniero coordinador del área de sistemas.*
7. El plan te pruebas tiene una cobertura a las áreas de:				*Revisión del plan de pruebas de los diferentes recursos del sistema.*
▪ Software de aplicación.		3		
▪ Instalaciones.		3		
▪ Tecnología.		3		
▪ Usuarios.		3		
8. ¿El personal encargado de los diseños de historia clínica en el sistema dinámica gerencial y la administración aseguran, el cumplimiento de los requerimientos de los usuarios (médicos y enfermeras) y los requerimientos del hospital en relación a la gestión de historias clínicas?	4			*Entrevista a Ingenieros del área que realizaron los diseños de historia clínica, Ingeniero coordinador desistemas.*
9. ¿Se ha establecido un programa de actividades, para el proceso recopilación de requerimientos y diseños de historias clínicas y se han cumplido en las fechas estipuladas?	4			*Entrevista a ingeniero coordinador del área de sistemas, entrevistas a ingenieros a cargo del módulo de Historia clínica.*
10. ¿La empresa SYAC proveedora del módulo ha cumplido con las fechas limites de las actividades programadas en relación a la implantación del módulo?	4			*Entrevista a Ingeniero Coordinador del área de sistemas. Entrevista a representante de SYAC.*
11. ¿Existe políticas para la escogencias de proveedores de tecnologías de información al hospital?	2			*Entrevista a Ingeniero Coordinador*
12. ¿Se han realizado mediciones o evaluaciones para determinar la satisfacción del usuario final?	2			*Entrevista a representante de SYAC. Entrevista a ingeniero coordinador del área de sistemas y a usuarios finales.*
13. ¿El usuario a participado activamente de las actividades relacionadas con la implantación del módulo de historia clínica?	3			*Entrevista a representante de SYAC. Entrevista a ing. coordinador del área y a usuarios finales. Entrevista a ingenieros del área de sistemas*
TOTALES	***58***	***45***		
	58/103	***45/103***		
TOTAL ENCUESTA	***103***			

$$\% \text{ Riesgo} = \frac{58 * 100}{103 - 0} = 56\% \text{ (Medio)}$$

Tipo de Registro: Cuestionario Cuantitativo.			
ENTIDAD AUDITADA:	Hospital Universitario Departamental de Nariño		
AREA AUDITADA:	Módulo de Historia Clínica	**SISTEMA:**	Dinámica Gerencial
RESPONSABLES:	Jenny Burgos García y Maria Carolina Domínguez		
DOMINIO:	ADQUISICION E IMPLEMENTACION : (AI)	**PROCESO:**	Administración De Cambios: (AI6)

PREGUNTA	SI	NO	NA	*FUENTE*
1. ¿Existen políticas o normas en el Hospital relacionados con la implantación de sistemas de información y el control de cambios?		3		*Entrevista a Ingeniero Coordinador del área de sistemas.*
2. ¿El control de cambios es un procedimiento formal para el personal de área de sistemas, relacionados con el manejo del módulo de historia clínica?		3		*Entrevista a Ingeniero Coordinador del área de sistemas, e Ingenieros del área de sistemas a cargo del módulo de historia clínica.*
3. ¿Se lleva una documentación en bitácoras del monitoreo del proceso de cambios en el módulo de historia clínica?		3		*Entrevista a Ingenieros a cargo del módulo.*
4. Dentro del registro en la bitácoras para el control e cambios se incluye:				*Revisión de la documentación o bitácoras del proceso de cambios.*
▪ Registro de si los cambios fueron resueltos a satisfacción e los usuarios.		3		
▪ Registro de todos lo cambios realizados al módulo.	3			
▪ fecha del cambio solicitado	3			
▪ persona(s) que lo solicitan	3			
▪ solicitud aprobada de cambios	3			
▪ aprobación del cambio realizado - función de servicios de información	3			
▪ aprobación del cambio realizado – usuarios		3		
▪ fecha de actualización de documentación	3			
▪ aprobación del cambio por parte de aseguramiento de la calidad		3		
▪ aceptación por parte de operaciones		3		
5. ¿Existen el uso de otras herramientas informáticas como programas y plataformas que permitan el tramite de cambios para el módulo?	*2*			*Entrevista a representante de SYAC Entrevista a ingenieros a cargo el módulo.*

PREGUNTA	SI	NO	NA	*FUENTE*
6. ¿El uso de estas herramientas informáticas permiten hacer un monitoreo de los cambios?	2			*Entrevista a representante de SYAC* *Entrevista a ingenieros a cargo el módulo.*
7. Para la realización de un cambio se llevan a cabo los siguientes pasos:				*Revisión en la documentación sobre solicitud de cambios.*
▪ Solicitud del cambio.	2			
▪ Especificación el Cambio.	2			
▪ Realización de pruebas sobre el cambio.	2			
▪ Prueba de aceptación por parte del usuario.	2			
▪ Determinación y aceptación del impacto general y específico por parte de la Gerencia.	2			
▪ Proceso de distribución, (capacitación a los usuarios finales sobre el manejo el cambio en el módulo)	2			
TOTALES	***34***	***21***		
	34/55	*21/55*		
	55			

$$\% \text{ Riesgo} = \frac{34 * 100}{55 - 0} = 61\% \text{ (Medio)}$$

Tipo de Registro: Cuestionario Cuantitativo.			
ENTIDAD AUDITADA:	Hospital Universitario Departamental de Nariño		
AREA AUDITADA:	Modulo de Historia Clínica	**SISTEMA:**	Dinámica Gerencial
RESPONSABLES:	Jenny Burgos García y Maria Carolina Domínguez		
MATERIAL DE SOPORTE: COBIT			
DOMINIO:	ENTREGA Y SOPORTE	**PROCESO:**	Administración De Servicios Prestados Por Tercero: (DS2)

PREGUNTA	SI	NO	NA	*FUENTE*
1. Existen políticas para:				Entrevista Ingeniero Coordinador del Área de Sistemas
• Creación de contratos informáticos con terceros?	5			
• Definición del contenido de los contratos en cuanto a la propiedad o administración del módulo?		5		
• Mantenimiento, monitoreo y renegociación de los contratos.	5			
2. Existen políticas para:				Entrevista a Ingeniero Coordinador del área de sistemas e ingenieros de soporte de SYAC
• Políticas de manejo se seguridad lógica y física, con terceros?		5		
• Acuerdo de confidencialidad para relaciones con terceras partes.	5			
• Escoger al proveedor de servicios Informáticos?	3			
3. ¿El contrato representa un registro completo de las relaciones con proveedores como tercera persona?	4			Revisión del contrato de outsourcing con SYAC módulo de historia Clínica

PREGUNTA	SI	NO	NA	FUENTE
4. El contenido de los contratos incluye lo siguiente:				Verificación del contrato de modulo de historia clínica electrónica con sistemas y asesorias de Colombia SYAC
- aprobación formal administrativa y legal	4			
- entidad legal que proporciona los servicios	4			
- servicios proporcionados	4			
- acuerdos cualitativos y cuantitativos de nivel de servicio	3			
- costo de los servicios y frecuencia de su pago	5			
- proceso de solución de problemas	4			
- sanciones por bajo desempeño	4			
- proceso de disolución	4			
- proceso de modificación	4			
- reporte de servicio - contenido, frecuencia y distribución	4			
- funciones entre las partes del contrato durante la vida del mismo	4			
- aseguramiento de continuidad que indica que el servicio será proporcionado por el proveedor	5			
- usuarios de los servicios y procesos y frecuencia de las comunicaciones del proveedor	4			
- duración del contrato	5			
- nivel de acceso proporcionado al proveedor	5			
- requerimientos de seguridad	5			
- garantías de confidencialidad	5			
- derecho a acceso y derecho a auditar	5			
- Especificaciones del sistema a contratar.	4			
- Especificaciones de los programas a desarrollar.	4			
- Pruebas de aceptación.	4			
- Resultados a obtener y que, en algún caso, formaran el propio objeto del contrato.	4			
5. Los acuerdos escritos han sido negociados apropiadamente		3		Revisión de contrato entre SYAC y HUDN
6. Los terceros en potencia se han calificado adecuadamente mediante la evaluación de sus habilidades para proveer el servicio requerido (especial cuidado)		2		Revisión de contrato entre SYAC y HUDN

PREGUNTA	SI	NO	NA	*FUENTE*
7. Los anexos del contrato se incluyen:				*Revisión de contrato entre SYAC y HUDN*
- Especificaciones del sistema a contratar.		3		
- Especificaciones de las tareas o procesos a desarrollar.		3		
TOTALES	***116***	***21***		
	116/137	***21/137***		
TOTAL ENCUESTA	***137***			

% Riesgo = $\frac{116 * 100}{137 - 0}$ = 84% (Alto)

Tipo de Registro: Cuestionario Cuantitativo.			
ENTIDAD AUDITADA:	Hospital Universitario Departamental de Nariño		
AREA AUDITADA:	Modulo de Historia Clínica	**SISTEMA:**	Dinámica Gerencial
RESPONSABLES:	Jenny Burgos García y Maria Carolina Domínguez		
MATERIAL DE SOPORTE: COBIT			
DOMINIO:	ENTREGA DE SERVICIOS Y SOPORTE: (DS)	**PROCESO:**	Administración de Desempeño y Capacidad : (DS3)

PREGUNTA	SI	NO	NA	FUENTE
1. ¿Existen Políticas y procedimientos del Hospital en relación al reporte del desempeño del modulo, carga de trabajo, administración de la capacidad y programación de actividades?	4			Entrevista al Representante de SYAC Ingeniero Coordinador Área de sistemas
2. ¿Existen Políticas y procedimientos para el modulo de historia clínica en relación a la disponibilidad de la organización, la planeación de la disponibilidad y el monitoreo?	4			Entrevista al Representante de SYAC Ingeniero Coordinador Área de sistemas
3. ¿Existen representaciones del producto por parte del proveedor con respecto a las normas de capacidad y desempeño? Si existen en estos se incluyen: • Una lista de todos los productos actuales de software de SYAC. • Reportes de monitoreo de redes de comunicación • Minutas de las reuniones en las que se discuten la planeación de la capacidad, las expectativas de desempeño y la "afinación" del desempeño. • Documentos de disponibilidad, capacidad, carga de trabajo y planeación de recursos. • Reportes relacionados con el desempeño operativo dentro de la función de servicios de información, incluyendo el reporte y la historia de la solución de problemas.	3 2 2 5 5 5			Entrevista al Representante de SYAC Ingeniero Coordinador Área de sistemas
4. Existe un plan de disponibilidad, está actualizado y refleja los requerimientos del usuario	4			Entrevista a Ingeniero Coordinador del área de sistemas.

PREGUNTA	SI	NO	NA	*FUENTE*
5. Existe una lista de todos los productos actuales del proveedor en lo referente a, software, hardware (si lo provee) comunicaciones y periféricos (si los provee)?	3			*Entrevista a Ingeniero Coordinador del área de sistemas y a Técnico en mantenimiento.*
6. Existen los Reportes relacionados con el desempeño operativo dentro de la función de servicios de información, incluyendo el reporte y la historia de la solución de problemas?	4			*Entrevista a Ingenieros del área de Información y sistemas del HUDN.*
7. Se lleva a cabo y se reporta un monitoreo continuo del desempeño de todo el equipo y de la capacidad, y si la falta de un desempeño adecuado es considerada por la administración y si se consideran formalmente las oportunidades de mejoras al desempeño	4			*Entrevista a Ingeniero Coordinador del área de sistemas.*
TOTALES	***45***	***0***	***0***	
	45/45	***0/45***		
TOTAL ENCUESTA	***45***			

$$\% \text{ Riesgo} = \frac{45 * 100}{45 - 0} = 100\% \text{ (Alto)}$$

Tipo de Registro: Cuestionario Cuantitativo.			
ENTIDAD AUDITADA:	Hospital Universitario Departamental de Nariño		
AREA AUDITADA:	Modulo de Historia Clínica	**SISTEMA:**	Dinámica Gerencial
RESPONSABLES:	Jenny Burgos García y Maria Carolina Domínguez		
DOMINIO:	ENTREGA DE SERVICIOS Y SOPORTE (DS)	**PROCESO:**	Garantizar La Seguridad De Sistemas : (DS5)

PREGUNTA	SI	NO	NA	FUENTE
1. ¿Existen Políticas y procedimientos globales de la Institución referentes a la seguridad y el acceso de los sistemas de información? (en general)	5			Entrevista Ing. Coordinador de área de sistemas
2. ¿Existen Políticas y procedimientos de TI relacionadas con: seguridad y acceso Al modulo de historia clínica?	5			Entrevista a Ingeniero representante de SYAC. Entrevista a Ingenieros del área de sistemas encargados del diseño de historias clínicas.
3. ¿Existen Políticas de seguridad que son exigidas legalmente al Hospital para temas servicios de salud en Historias clínica, que incluye:				
• Administración de cuentas de usuarios.	4			
• Política de seguridad del usuario o de protección de la información.	4			
• Estándares relacionados con el comercio electrónico.	4			
• Procedimientos de control de cambios de software de seguridad.	4			
• Reportes de violaciones a la seguridad y procedimientos de revisión administrativa.	4			
• Inventario de dispositivos de encriptación de datos y de estándares de encriptación.	3			
• Lista de los proveedores y clientes con acceso a los recursos del modulo de Historia Clínica.	4			
• Proveedor de servicios de transmisión de datos al hospital, (proveedor de Internet).	4			
• Practicas de administración de redes relacionadas con pruebas contiguas de seguridad.	4			
• Copias de documentos firmados por los usuarios relacionados con seguridad y concientización.	4			
• *contenido del material de entrenamiento de seguridad para los usuarios del modulo.*	4			

PREGUNTA	SI	NO	NA	FUENTE
4. ¿Existe un esquema de clasificación de datos en operación que indique que todos los recursos del sistema cuentan con un propietario responsable de su seguridad y contenido?	3			Entrevista a Ingeniero representante de SYAC. Entrevista a Ingenieros del área de sistemas encargados del diseño de historias clínicas.
5. Se cuenta con reporte de fallos a la seguridad (si es afirmativo marque los ítems): • intentos no autorizados • acceso al sistema (signo n) • intentos no autorizados para consultar o modificar las definiciones y reglas de seguridad • privilegios de acceso a recursos por ID de usuario • modificaciones autorizadas a las definiciones y reglas de seguridad • accesos autorizados a los recursos • cambio de status de la seguridad del sistema	 4 4 4 4 3 3 2			Entrevista ing. Coordinador del área de sistemas, Entrevista a Técnico en sistemas.
6. ¿Existen módulos criptográficos y procedimientos de mantenimiento de llaves, si estos son administrados centralizadamente, y si son utilizados para todas las actividades de acceso externo y de transmisión?	2			Entrevista ing. Coordinador del área de sistemas
7. ¿Existen estándares de administración de llave criptográfica tanto para la actividad centralizada como para la de los usuarios?	*2*			Entrevista ing. Coordinador del área de sistemas
8. Los mecanismos de autenticidad en uso proveen las siguientes facilidades: • uso individual de datos de autenticación (ej: password nunca son reutilizados) • se realizan actualizaciones periódicas de passwords? • Autentificación múltiple (Se utilizan dos o mas mecanismos de autentificación diferentes)	 *3* *3* *3*			Entrevista ing. Coordinador del área de sistemas
9. El número de sesiones concurrentes correspondiente al mismo usuario están limitadas?	*2*			Entrevista ing. Coordinador del área de sistemas
10. Al ingresar al sistema aparece un mensaje de advertencia preventivo en relación al uso adecuado del hardware, software o conexión?	*3*			Entrevista ing. Coordinador del área de sistemas
11. Se despliega una pantalla de advertencia antes de completar la entrada para informar al lector que los accesos no autorizados podrían causar responsabilidades legales?	*3*			Entrevista ing. Coordinador del área de sistemas
12. Existe una política para manejo de passwords? Si existe entonces a los usuarios se les informa o se les forza a: • ¿Cambio inicial de password la primera vez de uso? • ¿Longitud adecuada mínima del password? • Verificación de password en la lista de valores no permitidos (ver. Dd) • Protección adecuada para los password de emergencia?	*3* *2* *2* *2* *2*			Entrevista ing. Coordinador del área de sistemas
13. El procedimiento formal para la resolución de problemas incluye: • ID de usuario suspendido después de 5 intentos de entrada fallidos • ¿Fecha del último acceso y el número de intentos fallidos se despliega al usuario autorizado una vez ingresado? ¿El tiempo de autenticación se limita?	 *2* *2* *2*			

PREGUNTA	SI	NO	NA	*FUENTE*
• ¿Hay desactivación de claves de acceso a los empleados temporales?	2			*Entrevista ing. Coordinador del área de sistemas.*
TOTALES	***120***	***0***		
	120/120			
TOTAL ENCUESTA	***120***			

% Riesgo = $\frac{120 * 100}{120 - 0}$ = 100% (Alto)

Tipo de Registro: Cuestionario Cuantitativo.			
ENTIDAD AUDITADA:	Hospital Universitario Departamental de Nariño		
AREA AUDITADA:	Modulo de Historia Clínica	**SISTEMA:**	Dinámica Gerencial
RESPONSABLES:	Jenny Burgos García y Maria Carolina Domínguez		
MATERIAL DE SOPORTE: COBIT			
DOMINIO:	ENTREGA DE SERVICIOS Y SOPORTE DS	**PROCESO:**	Educación Y Entrenamiento De Usuarios: (DS7)

PREGUNTA	SI	NO	NA	FUENTE
1. Existen políticas y procedimientos generales para la organización con respecto al entrenamiento sobre controles y conciencia de seguridad, beneficios para los empleados enfocados al desarrollo, programas de entrenamiento para los usuarios de servicios, instalaciones educacionales y requerimientos de educación continua profesional?.		5		Entrevista a Ing. Coordinador de área de sistemas
2. Existen Programas, políticas y procedimientos de entrenamiento y de educación de TI relacionados con concientización en controles y seguridad, controles y seguridad técnica		4		Entrevista a Ing. Coordinador de área de sistemas
3. Revisión de Programas de entrenamiento disponibles (tanto internos como externos) para concientización en controles y seguridad introductorias y continuos así como entrenamiento dentro de la organización.		4		Revisión de Documentación correspondiente a capacitación del personal.
4. Se cuenta con un programa de educación/entrenamiento enfocado a los principios de seguridad y control de los sistemas de información		4		Revisión de Documentación correspondiente a capacitación del personal.
5. Existe disponibilidad de oportunidades y frecuencia de entrenamiento interno, considerando también la asistencia de los empleados	3			Revisión de Documentación correspondiente a capacitación del personal
6. Se cuenta con políticas y procedimientos vigentes relacionados con entrenamiento y si éstos están actualizados con respecto a la configuración técnica de los recursos de TI?.	5			Entrevista a Ing. Coordinador de área de sistemas.
7. Los nuevos empleados tienen conocimiento y conciencia de la responsabilidad de seguridad y control con respecto a la utilización y la custodia de los recursos de TI.		4		Entrevista a Ing. Coordinador de área de sistemas.

PREGUNTA	SI	NO	NA	*FUENTE*
8. Se requiere a todos los empleados asistir a entrenamientos de conciencia de control y seguridad continuamente, los cuales incluirían, sin limitarse a:		3		Entrevista a Ing. Coordinador de área de sistemas
• principios generales de seguridad de sistemas		3		
• conducta ética de TI		3		
• prácticas de seguridad para la protección contra daños ocasionados por fallas que afecten la disponibilidad, • confidencialidad, integridad y desempeño de las funciones en una forma segura		3 3		
9. Dentro de los manuales de entrenamiento para usuarios finales, se ha incluido temas relacionados a los controles de seguridad, confidencialidad, confiabilidad, disponibilidad e integridad de la información?		4		Verificación de los manuales de entrenamiento de usuarios o de capacitación de los mismos.
10. En lo referente a capacitación de Usuarios: ¿Se brindan asesorías y soporte en las áreas que se requiera? ¿Se imparten cursos de capacitación a personal asistencial temporal? ¿Existe un reglamento para proporcionar estos servicios? ¿Existe un horario definido para dar alguno de estos servicios? ¿Existen procedimientos para solicitar estos servicios? ¿Existe el personal calificado para proporcionar este tipo de servicios?	 4 4 4 4 3 3			
	30	***40***		
	30/70	***40/70***		
		70		

$$\% \text{ Riesgo} = \frac{30 * 100}{70 - 0} = 42\% \text{ (Medio)}$$

Tipo de Registro: Cuestionario Cuantitativo.			
ENTIDAD AUDITADA:	Hospital Universitario Departamental de Nariño		
AREA AUDITADA:	Modulo de Historia Clínica	**SISTEMA:**	Dinámica Gerencial
RESPONSABLES:	Jenny Burgos García y Maria Carolina Domínguez		
MATERIAL DE SOPORTE: COBIT			
DOMINIO:	ENTREGA DE SERVICIOS Y SOPORTE DS	**PROCESO:**	Administración de la configuración DS9

PREGUNTA	SI	NO	NA	FUENTE
1. Existe un inventario de la configuración: hardware, software de sistema operativo, software de aplicaciones, instalaciones y archivos de datos –dentro y fuera de las instalaciones (CE)?.	4			Entrevista a Coordinador del área de sistemas, Entrevistas a Técnico en mantenimiento.
2. Existen políticas y procedimientos organizacionales relacionados con la adquisición, inventario y disposición de software y equipo computacional comprado, rentado o arrendado con opción de compra	4			Entrevista a Coordinador del área de sistemas, Entrevistas a Técnico en mantenimiento
3. Existen políticas organizacionales relacionadas con la utilización de software o equipo no autorizado?	3			Entrevista a Coordinador del área de sistemas, Entrevistas a Técnico en mantenimiento
4. Existen políticas y procedimientos de la función de servicios de información relacionados específicamente con la adquisición, disposición y mantenimiento de los recursos de la configuración?	3			Entrevista a Coordinador del área de sistemas, Entrevistas a Técnico en mantenimiento
5. Existen políticas y procedimientos de TI relacionados con las funciones de aseguramiento de la calidad y de control de cambios en cuanto a la transferencia independiente y el registro de la migración del desarrollo de software nuevo y modificado hacia los archivos y estatus de producción		3		Entrevista a Coordinador del área de sistemas, Entrevistas a Técnico en mantenimiento
6. Existe un Inventario del contenido del almacenamiento externo– equipo, archivos, manuales y formas – incluyendo material en manos de los proveedores?	4			Entrevista a Coordinador del área de sistemas, Entrevistas a Técnico en mantenimiento

PREGUNTA	SI	NO	NA	*FUENTE*
TOTALES	***18***	***3***		
	18/21	***3/21***		
TOTAL ENCUESTA	***21***			

% Riesgo = $\frac{18 * 100}{21 - 0}$ = 85 % (Alto)

FIRMAS AUDITORES RESPONSABLES:

JENNY BURGOS GARCIA:

MARIA CAROLINA DOMINGUEZ

4.2.4. Plan de Pruebas

El plan de pruebas es una herramienta muy importante en el desarrollo de la auditoría, en este se puede programar de forma secuencial, las diferentes pruebas a realizarse en base a los aspectos observados por el auditor durante el desarrollo del proyecto, el plan de pruebas permite definir el tipo de prueba, como se realizara la prueba y el tiempo estimado para desarrollo, a continuación se muestra el plan de pruebas diseñado para este proyecto:

PRUEBA	PROCESO	TIPO	QUE SE VA HA COMPARAR	TIEMPO
- Análisis del Manual de Sistema del Módulo de Historia Clínica electrónica. (1)	PO2	ANALISIS	Se compara, la documentación que forma parte del manual del sistema, puesto que no existe formalmente un manual técnico del sistema, con las especificaciones que para nuestro criterio y conocimiento, debe contener este tipo de manual.	1 HORA
- Análisis del Modelo y Diccionario de Datos del Módulo de Historia Clínica Electrónica. (6)	PO2	EJECUCION	Se analizara el diccionario de datos y se revisara que cuente con la información necesaria descrita en este tipo de manual, tomando como criterio el planteamiento del COBIT, igualmente se compara la correspondencia del diccionario de datos y la base de datos en producción.	3 HORAS
- Revisión de la base de datos, para verificar si los datos están clasificados según algún tipo de criterio. (16,17,18)	PO2	EJECUCION	Se revisara en la base de datos, como se encuentran definidos los datos, se revisara los niveles de acceso, si existe algún tipo de protección, se verificara si hay inconsistencias en los datos y si existen datos obsoletos.	2 HORA
- Revisión de los tipos de usuarios que pueden ingresar al sistema, verificando los recursos del módulo a los que tienen acceso. (16,17,18)	PO2	EJECUCION	Se ingresará con los password creados para las pruebas y capacitaciones, a las diferentes áreas: como triage, urgencias, hospitalización y enfermería, para verificar que los recursos a los que tienen acceso correspondan a su usuario.	1 HORA

