AUDITORIA AL SISTEMA DE INFORMACIÓN DINÁMICA GERENCIAL HOSPITALARIA EN EL MÓDULO DE CITAS MÉDICAS PARA EL HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO E.S.E

JAYDIVI CASTILLO GUERRERO
LYDA JOHANA CASTRO AGUAS
JOHANA MARCELA NARVAEZ ORDOÑEZ

UNIVERSIDAD DE NARIÑO
FACULTAD DE INGENIERÍA
PROGRAMA DE INGENIERÍA DE SISTEMAS
SAN JUAN DE PASTO
2013

AUDITORIA AL SISTEMA DE INFORMACIÓN DINÁMICA GERENCIAL HOSPITALARIA EN EL MÓDULO DE CITAS MÉDICAS PARA EL HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO E.S.E

JAYDIVI CASTILLO GUERRERO
LYDA JOHANA CASTRO AGUAS
JOHANA MARCELA NARVAEZ ORDOÑEZ

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

DIRECTORES:
ING. FRANCISCO NICOLAS SOLARTE SOLARTE
ING. JOSE JAVIER VILLALBA ROMERO

UNIVERSIDAD DE NARIÑO
FACULTAD DE INGENIERÍA
PROGRAMA DE INGENIERÍA DE SISTEMAS
SAN JUAN DE PASTO
2013

NOTA DE RESPONSABILIDAD

Las ideas y conclusiones aportadas en este Trabajo de Grado son responsabilidad de los autores.

Artículo 1 del Acuerdo No. 324 de octubre 11 de 1966, emanado del honorable Concejo Directivo de la Universidad de Nariño.

NOTA DE ACEPTACIÓN

_____

_____

_____

_____

JURADO

_____

JURADO

San Juan de Pasto, Noviembre de 2013

AGRADECIMIENTOS

A Dios y la Santísima Virgen María, por bendecirnos para llegar hasta donde hemos llegado y darnos la oportunidad de darle sentido a nuestra vida, de poner delante de nosotras muchas personas maravillosas que han sido un gran apoyo para lograr nuestras metas.

A nuestras familias y seres más queridos sus consejos, apoyo, ánimo y compañía en los momentos más difíciles y en los momentos de alegría fueron muy valiosos para seguir este camino.

A nuestro director, el Ingeniero Francisco Solarte su guía en este proceso hizo posible desarrollar este trabajo de manera satisfactoria.

Al Ingeniero Javier Villalba por sus valiosos aportes en el desarrollo de este trabajo de grado.

A todos los docentes de la Universidad de Nariño que sus conocimientos hicieron posible nuestra formación académica.

A nuestros amigos y compañeros con quienes compartimos el trabajo diario durante estos años y los mejores momentos vividos durante esta etapa como estudiantes de la Universidad de Nariño.

DEDICATORIAS

A Dios por ser siempre la luz en mi camino, por darme la sabiduría, la fuerza y la fortaleza para enfrentar, y culminar este reto con éxito a pesar de todas las dificultades.

A mis padres Florencia de Jesús Guerrero Biojo y Segundo Nemeas Castillo Granja por darme la vida e inculcarme buenos valores para ser la persona que soy y por brindarme la oportunidad de estudiar, por ser el apoyo constante e innegable en todo mi proceso de formación personal y profesional.

A todo mi familia y en especial a mis hermanos Jurany Jusely Armero Guerrero, Harold Arnovio Armero Guerrero, a mis sobrinos Johan Arley Armero Guerrero, Daniel Enrrique Riascos Armero y Luz Yaritza Quiñones Armero, por alentarme cada día para que siguiera adelante y no decayera en mi proceso de formación.

A mi tía Luz Elfrides Montaño Rincón por ser mi segunda madre, por brindarme su ayuda en aquellos momentos más difíciles y por ser mi refugio cuando más lo necesitaba, y por darme su apoyo incondicional e incomparable en este proceso.

Jaydivi Castillo Guerrero

A Dios y a la Virgen que me dan la oportunidad de despertarme cada mañana, por tenerme con salud y bienestar, por iluminar mi mente y corazón para terminar con mis estudios en la universidad.

A mi padre VICTOR MANUEL CASTRO PALERMO quien ha sido mi apoyo moral, y me ha ayudado a comprender muchas de mis cosas.

A mis dos madres MARIA ASENCION OBANDO AGUAS y LIBIA GENITH ANDRADE CORTES me llevan en todas sus oraciones y han dado todo lo que son y lo que tiene para que esté bien, y cumpla mis proyectos y sueños.

A MICHAEL JAIR ARIZALA QUIÑONES que ha estado en los buenos y malos momentos de mi vida brindándome todo su amor.

Y a todas las personas que de una u otra manera han formado parte en vida y en este proceso.

Lyda Johana Castro Aguas

A Dios porque su bondad infinita me dio esta oportunidad y la fortaleza para culminar mis estudios universitarios.

A nuestra Madre de los Cielos, porque su luz estuvo presente todos los días.

A mi madre MARIA EUGENIA ORDOÑEZ CAICEDO, sus sacrificios, su apoyo y sus consejos me dieron la fuerza para luchar cada día.

A mi abuela CARMELA CAICEDO DE ORDOÑEZ por su amor, su ayuda y la voluntad de colaborarme cada día.

A JUAN JOSE CALDERON SOLARTE por su comprensión y amor.

A todos aquellos que de alguna u otra manera respaldaron este proyecto de vida.

Y a quienes se han ido, y están presentes en mi corazón y que también me acompañaron en esta etapa de mi vida.

Johana Marcela Narváez Ordoñez

RESUMEN

La auditoría al Sistema de Información Dinámica Gerencial Hospitalaria en el módulo de citas médicas para el Hospital Universitario Departamental de Nariño E.S.E, es primordial para evaluar y mejorar los procesos que se llevan a cabo en esta área.

Se presenta la ejecución de una auditoria a la entidad antes mencionada en el módulo de citas médicas, con el fin de detectar debilidades en el área que pueden afectar negativamente a toda la organización, tomando como guía de trabajo COBIT (objetivo de control para la información y tecnologías relacionadas).

El desarrollo del trabajo parte de la descripción del problema encontrado en el hospital, definición de los objetivos y el alcance del proyecto, continuando con el marco teórico que muestra los conceptos claves que se manejan en las auditorias, en seguida se describe la metodología que se utilizó para desarrollar el trabajo a través de las fases de: conocimiento, planeación de la auditoria, ejecución y el informe final. Luego en el desarrollo del proyecto se muestran algunas características generales del Hospital Universitario Departamental de Nariño E.S.E. y del módulo de citas médicas, más adelante se encuentran el programa y el plan de auditoria, además de los formatos utilizados para registrar las actividades de evaluación al módulo y el resultado de la auditoria a través de los hallazgos encontrados en diferentes temas, junto con estas la aplicación de pruebas que respalden las debilidades encontradas y las recomendaciones para el mejoramiento de los procesos que se realizan en el área de citas médicas.

Para finalizar el proyecto se encuentra el informe gerencial y general que muestra un resumen de todos los hallazgos observados.

ABSTRACT

The audit to the information system dynamics hospital management in the module of medical appointment for Departmental University Hospital of Nariño E.S.E, is essential to evaluate and improve processes which are carried out in this area.

We present the implementation of an audit the aforementioned entity in the module of medical appointment, in order to detect weaknesses in the area that can negatively affect to the entire organization taking as a working guide Cobit (control objectives for information and related technology).

The development work starts with the description of the problem encountered in the hospital, defining the objectives and scope of the project, continuing with the theoretical framework showing the key concepts that are used in audits, we next describe the methodology used to develop the work through phases: knowledge, audit planning, execution and final report. Then in the project development are some general characteristics of the Departmental University Hospital of Nariño E.S.E, and of the module and appointments, later found the program and the audit plan as well as the formats used to record the activities of the module assessment and the result of the audit by the findings on different subjects, along with these the application of evidence supporting the weaknesses found and recommendations for improving the processes that take place in the area of medical appointments.

To finish the project is the general report and the managerial report, it shows a summary of all findings observed.

TABLA DE CONTENIDO

LISTA DE TABLAS

TABLA DE FIGURAS

GLOSARIO

Antecedentes: Acción, dicho o circunstancia anterior que sirve para juzgar hechos posteriores.

Audisis: Auditoría Integral y Seguridad de Sistemas de Información Ltda., es una firma de Auditores – Consultores Gerenciales, constituida legalmente el 23 de Septiembre de 1.988. Como Asesores - Consultores Gerenciales estamos siempre comprometidos con los valores éticos que garantizan la satisfacción de las necesidades de nuestros clientes con honestidad, objetividad, integridad, diligencia, confidencialidad, equidad y respeto por los derechos humanos.

Auditor: Una persona o empresa encargada de realizar un análisis independiente (auditoría) sobre el funcionamiento de una organización, para luego emitir su opinión.

Auditoria: Examen sistemático para determinar si los procesos de conocimiento están en acuerdo con lo pre establecido y su nivel de efectividad para el logro de los objetivos y metas. Dicho examen se hace por agentes internos o externos.

Autentificación de Usuario: Proceso que tiene por objetivo asegurar la identificación de una persona o sistema.

Causas: Aquello que se considera como fundamento u origen de algo.

Cobit: (Objetivos de Control de las Tecnologías de la Información y Tecnologías Relacionadas) Publicados y mantenidos por ISACA. Su misión es investigar, desarrollar, publicar y promover un conjunto de objetivos de control de Tecnología de Información rectores, actualizados, internacionales y generalmente aceptados para ser empleados por gerentes de empresas y auditores.

Copia de seguridad: Una copia de seguridad, copia de respaldo o backup (su nombre en inglés) en tecnologías de la información e informática es una copia de los datos originales que se realiza con el fin de disponer de un medio de recuperarlos en caso de su pérdida. Las copias de seguridad son útiles ante distintos eventos y usos: recuperar los sistemas informáticos y los datos de una catástrofe informática, natural o ataque; restaurar una pequeña cantidad de archivos que pueden haberse eliminado accidentalmente, corrompido, infectado por un virus informático u otras causas; guardar información histórica de forma

más económica que los discos duros y además permitiendo el traslado a ubicaciones distintas de la de los datos originales**.**

Datos: Unidad mínima de información, que por sí misma no tiene sentido para quien la posee; sin embargo adquiere mayor relevancia cuando conforma un conjunto coherente para el que la interpreta.

Desastre: Interrupción en el funcionamiento de una comunidad, sociedad o sistema, con pérdidas humanas, materiales, económicas o ambientales generalizadas, que puede exceder la capacidad de la comunidad afectada para hacerle frente haciendo uso de sus propios recursos.

Entrenamiento: Se refiere a la adquisición de conocimiento, habilidades, y capacidades como resultado de la enseñanza de habilidades o prácticas y conocimiento relacionado con aptitudes que encierran cierta utilidad.

Funcionalidad: Es la capacidad del producto del software para proveer funciones que cumplan con necesidades específicas o implícitas, cuando el software es utilizado bajo ciertas condiciones.

Es el conjunto de atributos que se refieren a la existencia de un conjunto de funciones y sus propiedades específicas.

Las características de un servicio de TIC que permiten que cubra las necesidades o requerimientos de un usuario.

Hallazgo: Toda situación irregular encontrada durante el proceso de una auditoría. En su descripción se debe incluir información necesaria para que el lector pueda entender y juzgar el hallazgo sin explicación adicional.

Hardware: Se refiere a todas las partes tangibles de un sistema informático; sus componentes son: eléctricos, electrónicos, electromecánicos y mecánicos.1 Son cables, gabinetes o cajas, periféricos de todo tipo y cualquier otro elemento físico involucrado.

Informe: En términos generales un informe es un trabajo cuyos resultados o cuyo producto es esperado por personas distintas a quien lo realiza, o bien el mismo es encargado por terceros (por ejemplo un profesor, o un jefe, o ejecutivo,etc). En cualquier caso siempre es necesario preparar todo el material que permita escribir un informe. Lo esencial es dar cuenta de algo que sucedió, con una explicación que permita comprenderlo.

Metodología: Se refiere a la descripción de las unidades de análisis, o de investigación, las técnicas de observación y recolección de datos, los instrumentos, los procedimientos y las técnicas de análisis.

Módulo: Es una parte de un programa de ordenador. De las varias tareas que debe realizar un programa para cumplir con su función u objetivos, un módulo realizará una de dichas tareas (o quizá varias en algún caso).

Objetivo: Son los propósitos perseguidos en función de los recursos disponibles. Es la situación que se desea obtener al final del período de duración del proyecto, mediante la aplicación de los recursos y las acciones previstas.

Papeles de trabajo: Registra el planeamiento, naturaleza, oportunidad y alcance de los procedimientos de auditoría aplicados por el auditor y los resultados y conclusiones extraídas a la evidencia obtenida. Se utilizan para controlar el progreso del trabajo realizado para respaldar la opinión del auditor. Los papeles de trabajo pueden estar constituidos por datos conservados en papel, película, medios electrónicos u otros medios.

Plan de contingencia: Conjunto de medidas encaminadas a restaurar el funcionamiento normal de una actividad tras la alteración producida por un accidente.

Proceso: Subsistemas o funciones en las que se divide el sistema.

Recomendaciones: Constituyen las medidas sugeridas a la administración de la entidad examinada, orientadas a promover la superación de las observaciones o hallazgos emergentes de la evaluación de la gestión.

Requerimientos: Un requerimiento es una necesidad documentada sobre el contenido, forma o funcionalidad de un producto o servicio. Se usa en un sentido formal en la ingeniería de sistemas o la ingeniería de software.

Seguridad: La capacidad de las redes o de los sistemas de información de resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles.

Sistematización: La palabra ‘sistematización’ proviene de la idea de sistema, de orden o clasificación de diferentes elementos bajo una regla o parámetro similar. La sistematización es, entonces, el establecimiento de un sistema u orden que

tiene por objetivo permitir obtener los mejores resultados posibles de acuerdo al fin que se tenga que alcanzar.

Software: Se conoce como software al equipamiento lógico o soporte lógico de una computadora digital; comprende el conjunto de los componentes lógicos necesarios que hacen posible la realización de tareas específicas.

Sub-modulo: Es el componente más simple de un sistema integrado, el cual se encuentra repetido. Puede combinarse de diferentes maneras para lograr diversas formas.

TI (Tecnología de la Información): (TI) Conjunto de recursos físicos (hardware), lógicos (software), de comunicación, de datos y otros medios que se manejan en el contexto de un sistema de información basado en ordenadores.

Usuario: Un usuario es la persona que utiliza o trabaja con algún objeto o que es destinataria de algún servicio público, privado, empresarial o profesional.

INTRODUCCIÓN

Para toda institución, tener una organización clara y ordenada de los elementos que hagan parte de ella ya sea del recurso humano como del tecnológico o presupuestal significa consolidar liderazgo, permitiendo a quienes son responsables de la toma de decisiones, pensar en soluciones que mejoren la estructura organizacional. Además de esto resulta importante hacer un seguimiento permanente con el fin de mejorar la eficacia y eficiencia y con ello un mejor procesamiento de la información.

Los cambios tecnológicos son un beneficio para el mundo actual ya que por medio de estos las empresas tanto públicas como privadas han mejorado la prestación de sus servicios y la realización de sus procesos y/o actividades, lo que contribuye a alcanzar un nivel de calidad, con relación a 10 años atrás.

Uno de los sectores donde más se evidencian cambios es en el sector de la salud, que implementa nuevas tecnologías para el manejo de pacientes y de sus datos y mejorar de esta manera para la prestación de sus servicios.

El Hospital Universitario Departamental de Nariño E.S.E es una empresa pública perteneciente al sector de la salud, que ha hecho un uso eficiente de los beneficios tecnológicos, renovando tanto hardware como software, para la puesta en marcha de un sistema de información de alta calidad que permita brindar un mejor servicio a sus usuarios al tiempo que agiliza sus procesos.

Uno de los elementos importantes dentro del Hospital Universitario Departamental de Nariño E.S.E es el área de Citas Médicas, actualmente la falta de una auditoria en esta área del hospital no ha permitido identificar el porqué de problemas como el incumplimiento de las citas, la falta de facturación, problemas con las EPS, una agenda que no llena los requerimientos necesarios para todos los usuarios; es así como en aras del mejoramiento continuo se hace indispensable una auditoria al Módulo de Citas Médicas con el fin de determinar su confiabilidad, a través de una evaluación que permita saber hasta qué punto este campo se está manejando de manera correcta y si se ha cumplido con las expectativas de los usuarios.

Una auditoria al Sistema de Información Dinámica Gerencial en el Modulo de Citas Médicas permitirá al Hospital Universitario Departamental de Nariño E.S.E saber que fallas ocasionan un desarrollo inadecuado de las operaciones, así mismo es

una oportunidad de mejora en el sistema lo que garantiza continuidad en la certificación de calidad del hospital.

IDENTIFICACIÓN DEL PROBLEMA

TÍTULO

AUDITORIA AL SISTEMA DE INFORMACION DINAMICA GERENCIAL HOSPITALARIA EN EL MODULO DE CITAS MEDICAS PARA EL HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO.

LÍNEA DE INVESTIGACIÓN

La propuesta planteada tiene como línea de investigación la siguiente:

Línea Sistemas Computacionales: Esta línea tiene con objetivo planificar, diseñar, implantar administrar y evaluar sistemas computacionales y servicios basados en estos sistemas complejos de información.

El proyecto se clasificó dentro de la Auditoria de Sistemas ya que permite evaluar los riesgos y controles dentro del módulo de Citas Médicas del Sistema de Información de Dinámica Gerencial Hospitalaria.

DESCRIPCIÓN DEL PROBLEMA

Planteamiento del Problema

El Hospital Universitario Departamental de Nariño E.S.E con el otorgamiento de la Certificación de Calidad acentúa el liderazgo que tiene en la región y el compromiso de seguir en la búsqueda de la mejora de los procesos que se llevan a cabo en el área de la salud, buscando entregar a todos los usuarios un servicio de excelencia que cumpla con las políticas de prestación de servicios planteadas por el Ministerio de la Salud y Protección Social como son: Acceso, Calidad y Eficiencia, no obstante al Módulo de Citas Médicas no se le ha realizado una evaluación previa que permita establecer el grado de confiabilidad de las procedimientos que se ejecutan en los sub-módulos de: archivos, procesos, informes y utilidades con el fin de conocer hasta donde el funcionamiento actual mitiga problemas como:

- El desbalance que existe entre la cobertura del hospital y la demanda del servicio, se tiene en promedio 6.200 llamadas mensuales y solo se tiene agenda para 4.000 citas.
- El incumplimiento de los horarios de las citas médicas por parte de los profesionales de la salud que se ve evidenciado cuando a un paciente se le asigna un turno para una cita, el paciente es atendido una o dos horas después de la hora asignada.
- La falta de control de la facturación de cada cita.
- No existe un adecuado manejo en cuanto al incumplimiento de las citas por parte de los pacientes.
- Las EPS no reportan a sus usuarios las citas asignadas

Por lo tanto se hizo necesaria la realización de una auditoria que permita identificar las causas que dan origen a los errores existentes, siguiendo un plan de trabajo para llegar a conclusiones fundamentadas y objetivas, igualmente se dio recomendaciones pertinentes con la intención de mejorar conceptos como la seguridad, la eficacia y eficiencia en el servicio para de esta manera dejar a disposición de la dirección del Hospital Universitario Departamental de Nariño E.S.E junto con sus funcionarios la puesta en marcha de las posibles soluciones que la auditoria haya arrojado.

Formulación del Problema

¿Cómo determinar la confiabilidad del Módulo de Citas Médicas y las recomendaciones necesarias para garantizar el correcto funcionamiento de la asignación y ejecución de las citas médicas mediante la aplicación de procesos de auditoria al Hospital Universitario Departamental de Nariño E.S.E?

Sistematización del Problema

¿Cómo determinar el grado de seguridad en los procesos del módulo de citas médicas?

¿Cómo las capacitaciones dadas a los funcionarios afectan el desempeño del módulo de citas médicas?

¿Cómo determinar el conocimiento de los usuarios sobre los planes de contingencia adoptados por la organización?

¿Qué impacto tuvo los requerimientos del área de citas médicas para la adquisición del software?

¿Cómo el material de apoyo ayuda a los funcionarios?

¿Cómo afecta el funcionamiento del aplicativo en el trabajo de citas médicas?

¿Cómo afectan las operaciones establecidas en el trabajo de citas médicas?

OBJETIVO

Objetivo General

Evaluar el SISTEMA DE INFORMACION DINAMICA GERENCIAL en el MODULO DE CITAS MEDICAS para el Hospital Universitario Departamental De Nariño con el fin de establecer el grado de confiabilidad y elaborar las recomendaciones necesarias que garanticen el correcto funcionamiento de sus procesos.

Objetivos Específicos

- Conocer el funcionamiento del sistema DGH específicamente en el módulo de citas médicas, recolectando información sobre la documentación, el tipo de seguridad del sistema y los usuarios del mismo.

- Planear las actividades que se llevara a cabo dentro de la auditoria dentro de ellas el funcionamiento de los procesos internos de prestación del servicio, la preparación del plan de auditoria, el programa de auditoria y los papeles de trabajo.

- Ejecutar las pruebas sobre los procesos y el módulo de citas médicas para buscar evidencia que demuestre los hallazgos y confirmen la existencia de riesgos y vulnerabilidades dentro del proceso.

- Elaborar el informe final de hallazgos y recomendaciones que servirán para ajustar los planes de mejoramiento.

JUSTIFICACION

Durante el tiempo de implementación y puesta en marcha del Sistema Dinámica Gerencial Hospitalaria en el Hospital Universitario Departamental De Nariño E.S.E., no se ha practicado ninguna auditoria al Módulo de Citas Médicas razón por la cual no se tiene en claro las causas que dan origen a los problemas que se presentan actualmente, factores que afectan el desarrollo de los planes de trabajo, ya que no solo es una simple tarea de asignación de una cita sino que alrededor

de esta actividad existen otros procesos que la complementan . Hay que recordar que una cita médica es uno de los puntos de entrada a la organización hospitalaria, y es desde el momento de la comunicación entre el usuario y el hospital donde se mide la satisfacción de un servicio.

La auditoría al Sistema Dinámica Gerencial Hospitalaria en el Modulo de Citas Médicas beneficia a las directivas y a sus funcionarios porque tendrán una visión clara de cuáles son los inconvenientes, como afrontarlos y cómo prevenir errores a largo plazo e incluso percatarse de errores que pasaban desapercibidos para quienes manejan el modulo. Si se aplican las recomendaciones los usuarios sabrán en la práctica lo que son los procesos de calidad y como estos mejoran la prestación del servicio.