PRUEBA	PROCESO	TIPO	QUE SE VA HA COMPARAR	TIEMPO
- Revisión de cumplimiento de los requerimientos externos y gubernamentales en el módulo y en el diseño de las historias clínicas. (3-)	PO8	EJECUCION	Se revisara que el diseño de la historia clínica de urgencia contenga la información del ítem XI de formato de historia clínica que corresponde al registro de Lesión de causa externa. Se verificara en el módulo que se cumpla con la resolución 3881 del 21/04/1982, es decir que cumpla con: integridad, secuencialidad, racionalidad, disponibilidad oportunidad, hoja de identificación e Historia clínica de ingreso (identificación, anamnesis, antecedentes familiares y personales, examen físico, impresión diagnostica y conducta entre otros).	1 HORA
- Análisis de las normas de seguridad y ergonomía, para el recurso humano involucrado con el manejo el módulo de historia clínica. (5)	PO8	ANALISIS	Analizar que existan políticas de ergonomía y seguridad, analizar que el programa de salud ocupacional contengan todos los temas de seguridad personal, situaciones correctas de ergonomía y seguridad, causas de accidentes de trabajo, programa de capacitaciones.	1 HORA
- Analizar las políticas para el aseguramiento del software y la gestión de contratos con aseguradoras. (10)	PO8	ANALISIS	Analizar que el contrato con la aseguradora cumpla con las políticas expuestas para el aseguramiento del software.	1 HORA
- Análisis de la documentación de la metodología de evaluación de riesgos. (2)	PO9	ANALISIS	Analizar si la documentación de la metodología de la evaluación de riesgos contiene aspectos relacionados con: Mantenimiento de hardware y de red, manejo del usuario de sus recursos de software y hardware, cambios en los requerimientos de usuarios, cambios de requerimientos externos, seguridad en los usuarios, seguimiento a incidentes ocurridos anteriormente y gestión de riesgos.	1 HORA
- Análisis de seguro contra riesgos. (13, 14)	PO9	ANALISIS	Verificar que el seguro contra riesgos contenga: desastres naturales (incendio, inundación, terremotos tornados entre otros), violación de la información por parte de usuarios, perdida de información de pacientes.	30 minutos
- Análisis del plan de calidad en relación a las tecnologías de información. (2,3)	PO11	ANALISIS	Analizar que el plan de calidad contenga: Planeación a corto y largo plazo, la infraestructura de información requerida para soportar los sistemas e interfases, capacitaciones del personal involucrado con el módulo, recursos financieros y humanos, filosofía de mejoramiento continúo.	1 HORA

PRUEBA	PROCESO	TIPO	QUE SE VA HA COMPARAR	TIEMPO
- Análisis del plan de calidad (Gerencia de la Información) en relación a las tecnologías de información. (3)	PO11	ANALISIS	Revisar si el plan de calidad se encuentra actualizado, si se hace una revisión o seguimiento de su cumplimiento, y si existen métricas para medir las actividades de las metas de calidad en el hospital, y como se encuentra el estándar de gerencia de la información del Hospital en relación a estándares de certificación como la ISO 27001.	1 HORA
- Análisis del modelo del ciclo de vida de desarrollo de sistemas. (8,9)	PO11	ANALISIS	Determinar si el ciclo de vida de desarrollo de sistemas permite: desarrollar, adquirir, implementar y mantener sistemas de información computarizados y tecnologías relacionadas, si cumple con los planes a corto y largo plazo de la gerencia y el área de sistemas, si es escalable y permite lleva un orden secuencial de las diferentes fases de los ciclo de vida.	1 HORAS
- Revisión del cumplimiento de los requerimientos de entrada para el módulo de historia clínica. (3)	AI2	EJECUCION	Comparar si las interfases del módulo y los diseños de historia clínica, suplen los **requerimientos de Entrada** del hospital y de los usuarios finales como médicos y enfermeras, en cada una de las áreas o especialidades como: triage, urgencias, hospitalización y consulta externa. Verificar si las opciones de diagnostico corresponde a los requerimientos del hospital.	2 HORA
- Revisión del cumplimiento de los requerimientos de procesamiento para el módulo de historia clínica. (4)	AI2	EJECUCION	Comparar si las interfases del módulo y los diseños de historia clínica, suplen los **requerimientos de Procesamiento** del hospital y de los usuarios por areas.	2 HORA
- Revisión del cumplimiento de los requerimientos de salida para el módulo de historia clínica. (5)	AI2	EJECUCION	Comparar si las interfases del módulo y los diseños de historia clínica, contienen la información correspondiente a **los requerimientos de salida** del hospital en las diferentes áreas. Verificar si las opciones de conducta como: Referencia, contrareferencia, salida y Hospitalización, corresponden a los requerimientos de salida del hospital y de igual manera los reportes como: Ordenes médicas, exámenes auxiliares, hoja de droga entre otros están acorde a las necesidades de la institución.	2 HORAS
- Revisión de los controles internos y seguridad del módulo, verificando que cumplan los requerimientos del Hospital. (6)	AI2	EJECUCION	Revisar en el módulo de historia clínica que existan **controles de seguridad**, en relación a la asignación de claves de usuarios, verificar que sea posible cambiar continuamente estas claves, y que exista la clasificación de acceso de usuarios a los recursos del módulo.	2 HORAS

PRUEBA	PROCESO	TIPO	QUE SE VA HA COMPARAR	TIEMPO
- Revisión de las interfases del módulo de Historia clínica. (7)	AI2	EJECUCION	Verificar que las interfases del módulo sean amigables, es decir que sean de fácil manejo para los usuarios finales (médicos y enfermeras), determinar si cumplen con los requerimientos de los usuarios, verificar que existan herramientas de ayuda que le permitan al usuario operar el módulo en situaciones particulares.	2 HORAS
- Revisión de las validaciones del módulo. (8)	AI2	EJECUCION	Verificar que dentro de las diferentes opciones del módulo y los diseños de historia clínica se hayan realizado las validaciones necesarias según el tipo de información que se maneja.	2 HORAS
- Revisión del ciclo de vida de desarrollo de sistemas. (9)	AI2	ANALISIS	Revisar si las especificaciones del ciclo de vida de desarrollo de sistemas incluyen: la comunicación con el usuario, mecanismos para la recopilación de requerimientos de entrada, procesamiento, salida de datos y controles de seguridad.	1 HORA
- Revisión de los manuales de usuario. (13)	AI2	ANALISIS	Revisar si el manual de usuario contiene información sobre: especificaciones de todos lo botones del módulo, manejo de módulo de forma secuencial, especificaciones y manejo de las diferentes interfases del módulo.	1 y ½ HORA
- Revisión del plan de pruebas. (15)	AI2	ANALISIS	Revisar si el plan de pruebas incluye: reevaluación de interfases, aspectos de seguridad, satisfacción de usuario, entradas procesos y salidas etc.	1 HORA
- Revisión de la metodología del ciclo de vida de desarrollo de sistemas. (3)	AI5	ANALISIS	Revisar si la metodología del ciclo de vida de desarrollo de sistemas incluye: entrenamiento a Ingenieros, adecuación de desempeño, pruebas del módulo, pruebas prototipo y paralelo, pruebas de aceptación de usuarios, pruebas y acreditación de seguridad, pruebas operativas, controles de cambio, revisiones de modificaciones e implementaciones, pruebas de post-implementación.	1 HORA
- Revisión del programa de entrenamiento para los Ingenieros del área de sistemas, en relación al proceso de implantación del módulo y los diseños de historias clínica.(5)	AI5	ANALISIS	Determinar si el la documentación sobre el entrenamiento de usuarios incluye: - Diferencias con respectos a otros módulos de Dinámica gerencial. - Cambios que afecten las entradas procesamientos y salidas de datos. - Programación de actividades. - Interacción con otros módulos del sistema dinámica gerencial.	1 HORA

PRUEBA	PROCESO	TIPO	QUE SE VA HA COMPARAR	TIEMPO
			- Errores y corrección de errores. - Concientización de los usuarios sobre sus responsabilidades en el diseño, aprobación, pruebas del módulo de historia clínica.	
- Revisión del cronograma de actividades para la implantación del módulo de Historia Clínica.(9)	AI5	ANALISIS	Verificar el cumplimiento del cronograma de actividades para la implantación del módulo de historia clínica, como: fechas limites para recolección de requerimientos, entrega de diseño de historias clínica, capacitación de usuarios, realización de pruebas, instalación en las diferentes áreas y puesta en producción.	1 HORA
- Programa de entrenamiento para usuarios finales (médicos y enfermeras) (13).	AI5	ANALISIS	Verificar que exista: Buena comunicación con los usuarios, programación de capacitaciones, registro de capacitación de usuarios, talleres de capacitación, aprobación de usuarios.	1 HORA
- Revisión de la documentación que se lleva sobre los cambios realizados en el módulo de historia clínica.(4)	AI6	ANALISIS	Determinar si dentro de la documentación del seguimiento de cambios incluye: -Registro de si los cambios fueron resueltos a satisfacción e los usuarios. - Registro de todos lo cambios realizados al módulo. - fecha del cambio solicitado. - persona(s) que lo solicitan. - solicitud aprobada de cambios. - aprobación del cambio realizado - función de servicios de información. - aprobación del cambio realizado – usuarios. - fecha de actualización de documentación. - aprobación del cambio por parte de aseguramiento de la calidad. - aceptación por parte de operaciones.	1 HORA
- Revisión de la plataforma usada para el proceso de soporte y cambios. (5)	AI6	EJECUCION	Determinar si esta herramienta permite realizar un monitoreo y registro completo de los cambios.	1 Y ½ HORA

PRUEBA	PROCESO	TIPO	QUE SE VA HA COMPARAR	TIEMPO
- Análisis del Contrato y adquisición del Módulo de Historia Clínica electrónica.	DS2	ANALISIS	Se compara el contrato que hace referencia a Historia Clínica con las normas de contratos informáticos, y se revisan las políticas para la escogencia del proveedor.	2 HORAS
- Análisis del Modelo y Diccionario de Datos del Módulo de Historia Clínica Electrónica.	DS3	EJECUCION	Se analizara el diccionario de datos y se revisara que cuente con la información necesaria descrita en este tipo de manual, tomando como criterio el planteamiento del COBIT, igualmente se compara la correspondencia del diccionario de datos y la base de datos en producción.	4 HORAS
- Revisión de la base de datos, para verificar si los datos están clasificados según algún tipo de criterio.	DS5	EJECUCION	Se revisara en la base de datos, como se encuentran definidos los datos, se revisara los niveles de acceso, si existe algún tipo de protección, se verificara si hay inconsistencias en los datos y si existen datos obsoletos.	3 HORAS
- Revisión de los tipos de usuarios que pueden ingresar al sistema, verificando los recursos del módulo a los que tienen acceso.	DS7	EJECUCION	Se ingresará con los password creados para las pruebas y capacitaciones, a las diferentes áreas: como triage, urgencias, hospitalización y enfermería, para verificar que los recursos a los que tienen acceso correspondan a su usuario.	2 HORAS
-Se revisará el proceso de capacitación a usuarios finales (personal asistencial) dentro del Módulo de Historia Clinica.net, y el manual de capacitación que se entrega a los usuarios, así como el cronograma dispuesto para los entrenamientos.	DS7	EJECUCION Y ANALISIS	Se compara el proceso de capacitación y entrenamiento de usuarios tanto personal asistencial como ingenieros de soporte del Hospital Universitario Departamental por parte de la compañía proveedora del software.	2 HORAS

PRUEBA	PROCESO	TIPO	QUE SE VA HA COMPARAR	TIEMPO
- Se realizará un rastreo de la red, mapeo de puertos, pruebas al servidor de aplicación con el fin de verificar el número y el total de puertos abiertos, así como el acceso y seguridad de los sistemas al interior del Hospital Universitario Departamental de Nariño.	DS9	EJECUCION	Se compara la seguridad lógica de la organización con los estándares que existen actualmente para la protección, para ello se utilizan las herramientas de software y los sniffers correspondientes.	8 HORAS
- Se revisará el Inventario de hardware y adquisición de equipos para la implementación del Módulo de Historia Clínica dentro de la institución.	DS9	EJECUCION Y ANALISIS	Se compara si se encuentra al interior de la organización la actualización de Hardware y si es correspondiente con los requisitos para implementar Historia Clínica .net.	3 HORAS
- Comparar la clasificación de los datos con otro modelo de datos.	M2	EJECUCION	Se compara la clasificación de los datos del módulo de historia clínica, con el de otra institución de salud como por ejemplo salud coop.	4 HORAS
- Se revisarán las políticas al interior de la organización referente a los tipos de controles para las tecnologías de información y referente al módulo de historia clínica.net	M2	ANALISIS	Se compara las políticas del Hospital Universitario Departamental de Nariño referente a los tipos de control con las normas generales y existentes que se deben aplicar a los sistemas de información para Colombia y especialmente para las entidades de salud del Estado.	4 HORAS

4.2.5. Hallazgos y Recomendaciones de la Auditoría

Planeacion y Organización (PO)

PO2 - Definición de la Arquitectura de Información:

En este proceso se verificará si se están cumpliendo los requerimientos del hospital y si el modelo de información define los sistemas apropiados, para optimizar la utilización de los datos, en su análisis se encontraron los siguientes hallazgos:

No Preg.	DETALLE	QUE OCASIONA IMPACTO EN HC	NIVEL DE RIESGO	QUIENES INTERVIENEN	RECOMENDACIÓN
1	**Hallazgo:** No existe un Manual de Sistema (Técnico), solo se cuenta con documentación o manuales muy básicos relacionados con: Instalación y configuración de Dinámica gerencial, manuales sobre la gestión del Módulo de Historia Clínica donde se especifica como diseñar los modelos de historia clínica, como almacenar información de manera eficaz y oportuna entre otros. **Criterio:** De acuerdo al enfoque del COBIT, dentro de la definición de arquitectura de información se hace necesario, que se cuente con la información del manual de sistemas, para el buen desempeño del recurso humano, frente al proceso de implantación del módulo de historia clínica. **Causa:** Dentro de las políticas de la empresa SYAC, se establece que la información relacionada con el soporte del sistema Dinámica Gerencial, debe ser muy restringida, esto con el fin de que el Hospital este obligado a solicitar el soporte del mismo, por lo tanto se entrega poca documentación acerca del sistema Dinámica gerencial.	Al no existir un manual de sistema de Dinámica gerencial y en especial del módulo de Historia clínica, se genera que el recurso humano del área de sistemas, no cuenten con toda la información necesaria para poder prestar el soporte requerido en un determinado momento, lo cual disminuye la eficacia e integridad del módulo.		**Responsables:** Empresa Syac. **Afectados:** Personal de área de sistemas del HUDN.	Se recomienda que la empresa SYAC, desarrolle y documente el Manual de Sistema de Dinámica gerencial, donde se haga una descripción muy detalla de las características física y técnicas de cada elemento del módulo de historia clínica. Finalmente se recomienda que el Manual de Sistemas se entregue al personal del área de sistemas involucrado con el soporte de este módulo.

No Preg.	DETALLE	QUE OCASIONA IMPACTO EN HC	NIVEL DE RIESGO	QUIENES INTERVIENEN	RECOMENDACIÓN
2	**Hallazgo:** La documentación que contiene la información relacionada con el manual de sistemas, trata temas como gestión y configuración del módulo de historia clínica y le hace falta varios aspectos importantes que deben ir referenciados en este tipo de manual. **Criterio:** Partiendo de nuestro conocimiento, planteamos unos lineamientos que se deben tener en cuenta dentro del manual de sistemas, para que este sea integral y represente toda la arquitectura del módulo. En vista de que no se cuenta con un manual técnico se hace las anotaciones correspondientes. **Causa:** La no existencia de este manual de sistemas y la poca documentación en relación con el mismo, reflejan que existe una inconsistencia grande en la parte de documentación para el personal de sistemas del HUDN.	Carencia de información acerca del módulo de historia clínica, esto afectara en el momento en que el personal del área de sistemas necesite realizar soporte al módulo de historia clínica.		**Responsables:** Empresa Syac. **Afectados:** Personal de área de sistemas del HUDN	El manual de sistema del Dinamia gerencial deberá contener: 1. Índice Relación de los capítulos y páginas correspondientes que forman parte del documento 2. Introducción: Se debe presentar una breve descripción del sistema desarrollado, que contemple el ámbito abarcado, cual es su función principal y un detalle de las funciones macros o partes que lo componen. 2.1. Objetivo general del sistema. 2.2. Objetivos específicos. 3. Contenido técnico 3.1. Definición de reglas del negocio implementadas en el sistema desarrollado. 3.2. Instalación y configuración del módulo (Parámetros y requerimientos). 3.3. Diagramas de flujo de datos, junto con su respectivo diccionario de datos. 3.4. Controles de auditoría implementados en el sistema. 3.5. Descripción de campos requeridos por pantalla con presentación de pantallas. 3.6. Diagrama de navegación y configuración del sistema. 3.7. Requerimientos de interfase con otros sistemas. 3.8. Modelo lógico de datos, diagrama entidad-relación. 3.9. Modelo de datos físico. 3.10. Matriz de procesos de la Institución. 3.11. Matriz de programas versus entidades. 3.12. Plataforma de usuario: Indica los requerimientos mínimos de hardware y software para que el sistema se pueda instalar y ejecutar correctamente. 3.13. Áreas de aplicación y/o alcance de los procedimientos. Esfera de acción que cubren los procedimientos (Entradas procesos y salidas).

No Preg.	DETALLE	QUE OCASIONA IMPACTO EN HC	NIVEL DE RIESGO	QUIENES INTERVIENEN	RECOMENDACIÓN
2					4. Responsables. 4.1. Mapa de navegación: Muestra a través de diagramas de flujos, la interconexión entre cada una de las pantallas del sistema, lo que serviría para saber como llegar a determinada parte de la aplicación, detallando los menús, submenús y donde nos lleva cada uno. 4.2. Descripción gráfica del mapa de navegación: muestra el mapa de navegación representado con las pantallas del módulo de historia clínica. 4.3. Descripción paso a paso de los procesos, así como pantallas, botones, cuadros de texto, etc, igualmente indicar el código base de cada rutina, pantalla, botón, etc.
3	**Hallazgo:** Al no existir un manual de sistemas, también se evidencia que no existe una información actualizada en relación a los lineamientos que expone este manual. **Criterio:** De acuerdo a los lineamientos del COBIT, se hace necesario mantener una información técnica del módulo actualizada. **Causa:** Que la empresa SYAC, no haya elaborado formal e integralmente un manual se sistemas y únicamente se realicen capacitaciones personales a sus usuarios las cuales están poco documentadas.	Inexistencia de información actualizada para el personal del área de sistemas, en el momento que se requiera afrontar rápida y eficazmente, los cambios realizados en el módulo de historia clínica.	MEDIO	**Responsables:** Empresa Syac. **Afectados:** Personal de área de sistemas del HUDN	Se recomienda que cada vez que se realiza un cambio en el módulo de historia clínica, se actualice el manual de sistemas.
4	**Hallazgo:** Al no existir un manual de sistemas, también se evidencia que no existe un procedimiento establecido para mantener actualizado este tipo de manual. **Criterio:** De acuerdo al enfoque del COBIT, se hace necesario establecer procedimientos que permitan mantener actualizado el manual del sistema. **Causa:** Al no existir una manual de sistemas, se concluye que no existen políticas o procedimientos en relación a la gestión del mismo.	Al no existir procedimientos relacionados con el manual de sistemas en la empresa SYAC, que es la responsable del módulo, se define la carencia de este tipo de información y la falta de elaboración de este manual.	MEDIO	**Responsables:** Empresa Syac. **Afectados:** Personal de área de sistemas del HUDN	Se recomienda que la empresa SYAC Establesca políticas y procedimientos relacionados con la elaboración de este tipo de manual, que además garanticen una continua actualización, brindando información oportuna y verdadera.

No Preg.	DETALLE	QUE OCASIONA IMPACTO EN HC	NIVEL DE RIESGO	QUIENES INTERVIENEN	RECOMENDACION
6	**Hallazgo:** - En el diccionario de datos no existe la descripción del personal encargado de hacer el mantenimiento del mismo. - El diccionario de datos no describe la clasificación de usuarios, niveles de acceso y restricciones. - En el diccionario de datos no se describe los roles y privilegios de los usuarios. **Criterio:** De acuerdo a nuestro conocimiento, al hacer la revisión del Diccionario de datos se evidencia la carencia de estos aspectos que son de vital importancia para la gestión y soporte del módulo. **Causa:** Para la elaboración del diccionario de datos, no se tuvo en cuenta aspectos muy importantes, como la descripción del personal de mantenimiento del diccionario de datos, usuarios privilegios y niveles de acceso.	Falta de información sobre los aspectos relacionados con la información, su estructura y su gestión, lo cual dificulta el correcto desempeño de los funcionarios del área de sistemas encargados del módulo de historia clínica.	MEDIO	**Responsables:** Empresa Syac. **Afectados:** Personal de área de sistemas del HUDN.	Se hace necesario, complementar el diccionario de : datos con la especificación de : - Descripción detallada del personal encargado de mantener actualizado el diccionario de datos. - Clasificación de los tipos de usuarios, cuales son los niveles de acceso y las restricciones para el ingreso de los mismos. - Descripción de los roles de los diferentes usuarios y los privilegios, en el módulo de Historia Clínica.
7	**Hallazgo:** No se ha dado ha conocer el Diccionario de Datos a algunos de los Ingenieros del área de sistemas, en especial al personal nuevo y el personal que no esta directamente relacionado con el soporte de Dinámica Gerencial. **Criterio:** Tomando como base el enfoque del COBIT, se hace necesario, que exista una buena comunicación entre el representante de SYAC y el personal del área de sistemas, para el buen desempeño de las funciones. **Causa:** Cuando se actualiza el sistema dinámica gerencial, se van incluyendo nuevas opciones y herramientas, las cuales no son comunicadas al personal de sistemas del HUDN, en este caso los ingenieros no saben que se cuenta en el módulo de historia clínica, con una opción para acceder al su diccionario de datos.		MEDIO	**Responsables:** Empresa Syac. **Afectados:** Personal de área de sistemas del HUDN.	Se recomienda que cada ves que se instalen nuevas actualizaciones, se informe al personal del área de sistemas, los cambios realizados de acuerdo a la versión anterior, para este caso en la ultima versión ya se cuenta con la opción de consultar e imprimir el diccionarios de datos, opción que no estaba incluida en las versiones anteriores. Este tema es de desconocimiento para el personal nuevo y el personal que tienen poco contacto con las labores de soporte del módulo.

No Preg.	DETALLE	QUE OCASIONA IMPACTO EN HC	NIVEL DE RIESGO	QUIENES INTERVIENEN	RECOMENDACION
12	**Hallazgo:** No se puede determinar si la Arquitectura de información del módulo cuenta con la información requerida para este tipo de modelo como: definición de entradas, procesos, salidas, elementos con los que interactúa entre otros. **Criterio:** De acuerdo al COBIT, se hace necesario la definición de la Arquitectura de Información, para establecer claramente los requerimientos de la Institución, los planes a corto y largo plazo, el modelo de datos corporativo, los sistemas de información asociados entre otros, que son de gran importancia para el buen desempeño del área de sistemas. **Causa:** No se cuenta con la información relacionada con el modelo de arquitectura de información por parte de la empresa SYAC.	Inconsistencias en el modelo de arquitectura de información, en el modelo de datos, en los sistemas asociados, también se genera elementos obsoletos en el diccionario de datos y en las reglas de sintaxis.	MEDIO	**Responsables:** Empresa Syac. **Afectados:** Personal de área de sistemas del HUDN.	Dar a conocer el modelo de arquitectura de información, el cual deberá contener los siguientes lineamientos: - Identificación de entradas. - Identificación de procesos. - Identificación de sitios de almacenamiento (base de datos). - Identificación de reportes. - Identificación de la interacción con otros sistemas. - Diseño de interacción de los elementos e identidades del módulo. - Definición de usuarios finales. - Requerimientos del Hospital. - Planes de la gerencia a corto y largo plazo. -Costos, riesgos y aprobaciones para hacer modificaciones al modelo. - Cambios realizados al módulo.
13	**Hallazgo:** No se ha dado ha conocer el modelo de arquitectura de información del módulo de historia clínica, al personal del área de sistemas del Hospital Universitario departamental de Nariño. **Criterio:** El modelo de la arquitectura de información toma como base los planes a corto y largo plazo, considera los costos y riesgos asociados y asegura que las aprobaciones formales de la Gerencia sean obtenidas antes de hacer modificaciones al modelo. **Causa:** Falta de información por parte de la empresa SYAC.	Desconocimiento por parte del personal de área de sistemas de los lineamientos básicos de la Arquitectura del módulo de Historia Clínica, lo cual afectara el desempeño de la misma.	MEDIO	**Responsables:** Empresa Syac. **Afectados:** Personal de área de sistemas del HUDN.	Se recomienda que la empresa SYAC, presente la documentación sobre el modelo de arquitectura de Información, la socialice con el personal de área de sistemas y especifique su enfoque.

No Preg.	DETALLE	QUE OCASIONA IMPACTO EN HC	NIVEL DE RIESGO	QUIENES INTERVIENEN	RECOMENDACION
17	**Hallazgo:** No existen políticas y procedimientos para la clasificación de los datos. **Criterio:** De acuerdo al planteamiento del COBIT, se hace necesario que existan la definición de políticas y procedimientos que brinden las pautas para realizar la clasificación de los datos. **Causa:** En el área de sistemas del HUDN, se han clasificado los datos, pero no se han establecido formalmente políticas y procedimientos para los mismos.	Desorganización de los datos, restándole rendimiento al funcionamiento del módulo y el desempeño de los funcionarios del área de sistemas.	**BAJO**	**Responsables:** Área de Sistemas del HUDN. **Afectados:** Área de Sistemas del HUDN y usuario del módulo.	Se deben establecer políticas y normas, que garanticen que se realizara un marco de referencia o procedimientos relacionados con la clasificación formal de los datos.
18	**Hallazgo:** Al no contar con políticas para la clasificación de los datos, se evidencia que no existe la definición de pautas para la clasificación de los datos de acuerdo a categorías, propiedad de los datos entre otros. **Criterio:** De acuerdo al COBIT, dentro de la clasificación de los datos es necesario tener en cuenta, la seguridad, la propiedad de los datos y estándares de clasificación para datos. **Causa:** Los datos se han clasificado de acuerdo a las necesidades de manera informal, sin la definición de políticas, procedimientos o marcos que garanticen una correcta clasificación.	Existencia de datos cuya propiedad no ha sido determinada, Clases de datos que hayan sido definidos de forma inapropiada. Niveles de seguridad de datos inconsistentes con la regla de "necesidad de conocer".	**BAJO**	**Responsables:** Área de Sistemas del HUDN. **Afectados:** Área de Sistemas del HUDN y usuario del módulo.	Deberá establecerse un marco de referencia, políticas o procedimientos para la clasificación general de los datos en clases de información, teniendo en cuenta los siguientes criterios: - Categorías de seguridad. - Propiedad de los datos. - Datos públicos. - Datos Privados. - Datos Secretos. - Estándares de clasificación “Default”, para los activos de datos que no contienen un identificador de clasificación.

No Preg.	DETALLE	QUE OCASIONA IMPACTO EN HC	NIVEL DE RIESGO	QUIENES INTERVIENEN	RECOMENDACION
20	**Hallazgo:** Dentro de las políticas y procedimientos de las funciones de los servicios informáticos, hace falta incluir: - Definición de políticas para los niveles de seguridad y clasificación de los datos. - Niveles de acceso a los datos. **Criterio:** De acuerdo al planteamiento del COBIT dentro de la definición de la función de servicios informáticos, se deben incluir políticas que indiquen cual es el manejo que deben dar los técnicos de sistemas, a la seguridad y clasificación de los datos. **Causa:** Falta de definición de políticas o funciones de la oficina de sistemas en relación al manejo de la seguridad y clasificación de los datos.	Desorganización en el manejo de los datos por parte de los técnicos del área de sistemas, lo que puede producir una mala manipulación de los mismos, colocándolos en riesgos puesto que pueden ser accedidos fácilmente por personal que no esta autorizado.	MEDIO	**Responsables:** Área de Sistemas del HUDN. **Afectados:** Área de Sistemas del HUDN y usuario del módulo	Se recomienda establecer funciones y políticas que garanticen: - Niveles de seguridad definidos para cada clasificación de datos. - Niveles de acceso definidos y apropiados para la clasificación de los datos.

PO8 - Asegurar el Cumplimiento de Los Requerimientos Externos

El objetivo principal con el análisis de este proceso es verificar que dentro de la implantación del módulo de historia clínica, se hayan tenido en cuenta el cumplimiento de las obligaciones legales, regulatorias y contractuales, identificando cuales son los requerimientos externos para el módulo y verificando su cumplimiento, en este análisis se encontraron los siguientes hallazgos:

No Preg.	DETALLE	QUE OCASIONA IMPACTO EN HC	NIVEL DE RIESGO	QUIENES INTERVIENEN	RECOMENDACION
5	**Hallazgo:** las normas ergonomía y seguridad incluyen: - Dar ha conocer al personal de sistemas y asistencial relacionado con el módulo, el programa de ergonomía y seguridad. - Explicar a los usuarios y recurso humano del área de sistemas, cuales son las situaciones correctas de ergonomía y seguridad. - Realizar periódicamente capacitaciones para la prevención de riesgos. Pero estas actividades van orientadas al personal de Nomina, no se incluye personal de cooperativas y personal nuevo. - La dotación de elementos de trabajos ergonómicos al personal del área de sistemas y asistencial es mínimo.	La inadecuada gestión de los procedimientos y programas de ergonomía y seguridad, pueden poner en riesgos la seguridad y salud del personal involucrado con el módulo de Historia Clínica: Médicos, enfermeras, e Ingenieros del área de sistemas.	MEDIO	**Responsable:** Coordinador de Salud Ocupacional **Afectados:** Personal de área de sistemas, Usuarios (Médicos y enfermeras)	Se recomienda involucrar el las actividades de capacitación de los temas de ergonomía y seguridad (programas, normas, causas, prevención entre otros), a todo el personal involucrado con el módulo de historia clínica, sin importar el tipo de contratación. Se recomienda utilizar mejores estrategias de comunicación de la realización de actividades, por ejemplo la entrega oportuna de oficios a todo el recurso humano involucrado, informando la realización de estas actividades estipulando fecha, hora, tema y responsable. Se recomienda exigir la asistencia del personal convocado a capacitaciones por parte de la Coordinación del área de Salud Ocupacional.

No Preg.	DETALLE	QUE OCASIONA IMPACTO EN HC	NIVEL DE RIESGO	QUIENES INTERVIENEN	RECOMENDACION
5	- No se ha capacitación al personal de sistemas, encargado de la instalación de equipos en los diferentes puestos de trabajo de los médicos y enfermeras, acerca de las condiciones correctas ergonómicas. **Criterio:** Tomando como base las obligaciones de las empresas para con el recurso humano, en relación a las normas de seguridad y ergonomía en aspectos como: prevención, evaluación de riesgos, medidas de protección, información y capacitación entre otros, que son necesarios para crear un ambiente idóneo para el buen funcionamiento de la institución. **Causa:** Las capacitaciones y actividades de salud ocupacional están dirigidas al personal de nomina y no se tiene en cuenta el personal de cooperativas, generalmente el personal nuevo desconoce estos temas. - No se usan buenas estrategias para informar que se van ha realizar actividades como charlas, capacitaciones, etc. - No se exige la presencia del personal en las actividades de salud ocupacional, lo que hace que el recurso humano del HUDN, no tome con seriedad estos temas.	Partiendo de que el personal encargado de la instalación y adecuación de los equipos de cómputo y red, no ha sido capacitado correctamente en los temas de ergonomía y seguridad, se puede producir una situación de riesgo para los usuarios finales.		**Responsable:** Coordinador de Salud Ocupacional **Afectados:** Personal de área de sistemas, Usuarios (Médicos y enfermeras)	Se recomienda que dentro del programa de ergonomía se incluyan aspectos relacionados con la capacitación de las personas encargadas de la instalación y adecuación de los equipos de cómputo y de red, para los usuarios del módulo de historia clínica como los médicos y enfermeras entre otros. Se recomienda mejorar y dotar elementos de trabajo que cumplan con los lineamientos de seguridad y ergonomía.
7	**Hallazgo:** Existe la definición de políticas que garantizan la seguridad de la información del Hospital, pero en ellas no se han tenido en cuenta aspectos relacionados con los usuarios, la gestión de la información, supervisión de usuarios, claves, políticas para garantizar la seguridad de la información, que indiquen cual es el correcto manejo de las tecnologías de información, por parte de los médicos y enfermeras.	Violación y pérdida de la información por parte de persona externas a la Institución, quebrantando las normas y generando errores que difícilmente podrán ser corregidos.		**Responsable:** Coordinación del área de sistemas. **Afectados:** Usuarios (Médicos y enfermeras), desempeño del Módulo de historia clínica.	Se recomienda que dentro de las políticas de seguridad en el Hospital se incluya la definición de: - Normas relacionadas con el flujo de datos entre las áreas que interactúan con el módulo. - Políticas relacionadas con la administración del sistema. - Clasificación de datos de acuerdo a niveles de Importancia y confidencialidad. - Administración de usuarios sobre los recursos como: correo electrónico, Chat, contraseñas, descarga de archivos, instalación de aplicaciones, instalación de otros dispositivos en el PC, uso de la Internet e intranet, cuentas de usuarios.

7	**Criterio:** De acuerdo a la norma ISO 27001, existen unos lineamientos básicos para la gestión de seguridad. **Causa:** Dentro de las políticas de seguridad de la información en el Hospital no se han tenido en cuentas aspecto como el correo electrónico, clasificación de los datos, flujo de los datos, capacitación en seguridad a los usuarios del módulo.				
10	**Hallazgo:** Existen contratos en relación al aseguramiento del software pero no se han definido políticas sobre su cobertura, y no existe claridad de los aspectos que incluye el seguro, por parte de Control Interno y la Coordinación de sistemas de información. **Criterio:** Es de vital importancia que las instituciones de salud cuenten con seguros, pues existen situaciones adversas que pueden poner en peligro los sistemas y la información como robos, incendios, atentados entre otros. **Causa:** Falta de definición de políticas y normas que garanticen que se cuenten con seguros que cubran todas las situaciones de riesgos.	Falta de prevención y protección de las tecnologías de información del Hospital, en relación a riesgos del entorno, de personas externas entre otros.	MEDIO	**Responsable:** Subgerencia administrativa. Coordinación del área de sistemas. **Afectados:** Todo el personal de la Institución.	Se recomienda establecer lineamientos y normas relacionados con el cubrimiento de las aseguradoras y verificar que se incluyan: - Riesgos ocasionados por incendio, terremotos, lluvias, terrorismo, entre otros desastres. - Robo, lucro cesante. - Deshonestidad, desaparición y destrucción. - Responsabilidad civil. - Transporte.
11	**Hallazgo**: No se han realizado auditorías al módulo. **Criterio:** Es de gran importancia para la gestión de riesgos y evaluación de funcionamiento del software que se realicen periódicamente auditorías, que permitan inventariar y determinar aquellas falencias, con el fin de brindar alternativas y medidas correctivas en los diferentes procesos y elementos relacionados con el desempeño del software. **Causa:** En vista de se esta implantando el módulo de Historia clínica, todavía no se han realizado Auditorías.	Falta de información acerca de la situación actual del módulo de Historia clínica, en su proceso de implantación.	**BAJO**	**Responsable:** Coordinación del área de sistemas. **Afectados:** Usuarios (Médicos y enfermeras), desempeño del Módulo de historia clínica.	Se recomienda realizar periódicamente (semestralmente), auditorías al módulo de historia clínica, para determinar los aspectos en los que se requiere realizar cambios y plantear medidas correctivas.

(PO9) - Evaluación de Riesgos

Mediante este análisis se busca evidenciar si se esta realizando una gestión de riesgos, que permitan responder en un momento determinado a las amenazas que se puedan originar, brindando medidas económicas para mitigar los riesgos, de esta forma se encontraron los siguientes hallazgos:

No Preg.	DETALLE	QUE OCASIONA IMPACTO EN HC	NIVEL DE RIESGO	QUIENES INTERVIENEN	RECOMENDACION
1	**Hallazgo:** No existen la definición de políticas y procedimientos en relación a la evaluación de riesgos en el módulo de historia clínica. **Criterio**: De acuerdo al planteamiento del COBIT y la norma ISO 27001. **Causa:** La coordinación del área de sistemas y control interno, no han establecido procedimientos relacionados a la gestión de riesgos.	Desorganización y ocurrencia de incidentes graves dentro de las tecnologías de información, acumulación de errores, sin un planteamiento de solución.	ALTO	**Responsables:** Coordinación del área de sistemas y control interno. **Afectados:** Usuarios Desempeño del módulo de historia clínica.	Se recomienda al área de control interno y junto a la ayuda y perspectivas que se maneje el coordinador de información y sistemas del Hospital, planteen las políticas que indique y garanticen como se manejara todo lo relacionado a la gestión de Riesgos, para las tecnologías de Información.
2	**Hallazgo:** Existe un marco de referencia usado por las áreas de control interno y calidad que es el "MECI" para la administración de riesgos, pero el enfoque no ha sido implementado en el área de información y sistemas, esto se evidencia al no encontrar ninguna información o procedimientos para la gestión de riesgos, igualmente el personal de esta área ha corroborado que no se lleva a cabo gestión de este dominio.	Desorganización, mala administración de riesgos en las tecnologías de información, falta de evaluación, interrupción de los planes a corto y	ALTO	**Responsables:** Coordinación del área de sistemas y control interno. **Afectados:** Usuarios Desempeño del módulo de historia clínica. y Gerencia.	Se recomienda que las oficinas de sistemas y de control interno, presenten un programa enfocado al área de información y sistemas, donde se sugiera la cobertura de las actividades relacionadas en el "MECI", de acuerdo a sus 3 Subsistemas que son: 1. Control Interno. 2. Control de Gestión. 3. Control de Evaluación.

No Preg.	DETALLE	QUE OCASIONA IMPACTO EN HC	NIVEL DE RIESGO	QUIENES INTERVIENEN	RECOMENDACION
2	**Criterio:** De acuerdo al modelo de control estándar "MECI" y a las normas ISO 27001 usada como estándar de comparación en esta auditoría, se deben dar tratamiento a los riesgos, para lograr una organización, prevención, gestión de calidad, identificación, análisis, valoración y administración de riesgos **Causa:** Falta de organización, falta de planteamiento de procesos y actividades, por parte de control interno y del área de sistemas sobre los procesos a seguir, definiendo el personal involucrado con el soporte del módulo y el direccionamiento de estas áreas.	Y largo plazo, e impacto en el presupuesto de los mismos.	ALTO		Y se incluyan los siguientes aspectos: - Mantenimiento de hardware y de red. - Manejo del usuario de sus recursos de software y hardware. -Cambios en los requerimientos de usuarios. - Cambios de requerimientos externos. - Medidas de seguridad para usuarios. - Seguimiento a incidentes ocurridos anteriormente. - Gestión de riesgos. Esto con el fin de que el área de sistemas, este enterada de los lineamiento a seguir y cuales serian sus funciones para la administración de riesgos, como encargados del soporte del módulo de Historia clínica y el sistema en general.
4	**Hallazgo:** No se realiza periódicamente una evaluación de riesgos sobre las tecnologías de información. **Criterio**: De acuerdo a la ISO 27001, se hace necesario una evaluación de riesgos, donde se haga el estudio sistemático de activos, amenazas, vulnerabilidades e impactos a fin de evaluar la probabilidad y las consecuencias de los riesgos. **Causa:** Falta de evaluación periódica de riesgos que se pueden presentar en las tecnologías de información.	Acumulación de errores, mal funcionamiento del módulo de historia clínica, inestabilidad de la aplicación, perjuicio económico, alta probabilidad de que el riesgo ocurra.	ALTO	**Responsables:** Coordinación del área de sistemas y control interno. **Afectados:** Usuarios del módulo, Desempeño del módulo de historia clínica.	Realizar continuamente la evaluación de riesgos, una vez identificados, realizar un seguimiento que permita determinar las medidas correctivas o controles, para que estos no vuelvan a suceder y de forma contraria indique la manera de convivir con ellos, ejerciendo controles que los mantengan como "Aceptables".
5	**Hallazgo:** No se lleva un reporte o documentación relacionada con el seguimiento a la identificación de riesgos. **Criterio:** Según el enfoque del COBIT, se hace necesario documentar la gestión de riesgos, esto con el fin de ser comunicados a la gerencia de tal forma que apoye la toma de decisiones y de igual manera se informe al personal involucrado con las tecnologías de	Que no se lleve un proceso de control y prevención, de los riesgos que pueden surgir en las tecnologías de información, su entorno y su recurso humano.	ALTO	**Responsables:** Coordinación del área de sistemas y control interno. **Afectados:** Usuarios Desempeño del módulo de historia clínica.	Llevar un registro sobre la gestión o administración de riesgos estipulando: - Fecha de revisión. - Responsable. - Módulo analizado. - Proceso afectado. - Riesgo identificado.

No Preg.	DETALLE	QUE OCASIONA IMPACTO EN HC	NIVEL DE RIESGO	QUIENES INTERVIENEN	RECOMENDACIÓN
5	Información para la aplicación de los controles respectivos. **Causa:** Que no se lleve un registro sobre la gestión de riesgos y que estos sean dados ha conocer a la gerencia y el personal involucrado.	Igualmente esto hace inestable la aplicación.	ALTO		- Controles aplicables y correctivos sugeridos. - Veces que se ha presentado el riesgo. - Nivel de riesgo. Comunicar este documento a la gerencia para que se tomen los correctivos sugeridos.
7	**Hallazgo:** No existe un enfoque cuantitativo y/o cualitativo (o combinado) formal, para la identificación y medición de riesgos, amenazas y exposiciones. **Criterio:** De acuerdo a la norma ISO 27001, el análisis de riesgos es un ejercicio subjetivo en cualquier entorno donde se obtenga rentabilidad al asumir los riesgos y sea preferible estar "aproximadamente en lo correcto que exactamente errado". **Causa:** No se ha establecido un enfoque para la medición de riesgos.	Carencia de un método efectivo o herramientas que permitan hacer seguimiento de los riesgos.	MEDIO	**Responsables:** Coordinación del área de sistemas y control interno. **Afectados:** Usuarios Desempeño del módulo de historia clínica.	Se recomienda que control interno o el área de información y sistemas, establezca el análisis cualitativo de riesgos, de tal forma que se permitan hacer mediciones, que determinen la importancia de implementar controles a los riesgos en un determinado periodo de tiempo.
8	**Hallazgo:** No existe categorización de los riesgos del módulo de acuerdo a su nivel de importancia e impacto **Criterio**: De acuerdo a la ISO 27001, es importante analizar el impacto de los riesgos en concordancia a su representación económica. **Causa:** Que los riesgos no hayan sido clasificado de acuerdo a su nivel de importancia e impacto.	Que no exista una clasificación de riesgos, que permitan a la gerencia determinar las soluciones a los que tienen prioridad.	ALTO	**Responsables:** Coordinación del área de sistemas y control interno. **Afectados:** Usuarios, Desempeño del módulo de historia clínica.	Se recomienda que en base al análisis cualitativo, se clasifiquen los riesgos de acuerdo a nivel de importancia en impacto en el Sistema de información, analizando su equivalencia con el factor económico representativo para el Hospital y teniendo en cuenta los planes a corto y largo plazo del mismo.

No Preg.	DETALLE	QUE OCASIONA IMPACTO EN HC	NIVEL DE RIESGO	QUIENES INTERVIENEN	RECOMENDACION
9	**Hallazgo:** No existe un plan de acción contra riesgos. **Criterio:** En base a la ISO 27001, se hace necesarios el establecimiento de un plan de acción contra riesgos o el establecimiento de controles, para que los errores no sucedan varias veces y para determinar si los controles han sido los adecuados. **Causa:** Falta de definición de controles o de un plan de acción contra riesgos.	Que no existan controles y medidas de prevención contra los riesgos identificados, lo cual puede ser contraproducente con el sistema y la infraestructura física.	MEDIO	**Responsables:** Coordinación del área de sistemas y control interno. **Afectados:** Usuarios, Desempeño del módulo de historia clínica.	Se recomienda que se establezcan controles a nivel de: - Procesamiento. - Tecnología. - Actividad Humana - De acuerdo a la ISO 27001 A.10.4 se exige la implementación de controles de Software malicioso. - De acuerdo a la ISO 27001 A.10.8.4 se exige que la información "que hace parte de mensajes electrónicos debe tener la protección apropiada", es decir halla un control sobre los usuarios y la información que manipulan.
11	**Hallazgo:** No se ha realizado un proceso informativo y de toma de conciencia de la evaluación de riesgos, al personal del área de sistemas, sobre el desempeño y funcionamiento de las tecnologías de información. **Criterio:** De acuerdo con el enfoque del COBIT, se hace necesarios que exista buena comunicación entre todo el personal involucrado con la administración de riesgos. **Causa:** Falta dar a conocer y difundir los programas y actividades planeadas en relación a la administración de riesgos por parte de las áreas de control interno y el área de información y sistemas.	Desconocimiento del recurso humano sobre sus funciones y su papel dentro de la administración de riesgos.	ALTO	**Responsables:** Coordinación del área de sistemas y control interno. **Afectados:** Usuarios Desempeño del módulo de historia clínica.	Se recomienda a los responsables de la gestión de riesgos realizar: actividades, reuniones y planes junto al recurso humano involucrado, con el fin de asignar responsabilidades, y comunicar cual es el programa para la identificación, evaluación, seguimiento y establecimiento de controles contra los riesgos relacionados con las tecnologías de información.

No Preg.	DETALLE	QUE OCASIONA IMPACTO EN HC	NIVEL DE RIESGO	QUIENES INTERVIENEN	RECOMENDACION
12	**Hallazgo:** No se envía periódicamente reportes sobre la evaluación de riesgos a la Gerencia del Hospital **Criterio:** Según el enfoque del COBIT, se hace necesario una gestión estratégica en relación a los riesgos, comunicando el resultado de su análisis a la gerencia de la empresa. **Causa :** Falta de comunicación de la evaluación de riesgos a la gerencia y administración del hospital	Desconocimiento por parte de la gerencia y el área administrativa acerca del los posibles riesgos y el impacto que esto pueden ocasiona en el Hospital.	ALTO	**Responsables:** Coordinación del área de sistemas y control interno. **Afectados:** Usuarios Desempeño del módulo de historia clínica.	Entregar oportunamente un informe relacionado con la evaluación de riesgos.
13 14	**Hallazgo:** Si existe un seguro contra riesgos pero este no incluye aspectos relacionados con amenazas como violación de la información. **Criterio:** De acuerdo al enfoque del COBIT, es necesario la definición de políticas sobre el cubrimiento que deben tener las aseguradoras en relación a las tecnologías de información, sobre todo en casos no frecuentes como: violación o pérdida de información. **Causa:** Que no se cuente con un cubrimiento total de parte de la aseguradora en relación a las tecnologías de información, contando con que día a día dentro de los requerimientos del Hospital esta la de la sistematización integral de todos los procesos, haciendo aun más necesario la contratación de un seguro que incluya el cubrimiento de riesgos que no han sido tenido en cuenta hasta la fecha.	Que el sistema y la información no solo del módulo de historia clínica si no también de todo Dynamica gerencial, se encuentre en riesgo si llegan a suceder una situación que no ha sido contemplada.	MEDIO	**Responsables:** Área de información y sistemas, gerencia de la Institución. **Afectados:** Usuarios, pacientes y personal involucrado con el módulo de historia clínica.	Establecer políticas en relación a los seguros contra riesgos en relación a las tecnologías de información, y contratación de un seguro integral que incluya: - Incendio, inundaciones, terremotos, tornados, terrorismo y otros desastres naturales no predecibles. - Violaciones a las responsabilidades fiduciarias del empleado. - Interrupción del negocio, pérdidas de ingresos, perdida de pacientes, etc. - Otros riesgos no cubiertos generalmente por la tecnología de información y planes de riesgo/continuidad del negocio.

(PO11) - Administración De Calidad

Con el estudio de este proceso se busca determinar si se cumplieron los requerimientos de los usuarios como: médicos, enfermeras y en general los requerimientos de la institución sobre la gestión de historia clínica y su relación con los demás módulos. De esta forma se encontraron los siguientes hallazgos:

No Preg.	DETALLE	QUE OCASIONA IMPACTO EN HC	NIVEL DE RIESGO	QUIENES INTERVIENEN	RECOMENDACIÓN
3	**Hallazgo:** Existe un plan de calida pero en relación a las tecnologías de información no se especifican aspectos como: la infraestructura de información o instalaciones requeridas para soportar los sistemas implementados, y el entrenamiento requerido para desarrollar y soportar el ambiente de las Tecnologías de Información. **Criterio**: Según el enfoque del COBIT, el plan de calidad, debe especificar características de las instalaciones para los sistemas implementados, asegurando que se haga monitoreo de la infraestructura tecnológica en relación a los cambios, de forma que estén correctamente planeados, monitoreados, probados, documentados e incluyan el entrenamiento y los recursos necesarios.	Inestabilidad en relación a los planes futuros, y a los cambios del entorno, puesto que el plan de calidad permite que exista una planificación adecuada, la definición correcta de procedimientos orientados a los sistemas implementados, los recursos tecnológicos		**Responsables** Coordinación del área de información y sistemas y Área administrativa. **Afectados:** Usuarios finales del módulo (médicos y enfermeras), Área de información y sistemas	Teniendo en cuenta que el enfoque del plan de calidad de la Institución esta dirigido a: - La Salud y prevención - La Excelencia clínica - La Equidad - Las Tecnologías de información - La Transparencia - El Recurso humano Se recomienda que dentro del plan de Calidad del área de Información y sistemas, se incluyan los aspectos relacionados con la infraestructura de información requerida para soportar los sistemas e interfases, el entrenamiento requerido para desarrollar y soportar el ambiente de TI escogido como objetivo, con el fin de determinar si los paquetes de software comercial adquiridos con la empresa SYAC, satisfacen las necesidades del Hospital en el proceso de acreditación.