ALCANCE Y DELIMITACION

La gestión de Citas Medicas es una herramienta para la administración del recurso médico, la optimización y la correcta planeación de citas de cada uno de los profesionales por especialidad que se encuentran vinculados al Hospital Universitario Departamental de Nariño E.S.E. El módulo de citas médicas no solo abarca la acción en sí de la petición de una cita por parte del paciente, sino que comprende también el proceso en que transcurre la cita, y los resultados que de ella salgan. Una visión general de la estructura del módulo de citas médicas está compuesta por archivos, procesos, informes, utilidades y unidades. El alcance del proyecto evaluó los siguientes aspectos: Seguridad, recursos humanos, licenciamiento, continuidad del servicio, objetivos de la organización, uso del software, ambiente físico y operaciones.

- En cuanto a la seguridad se evaluó si se cumplen las políticas generales de seguridad de la organización en cuanto a los procedimientos que se llevan a cabo en el módulo de citas médicas.

- En cuanto a recursos humanos se evaluó como se realiza el entrenamiento y desempeño de los funcionarios en el módulo de citas médicas.

- En el licenciamiento se evaluó el cumplimiento de la documentación de adquisición del software DGH

- Se evaluó si existen planes de contingencia para el módulo y que tanto conocen los funcionarios sobre estos planes.

- Se evaluó las necesidades o requerimientos del módulo de Citas Médicas que se tuvieron en cuenta para la adquisición del Software.

- En cuanto al uso del software se revisó el material de apoyo que existe para el personal del módulo, así mismo se valoró la funcionalidad del aplicativo.

- Se evaluó si existen planes de contingencia contra desastre para el módulo y que tanto conocen los funcionarios sobre estos planes.

- Se revisó si están definidos los procedimientos e instrucciones de operación para el módulo de citas médicas.

Para el proceso de auditoría se utilizó el método de auditoría COBIT como un estándar para la buena práctica de la auditoria.

1. MARCO TEÓRICO

1.1. ANTECEDENTES

Los trabajos de grado que se muestran a continuación sirvieron como guía o punto de partida para la realización de la auditoria al Módulo de Citas Médicas del Sistema de información Dinámica Gerencial Hospitalaria implementado en el Hospital Universitario Departamental de Nariño E.S.E.

A través del análisis sobre cómo se llevaron a cabo las auditorias ya presentadas y la observación del estado actual del sistema de información utilizado en el Hospital Universitario Departamental de Nariño E.S.E se proyectó la auditoría para que de esta manera evaluar los procedimientos que se siguen en el módulo de Citas Médicas.

Las siguientes auditorias sirvieron como base para auditar el procesamiento de la información ya que toman el estándar COBIT, el cual permite a través de la identificación de los dominios, procesos y objetivos de control, evaluar los requerimientos de un sistema.

Y en particular para la auditoria del Módulo de Citas Médicas se utilizaron como referencia para observar cómo se llevaron a cabo las evaluaciones de los procesos.

Algunos de los proyectos que se han realizado alrededor del tema de auditoría de Sistemas de Información son los siguientes:

- **TÍTULO DEL PROYECTO**: AUDITORIA DEL MODULO DE HISTORIA CLINICA ELECTRONICA DEL SISTEMA DE INFORMACION EN EL HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO.

  AUTORES DEL PROYECTO: JENNY NAYIBI BURGOS GARCIA y MARIA CAROLINA DOMÌNGUEZ GÒMEZ

  OBJETIVO GENERAL: Evaluar el proceso y el módulo de historias clínicas electrónicas, que garanticen la confiabilidad, integridad y seguridad permitiendo adelantar actividades de mejoramiento del sistema del Hospital Universitario Departamental de Nariño E.S.E.

  CONCLUSIONES: Mediante el proceso de auditoría al módulo de historia clínica, se pudo realizar una evaluación crítica, que permitió tomar varios

criterios y evidencias el relación a los aspectos a evaluar como son: el proceso de entrada, salida, y procesamientos de datos del Módulo de historia clínica.NET, el cumplimiento de los requisitos externos e internos, la infraestructura física, la seguridad física y lógica y recursos involucrado con el módulo, de tal formas 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.

El proyecto AUDITORIA DEL MODULO DE HISTORIA CLINICA ELECTRONICA DEL SISTEMA DE INFORMACION EN EL HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO es un importante referente ya que fue un trabajo de auditoria desarrollado dentro del Hospital Universitario Departamental de Nariño y toma uno de los procesos relacionados con el módulo de citas médicas como lo es Historias Clínicas.

- **TÍTULO DEL PROYECTO**: AUDITORIA DE SISTEMAS APLICADA AL SISTEMA INTEGRAL DE INFORMACION EN LA SECRETARIA DE PLANEACION MUNICIPAL DE LA ALCALDIA DE PASTO

  AUTOR DEL PROYECTO: OSCAR JULIÁN ESTRADA OBANDO

  RESUMEN: Este trabajo fue realizado para ejecutar una auditoria de Sistemas tendiente a identificar las vulnerabilidades de seguridad fisica y lógica que presenta el sistema integral de información (SII) en la Secretaria de Planeación Municipal de la Alcaldía de Pasto.

  Para lleva a cabo el proceso de auditoria se tomó como marco de referencia el estándar COBIT – Objetivos de Control para tecnologías de la información, se seleccionaron y evaluaron diferentes procesos dentro de los dominios de planeación y organización, adquisición e implementación, entrega y soporte y monitoreo. Dentro de cada uno de los dominios se identificaron los objetivos de control que hace referencia a la seguridad física y lógica. Además se elaboraron los formatos de fuentes de conocimiento y pruebas. Los cuestionarios cuantitativos y la matriz de probabilidad e impacto para los diferentes procesos que se van a auditar.

CONCLUSIÓN: La auditoría de sistemas es la herramienta que a través de una serie de procedimientos metódicos de observación, análisis y ejecución, permiten identificar las diferentes vulnerabilidades de seguridad física y lógica. Así mismo es el instrumento por medio del cual se realizan recomendaciones para corregir las deficiencias encontradas y fortalecer las medidas de seguridad, encaminadas a garantizar la integridad, confidencialidad y confiabilidad de la información.

No existe en la Alcaldía Municipal de Pasto, políticas claras a garantizar la seguridad física y lógica de los datos que alimenta y son el insumo principal de los diferentes sistemas de información que existen en las dependencias que conforman la administración municipal.

El aporte que el proyecto AUDITORIA DE SISTEMAS APLICADA AL SISTEMA INTEGRAL DE INFORMACION EN LA SECRETARIA DE PLANEACION MUNICIPAL DE LA ALCALDIA DE PASTO hizo en el trabajo, está en el aspecto de la seguridad física de las instalaciones, fundamental para la protección de los datos de la institución.

- **TÍTULO DEL PROYECTO**: PROPUESTA DE SERVICIOS PROFESIONALES EN AUDITORIA DE SISTEMAS PARA EL HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO E.S.E, EN LA CIUDAD DE PASTO

  AUTORES DEL PROYECTO: AUDISIS

  OBJETIVOS

  a) Revisar las actividades técnicas, operativas y administrativas de los Servicios de Sistemas de Información del Hospital Universitario Departamental de Nariño E.S.E., en San Juan de Pasto, para evaluar y verificar que se ejecutan de acuerdo con las buenas prácticas de Gestión de Servicios de Tecnología de Información (TI), administración de riesgos y seguridad de Tecnología de Información.
  b) Revisar el funcionamiento del Sistema de Información del Hospital Dinámica Gerencial Hospitalaria (integrado por las aplicaciones de computador que soportan el desarrollo de las operaciones), para verificar que satisfacen las necesidades de la organización de manera eficiente, segura y confiable y que dispone de los controles necesarios para mitigar los riesgos críticos que podrían afectar a la organización.

c) Informar a los niveles altos de la Dirección del Hospital, las debilidades y deficiencias identificadas por la auditoria, así como reconocer la implementación de las buenas prácticas que se consideran necesarias para solucionar las debilidades de seguridad identificadas y reducir los riesgos existentes a nivel aceptable de riesgos residual.

La PROPUESTA DE SERVICIOS PROFESIONALES EN AUDITORIA DE SISTEMAS PARA EL HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO E.S.E, EN LA CIUDAD DE PASTO no es documento que muestra paso a paso como es la auditoria, el documento sirvió de referente en cuanto a la evaluación de los riesgos.

1.2. CONCEPTO DE AUDITORIA

La auditoría nace como órgano de control de algunas instituciones estatales y privadas. Su función inicial es estrictamente económico – financiero, y los casos inmediatos se encuentra en las peritaciones judiciales y las contrataciones de contables expertos por parte de Bancos Oficiales.

La función auditora debe ser absolutamente independiente; no tiene carácter ejecutivo, ni son vinculantes sus conclusiones. Queda a cargo de la empresa tomar las decisiones pertinentes. La auditoría contiene elementos de análisis, de verificación y de exposición de debilidades y disfunciones. Aunque pueden aparecer sugerencias y planes de acción para eliminar las disfunciones y debilidades antedichas; estas sugerencias plasmadas en el Informe final reciben el nombre de Recomendaciones.

Las funciones de análisis y revisión que el auditor informático realiza, puede chocar con la psicología del auditado, ya que es un informático y tiene la necesidad de realizar sus tareas con racionalidad y eficiencia. La reticencia del auditado es comprensible y, en ocasiones, fundada. El nivel técnico de auditor es a veces insuficiente, dada la gran complejidad de los Sistemas, unidos a los plazos demasiado breves de los que suelen disponer para realizar su tarea.

Además del chequeo de los Sistemas, el auditor somete al auditado a una serie de cuestionario. Dichos cuestionarios, llamados CheckList, son guardados celosamente por las empresas auditoras, ya que son activos importantes de su

actividad. Las CheckList tienen que ser comprendidas por el auditor al pie de la letra, ya que si son mal aplicadas y mal recitadas se pueden llegar a obtener resultados distintos a los esperados por la empresa auditora. La CheckList puede llegar a explicar cómo ocurren los hechos pero no por qué ocurren. El cuestionario debe estar subordinado a la regla, realizan actividades teóricamente inadecuadas o se omiten otras correctas.

El auditor sólo puede emitir un juicio global o parcial basado en hechos y situaciones incontrovertibles, careciendo de poder para modificar la situación analizada por él mismo.[1]

1.3. ASPECTOS GENERALES SOBRE AUDITORÍA

La Auditoría puede definirse como una función de dirección cuya finalidad es analizar y apreciar, con vistas a las eventuales las acciones correctivas, el control interno de las organizaciones para garantizar la integridad de su patrimonio, la veracidad de su información y el mantenimiento de la eficacia y eficacia de sus sistemas de gestión de información.

Una de sus funciones es asesorar a la gerencia con el propósito de:

- Delegar efectivamente las funciones.
- Mantener adecuado control sobre la organización.
- Reducir a niveles mínimos el riesgo inherente.
- Revisar y evaluar cualquier fase de la actividad de la organización, contable, financiera, administrativa, operativa.

Durante la realización los auditores se encuentran cotidianamente con nuevas tecnologías de avanzada en las entidades, por lo que requieren de la incorporación sistemática de herramientas con iguales requerimientos técnicos, así como de conocimientos cada vez más profundos de las técnicas informáticas más extendidas en el control de la gestión.

[1] http://www.slideshare.net/fbogota/auditoria-de-sistemas-introduccion-presentation

1.4. TIPOS DE AUDITORÍA

1.4.1. Auditoria interna. Revisión que hace un profesional de auditoría el cual labora en la misma empresa auditada para evaluar el desempeño y cumplimiento de actividades, operaciones y funciones y emitir un dictamen de carácter doméstico sobre las actividades de la empresa. Es como un complemento de otros elementos de control administrativo, la función de una auditoría interna es establecer con suficiente competencia técnica, independencia y autoridad para revisar los objetivos de control de sistemas de información y para preparar reportes en donde se encuentren y den recomendaciones aplicables a todas las áreas de sistemas de información.

Su función debe ser establecida por el administrador general quien dictara sus responsabilidades y autoridad para realizar su función de auditoria interna, esto debe ser periódicamente revisado para verificar que se mantenga lo establecido.

Ventajas:

- Conocimiento más profundo de las actividades y operaciones de la empresa.
- Revisión más profunda.
- Informe doméstico confidencial.
- No tiene un costo adicional.
- Detección de problemas a tiempo.

Desventajas:

- La veracidad puede ser cuestionable por la posible injerencia de las autoridades de la empresa.
- Pueden existir presiones en el informe de auditoría.
- Pueden presentarse vicios en la forma que se utilizan las herramientas o en la evaluación o en el informe.

1.4.2. Auditoria externa. La realizan los auditores que son independientes a la empresa, de tal forma que el auditor externo puede aplicar con completa libertad los métodos, técnicas y herramientas con el fin de evaluar las actividades, operaciones y funciones para determinar el cumplimiento de los objetivo

institucionales y emitir dictamen independiente de carácter externo en donde se exponen los resultados en donde se pondrán las recomendaciones.

Ventajas:

- El trabajo es independiente al de la empresa.
- Aprovechar la experiencia de un externo en otras empresas.
- Aplicación de nuevas técnicas ya probadas.
- En ocasiones pueden ser un requisito legal.

Desventajas:

- Falta de conocimiento sobre la empresa.
- Dificultad para recopilar información.
- El alcance puede ser limitado.
- El ambiente puede ser difícil.
- Alta inversión en tiempo, dinero y esfuerzo.[2]

1.4.3. Auditoría financiera. Es aquella que emite un dictamen u opinión profesional en relación con los estados financieros de una unidad económica en una fecha determinada y sobre el resultado de las operaciones y los cambios en la posición financiera cubiertos por el examen la condición indispensable que esta opinión sea expresada por un Contador Público debidamente autorizado para tal fin.[3]

1.4.4. Auditoría informática. Se ocupa de analizar la actividad que se conoce como técnica de sistemas en todas sus facetas. Hoy, la importancia creciente de las telecomunicaciones ha propiciado que las comunicaciones. Líneas y redes de las instalaciones informáticas, se auditen por separado, aunque formen parte del entorno general de sistemas.

Su finalidad es el examen y análisis de los procedimientos administrativos y de los sistemas de control interno de la compañía auditada. Al finalizar el trabajo realizado, los auditores exponen en su informe aquellos puntos débiles que hayan podido detectar, así como las recomendaciones sobre los cambios convenientes a introducir, en su opinión, en la organización de la compañía.

[2] http://anaranjo.galeon.com/tipos_audi.html

[3] http://www.gerencie.com/auditoria-financiera.html

Normalmente, las empresas funcionan con políticas generales, pero hay procedimientos y métodos, que son términos más operativos. Los procedimientos son también sistemas; si están bien hechos, la empresa funcionará mejor. La auditoría de sistemas analiza todos los procedimientos y métodos de la empresa con la intención de mejorar su eficacia.[4]

1.4.5. Auditoría de la seguridad informática. La Auditoría de la seguridad en la informática abarca los conceptos de seguridad física y lógica.

La seguridad física es uno de los aspectos más olvidados a la hora del diseño de un sistema informático. Si bien algunos de los aspectos de seguridad física básicos se prevén, otros, como la detección de un atacante interno a la empresa que intenta acceder físicamente a una sala de cómputo de la misma, no. Esto puede derivar en que para un atacante sea más fácil lograr tomar y copiar una cinta de backup's de la sala de cómputo, que intentar acceder vía lógica a la misma.

Así, la Seguridad Física consiste en la "aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial". Se refiere a los controles y mecanismos de seguridad dentro y alrededor del centro de cómputo, así como los medios de acceso remoto al y desde el mismo; implementados para proteger el hardware y medios de almacenamiento de datos.

Las principales amenazas que se prevén en Seguridad Física son:

- Desastres naturales, incendios accidentales, tormentas e inundaciones
- Amenazas ocasionadas por el hombre
- Disturbios, sabotajes internos y externos deliberados.

Evaluar y controlar permanentemente la seguridad física de las instalaciones de cómputo y del edificio es la base para comenzar a integrar la seguridad como una función primordial dentro de cualquier organización.

Tener controlado el ambiente y acceso físico permite:

- Disminuir siniestros
- Trabajar mejor manteniendo la sensación de seguridad
- Descartar falsas hipótesis si se produjeran incidentes
- Tener los medios para luchar contra accidentes

[4] http://www.gerencie.com/auditoria-informatica.html

Luego de verse como el sistema puede ser afectado por la falta de seguridad física, es importante recalcar que la mayoría de los daños que puede sufrir un centro de cómputo no será sobre los medios físicos sino contra información que esté almacena y procesa. Así, la seguridad física sólo es una parte del amplio espectro que se debe cubrir para no vivir con una sensación ficticia de seguridad. Como ya se ha mencionado, el activo más importante que se posee es la información, y por lo tanto deben existir técnicas, más allá de la seguridad física que la asegure. Estas técnicas las brinda la Seguridad Lógica.

La Seguridad lógica consiste en la "aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos, a las personas con autorización para hacerlo".

Existe un viejo dicho en la seguridad informática que dicta que "todo lo que no está permitido debe estar prohibido" y esto es lo que debe asegurar la Seguridad Lógica.

Los objetivos que se plantean serán:

- Restringir el acceso a los programas y archivos
- Asegurar que los operadores puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no correspondan.
- Asegurar que se estén utilizando los datos, archivos y programas correctos en y por el procedimiento correcto.
- Que la información transmitida sea recibida por el destinatario al cual ha sido enviada y no a otro.
- Que la información recibida sea la misma que ha sido transmitida.
- Que existan sistemas alternativos secundarios de transmisión entre diferentes puntos.
- Que se disponga de pasos alternativos de emergencia para la transmisión de información.[5]

1.4.6. Auditoria operacional. Es la valoración independiente de todas las operaciones de una empresa, en forma analítica, objetiva y sistemática, para determinar si se llevan a cabo políticas y procedimientos aceptables; si se siguen las normas establecidas, si se utilizan los recursos de forma eficaz y económica y si los objetivos de la Organización se han alcanzado; para así maximizar resultados que fortalezcan el desarrollo de la empresa.

[5] http://seguridad-informatica-1-iutll.blogspot.com/2012/11/seguridad-fisica-y-logica.html

El Objetivo de la Auditoria Operativa es identificar las áreas de reducción de Costos, mejorar los métodos operativos e incrementar la rentabilidad con fines constructivos y de apoyo a las necesidades examinadas. Además determina si la producción del departamento cumple con las especificaciones dadas; en consecuencia se dan variados informes, presupuestos y pronósticos así como también los Estados Financieros.

La Auditoria Operativa determina si existe alguna deficiencia importante de políticas, procedimientos y prácticas contables defectuosas; las necesidades de Compras o Gastos, que se hayan realizado durante el ejercicio; la razonabilidad de la políticas y normas que se dan en la empresa; revisión de la financiación de las adquisiciones para determinar si afectan la cantidad, calidad y las clases de compras que haya realizado la empresa.[6]

1.4.7. Auditoria administrativa. Es el revisar y evaluar si los métodos, sistemas y procedimientos que se siguen en todas las fases del proceso administrativo aseguran el cumplimiento con políticas, planes, programas, leyes y reglamentaciones que puedan tener un impacto significativo en operación de los reportes y asegurar que la organización los esté cumpliendo y respetando.

Es el examen metódico y ordenado de los objetivos de una empresa de su estructura orgánica y de la utilización del elemento humano a fin de informar los hechos investigados.

Su importancia radica en el hecho de que proporciona a los directivos de una organización un panorama sobre la forma como está siendo administrada por los diferentes niveles jerárquicos y operativos, señalando aciertos y desviaciones de aquellas áreas cuyos problemas administrativos detectados exigen una mayor o pronta atención.

- Fernández Arena J.A dice que la auditoria administrativa es la revisión objetiva, metódica y completa, de la satisfacción de los objetivos institucionales, con base en los niveles jerárquicos de la empresa, en cuanto a si estructura, y a la participación individual de los integrantes de la institución.

[6] http://www.gerencie.com/auditoria-operativa.html

- Norbeck: “La Auditoria administrativa es una técnica de control relativamente nueva que proporciona a la gerencia un método para evaluar la efectividad de los procedimientos operativos y los controles internos”.

- William P. Leonard: “La Auditoria administrativa puede definirse como un examen completo y constructivo de la estructura organizativa de una empresa, institución o departamento gubernamental; o de cualquier otra entidad y de sus métodos de control, medios de operación y empleo que dé a sus recursos humanos y materiales”.[7]

1.4.8. Auditoría integral. Es el examen crítico, sistemático y detallado de los sistemas de información financiero, de gestión y legal de una organización, realizado con independencia y utilizando técnicas específicas, con el propósito de emitir un informe profesional sobre la razonabilidad de la información financiera, la eficacia eficiencia y economicidad en el manejo de los recursos y el apego de las operaciones económicas a las normas contables, administrativas y legales que le son aplicables, para la toma de decisiones que permitan la mejora de la productividad de la misma.

1.4.9. Auditoría de gestión ambiental. La creciente necesidad de controlar el impacto ambiental que generan las actividades humanas ha hecho que dentro de muchos sectores industriales se produzca un Incremento de la sensibilización respecto al medio ambiente. Debido a esto, las simples actuaciones para asegurar el cumplimiento legislativo han dado paso a sistemas de gestión medioambiental que permiten estructurar e integrar todos los aspectos medioambientales, coordinando los esfuerzos que realiza la empresa para llegar a objetivos previstos. Es necesario analizar y conocer en todo momento todos los factores de contaminación que generan las actividades de la empresa, y por este motivo será necesario que dentro del equipo humano se disponga de personas cualificadas para evaluar el posible impacto que se derive de los vectores ambientales. Establecer una forma sistemática de realizar esta evaluación es una herramienta básica para que las conclusiones de las mismas aporten mejoras al sistema de gestión establecido.

La aplicación permanente del concepto mejora continua es un referente que en el campo medioambiental tiene una incidencia práctica constante, y por este motivo

[7] http://www.gerencie.com/auditoria-administrativa.html

la revisión de todos los aspectos relacionados con la minimización del impacto ambiental tiene que ser una acción realizadas sin interrupción.[8]

1.4.10. Auditoría de sistemas de información. La palabra auditoria 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 específico que es el de evaluar la eficiencia y eficacia con que se está operando para que, por medio del señalamiento de cursos alternativos de acción, se tomen decisiones que permitan corregir errores, en caso de que existan, o bien mejorar la forma de actuación.

Algunos autores proporcionan otros conceptos pero todos coinciden en hacer énfasis en la revisión, evaluación y elaboración de un informe para el ejecutivo encaminado a un objetivo específico en el ambiente computacional y los sistemas.

A continuación, se detallan algunos conceptos recogidos de algunos expertos en la materia:

Auditoria de Sistemas, es:

- La verificación de controles en el procesamiento de la información, desarrollo de sistemas e instalación con el objetivo de evaluar su efectividad y presentar recomendaciones a la Gerencia.

- La actividad dirigida a verificar a juzgar información.

- 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.