No Preg.	DETALLE	QUE OCASIONA IMPACTO EN HC	NIVEL DE RIESGO	QUIENES INTERVIENEN	RECOMENDACIÓN
	Causa: Dentro del plan de calidad no se relaciona los requerimientos de la infraestructura de información y el entrenamiento requerido para desarrollar y soportar el ambiente de TI escogido como objetivo.	y el papel que debe cumplir el recurso humano en estos aspectos, orientado a la visión de la institución a corto y largo plazo			También se debe tener en cuenta que el plan de calidad debe permitir a la institución que: - Las políticas de calidad, los procedimientos y los requisitos de la organización, sean conocidas por todo el recurso humano de la misma. - Describir e implementar un sistema de la calidad eficaz. - Suministrar control adecuado de las prácticas y facilitar las actividades de aseguramiento. - Suministrar las bases documentales para las auditorías. - Adiestrar al personal en los requisitos del sistema de la calidad.
6	**Hallazgo:** Existe el enfoque de aseguramiento de calidad que es el "Estándar de la Gerencia de la Información " el cual va dirigido a 8 grandes objetivos estratégicos, pero se deben incluir procesos en relación a los requerimientos externos, revisiones periódicas, y debe ser comunicado o formalizado ante el personal del área de información y sistemas. **Criterio:** Dentro el proceso de acreditación en el que se encuentra el Hospital, es de vital importancia que dentro del la definición de enfoque de calidad se incluyan los temas relacionados con revisiones de las implementaciones de sistemas, los cambios en requerimiento externos y revisión de las recomendaciones en procesos de auditorías. **Causa:** Que dentro del enfoque de calidad no se incluyan los aspectos mencionados anteriormente.	Falta de definición de elementos tecnológicos e infraestructura para los sistemas implementados, donde no existe seguimiento de revisiones a los mismos.		**Responsable:** Gerencia, Coordinación de información y sistemas. **Afectados:** Usuarios, desempeño del módulo de historia clínica.	Se recomienda que en el enfoque de aseguramiento de calidad se incluyan: - Especificaciones sobre las revisiones o auditorías. -Revisiones de post-implementación de las versiones del módulo, para verificar si va de acuerdo al ciclo de vida usado en versiones anteriores. - Revisión del cumplimiento de los requerimientos nuevos del hospital para historias clínicas. - Recomendaciones a las que se les hace seguimiento periódicamente y que son reportadas al personal administrativo encargado de la toma de decisiones del Hospital. Se recomienda que se tenga en cuenta los ítems de la ISO 27001 sobre: 4.3 documentación, 4.3.2. Control de documentos, 4.3.3 registros.

No Preg.	DETALLE	QUE OCASIONA IMPACTO EN HC	NIVEL DE RIESGO	QUIENES INTERVIENEN	RECOMENDACIÓN
9	**Hallazgo:** Dentro del ciclo de vida de desarrollo de sistemas definido para el HUDN, se encontró que: - Tiene poca documentación. - No cuenta con diagramas de flujo de la programación del módulo. - No ha sido comunicado formalmente al personal del área de información y sistemas. **Criterio:** Es importante que el área de información y sistemas, para su correcto desempeño ponga en claro lineamientos y funciones de su recurso humano, para que exista una buena organización no se presente discrepancias y sobrecarga de trabajo por la falta de estructuración. **Causa:** No se ha realizado una documentación completa y formal del ciclo de vida de desarrollo de sistemas, donde se especifique todos los aspectos relacionados a la gestión del desarrollo del software, para los procesos del Hospital.	Desorden en las actividades de soporte al módulo de Historia clínica, por parte de los ingenieros del área de información y sistemas.	MEDIO	**Responsable:** Coordinación del área de sistemas e Ingenieros de área. **Afectados:** Personal del área de sistemas.	Se recomienda que dentro de la documentación relacionada con el ciclo de vida de desarrollo de sistemas para la institución se incluya: - Especificación de los controles suficientes durante el proceso de desarrollo para sistemas y tecnologías nuevas. - Una comunicación con todos los empleados apropiados involucrados en el desarrollo y mantenimiento de sistemas. - Que se utilicen procedimientos para los cambios tecnológicos. - Que se utilicen procedimientos para asegurar la aceptación y aprobación de los usuarios. - Diagramas de flujos de la programación si es posible o de lo contrario del funcionamiento lógico de los diferentes módulos del sistema implementado en la institución.
10	**Hallazgo:** El módulo de historia clínica no se ha desarrollado de acuerdo al ciclo de vida de desarrollo de sistemas que usa el Hospital. **Criterio:** Según el planteamiento del COBIT, es de vital importancia que exista una correspondencia entre el ciclo de vida usado por el Hospital con el de terceras partes, puesto que esto puede afectar negativamente a la organización en el logro de su misión y metas. **Causa:** El módulo de Historia Clínica por ser desarrollado por una empresa externa, maneja sus propias políticas y normas, por tal razón manejan un ciclo de vida diferente al del hospital y del cual no se posee documentación, puesto que la empresa SYAC, no facilito la información relacionada a este punto, puesto que así lo contemplan sus políticas administrativas.	Dificultades para prestar un soporte adecuado por parte de los Técnicos del área de Información y sistemas.	MEDIO	**Responsable:** Coordinación del área de sistemas, empresa SYAC. **Afectados:** Usuarios, desempeño del módulo de historia clínica. Personal de área de sistemas	Se recomienda que el Hospital y Syac unifiquen el ciclo de vida de desarrollo de sistemas, teniendo en cuenta que SYAC es la empresa proveedora de Software la cual es dueña del programa y se encarga del desarrollo y cambio del mismo, se recomienda que el Hospital adopte el mismo ciclo de vida de desarrollo de la empresa SYAC, lo documente y lo formalice para que sea usado por el personal técnico, del área de información y sistemas, facilitando de esta forma las actividades de soporte y desarrollo para el sistema Dynamica Gerencial y en especial el módulo de Historia clínica.

Adquisición e Implementación (AI)

(AI2) - Adquisición y Mantenimiento De Software De Aplicación

En este proceso se estudiara si se cumplieron con los requerimientos funcionales y operacionales sobre la gestión de historias clínicas de pacientes, como también si se realizo una implementación estructurada, integral y clara para los usuarios finales, de esta forma se encontraron los siguientes hallazgos:

No Preg.	DETALLE	QUE OCASIONA IMPACTO EN HC	NIVEL DE RIESGO	QUIENES INTERVIENEN	RECOMENDACIÓN
7	**Hallazgo:** Dentro del módulo de Historia Clínica no se cuenta con la opción de ayuda en línea como tal, lo que se tiene dentro de la opción de ayuda del módulo, es un link que carga el manual de usuario, donde esta especificado el diligenciamiento general de opciones del módulo, ha este manual le hace falta la información sobre la gestión de las interfases de las historias clínicas de las áreas de urgencia y especialidades. **Criterio:** De acuerdo al enfoque de COBIT, y de acuerdo a nuestro criterio, en todo programa y aplicación es de vital importancia brindar herramientas de ayuda, que les permitan a los usuarios realizar una correcta gestión del aplicativo.	Falta de documentación para los usuarios, sobre el manejo del módulo de historia clínica y el diligenciamiento de los procesos e interfases.	ALTO	**Responsable:** Empresa SYAC, Área de información y sistemas. **Afectados:** Usuarios finales (médicos y enfermeras)	Se recomienda que la empresa SYAC, desarrolle una ayuda para el usuario, donde se brinde una información completa no solo de las opciones de: - Archivo - Procesos - Reportes - Utilidades Si no también se incluya el manejo de las interfases de las diferentes Historia clínicas de urgencias y especialidades, que fueron desarrolladas por parte de los técnicos del hospital. Alternativamente se recomienda elaborar una verdadera ayuda en línea para los usuarios, en donde se incluya un buscador ya sea por palabra, tema, sección o procedimiento, que indique el manejo de las interfases, los procesos, las herramientas y funciones que ofrece el módulo de Historia Clínica.

No Preg.	DETALLE	QUE OCASIONA IMPACTO EN HC	NIVEL DE RIESGO	QUIENES INTERVIENEN	RECOMENDACIÓN
7	**Causa:** Elaboración de una ayuda muy básica que no permite a los usuarios encontrar información de calidad sobre el manejo del módulo de historia clínica.				
8	**Hallazgo:** Dentro de la opción de parametrización del módulo de historia clínica, al realizar una determinada configuración, se ha encontrado que no se están cumpliendo las validaciones configuradas, en relación a la opción de diagnostico por edades. **Criterio:** De a cuerdo al enfoque del COBIT, y de acuerdo a nuestro criterio se hace necesario que el módulo este totalmente validado, esto con el fin de evitar que se almacene información incorrecta dentro de las base de dato de historia clínica, y de igual manera se garantice que las opciones de archivos, procesos, reportes y utilidades sean realizadas correctamente. **Causa:** Falta de revisión de la nuevas versiones del módulo de historia clínica, en relación al desarrollo de sus operaciones, herramientas y opciones.	Que la información de pacientes sea almacena de forma incorrecta, y que las operaciones de diagnostico no que realicen de forma adecuada.	ALTO	**Responsables:** Empresa SYAC. **Afectados:** Técnicos del área de información y sistemas, usuarios finales (medico y enfermeras), desempeño el módulo.	Se recomienda que el Hospital solicite a SYAC, la revisión y corrección de la parametrización del módulo en la parte de diagnostico por edades.
9	**Hallazgo:** Dentro de la documentación de la metodología del ciclo de vida no se habla sobre aspecto como: - Importancia de la comunicación entre los usuarios (médicos y enfermeras) y los diseñadores de las Historias Clínicas. - Mecanismos adecuados para la recopilación de requerimientos de control interno y seguridad.	Mal entendidos en los requerimientos de los usuarios finales del módulo, perdida de tiempo en desarrollo de los diseños de Historias clínicas, retraso en la implantación del módulo.	MEDIO	**Responsables:** Personal de área de sistemas. **Afectados:** Usuarios. Desempeño del módulo.	Se recomienda que se establezcan funciones, que se delimiten bien las fechas de entrega, las actividades y mecanismos a utilizar para el proceso de diseños de historias clínicas y la implantación del módulo en las diferentes áreas (triage, urgencia, hospitalización y consulta externa). Esto con el fin de exista una organización y armonía entre todo el personal involucrado en este proceso.

No Preg.	DETALLE	QUE OCASIONA IMPACTO EN HC	NIVEL DE RIESGO	QUIENES INTERVIENEN	RECOMENDACIÓN
9	**Criterio:** De acuerdo al enfoque del COBIT, dentro del ciclo de vida de desarrollo de sistemas se debe garantizar buenos mecanismos para asegurar una correcta apropiación de los requerimientos y necesidades del Hospital frente a las Historia Clínicas. **Causa:** Falta de la definición de procedimientos y actividades que garanticen no solo una buena comunicación entre los diseñadores de las historia clínicas y los usuarios, si no también entre los lideres en el proceso de implantación del módulo, y el equipo de sistemas del Hospital.				
14	**Hallazgo:** No existe el planteamiento de un plan de pruebas a realizarse en el proceso de implantación del módulo de historia clínica. **Criterio:** Según los enfoque de las ISO 27001 y el COBIT, para asegurar el correcto funcionamiento del módulo es necesario que en el proceso de implantación y posteriormente con los cambios de versiones de Dynamica gerencial, se establezca un plan de pruebas a realizarse al módulo, para garantizar su correcto funcionamiento antes de ser puesto en producción con los usuarios finales, disminuyendo la ocurrencia de fallos futuros. **Causa:** Falta de la definición formal de un plan de pruebas para realizar al módulo de historia clínica.	Que una vez puesto en marcha el módulo de historia clínica, surjan errores y fallos que pudieron ser detectados anteriormente, ocasionando el mal desempeño del módulo.	MEDIO	**Responsables:** Personal de área de sistemas. **Afectados:** Usuarios. Desempeño del módulo.	Se recomienda definir políticas que garanticen la correcta elaboración de un plan de pruebas aplicables, en los procesos de implantación del módulo de historia clínica de sistema Dynamica gerencial, como también en futuras actualizaciones.
15	**Hallazgo:** Al no existir la definición de un plan de pruebas, no se cuenta con la especificación de pautas y pruebas a aplicarse para probar el buen desempeño del módulo de historia clínica.		MEDIO	**Responsables:** Personal de área de sistemas.	Se recomienda elaborar un plan de pruebas para realizarse al módulo que contenga: 1. Objetivo del plan de pruebas. 2. Tipo de pruebas. 2.1. Tiempo de duración de la Prueba.

No Preg.	DETALLE	QUE OCASIONA IMPACTO EN HC	NIVEL DE RIESGO	QUIENES INTERVIENEN	RECOMENDACIÓN
15	**Criterio:** De acuerdo al COBIT y la norma ISO 27001, antes de poner producción el sistema, es necesario que pase un plan de pruebas que garantizarán su correcto funcionamiento o permita establecer los correctivos que son necesarios para el módulo. **Causa:** Antes de la implantación del módulo se realizan pruebas empíricas básicas y no tiene un modelo ha seguir de las pruebas necesarias para realizarse, como las pruebas prototipo, paralelo, revisión de procesos, entrada y salida de datos en base al criterio de los usuarios.	Presentación de fallos cuando el módulo ya se encuentre en total funcionamiento, los cuales pudieron haber sido corregidos anteriormente.		**Afectados:** Usuarios. Desempeño del módulo	2.2. Pruebas Unitarias: Estas pruebas servirán para probar que cada componente realiza adecuadamente el propósito para el que fue concebido. 2.3. Pruebas Integrales: Estas pruebas servirán para probar que cada componente se interconecta adecuadamente con los componentes que interactúa. 2.4. Pruebas de Sistema: Estas pruebas servirán para probar que cada Caso de Uso se integra apropiadamente en cadenas de ejecución de procesos del negocio. 2.5. Pruebas de Aceptación: Estas pruebas servirán para demostrar al Cliente que el producto satisface los requerimientos para los Casos de Prueba seleccionados. 2.6. Pruebas para validación de campos y opciones. 2.7. Pruebas prototipo y paralelo.

(AI5) - Instalación y Acreditación De Sistemas

En este proceso se trata de evidenciar si se realizo una correcta implantación del módulo de historia clínica en relación a la aceptación de usuario final, capacitaciones y pruebas finales, en este análisis se encontraron los siguientes hallazgos:

No Preg.	DETALLE	QUE OCASIONA IMPACTO EN HC	NIVEL DE RIESGO	QUIENES INTERVIENEN	RECOMENDACIÓN
3	**Hallazgo:** La metodología formal del ciclo de vida de desarrollo no incluye pruebas de acreditación, de seguridad y capacitación del recurso humano, seguimiento de operaciones de implementación. **Criterio:** Basados en el COBIT, se hace necesario que dentro del ciclo de vida se garanticen el cumplimiento de las actividades de seguimiento, pruebas y capacitación, que permitan la correcta implantación del módulo, ayudando en el proceso de acreditación del Hospital.	Falta de definición de elementos relacionados con los procesos de desarrollo de sistemas e implantación del módulo de historia clínica.		**Responsable:** Personal del área de Información y sistemas **Afectados:** Personal del área de sistemas, Usuarios del módulo.	Se recomienda que dentro de la metodología del ciclo de vida de desarrollo de sistemas se incluya: - Entrenamiento a ingenieros a cargo del módulo de historia clínica. - Pruebas del módulo. - Pruebas prototipo y paralelo y post-implementación. - Pruebas de acreditación seguridad. - Controles de cambio.

No Preg.	DETALLE	QUE OCASIONA IMPACTO EN HC	NIVEL DE RIESGO	QUIENES INTERVIENEN	RECOMENDACIÓN
3	**Causa:** Que se haya definido de forma global una metodología relacionada con el ciclo de vida de desarrollo de sistemas, pero esta no haya sido detalla, que no se haya definido sus características, elementos, cobertura y no se encuentre documentada completamente, para ser dada a conocer formalmente a todo el personal involucrado con las tecnologías de información y su proceso de acreditación.				
5	**Hallazgo:** Se realizan capacitaciones para el personal de área de sistemas, pero no se cuenta con un programa de entrenamiento formal, que permita determinar si estas son lo suficientemente estructuradas. En el análisis sobre las capacitaciones realizadas se evidencia que no han tratado los temas de: - Diferencias del módulo de historia clínica, con otros módulos del sistema Dinámica gerencial. - Errores y corrección de errores. **Criterio:** De acuerdo a la perspectiva del COBIT, dentro del ciclo de vida de desarrollo de sistemas es de gran importancia la definición de estos aspectos, puesto que de ellos dependen la correcta implantación del módulo y su soporte. **Causa:** Que no se haya realizado una descripción y definición integral de la metodología del ciclo de vida de desarrollo de sistemas para el hospital, donde se especifique y se delimiten bien las funciones y procesos en relación al desarrollo de software, el soporte de los módulo ya existentes, y la implantación de módulos nuevos como lo es el caso de Historia Clínica	Falta de la definición de lineamientos y funciones en relación al proceso de instalación y acreditación del módulo de historia clínica, produciendo retrasos en el desarrollo de las actividades, dificultad en momento de realizar las operaciones, surgimiento de fallas en el desempeño del módulo.	MEDIO	**Responsable:** Empresa SYAC **Afectados:** Personal del área de sistemas, Usuarios del módulo.	Teniendo en cuenta que dentro del proceso de instalación y acreditación de sistemas, se hace necesario que los técnicos tengan un completo manejo y conocimiento del módulo de historia clínica, se requiere que se diseñe un programa formal de entrenamiento para el personal del área de sistemas, que sea socializado y que incluya: - Capacitación en relación a las diferencias del módulo de historia clínica, con otros módulos del sistema Dinámica gerencial. - Gestión de errores, en relación a los posibles errores y las estrategias o metodologías para la corrección de estos errores. Puesto que los demás aspectos requeridos para las capacitaciones si han sido abordados correctamente.

No Preg.	DETALLE	QUE OCASIONA IMPACTO EN HC	NIVEL DE RIESGO	QUIENES INTERVIENEN	RECOMENDACIÓN
6	**Hallazgo:** No existe un plan de Pruebas para el proceso de implantación del módulo por parte del área de sistemas del Hospital, que es de vital importancia dentro de este proceso. **Criterio:** En base el enfoque del COBIT, es necesario que el área de información y sistemas, plantee un plan de pruebas independiente de la empresa SYAC, para verificar el correcto funcionamiento del módulo antes de ser puesto en producción. **Causa:** Falta de definición de un plan de pruebas por parte del área de información y sistemas del hospital e igualmente por parte de SYAC.	Dificultades en el proceso de instalación del módulo de historia clínica.	MEDIO	**Responsable:** Coordinación el área de sistemas. Empresa SYAC **Afectados:** Usuarios del módulo. Desempeño del módulo de Historia Clínica.	Se recomienda que se elabore un plan de pruebas con las características descritas en el proceso AI2 Adquisición y mantenimiento de software de aplicación.
7	**Hallazgo:** Como se menciona anteriormente en el proceso AI2 no existe la definición de un plan de pruebas por parte del Hospital ni tampoco por parte de la empresa SYAC, de esta forma se evidencia no se han incluido ningún tipo de pruebas relacionadas con la infraestructura física, el concepto de los usuarios y las instalaciones y en general el entorno del módulo. **Criterio:** De acuerdo al enfoque del COBIT es de gran importancia que además de las pruebas del software como tal, es fundamental realizar pruebas al entorno, como las instalaciones, la red los equipos de cómputo y el papel de los usuarios. **Causa:** Que no exista la definición formal de un plan de pruebas de parte del área de información y sistemas ni tampoco por parte de la empresa SYAC.	Dificultades en el proceso de instalación del módulo de historia clínica, y de los equipos de cómputo e infraestructura física.	MEDIO	**Responsable:** Coordinación el área de sistemas. Empresa SYAC **Afectados:** Usuarios del módulo. Técnicos de área de información y sistemas Desempeño del módulo de Historia Clínica.	Se recomienda que junto a las características del plan de pruebas descritas en el proceso AI2, se tenga en cuenta que el plan de pruebas tenga una cobertura a: Software de aplicación, Instalaciones, Tecnologías y usuarios.

(AI6) - Administración De Cambios

En este proceso se tratan de evidenciar todos los procedimientos que se deben llevar a cabo en el Hospital, relacionados con el seguimiento a cambios, con el fin de minimizar las alteraciones, interrupciones y errores en relación al desempeño del módulo de historia clínica, garantizando que los cambios que se propongan se evalúen cuidadosamente, que las personas indicadas tomen decisiones sobre esos cambios, que se comuniquen oportunamente a todos los afectados, y que los cambios se incorporen de una forma disciplinada; en el estudio de este proceso se encontraron los siguientes hallazgos:

No Preg.	DETALLE	QUE OCASIONA IMPACTO EN HC	NIVEL DE RIESGO	QUIENES INTERVIENEN	RECOMENDACION
1	**Hallazgo:** Dentro del estándar Gerencia de la Información, hace falta incluir un lineamiento relacionado con el seguimiento y control de cambios en los sistemas de información implantados, de esta forma se evidencia que no se han implementados ni procedimientos ni funciones para hacer seguimiento, identificación y establecer controles sobre los cambios. **Criterio:** De acuerdo al enfoque del COBIT, es necesario establecer procedimientos y funciones al personal de área de sistemas, que le permitan llevar un registro de los cambios que se van efectuando en el sistema de información, no solo a nivel interno si no también los cambios externos o del entorno. **Causa**: Falta de definición de lineamientos en el estándar gerencia de la información, sobre la implementación de procedimientos y funciones para el recurso humano involucrado sobre la correcta gestión de cambios en el sistema de información.	Al no existir una política o lineamiento en relación a la gestión de cambios, se evidencia que no se han definidos procedimientos sobre la administración de los mismos, esto ocasiona desorganización, falta de información para hacer el soporte, problemas de calidad, desempeño y efectividad del módulo.		**Responsable:** Coordinación del área de sistemas **Afectado:** Personal del área de sistemas, Usuarios del módulo.	Se recomienda que dentro del estándar Gerencia de la Información, se incluya un lineamiento que garantice el establecimiento de procesos y funciones para el personal del área de sistemas, en relación a la administración de los cambios en el sistema, es importante resaltar que Dynamica Gerencial es un sistema Integral, donde se esta migrado toda su funcionalidad al lenguaje .NET, y por tal razón se están realizando constantes actualizaciones que implican cambios no solo en el módulo de Historia clínica si no también en los demás módulos, por tal razón y en vista de las constantes actualizaciones se determina que es de gran importancia llevar un control sobre los cambios realizados a cada versión.

No Preg.	DETALLE	QUE OCASIONA IMPACTO EN HC	NIVEL DE RIESGO	QUIENES INTERVIENEN	RECOMENDACIÓN
2	**Hallazgo:** A pesar de que existe una plataforma por parte de la empresa SYAC, para llevar un registro de los cambios solicitados por el hospital a esta empresa, es necesario que como proceso independiente el área de información y sistemas establezca una guía formal donde se especifique como hacer el seguimiento a los cambios, no solo de los que son solicitados a SYAC, si no también de los cambios observados en cada actualización de Dynamica Gerencial. **Criterio:** En base en la perspectiva del COBIT, es necesario llevar un registro de los cambios, donde se evidencie un seguimiento cronológico, se clasifiquen de acuerdo a su nivel de importancia e impacto, se determine si se hizo solicitud y autorización del cambio, entre otros, con el fin de minimizar los errores e interrupciones del funcionamiento del aplicativo. **Causa:** Que dentro del área de información y sistemas del hospital, no exista la definición de un procedimiento que permita llevar un registro de la gestión de los cambios relacionados con el módulo de historia clínica.	Que no exista documentación ni control sobre los cambios que van sufriendo las diferentes versiones del sistema, sin poder determinar si los cambios realizados realmente fueron necesarios y han sido para el beneficio de desempeño del módulo de historia clínica.		**Responsable:** Coordinación del área de sistemas **Afectado:** Personal e área de sistemas, Usuarios del módulo	Se recomienda establecer un procedimiento o guía a seguir para llevar continuamente el registro de los cambios realizados en el módulo de historia clínica, ya sea por solicitud por parte del Hospital a Syac, como también para registrar los cambios que se observan cuando se realiza una actualización del sistema Dynamica Gerencial, esto con el fin principal de conocer con profundidad el módulo, verificar si los cambios son necesarios y si realmente son un beneficio para el módulo o por el contrario a desmejorado su rendimiento. Este registro debe contener: - Fecha de observación del cambio, día de actualización. - Numero de cambio. - Numero de actualización, (No versión). - Detalle de Cambio: se especifica el cambio observado en comparación con el estado anterior. - Sección o interfaz: se discrimina la interfaz en la que ha realizado el cambio, si es un proceso se especifica su ubicación grafica, en el módulo. - Estado: se refiere a si se encuentra en funcionamiento optimo, medio o bajo. - Observaciones: En caso de que exista alguna implicación con el cambio realizado. Para la solicitud de cambios se debe llevar adicionalmente los siguientes registros: • Fecha del cambio solicitado. • Persona(s) que lo solicitan. • Solicitud aprobada de cambios. • Aprobación del cambio realizado - función de servicios de información. • Aprobación del cambio realizado – usuarios. • Fecha de actualización de documentación. • Fecha de paso a producción. • Aprobación del cambio por parte de aseguramiento de la calidad. • Aceptación por parte de operaciones.