- El proceso de recolección y evaluación de evidencia para determinar si un sistema automatizado:

    - ✓ Salvaguarda activos:
        - Daños

[8] http://anaranjo.galeon.com/conceptos.htm

- Destrucción
- Uso no autorizado
- Robo

✓ Mantiene integridad de los datos:
- Información Precisa
- Completa
- Oportuna
- Confiable

✓ Alcanza metas organizacionales:
- Contribución de la función informática
- Consume recursos eficientemente
- Utiliza los recursos adecuadamente
- En el procesamiento de la información

- Es el examen o revisión de carácter objetivo (independiente), crítico (evidencia), sistemático (normas), selectivo (muestras) de las políticas, normas, prácticas, funciones, procesos, procedimientos e informes relacionados con los sistemas de información computarizados, con el fin de emitir una opinión profesional (imparcial) con respecto a:

✓ Eficiencia en el uso de los recursos informáticos
✓ Validez de la información
✓ Efectividad de los controles establecidos

Pinilla Cavero propuso el siguiente concepto de la Auditoria Informática o de Sistemas " La auditoría Informática tiene como objeto de estudio el área de sistemas computarizados y tiene como objetivo, emitir una opinión independiente sobre la validez técnica del sistema de control interno informativo y sobre el grado de confiabilidad de la información generosa por el sistema auditado"

Según José Antonio Echenique "Es la revisión y evaluación de los controles, sistemas procedimientos de informática; de los equipos de cómputo, su utilización, eficiencia y seguridad, de la organización que participan en el procesamiento de la información, a fin de que por medio de señalamiento de cursos alternativo se logre una utilización más eficiente y segura de la información y servirá para una adecuada toma de decisiones".

Según Lázaro Blanco “La Auditoria informativa es de rama de la ciencia económica que tiene por objeto la revisión, comprobación, examen, estudio y análisis de las informaciones procesadas por las computadoras , empleando técnicos, métodos y artes apropiadas, con la finalidad de exponer los hechos y situaciones económicas financieras y de evaluación el Estado General de la gestión de dichas entidades.

La Auditoria de Sistemas no solo busca detectar errores o problemas en las informaciones procesadas en los sistemas informáticas , sino además, mejorar el diseño de dichas aplicaciones, aumentar la eficiencia de la dirección que utiliza las mencionadas informaciones, y garantizar la seguridad y protección de los datos almacenados y de todos los recursos informativos.

Ello implica que el auditor debe unir a los conocimientos tradicionales sobre las actividades contables, un conjunto de conocimientos y habilidades mucho más amplio sobre técnicas de computación, análisis y diseño de sistemas y gestión.

Relacionados con las siguientes materias:

- Sistemas operativos de las computadoras
- Lenguaje de programación
- Técnicas de seguridad
- Contratos sobre sistemas informativos
- Métodos y técnicas de Auditoria en general
- Software de auditoria
- Procedimientos contables y estadísticas
- Contratos financieros
- Teoría de Bases de datos
- Programación de computadoras
- Técnicas de encriptación
- Legislación vigente
- Políticas de la entidad que audita[9]

1.5. AUDITORIA DE SISTEMAS COMO OBJETO DE ESTUDIO

Cuando se generalizó el uso de las nuevas tecnologías, surgió también la necesidad de realizar auditorías sobre los sistemas de tratamiento de información. En este sentido se podría decir que la auditoria informática

[9] www.docentes.utonet.edu.bo/jmercador/wp-content

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 (bestpractices) de los sistemas.[10]

1.5.1. Alcance de la auditoria de sistemas. El alcance ha de definir con precisión el entorno y los límites en que va a desarrollarse la auditoria informática, se complementa con los objetivos de ésta. El alcance ha de figurar expresamente en el Informe Final, de modo que quede perfectamente determinado no solamente hasta que puntos se ha llegado, sino cuales materias fronterizas han sido omitidas. Ejemplo: ¿Se someterán los registros grabados a un control de integridad exhaustivo*? ¿Se comprobará que los controles de validación de errores son adecuados y suficientes*? La indefinición de los alcances de la auditoria compromete el éxito de la misma.

Control de integridad de registros:

Hay Aplicaciones que comparten registros, son registros comunes. Si una Aplicación no tiene integrado un registro común, cuando lo necesite utilizar no lo va encontrar y, por lo tanto, la aplicación no funcionaría como debería.

Control de validación de errores:

Se corrobora que el sistema que se aplica para detectar y corregir errores sea eficiente**.**[11]

1.5.2. Objetivos de la auditoria 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 recomendación de seguridades y controles.
- Conocer la situación actual del área informática y las actividades y esfuerzos necesarios para lograr los objetivos propuestos.

[10] http://www.slideshare.net/oosorioj/seguridad-en-el-control-de-aplicaciones
[11] http://www.slideshare.net/NatiiRossalesHidrobo/alcance-de-la-auditora-informtica

- Seguridad de personal, datos, hardware, software e instalaciones.
- Apoyo de función informática a las metas y objetivos de la organización.
- Seguridad, utilidad, confianza, privacidad y disponibilidad en el ambiente informático.
- Minimizar existencias de riesgos en el uso de Tecnología de información.
- Decisiones de inversión y gastos innecesarios.
- Capacitación y educación sobre controles en los Sistemas de Información.[12]

1.6. El AUDITOR

Ha de revisar los diferentes controles internos definidos en cada una de las funciones informáticas y el cumplimiento de normativa interna y externa, de acuerdo al nivel de riesgo, conforme a los objetivos definidos por la Dirección de Negocio y la Dirección de Informática. Informará a la Alta Dirección de los hechos observados y al detectarse deficiencias o ausencias de controles recomendarán acciones que minimicen los riesgos que pueden originarse.

1.6.1. Funciones del auditor

- Brindar soluciones
- Ser como el doctor que evalúa al paciente y le recomienda el tratamiento idóneo para estar en óptimas condiciones de salud. Según la situación del enfermo recomendará tratamientos ligeros o fuertes y estrictos.
- No debe ser capataz o policía del negocio como tantas veces se ha planteado de manera sarcástica en las organizaciones.

1.6.2. Perfiles profesionales de los auditores informáticos

Tabla 1: Perfiles Profesionales de los Auditores Informáticos[13]

Profesión	Actividades y conocimientos deseables
Informático Generalista	Con experiencia amplia en ramas distintas. Deseable que su labor se haya desarrollado en Explotación y en Desarrollo de Proyectos. Conocedor de Sistemas.

[12] http://anaranjo.galeon.com/objetiv_audi.htm
[13] http://www.slideshare.net/VIVIANA1234567890/un3-informe-final-de-la-auditoria-de-sistemas

Experto en Desarrollo de Proyectos	Amplia experiencia como responsable de proyectos. Experto analista. Conocedor de las metodologías de Desarrollo más importantes.
Técnico de Sistemas	Experto en Sistemas Operativos y Software Básico. Conocedor de los productos equivalentes en el mercado. Amplios conocimientos de Explotación.
Experto en Bases de Datos y Administración de las mismas.	Con experiencia en el mantenimiento de Bases de Datos. Conocimiento de productos compatibles y equivalentes. Buenos conocimientos de explotación
Experto en Software de Comunicación	Alta especialización dentro de la técnica de sistemas. Conocimientos profundos de redes. Muy experto en Subsistemas de teleproceso.
Experto en Explotación y Gestión de CPD´S	Responsable de algún Centro de Cálculo. Amplia experiencia en Automatización de trabajos. Experto en relaciones humanas. Buenos conocimientos de los sistemas.
Técnico de Organización	Experto organizador y coordinador. Especialista en el análisis de flujos de información.
Técnico de evaluación de Costes	Economista con conocimiento de Informática. Gestión de costes.

1.7. METODOLOGÍAS DE AUDITORIAS DE SISTEMAS

1.7.1. Técnicas de auditoría. Definir las técnicas de auditoría como los métodos prácticos de investigación y prueba que utiliza el auditor para obtener la evidencia necesaria que fundamente sus opiniones y conclusiones, su empleo se basa en su criterio o juicio, según las circunstancias.

Es un método o detalle de procedimiento, esencial en la práctica acertada de cualquier ciencia o arte. En la auditoría. Las técnicas son métodos asequibles para obtener material de evidencia.

Las técnicas y los procedimientos están estrechamente relacionados. Si las técnicas son desacertadas, la auditoría no alcanzará las normas aceptadas de ejecución.

1.7.1.1. Clases de técnicas de auditoría. Las técnicas se clasifican generalmente con base en la acción que se va a efectuar. Estas acciones

verificadoras pueden ser oculares, verbales, por escrito, por revisión del contenido de documentos y por examen físico.

Siguiendo esta clasificación las técnicas de auditoría se agrupan específicamente de la siguiente manera:

- Ocular
- Verbal
- Escrita
- Documental
- Inspección Física.

1.7.1.2. Procedimientos. Son el conjunto de técnicas de investigación aplicables a una partida o a un grupo de hechos y circunstancias relativas a los estados financieros sujetos a examen mediante los cuales el contador público obtiene las bases para fundamentar su opinión.

Es la combinación de dos o más técnicas, mientras que la conjugación de dos o más procedimientos de auditoria derivan los programas de auditoria, y al conjunto de programas de auditoria se le denomina plan de auditoría.

1.7.1.3. Criterios. Los criterios de Auditoría Financiera se definen entonces, como las normas y principios de contabilidad prescritos por la Contaduría general de la Nación, que viene a ser el conjunto de postulados, conceptos y limitaciones que fundamentan y circunscriben la información contable.[14]

1.7.2. Instrumentos de recolección de información para efectuar la auditoría de sistemas

1.7.2.1. Entrevistas. La entrevista es una de las actividades personales más importante del auditor; en ellas, éste recoge más información, y mejor matizada, que la proporcionada por medios propios puramente técnicos o por las respuestas escritas a cuestionarios.

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

[14] http://www.gerencie.com/auditoria-tecnicas.html

sencillamente y con pulcritud a una serie de preguntas variadas, también sencillas. Sin embargo, esta sencillez es solo aparente.

1.7.2.2. Cuestionarios. Conjunto de preguntas a las que el sujeto puede responder oralmente o por escrito, cuyo fin es poner en evidencia determinados aspectos.

Características:

Las auditorías informáticas se materializan recabando información y documentación de todo tipo. Los informes finales de los auditores dependen de sus capacidades para analizar las situaciones de debilidad o fortaleza de los diferentes entornos. El trabajo de campo del auditor consiste en lograr toda la información necesaria para la emisión de un juicio global objetivo, siempre amparado en hechos demostrables, llamados también evidencias. Estos cuestionarios no pueden ni deben ser repetidos para instalaciones distintas, sino diferentes y muy específicos para cada situación, y muy cuidados en su fondo y su forma.

1.7.2.3. Lista de chequeo o Checklists. 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 la cumplimentación sistemática de sus Cuestionarios, de sus Checklists.

1.7.2.4. Encuesta. Es un instrumento de recolección de información que se realiza utilizando un formato de cuestionario conformado por un conjunto de preguntas.

La encuesta sirve básicamente para investigar, indagar o sondear sobre un asunto determinado y/o para medir, una o más variables dentro de una investigación o estudio, dentro de una población objetivo que reúna las condiciones requeridas de acuerdo con el objeto del proyecto o tema.

Las encuestas pueden ser útiles para recopilar la información pertinente para la auditoría. Pueden ser enviadas por correo u otro método a las personas,

organizaciones, firmas privadas y otras personas que se supone conocen el programa o área de la auditoria, en la cual se interesa o pueden ser aplicadas directamente por los auditores.

Las personas que contesten las encuestas pueden estar asociadas con el programa o área de la auditoria directa o indirectamente como beneficiarios, usuarios, administradores, contratistas o simplemente como posibles fuentes de información que podrían servir de ayuda en la labor de auditoria.

1.7.2.5. Observación directa. El auditor debe estar alerta ante cualquier situación que se produzca y todas las actividades que se llevan a cabo. La idea es ver que nada este fuera de lo normal.

Es una técnica de aplicación muy general y su aporte no es muy concluyente, pues el auditor no la puede vincular a procedimientos específicos de verificación.

1.7.2.6. Documentación. Cuando se entiende la finalidad de este instrumento. El auditor comprenderá que la misma puede ser utilizada para analizar un proceso o el resultado de un sistema.

Cada auditor debe de justificar las acciones realizadas para encontrar un posible error, también sirve para encontrar nuevas posibles soluciones a un sistema decadente pero bien realizado, para que pueda dar mejores alternativas y mejores resultados de las necesidades a la empresa que se está aplicando

Este instrumento es un complemento del conocimiento que pueda tener el auditor en el proceso auditado.

1.7.3. Pasos a seguir para la realización de la auditoría

Estudio preliminar: Para realizar la auditoria se examinaron las funciones y actividades generales del área o departamento de sistemas, con el fin de tener un contacto inicial con el personal de dicha área que es la encargada del manejo general del sistema de información DGH y también al Call Center ya que es aquí donde funciona y opera el Módulo de Citas Médicas con el fin conocer a grandes rasgos cómo actúa el sistema y en específico cómo funciona el modulo.

Para la realización de la auditoria se debió conocer lo siguiente:

- Organización: Ya que es importante conocer que área o departamento es el responsable de dicho proceso y quien es la persona responsable o encargada.

- Organigrama: Porque permite conocer la estructura oficial dentro de la organización a auditar.

- Relaciones Jerárquicas y funcionales de la Organización: Es de vital importancia conocer dentro de la organización como está estructurada en cuanto a las relaciones jerárquicas y funcionales porque esto permite evidenciar el rango que ocupa cada funcionario de la misma.

- Corrientes de información: Es necesario identificar como se lleva a cabo el manejo y flujo de la información dentro del Módulo de citas Médicas ya que este permite identificar si el mismo intercambia o proporciona información a otros módulos del sistema.

- Flujos de información: Dentro del proceso de auditoría es necesario verificar que los nombres de los cargos dentro de la organización correspondan a las funciones que realiza esa persona.

  Puede ocurrir que bajo nombres de cargos diferentes se realicen funciones idénticas, en este caso se estaría realizando tareas redundantes lo cual podría conllevar a deficiencias estructurales.

- Entorno operacional: Es necesario que los auditores conozcan el lugar donde se va a realizar la auditoria en cuanto a Ubicación geográfica del o los centros de procesamiento de información de la empresa, Arquitectura y configuración de Hardware y Software, Situación geográfica de los Sistemas y Aplicaciones bases de datos.

- Determinación de recursos de la auditoría de sistemas. Por medio de los resultados del estudio preliminar es posible determinar los

recursos humanos y físicos que son necesarios en el proceso de auditoría.

1.7.4. COBIT (Control Objectives for Information and Related Technology)

Cobit, es una herramienta del gobierno del TI que han 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.

El fin primordial de 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.

La herramienta COBIT se aplica a los sistemas de información de toda la empresa, incluyendo las computadoras personales, mini computadoras y ambientales distribuidos, está 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.

COBIT está orientado a los siguientes usuarios:

La gerencia: para apoyar sus decisiones de inversión de TI y control sobre el rendimiento de las mismas y 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 determinación del control mínimo requerido.

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

Características principales del COBIT:

- Está orientado al negocio.
- Alineado con estándares y regulaciones “de facto”.
- Basado en revisión crítica y analítica de las tareas y actividades en TI.
- Alineado con estándares de control y auditoria (coso, ifac, iia, isaca, aicpa).

El concepto fundamental del marco referencial COBIT se refiere a que 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 la Tecnología de Información que deben ser administrados por procesos de TI.

Requerimientos de negocio para la información: Para satisfacer los objetivos del negocio, la información necesita concordar con ciertos criterios a los que COBIT hace referencia:

- Requerimientos de calidad: calidad, costo y entrega(de servicio)
- Requerimientos fiduciarios: efectividad y eficiencia de operaciones, confiabilidad de la información y cumplimiento de las leyes y regulaciones.
- Requerimientos de seguridad: confidencialidad, integridad y disponibilidad

Definiciones de COBIT:

- **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 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.

- **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.

Los recursos de TI identificados en COBIT pueden explicarse o definirse como se muestra a continuación:

- **Información**: son los datos en todas sus formas, de entrada, procesados y generados por los sistemas de información, en cualquier forma en que sean utilizados por el negocio.

- **Aplicaciones**: Se entiende como sistemas de aplicación la suma de procedimientos manuales y programados.

- **Infraestructura**: es la tecnología y las instalaciones (hardware, sistemas operativos, sistemas de administración de base de datos, redes, multimedia, etc., así como el sitio donde se encuentran y el ambiente que los soporta) que permiten el procesamiento de las aplicaciones.

- **Personal**: Son las habilidades de las personas como el conocimiento para planear, organizar, adquirir, implementar, entregar, soportar, monitorear y evaluar los sistemas y servicios de información.

El COBIT se divide en tres niveles:

- **Dominios**: COBIT define las actividades de TI en un modelo genérico de procesos organizado en cuatro dominios. Estos dominios son Planear y Organizar, Adquirir e Implementar, Entregar y Dar Soporte y Monitorear y Evaluar. Los dominios se equiparan a las áreas tradicionales de TI de planear, construir, ejecutar y monitorear.

- **Procesos**: conjunto de objetivos de control de alto nivel con “cortes” naturales.

- **Objetivos de Control**: COBIT define objetivos de control para los 34 procesos, así como para el proceso general y los controles de aplicación. Los objetivos de control de TI proporcionan un conjunto completo de requerimientos de alto nivel a considerar por la gerencia para un control efectivo de cada proceso de TI. Ellos:

    - ✓ Son sentencias de acciones de gerencia para aumentar el valor o reducir el riesgo.

    - ✓ Consisten en políticas, procedimientos, prácticas y estructuras organizacionales.

- ✓ Están diseñadas para proporcionar un aseguramiento razonable de que los objetivos de negocio se conseguirán y que los eventos no deseables se prevendrán, detectarán y corregirán.

Cada uno de los procesos de TI de COBIT tiene un objetivo de control de alto nivel y varios de objetivos de control detallados. Como un todo, representan las características de un proceso bien administrado.

Los objetivos de control detallados se identifican por dos caracteres que representan el dominio (PO, AI, DS y ME) más un número de proceso y un número de objetivo de control. Además de los objetivos de control detallados, cada proceso COBIT tiene requerimientos de control genéricos que se identifican con PCn, que significa Control de Proceso número. Se deben tomar como un todo junto con los objetivos de control del proceso para tener una visión completa de los requerimientos de control.
Las definiciones para los dominios mencionados son los siguientes:

- **Planeación y Organización (PO)**: 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.

- **Adquirir e Implementar (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 del negocio. Además, este dominio cubre los cambios y el mantenimiento realizados a sistemas existentes.

- **Entrega 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.

- **Monitorear y Evaluar (ME)**: 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.

2. METODOLOGIA

A través del seguimiento de pasos lógicos se llegó al resultado final de la auditoria

FASE UNO: CONOCIMIENTO

En esta etapa se conoció el Sistema de Información Dinámica Gerencial Hospitalaria en el módulo de citas médicas a través de documentación entregada por el hospital y la entrada a la dirección www.syac.net.co que contiene información acerca del producto software, así mismo para esta etapa se realizó una visita preliminar a las instalaciones del Hospital Universitario Departamental de Nariño E.S.E. en el área de Citas Médicas con el fin de realizar observación directa y tener contacto con los funcionarios que trabajan en este módulo por medio de entrevistas que permitan hacer una evaluación previa de los procesos que se manejan.

FASE DOS: PLANEACION DE LA AUDITORIA

En esta etapa se especificaron las actividades necesarias para la ejecución de la auditoria:

1. Definición de los puntos que se evaluaron en la auditoria.
2. Definición de los objetivos de la auditoria.
3. Elaboración del plan y programa de auditoría, para identificar dentro de los dominios del COBIT, que procesos y que objetivos de control evaluar.
4. Elaboración del presupuesto para la realización la auditoria.
5. Identificación y selección de los métodos, herramientas, instrumentos y procedimientos necesarios para la auditoria.
6. Definición de los recursos necesarios para la realización la auditoría.
7. Recolección de datos sobre el funcionamiento del sistema.

FASE TRES: EJECUCION DE LA AUDITORIA

En esta etapa se llevaron a cabo las tareas previstas en la fase de Planificación de la Auditoria.

1. Solicitud de Manuales y Documentación.
2. Recopilación de la información organizacional: estructura orgánica, recursos humanos.
3. Aplicación de entrevistas a los funcionarios
4. Entrevistas al Jefe de Sistemas del Hospital Universitario Departamental de Nariño E.S.E y a los usuarios más relevantes del Módulo de Citas Médicas.
5. Elaboración de cuestionarios.
6. Aplicación de Cuestionarios al personal.
7. Evaluación de los Recursos Humano y la situación actual del Módulo.
8. Evaluación del Sistema.
9. Realización de pruebas para determinar el grado de confiabilidad de los datos del sistema.
10. Realización de pruebas de cumplimiento para determinar si los procedimientos están funcionando efectivamente de acuerdo a lo que exista en la documentación solicitada.
11. Realización del análisis de riesgos y vulnerabilidades existentes en el Modulo.

FASE CUATRO: INFORME FINAL DE LA AUDITORIA

En esta etapa se hizo un análisis de los datos obtenidos para hacer un diagnóstico de la situación real encontrada.

1. Elaboración de los hallazgos donde se identificaron las causas que originaron las fallas, los recursos que afectan y las recomendaciones que se proponen.

2. Elaboración de la matriz de riesgos donde se muestra el grado de probabilidad y de impacto de las vulnerabilidades encontradas.

3. Elaboración del informe final de riesgos y recomendaciones y socialización.

3. DESARROLLO DEL TRABAJO

El proceso de auditoria realizado presenta Papeles de Trabajo que son los documentos en donde se registran los datos, información, pruebas realizadas y los hallazgos obtenidos durante este trabajo. Esta documentación puede también estar almacenada en cd o fotocopias de documentos claves para la organización.

Los Papeles de Trabajo se dividen en dos grupos en: Archivo Corriente y Archivo Permanente:

El archivo permanente son los documentos que contienen información de la entidad y sirven de consulta para auditorias posteriores, esos documentos pueden ser: reglamentos, contratos, funciones, manuales, instructivos, normas.

El archivo corriente son documentos que soportan la labor y evidencias del proceso de auditoría, comprende la evaluación que hizo el auditor a la entidad, tales documentos son: pruebas, análisis, gráficos, hojas de hallazgos, cuestionarios, programas de auditoria

3.1. ARCHIVO PERMANENTE

El objetivo principal de preparar y mantener un archivo permanente es el de tener disponible la información que se necesita en forma continua sin tener que reproducir esta información cada año.

El archivo permanente debe contener toda aquella información que es válida en el tiempo y no se refiere exclusivamente a un solo período. Este archivo debe suministrar al equipo de auditoría la mayor parte de la información sobre el negocio del cliente para llevar a cabo una auditoría eficaz y objetiva.

Ventajas del archivo permanente:

- Hace posible que el análisis y revisión de las cuentas del período sea más riguroso, ya que existe información comparativa con años anteriores.
- Un más rápido y mejor entendimiento por el auditor de las características principales del negocio del cliente y de la industria.
- Evita que todos los años se hagan las mismas preguntas al personal del cliente.
- Reduce el tiempo de ejecución y revisión de la auditoria.

- Evita muchos problemas en el caso de que sea necesario cambiar el equipo de auditoria.

3.1.1. Leyes y decretos comúnes

- Decreto 1011 de abril 3 de 2006 se reglamenta el sistema obligatorio de garantía de calidad de atención en salud del sistema general de seguridad social en salud, sogcs.

- Resolución 001043 de abril 3 de 2006 por la cual se establecen las condiciones que deben cumplir los Prestadores de Servicios de Salud para habilitar sus servicios e implementar el componente de auditoría para el mejoramiento de la calidad de la atención y se dictan otras disposiciones.

- Decreto 1599 de mayo 20 de 2005 por el cual se adopta el Modelo Estándar de Control Interno para el Estado Colombiano (MECI).

3.1.2. Hospital Universitario Departamental de Nariño. El Hospital Universitario Departamental de Nariño es una Empresa Social del Estado encargada de prestar los servicios de salud pública a todos los habitantes de la ciudad de San Juan de Pasto y todo el departamento de Nariño en general, el cual cuenta con todo el personal capacitado y cualificado para brindarle a toda la comunidad nariñense los mejores servicio en cuanto a salud se refiere.

El compromiso del **Hospital Universitario Departamental de Nariño** es superar las necesidades y expectativas de nuestros clientes internos y externos, contribuyendo positivamente al mejoramiento de la calidad de vida de los habitantes de nuestra región, para lo cual decidimos establecer y mejorar continuamente un 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 nuestros usuarios y su familia, involucrando en este propósito el desarrollo integral y participativo tanto de los trabajadores como de nuestros proveedores, logrando con ello el crecimiento de la organización.

3.1.2.1. Antecedentes del Hospital Universitario Departamental de Nariño

El Hospital Universitario Departamental de Nariño E.S.E., es la única organización de la red pública de nivel III de la región, funciona desde el 15 de diciembre de 1975 y en octubre de 1990, mediante Resolución del Ministerio de Salud No. 14676.

El Hospital Departamental de Nariño es clasificado como un organismo para atención de nivel III. A partir del 10 de diciembre de 1994, se constituye en una Empresa social del Estado por ordenanza 067 expedida en la Asamblea Departamental de Nariño, proyectándose con los avances de la Ciencia, la Tecnología y la Gerencia Moderna a la comunidad del Sur Occidente del País.

Enmarca su accionar actual, circunscrito al entorno del Sistema de la Seguridad Social en Salud, fortaleciendo su estructura organizacional y empresarial frente al reto de este milenio enfocado hacia el III y IV nivel de complejidad.

Actualmente el Hospital Departamental de Nariño E.S.E. cambia su razón social por Hospital Universitario Departamental de Nariño E.S.E.

3.1.2.2. Misión

Contamos con **Talento Humano** altamente calificado y comprometido con la seguridad integral del paciente, quienes, a través del conocimiento científico, moderna tecnología y eficiente gestión financiera brindan con afecto, respeto y amabilidad, respuestas a las necesidades y expectativas en salud de nuestros usuarios y sus familias, constituyéndose además en la principal base docente de prácticas de formación e investigación académica en la región.

3.1.2.3. Visión

En el año 2016 el **Hospital Universitario Departamental de Nariño E.S.E.,** se posicionará como una organización Acreditada, financieramente auto sostenible, reconocida a nivel nacional, por sus altos estándares de humanización de la atención, seguridad del paciente, gestión tecnológica, gestión científica, y orientación académica, protectora del medio ambiente, comprometida con el desarrollo integral de nuestro talento humano y con la calidad de vida de nuestros usuarios y sus familias.

3.1.2.4. Objetivos estratégicos

- ✓ Implementar una cultura de excelencia empresarial.
- ✓ Estandarización de procesos asistenciales con Base en el Sistema Único de Acreditación.

- ✓ Estandarización de procesos administrativos y de apoyo con Base en el SUA.
- ✓ Administración efectiva de los recursos financieros y físicos.
- ✓ Disminuir el impacto ambiental generado por el desarrollo de los procesos de la cadena productiva y de apoyo.
- ✓ Adquisición de tecnología y modernización de la infraestructura.
- ✓ Promover el desarrollo integral del personal.
- ✓ Promover los procesos de docencia e investigación.

3.1.2.5. Organigrama Hospital Universitario Departamental de Nariño

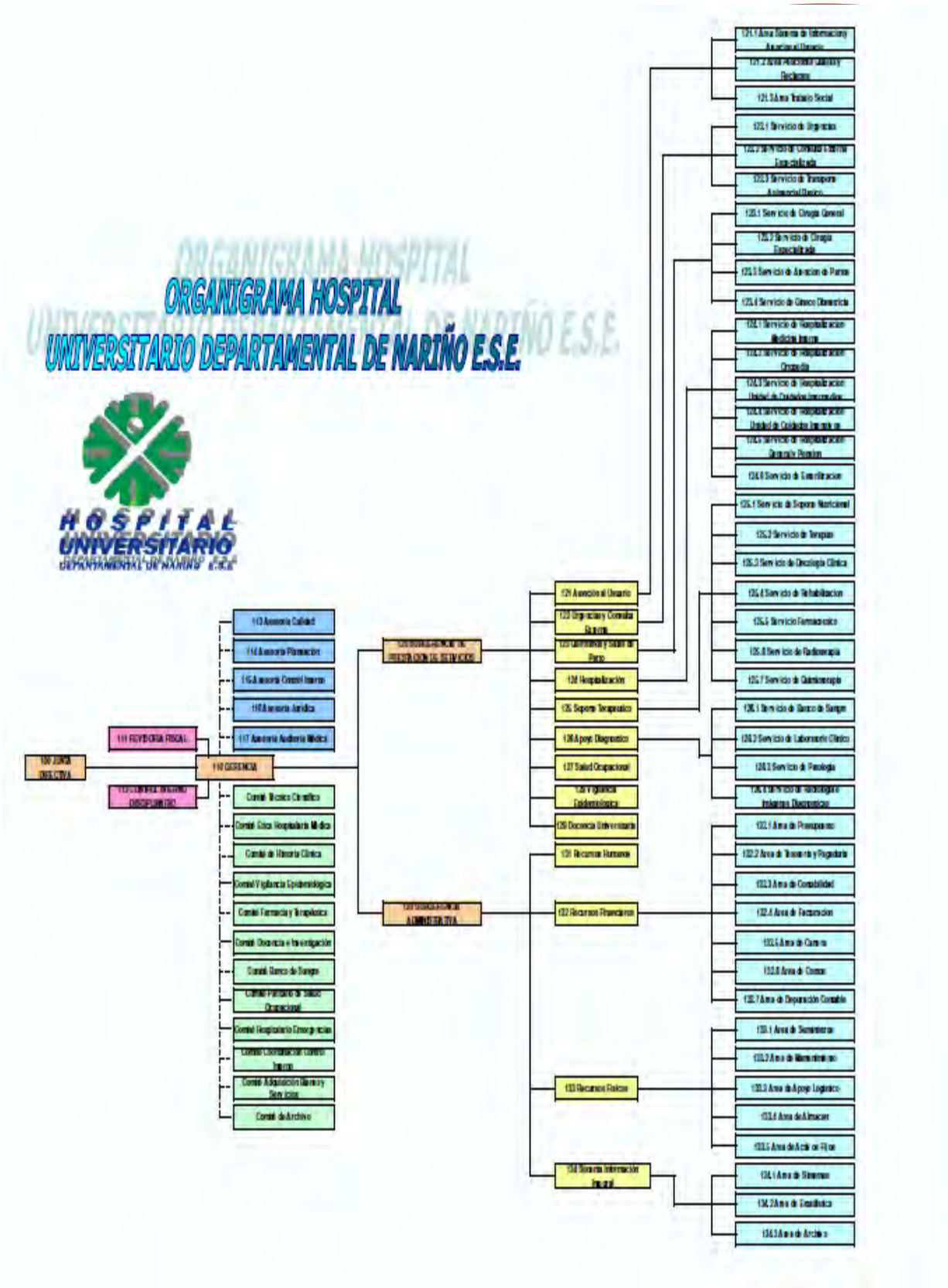


Figura 1: Organigrama Hospital Universitario Departamental de Nariño

3.1.2.6. Valores institucionales

- Liderazgo
- Servicio al Cliente
- Trabajo en Equipo
- Seguridad
- Creatividad e innovación
- Conciencia Social
- Conciencia económica
- Conciencia ecológica

3.1.2.7. Sistema de Información Dinámica Gerencial Hospitalaria (DGH)

El sistema de información Dinámica Gerencial Hospitalaria **DGH.NET** es una aplicación que fue desarrollado en los lenguajes de programación **MICROSOFT VISUAL STUDIO 2008 NET FRAMEWORK3.5** con arquitectura Cliente-Servidor y para el manejo de las bases de datos se utilizan Postgress; los desarrolladores de este software es la empresa Sistemas y Asesorías de Colombia S.A. dedicada al desarrollo e implementación de sistemas de información.

Es un sistema de información 100% Web y completamente integrado para el sector salud. Está compuesto por módulos que integran todas las áreas que conforman las INSTITUCIONES PRESTADORAS DE SALUD, públicas y privadas y de todos los niveles de atención. Es decir, que a partir del acto médico afecta las demás unidades funcionales y su correspondiente resultado en el área administrativa y ventajas de la implementación del sistema de información son: seguridad, modularidad, integridad, amigabilidad, desarrollo sostenido, garantía, relación costo beneficio.

Este se divide en dos grandes partes la parte Administrativa y financiera y la parte Operativos y Asistenciales dentro de este el modulo se ubica en la parte de operativos y asistenciales.

3.1.3. Módulo de citas médicas. Este módulo es la mejor herramienta para la administración del recurso médico, la optimización y correcta planeación de citas, (Agenda Medica de Consulta externa y actividades ambulatorias) de cada uno de los profesionales por especialidad, que se encuentran vinculados a la institución para el mejoramiento de su producción en tiempos por paciente, controlando a detalle las actividades realizadas para cada uno de ellos**.**

En el módulo de Citas médicas aquí se hace unas entradas, se efectúan unos procesos y se entregan una salidas, todo los procesos que se realizan en esta son de forma sistematizada y está compuesto por cuatro sub-módulos archivos, procesos, informes, utilidades y unidades.

Características generales

- Registro de las diferentes actividades que realizan los profesionales de la salud, estas son parametrizables por la institución tales como: actividades de Consulta, Docencia, Investigación, toma de exámenes, bloqueos de agendas, etc.
- La definición de variables que deciden el funcionamiento del módulo como: determinar la labor de sábados y festivos, formato de hora, mensajes que se desea aparezca en la impresión de la cita, consecutivos de citas, logos, realiza control de asignación de citas por especialidad.
- El registro de la agenda por especialidad médica e individual para cada uno de los profesionales de la salud, por rangos de fechas eligiendo semanal, mensual, o selección de días.
- Cada programación de una cita permite identificar claramente el profesional de la salud que atiende, el paciente, numero del consultorio, fecha y hora de la cita, motivo de la consulta, si la solicitud de la cita se realizó telefónicamente o presencial, las indicaciones médicas, y el protocolo de medicamentos asociado, de una forma ágil y oportuna, mejorando los niveles de producción y mejorando la atención al usuario**.**
- Genera indicadores de gestión que para evaluar la productividad de cada uno de los profesionales de la salud.
- Finalmente, permite el manejo de estados de citas como cumplimiento, cancelación e incumplimiento.

Características específicas

- Identifica las actividades por colores, tiempo de duración; así como, la actividad grupal y el número de pacientes a atender.
- Crea y parámetriza a los profesionales de la salud, adicionalmente asocia más de una especialidad, maneja estados y actividades por profesional.
- Define consultorios por sedes.
- Define motivos de cancelación de citas, con su justificación.
- Asigna citas extras sin que se modifique el horario del profesional de la salud.
- Permite la impresión de las planillas de programación de citas por especialidades por rango de fechas y por profesional.
- Registra la solicitud, entrega y devolución de historias clínicas.
- Permite la generación de informes estadísticos: oportunidad de cita, censo poblacional, auditoria de citas e indicadores de morbilidad.
- Permite la reprogramación de citas de forma ágil y segura.
- Genera informes de indicadores de eficiencia, oportunidad de citas, estadísticos y auditorios de citas médicas por pacientes.
- Genera informes de las novedades de citas por rango de fechas.
- Permite autorizar usuarios para la asignación de citas por especialidad y centro de atención o sedes.

- Permite actualizar en línea los indicadores de cumplimiento, productividad de cada médico: citas extras, rendimiento médico, citas incumplidas, citas cumplidas.
- Permite identificar en la boleta de impresión de citas médicas, todos los datos de la atención.
- Permite el bloqueo de turnos de médico por rangos de fecha

Visión general

A continuación, se muestra un cuadro sintético de las utilidades del Módulo de Citas Médicas con sus respectivas entradas, procesos y salidas de datos.

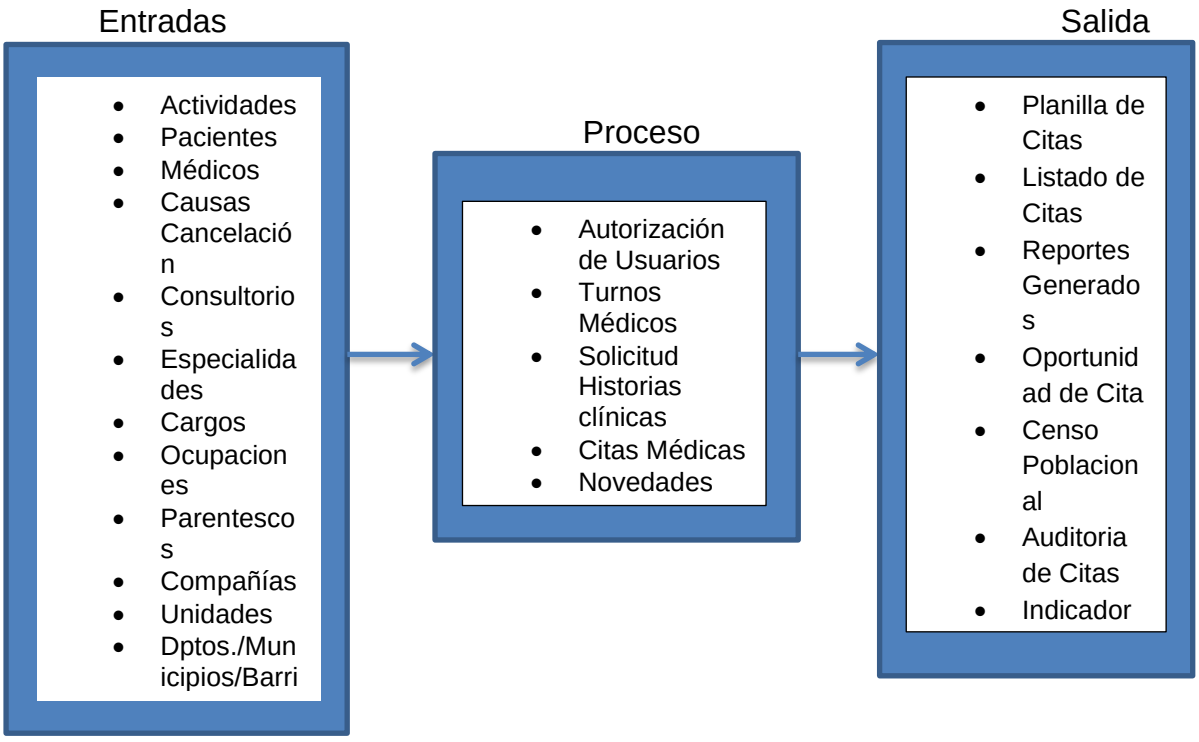


Figura 2: Cuadro Sintético de las utilidades del módulo de citas médicas

3.1.3.1. Sub-Módulo de archivos

- Actividades
- Pacientes
- Médicos
- Causas Cancelación
- Consultorios
- Especialidades
- Cargos
- Ocupaciones

- Parentescos
- Compañías
- Unidades
- Deptos./Municipios/Barrios
- Días Festivos
- Terceros
- Centros de Atención

3.1.3.2. Sub-Modulo de procesos

- Autorizaciones de Usuarios
- Turnos Médicos
- Solicitud Historias Clínicas
- Citas Médicas
- Novedades Citas
- Citas en Espera

3.1.3.3. Sub-Modulo de informes

- Planilla de Citas
- Listado de Citas
- Reportes Generados
- Oportunidad de Cita
- Censo Poblacional
- Auditoria de Citas
- Indicadores de Morbilidad
- Listado de Citas en Espera

3.1.3.4. Sub-Modulo de utilidad y unidades

- Parámetros

3.1.3.5. Diagrama de procesos del módulo de citas médicas

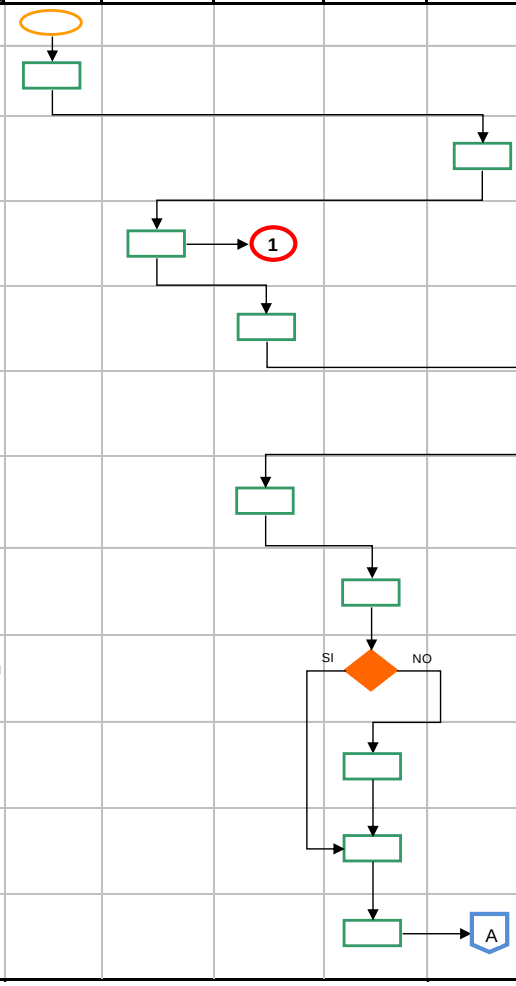
HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO E.S.E	PROCESO: GESTION DE LA INFORMACION	CODIGO:	FECHA DE ELABORACIÓN:	ACREDITACION EN SALUD
		PRSGI - 07	21 de Julio de 2008	
	SUBPROCESO: ASIGNACION DE CITAS POR EPS	VERSIÓN:	FECHA DE ACTUALIZACIÓN:	
			11 de Julio de 2011	
		01	HOJA: 1 DE: 2	

OBJETIVO: Asignar las citas a las diferentes EPS de acuerdo a los lineamientos establecidos por la normatividad vigente.

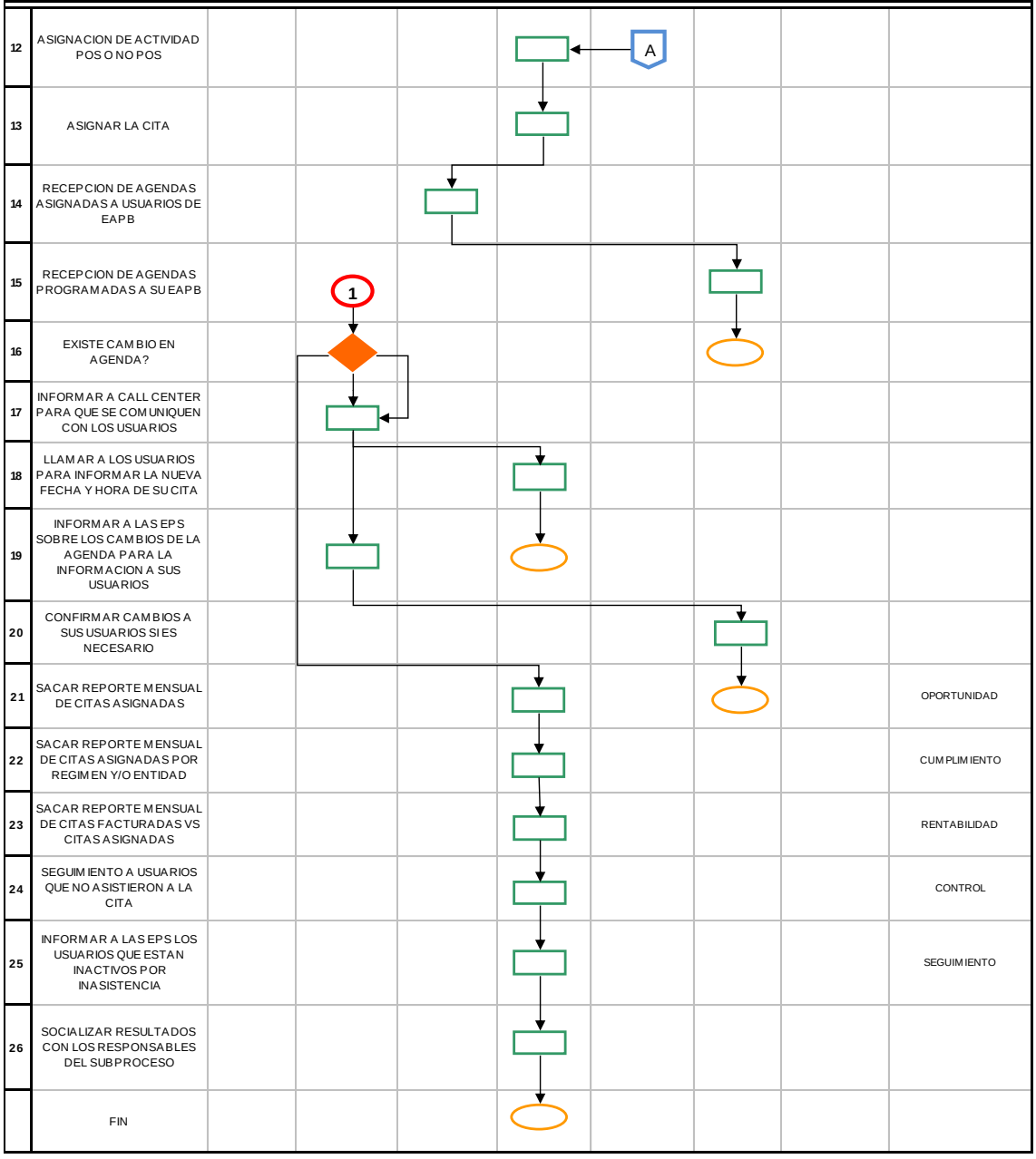
ALCANCE: Todos los pacientes remitidos por médico general y/o especialistas de acuerdo a la demanda por EPS´s y las Institución

RESPONSABLE: Coordinador de Gestión de la Información - Auxiliares Administrativas Call Center

	DESCRIPCION / RESPONSABLE	ASESOR AUDITORIA MEDICA	COOR. CONSULTA EXTERNA	ATENCION AL USUARIO HUDN ESE	AUXILIAR ADMINSITRATIVO CALL CENTER HUDN	PROFESIONAL ESPECIALIZADO COORDINADOR SISTEMAS DE INFORMACION	COORDINADOR SIAU EPS	REGISTROS	PUNTOS DE CONTROL
	INICIO								
1	DEFINICION DE EPS A ATENDER EN EL PERIODO RESPECTIVO SEGÚN CRITERIOS DETERMINADOS								
2	ASIGNACION DE CUPOS DE CITAS POR EPS DE ACUERDO AL PORCENTAJE DE PARTICPACION								
3	ELABORACION DE AGENDA MEDICA POR ESPECIALIDADES								
4	RECEPCION DE CUPOS POR CADA EPS SEGÚN ASIGNACION PORCENTUAL								
5	RECEPCION DE FORMATOS DE SIAU EAPB Y DESIGNACION DE CUPOS PARA SUS USUARIOS							FRSGI - 08 y FRSGI-09	
6	RECEPCION DE LA ASIGNACION DE USARIOS POR EPS DE ACUERDO AL FORMATO REGISTRO DE USUARIOS POR EAPB							FRSGI - 08	
7	RECEPCION DEL FORMATO REGISTRO DE USUARIOS POR EAPB DILIGENCIADO PARA INICIAR LA DISTRIBUCION DE LOS USUARIOS							FRSGI - 08	
8	VERIFICAR EN EL SISTEMA SI TIENE HISTORIA CLINICA								
9	REALIZAR LA ADMISION DEL USUARIO EN EL SISTEMA DE ACUERDO AL INSTRUCTIVO							IRSGI - 06	
10	VERIFICAR A QUE REGIMEN PERTENECE								
11	REVISAR EL MOTIVO DE CONSULTA O DIAGNOSTICO								



HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO E.S.E	PROCESO: GESTION DE LA INFORMACION	CODIGO:	FECHA DE ELABORACIÓN:	ACREDITACION EN SALUD
		PRSGI - 07	21 de Julio de 2008	
	SUBPROCESO: ASIGNACION DE CITAS POR EPS	VERSIÓN:	FECHA DE ACTUALIZACIÓN:	
			11 de Julio de 2011	
		01	HOJA: 2 DE: 2	



ELABORADO POR:	REVISADO POR:	APROBADO POR:
Gestión de Información y Gestión de Calidad	Asesor de Planeación	Gerencia

Figura 3: Diagrama de proceso módulo de citas médicas

3.2. ARCHIVO CORRIENTE

3.2.1. Programa de auditoría. Para la elaboración de este se utilizó el método de auditoria Cobit el cual es una herramienta que sirve de guía porque es estándar para la buena práctica de la auditoria, y con base en este, se eligieron cada uno de los procesos y objetivos de control que son importantes y necesarios para evaluar y aplicar en el módulo de citas médicas.