Entrega de Servicios y Soporte (DS)

(DS2) - Administración de Servicios Prestados por Terceros

Median el estudio de este proceso se busca verificar que las tareas y responsabilidades de las terceras partes estén claramente definidas, que cumplan y continúen satisfaciendo las necesidades de la Institución, mediante su estudio se encontraron los siguientes hallazgos:

No Preg	DETALLE	QUE OCASIONA IMPACTO EN HC	NIVEL DE RIESGO	QUIENES INTERVIENEN	RECOMENDACIÓN
	Hallazgo: Dentro del contrato OJ006-2008 no se incluye el plan de contingencia para garantizar la continuidad del proyecto, no se especifica los programas a desarrollar por parte de SYAC y no hace referencia a las pruebas de aceptación al módulo de Historias Clinicas.Net. **Criterio:** Se compara el contrato OJ006-2008 con el estándar del CECUA que hace relación a los tipos de contratos informáticos. **Causa:** No poseer un adecuado manejo de la contratación informática, se debe primordialmente a falta de apropiación de las leyes que para tal fin se han venido creando, generalmente al interior de las empresas el tema tecnológico no es considerado como un bien tangible y de allí se deriva que su legislación y normatividad sea pasada por alto.	El impacto que ocasiona la no inclusión de planes de contingencia, la falta de programas a desarrollar por parte de la empresa proveedora y la falta de referencia a las pruebas de aceptación dentro de las cláusulas del contrato, generan un grado importante de incertidumbre e inseguridad para la organización y su entorno.		**Responsables:** Área de Sistemas, Ingeniero Proveedor del Dinámica .Net, Gerencia del HUDN Interventores de contrato OJ006-2008 **Afectados:** Usuarios del módulo, área de sistemas.	En las empresas, en la protección de la información intervienen diferentes disciplinas, desde la informática, la gerencial, la logística, la matemática hasta la jurídica, entre muchas otras, que deben ser tenidas en cuenta por la oficina jurídica para garantizar que al interior de la organización se estipule todos los aspectos que rodean el sistema de información que se va ha implementar. A pesar que la empresa SYAC mantenga su dinámica de actuar de buena fe en este tipo de contratación, el Hospital Universitario Departamental de Nariño debe incorporar dentro de las clausulas contractuales el plan de contingencia que el proveedor le haga entrega, así como las pruebas de aceptación a los procesos que se implementan dentro de la Institución especialmente al Módulo de Historia Clínica que es uno de los módulos adquiridos y nuevos de la organización. El fin de incluir estos aspectos radica en que se debe documentar completamente para efectos legales, jurídicos y de otra índole todas las particularidades de que son objeto los contratos informáticos para que el volumen de inclusiones por “otros si” o modificaciones a los términos iníciales, no afecte el normal desarrollo de los procesos a implementarse e implantarse dentro de la institución, para que no se extiendan o amplíen como viene ocurriendo los tiempos de entrega y se generen sobrecostos y en la contratación.

No Preg.	DETALLE	QUE OCASIONA IMPACTO EN HC	NIVEL DE RIESGO	QUIENES INTERVIENEN	RECOMENDACIÓN
		La oficina Jurídica y las demás dependencias involucradas en el proceso de implementación del Módulo de Historia Clínica deben tener claro los aspectos de contratación informática, para que futuro esto no perjudique el desempeño óptimo del módulo.			

No Preg.	DETALLE	QUE OCASIONA IMPACTO EN HC	NIVEL DE RIESGO	QUIENES INTERVIENEN	RECOMENDACIÓN
49	**Hallazgo:** Dentro del contrato OJ006-2008 no existen especificaciones del sistema a contratar, de los procesos a desarrollar. **Criterio:** Se compara el contrato de compra – venta OJ00-2008 adquisición de módulos de actualización, mantenimiento y soporte entre el hospital universitario departamental de Nariño E.S.E y sistemas y asesorías de Colombia LTDA (SYAC), con el estándar del CECUA y la ISO 27001 **Causa:** Que dentro del contrato no se hayan tenido en cuenta algunos lineamientos o fundamentos para la contratación informática.	Esto produce que no se encuentre bien definido para el área de información y sistemas, los interventores y toda la institución, los aspectos que incluye la implantación el módulo de historia clínica, las responsabilidades de la empresa SYAC, para el con hospital, en relación a los componentes y funcionalidades del módulo, igualmente esto ocasiona mal entendidos entre ambas partes, incumplimientos de actividades, rastrazos en los cronogramas y generación de documentos anexos al contrato para clarificar los aspectos que no se		**Responsables:** Área de Sistemas, Ingeniero Proveedor del Dinámica .Net, Gerencia del HUDN Interventores de contrato OJ006-2008 **Afectados:** Usuarios del módulo, área de sistemas.	Se recomienda comparar el contrato OJ006-2008 con el estándar del CECUA, Confederación de asociaciones Europeas de Usuarios de tecnologías de la información, esta es una herramienta que brinda algunos criterios a tener en cuenta en relación a la contratación informática, se debe tener en cuenta los procesos a desarrollar por parte de la compañía que presta el servicio, las tecnologías de información deben abarcar el total de procesos y su documentación correspondiente para garantizar que el sistema de información a implementar cuenta con los estándares correspondientes de calidad y seguridad y se ajusta a la ley dentro de lo que se requiere para su implantación. Para el proceso que viene adelantando el Hospital Universitario Departamental de Nariño en el aspecto de Acreditación, y de acuerdo a la normativa que se sigue, es importante que se incluya dentro de los procesos de contratación informática los aspectos referentes a las leyes que rigen actualmente y los estándares creados para su definición. En las entidades de salud que adquieren el servicio de Dinámica Gerencial, el proceso de especificación del sistema debe de ser mucho más exigente, y estar siempre disponible.

No Preg.	DETALLE	QUE OCASIONA IMPACTO EN HC	NIVEL DE RIESGO	QUIENES INTERVIENEN	RECOMENDACIÓN
49		Incluyeron inicialmente al hacer el contrato inicial el sistema de información con la empresa SYAC.			
	Hallazgo: Dentro del contrato de compra – venta OJ006-2008 adquisición de módulos de actualización, mantenimiento y soporte entre el hospital universitario departamental de Nariño E.S.E y sistemas y asesorias de Colombia LTDA (SYAC), no se hace relación a la protección de datos. **Criterio:** La norma ISO 27 001 señala en el dominio A.15.1.4., referido a la protección de datos, como control el siguiente: "Se debe garantizar la protección de los datos personales y la privacidad, de acuerdo con la legislación y los reglamentos pertinentes y, si se aplica con las cláusulas del contrato". Para el cumplimiento de este control, quizás el referente internacional más representativo en materia de Protección de Datos Personales es la Directiva 95/46/CE, la cual establece el marco de regulación para los países miembros de la Unión Europea; norma que ha sido desarrollada en cada uno de esos países, producto de la conciencia de los ciudadanos sobre el destino de sus datos y el	Esto puede ocasionar que los datos se encuentren expuestos, para ser manipulados por cualquier persona, igualmente no existen mecanismos que los protejan por tal razón puede exigir perdida o violación de la información, falta de integridad, ocasionando una mala gestión de la oficina de sistemas, perjudicando el correcto desempeño del módulo.	ALTO	**Responsables:** Área de Sistemas, Ingeniero Proveedor del Dinámica .Net, Gerencia del HUDN Interventores de contrato OJ006-2008 **Afectados:** Usuarios del módulo, área de sistemas.	La ISO 27 001 es una herramienta de gestión estratégica que conduce a lograr la protección de la información, bien en un contexto en el cual la empresa pretenda alcanzar una certificación, o bien que sólo pretenda incorporar buenas prácticas de seguridad de la información, no sólo en sus procesos internos, sino también en sus procesos externos. El no dotar a las bases de datos personales de la seguridad y medidas de protección adecuadas por parte de las organizaciones que las poseen, en primer lugar implica un desconocimiento de lo dispuesto en la norma ISO 27001; segundo, la violación a un derecho constitucional, el cual puede ser garantizado a través de acciones de tutela, con el riesgo de indemnizar los perjuicios causados; tercero, es una limitante en el comercio internacional, pues los países europeos y algunos latinoamericanos impiden la transferencia internacional de datos con países o empresas que no garanticen un nivel adecuado de protección de datos y las sanciones que tienden a imponerse

No Preg.	DETALLE	QUE OCASIONA IMPACTO EN HC	NIVEL DE RIESGO	QUIENES INTERVIENEN	RECOMENDACIÓN
	Compromiso del Estado de garantizar las libertades públicas vinculadas al derecho fundamental a la intimidad. En consecuencia, en materia de seguridad de la información y en desarrollo de este Derecho Fundamental, consignado en el dominio de la norma ISO 27 001 antes citado, debe procurarse por parte de la organización que toda base de datos, tenga connotación comercial o no, cuente con las medidas jurídicas, tecnológicas y físicas que aseguren su protección. **Causa:** La protección de los datos es un factor importante dentro de los sistemas de información, aunque a veces se presume la buena voluntad de los contratantes es imprescindible que se estipule en las cláusulas la protección de los datos y se evidencia que en el contrato con se ha incluido cláusulas de protección de los datos.	Igualmente esto puede ocasionar carga adicional de trabajo, del grupo encargado del soporte del módulo de Historia clínica.			por violación a este derecho fundamental de la protección de datos personales y habeas data son muy cuantiosas en términos económicos.
	hallazgo: Dentro del contrato de compra – venta OJO006-2008 adquisición de módulos de actualización, mantenimiento y soporte entre el hospital universitario departamental de Nariño E.S.E y sistemas y asesorias de Colombia LTDA (SYAC), no se hace relación a la protección de datos, no se especifica el acceso al código fuente de la aplicación en caso de que el proveedor desaparezca del mercado, como se estipula en el dominio de la norma ISO 27001.	El hecho de no se haya tenido en cuenta la situación en la que la empresa SYAC, desaparezca del mercado, pone en riesgo todo el sistema de información del HUDN.		**Responsables:** Área de Sistemas, Ingeniero Proveedor del Dinámica .Net. Gerencia del HUDN, Interventores de contrato OJ006-2008,	Como la legislación contempla dentro de contratación informática, la voluntad de las partes, se recomienda que dentro del contrato de compra –venta OJ006-2008 se integre a sus cláusulas, el acceso al código fuente de la aplicación de Dinámica Gerencial en el caso fortuito que la compañía deje de existir. En términos de contratos de licencia de uso sobre aplicaciones informáticas normalmente media, la entrega de la correspondiente licencia y del ejecutable que permite la instalación de sistema de información.

No Preg.	DETALLE	QUE OCASIONA IMPACTO EN HC	NIVEL DE RIESGO	QUIENES INTERVIENEN	RECOMENDACIÓN
	criterio: La norma ISO 27001 señala en el dominio a.15.1.4., referido a la protección de datos, como control el siguiente: “se debe garantizar la protección de los datos personales y la privacidad, de acuerdo con la legislación y los reglamentos pertinentes y, si se aplica con las cláusulas del contrato”. Para el cumplimiento de este control, quizás el referente internacional más representativo en materia de protección de datos personales es la directiva 95/46/ce, la cual establece el marco de regulación para los países miembros de la unión europea; norma que ha sido desarrollada en cada uno de esos países, producto de la conciencia de los ciudadanos sobre el destino de sus datos y el compromiso del estado de garantizar las libertades públicas vinculadas a la derecho fundamental a la intimidad. En consecuencia, en materia de seguridad de la información y en desarrollo de este derecho fundamental, consignado en el dominio de la norma ISO 27001 antes citado, debe procurarse por parte de la organización que toda base de datos, tenga connotación comercial o no, cuente con las medidas jurídicas, tecnológicas y físicas que aseguren su protección. **Causa:** Cuando se elaboró el contrato se dejaron de definir muchos lineamientos de situaciones que no se contemplan en contratación informática.	Puesto que dado este caso, en primera instancia el hospital dependería del buen proceder de la empresa SYAC para hacer entrega del código fuente de la aplicación, sin pedir una remuneración adicional. De caso contrario existe el riesgo de que sea exigido un monto adicional por la entrega del código. En segunda medida se evidencia que el sistema dynamica gerencial dentro del Hospital se quedaría sin soporte.		Oficina Jurídica del Hospital Universitario Departamental de Nariño **Afectados:** Todo el personal administrativo y asistencia del HUDN, Gerencia de la Institución, Usuarios.	La ISO 27001 plantea la importancia de que la organización pueda garantizar el acceso al código fuente de la aplicación cuyo uso se concede, en caso de que el titular del programa de ordenador desaparezca del mercado; situación que exige regular tal hipótesis en términos de seguridad de la información.

(DS3) - Administración de Desempeño y Capacidad

En este proceso se buscar evaluar si la capacidad y desempeño del módulo son los adecuados, son disponibles y si se esta haciendo el mejor uso de estos para alcanzar el desempeño deseado, en el análisis de este proceso se encontró que:

No Preg	DETALLE	QUE OCASIONA IMPACTO EN HC	NIVEL DE RIESGO	QUIENES INTERVIENEN	RECOMENDACIÓN
	Hallazgo: No existe un monitoreo continuo del desempeño y capacidad del módulo de Historia clínica, igualmente no se tienen en cuenta las mejoras. **Criterio:** En relación a la administración de desempeño y capacidad, el Hospital Universitario Departamental de Nariño, afirma poseer las políticas y procedimientos en relación al reporte de desempeño del módulo de historia clínica, carga de trabajo, administración de la capacidad y programación de actividades. Sin embargo al revisar la documentación las políticas no se encuentran documentadas	Esto produce que el módulo se este sub-utilizando en la realización de su objetivo general, igualmente no se aprovechen todos sus recursos para una optima gestión del módulo en relación a los tiempos de oportunidad de la atención a pacientes, descuidando las		**Responsables:** Área de Sistemas, Ingeniero Proveedor del Dinámica .Net, Gerencia del HUDN Interventores de contrato OJ006-2008 **Afectados:** Usuarios del módulo, área de sistemas.	La Administración Del Desempeño incluye procesos que comunican eficazmente las metas alineadas de la compañía, evalúan el desempeño de los empleados y los recompensan de manera justa. La planeación clara de objetivos, el desarrollo de habilidades y una verdadera cultura de compensación de acuerdo al desempeño son prácticas de administración del talento que las compañías exitosas utilizan para demostrar a sus empleados que son valorados por la organización. Se ha comprobado que el desempeño eficaz y la administración del talento aumentan la moral del empleado y la productividad en general. Para que cualquier empresa supere a su competencia necesita contar con empleados productivos y comprometidos.

No Preg.	DETALLE	QUE OCASIONA IMPACTO EN HC	NIVEL DE RIESGO	QUIENES INTERVIENEN	RECOMENDACIÓN
	Para medir el desempeño, se necesita evaluarlo a través de indicadores de desempeño. Estos indicadores deben ayudar a la gerencia para determinar cuan efectiva y eficiente es la labor de los empleados en el logro de los objetivos, y por ende, el cumplimiento de la misión organizacional. Así mismo, deben estar incorporados en un sistema integral de medición del desempeño que haga posible el seguimiento simultáneo y consistente en todos los niveles de la operación de la empresa, desde el logro de los objetivos estratégicos de la empresa al más alto nivel hasta el desempeño individual de cada ejecutivo y empleado. Uno de los últimos sistemas aplicados y que goza de mucha aceptación para la evaluación del desempeño, es la denominada evaluación de 360 grados. Este es el proceso mediante el cual se le permite al empleado dar su opinión, y poder evaluar a la administración en la misma manera en que ha sido evaluado, al cual se le han venido incorporando diversos cambios y mejoras a fin de adaptarlo a las necesidades específicas de cada empresa. Los nuevos enfoques de la administración del desempeño ha vislumbrado que este es un proceso dinámico de mejora continua y que debe ser flexible al cambio. En la actualidad las compañías monitorean sus procesos de cambio y medición del desempeño del empleado a través de la inclusión de diversos softwares especializados.	Directivas de los estándares que están involucrados con la acreditación del Hospital.			El incremento en costos, en competidores y el tiempo que implica contratar y entrenar a nuevos talentos, han hecho que la retención de los empleados sobresalientes sea esencial para la rentabilidad de la empresa. Al reconocer las debilidades y desarrollar las habilidades necesarias, los gerentes pueden planear la sucesión, mientras los empleados pueden progresar con objetivos profesionales alcanzables. Un factor muy importante para la administración del desempeño es la evaluación continua, pues este sistema no puede ser por ningún motivo estático, debe evolucionar constantemente y ser cuidadosamente monitoreado para una mejora continua. Las tecnologías de Información han hecho su inserción en la administración del desempeño de las organizaciones. Esta herramienta ha venido a facilitar los procesos, sin embargo muchas de estas compañías se han dejado llevar por el frenesí de utilizar Al interior de la Oficina de Información y Sistemas existe sobrecarga de trabajo debido a la falta de políticas claras dentro de la organización. Se recomienda realizar evaluaciones periódicas del desempeño y documentar políticas de administración del mismo para evitar que al interior del área de sistemas e información se sature la carga de trabajo y se evidencie el descontento general por parte del talento humano que labora en la institución. Se hace necesario hacer una evaluación de los puestos de trabajo y capacitar personal que ayude en las tareas asignadas a la oficina de sistemas.

No Preg.	DETALLE	QUE OCASIONA IMPACTO EN HC	NIVEL DE RIESGO	QUIENES INTERVIENEN	RECOMENDACIÓN
	Causa: No se está llevando a cabo un seguimiento del desempeño del módulo de historia clínica, en relación a los procesos y resultados que debe emitir, en las diferentes áreas como triage, urgencia, hospitalización y consulta externa.				Pocas son las compañías líderes, que aplican muchos de los principios básicos y la tecnología de métodos de administración de desempeño para proyectarse hacia el futuro. No tiene ningún sentido evaluar al empleado, e indicarle en que estuvo mal, dándole retroalimentación, si ésta no funciona para proyectarlo hacia el futuro mejorando su desempeño para alinearse con los objetivos de la compañía. Se sugiere, la incorporación de puntos de mejora que se establezcan en el tiempo para chequear el progreso de los empleados a través de metas específicas, más que esperar hasta la próxima evaluación del desempeño para determinar el progreso. Todo el software existente al interior de la organización debe estar monitoreado por la gerencia o la dependencia que se encargue de hacer seguimiento al mismo, y plantear que la evaluación del desempeño no puede observarse como un fenómeno de revisión de desempeño, sino que debe ser usado para mejorar el futuro, haciéndolo parte de él.

(DS5) - Garantizar la seguridad de Sistemas

En este proceso se busca evaluar los mecanismos de seguridad para salvaguardar la información contra uso no autorizados, divulgación, modificación, daño o pérdida, en este análisis se encontraron los siguientes hallazgos:

No Preg	DETALLE	QUE OCASIONA IMPACTO EN HC	NIVEL DE RIESGO	QUIENES INTERVIENEN	RECOMENDACIÓN
57	**Hallazgo:** No existen políticas al interior del Hospital Universitario Departamental relacionado con el comercio electrónico, ni estándares de encriptación, las políticas de seguridad se basan solo en proceso de realizar copias de seguridad a la información dentro de la institución. Esto se puede asegurar por la entrevista sostenida con el coordinador del Área de sistemas y el análisis de los procesos que se llevan al interior del área. **Criterio:** Toda organización debe implementar políticas para el acceso a los recursos informáticos, especialmente el acceso a Internet, comercio electrónico y tecnologías de información.	Esto puede ocasionar que no se proteja, asegure y administre la información correctamente perjudicando su integridad, causando desorganización y caos en el manejo de la información.		**Responsables:** Alta gerencia, Área de Información y sistemas. **Afectados:** Usuarios, Área de información y sistemas, Funcionarios de Hospital.	Se recomienda al interior de la organización del Hospital Universitario Departamental de Nariño construir un documento formal que las incluya. La política de seguridad es una herramienta de gran valor para enfrentar el Plan de seguridad de una instalación y debe entenderse como un proceso integral que parte de la situación real y se construye teniendo en cuenta los recursos y riesgos a que está expuesta la organización, convirtiéndola en una guía de operación y actuación para proteger los activos y garantizar la continuidad y calidad de los servicios. Es indispensable que la política de seguridad que se implemente en el hospital universitario Departamental tenga dos propósitos centrales:

No Preg.	DETALLE	QUE OCASIONA IMPACTO EN HC	NIVEL DE RIESGO	QUIENES INTERVIENEN	RECOMENDACIÓN
57	La realización de Copias de seguridad, es un proceso basado en el sentido común, que se puede asociar a una política clara y sencilla que involucre los actores de la institución. Hasta hace poco tiempo, el comercio electrónico estaba vinculado estrictamente a la transmisión de datos comerciales seguros vía computador (Electronic Data Interchange - EDI), solamente al alcance del sector financiero y las grandes firmas comerciales. El desarrollo del Internet y en especial de la WWW puso el comercio electrónico al alcance de un número mayor de personas y se convirtió en una gran oportunidad de negocios. El rápido desarrollo del comercio electrónico, ha generado discusión sobre temas tan importantes como la globalización, la apertura contractual y financiera, el respeto por la propiedad, en especial la propiedad intelectual, la privacidad y seguridad, la interconectividad e interoperatividad, y los riesgos. **Causa:** Que dentro de la políticas de seguridad de la Institución no se ha incluido leyes como: ley 527 de 1999 y el Decreto 1747 de 2000 en donde se legisla el uso y las políticas al interior de las organizaciones para el comercio electrónico, la ley 527 en el artículo numero 2, define los mensajes de datos, el comercio electrónico, la firma digital, entidad de certificación, intercambio electrónico de datos y sistema de información.	Igualmente al no existir políticas internas sobre la gestión de seguridad por parte de los usuarios, puede ocasionar que la información se violada, o se utilizada bajo otros fines, que pueden perjudicar la organización.			• Informar a todos los usuarios sobre las obligaciones que deben asumir respecto a la seguridad asociada a los recursos de tecnología de información. • Dar las guías o exponer los controles y criterios al personal de la institución para actuar ante posibles amenazas y problemas presentados. Esta política debe involucrar a los diferentes sectores de la organización: • Alta gerencia • Responsables de Tecnologías de Información • Encargados de la seguridad • Auditores • Coordinadores de las dependencias y los usuarios. El documento formal debe definir elementos asociados a la adquisición de hardware, software, y contratación de servicios externos. Las políticas de seguridad de la información es el conjunto de normas, reglas, procedimientos y prácticas, que regulan la protección de la información contra la pérdida de confidencialidad, integridad y disponibilidad, tanto en forma accidental como intencionada. El hospital a través de la coordinación de sistemas, debe adoptar los mecanismos que le permitan el resguardo, confiabilidad y oportunidad de su información.

(DS-7) - Educación y entrenamiento de Usuarios

En la evaluación de este proceso se busca identificar si los programas de capacitación ofrecidos cumplen con las necesidades de entrenamiento, igualmente la capitación de usuarios en cuento a seguridad y recursos de las tecnologías de información, en la evaluación de este proceso se han encontrado:

No Preg	DETALLE	QUE OCASIONA IMPACTO EN HC	NIVEL DE RIESGO	QUIENES INTERVIENEN	RECOMENDACION
	Hallazgo: Dentro del Hospital Universitario Departamental de Nariño No existen políticas y procedimientos generales con respecto a entrenamiento sobre controles y conciencia de seguridad. El coordinador del área de información y sistemas de la organización no ha realizado una gestión en conjunto con el área de salud ocupacional, para capacitar a todos los involucrados con el manejo de las tecnologías de información y riesgos de trabajo que estas pueden traer. Al personal temporal de la institución no le hacen participe del programa de capacitación de salud ocupacional y no existe un reglamento en donde se exija que cumplan estos programas con todo el recurso humano de la entidad.	Debido a la ausencia de conocimiento de las políticas del hospital a nivel del programa de salud Ocupacional referente a las tecnologías de información, su entorno y las dependencias,	MEDIO	**Responsables:** Coordinador del área de Sistemas Técnicos en sistemas del área.	La coordinación de sistemas en acople con la oficina de Salud ocupacional, deben instaurar un programa de toma de conciencia en Tecnologías de Información que le brinde al personal de las áreas involucradas en la administración y las asistenciales que integran los sistemas de información de la organización, la capacitación oportuna y suficiente acerca del desempeño tecnológico.

No Preg.	DETALLE	QUE OCASIONA IMPACTO EN HC	NIVEL DE RIESGO	QUIENES INTERVIENEN	RECOMENDACION
	Criterio: Política sobre controles y conciencia sobre seguridad, al interior del Hospital Universitario Departamental de Nariño se define las funciones de la entidad acreditadora y se adoptan otras funciones dentro del manual de gerencia de sistemas de información con fecha 8 de mayo de 2006, el propósito del estándar de la gerencia de la información es señalar los elementos sustanciales de la organización para el diseño y puesta en marcha de un proceso coherente de gerencia de la información y de los recursos utilizados para su adecuado desarrollo. Con esto se garantiza la estructura y coherencia de la Información para generar habilidades de respuesta a los requerimiento tanto de los clientes como del personal que labora al interior de la empresa, este estándar se mide con indicadores, factores de calidad del proceso de atención, en donde se prioriza el riesgo, el volumen, su incidencia sobre factores claves de calidad y dentro de su medición, se desarrollan procesos de mejoramiento, que son compartidos y monitorizados permanentemente. En el literal Número 1, hace referencia a que los procesos de la gerencia de la información, están diseñados para identificar las necesidades de información al interior de cada una de las unidades funcionales, especialmente aquellas relacionadas con el proceso de atención, estas necesidades incluyen:	Ocasiona que no se presenten a las capacitaciones, que no conozcan los instructivos correspondientes y que no tengan en cuenta las normas de seguridad y ergonomía.		Oficina de salud Ocupacional. **Afectados:** Usuarios y recurso humano de la Institución	No es conveniente centrar el conocimiento acerca de la tecnología en una sola oficina, que para el Hospital Universitario Departamental de Nariño, se conoce como la oficina de Información y Sistemas, el personal de planta de la institución, así como el personal temporal deben acudir a capacitaciones periódicas en Tecnologías de Información que le brinden un conocimiento apropiado para que la oficina de Información y sistemas no sobrecargue su trabajo.

No Preg.	DETALLE	QUE OCASIONA IMPACTO EN HC	NIVEL DE RIESGO	QUIENES INTERVIENEN	RECOMENDACION
	• Procesos de atención a clientes. • Planeación de la organización. • Asignación de recursos. • Productividad. • Educación del personal. • Investigación. • Necesidades del cliente. • Direccionamiento organizacional. • Mejoramiento de la calidad. • Coordinación de servicios frente a la atención del cliente. Dentro del plan de gerencia se incluye: • Identificación de las necesidades de información. • Captura de datos. • Análisis de la información. • Transmisión. • Estandarización. • Uso de la tecnología. • Procesos de implementación basada en prioridades. • Almacenamiento, conservación y depuración de la información. • Seguridad y confidencialidad de la información. • Sistema de mejoramiento. **Causa:** Falta de gestión sobre capacitación del recurso humano del hospital, en salud ocupacional para el manejo de las tecnologías de Información, por parte de el área de sistemas y el área de salud ocupacional.				

(DS-9) - Administración de la configuración

Mediante el estudio de este proceso se buscar evaluar de todos los componentes de TI, prevenir alteraciones no autorizadas, verificar la existencia física y proporcionar una base para el sano manejo de cambios, se evaluaran si existen los controles que identifiquen y registren todos los activos de TI así como su localización física y un programa regular de verificación que confirme su existencia, en relación ha este proceso se encontraron los siguientes hallazgos:

No Preg.	DETALLE	QUE OCASIONA IMPACTO EN HC	NIVEL DE RIESGO	QUIENES INTERVIENEN	RECOMENDACION
	Hallazgo: La oficina de control interno no posee documentación y no tiene conocimiento acerca de los tipos de controles que se deben adoptar en materia informática, esta oficina depende directamente de la alta gerencia, se ha encontrado que el Hospital Universitario Departamental de no posee políticas de seguridad informática en cuanto al uso de aplicaciones electrónicas que comprenden: • Cuentas de usuario • Internet • Correo electrónico • Políticas de uso de computadores, impresoras y periféricos.	Esto puede producir problemas como: mala utilización de los recursos computacionales, adquisición de virus informáticos que pueden entorpecer el funcionamiento normal del sistema de Información, bajo rendimiento laboral por dedicarse a otras aplicaciones no propias del puesto de trabajo.			Cada vez se hace más necesario un análisis del trafico de: • Correo electrónico y corporativo. • Páginas web que se visitan desde los ordenadores de la empresa. • Internet no puede ser de libre uso dentro de la empresa, por motivos diversos y tiene que ver con el costo que representa para la empresa, el servicio de banda ancha, la baja en la productividad laboral, el riesgo informático que representa recibir cadenas de e-mails con virus, o navegar por sitios poco seguros Se deben incorporar dentro de las políticas de la organización, unas directrices especiales con el propósito de asegurar que los funcionarios utilicen correctamente los recursos tecnológicos que la empresa pone a su disposición para el desarrollo de las funciones institucionales; dichas políticas deben

No Preg.	DETALLE	QUE OCASIONA IMPACTO EN HC	NIVEL DE RIESGO	QUIENES INTERVIENEN	RECOMENDACION
	Criterio: Control interno informático es una herramienta enfocada a la adecuada gestión de los sistemas de información, la ley 527 de 1999 define y reglamenta el acceso y uso de los mensajes de datos, entre ellos, el correo electrónico, como un servicio de carácter estratégico en las empresas y una herramienta de utilidad en el trabajo diario, por lo que se hace necesario reglamentar para los usuarios internos el procedimiento de utilización. El propósito de las políticas es asegurar que los funcionarios utilicen correctamente los recursos tecnológicos que la empresa pone a su disposición para el desarrollo de las funciones institucionales. **Causa:** Que no existen políticas que garanticen la implementación de un sistema de gestión de seguridad principalmente el manejo que le dan los usuarios a la Internet, correos corporativos, y uso de todos los recursos de sus computadores personales, para la protección de la información en el hospital.				ser de obligatorio cumplimiento y estas incluyen cuentas de usuario, claves de acceso, Internet y correo electrónico. En relación a las cuentas de usuario, la cual constituye la principal vía de acceso a los sistemas de información que posee la empresa, en donde se aísla al usuario del entorno, impidiendo que pueda dañar a otros usuarios, y permitiendo a su vez que pueda personalizar su entorno sin que esto afecte a otros. Cada persona que acceda al sistema debe tener una sola cuenta de usuario, esto permite realizar un seguimiento y control, evita que se interfieran las configuraciones de distintos usuarios. Políticas de Claves de acceso: dentro de las políticas para las claves de acceso, que evitan ingresos no autorizados a información de la empresa, se deben tener en cuenta las siguientes sugerencias: • No utilizar como clave de acceso su nombre, apellido, o algún otro dato personal o familiar. • No utilizar palabras simples que puedan ser encontradas rápidamente. • No comentar a nadie su clave de acceso. • Las claves de acceso se deben memorizar y no anotar. • Al tercer intento de ingreso fallido el sistema debe bloquear la cuenta. La longitud del password por norma general y según la política de seguridad de información debe contener mínimo 6 caracteres y máximo 10 de tipo alfanumérico y que combine al menos 2 características como mayúsculas, minúsculas o símbolos.

No Preg.	DETALLE	QUE OCASIONA IMPACTO EN HC	NIVEL DE RIESGO	QUIENES INTERVIENEN	RECOMENDACION
					• La clave de acceso o password debe cambiarse cada 90 días. Política de uso de la Internet: la gerencia informática, supervisará e identificará dentro de las categorías, los web sites más visitados por los usuarios de la empresa, los tipos de pornografía, violencia, ocio, screensavers, gift animation, tarjetas electrónicas, música y otros no relacionados con las funciones de la entidad. Se debe proceder a bloquear los websites y los demás que constituyan objeto no institucional. Para los efectos de la ley de tecnologías de Información y el desarrollo de las políticas al interior de la organización, no debe haber accesos a webmail, no corporativos. Dentro de la mensajería instantánea se abren nuevas oportunidades a los virus para que se propaguen, adicionalmente permiten la vulnerabilidad para que personas tengan acceso a la información corporativa (spyware). Entre las amenazas más frecuentes están: • Gusanos y virus. • Programas de puertas traseras – troyanos. • Secuestro de sesiones o suplantación de personalidad • Denegación de Servicio • Divulgación de información No autorizada. Por lo tanto se sugiere que el acceso al Messenger no sea posible para ningún funcionario, y se recomienda adoptar las políticas en cuanto al uso de computadores, impresoras, periféricos que se han diseñado en el marco legal de la ley 527 de 1999.

No Preg.	DETALLE	QUE OCASIONA IMPACTO EN HC	NIVEL DE RIESGO	QUIENES INTERVIENEN	RECOMENDACION
	Hallazgo: En relación a la infraestructura física y de red del Hospital Universitario Departamental de Nariño, y en base a la evidencia observada se encontró: - En los cuartos de equipos correspondientes a los pisos 1, 3 y 5 no se encuentran elementos de bioseguridad como extintor, sistema de ventilación, adecuación de tomas eléctricas, señalización. - Distribución inadecuada del cableado estructurado en el cuarto del servidor y los 2 cuartos de equipos del primer piso. - Falta de identificador de los Pach panel. - En el cuarto de equipos del tercer piso no existe mapa de correspondencia. - No existen punto para gestión de pruebas. - El cuarto de servidor y los cuartos de equipos del primer piso, no cumplen con las normas del cableado estructurado, en relación a pach panel, distribución del cableado, tomas eléctricas, espacio físico, ventilación. - En los cuartos de equipos del tercer y quinto piso se encontraron elementos no pertenecientes a esta área como papel, cajas, ollas, cuadros y otros elementos que además dificultan el acceso al cuarto y no son propios del área.	Esto ocasiona que exista mucha desorganización en el área de información y sistemas, en relación a las actividades de mantenimiento, dificulta la correcta administración y mantenimiento de la red, conjuntamente ocasiona inseguridad de la red por presentar fácil acceso a los diferentes puntos. Al no existir una correcta identificación de los puntos, se dificulta hacer la corrección de errores, y un mal desempeño de la red que simultáneamente perjudica el desempeño de las aplicaciones.	ALTO	**Responsables:** Alta Gerencia, Área de información y sistemas. **Afectados:** Usuarios de todos los recursos informáticos.	Se recomienda que la gerencia junto con el área de información y sistemas, trabaje en conjunto para mirar la viabilidad de migrar todo el cableado de la organización a categoría 6A Incluir dentro de todos los cuartos de equipos los elementos de bioseguridad que cumplan con la normativa, e inspeccionar periódicamente que estos elementos se encuentren en buen estado, ya que en la actualidad solo se cuenta con el detector de temperatura. Ajustarse a la norma de distribución de cableado estructurado en los cuartos de equipos del primer piso, en donde se observa desorganización. Se recomienda que se haga una correcta identificación de cada punto de red en los diferentes cuartos de equipos, así como también se incluir dentro del rack el mapa de correspondencia e puntos. Se recomienda plantear políticas permitan la implementación del diseño de una sed segmentada.

No Preg.	DETALLE	QUE OCASIONA IMPACTO EN HC	NIVEL DE RIESGO	QUIENES INTERVIENEN	RECOMENDACION
	Criterio: En base al COBIT, es necesario contar con una adecuada infraestructura física y el diseño de un red de datos, que permitan la desempeño transparente de los recursos informáticos, como el sistema operativo, los sistemas de información. **Causa:** Falta de migración del cableado del cuarto del servidor y del los cuartos de equipos del primer pisos de categoría 5B a 6A, falta de organización en los demás cuartos de equipos por parte del personal encargado del las actividades de mantenimiento a la red y los equipos de cómputo, falta de cumplimiento de las normas de cableado estructurado, puesto que es de gran importancia contar con una correcta distribución de los puntos de red e identificación del los mismos, que llegan a los pach panel y esto se encuentra muy desorganizado, falta de definición de políticas que garanticen que exista un buen manejo de la infraestructura física por sus responsables igualmente falta de definición de políticas en cuanto al diseño de la red.				
	Hallazgo: Al realizar el plan de pruebas de auditoría, a la red cableada e inalámbrica, se encontraron fallas de seguridad en los siguientes aspectos:	Los usuarios no tienen libre uso de los recursos informáticos que le brinda el hospital, y al no poseer ningún tipo de capacitación sobre la correcta gestión de la seguridad sobre los mismos,			Se recomienda al área de información y sistemas que dentro de la políticas de Seguridad que solo incluyen la realización de copias de seguridad se establezcan lineamientos sobre:

No Preg.	DETALLE	QUE OCASIONA IMPACTO EN HC	NIVEL DE RIESGO	QUIENES INTERVIENEN	RECOMENDACION
	- Antivirus desactualizados en todos los equipos de las áreas involucradas con el manejo de módulo de historia clínica. - Falta de antivirus en algunos equipos como en el área de Oncología. - Desactivación de firewalls. - Uso de aplicaciones indiscriminadamente como messenger, yahoo, skipe, ares, a tube cátcher y otras aplicaciones que no son propias de las labores de los puestos de trabajo. - Acceso a Internet indiscriminado. - Acceso a correo electrónico. Todo esto producto de la no implementación al interior de la organización, de políticas que disminuyan los riesgos y la escasa capacitación del personal en cuento a tecnologías de información. En relación a las pruebas realizadas a la base de datos se encontró: - Existen datos repetidos. - Existen tablas que relacionan los mismos datos. - No existe una correcta normalización de la base de datos. **Criterio:** De acuerdo a la norma ISO 27001 en sus dominios de políticas de seguridad de la información y la organización de la misma, como también en el dominio de seguridad física y del entorno, sugiere a las entidades que implementen políticas de seguridad en relación a: usuarios y gestión de sus recursos,	puede ocasionar problemas a nivel de la adquisición de virus, que pueden dañar la aplicaciones, las bases de datos y en general toda la información de la institución, igualmente puede surgir violación, perdida o daño de información por parte de personas inescrupulosas que accedan a los recursos de la red LAN e Inalámbrica. Y finalmente esto ocasiona el mal desempeño del aplicativo, sobrecarga de trabajo de los funcionarios del área de sistemas		**Responsables:** Área de Información y Sistemas. **Afectados:** Todos los Usuarios del Hospital,	Restricción al uso de ciertas páginas de internet, restringir desde el servidor el acceso libre a internet. Establecer restricciones sobre el uso del correo electrónico, y descarga de archivos. Establecer políticas que garanticen que los usuarios no instalen otras aplicaciones, hacer un monitoreo continuo en los equipos de los usuarios para verificar que no se han instalado nuevas aplicaciones, y de ser necesario, restringir las cuentas de administradores, o instalar programas especializados en mantener la configuración inicial del equipo. Capacitar a los usuarios sobre el manejo y actualización de antivirus, sobre el manejo de aspectos de seguridad e informática. Mantener activos los firewall del los equipos y principalmente del servidor, que ayuden a impedir que piratas informáticos o software mal intencionado tengan acceso al equipo, a través de la red e internet. Realización de un documento formal donde se especifique el uso de aplicaciones en los equipos de entidad y las directrices generales que se implementaran acerca de las tecnologías de información dentro de la institución, darlas a conocer a todo el recurso humano del hospital y darle a conocer la ventaja de aplicación de las norma y procedimientos de seguridad.

No Preg.	DETALLE	QUE OCASIONA IMPACTO EN HC	NIVEL DE RIESGO	QUIENES INTERVIENEN	RECOMENDACION
	Capacitaciones en seguridad para usuarios, definición de los recursos de internet a los que se debe acceder, restricciones sobre los recursos del hardware y la instalación de aplicaciones, para una correcta gestión de seguridad. **Causa:** Que dentro de la institución no se hayan definido políticas de seguridad, ni tampoco se hayan establecido procedimientos ni funciones sobre los responsables para mantener un control sobre la seguridad	puede ocasionar problemas a nivel de la adquisición de virus, que pueden dañar la aplicaciones, las bases de datos y en general toda la información de la institución, igualmente puede surgir violación, perdida o daño de información por parte de personas inescrupulosas que accedan a los recursos de la red LAN e Inalámbrica. Y finalmente esto ocasiona el mal desempeño del aplicativo, sobrecarga de trabajo de los funcionarios del área de sistemas	ALTO	**Responsables:** Área de Información y Sistemas. **Afectados:** Todos los Usuarios del Hospital,	

5. INFORME FINAL DE AUDITORÍA

5.1. INTRODUCCIÓN

Este documento muestra el resumen de los resultados obtenidos de la realización del proyecto de auditoria al módulo de historia clínica electrónica, del sistema dinámica gerencial en el hospital universitario departamental de Nariño, su enfoque se encuentra basado en los principios del COBIT (Control objectives for information and related Technology) de la information systems audit and control asociation (ISACA) y la norma ISO 27001 que especifica los requisitos del sistema de gestión de seguridad de la información(SGSI).

La importancia de la realización de este proyecto, contribuirá de forma significativa, al área de información y sistemas del hospital, para brindar una perspectiva de su funcionamiento y trabajo, igualmente nos mostrara un balance de como ha sido hasta el momento el proceso de implantación del módulo de historia clínica .NET, permitiendo crear juicios y criterios para tener en cuenta en un futuro cuando el módulo se encuentre en producción total.

El proyecto de auditoria al módulo de historia clínica electrónica, se ha basado principalmente en el estudio del cumplimiento de los requerimientos de la institución, la seguridad física y lógica, el desempeño del módulo y la gestión y administración del recurso humano encargado de su implantación, esto con el fin de obtener los fundamentos necesarios para poder realizar un examen critico y brindar la recomendaciones para mejorar la eficiencia y eficacia de una de las dependencias cuyo fin primordial es cuidar el buen manejo de unos de los activos más importantes de la institución “su información”.

Finalmente es importante resaltar que con el desarrollo de esta auditoria, se contribuye con el proceso de acreditación del hospital, forjando los primeros

antecedentes relacionados con la evaluación de un sistema de gestión de seguridad de información (SGSI) de calidad, como lo enmarca el estándar usado para su estudio que es la ISO 27001, y que permitirá el mejoramiento futuro del desempeño del módulo de historia clínica hacia los habitantes de la región de Nariño.

5.2. VISIÓN GENERAL DE LA METODOLOGÍA EMPLEADA

El contexto para el desarrollo del proyecto de auditoria es el módulo de historia clínica .NET del sistema dinámica gerencial, la metodología utilizada para su desarrollo parte de un estudio preliminar de todo el entorno de la institución en relación a su infraestructura física, el sistema de información, las dependencias, el recurso humano y sus diferentes procesos, con fin de plantear los objetivos y definir el alcance y las limitaciones de la auditoria, luego se realizo la asignación de recursos en relación al espacio físico, los equipos de computo, impresora, scanner entre otros, lo cual fue pactado por el grupo Auditor (Jenny Burgos – Ma. Carolina Domínguez Gómez) con el coordinador del área de información y sistemas, una vez conocido el entorno se planteo un programa de auditoria donde se especificaron los procesos a evaluar, los documentos a analizar, las pruebas y actividades ha desarrollar, esto con el fin de recolectar las evidencias e identificar los riesgos relacionados con la gestión del módulo de historia clínica, brindando las bases necesarias para definir los hallazgos y realizar las recomendaciones respectivas a cada uno de ellos, como también establecer los controles requeridos para eliminar o disminuir el riesgo, por último se elaboro un informe final donde se expone los aspectos evaluados y los hallazgos encontrados con el fin de plantear los controles ha seguir por parte de la administración, este informe será socializado con el coordinador del área de información y sistemas a cargo de la revisión de los resultados de este proyecto.

5.3. DESCRIPCIÓN GENERAL DE LAS HERRAMIENTAS UTILIZADAS

Para la realización de este proyecto se utilizaron los siguientes estándares:

COBIT: (Control objectives for information and related technology) de la information systems audit and control asociation (ISACA)

COBIT se aplica a los sistemas de información de toda la empresa, incluyendo las computadoras personales, mini computadoras y ambientes distribuidos, esta basado en la filosofía de que los recursos de TI necesitan ser administrados por un conjunto de procesos naturalmente agrupados para proveer la información pertinente y confiable que requiere una organización para lograr sus objetivos.

La estructura del COBIT se encuentra dividida en:

- Dominios: Agrupación natural de procesos, normalmente corresponden a un dominio o una responsabilidad organizacional.
- Procesos: Conjuntos o series de actividades unidas con delimitación o cortes de control.
- Actividades: Acciones requeridas para lograr un resultado medible, se definen 34 objetivos de control generales, uno para cada uno de los procesos de las TI, estos procesos están agrupados en cuatro grandes dominios.

El COBIT esta enfocado principalmente a la evaluación de aspectos como: la efectividad, la eficiencia, la Integridad, la disponibilidad, el cumplimiento y la confiabilidad de la información.

Los recursos que utiliza son: los datos, las aplicaciones, la tecnología, las instalaciones y el personal, asignando un nivel de clasificación para cada uno de estos recursos como: *primario, secundario o blanco* de acuerdo a su nivel de importancia.

Para el desarrollo de esta auditoria se tomaron la mayoría de procesos de todos los dominios de COBIT que son:

- *Planeación y organización:* Este dominio se refiere a la identificación de la forma en que la tecnología de información puede contribuir de la mejor manera al logro de los objetivos del negocio, además, la consecución de la visión estratégica necesita ser planeada, comunicada y administrada desde diferentes perspectivas, finalmente, deberán establecerse una organización y una infraestructura tecnológica apropiadas.
- *Adquisición e implementación:* Para llevar a cabo la estrategia de TI, las soluciones de TI deben ser identificadas, desarrolladas o adquiridas, así como implementadas e integradas dentro del proceso del negocio, este dominio cubre los cambios y el mantenimiento realizados a sistemas existentes.
- *Entrega y soporte:* En este dominio se hace referencia a la entrega de los servicios requeridos, que abarca desde las operaciones tradicionales hasta el entrenamiento, pasando por seguridad y aspectos de continuidad, con el fin de proveer servicios, deberán establecerse los procesos de soporte necesarios, e incluir el procesamiento de los datos por sistemas de aplicación, frecuentemente clasificados como controles de aplicación.
- *Monitoreo:* Todos los procesos necesitan ser evaluados regularmente a través del tiempo para verificar su calidad y suficiencia en cuanto a los requerimientos de control.

ISO 27001

Como código de práctica, la norma BS7799-1 era un documento de orientación y recomendaciones el cual se internacionalizó como ISO/IEC 17799 en diciembre del año 2000, la segunda parte conocida como BS7799-2 se internacionalizó como ISO/27001 en noviembre de 2005 y contó con más de 1700 empresas certificadas en BS7799-2, este esquema se publicó por ISO como estándar ISO 27001, al tiempo que se revisó y actualizó ISO17799, esta

última norma se renombra como ISO 27002:2005 el 1 de Julio de 2007, manteniendo el contenido así como el año de publicación formal de la revisión.

La norma ISO 27001 contempla diez dominós que son:

- Política de seguridad de la información.
- Organización de la seguridad de la información.
- Gestión de activos.
- Seguridad de los recursos humanos.
- Seguridad física y del entorno.
- Gestión de comunicaciones y operaciones.
- Control de acceso.
- Adquisición, desarrollo y mantenimiento de sistemas de información.
- Gestión de incidentes de la seguridad de la información.
- Cumplimiento.

5.4. ACTIVIDADES PARA LA RECOLECCIÓN DE INFORMACIÓN

Las actividades realizadas para la recolección de evidencias en los diferentes procesos del programa de auditoria fueron:

- Realización de Cuestionarios:

  Se realizaron cuestionarios, donde se plantearon preguntas las cuales permitieron recolectar información de cómo se están llevando a cabo las operación en relación al módulo de historia clínica, el conjunto de estas preguntas recibe el nombre de Checklist, con una posible respuesta binaria (SI - NO). El cuestionario nos permite medir o calificar el proceso, para ello es necesario dar un puntaje máximo entre 1 y 5 a cada pregunta, de acuerdo a su nivel de importancia según criterio propio, la sumatoria del puntaje de todas las preguntas nos da el total de la encuesta, luego se prosigue a calificar la columna del SI, sumando el puntaje de sus preguntas, y las columnas del NO Y NA, el estudio se centra en la respuestas de la columna del NO, es necesario que conjuntamente se trabaje en la obtención de pruebas que permitan

ratificar los resultados de la encuesta, y determinar las conclusiones respectivas.

- Entrevistas: Sirve como instrumento para que el auditor pueda conocer las funciones del personal auditado y como se están llevando a cabo los procesos dentro de la organización.
- Recolección de políticas, manuales, guías y todo documento relacionado con los aspectos ha evaluar sobre el módulo de historia clínica electrónica.
- Realización de pruebas de ejecución, de acuerdo al programa de pruebas de la auditoria, como el uso de sniffers, mapeo de puertos, escaneo de la red entre otros.

5.5. VISIÓN GENERAL DEL PROGRAMA DE AUDITORÍA

A continuación se relaciona una visión global del programa de auditoria a seguir, para evaluar el módulo de historia clínica electrónica del hospital departamental de Nariño, donde se aplica la metodología denominada COBIT.