Los siguientes son los procesos que se valoraron con sus respectivos objetivos de control:

Objetivos de control para el módulo de citas médicas del Hospital Universitario Departamental de Nariño

Dominio: Planear y Organizar (PO)

- **Proceso (PO7): Administración de los Recursos Humanos**

Adquirir, mantener y motivar una fuerza de trabajo para la creación y entrega de los servicios de TI para el negocio. Esto se logra siguiendo practicas definidas y aprobadas que apoyen el reclutamiento, entrenamiento, la evaluación del desempeño, la promoción y la terminación. Este proceso es crítico, ya que las personas son activo importante, y el ambiente de gobierno y de control interno depende fuertemente de la motivación y competencia personal.

✓ **Objetivo de Control (PO7.1):** Reclutamiento y Retención del Personal

Asegurarse que los procesos de reclutamiento del personal de TI estén 6de acuerdo a las políticas y procedimientos generales de personal de la organización (Ej. contratación, un ambiente positivo de trabajo y orientación). La gerencia implementa procesos para garantizar que la organización cuente con una fuerza de trabajo posicionada de forma apropiada, que tenga las habilidades necesarias para alcanzar las metas organizacionales.

✓ **Objetivo de Control (PO7.2):** Competencias del personal

Verificar de forma periódica que el personal tenga las habilidades para cumplir sus roles con base en su educación, entrenamiento y/o experiencia. Definir los requerimientos esenciales de habilidades para TI y verificar que se les dé mantenimiento, usando programas de calificación y certificación según sea el caso.

✓ **Objetivo de Control (PO7.3):** Asignación de Roles

Definir, monitorear y supervisar los marcos de trabajo para los roles, responsabilidades y compensación del personal, incluyendo el requerimiento de adherirse a las políticas y procedimientos administrativos, así como al código de ética y prácticas profesionales. El nivel de supervisión debe estar de acuerdo con la sensibilidad del puesto y el grado de responsabilidades asignadas.

✓ **Objetivo de Control (PO7.4):** Entrenamiento del Personal de TI

Proporcionar a los empleados de TI la orientación necesaria al momento de la contratación y entrenamiento continuo para conservar su conocimiento, aptitudes, habilidades, controles internos y conciencia sobre la seguridad, al nivel requerido para alcanzar las metas organizacionales.

✓ **Objetivo de Control (PO7.5):** Dependencia Sobre los Individuos

Minimizar la exposición a dependencias críticas sobre individuos clave por medio de la captura del conocimiento (documentación), compartir el conocimiento, planeación de la sucesión y respaldos de personal.

✓ **Objetivo de Control (PO7.6):** Procedimientos de Investigación del Personal

Incluir verificaciones de antecedentes en el proceso de reclutamiento de TI. El grado y la frecuencia de estas verificaciones dependen de que tan delicada ó crítica sea la función y se deben aplicar a los empleados, contratistas y proveedores.

✓ **Objetivo de Control (PO7.7):** Evaluación del Desempeño del empleado

Es necesario que las evaluaciones de desempeño se realicen periódicamente, comparando contra los objetivos individuales derivados de las metas organizacionales, estándares establecidos y responsabilidades específicas del puesto. Los empleados deben recibir adiestramiento sobre su desempeño y conducta, según sea necesario.

✓ **Objetivo de Control (PO7.8):** Cambios y Terminación de Trabajo

Tomar medidas expeditas respecto a los cambios en los puestos, en especial las terminaciones. Se debe realizar la transferencia del conocimiento, reasignar responsabilidades y se deben eliminar los

privilegios de acceso, de tal modo que los riesgos se minimicen y se garantice la continuidad de la función.

Tareas realizadas para evaluar el dominio Planeación y Organización

DOMINIO	PROCESO	OBJETIVOS DE CONTROL	ACTIVIDADES REALIZADAS
Planear y Organizar (PO)	**(PO7): Administración de los Recursos Humanos**	**(PO7.1):** Reclutamiento y Retención del Personal	• Se observó cómo era la estructura de recursos humanos dentro del módulo. • Se preparó una serie de preguntas orientadas al perfil de los funcionarios. • Estas preguntas se dividieron en entrevistas y listas de chequeo. • Se aplicó la entrevista. • Se revisó la documentación sobre capacitación entregada. • Se aplicó la lista de chequeo para verificar que se siga un plan de reclutamiento, entrenamiento y evaluación de desempeño del personal. • Se analizaron los resultados arrojados en las entrevistas y listas de chequeo.
		(PO7.2): Competencias del personal	
		(PO7.3): Asignación de Roles	
		(PO7.4): Entrenamiento del Personal de TI	
		(PO7.5): Dependencia Sobre los Individuos	
		(PO7.6): Procedimientos de Investigación del Personal	
		(PO7.7): Evaluación del Desempeño del empleado	
		(PO7.8): Cambios y Terminación de Trabajo	

Dominio: Adquirir e Implementar (AI)

- **Proceso (AI1): Identificar soluciones automatizadas**

La necesidad de una nueva aplicación o función requiere de un análisis antes de la compra o desarrollo para que garantizar que los requisitos del negocio se satisfacen con un enfoque efectivo y eficiente. Este proceso cubre la definición de las necesidades, considera las fuentes alternativas, realiza una revisión de la factibilidad tecnológica y económica, ejecuta un análisis de riesgo y de costo-beneficio y concluye con una decisión final de “desarrollar” o “comprar”. Todos estos pasos permiten a las organizaciones minimizar el costo para Adquirir e Implementar soluciones, mientras que al mismo tiempo facilitan el logro de los objetivos del negocio.

- ✓ **Objetivo de Control (AI1.1):** Definición y Mantenimiento de los Requerimientos Técnicos y Funcionales del Negocio

Identificar, dar prioridades, especificar y acordar los requerimientos de negocio funcionales y técnicos que cubran el alcance completo de todas las

iniciativas requeridas para lograr los resultados esperados de los programas de inversión en TI.

- ✓ **Objetivo de Control (AI1.2):** Reporte de Análisis de Riesgos

Identificar, documentar y analizar los riesgos asociados con los requerimientos del negocio y diseño de soluciones como parte de los procesos organizacionales para el desarrollo de los requerimientos.

- **Proceso (AI4): Facilitar la operación y uso**

El conocimiento sobre los nuevos sistemas debe estar disponible. Este proceso requiere la generación de documentación y manuales para usuarios y para TI, y proporciona entrenamiento para garantizar el uso y la operación correctos de las aplicaciones y la infraestructura.

- ✓ **Objetivo de Control (AI4.1):** Plan para Soluciones de Operación

Desarrollar un plan para identificar y documentar todos los aspectos técnicos, la capacidad de operación y los niveles de servicio requeridos, de manera que todos los interesados puedan tomar la responsabilidad oportunamente por la producción de procedimientos de administración, de usuario y operativos, como resultado de la introducción o actualización de sistemas automatizados o de infraestructura.

- ✓ **Objetivo de Control (AI4.3):** Transferencia de Conocimiento a Usuarios Finales

Transferencia de conocimiento y habilidades para permitir que los usuarios finales utilicen con efectividad y eficiencia el sistema de aplicación como apoyo a los procesos del negocio. La transferencia de conocimiento incluye el desarrollo de un plan de entrenamiento que aborde al entrenamiento inicial y continuo, así como el desarrollo de habilidades, materiales de entrenamiento, manuales de usuario, manuales de procedimiento, ayuda en línea, asistencia a usuarios, identificación de usuario clave, y evaluación.

- ✓ **Objetivo de Control (AI4.4):** Transferencia de Conocimiento de Operaciones y Soporte

Transferir el conocimiento y las habilidades para permitir al personal de soporte técnico y de operaciones que entregue, apoyen y mantengan la aplicación y la infraestructura asociada de manera efectiva y eficiente de acuerdo a los niveles de servicio requeridos. La transferencia del conocimiento debe incluir a l entrenamiento inicial y continuo, el desarrollo de las habilidades, los materiales de entrenamiento, los manuales de operación, los manuales de procedimientos y escenarios de atención al usuario.

- **Proceso (AI5): Adquirir recursos de TI**

Se deben suministrar recursos TI, incluyendo personas, hardware, software y servicios. Esto requiere de la definición y ejecución de os procedimientos de adquisición, la selección de proveedores, el ajuste de arreglos contractuales y la adquisición en sí. El hacerlo así garantiza que la organización tenga todos los recursos de TI que se requieren de una manera oportuna y rentable.

✓ **Objetivo de Control (AI5.2):** Administración de Contratos con Proveedores
Formular un procedimiento para establecer, modificar y concluir contratos para todos los proveedores. El procedimiento debe cubrir, como mínimo, responsabilidades y obligaciones legales, financieras, organizacionales, documentales, de desempeño, de seguridad, de propiedad intelectual y responsabilidades de conclusión, así como obligaciones (que incluyan cláusulas de penalización). Todos los contratos y las modificaciones a contratos las deben revisar asesores legales.

✓ **Objetivo de Control (AI5.3):** Selección de Proveedores
Seleccionar proveedores de acuerdo a una práctica justa para garantizar las mejor viable y encajable según los requerimientos especificados. Los requerimientos deben estar optimizados con las entradas de los proveedores potenciales.

✓ **Objetivo de Control (AI5.4):** Adquisición de Recursos de TI
Proteger y hacer cumplir los intereses de la organización en todo los contractos de adquisiciones, incluyendo los derechos y obligaciones de todas las partes en términos contractuales para la adquisición de software, recursos de desarrollo, infraestructura y servicios.

Tareas realizadas para evaluar el dominio Adquisión e Implementación.

DOMINIO	PROCESO	OBJETIVOS DE CONTROL	ACTIVIDADES REALIZADAS
Adquirir e Implementar (AI)	**(AI1): Identificar soluciones automatizadas**	**(AI1.1):** Definición y Mantenimiento de los Requerimientos Técnicos y Funcionales del Negocio	• Se preparó una serie de preguntas orientadas a averiguar: bajo que requerimientos el hospital justifica su procedimiento, como se hizo la trasferencia del conocimiento y como fue el proceso de licenciamiento del software. • Estas preguntas se dividieron en entrevistas y listas de chequeo. • Se aplicó la entrevista.
		(AI1.2): Reporte de Análisis de Riesgos	
	(AI4): Facilitar la operación y uso	**(AI4.1):** Plan para Soluciones de Operación	
		(AI4.3): Transferencia de Conocimiento a Usuarios Finales.	
		(AI4.4): Transferencia de Conocimiento de Operaciones y Soporte	
	(AI5): Adquirir recursos de TI	**(AI5.2):** Administración de Contratos con Proveedores	

		(AI5.3): Selección de Proveedores	• Se revisó la documentación sobre licenciamiento, manuales, normas. • Se aplicó la lista de chequeo para verificar que se siga un plan de transferencia de conocimiento. • Se analizaron los resultados arrojados en las entrevistas y listas de chequeo.
		(AI5.4): Adquisición de Recursos de TI	

Dominio: Entrega y Soporte (DS)

- **Proceso (DS4): Garantizar la Continuidad del Servicio**

La necesidad de brindar continuidad en los servicios de TI requiere desarrollar, mantener y probar planes de continuidad de TI, almacenar respaldo fuera de las instalaciones y entrenar de forma periódica sobre los planes de continuidad. Un proceso efectivo de continuidad de servicios, minimiza la probabilidad y el impacto de interrupciones mayores en los servicios de TI, sobre funciones y procesos claves del negocio.

✓ **Objetivo de Control (DS4.2):** Planes de Continuidad de TI

Desarrollar planes de continuidad de TI con base en el marco de trabajo, diseñado para reducir el impacto de una interrupción mayor de las funciones y los procesos clave del negocio. Los planes deben considerar requerimientos de resistencia, procesamiento alternativo, y capacidad de recuperación de todos los servicios críticos de TI. También deben cubrir los lineamientos de uso, los roles y responsabilidades, los procedimientos, los procesos de comunicación y el enfoque de pruebas.

✓ **Objetivo de Control (DS4.3):** Recursos Críticos de TI

Centrar la atención en los puntos determinados como los más críticos en el plan de continuidad de TI, para construir resistencia y establecer prioridades en situaciones de recuperación. Evitar la distracción de recuperar los puntos menos críticos y asegurarse de que la respuesta y la recuperación están alineadas con las necesidades prioritarias del negocio, asegurándose también que los costos se mantienen a un nivel aceptable y se cumple con los requerimientos regulatorios y contractuales. Considerar los requerimientos de resistencia, respuesta y recuperación para diferentes niveles de prioridad, por ejemplo, de una a cuatro horas, de cuatro a 24 horas, más de 24 horas y para periodos críticos de operación del negocio.

✓ **Objetivo de Control (DS4.4):** Mantenimiento del Plan de Continuidad de TI

Exhortar a la gerencia de TI a definir y ejecutar procedimientos de control de cambios, para asegurar que el plan de continuidad de TI se mantenga actualizado y que refleje de manera continua los requerimientos actuales del negocio. Es esencial que los cambios en los procedimientos y las responsabilidades sean comunicados de forma clara y oportuna.

✓ **Objetivo de Control (DS4.5):** Pruebas del Plan de Continuidad de TI

Probar el plan de continuidad de TI de forma regular para asegurar que los sistemas de TI pueden ser recuperados de forma efectiva, que las deficiencias son atendidas y que el plan permanece aplicable. Esto requiere una preparación cuidadosa, documentación, reporte de los resultados de las pruebas y, de acuerdo con los resultados, la implementación de un plan de acción. Considerar el alcance de las pruebas de recuperación en aplicaciones individuales, en escenarios de pruebas integrados, en pruebas de punta a punta y en pruebas integradas con el proveedor.

✓ **Objetivo de Control (DS4.6):** Entrenamiento del Plan de Continuidad de TI

Asegurarse de que todos las partes involucradas reciban sesiones de habilitación de forma regular respecto a los procesos y sus roles y responsabilidades en caso de incidente o desastre. Verificar e incrementar el entrenamiento de acuerdo con los resultados de las pruebas de contingencia.

✓ **Objetivo de Control (DS4.7):** Distribución del Plan de Continuidad de TI

Determinar que existe una estrategia de distribución definida y administrada para asegurar que los planes se distribuyan de manera apropiada y segura y que estén disponibles entre las partes involucradas y autorizadas cuando y donde se requiera. Se debe prestar atención en hacerlos accesibles bajo cualquier escenario de desastre.

✓ **Objetivo de Control:** Recuperación y Reanudación de los Servicios de TI

Planear las acciones a tomar durante el período en que TI está recuperando y reanudando los servicios. Esto puede representar la activación de sitios de respaldo, el inicio de procesamiento alternativo, la comunicación a clientes y a los interesados, realizar procedimientos de reanudación, etc. Asegurarse de que los responsables del negocio entienden los tiempos de recuperación de TI y las inversiones necesarias en tecnología para soportar las necesidades de recuperación y reanudación del negocio.

- ✓ **Objetivo de Control (DS4.9):** Almacenamiento de Respaldos Fuera de las Instalaciones.

Almacenar fuera de las instalaciones todos los medios de respaldo, documentación y otros recursos de TI críticos, necesarios para la recuperación de TI y para los planes de continuidad del negocio. El contenido de los respaldos a almacenar debe determinarse en conjunto entre los responsables de los procesos de negocio y el personal de TI. La administración del sitio de almacenamiento externo a las instalaciones, debe apegarse a la política de clasificación de datos y a las prácticas de almacenamiento de datos de la empresa. La gerencia de TI debe asegurar que los acuerdos con sitios externos sean evaluados periódicamente, al menos una vez por año, respecto al contenido, a la protección ambiental y a la seguridad. Asegurarse de la compatibilidad del hardware y del software para poder recuperar los datos archivados y periódicamente probar y renovar los datos archivados.

- ✓ **Objetivo de Control (DS4.10):** Revisión Post Reanudación

Una vez lograda una exitosa reanudación de las funciones de TI después de un desastre, determinar si la gerencia de TI ha establecido procedimientos para valorar lo adecuado del plan y actualizar el plan en consecuencia.

- **Proceso (DS5): Garantizar la seguridad de los Sistemas**

La necesidad de mantener la integridad de la información y de proteger los activos de TI, requieren de un proceso de administración de la seguridad. Este proceso incluye el establecimiento y mantenimiento delos roles y responsabilidades de seguridad, políticas, estándares y procedimientos de TI. La administración de la seguridad también incluye realizar monitoreo de seguridad identificados. Una efectiva administración de la seguridad protege todos los activos de TI para minimizar el impacto en el negocio causado por vulnerabilidades o incidentes de seguridad.

- ✓ **Objetivo de Control (DS5.2):** Plan de Seguridad de TI

Trasladar los requerimientos de negocio, riesgos y cumplimiento dentro de un plan de seguridad de TI completo, teniendo en consideración la infraestructura de TI y la cultura de seguridad. Asegurar que el plan esta implementado en las políticas y procedimientos de seguridad junto con las inversiones apropiadas en los servicios, personal, software y hardware. Comunicar las políticas y procedimientos de seguridad a los interesados y a los usuarios.

- ✓ **Objetivo de Control (DS5.3):** Administración de Identidad

Asegurar que los usuarios (internos, externos y temporales) y su actividad en sistemas de TI (aplicación de negocio, entorno de TI, operación de sistemas, desarrollo y mantenimiento) deben ser identificables de manera única. Permitir que el usuario se identifique a través de mecanismos de autenticación. Confirmar que los permisos de acceso del usuario al sistema y los datos están en línea con las necesidades del negocio definidas y documentadas y que los requerimientos de trabajo están adjuntos a las identidades del usuario. Asegurar que los derechos de acceso del usuario se solicitan por la gerencia del usuario, aprobados por el responsable del sistema e implementado por la persona responsable de la seguridad. Las identidades del usuario y los derechos de acceso se mantienen en un repositorio central. Se despliegan técnicas efectivas en coste y procedimientos rentables, y se mantienen actualizados para establecerla identificación y habilitar los derechos de acceso.

- ✓ **Objetivo de Control (DS5.4)**Administración de Cuentas del Usuario

Garantizar que la solicitud, establecimiento, emisión, suspensión, modificación y cierre de cuentas de usuario y de los privilegios relacionados, sean tomados en cuenta por un conjunto de procedimientos de la gerencia de cuentas de usuario. Debe incluirse un procedimiento de aprobación que describa al responsable de los datos o del sistema otorgando los privilegios de acceso. Estos procedimientos deben aplicarse a todos los usuarios, incluyendo administradores (usuarios privilegios), usuarios externos e internos, para casos normales y de emergencia. Los derechos y obligaciones relativos al acceso a los sistemas e información de la empresa deben acordarse contractualmente para los tipos de usuarios. Realizar revisiones regulares de la gestión de todas las cuentas y los privilegios asociados.

- ✓ **Objetivo de Control (DS5.5):** Pruebas, Vigilancia y Monitoreo de la Seguridad

Garantizar que la implementación de la seguridad en TI sea probada y monitoreada de forma pro-activa. La seguridad en TI debe ser reacreditada periódicamente para garantizar que se mantiene el nivel de seguridad aprobado. Una función de ingreso al sistema (logging) y de monitoreo permite la detección oportuna de actividades inusuales o anormales que puedan requerir atención.

✓ **Objetivo de Control (DS5.7):** Protección de la Tecnología de Seguridad

Definir claramente y comunicar las características de incidentes de seguridad potenciales para que puedan se clasificados propiamente y tratados por el proceso de gestión de incidentes y problemas.

✓ **Objetivo de Control (DS5.8):** Administración de Llaves Criptográficas

Determinar que las políticas y procedimientos para organizar la generación, cambio, revocación, destrucción, distribución, certificación, almacenamiento, captura, uso y archivo de llaves criptográficas estén implantadas, para garantizar la protección de las llaves contra modificaciones y divulgación no autorizadas.