1. Dominio: PO - Planeacion y organización:

PO2 - Definición de la arquitectura de información:

2.1. Modelo de la arquitectura de información.

2.2. Diccionario de datos y reglas de sintaxis de datos de la corporación.

2.3. Esquema de clasificación de datos.

2.4. Niveles de seguridad.

PO8 Aseguramiento del cumplimiento de requerimientos externos:

8.1. Revisión de requerimientos externos.

8.2. Prácticas y procedimientos para el cumplimiento de requerimientos externos.

8.3. Cumplimiento de los estándares de seguridad y ergonomía.

8.4. Privacidad, propiedad intelectual y flujo de datos.

8.5. Comercio electrónico.

8.6. Cumplimiento con los Contratos de Seguros.

PO9 - Evaluación de riesgos:

9.1. Evaluación del riesgo del negocio.

9.2. Enfoque de evaluación de riesgos.

9.3. Identificación de riesgos.

9.4. Medición de riesgos.

9.5. Plan de acción contra riesgos.

9.6. Aceptación de riesgos.

PO11- Administración de calidad:

11.1. Plan general de calidad.

11.2. Enfoque de aseguramiento de calidad.

11.3. Planeación del aseguramiento de calidad.

11.4. Revisión del aseguramiento de calidad sobre el cumplimiento de estándares y procedimientos de TI.

11.5. Metodología del ciclo de vida de desarrollo de sistemas.

11.6. Metodología del ciclo de vida de desarrollo de sistemas para cambios mayores a la tecnología actual.

11.7. Actualización de la metodología del ciclo de vida de desarrollo de sistemas.

11.8. Coordinación y comunicación.

11.9. Marco referencial de adquisición y mantenimiento para la infraestructura de tecnología.

11.10. Relaciones con terceras partes como implementadores.

11.11. Estándares para la documentación de programas.

11.12. Estándares para pruebas de programas.

11.14. Pruebas piloto/paralelo.

11.15. Documentación de las pruebas del sistema.

11.16. Evaluación del aseguramiento de la calidad sobre el cumplimiento de estándares de desarrollo.

11.17. Revisión del aseguramiento de calidad sobre el logro de los objetivos de la función de servicios de información.

11.18. Métricas de Calidad.

11.19. Reportes de revisión de aseguramiento de calidad.

2. Dominio: AI - Adquisición e implementación

AI2 - Adquisición y mantenimiento de software de aplicación:

2.3. Aprobación del diseño.

2.4. Definición y documentación de requerimientos de archivos.

2.6. Diseño para la recopilación de datos fuente.

2.7. Definición y documentación de requerimientos de entrada de datos.

2.8. Definición de interfaces.

2.9. Interfase usuario-máquina.

2.10. Definición y documentación de requerimientos de procesamiento.

2.11. Definición y documentación de requerimientos de salida de datos.

2.12. Controlabilidad.

2.13. Disponibilidad como factor clave de diseño.

2.14. Consideraciones de integridad de tecnología para software de programas de aplicación.

2.15. Pruebas de software de aplicación.

AI5 - Instalación y acreditación de sistemas:

5.1. Entrenamiento.

5.2. Adecuación del desempeño del software de aplicación.

5.4. Pruebas de cambios.

5.5. Criterios y desempeño de pruebas en paralelo/ piloto.

5.6. Prueba de aceptación final.

5.8. Prueba operacional.

5.9. Paso a producción.

5.10. Evaluación de la satisfacción de los requerimientos del usuario.

5.11. Revisión gerencial post – implementación.

AI6 - Administración de cambios:

6.2. Evaluación del impacto.

6.3. Control de cambios.

6.4. Documentación y procedimientos.

6.5. Mantenimiento Autorizado.

3 Dominio: DS - Entrega de servicios y soporte

DS2 - Administración de servicios prestados por terceros:

2.1. Interfases con proveedores.

2.2. Relaciones de dueños.

2.3. Contratos con terceros.

2.4. Calificación de terceros.

2.6. Continuidad de servicios.

2.7. Relaciones de seguridad.

2.8. Monitoreo.

DS3 - Administración de desempeño y capacidad:

3.1. Requerimientos de disponibilidad y desempeño.

3.2. Plan de disponibilidad.

3.3. Monitoreo y reporte.

3.4. Herramientas de modelado.

3.5. Manejo Proactivo del desempeño.

3.6. Pronóstico de carga de trabajo.

3.8. Disponibilidad de recursos.

DS5 - Garantizar la seguridad de sistemas:

5.1. Administrar medidas de seguridad.

5.2. Identificación, autenticación y acceso.

5.3. Seguridad de acceso a datos en línea.

5.4. Administración de cuentas de usuario.

5.5. Revisión gerencial de cuentas de usuario.

5.6. Control de usuarios sobre cuentas de usuario.

5.7. Vigilancia de seguridad.

5.8. Clasificación de datos.

5.9. Clasificación de datos.

5.10. Reportes de violación y de actividades de seguridad.

5.11. Manejo de incidentes.

5.14. Autorización de transacciones.

5.16. Sendero seguro.

5.17. Protección de funciones de seguridad.

5.19. Prevención, detección y corrección de software “malicioso”.

5.20. Arquitectura de firewalls y conexión a redes públicas.

5.21. Protección de valores electrónicos.

DS7 - Educación Y Entrenamiento De Usuarios:

7.1. Identificación de necesidades de entrenamiento.

7.2. Organización del entrenamiento.

7.3. Entrenamiento sobre principios y conciencia de seguridad.

DS9 - Administración de la configuración:

9.1. Registro de la configuración.

9.2. Configuración base.

9.3. Registro de estatus.

9.4. Control de la configuración.

9.5. Software no autorizado.

9.6. Almacenamiento de software.

4. Dominio: M - Monitoreo

M2 - Evaluar lo adecuado del control interno:

2.1. Monitoreo de control interno.

2.2. Operación oportuna de controles internos.

2.4. Seguridad de operación y aseguramiento de control interno.

5.6. HALLAZGOS Y RECOMENDACIONES DE LA AUDITORÍA

1. Dominio: PO - Planeacion y organización

PO2 - Definición de la arquitectura de información

1. Hallazgo: No existe la elaboración formal e integral de un Manual de sistemas (Técnico), por parte de la empresa SYAC para el área de sistemas del hospital universitario departamental de Nariño, se ha encontrado que solo se cuenta con un manual básico sobre la configuración del módulo, y algunos documentos referenciales a capacitaciones sobre el soporte del mismo, igualmente se evidencia que esta documentación no se encuentra actualizada y varia de acuerdo a la ultima versión del módulo que va sujeta a las continuas actualizaciones que se han realizado al sistema dinámica gerencial.

Recomendación: Se recomienda que la empresa SYAC, desarrolle y documente el manual de sistema de dinámica gerencial, donde se haga una descripción muy detalla de las características física y técnicas de cada elemento del módulo de historia clínica.

El manual debe contener:

1. Índice de relación de los capítulos y páginas correspondientes que forman parte del documento.

2. Introducción: Se debe presentar una breve descripción del sistema desarrollado, que contemple el ámbito abarcado, cual es su función principal y un detalle de las funciones macros o partes que lo componen.

2.1. Objetivo general del sistema.

2.2. Objetivos específicos.

3. Contenido técnico.

3.1. Definición de reglas del negocio implementadas en el sistema desarrollado.

3.2. Configuración del módulo (parámetros y requerimientos).

3.3. Diagramas de flujo de datos, junto con su respectivo diccionario de datos.

3.4. Controles de auditoria implementados en el sistema.

3.5. Descripción de campos requeridos por pantalla con presentación de pantallas.

3.6. Diagrama de navegación y configuración del sistema.

3.7. Requerimientos de interfases con otros sistemas.

3.8. Modelo lógico de datos, diagrama entidad-relación.

3.9. Modelo de datos físico.

3.10. Matriz de procesos de la institución.

3.11. Matriz de programas versus entidades.

3.12. Plataforma de usuario: Indica los requerimientos mínimos de hardware y software para que el sistema se pueda instalar y ejecutar correctamente.

3.13. Áreas de aplicación y/o alcance de los procedimientos. Esfera de acción que cubren los procedimientos (entradas procesos y salidas).

4. Responsables.

4.1. Mapa de navegación: Muestra a través de diagramas de flujos, la interconexión entre cada una de las pantallas del sistema, lo que serviría para saber como llegar a una determinada parte de la aplicación, detallando los menús, submenús y donde nos lleva cada uno.

4.2. Descripción gráfica del mapa de navegación: muestra el mapa de navegación representado con las pantallas del módulo de historia clínica.

4.3. Descripción paso a paso de los procesos, así como pantallas, botones, cuadros de texto, etc., igualmente indicar el código base de cada rutina, pantalla, botón, etc.

2. Hallazgo: En el diccionario de datos no existe la descripción del personal encargado de hacer el mantenimiento del mismo, de igual forma no todo el personal del área de sistemas conoce este diccionario.

El diccionario de datos no describe la clasificación de usuarios, niveles de acceso y restricciones, como tampoco se especifican los roles y privilegios de los usuarios.

Recomendación: Se recomienda que la empresa SYAC informe y de a conocer a todo el personal de área de información y sistemas el diccionario de datos del módulo de historia clínica, igualmente se hace necesario, complementar el diccionario de datos con la especificación de:

- Descripción detallada del personal encargado de mantener actualizado el diccionario de datos.
- Clasificación de los tipos de usuarios, cuales son los niveles de acceso y las restricciones para el ingreso de los mismos.
- Descripción de los roles de los diferentes usuarios y sus privilegios, en el módulo de historia clínica.

3. Hallazgo: No se ha diseñado formalmente un modelo de arquitectura de información por parte de la empresa SYAC, para ser entregado al área de información y sistemas del hospital, es necesario que el personal de esta área conozca profundamente todos los componentes del módulo, ya que ellos serán los encargados de brindar el soporte requerido cuando el módulo se encuentre en producción total.

Recomendación: Se recomienda que la empresa SYAC, presente la documentación sobre el modelo de arquitectura de información, la socialice con el personal de área de sistemas y especifique su enfoque.
El modelo de arquitectura de información debe contener:

- Identificación de entradas.
- Identificación de procesos.
- Identificación de sitios de almacenamiento (base de datos).
- Identificación de reportes.
- Identificación de la interacción con otros sistemas.

- Diseño de interacción de los elementos e identidades del módulo.
- Definición de usuarios finales.
- Requerimientos del hospital.
- Planes de la gerencia a corto y largo plazo.
- Costos, riesgos y aprobaciones para hacer modificaciones al modelo.
- Cambios realizados al módulo.

4. Hallazgo: Se ha realizado una clasificación de los datos, pero es necesario mejorar este modelo, ya que no se ha tenido en cuenta algunos factores que garantizan un esquema de seguridad.

Recomendación: Se recomienda que dentro del área de información y sistemas se establezcan políticas sobre la clasificación de los datos que garantice:

- Niveles de seguridad definidos para cada clasificación de datos.
- Niveles de acceso definidos y apropiados para la clasificación de los datos.

También es necesario que dentro del modelo de clasificación de los datos se tengan en cuenta los siguientes criterios:

- Categorías de seguridad.
- Propiedad de los datos.
    - Datos públicos.
    - Datos Privados.
    - Datos Secretos.
- Estándares de clasificación “default”, para los activos de datos que no contienen un identificador de clasificación

PO8 - Asegurar el cumplimiento de los requerimientos externos

5. Hallazgo: Las normas ergonomía y seguridad incluyen:

- Dar a conocer al personal de sistemas y asistencial relacionado con el módulo, el programa de ergonomía y seguridad.

- Explicar a los usuarios finales del módulo y el recurso humano del área de información y sistemas, cuales son las situaciones correctas de ergonomía y seguridad.
- Realizar periódicamente capacitaciones para la prevención de riesgos.

Pero estas actividades van orientadas al personal de Nomina, no se incluye personal de cooperativas y el personal nuevo.

La dotación de elementos de trabajos ergonómicos al personal del área de sistemas y asistencial es mínimo.

No se ha capacitado al personal de sistemas, encargado de la instalación de equipos en los diferentes puestos de trabajo de los médicos y enfermeras, acerca de las condiciones correctas ergonómicas.

Recomendación: Se recomienda que las actividades relacionadas con los aspectos de salud ocupacional sean realizadas periódicamente con todo el personal que se desenvuelve en el área de sistemas y los usuarios finales del módulo, igualmente se recomienda exigir la asistencia del personal convocado a capacitaciones por parte de la Coordinación del área de Salud Ocupacional.

Se recomienda utilizar mejores estrategias de comunicación de la realización de las actividades de salud ocupacional, por ejemplo la entrega oportuna de oficios a todo el recurso humano involucrado, informando la realización de estas actividades estipulando fecha, hora, tema y responsable.

Se recomienda que dentro del programa de ergonomía se incluyan aspectos relacionados con la capacitación de las personas encargadas de la instalación y adecuación de los equipos de cómputo y de red, para los usuarios del módulo de historia clínica como los médicos y enfermeras entre otros.

Se recomienda mejorar y dotar elementos de trabajo que cumplan con los lineamientos de seguridad y ergonomía.

6. Hallazgo: Existe la definición de algunas políticas en relación a la seguridad de la información del hospital, pero en ellas no se han tenido en cuenta aspectos relacionados con los usuarios, la gestión de la información, supervisión de usuarios, claves, políticas para garantizar la seguridad de la información que indiquen cual es el correcto manejo de las tecnologías de información, por parte de los médicos y enfermeras.

Recomendación: Se recomienda que dentro de las políticas de seguridad en el hospital se incluya la definición de:

- Normas relacionadas con el flujo de datos entre las áreas que interactúan con el módulo.
- Políticas relacionadas con la administración del sistema.
- Clasificación de datos de acuerdo a niveles de Importancia y confidencialidad.
- Administración de usuarios sobre los recursos como: correo electrónico, Chat, contraseñas, descarga de archivos, instalación de aplicaciones, instalación de otros dispositivos en el PC, uso de la Internet e intranet, cuentas de usuarios.

7. Hallazgo: Existen contratos en relación al aseguramiento del software pero no se han definido políticas sobre su cobertura, y no existe claridad de los aspectos que incluye el seguro, por parte de control interno y la coordinación del área de información y sistemas, es de vital importancia que las instituciones de salud cuenten con seguros, pues existen situaciones adversas que pueden poner en peligro los sistemas y la información como robos, incendios, atentados entre otros.

Recomendación: Se recomienda establecer lineamientos y normas relacionados con el cubrimiento de las aseguradoras y verificar que se incluyan:

- Riesgos ocasionados por terremotos, lluvias, terrorismo, entre otros desastres.
- Robo, lucro cesante.
- Deshonestidad, desaparición y destrucción.
- Responsabilidad civil.
- Transporte.

(PO9) - Evaluación de riesgos

8. Hallazgo: No existen la definición de políticas y procedimientos en relación a la evaluación de riesgos en el módulo de historia clínica.

Existe un marco de referencia usado por las áreas de control interno y calidad que es el “MECI” para la administración de riesgos, pero el enfoque no ha sido implementado en el área de información y sistemas.

No se hace una gestión de riesgos.

Recomendación: Se recomienda que las oficinas de sistemas y de control interno, presenten un programa enfocado al área de información y sistemas, donde se sugiera la cobertura de las actividades relacionadas en el “MECI”, de acuerdo a sus 3 Subsistemas que son:

1. Control Interno.
2. Control de Gestión.
3. Control de Evaluación.

Y se incluyan los siguientes aspectos:

- Mantenimiento de hardware y de red.
- Manejo del usuario de sus recursos de software y hardware.
- Cambios en los requerimientos de usuarios.

- Cambios de requerimientos externos.
- Medidas de seguridad para usuarios.
- Seguimiento a incidentes ocurridos anteriormente.
- Gestión de riesgos.

También se recomienda realizar periódicamente una evaluación de riesgos, con el fin de tomar las medidas correctivas para eliminarlos o disminuirlos, esta evaluación debe ser registrada en un documento que permita mostrar el seguimiento que se le ha hecho a las personas responsables, en la documentación se debe registrar:

- Fecha de revisión.
- Responsable.
- Módulo analizado.
- Proceso afectado.
- Riesgo identificado.
- Veces que se ha presentado el riesgo.
- Nivel de riesgo.
- Controles aplicables y correctivos sugeridos.

9. Hallazgo: No existe un plan de acción contra riesgos, los riesgos no han sido categorizados.

Recomendación: Se recomienda que se utilice un análisis cualitativo, que permita clasificar los riesgos de acuerdo a su nivel de importancia e impacto en el sistema de información, analizando su equivalencia con el factor económico representativo para el hospital y teniendo en cuenta los planes a corto y largo plazo del mismo.

Se recomienda que se establezcan controles a nivel de:

- Procesamiento.
- Tecnología.
- Actividad Humana

- De acuerdo a la ISO 27001 A.10.4 se exige la implementación de controles de Software malicioso.
- De acuerdo a la ISO 27001 A.10.8.4 se exige que la información “que hace parte de mensajes electrónicos debe tener la protección apropiada”, es decir halla un control sobre los usuarios y la información que manipulan.

10. Hallazgo: No se ha realizado un proceso informativo y de toma de conciencia de la evaluación de riesgos, al personal del área de sistemas, sobre el desempeño y funcionamiento de las tecnologías de información.

Recomendación: Se recomienda a los responsables de la gestión de riesgos realizar: actividades, reuniones y planes junto al recurso humano involucrado, con el fin de asignar responsabilidades, y comunicar cual es el programa para la identificación, evaluación, seguimiento y establecimiento de controles contra los riesgos relacionados con las tecnologías de información.

(PO11) - Administración de calidad

11. Hallazgo: Existe un plan de calida pero en relación a las tecnologías de información no se especifican aspectos como: la infraestructura de información o instalaciones requeridas para soportar los sistemas implementados, y el entrenamiento requerido para desarrollar y soportar el ambiente de las tecnologías de información.

Recomendación: Se recomienda que dentro del plan de calidad del área de información y sistemas, se incluyan los aspectos relacionados con:

- La infraestructura de información requerida para soportar los sistemas e interfases.
- El entrenamiento requerido para desarrollar y soportar el ambiente de TI escogido como objetivo, con el fin de determinar si los paquetes de

software comercial adquiridos con la empresa SYAC, satisfacen las necesidades del hospital en el proceso de acreditación.

También se debe tener en cuenta que el plan de calidad debe permitir a la institución que:

- Las políticas de calidad, los procedimientos y los requisitos de la organización, sean conocidas por todo el recurso humano de la misma.
- Describir e implementar un sistema de calidad eficaz.
- Suministrar control adecuado de las prácticas y facilitar las actividades de aseguramiento.
- Suministrar las bases documentales para las auditorias.
- Adiestrar al personal en los requisitos del sistema de calidad.

12. Hallazgo: Existe el enfoque de aseguramiento de calidad que es el "estándar de la gerencia de la información " el cual va dirigido a 8 grandes objetivos estratégicos, pero se deben incluir procesos en relación a los requerimientos externos, revisiones periódicas, y debe ser comunicado o formalizado ante el personal del área de información y sistemas.

Recomendación: Se recomienda que en el enfoque de aseguramiento de calidad se incluyan:

- Especificaciones sobre las revisiones o auditorias.
- Revisiones de post-implementación de las versiones del módulo, para verificar si va de acuerdo al ciclo de vida usado en versiones anteriores.
- Revisión del cumplimiento de los requerimientos nuevos del hospital para historias clínicas.
- Recomendaciones a las que se les hace seguimiento periódicamente y que son reportadas al personal administrativo encargado de la toma de decisiones del hospital.

Se recomienda que se tenga en cuenta los ítems de la ISO 27001 sobre: 4.3 documentación, 4.3.2. Control de documentos, 4.3.3. registros para el plan de calidad.

13. Hallazgo: Dentro del ciclo de vida de desarrollo de sistemas definido para el HUDN, se encontró que:

- Tiene poca documentación.
- No cuenta con diagramas de flujo de los procesos del sistema de información.
- No ha sido comunicado formalmente al personal del área de información y sistemas.

Recomendación: Se recomienda que dentro de la documentación relacionada con el ciclo de vida de desarrollo de sistemas para la institución se incluya:

- Especificación de los controles suficientes durante el proceso de desarrollo para sistemas y tecnologías nuevas.
- Una comunicación con todos los empleados involucrados en el desarrollo y mantenimiento de sistemas.
- Que se utilicen procedimientos para los cambios tecnológicos.
- Que se utilicen procedimientos para asegurar la aceptación y aprobación de los usuarios.
- Diagramas de flujos de la programación si es posible o de lo contrario del funcionamiento lógico de los diferentes módulos del sistema implementado en la institución.

2. Dominio: AI - Adquisición e Implementación

(AI2) - Adquisición y Mantenimiento De Software De Aplicación

14. Hallazgo: Dentro del módulo de historia clínica no se cuenta con la opción de ayuda en línea, únicamente se ha incluido un link que carga el manual de usuario, donde esta especificado el diligenciamiento general de los diferentes componentes del módulo, dentro del manual hace falta especificar la información sobre la gestión de las interfases de las historias clínicas de las áreas de urgencia y especialidades.

Recomendación: Se recomienda que la empresa SYAC, desarrolle e incluya dentro del sistema de información, una ayuda para el usuario donde se brinde una información completa no solo de las opciones de:

- Archivo
- Procesos
- Reportes
- Utilidades

Si no también se incluya el manejo de las interfases de las diferentes historias clínicas de urgencias y especialidades, que fueron desarrolladas por parte de los técnicos del hospital.

Alternativamente se recomienda elaborar una verdadera ayuda en línea para los usuarios, en donde se incluya un buscador ya sea por palabra, tema, sección o procedimiento, que indique el manejo de las interfases, los procesos, las herramientas y funciones que ofrece el módulo de historia clínica.

15. Hallazgo: Dentro de la opción de parametrización del módulo de historia clínica, al realizar una determinada configuración, se ha encontrado que no se están cumpliendo las validaciones configuradas, en relación a la opción de diagnostico por edades.

Recomendación: Se recomienda que el hospital solicite a SYAC, la revisión y corrección de la parametrización del módulo en la parte de diagnostico por edades.

16. Hallazgo: Dentro de la documentación de la metodología del ciclo de vida no se habla sobre aspectos como:

- Importancia de la comunicación entre los usuarios (médicos y enfermeras) y los diseñadores de las historias clínicas.
- Mecanismos adecuados para la recopilación de requerimientos de control interno y seguridad.

Recomendación:

Se recomienda que se establezcan funciones, que se delimiten bien las fechas de entrega, las actividades y mecanismos a utilizar para el proceso de diseños de historias clínicas y la implantación del módulo en las diferentes áreas (triage, urgencias, hospitalización y consulta externa). Esto con el fin de exista una organización y armonía entre todo el personal involucrado en este proceso.

17. Hallazgo:

No existe el planteamiento de un plan de pruebas a realizarse en el proceso de implantación del módulo de historia clínica.

Recomendación:

Se recomienda definir políticas que garanticen la correcta elaboración de un plan de pruebas aplicables, en los procesos de implantación del módulo de historia clínica de sistema dinámica gerencial, como también en futuras actualizaciones.

Se recomienda que el plan de pruebas contenga:

1. Objetivo del plan de pruebas.
2. Tipo de pruebas.
2.1. Tiempo de duración de la prueba.
2.2. Pruebas Unitarias: Estas pruebas servirán para probar que cada componente realiza adecuadamente el propósito para el que fue concebido.
2.3. Pruebas Integrales: Estas pruebas servirán para probar que cada componente se interconecta adecuadamente con los componentes que interactúa.
2.4. Pruebas de sistema: Estas pruebas servirán para probar que cada Caso de Uso se integra apropiadamente en cadenas de ejecución de procesos del negocio.

2.5. Pruebas de Aceptación: Estas pruebas servirán para demostrar al Cliente que el producto satisface los requerimientos para los Casos de Prueba seleccionados.
2.6. Pruebas para validación de campos y opciones.
2.7. Pruebas prototipo y paralelo.

(AI5) - Instalación y Acreditación De Sistemas

18. Hallazgo:

La metodología formal del ciclo de vida de desarrollo no incluye pruebas de acreditación, de seguridad y capacitación del recurso humano, seguimiento de operaciones de implementación.

Recomendación:

Se recomienda que dentro de la metodología del ciclo de vida de desarrollo de sistemas se incluya:

- Entrenamiento a ingenieros a cargo del módulo de historia clínica.
- Pruebas del módulo.
- Pruebas prototipo, paralelo y post-implementación.
- Pruebas de acreditación y seguridad.
- Controles de cambio.

19. Hallazgo:

Se realizan capacitaciones para el personal de área de sistemas, pero no se cuenta con un programa de entrenamiento formal, que permita determinar si estas son lo suficientemente estructuradas.

En el análisis sobre las capacitaciones realizadas se evidencia que no han tratado los temas de:

- Diferencias del módulo de historia clínica, con otros módulos del sistema dinámica gerencial.
- Errores y corrección de errores.

Recomendación: Teniendo en cuenta que dentro del proceso de instalación y acreditación de sistemas, se hace necesario que los técnicos tengan un completo manejo y conocimiento del módulo de historia clínica, se requiere que se diseñe un programa formal de entrenamiento para el personal del área de sistemas, que sea socializado y que incluya:

- Capacitación en relación a las diferencias del módulo de historia clínica, con otros módulos del sistema dinámica gerencial.
- Gestión de errores, en relación a los posibles errores y las estrategias o metodologías para la corrección de estos errores.

(AI6) - Administración De Cambios

20. Hallazgo: Dentro del estándar gerencia de la información, hace falta incluir un lineamiento relacionado con el seguimiento y control de cambios en los sistemas de información implantados.

Recomendación: Se recomienda que dentro del estándar Gerencia de la información, se incluya un lineamiento que garantice el establecimiento de procesos y funciones para el personal del área de sistemas, en relación a la administración de los cambios en el sistema, es importante resaltar que dinámica gerencial es un sistema Integral, donde se esta migrado toda su funcionalidad al lenguaje .NET, y por tal razón se están realizando constantes actualizaciones que implican cambios no solo en el módulo de historia clínica si no también en los demás módulos, por tal razón y en vista de las constantes actualizaciones se determina que es de gran importancia llevar un control sobre los cambios realizados a cada versión.

21. Hallazgo: A pesar de que existe una plataforma por parte de la empresa SYAC, para llevar un registro de los cambios solicitados por el hospital a esta empresa, es necesario que como proceso independiente el área de información y sistemas establezca una guía formal donde se especifique como hacer el seguimiento a los cambios, no solo de los que son solicitados a SYAC, si no

también de los cambios observados en cada actualización de dinámica gerencial.

Recomendación: Se recomienda establecer un procedimiento o guía a seguir para llevar continuamente el registro de los cambios realizados en el módulo de historia clínica, ya sea por solicitud por parte del hospital a SYAC, como también para registrar los cambios que se observan cuando se realiza una actualización del sistema dinámica gerencial, esto con el fin principal de conocer con profundidad el módulo, verificar si los cambios son necesarios y si realmente son un beneficio para el módulo o por el contrario a desmejorado su rendimiento.

Este registro debe contener:

- Fecha de observación del cambio, día de actualización.
- Numero de cambio.
- Numero de actualización, (No versión).
- Detalle de Cambio: Se especifica el cambio observado en comparación con el estado anterior.
- Sección o Interfaz: Se discrimina la interfaz en la que ha realizado el cambio, si es un proceso se especifica su ubicación grafica, en el módulo.
- Estado: Se refiere a si se encuentra en funcionamiento optimo, medio o bajo.
- Observaciones: En caso de que exista alguna implicación con el cambio realizado.

Para la solicitud de cambios se debe llevar adicionalmente los siguientes registros:

- Fecha del cambio solicitado.
- Persona(s) que lo solicitan.
- Solicitud aprobada de cambios.

- Aprobación del cambio realizado - función de servicios de información.
- Aprobación del cambio realizado – usuarios.
- Fecha de actualización de documentación.
- Fecha de paso a producción.
- Aprobación del cambio por parte de aseguramiento de la calidad.
- Aceptación por parte de operaciones.

(DS2) – Entrega de Servicios y Soporte

Para este Dominio se analizaron los procesos referentes a:

DS2: Administración de servicios prestados por terceros

DS3: Administración de desempeño y capacidad

DS5: Garantizar la seguridad de sistemas

DS7: Educación y entrenamiento de usuarios

DS9: Administración de la configuración

22. Hallazgo: Dentro del contrato OJ006-2008 no se incluye el plan de contingencia para garantizar la continuidad del proyecto, no se especifica los programas a desarrollar por parte de SYAC y no hace referencia a las pruebas de aceptación al módulo de historias clinicas.Net.

Recomendación: En las empresas, en la protección de la información intervienen diferentes disciplinas, desde la informática, la gerencial, la logística, la matemática hasta la jurídica, entre muchas otras, que deben ser tenidas en cuenta por la oficina jurídica para garantizar que al interior de la organización se estipule todos los aspectos que rodean el sistema de información que se va ha implementar.

23. Hallazgo: Dentro del contrato de compra – venta OJ006-2008 adquisición de módulos de actualización, mantenimiento y soporte entre el hospital universitario departamental de Nariño E.S.E y la empresa SYAC (sistemas y asesorías de Colombia LTDA), no se hace relación a la protección de datos.

Recomendación: La ISO 27 001 es una herramienta de gestión estratégica que conduce a lograr la protección de la información, bien en un contexto en el cual la empresa pretenda alcanzar una certificación, o bien que sólo pretenda incorporar buenas prácticas de seguridad de la información, no sólo en sus procesos internos, sino también en sus procesos externos.

El no dotar a las bases de datos personales de la seguridad y medidas de protección adecuadas por parte de las organizaciones que las poseen, en primer lugar implica un desconocimiento de lo dispuesto en la norma ISO 27001; segundo, la violación a un derecho constitucional, el cual puede ser garantizado a través de acciones de tutela, con el riesgo de indemnizar los perjuicios causados; tercero, es una limitante en el comercio internacional, pues los países europeos y algunos latinoamericanos impiden la transferencia internacional de datos con países o empresas que no garanticen un nivel adecuado de protección de datos y las sanciones que tienden a imponerse.

24. Hallazgo: Dentro del contrato de compra – venta OJO006-2008 adquisición de módulos de actualización, mantenimiento y soporte entre el hospital universitario departamental de Nariño E.S.E y la empresa SYAC (sistemas y asesorías de Colombia LTDA), no se hace relación a la protección de datos, no se especifica el acceso al código fuente de la aplicación en caso de que el proveedor desaparezca del mercado, como se estipula en el dominio de la norma ISO 27001.

Recomendación: Como la legislación contempla dentro de contratación informática, la voluntad de las partes, se recomienda que dentro del contrato de compra –venta OJ006-2008 se integre a sus cláusulas, el acceso al código fuente de la aplicación de dinámica gerencial en el caso fortuito que la compañía deje de existir.
En términos de contratos de licencia de uso sobre aplicaciones informáticas normalmente media, la entrega de la correspondiente licencia y del ejecutable que permite la instalación de sistema de información.

25. Hallazgo: No existen políticas al interior del hospital universitario departamental relacionado con el comercio electrónico, ni estándares de encriptación, las políticas de seguridad se basan solo en proceso de realizar copias de seguridad a la información dentro de la institución. Esto se puede asegurar por la entrevista sostenida con el coordinador del Área de sistemas y el análisis de los procesos que se llevan al interior del área.

Recomendación: Se recomienda al área de información y sistemas del hospital universitario departamental de Nariño construir un documento formal que garantice la seguridad de la información.

La política de seguridad es una herramienta de gran valor para enfrentar el Plan de seguridad de una instalación y debe entenderse como un proceso integral que parte de la situación real y se construye teniendo en cuenta los recursos y riesgos a que está expuesta la organización, convirtiéndola en una guía de operación y actuación para proteger los activos y garantizar la continuidad y calidad de los servicios. Es indispensable que la política de seguridad que se implemente en el hospital universitario departamental de Nariño tenga dos propósitos centrales:

- Informar a todos los usuarios sobre las obligaciones que deben asumir respecto a la seguridad asociada a los recursos de tecnología de información.
- Dar las guías o exponer los controles y criterios al personal de la institución para actuar ante posibles amenazas y problemas presentados.

Esta política debe involucrar a los diferentes sectores de la organización:

- Alta gerencia.
- Responsables de tecnologías de información.
- Encargados de la seguridad.
- Auditores.
- Coordinadores de las dependencias y los usuarios.

El documento formal debe definir elementos asociados a la adquisición de hardware, software, y contratación de servicios externos.

Las políticas de seguridad de la información es el conjunto de normas, reglas, procedimientos y prácticas, que regulan la protección de la información contra la pérdida de confidencialidad, integridad y disponibilidad, tanto en forma accidental como intencionada. El hospital a través de la coordinación de sistemas, debe adoptar los mecanismos que le permitan el resguardo, confiabilidad y oportunidad de su información.

6. INFORME EJECUTIVO

En San Juan de Pasto, a los veinte días del mes de noviembre del dos mil ocho, las estudiantes del programa de ingeniería de sistemas de la universidad de Nariño, realizaron la auditoria al módulo de historia clínica electrónica en el sistema de información dinámica gerencial del hospital universitario departamental de Nariño, con miras a realizar una evaluación al desempeño y capacidad del módulo adquirido por la institución y que se encuentra en proceso de implantación e implementación, así como el cumplimiento de las normas y demás disposiciones que rigen actualmente para garantizar la seguridad informática al interior del hospital y compararlo con es estándar del Cobit que se usó para realizar esta auditoria y que son aplicables en los diferentes procesos, en el período comprendido entre el 1° de abril y el 20 de noviembre de 2008.

La auditoria utilizó las técnicas y normas de auditoria generalmente aceptadas lo cual proporciona una base razonable para fundamentar y emitir una opinión sobre la el desenvolvimiento del modulo al interior del hospital y el grado de aceptación de usuarios y personal profesional encargado del mismo así como el concepto sobre los beneficios y mejoras que trae el modulo y recomendaciones a tener en cuenta en aspectos identificados como debilidades que dándoles un enfoque apropiado contribuyen notablemente al mejoramiento del sistema y sus usuarios. Todo lo anterior, teniendo en cuenta los principios eficiencia, eficacia y equidad y el cumplimiento de las disposiciones legales, reglamentarias o internas aplicables en cada una de sus actuaciones.

Simultáneamente, el equipo auditor en el trabajo de campo confrontó y validó la información reportada por la entidad, en la documentación obtenida de la misma y a través de un proceso de observación y evaluación tanto a profesionales del área como a los usuarios finales involucrados en el módulo

de historia clínica. Los procesos evaluados en la auditoria al módulo de historia clínica electrónica fueron: el proceso de entrada, salida y procesamientos de datos del módulo de historia clínica .net, el cumplimiento de los requerimientos externo e internos, la infraestructura física, la seguridad física y lógica y recurso involucrado con el módulo, por ello se ha evidenciado debilidad en el establecimiento de políticas al interior del hospital universitario departamental de Nariño en cuanto a seguridad informática y protección de la información así como el uso y herramientas de las mismas, y en donde los usuarios sean capacitados en las tecnologías de información que adopta el hospital y al mismo tiempo se apropien del uso de ellas y garanticen el óptimo desempeño de las aplicaciones en las cuales desempeñan su labor diaria, estas políticas deben estar apoyadas en la actual legislación colombiana y los estándares creados para ello, igualmente es importante resaltar la implementación de procedimientos basados en el sistema de gestión de seguridad de la información a la que hace relación la ISO 27001. En términos generales el aplicativo dinámica gerencial y específicamente el Modulo de historia clínica electrónica que implementa el hospital departamental es una herramienta confiable y de gran valor para la entidad, porque brinda la agilidad en los procesos asistenciales e incremento en atención al cliente y calidad de servicio. Sin embargo es importante que las oficinas encargadas tanto de la seguridad lógica como de la contratación de tecnologías de información incorporen dentro de sus áreas, la afiliación de métodos, procedimientos y políticas tanto para el uso de estas tecnologías como para la compra de nuevos aplicativos informáticos, con el fin de que se cumplan los parámetros establecidos por los estándares y que al mismo tiempo se vea reflejado en el proceso de acreditación que adelanta el hospital universitario departamental y continúe en la línea de calidad y oportunidad en la atención y gestión de sus actividades.

Basados en los principios y mejoras continuas que rige el SGSI (sistema de gestión de seguridad de la información), de la norma ISO 27001 y el COBIT (Control Objectives for Information and related Technology), este documento de

auditoria de sistemas implementado en esta organización, busca mostrar los resultados finales de la auditoria finalizada el 30 de Octubre de 2008.

Este estudio se realizo con el objetivo de evaluar el proceso y el módulo de historia clínica electrónica, que garanticen la confiabilidad, integridad y seguridad permitiendo adelantar actividades de mejoramiento del sistema del hospital universitario departamental de Nariño.

De manera general los aspectos que se evaluaron en esta auditoria fueron: el proceso de entrada, procesamiento y salida de datos del módulo de historia clínica .NET, la seguridad física y lógica, la infraestructura física, el cumplimiento de los requerimientos del hospital en relación al módulo de historia clínica, el desempeño del módulo y papel del recurso humano involucrado con su gestión, se utilizo el enfoque del COBIT y los dominios utilizados fueron: planeacion y organización, adquisición e implementación, entrega de servicios y soporte y monitoreo, como también la norma ISO 27001 que evalúa en base a un (SGSI) sistema de gestión de seguridad de la información.

Para poder adquirir la información y buscar las evidencias se realizaron entrevistas, cuestionarios a las personas involucradas con el módulo, se reviso la infraestructura física, se recolectaron evidencias a través de un archivo fotográfico, se diseño un plan de pruebas para la auditoria, se reviso la documentación pertinente entre otras herramientas.

1. Hallazgo: No existe la elaboración formal e integral de un manual de sistemas (Técnico), por parte de la empresa SYAC para el área de sistemas del hospital universitario departamental de Nariño.
En el diccionario de datos no existe la descripción de los roles y privilegios de los usuarios, la clasificación de usuarios y los niveles de acceso, igualmente se evidencia que no existe una correspondencia total a la versión actual.

No se ha diseñado formalmente un modelo de arquitectura de información por parte de la empresa SYAC, para ser entregado al área de información y sistemas del hospital.

Recomendación: Se recomienda que la empresa SYAC, desarrolle y documente el Manual de sistema de dinámica gerencial, donde se haga una descripción muy detalla de las características física y técnicas de cada elemento del módulo de historia clínica.

Se recomienda que la empresa SYAC informe y de a conocer a todo el personal de área de información y sistemas el diccionario de datos del módulo de historia clínica, los actualice constantemente y complemente los datos de clasificación de usuarios y niveles de acceso.

Se recomienda que la empresa SYAC, presente la documentación sobre el modelo de arquitectura de información, la socialice con el personal de área de sistemas y especifique su enfoque.

2. Hallazgo: Se ha realizado una clasificación de los datos, pero es necesario mejorar este modelo, ya que no se ha tenido en cuenta algunos factores que garantizan un esquema de seguridad.

Recomendación: Se recomienda que dentro del área de información y sistemas se establezcan políticas que garanticen la implementación un modelo integral de clasificación de los datos.

3. Hallazgo: No existen la definición de políticas y procedimientos en relación a la evaluación de riesgos en el módulo de historia clínica y en general en relación al manejo de las tecnologías de información, con lo cual se evidencia que no se hace una gestión de riesgos.

Recomendación: Se recomienda que las oficinas de sistemas y de control interno, presenten un programa enfocado al área de información y sistemas, donde se sugiera como realizar la gestión de Riesgos.

4. Hallazgo: Dentro del estándar gerencia de la información hace falta definir lineamientos que garanticen que se haga la especificación de los requerimiento físicos y lógicos para soportar los sistemas implementados, capacitación idónea del recurso humano involucrado con estos procesos, cumplimiento de los requerimientos internos y externos, revisiones periódicas que deben ser comunicadas y formalizadas ante la gerencia.

Recomendación: Se recomienda que se incluyan en este estándar los aspectos relacionados con los requerimientos de los sistemas implementados y las revisiones o auditorias aplicables a los mismos.

5. Hallazgo: Dentro del módulo de historia clínica no se cuenta con la opción de ayuda en línea.

Recomendación: Se recomienda que la empresa SYAC, desarrolle una ayuda en línea para el usuario, donde se brinde una información completa e integral de la gestión del módulo de historia clínica.

6. Hallazgo: No existen la definición de políticas y procedimientos en relación a la administración de cambios en el módulo de historia clínica y en general en relación al manejo de las tecnologías de información, con lo cual se evidencia que no se hace una gestión de cambios.

Recomendación: Se recomienda que área de información y sistemas, defina los lineamientos o políticas que garanticen la implementación de procedimientos para el registro, identificación, clasificación, y establecimientos de controles sobre los cambios realizados en las tecnologías de información.

7. Hallazgo: Dentro del contrato OJ006-2008 no se incluye el plan de contingencia para garantizar la continuidad del proyecto, no se especifica los programas a desarrollar por parte de SYAC y no hace referencia a las pruebas de aceptación al módulo de historias clinicas.Net, así como no se hace referencia a la protección de los datos.

Recomendación: En las empresas, en la protección de la información intervienen diferentes disciplinas, desde la informática, la gerencial, la logística, la matemática hasta la jurídica, entre muchas otras, que deben ser tenidas en cuenta por la oficina jurídica para garantizar que al interior de la organización se estipule todos los aspectos que rodean el sistema de información que se va a implementar.

8. Hallazgo: No existen políticas al interior del hospital universitario departamental relacionado con el comercio electrónico, ni estándares de encriptación, las políticas de seguridad se basan solo en proceso de realizar copias de seguridad a la información dentro de la institución. Esto se puede asegurar por la entrevista sostenida con el coordinador del Área de sistemas y el análisis de los procesos que se llevan al interior del área.

Recomendación: Se recomienda al interior de la organización del hospital universitario departamental de Nariño construir un documento formal que incluya las políticas de seguridad, ya que esta es una herramienta de gran valor para enfrentar el Plan de seguridad de una instalación y debe entenderse como un proceso integral que parte de la situación real y se construye teniendo en cuenta los recursos y riesgos a que está expuesta la organización. Esta política debe ser de amplio conocimiento y contener las especificaciones básicas y criterios que se encaminan en las tecnologías de información.

CONCLUSIONES

Mediante el proceso de auditoria al módulo de historia clínica, se pudo realizar una evaluación critica, que permitió formar varios criterios y evidencias en relación a los aspectos a evaluar como lo son: el proceso de entrada, salida y procesamientos de datos del Módulo de historia clínica .NET, el cumplimiento de los requerimientos externo e internos, la infraestructura física, la seguridad física y lógica y recurso involucrado con el módulo, de tal forma que se pudieron establecer los controles y recomendaciones necesarios, los cuales se deberán cumplir con el fin de garantizar la confiabilidad, integridad y seguridad permitiendo adelantar actividades de mejoramiento del sistema del hospital universitario departamental de Nariño.

Se puede concluir que el proceso de entrada, procesamiento y salida de datos esta muy acorde con los requerimientos de la institución, y es necesario únicamente hacer algunas revisiones en la parte de procesamiento, en relación a las validaciones en la opción de parametrización que permite configurar el Módulo, puesto que no se cumplen la validaciones de diagnostico por edades.

En relación a la seguridad lógica se han observado grandes debilidades, debido a que hace falta definir políticas sobre la gestión de seguridad y la implementación de herramientas, procedimientos y controles que garanticen una correcta administración de la seguridad al nivel lógico, de lo contrario se evidencia que existen riesgos que pueden poner en peligro la integridad de la información de todo el sistema de información de la institución.

En relación a la infraestructura física y de red, se determina de que a pesar de que se observa el esfuerzo que esta haciendo la institución al migrar de categoría 5 a 6, es de vital importancia que los pisos 1, 2, y 4 se les de el mismos tratamiento que los pisos 3 y 5, pues se encuentran en mal estado, principalmente el cuarto de servidor, que por su papel e importancia debe ser

unos de los primeros en migrar a categoría 6, igualmente se observó que existen debilidades en el diseño de seguridad de la red lógica, puesto que es insegura y requiere la definición de políticas que garanticen mas seguridad en este aspecto.

Se presentó para cada proceso evaluado en los dominios: planeacion y organización, adquisición e implementación, entrega de servicios y soporte y monitoreo, los hallazgos y evidencias encontradas, paralelamente se planteo las recomendaciones respectivas, para esto se utilizo el fundamento conceptual de la norma ISO 27001, el enfoque del COBIT, y diferentes conceptos relacionados en esta investigación.

RECOMENDACIONES

Establecer políticas que garanticen la realización periódica de Auditorías a todos los módulos del sistema dinámica gerencial.

Mejorar el sistema de seguridad física y lógica planteando políticas de seguridad apoyadas en la legislación colombiana y los estándares creados para tal fin, igualmente se sugiere la implementación de procedimientos basados en el sistema de gestión de seguridad de la información en relación a la ISO 27001.

Mejorar las instalaciones de red y los cuartos de equipos, migrando a categoría 6.

Realizar procesos de capacitación a los usuarios de los diferentes módulos de dinámica gerencial, en donde puedan apropiarse de las tecnologías de información y la seguridad informática.

Realizar las pruebas de seguridad lógica de la red, en relación a mapeo de puertos, sniffer propios de redes inalámbricas, pruebas por inyección de SQL para acceso a la base de datos, e intrusiones al servidor, con el fin de encontrar las debilidades y poder sugerir e implementar los controles respectivos.

Apropiar al interior de la oficina de información y sistemas y especialmente del personal, de la política de equidad de la institución que se relaciona en el sistema de direccionamiento estratégico, ya que se observa que todo el personal del área de sistemas es un grupo cerrado a nuevas inclusiones de personal femenino, poco colaborador y cada uno se preocupa por el trabajo individual manteniendo actitudes oscas al momento de prestar servicios, esto puede ocasionar problemas en procesos de auditorias, revisiones,

capacitaciones y desarrollo de actividades propias de la institución, es importante que se implementen actividades de integración y convivencia del grupo que opera en la oficina de sistemas de tal forma que se mejore el ambiente laboral y se incremente sustancialmente el desempeño del área.

BIBLIOGRAFIA

ARENS, Alvin A. Auditoria un enfoque Integral. Prentice Hall. Mexico1996, 301.

CALDER, Alan. Nueve claves para el éxito – Una visión general de la implementación de la Norma NTC-ISO/IEC 27001. IT Governance Publishing, Reino Unido,125.

COMITÉ DIRECTIVO (24) DE COBIT Y EL IT GOVERNANCE INSTITUTE TMCOBIT. Directrices de auditoria.3 Edición, Julio 2000, 229.

GUERRERO, José. Guía para el Desarrollo del Proyecto de Grado. Bogota: UNAD. 1999, 30.

MCCLURE, Stuart. Secretos y soluciones para la seguridad de redes. Mc Graw Hill. España, 514.

HERRADOR ALCALDE, Teresa Carmen. Introducción a la auditoría Interna. Editorial Tirant Lo Blanch, 236.

BARRIO, José Vilar. La auditoría de los sistemas de gestión de la calidad. Fundación ConfeMetal editorial, 244.

SÁNCHEZ, Israel Osorio. Auditoria 1. Ediciones Fiscales Isef, S.A. México, 247.

HERNÁNDEZ HERNÁNDEZ, Enrique. Auditoria de Informática un enfoque metodológico y practico. Grupo Adneti. 2004, 249.

SOTOMAYOR, Alfonso Amador. Control Interno y Auditoria. Lazcano garza editores, 207.

RAY WHITTINGTON/KURT, Pany. Principios de auditoria 14ed. Mc Graw Hill Interamericana Editores S.A de C.V, 736.

SOLÍS MONTES, Gustavo Adolfo. Reingeniería en auditoria Informática. Editorial Trillas S.A. de C.V, 384.

MUÑOZ RAZO, Carlos. Auditoría en sistemas computacionales. Pearson education, 270.

RIVAS, Alonso. Auditoría informática. Mc Graw Hill. Madrid 1998. 187.

REVISTAS

CANO, J. Inseguridad Informática y Computación: Dos conceptos emergentes de la seguridad de la información. information system control journal. vol4.255.

OLLATILU, O. Identifity theft and coprporation´due diligence information system control journal. vol6. Pearson education. London, 315.

VELASCO MELO, Arean Hernando, Derecho informático y gestión de la seguridad de la información. Universidad del norte, 366.

BIBLIOWEB

Evolución del Control de Gestión, Publicado por Apuntes Total, http://admindeempresas.blogspot.com/2008/05/evolucion-del-control-de-gestion.html

Dr. Hugo Daniel CARRION (Abogado especialista en Derecho Penal), Auditoria Informática frente a un caso de espionaje informático dentro de una empresa, Fecha: 19 Enero 2002,

http://www.delitosinformaticos.com/propiedadindustrial/auditoría.shtml

http://www.escet.urjc.es/~ai/T1Apuntes.pdf

http://www.eici.ucm.cl/Academicos/ygomez/descargas/Auditoría.../AUDITORÍA%20Y%20SEGURIDAD%20DE%20SISTEM

NMAP, 14 octubre de 2008,
http://es.wikipedia.org/wiki/Nmap

Auditoria Informática
http://es.wikipedia.org/wiki/Auditor%C3%ADa_inform%C3%A1tica

http://espanol.geocities.com/audiconsystem/auditori.htm

http://www.eumed.net/libros/2005/lv/lv.doc

Francisco Javier Nava García, Apuntes de auditoria Informática,
http://www.escet.urjc.es/~ai/T1Apuntes.pdf

M.B.A Alice Naranjo, auditoria de sistemas
http://www.galeon.com/anaranjo/tipos_audi.htm

Tipos de auditoria de Mitecnologico.com,
http://www.mitecnologico.com/Main/TiposDeAuditoría

Mario Tamayo y Tamayo, Lunes, 20 de Octubre de 2008 a las 13:28
http://www.monografias.com/trabajos15/invest-cientifica/invest-cientifica.shtml

Conceptos de la Auditoría de sistemas
http://www.monografias.com/trabajos3/concepaudit/concepaudit.shtml

http://www.monografias.com/trabajos39/la-auditoría/la-auditoría.shtm

http://www.monografias.com/trabajos14/auditoría/auditoría.shtml

Leopoldo de la Fuente Silva, Jueves, 28 de Agosto de 2008 a las 19:41
http://www.monografias.com/trabajos7/inci/inci.shtml

http://www.oxid.it/cain.html

David Rivera Rodríguez, Conceptos Básicos del Proceso de Auditoria, Abril de 2005,
http://www.ocpr.gov.pr/educacion_y_prevencion/conferencias/adiest-audit-intern-gob-2005/audit-intern-municipios-2005/03-CONCEPTOS-BASICOS-AUDITORÍA.pdf

http://www.soeduc.cl/apuntes/papeles%20de%20trabajo%20(Caso%20practico).doc

http://web.bemarnet.es/seguridad.html

http://vtroger.blogspot.com/2005/11/cain-y-abel.html

ANEXOS

Galería fotografía, ver formato digital.