✓ **Objetivo de Control (DS5.9):** Prevención, Detección y Corrección de Software Malicioso

Poner medicas preventivas, detectivas y correctivas (en especial contar con parches de seguridad y control de virus actualizados) en toda la organización para proteger los sistemas de la información y ala tecnología contra malware (virus, gusanos, spyware, correo basura).

✓ **Objetivo de Control (DS5.11):** Intercambio de Datos Sensitivos

Transacciones de datos sensibles se intercambian solo a través de una ruta o medio con controles para proporcionar autenticidad de contenido, prueba de envío, prueba de recepción y no repudio del origen.

- **Proceso (DS11): Administración de datos**

Una efectiva administración de datos requiere de la identificación de requerimientos de datos. El proceso de administración de información también incluye el establecimiento de procedimientos efectivos para administrar la librería de medios, el respaldo y la recuperación de datos y al eliminación apropiada de medios. Una efectiva administración de datos ayuda a garantizar la calidad, oportunidad y disponibilidad de la información del negocio.

✓ **Objetivo de Control (DS11.3):** Sistema de Administración de Librerías de Medios

Definir e implementar procedimientos para mantener un inventario de medios almacenados y archivados para asegurar su usabilidad e integridad.

✓ **Objetivo de Control (DS11.4):** Eliminación

Definir e implementar procedimientos para asegurar que los requerimientos de negocio para la protección de datos sensitivos y el

software se consiguen cuando se eliminan o transfieren los datos y/o el hardware.

- ✓ **Objetivo de Control (DS11.6):** Requerimientos de Seguridad para la Administración de Datos

Definir e implementar las políticas y procedimientos para identificar y aplicar los requerimientos de seguridad aplicables al recibo procesamiento, almacén y salida de los datos para conseguir los objetivos de negocio, las políticas de seguridad de la organización y requerimientos regulatorios.

- **Proceso (DS12): Administración del Ambiente Físico**

La protección del equipo de cómputo y del personal, requiere de instalaciones bien diseñadas y bien administradas. El proceso de administrar el ambiente físico incluye la definición de los requerimientos físicos del centro de datos (site), la selección de instalaciones apropiadas y el diseño de procesos efectivos para monitorear factores ambientales y administrar el acceso físico. La administración efectiva del ambiente físico reduce las interrupciones del negocio ocasionadas por daños al equipo de cómputo y al personal.

- ✓ **Objetivo de Control (DS12.1):** Selección y Diseño del Centro de Datos

Definir y seleccionar los centros de datos físicos para el equipo de TI para soportar la estrategia de tecnología ligada a la estrategia del negocio. Esta selección y diseño del esquema de un centro debe tomar en cuenta el riesgo asociado con desastres naturales y causados por el hombre. También debe considerar las leyes y regulaciones correspondientes, tales como regulaciones de seguridad y de salud en el trabajo.

- ✓ **Objetivo de Control (DS12.2):** Medidas de Seguridad Física

Definir e implementar medidas de seguridad física alineadas con los requerimientos del negocio. Las medidas deben incluir, pero no limitarse al esquema del perímetro de seguridad, de las zonas de seguridad, la ubicación de equipo crítico y de las áreas de envío y recepción. En particular, mantenga un perfil bajo respecto a la presencia de operaciones críticas de TI. Deben establecerse las responsabilidades sobre el monitoreo y los procedimientos de reporte y de resolución de incidentes de seguridad física.

- ✓ **Objetivo de Control (DS12.3):** Acceso Físico

Definir e implementar procedimientos para otorgar, limitar y revocar el acceso a locales, edificios y áreas de acuerdo con las necesidades del negocio, incluyendo las emergencias. El acceso a locales, edificios y áreas debe justificarse, autorizarse, registrarse y monitorearse. Esto aplica para todas las personas que accedan a las instalaciones,

incluyendo personal, clientes, proveedores, visitantes o cualquier tercera persona.

✓ **Objetivo de Control (DS12.4):** Protección Contra Factores Ambientales
Diseñar e implementar medidas de protección contra factores ambientales. Deben instalarse dispositivos y equipos especializados para monitorear y controlar el ambiente.

✓ **Objetivo de Control (DS12.5):** Administración de Instalaciones Físicas
Administrar las instalaciones, incluyendo el equipo de comunicaciones y de suministro de energía, de acuerdo con las leyes y los reglamentos, los requerimientos técnicos y del negocio, las especificaciones del proveedor y los lineamientos de seguridad y salud.

- **Proceso (DS13): Administración de operaciones**
Un procesamiento de información completo y apropiado requiere de una efectiva administración del procesamiento de datos y del mantenimiento de hardware. Este proceso incluye la definición de políticas y procedimientos de operación para una administración efectiva del procedimiento programado, protección de datos de salida sensitivos, monitoreo de infraestructura y mantenimiento preventivo de hardware. Una efectiva administración de operaciones ayuda a mantener la integridad de los datos y reduce los retrasos en el trabajo y los costos operativos de TI.

✓ **Objetivo de Control (DS13.1):** Procedimientos e Instrucciones de Operación
Definir, implementar y mantener procedimientos estándar para operaciones de TI y garantizar que e l personal de operaciones está familiarizado con todas las tareas de operación relativas a ellos. Los procedimientos de operación deben cubrir los procesos de entrega de turno (transferencia formal de la actividad, estatus, actualizaciones, problemas de operación, procedimientos de escalamiento, y reportes sobre las responsabilidades actuales) para garantizar la continuidad de las operaciones.

✓ **Objetivo de Control (DS13.2):** Programación de Tareas
Organizar la programación de trabajos, procesos y tareas en la secuencia más eficiente, maximizando el desempeño y la utilización para cumplir con los requerimientos del negocio. Deben autorizarse los programas iniciales así como los cambios a estos programas. Los procedimientos deben implementarse para identificar, investigar y aprobar las salidas de los programas estándar agendados.

✓ **Objetivo de Control (DS13.5):** Mantenimiento Preventivo del Hardware

Definir e implementar procedimientos para monitorear la infraestructura de TI y los eventos relacionados. Garantizar que en los registros de operación se almacena suficiente información cronológica para permitir la reconstrucción, revisión y análisis de las secuencias de tiempo de las operaciones y de las otras actividades que soportan o que están alrededor de las operaciones.

Tareas realizadas para evaluar el dominio Entrega y Soporte

DOMINIO	PROCESO	OBJETIVOS DE CONTROL	ACTIVIDADES REALIZADAS
Entrega y Soporte (DS)	**(DS4): Garantizar la Continuidad del Servicio**	**(DS4.2):** Planes de Continuidad de TI	• Se observó que se hace en el momento de falla en el sistema, como es el proceso operativo en el módulo y como está el ambiente físico. • Se preparó una serie de preguntas orientadas a averiguar: cuales y como son los planes de continuidad del servicio, seguridad, operaciones y ambiente físico. • Estas preguntas se dividieron en entrevistas y listas de chequeo. • Se aplicó la entrevista. • Se revisó documentación sobre los planes. • Se aplicó la lista de chequeo para verificar que los planes si cumplan con los parámetros principales y que los funcionarios actúen acorde a los planes. • Se analizaron los resultados arrojados en las entrevistas y listas de chequeo.
		(DS4.3): Recursos Críticos de TI	
		(DS4.4): Mantenimiento del Plan de Continuidad de TI	
		(DS4.5): Pruebas del Plan de Continuidad de TI	
		(DS4.6): Entrenamiento del Plan de Continuidad de TI	
		(DS4.7): Distribución del Plan de Continuidad de TI	
		(DS4.8): Recuperación y Reanudación de los Servicios de TI	
		(DS4.9): Almacenamiento de Respaldos Fuera de las Instalaciones.	
		(DS4.10): Revisión Post Reanudación	
	(DS5): Garantizar la seguridad de los Sistemas	**(DS5.2):** Plan de Seguridad de TI	
		(DS5.3): Administración de Identidad	
		(DS5.4) Administración de Cuentas del Usuario	
		(DS5.5): Pruebas, Vigilancia y Monitoreo de la Seguridad	
		(DS5.7): Protección de la Tecnología de Seguridad	
		(DS5.8): Administración de Llaves Criptográficas	
		(DS5.9): Prevención, Detección y Corrección de Software Malicioso	
		(DS5.11): Intercambio de Datos Sensitivos	
	(DS11): Administración de datos	**(DS11.4):** Eliminación	
		(DS11.6): Requerimientos de Seguridad para la Administración de Datos	
	(DS12): Administración del Ambiente Físico	**(DS12.1):** Selección y Diseño del Centro de Datos	
		(DS12.2): Medidas de Seguridad Física	
		(DS12.3): Acceso Físico	
		(DS12.4): Protección Contra Factores Ambientales	

		(DS12.5): Administración de Instalaciones Físicas	
	(DS13): Administración de operaciones	**(DS13.1):** Procedimientos e Instrucciones de Operación	
		(DS13.2): Programación de Tareas	
		(DS13.5): Mantenimiento Preventivo del Hardware	

3.2.2. Plan de Auditoria

Tabla 2: Plan de Auditoria

				INSTRUMENTO DE RECOLECCION DE INFORMACION				
ITEM A EVALUAR	**DOMINIO**	**PROCESO**	**OBJETIVO DE CONTROL**	**Entrevista**	**Lista de Chequeo**	**Observación directa**	**Manuales y documentación**	**Fuente**
Seguridad	*Entrega y Soporte*	DS5 Garantizar la Seguridad de los Sistemas	DS5.2 Plan de Seguridad de TI					Jefe de sistemas-auxiliares del módulo-administrador del módulo.
			DS5.3 Administración de Identidad					
			DS5.4 Administración de Cuentas del Usuario					
			DS5.5 Pruebas, Vigilancia y Monitoreo de la Seguridad					
			DS5.7 Protección de la Tecnología de Seguridad					
			DS5.8 Administración de Llaves Criptográficas					
			DS5.9 Prevención, Detección y Corrección de					

			Software Malicioso					
		DS11 **Administración** de datos	DS11.4 Eliminación					
			DS11.6 Requerimientos de Seguridad para la Administración de Datos					
Recursos Humanos	*Planeación y Organización*	PO7 Administrar los Recursos Humanos de TI.	PO7.1 Reclutamiento y Retención del Personal					Jefe de Sistemas- Líder del módulo-Auxiliares-
			PO7.2 Competencias del personal					Líder del módulo.
			PO7.3 Asignación de Roles					Jefe de Sistemas- Líder del módulo-Auxiliares
			PO7.4 Entrenamiento del Personal de TI					
			PO7.5 Dependencia Sobre los Individuos					
			PO7.6 Procedimientos de Investigación del Personal					Líder del módulo.
			PO7.7 Evaluación del Desempeño del empleado					Jefe de Sistemas- Líder del módulo-Auxiliares

			PO7.8 Cambios y Terminación de Trabajo					Jefe de Sistemas-Líder del módulo.
Licenciamiento	*Adquirir e Implementar*	AI5 Adquirir Recurso de TI	AI5.2 Administración de Contratos con Proveedores					Jefe de Sistemas.
			AI5.3 Selección de Proveedores					
			AI5.4 Adquisión de Recursos de TI					
Continuidad del Servicio	*Entrega y Soporte*	DS4 Garantizar la Continuidad del Servicio	DS4.2 Planes de Continuidad de TI					Jefe de sistemas.
			DS4.3 Recursos Críticos de TI					jefe de sistemas-Administrador
			DS4.4 Mantenimiento del Plan de Continuidad de TI					
			DS4.5 Pruebas del Plan de Continuidad de TI					
			DS4.6 Entrenamiento del Plan de Continuidad de TI					
			DS4.7 Distribución del Plan de Continuidad de TI					

			DS4.8 Recuperación y Reanudación de los Servicios de TI					
			DS4.9 Almacenamiento de Respaldos Fuera de las Instalaciones					
			DS4.10 Revisión Post Reanudación					
Objetivos de la Organización	*Adquirir e Implementar*	AI1 Identificar soluciones automatizadas	AI1.1 Definición y Mantenimiento de los Requerimientos Técnicos y Funcionales del Negocio					Jefe de Sistemas
			AI1.2 Reporte de Análisis de Riesgos					
Uso del Software	*Adquirir e Implementar*	AI4 Facilitar la Operación y el Uso	AI4.1 Plan para Soluciones de Operación					Jefe de sistema-Líder del módulo-auxiliares.
			AI4.3 Transferencia de Conocimiento a Usuarios Finales					
			AI4.4 Transferencia de Conocimiento de Operaciones y Soporte					

Ambiente Físico	*Entrega y Soporte*	DS12 Administración del Ambiente Físico	DS12.1 Selección y Diseño del Centro de Datos					Jefe de sistema-auxiliares del módulo-ingeniero.
			DS12.2 Medidas de Seguridad Física					
			DS12.3 Acceso Físico					
			DS12.4 Protección Contra Factores Ambientales					
			DS12.5 Administración de Instalaciones Físicas					
Operaciones	Entrega y Soporte	DS13 Administración de operaciones	DS13.1 Procedimientos e Instrucciones de Operación					Jefe de sistema-Líder del módulo-auxiliares.
			DS13.2 Programación de Tareas					Jefe de sistemas- Líder del módulo.
			DS13.5 Mantenimiento Preventivo del Hardware					

Dominios Cobit Evaluados

- Entrega y soporte
- Planear y organizar
- Adquirir e implementar

3.2.3. Diseño de los elementos de auditoría

Formato de entrevista: en este se registra una serie de preguntas con respuestas abiertas, que se utilizan para tener conocimiento de cómo funcionan los procesos de una determinada entidad, y profundizar sobre cuáles son las fortalezas y debilidades de la organización.

- Tabla 3: Formato de Entrevista

Tipo de registro: Entrevista				
Entidad Auditada	Hospital Universitario Departamental de Nariño E.S.E			**Nº Guía: ENT6**
Área Auditada	Módulo de Citas Medicas	**Sistema**	Dinámica Gerencial Hospitalaria	
Responsable	Jaydivi Castillo			
Objetivo	Verificar que la transferencia de conocimiento se realice de forma constante y que exista la documentación y manuales de usuarios para TI			
Respondido por	Líder del módulo de citas medicas			
R/PT:	**EVI_AUDIO_16**			

Nº	**PREGUNTA**
1	¿La empresa realiza capacitaciones a las personas afectadas con la implementación de una nueva herramienta de TI? Justifique su respuesta.
2	¿La capacitación que se brinda a los usuarios finales permite que las aplicaciones sean utilizadas de una manera eficaz y eficiente, para apoyar los procesos que se llevan dentro de la organización? ¿Por qué?
3	¿Es presentada la información documental de las aplicaciones a los usuarios finales como lo es el manual de usuario?
4	¿Son consultados los manuales de las aplicaciones por los usuarios de estas?
5	¿Conoce usted si la empresa tiene establecido un plan a la hora de capacitar a los usuarios para el manejo de aplicaciones?
6	¿Cuál es el apoyo que se da a los usuarios cuando tienen problemas con las aplicaciones que se manejan dentro de la empresa?
7	¿Cómo ha sido la aceptación por parte de los interesados de los reportes que han sido presentados?

TIPO DE REGISTRO: Hace referencia a que tipo de instrumento para la recolección de la información se trata.

Nº GUÍA: Se refiere al número o ID del cuestionario.

ENTIDAD AUDITADA: Hace referencia a la entidad u organización donde se realizó aplicando o realizando el de la auditoria en nuestro caso es el Hospital Universitario Departamental de Nariño.

ÁREA AUDITADA: Hace referencia al lugar, área o proceso donde se realiza la auditoria en nuestro caso el Modulo de Citas Médicas el cual tiene su funcionamiento en el Call Center.

RESPONSABLE: Es el grupo auditor encargado de llevar a cabo el proceso de auditoría.

OBJETIVO: Razón u objeto por la cual se realiza la dicho cuestionario

Sistema: Indica el software donde se está realizando el proceso de auditoria en nuestro caso el SISTEMA DE INFORMACION DINAMICA GERENCIAL HOSPITALARIA (DGH)

RESPONDIDO POR: Es la persona a la cual se le realiza

PREGUNTA: Espacio donde se indica la descripción dela consulta de la cual se indagara

R/PT: Respuestas papeles de trabajo y evidencias tomadas.

ENT: Numero referencias de la entrevista

Formato de Lista de Chequeo: es una lista de comprobación, que contiene preguntas, que sirven para inspeccionar si se cumple o no con ciertos requerimientos relacionados con los procesos desarrollados en una organización.

- Tabla 4: Formato Lista de Chequeo

Tipo de registro: Lista de Chequeo				**R/PT:**
Entidad Auditada	Hospital Universitario Departamental de Nariño E.S.E			**Nº Guía: LC4**
Área Auditada	Módulo de Citas Medicas	**Sistema**	Dinámica Gerencial Hospitalaria	
Responsable	Jaydivi Castillo Guerrero			
Objetivo	Verificar que la transferencia de conocimiento se realice de forma constante y que exista la documentación y manuales de usuario de TI, para el uso y manejo del módulo de citas médicas.			

Nº	**PREGUNTA**	**C**	**NC**	**N/A**
1	¿Se cuenta con un documento donde se pueda identificar los aspectos técnicos y la capacidad de operación del software?		X	
2	¿Se transfiere el conocimiento y habilidades al personal de administración y operaciones del módulo de citas médicas?	X		
3	Al momento de realizar la transferencia de conocimiento, los documentos de entrenamiento son entregados a los usuarios finales?		X	
4	Se realiza el entrenamiento continuo al personal de administración y operaciones del módulo para la transferencia de conocimiento.		X	
5	La transferencia de conocimiento se les realiza a todos los operadores del módulo de citas médicas.	X		
6	Existe una guía de procedimientos formales para el manejo del modulo	X		
7	Puede el administrador del módulo de citas médicas modificar los datos de entrada	X		
8	Cuentan los operadores del módulo de citas con una bitácora para mantener un registro de cualquier evento y acción tomado por ellos	X		

TIPO DE REGISTRO: Hace referencia a que tipo de instrumento para la recolección de la información se trata.

Nº DE GUÍA: Se refiere al número o ID del cuestionario.

ENTIDAD AUDITADA: Hace referencia a la entidad u organización donde se realizó aplicando o realizando el proceso de la auditoria en nuestro caso es el Hospital Universitario Departamental de Nariño.

ÁREA AUDITADA: Hace referencia al lugar, área o proceso donde se realiza la auditoria en nuestro caso el Modulo de Citas Médicas.

SISTEMA: Indica el software donde se está realizando el proceso de auditoria en nuestro caso el SISTEMA DE INFORMACION DINAMICA GERENCIAL HOSPITALARIA (DGH)

RESPONSABLE: Es el grupo auditor encargado de llevar a cabo el proceso de auditoría.

OBJETIVO: Razón u objeto por la cual se realiza la dicho cuestionario

LC2: Número Referencia de la lista de chequeo.

C: Conforme

NC: No conforme

NA: No aplica

R/PT: Respuestas papeles de trabajo y evidencias tomadas.

Formato de Hallazgos: se registran las deficiencias que se encontraron en el proceso de auditoría que finalmente se convierten en el resultado de esta, y son aspectos que se deben informar a la administración de la organización para que sean corregidos ya que pueden afectar de forma negativa el desarrollo normal de los procesos.

- Tabla 5: Formato de Hallazgos HUDN

Tipo de registro: Hallazgos de Auditoria				
Entidad Auditada	Hospital Universitario Departamental de Nariño E.S.E			**Nº Guía: H11**
Área Auditada	Módulo de Citas Medicas	Sistema	Dinámica Gerencial Hospitalaria	
Responsable	Jaydivi Castillo			
R/PT:	Entrevista: **ENT6_Nº Preg 3** Lista de Chequeo: **LC4_NºPreg 3, 4** Lista de Chequeo: **LC5_NºPreg 9** **EVI_AUDIO_16** **P11**			

Dominio	Adquirir e Implementar
Procesos	AI4 Facilitar la Operación y Uso
Objetivo de Control	AI4.3 Transferencia de Conocimiento a Usuarios Finales
Riesgos Asociados	Al no capacitar al personal de reemplazo genera riesgo como: ✓ el represamiento del trabajo. ✓ errores en la ejecución del software como por ejemplo ingreso de datos erróneos y por consiguiente incorrecta asignación de citas o de turnos médicos.
Descripción	
• Los funcionarios no tienen los manuales de usuario de las aplicaciones instaladas en los equipos del Call Center. • Al no existir información documental de la aplicación las auxiliares del módulo no tienen una herramienta de consulta.	
Recomendación	
• La oficina de gestión de información debe elaborar un manual de usuario que facilite el conocimiento sobre: ✓ cuáles son los datos del entrada,	

✓ como se debe obtener los resultados ✓ cuáles son los datos de salida ✓ como son los formatos de los documentos ✓ en qué momento se debe pedir una operación o una información específica. • El manual de usuario debe ser redactado en forma clara e ir de acuerdo al tipo de usuario que usa el sistema y debe entregarse como parte del entrenamiento de las funcionarias oficiales y del personal de reemplazo.
Causa
• El manual de usuario del aplicativo que tiene la oficina de gestión de Información no es distribuido entre los funcionarios. • La coordinación de gestión de información afirma que la capacitación inicial que se dio a los funcionarios es suficiente para comprender el software. • El manual de usuario que tiene la organización es de autoría del SYAC desarrollador del Sistema Dinámica Gerencial y Hospitalaria, por lo tanto es un manual que no está diferenciado de acuerdo a los perfiles de usuario.
Nivel de riesgo
En cuanto a la probabilidad de ocurrencia está clasificada en alto, y el impacto es alto.

TIPO DE REGISTRO: Hace referencia a que tipo de instrumento para la recolección de la información se trata.

ENTIDAD AUDITADA: Hace referencia a la entidad u organización donde se realizó aplicando o realizando el proceso de la auditoria en nuestro caso es el Hospital Universitario Departamental de Nariño.

Nº GUÍA: Se refiere al número o ID del cuestionario.

ÁREA AUDITADA: Hace referencia al lugar, área o proceso donde se realiza la auditoria en nuestro caso el Modulo de Citas Médicas.

SISTEMA: Indica el software donde se está realizando el proceso de auditoria en nuestro caso el SISTEMA DE INFORMACION DINAMICA GERENCIAL HOSPITALARIA (DGH).

RESPONSABLE: Es el grupo auditor encargado de llevar a cabo el proceso de auditoría.

R/PT: Respuestas papeles de trabajo y evidencias tomadas.

DOMINIO: Hace referencia a que dominio se evaluó siguiendo la metodología del COBIT.

PROCESO: Hace referencia a los procesos evaluados y donde re realizaron los hallazgos según la metodología del COBIT.

OBJETIVO DE CONTROL: Hace referencia a los objetivos de control evaluados dentro de cada proceso según la metodología del COBIT.

RIESGOS ASOCIADOS: En este campo se describen los riesgos que puede tener o que ya tiene la organización y en específico el Modulo de Citas Médicas.

DESCRIPCIÓN: En este campo se realiza la descripción de los hallazgos encontrado.

RECOMENDACIÓN: Aquí se realizan las recomendaciones necesarias de acuerdo a los hallazgos encontrados o a la descripción.

CAUSA: En este campo se describen las causas del hallazgo.

NIVEL DE RIESGO: Este campo hace referencia a los niveles de riesgo que está expuesta la organización y en específico el Módulo de Citas Médicas.

Formato de prueba: se registran los hechos comprobados y que sustentan los hallazgos encontrados y sirven para respaldar el resultado de la auditoria a través de evidencias.

Tabla 6: Formato Guía de Prueba

Tipo de registro: Guía de Pruebas				
Entidad Auditada	Hospital Universitario Departamental de Nariño E.S.E			**Nº Guía: P11**
Área Auditada	Módulo de Citas Medicas	Sistema	Dinámica Gerencial Hospitalaria	
R/PT:	Entrevista: **ENT6_Nº Preg 3** Lista de Chequeo: **LC4_NºPreg 3, 4** Lista de Chequeo: **LC5_NºPreg 9**			

Dominio	Adquirir e Implementar	
Procesos	AI4 Facilitar la Operación y Uso	
Objetivo de Control	AI4.3 Transferencia de Conocimiento a Usuarios Finales	
Riesgos Asociados	Al no capacitar al personal de reemplazo genera riesgo como: ✓ el represamiento del trabajo. ✓ errores en la ejecución del software como por ejemplo ingreso de datos erróneos y por consiguiente incorrecta asignación de citas o de turnos médicos.	
No.	**Evidencia**	**Descripción**
1	EVI_AUDIO_16 **Anexo No. XX:** Manual de Capacitación y Soporte	No se les presenta la información documentada o manual de usuarios del aplicativo a las auxiliares del módulo de citas médicas.
2		No se les realiza capacitaciones o entrenamiento continuo a las auxiliares para la transferencia de conocimiento.

TIPO DE REGISTRO: Hace referencia a que tipo de instrumento para la recolección de la información se trata.

ENTIDAD AUDITADA: Hace referencia a la entidad u organización donde se realizó aplicando o realizando el proceso de la auditoria en nuestro caso es el Hospital Universitario Departamental de Nariño.

Nº GUÍA: Se refiere al número o ID del cuestionario.

ÁREA AUDITADA: Hace referencia al lugar, área o proceso donde se realiza la auditoria en nuestro caso el Modulo de Citas Médicas.

SISTEMA: Indica el software donde se está realizando el proceso de auditoria en nuestro caso el SISTEMA DE INFORMACION DINAMICA GERENCIAL HOSPITALARIA (DGH).

RESPONSABLE: Es el grupo auditor encargado de llevar a cabo el proceso de auditoría.

DOMINIO: Hace referencia a que dominio se evaluó siguiendo la metodología del COBIT.

PROCESO: Hace referencia a los procesos evaluados y donde re realizaron los hallazgos según la metodología del COBIT.

OBJETIVO DE CONTROL: Hace referencia a los objetivos de control evaluados dentro de cada proceso según la metodología del COBIT.

RIESGOS ASOCIADOS: En este campo se describen los riesgos que puede tener o que ya tiene la organización y en específico el Modulo de Citas Médicas.

N°: Hace referencia al número de evidencia

R/PT: Respuestas papeles de trabajo y evidencias tomadas.

EVIDENCIA: Hace referencia a la evidencia encontrada en el hallazgo.

DESCRIPCIÓN: En este campo se realiza la descripción de la evidencia encontrada.

3.3. HALLAZGOS

A continuación, se describen los hallazgos encontrados en el Módulo de Citas Médicas del sistema de información Dinámica Gerencial Hospitalaria (DGH) en el Hospital Universitario Departamental de Nariño.

3.3.1. Dominios y procesos auditados en el módulo de citas médicas en el Hospital Universitario Departamental de Nariño E.S.E

Los hallazgos encontrados en el Modulo de Citas Médicas del sistema de información Dinámica Gerencial Hospitalaria (DGH) se presentan a continuación los dominios y procesos que fueron auditados:

- **DOMINIO: PLANEAR Y ORGANIZAR (PO)**
  - ✓ Administración de los Recursos Humanos (PO7)

- **DOMINIO: ADQUIRIR E IMPLEMENTAR (AI)**
  - ✓ Identificar Soluciones Automatizadas (AI1)
  - ✓ Facilitar la Operación y el Uso (AI4)
  - ✓ Administrar Recursos de TI (AI5)

- **DOMINIO: ENTREGA Y SOPORTE (DS)**
  - ✓ Garantizar la Continuidad del Servicio (DS4)
  - ✓ Garantizar la Seguridad de los Sistemas (DS5)
  - ✓ Administración de datos (DS11)
  - ✓ Administración del Ambiente Físico (DS12)
  - ✓ Administración de Operaciones (DS13)

ITEM	No.	HALLAZGO	RIESGO	PROBABILIDAD	IMPACTO
SEGURIDAD	1	• Las auxiliares del módulo de citas médicas no tienen una cuenta de usuario para iniciar sesión en el sistema operativo y la documentación que se encuentra en una de las particiones del sistema operativo está expuesta. • Las auxiliares del módulo no cambian la contraseña del sistema cada 6 meses, desde el punto de vista de las funcionarias no ha sido necesario, aunque este requisito de seguridad si está contemplado dentro del plan general de gestión de información de la institución. • En la política general de gestión de información no se tienen contempladas en que situaciones se debe hacer un cambio urgente de contraseña.	➢ La organización queda expuesta a riesgos de robo de documentación y archivos importantes que son vitales para el hospital. ➢ Al no hacerse un cambio periódico de contraseña el sistema está expuesto a que algún atacante pueda adivinar la contraseña.	**ALTA**	**ALTO**
	2	• Las auxiliares del módulo como la líder de este no han firmado ni renovado el acuerdo de cumplimiento sobre la seguridad y confidencialidad de la información. Dentro de este punto se incluye la falta de una firma que comprometa a los funcionarios a no revelar la contraseña. • A los funcionarios que trabajan en el área de citas médicas no se les hace entrega de un documento que contenga cuáles son sus derechos de acceso de acuerdo a su perfil. • Periódicamente la coordinación de gestión de información no hace revisión de los derechos de acceso establecidos por el sistema.	➢ La organización queda expuesta a riesgos relacionados con que los funcionarios puedan llevarse un reporte de datos o información confidencial o reservada.	**ALTA**	**ALTO**
	3	• Las personas externas que ingresan al Call center utilizan los equipos para asuntos personales. • Facebook está habilitado en los equipos del Call center	➢ La distracción interrumpe el desarrollo normal de los procesos en el módulo de citas médicas. **Al estar personas externas en el área:** ➢ La organización queda expuesta a riesgos de robo de documentación y archivos importantes que son vitales para el hospital. ➢ La visualización de información del sistema o de documentos que se encuentren sobre el escritorio que pueden ser críticos para la organización.	**ALTA**	**ALTO**

ITEM	No.	HALLAZGO	RIESGO	PROBABILIDAD	IMPACTO
SEGURIDAD	4	• Personas ajenas a las funcionarias del Call center utilizan el teléfono para asuntos personales. • Además el puesto de trabajo es utilizado por las funcionarias y personas externas para almorzar. • El puesto de trabajo es utilizado por las funcionarias y personas externas para mirar revistas de catálogo. • Las auxiliares del módulo de citas médicas no cierran ni bloquean el sistema al ausentarse por un momento del puesto de trabajo. • El equipos utilizados en Call Center no se tiene desactivado el panel de control • Los documentos que se dejan en el escritorio no se retiran al ausentarse del puesto de trabajo. • Se permite la conexión de dispositivos usb a los equipos del Call center.	➢ La distracción genera riesgos como: se interrumpe el desarrollo normal de los procesos en el módulo de citas médicas. ➢ El comer en el puesto de trabajo generaría accidentes como: derramar alimento sobre los equipos. **Al estar personas externas en el área:** ➢ La organización queda expuesta a riesgos de robo de documentación y archivos importantes que son vitales para el hospital. ➢ La visualización de información del sistema o de documentos que se encuentren sobre el escritorio que pueden ser críticos para la organización. ➢ Cambios en la configuración del equipo y desinstalación de alguna aplicación	**ALTA**	**ALTO**

ITEM	No.	HALLAZGO	RIESGO	PROBABILIDAD	IMPACTO
RECURSOS HUMANOS	5	• Aunque existe personal que reemplace a las auxiliares del módulo en el momento que ocurre ausencia temporal de estas funcionarias, esto genera contratiempos porque se debe hacer una inducción al personal de reemplazo sobre el manejo del módulo empezando por lo complejo que es el conocimiento de todos los médicos del Hospital Universitario Departamental de Nariño E.S.E. • No se tienen en cuenta los conocimientos de las funcionarias encargadas de manejo del módulo de citas médicas, para ser aprovechado posteriormente en la probabilidad de que estas funcionarias abandonen el cargo.	• Al no capacitar al personal de reemplazo genera riesgo como: ✓ el represamiento del trabajo. ✓ errores en la ejecución del software como por ejemplo ingreso de datos erróneos y por consiguiente incorrecta asignación de citas o de turnos médicos.	**ALTA**	**ALTO**
	6	• Las auxiliares del módulo de citas médica hacen caso omiso a las normas y reglamentaciones para el subproceso del Call center ya establecidas por la Junta Directiva como de la Coordinación de Urgencias, Consulta Externa y Coordinación de Gestión de información.	➢ Este represamiento de información lleva a la acumulación de trabajo afectando el desarrollo dinámico de la asignación de citas	**ALTA**	**ALTO**
CONTINUIDAD DEL SERVICIO	7	• No se lleva un control sobre el tiempo perdido por el usuario debido a interrupciones en el servicio ocasionadas por factores que afectan a la seguridad del edificio y los que afectan la integridad de los datos. • No se tiene un registro sobre los errores más comunes que permitan un análisis de probabilidad de ocurrencia de fallas en el área de citas médicas.	Al no existir control sobre las contingencias que se presentan, la administración no sabrá con certeza que problemas se presentan con mayor frecuencia y por lo tanto no habrá una toma correcta de decisiones, ya que no hay un dato de referencia que indique como está el problema en un periodo de tiempo y por lo tanto no se identifica cual es la causa del problema, aumentando los costos para la organización.	**ALTA**	**ALTO**

ITEM	No.	HALLAZGO	RIESGO	PROBABILIDAD	IMPACTO
CONTINUIDAD DEL SERVICIO	8	• Actualmente el módulo de citas médicas no cuenta con una alternativa que permita la continuidad del desarrollo de los procesos en caso de una falla total en el sistema principal. • No se han llevado pruebas que demuestren la eficacia del plan de recuperación de datos ante cualquier desastre. • No se tiene contemplado un informe que describa las acciones que se tomaron después de recuperado el sistema • No se han puesto a pruebas los planes de continuidad del servicio del módulo de citas médicas para verificar si son efectivos.	➢ Al no existir una alternativa que permita la continuidad del desarrollo de los procesos en el módulo de citas médicas, se generan los siguientes riesgos: la suspensión del servicio de citas y de turnos, y la suspensión de solicitudes de historias clínicas. ➢ Este represamiento de información lleva a la acumulación de trabajo afectando el desarrollo dinámico de la asignación de citas. ➢ El no probar el plan de recuperación de datos genera riesgo de pérdida total o parcial de datos.	**ALTA**	**ALTO**
	9	Las auxiliares del módulo de citas médicas no conocen de la existencia de un plan de continuidad o de contingencia de los recursos de TI involucrados en el módulo de citas y en la organización en general.	➢ Al no existir una alternativa que permita la continuidad del desarrollo de los procesos en el módulo de citas médicas, se generan los siguientes riesgos: la suspensión del servicio de citas y de turnos, y la suspensión de solicitudes de historias clínicas. ➢ Este represamiento de información lleva a la acumulación de trabajo afectando el desarrollo dinámico de la asignación de citas	**ALTA**	**ALTO**

ITEM	No.	HALLAZGO	RIESGO	PROBABILIDAD	IMPACTO
OBJETIVOS DE LA ORGANIZACION	10	No existe un estudio particular sobre las necesidades o requerimientos de hardware, software y procedimientos del área de citas médicas.	➢ Al no existir un análisis de requerimientos puede ocasionar riesgos como fallas continuas en el sistema ya que estas no se corrigen. ➢ Al no existir un análisis de requerimientos puede ocasionar riesgos como costos elevados para la organización ya que si el software no cumplió las expectativas de trabajo se debe pensar en otro.	**ALTA**	**ALTO**
USO DEL SOFTWARE	11	• Los funcionarios no tienen los manuales de usuario de las aplicaciones instaladas en los equipos del Call Center. • Al no existir información documental de la aplicación las auxiliares del módulo no tienen una herramienta de consulta.	Al no capacitar al personal de reemplazo genera riesgo como: ✓ el represamiento del trabajo. ✓ errores en la ejecución del software como por ejemplo ingreso de datos erróneos y por consiguiente incorrecta asignación de citas o de turnos médicos.	**ALTA**	**ALTO**
	12	• No existe documentación sobre los aspectos técnico del sistema Dinámica Gerencial Hospitalaria. • Las auxiliares del Call Center tienen habilitadas todas las funcionalidades del módulo de citas médicas del aplicativo DGH, a pesar de que algunas de sus funcionalidades no son de su competencia.	Una incorrecta instalación del software lleva a que el sistema trabaje erróneamente arrojando posibles datos equivocados y por ende el trabajo se puede ver afectado.	**BAJA**	**MEDIO**
	13	• Las auxiliares del Call Center tienen habilitadas todas las funcionalidades del módulo de citas médicas del aplicativo DGH, a pesar de que algunas de sus funcionalidades no son de su competencia.	Existe el riesgo de que personas propias o ajenas a la organización introduzcan datos que afecten el procesamiento de la información, por ejemplo el ingreso de datos falsos.	**ALTA**	**ALTO**

ITEM	No.	HALLAZGO	RIESGO	PROBABILIDAD	IMPACTO
AMBIENTE FISICO	14	• El aviso de alarma de evacuación no tiene una correcta visualización ya que sobre él hay una mesa de escritorio. • Dentro del área no existen equipos extintores como tampoco una salida de emergencia. El extintor más cercano se encuentra fuera del Call Center. • El área del Call Center está ubicado en un lugar con demasiado ruido.	➢ La inadecuada colocación de señales en el lugar de trabajo puede disminuir la productividad porque habría riesgo de lesión en el personal en el momento de que ocurra una desgracia. ➢ Al no haber un extintor en el área puede haber riesgos de pérdidas de vida, aunque exista un extintor cercano es probable que en un momento de emergencia la salida se pueda obstruir.	**ALTA**	**ALTO**
	15	• El diagrama de procesos esta desactualizado. • Solamente la organización tiene el diagrama de procesos para asignación de citas por EPS y no se tiene el diagrama para asignación de citas a particulares. • En un principio se dijo que la tarea de asignación de turno era una labor en conjunto del administrador del módulo de citas médicas con la líder del mismo, pero las funcionarias del Call Center también deben hacer esa tarea. • El encargado de la administración del Módulo de Citas Médicas no ejerce sus funciones porque se cree que no hay problemas dentro del módulo, y por lo tanto quien tiene más conocimiento según el propio administrador del módulo es el coordinador de gestión de información del hospital.	➢ Al no existir coordinación entre quienes dirigen el módulo de citas médicas puede provocar suspensión del servicio de citas, por la confusión de los usuarios.	**ALTA**	**ALTO**
FUNCIONAMIENTO	16	• La contraseña que asigna por defecto el sistema cuando la restablece se repite en usuarios diferentes ya sea que tengan perfil de administrador o usuario convencional. • Al llenar el código del paciente con caracteres alfabéticos no tiene ningún aviso de error previo, el error aparece solo hasta que se guarda al paciente en la base de datos. • Dos funcionalidades: la creación de médico y creación de especialistas se repiten en dos modulo, Historias clínicas y Citas médicas.	➢ La repetición de la contraseña que se asigna por defecto genera el siguiente riesgo: relacionado con que la organización queda expuesta a riesgos relacionados con que los funcionarios puedan llevarse un reporte de datos o información confidencial o reservada.	**ALTA**	**ALTO**

Tabla 7: Matriz de Riesgos

MATRIZ DE RIESGOS

PROBABILIDAD				
	Alta			H1,H2,H3,H4, H5,H6,H7,H8, H9,H10,H11,H13, H14,H15,H16
	Media			
	Baja		H12	
		Bajo	***Medio***	***Alto***
		IMPACTO		

Riesgos que no serán tomados en cuenta

Riesgos de mayor impacto y mayor probabilidad

3.3.2. Hallazgos en el módulo de citas médicas del Hospital Universitario Departamental de Nariño E.S.E

Referencia a los papeles de trabajo

En la celda R/PT se encuentra las evidencias que sustentan los hallazgos. Las evidencias pueden estar en ocho formas: en entrevista, en lista de chequeo, en audio, en video, en imágenes, en fotografías, anexos y en el formato de pruebas.

Referencia a entrevistas y lista de chequeo:

Si en la celda R/PT aparece: CUESTIONARIOS/Lista de Chequeo o CUESTIONARIOS/Entrevista se debe dirigir al CD y buscar la carpeta CUESTIONARIOS dentro de la cual se encontrara dos archivos tipo Word uno de ellos llamado lista de chequeo y otro entrevista.

Cada lista de chequeo y entrevista contiene un numero de guía, si es una entrevista tendrá **ENTXX** y el número de la pregunta.

Referencia a audio, fotografías, videos, imágenes:

Si en la celda R/PT aparece: EVIDENCIA FOTOGRAFICA/EVI_FOTO_XX, se debe dirigir al CD y buscar la carpeta EVIDENCIA FOTOGRAFICA y buscarla la fotografía según el número que aparezca en el formato de hallazgo.

Si en la celda R/PT aparece: EVIDENCIA EN AUDIO/EVI_AUDIO_XX, se debe dirigir al CD y buscar la carpeta EVIDENCIA EN AUDIO y buscarla el audio según el número que aparezca en el formato de hallazgo.

Si en la celda R/PT aparece: EVIDENCIA EN VIDEO/EVI_VIDEO_XX, se debe dirigir al CD y buscar la carpeta EVIDENCIA EN VIDEO y buscarla EL video según el número que aparezca en el formato de hallazgo.

Si en la celda R/PT aparece: EVIDENCIA IMÁGENES/EVI_IMG_X, se debe dirigir al CD y buscar la carpeta EVIDENCIA IMÁGENES y buscar la imagen según el número que aparezca en el formato de hallazgo.

Referencia a anexos:

Si en la celda R/PT aparece: **ANEXO No. 1-** o hasta el **ANEXO No. 10 -**, se debe dirigir al CD y buscar el anexo según el número que aparezca en el formato de hallazgo.

Del **ANEXO No. 11-** en adelante se debe dirigir en este documento en la parte de **ANEXOS.**

Referencia a formato de pruebas

Si en la celda R/PT aparece: **PXX** se debe dirigir a este mismo documento y buscar la guía de prueba según el número que aparezca en el formato de hallazgo.

NOTA: En la guía de pruebas aparecen de la misma forma las evidencias.

HALLAZGOS DE SEGURIDAD

Tabla 8: Hallazgo 1 HUDN

Tipo de registro: Hallazgos de Auditoria				
Entidad Auditada	Hospital Universitario Departamental de Nariño E.S.E			**Nº Guía: H1**
Área Auditada	Módulo de Citas Medicas	Sistema	Dinámica Gerencial Hospitalaria	
Responsable	Joana Marcela Narváez Ordoñez			
R/PT:	CUESTIONARIOS/Lista de Chequeo: **LC2_Nº Preg 1, 6, 8 ANEXO No. 6- POLITICA DE GESTION DE INFORMACION P1**			

Dominio	Entrega y Soporte
Procesos	DS5 Garantizar la Seguridad de los Sistemas
Objetivo de Control	DS5.2 Plan de Seguridad de TI DS5.3 Administración de Identidad DS5.4 Administración de Cuentas del Usuario
Riesgos Asociados	• La organización queda expuesta a riesgos de robo de documentación y archivos importantes que son vitales para el hospital. • Al no hacerse un cambio periódico de contraseña el sistema está expuesto a que algún atacante pueda adivinar la contraseña.

Descripción

- Las auxiliares del módulo de citas médicas no tienen una cuenta de usuario para iniciar sesión en el sistema operativo y la documentación que se encuentra en una de las particiones del sistema operativo está expuesta.
- Las auxiliares del módulo no cambian la contraseña del sistema cada 6 meses, desde el punto de vista de las funcionarias no ha sido necesario, aunque este requisito de seguridad si está contemplado dentro del plan general de gestión de información de la institución.
- En la política general de gestión de información no se tienen contempladas en que situaciones se debe hacer un cambio urgente de contraseña.

Recomendación

• En la política general de gestión de información se debe añadir como política de control de claves de acceso: crear una cuenta de usuario para iniciar sesión en el Sistema Operativo, y la contraseña correspondiente a la cuenta de usuario debe cumplir los mismos parámetros establecidos para el sistema Dinámica Gerencial Hospitalaria como son:
 	
  • La longitud mínima de la contraseña debe ser como mínimo de cuatro caracteres.
 	
  • La contraseña debe ser compleja es decir debe contener al menos una letra, un número y un carácter especial y debe ser diferente al nombre del usuario.
 	
• El personal de gestión de información y en concreto el administrador del módulo de citas médicas debe hacer cumplir las políticas de contraseña.
 	
• El personal deber concientizado en las sesiones de capacitación sobre la importancia del cambio de contraseña.
 	
• En la política general de gestión de información se debe añadir como política de contraseña las situaciones o eventos en que se debe cambiar la contraseña por ejemplo: ataque al sistema, cambio de momentáneo de personal, entrada de terceros al sistema.

Causa
• Las auxiliares del módulo por razones de seguridad no tienen el permiso para hacer cambios en sus equipos, este tipo de cambio debe solicitarse al líder del módulo. • El administrador del módulo no hace un control continuo de las actividades de seguridad que deben llevarse a cabo. • No existe un control que advierta a los funcionarios cuando es el tiempo de cambio de contraseña. • Desconocimiento de las funcionarias de la política de contraseña o de los riesgos de seguridad a que se expone la organización.
Nivel de riesgo
En cuanto a la probabilidad de ocurrencia está clasificada en alto, y el impacto es alto.

Tabla 9: Hallazgo 2 HUDN

Tipo de registro: Hallazgos de Auditoria				
Entidad Auditada	Hospital Universitario Departamental de Nariño E.S.E			**Nº Guía: H2**
Área Auditada	Módulo de Citas Medicas	Sistema	Dinámica Gerencial Hospitalaria	
Responsable	Joana Marcela Narváez Ordoñez			
R/PT:	CUESTIONARIOS/Lista de Chequeo: **LC1_Nº Preg 14, 18, 21** CUESTIONARIOS/Lista de Chequeo: **LC2_Nº Preg 4** **ANEXO No. 6- POLITICA DE GESTION DE INFORMACION P2**			

Dominio	Entrega y Soporte
Procesos	DS5 Garantizar la Seguridad de los Sistemas
	DS11 Administración de datos
Objetivo de Control	DS5.7 Protección de Tecnología de Seguridad
	DS11.6 Requerimientos de seguridad para la administración de datos
Riesgos Asociados	La organización queda expuesta a riesgos relacionados con que los funcionarios puedan llevarse un reporte de datos o información confidencial o reservada.
Descripción	
• Las auxiliares del módulo como la líder de este no han firmado ni renovado el acuerdo de cumplimiento sobre la seguridad y confidencialidad de la información. Dentro de este punto se incluye la falta de una firma que comprometa a los funcionarios a no revelar la contraseña. • A los funcionarios que trabajan en el área de citas médicas no se les hace entrega de un documento que contenga cuáles son sus derechos de acceso de acuerdo a su perfil. • Periódicamente la coordinación de gestión de información no hace revisión de los derechos de acceso establecidos por el sistema.	
Recomendación	
• La información se considera como uno de los activos principales del negocio por tal razón es recomendable incluir en los contratos laborables acuerdos o anexar pactos de confidencialidad que establezcan claramente las obligaciones de los trabajadores en ese sentido, con estos acuerdos informamos a los funcionarios de las pautas a seguir en el tratamiento de la información confidencial, y se debe renovar estos	

pactos anualmente para confirmar la obligación de los trabajadores a no revelar ningún tipo de información. • Elaborar un documento sobre los derechos de acceso de todos los funcionarios del hospital, este documento debe ser redactado de acuerdo a los módulos establecidos en la organización, además debe ser distribuido a los funcionarios de acuerdo a su perfil.
Causa
La falta de control de gestión de información y del administrador del módulo de citas médicas sobre las prácticas de seguridad básicas para evitar robo de información, hace que las funcionarias desconozcan las normas principales de seguridad.
Nivel de riesgo
En cuanto a la probabilidad de ocurrencia está clasificada en alto y el impacto es alto.

Tabla 10: Hallazgo 3 HUDN

Tipo de registro: Hallazgos de Auditoria				
Entidad Auditada	Hospital Universitario Departamental de Nariño E.S.E			**Nº Guía: H3**
Área Auditada	Módulo de Citas Medicas	Sistema	Dinámica Gerencial Hospitalaria	
Responsable	Joana Marcela Narváez O.			
R/PT:	CUESTIONARIOS/Lista de Chequeo: **LC1_Nº Preg 31** EVIDENCIA FOTOGRAFICA**/EVI_FOTO_4** EVIDENCIA FOTOGRAFICA/**EVI_FOTO_8** EVIDENCIA FOTOGRAFICA/**EVI_FOTO_9** **P3**			

Dominio	Entrega y Soporte
Procesos	DS5 Garantizar la Seguridad de los Sistemas
Objetivo de Control	DS5.2 Plan de Seguridad de TI DS5.5 Pruebas, Vigilancia y Monitoreo de la Seguridad
Riesgos Asociados	• La distracción interrumpe el desarrollo normal de los procesos en el módulo de citas médicas. **Al estar personas externas en el área:** • La organización queda expuesta a riesgos de robo de documentación y archivos importantes que son vitales para el hospital. • La visualización de información del sistema o de documentos que se encuentren sobre el escritorio que pueden ser críticos para la organización.

Descripción

- Las personas externas que ingresan al Call center utilizan los equipos para asuntos personales.

- Facebook está habilitado en los equipos del Call center, violando la política 5 de gestión de información sobre el manejo de correo electrónico, herramienta y uso del internet:

  ✓ El uso de Internet estará restringido según políticas de seguridad informática de la organización, desde el área de Gestión de Información se administran todos los accesos a Internet de los funcionarios que lo necesiten, evitando de esta forma colapsar el servicio de Internet.

✓ El correo interno y el uso de Internet deben ser utilizados exclusivamente en las operaciones de la organización.
Recomendación
• El coordinador de gestión de información debe hacer cumplir las sanciones establecidas en la política 5 de gestión de información sobre el manejo de correo electrónico, herramienta y uso del internet: *El usuario que sea sorprendido según el reporte diario del webmaster visitando sitios no autorizados por la empresa, en primera instancia se le hará el llamado de atención, en el segundo intento se le suspenderá el servicio como sanción a lo dispuesto en este documento.* • La oficina de gestión de información debe bloquear las páginas que no están autorizadas. • Sensibilizar a todo el personal sobre la importancia de la seguridad en el puesto de trabajo.
Causa
Las auxiliares del Call center y personas ajenas no son supervisados para controlar este tipo de acciones.
Nivel de riesgo
En cuanto a la probabilidad de ocurrencia está clasificada en alto, y el impacto es alto

Tabla 11: Hallazgo 4 HUDN

Tipo de registro: Hallazgos de Auditoria				
Entidad Auditada	Hospital Universitario Departamental de Nariño E.S.E			**Nº Guía: H4**
Área Auditada	Módulo de Citas Medicas	Sistema	Dinámica Gerencial Hospitalaria	
Responsable	Joana Marcela Narváez Ordoñez.			
R/PT:	CUESTIONARIOS/Lista de Chequeo: **LC3_Nº Preg 6, 8** **ANEXO No. 6- POLITICA DE GESTION DE INFORMACION** EVIDENCIA FOTOGRAFICA**/EVI_FOTO_1** EVIDENCIA FOTOGRAFICA**/EVI_FOTO_2** EVIDENCIA FOTOGRAFICA/**EVI_FOTO_3** EVIDENCIA FOTOGRAFICA**/EVI_FOTO_5** EVIDENCIA FOTOGRAFICA/**EVI_FOTO_9** EVIDENCIA FOTOGRAFICA**/EVI_FOTO_11** EVIDENCIA FOTOGRAFICA**/EVI_FOTO_15** EVIDENCIA FOTOGRAFICA**/EVI_FOTO_17** EVIDENCIA FOTOGRAFICA**/EVI_FOTO_18** EVIDENCIA FOTOGRAFICA**/EVI_FOTO_19** **P4**			

Dominio	Entrega y Soporte
Procesos	DS5 Garantizar la Seguridad de los Sistemas
Objetivo de Control	DS5.2 Plan de Seguridad de TI DS5.5 Pruebas, Vigilancia y Monitoreo de la Seguridad
Riesgos Asociados	• La distracción genera riesgos como: se interrumpe el desarrollo normal de los procesos en el módulo de citas médicas. • El comer en el puesto de trabajo generaría accidentes como: derramar alimento sobre los equipos. **Al estar personas externas en el área:** • La organización queda expuesta a riesgos de robo de documentación y archivos importantes que son vitales para el hospital. • La visualización de información del sistema o de documentos que se encuentren sobre el escritorio que pueden ser críticos para la organización.

	• Cambios en la configuración del equipo y desinstalación de alguna aplicación

Descripción

- Personas ajenas a las funcionarias del Call center utilizan el teléfono para asuntos personales.

- Además el puesto de trabajo es utilizado por las funcionarias y personas externas para almorzar.

- El puesto de trabajo es utilizado por las funcionarias y personas externas para mirar revistas de catálogo.

- Las auxiliares del módulo de citas médicas no cierran ni bloquean el sistema al ausentarse por un momento del puesto de trabajo.

- El equipos utilizados en Call Center no se tiene desactivado el panel de control

- Los documentos que se dejan en el escritorio no se retiran al ausentarse del puesto de trabajo.

- Se permite la conexión de dispositivos usb a los equipos del Call center

Los anteriores hechos demuestran que las auxiliares del módulo de citas médicas hacen caso omiso a las normas y reglamentaciones establecidas por la Coordinación de Gestión de información como son:

- Todos los escritorios o mesas de trabajo deben permanecer limpios para proteger documentos en papel y dispositivos de almacenamiento como CD,s, USB memorykey, disquetes, con fin de reducir los riesgos de acceso no autorizado, perdida y daño de la información durante el horario normal de trabajo y fuera del mismo.

- Las unidades de CD, Dvd, USB etc permanecerá inactivas para la protección de la información contenida en la red corporativa y para evitar la instalación de software no licenciado por la empresa.

- Así como las normas establecidas por la Junta Directiva como de la Coordinación de Urgencias, Consulta Externa y Coordinación de Gestión de información como son:

- Se encuentra totalmente prohibido hacer uso de los teléfonos del Call

Center por personas diferentes a las agentes, ya que esto incrementa el tiempo de espera. ➢ Ninguna persona ajena a nuestra organización podrá ingresar al área de facturación y Call center evitando así el desorden y el tráfico de influencias. ➢ Ninguna persona podrá ingresar al área del Call center, todo tipo de actividades de atención personalizada tendrá que hacerse por la ventanilla. Evitando el tráfico de influencias. ➢ Se encuentra prohibido realizar cualquier tipo de actividades ajenas a las establecidas en los subprocesos de facturación y Call center. ➢ Estas actividades se tendrán que realizar por fuera del sitio de trabajo.
Recomendación
• La oficina de gestión de información a través del administrador y líder del módulo de citas médicas debe brindar capacitaciones que den a conocer a las funcionarias del área de citas la importancia de seguir las normas ya establecidas para el subproceso del Call center, y hacer control continuo sobre el cumplimiento estas normas. • De haber incumplimiento se debe tomar cierto tipo de acción correctiva o de sanción a la persona que haga caso omiso a las normas, procurando que la persona entienda que es de vital importancia que las cumpla, evitando el tráfico de influencias, y el incremento en el tiempo de espera en las llamadas.
Causa
• Las auxiliares del módulo de citas médicas no cuentan con una visión clara sobre las reglamentaciones existentes impidiendo el desarrollo normal del trabajo de citas médicas. • El personal no es supervisado para controlar este tipo de acciones. • Los funcionarios de gestión de información consideran que el modulo está en riesgo bajo. • El administrador del módulo no hace un control continuo de las actividades de seguridad que deben llevarse a cabo.
Nivel de riesgo
En cuanto a la probabilidad de ocurrencia está clasificada en alto, y el impacto es alto

HALLAZGO DE RECURSOS HUMANOS

Tabla 12: Hallazgo 5 HUDN

Tipo de registro: Hallazgos de Auditoria				
Entidad Auditada	Hospital Universitario Departamental de Nariño E.S.E			**Nº Guía: H5**
Área Auditada	Módulo de Citas Medicas	Sistema	Dinámica Gerencial Hospitalaria	
Responsable	Lyda Johana Castro Aguas			
R/PT:	CUESTIONARIOS/Entrevista: **ENT3_Nº Preg 10, 17** EVIDENCIA EN AUDIO**/EVI_AUDIO_16** **P5**			

Dominio	Planeación y Organización
Procesos	PO7 Administrar los Recursos Humanos de TI
Objetivo de Control	PO7.1 Reclutamiento y Retención del Personal
	PO7.2 Competencias del personal
	PO7.4 Entrenamiento del Personal de TI
	PO7.5 Dependencia Sobre los Individuos
	PO7.7 Evaluación del Desempeño del empleado
Riesgos Asociados	• Al no capacitar al personal de reemplazo genera riesgo como: ✓ el represamiento del trabajo. ✓ errores en la ejecución del software como por ejemplo ingreso de datos erróneos y por consiguiente incorrecta asignación de citas o de turnos médicos.

Descripción

- Aunque existe personal que reemplace a las auxiliares del módulo en el momento que ocurre ausencia temporal de estas funcionarias, esto genera contratiempos porque se debe hacer una inducción al personal de reemplazo sobre el manejo del módulo empezando por lo complejo que es el conocimiento de todos los médicos del Hospital Universitario Departamental de Nariño E.S.E.

- No se tienen en cuenta los conocimientos de las funcionarias encargadas de manejo del módulo de citas médicas, para ser aprovechado posteriormente en la probabilidad de que estas funcionarias abandonen el cargo.

Recomendación
• La capacitación que se brinda en cuanto al software y a la operación del módulo no solo debe involucrar a las funcionarias nombradas sino que debe extenderse también a las auxiliares de consulta externa que son el personal de reemplazo, dicha capacitación debe suministrar los manuales de operación para que en el momento que tenga que ausentarse una funcionaria sea mucho más ágil el proceso de reemplazo. • Realizar un proceso documentado que permita recoger información sobre el conocimiento que los empleados tienen sobre su puesto de trabajo e ideas que mejoren los procesos operativos, lo que generaría mayor productividad.
Causa
• El entrenamiento va enfocado exclusivamente a las auxiliares del módulo de citas médicas, este entrenamiento se hace únicamente cuando hay un cambio en el proceso de citas médicas o actualización del software por lo tanto el entrenamiento es eventual. • La creencia de la administración de que citas médicas es un proceso estandarizado y que por lo tanto no genera mayores complicaciones.
Nivel de riesgo
En cuanto a la probabilidad de ocurrencia está clasificada en alto, y el impacto es alto

Tabla 13: Hallazgo 6 HUDN

Tipo de registro: Hallazgos de Auditoria				
Entidad Auditada	Hospital Universitario Departamental de Nariño E.S.E			**Nº Guía: H6**
Área Auditada	Módulo de Citas Medicas	Sistema	Dinámica Gerencial Hospitalaria	
Responsable	Lyda Johana Castro Aguas			
R/PT:	EVIDENCIA FOTOGRAFICA/**EVI_FOTO_1** EVIDENCIA FOTOGRAFICA/**EVI_FOTO_2** EVIDENCIA FOTOGRAFICA/**EVI_FOTO_3** EVIDENCIA FOTOGRAFICA/**EVI_FOTO_4** EVIDENCIA FOTOGRAFICA/**EVI_FOTO_5** EVIDENCIA FOTOGRAFICA/**EVI_FOTO_9** CUESTIONARIOS/Lista de Chequeo:**LC5_Nº Preg 5** **ANEXO No. 9- MANUAL DE CAPACITACION Y SOPORTE P6**			

Dominio	Planear y Organizar
Procesos	PO7 Administrar los Recursos Humanos de TI.
Objetivo de Control	PO7.2 Competencias del personal
	PO7.4 Entrenamiento del Personal de TI
	PO7.7 Evaluación del Desempeño del empleado
Riesgos Asociados	• Este represamiento de información lleva a la acumulación de trabajo afectando el desarrollo dinámico de la asignación de citas

Descripción

Las auxiliares del módulo de citas médica hacen caso omiso a las normas y reglamentaciones para el subproceso del Call center ya establecidas por la Junta Directiva como de la Coordinación de Urgencias, Consulta Externa y Coordinación de Gestión de información como son:

- Se encuentra totalmente prohibido hacer uso de los teléfonos del Call Center por personas diferentes a las agentes, ya que esto incrementa el tiempo de espera.

- Ninguna persona ajena a nuestra organización podrá ingresar al área de facturación y Call center evitando así el desorden y el tráfico de influencias.

- Ninguna persona podrá ingresar al área del Call center, todo tipo de actividades de atención personalizada tendrá que hacerse por la ventanilla. Evitando el tráfico de influencias.

- Se encuentra prohibido realizar cualquier tipo de actividades ajenas a las establecidas en los subprocesos de facturación y Call center. Estas actividades se tendrán que realizar por fuera del sitio de trabajo.

Recomendación

- La oficina de gestión de información a través del administrador y líder del módulo de citas médicas debe brindar capacitaciones que den a conocer a las funcionarias del área de citas la importancia de seguir las normas ya establecidas para el subproceso del Call center.

- De no ser así se debe tomar cierto tipo de acción correctivo o de sanción a la persona que haga caso omiso a las normas, procurando que la persona entienda que es de vital importancia que las cumpla, evitando el tráfico de influencias, y el incremento en el tiempo de espera en las llamadas.

Causa

- Las auxiliares del módulo de citas médicas no cuentan con una visión clara sobre sus funciones, normas y reglamentaciones ya existentes impidiendo el desarrollo normal del trabajo de citas médicas.

- También que el personal no es supervisado para controlar este tipo de acciones.

- Los funcionarios de gestión de información consideran que el modulo está en riesgo bajo.

Nivel de riesgo

En cuanto a la probabilidad de ocurrencia está clasificada en alto, y el impacto es alto

HALLAZGOS DE CONTINUIDAD DEL SERVICIO

Tabla 14: Hallazgo 7 HUDN

Tipo de registro: Hallazgos de Auditoria				
Entidad Auditada	Hospital Universitario Departamental de Nariño E.S.E			**Nº Guía: H7**
Área Auditada	Módulo de Citas Medicas	Sistema	Dinámica Gerencial Hospitalaria	
Responsable	Jaydivi Castillo			
R/PT:	CUESTIONARIOS/Lista de Chequeo: **LC6_Nº Preg 12** **ANEXO No. 4- PLAN DE CONTINGENCIA DE HARDWARE Y SOFTWARE JUNIO 2009** **P7**			

Dominio	Entrega y Soporte
Procesos	DS4 Garantizar la continuidad del Servicio
Objetivo de Control	DS4.2 Planes de Continuidad de TI
	DS4.3 Recursos Críticos de TI
	DS4.4 Mantenimiento del Plan de continuidad
	DS4.5 Pruebas del Plan de Continuidad de TI
	DS4.6 Entrenamiento del Plan de Continuidad de TI
	DS4.7 Distribución del Plan de Continuidad de TI
	DS4.8 Recuperación y Reanudación de los Servicios de TI
	DS4.9 Almacenamiento de Respaldos Fuera de las Instalaciones
	DS4.10 Revisión Post Reanudación
Riesgos Asociados	Al no existir control sobre las contingencias que se presentan, la administración no sabrá con certeza que problemas se presentan con mayor frecuencia y por lo tanto no habrá una toma correcta de decisiones, ya que no hay un dato de referencia que indique como está el problema en un periodo de tiempo y por lo tanto no se identifica cual es la causa del problema, aumentando los costos para la organización.

Descripción

- No se lleva un control sobre el tiempo perdido por el usuario debido a interrupciones en el servicio ocasionadas por factores que afectan a la seguridad del edificio y los que afectan la integridad de los datos.

- No se tiene un registro sobre los errores más comunes que permitan un análisis de probabilidad de ocurrencia de fallas en el área de citas médicas.

Recomendación
Elaborar un documento por cada eventualidad que genere interrupción del servicio, dicho documento debe contemplar los siguientes aspectos: contingencia, descripción de la contingencia, recurso afectado, tiempo de suspensión del servicio, firma del administrador de citas médicas. Esta documentación servirá de apoyo al plan de contingencia ya que se puede medir cuales son los eventos más frecuentes que se presentan en el área de citas médicas y que afectan su continuo desarrollo y a su vez este reporte servirá de apoyo a otras dependencias.
Causa
• El control de tiempo perdido por el usuario no está contemplado dentro del plan de contingencia. • Al estar citas médicas en una situación de riesgo bajo considerado por los administradores no ha sido para ellos necesario aun un control cada vez que se presente una contingencia.
Nivel de riesgo
En cuanto a la probabilidad de ocurrencia está clasificada en alto, y el impacto es alto

Tabla 15: Hallazgo 8 HUDN

Tipo de registro: Hallazgos de Auditoria				
Entidad Auditada	Hospital Universitario Departamental de Nariño E.S.E			**Nº Guía: H8**
Área Auditada	Módulo de Citas Medicas	Sistema	Dinámica Gerencial Hospitalaria	
Responsable	Jaydivi Castillo Guerrero.			
R/PT:	CUESTIONARIOS/Lista de Chequeo: **LC6 – N° Preg 4, 5, 8, 10, 11, 13** **ANEXO No. 4- PLAN DE CONTINGENCIA HARDWARE Y SOFTWARE JUNIO 2009** **P8**			

Dominio	Entrega y Soporte
Procesos	DS4 Garantizar la continuidad del Servicio
Objetivo de Control	DS4.2 Planes de Continuidad de TI
	DS4.3 Recursos Críticos de TI
	DS4.4 Mantenimiento del Plan de continuidad
	DS4.5 Pruebas del Plan de Continuidad de TI
	DS4.6 Entrenamiento del Plan de Continuidad de TI
	DS4.7 Distribución del Plan de Continuidad de TI
	DS4.8 Recuperación y Reanudación de los Servicios de TI
	DS4.9 Almacenamiento de Respaldos Fuera de las Instalaciones
	DS4.10 Revisión Post Reanudación
Riesgos Asociados	• Al no existir una alternativa que permita la continuidad del desarrollo de los procesos en el módulo de citas médicas, se generan los siguientes riesgos: la suspensión del servicio de citas y de turnos, y la suspensión de solicitudes de historias clínicas. • Este represamiento de información lleva a la acumulación de trabajo afectando el desarrollo dinámico de la asignación de citas. • El no probar el plan de recuperación de datos genera riesgo de pérdida total o parcial de datos.
Descripción	

• Actualmente el módulo de citas médicas no cuenta con una alternativa que permita la continuidad del desarrollo de los procesos en caso de una falla total en el sistema principal. • No se han llevado pruebas que demuestren la eficacia del plan de recuperación de datos ante cualquier desastre. • No se tiene contemplado un informe que describa las acciones que se tomaron después de recuperado el sistema • No se han puesto a pruebas los planes de continuidad del servicio del módulo de citas médicas para verificar si son efectivos.
Recomendación
• Anexar al plan de contingencia del hospital la documentación correspondiente a las tareas que deben seguirse y los responsables que deben ejecutarlas y capacitar al personal sobre el plan alternos de citas médicas. • Una vez se tenga este plan realizar las pruebas pertinentes para intentar valorar el impacto real de un posible problema dentro de los escenarios establecidos como posibles. • Elaborar el formato en el que se pueda hacer un informe del evento que llevo a la recuperación del sistema.
Causa
Al estar citas médicas en una situación de riesgo bajo considerado por los administradores no ha sido para ellos necesaria una documentación que respalde la continuidad del servicio en caso de una falla de gravedad en el sistema.
Nivel de riesgo
En cuanto a la probabilidad de ocurrencia está clasificada en alto, y el impacto es alto

Tabla 16: Hallazgo 9 HUDN

Tipo de registro: Hallazgos de Auditoria				
Entidad Auditada	Hospital Universitario Departamental de Nariño E.S.E			**Nº Guía: H9**
Área Auditada	Módulo de Citas Medicas	Sistema	Dinámica Gerencial Hospitalaria	
Responsable	Jaydivi Castillo Guerrero			
R/PT:	CUESTIONARIOS/Entrevista: **ENT4 – N° Preg 1** EVIDENCIA EN AUDIO/**EVI_AUDIO_7** **P9**			

Dominio	Entrega y Soporte
Procesos	DS4 Garantizar la continuidad del Servicio
Objetivo de Control	DS4.2 Planes de Continuidad de TI
	DS4.3 Recursos Críticos de TI
	DS4.4 Mantenimiento del Plan de continuidad
	DS4.5 Pruebas del Plan de Continuidad de TI
	DS4.6 Entrenamiento del Plan de Continuidad de TI
	DS4.7 Distribución del Plan de Continuidad de TI
	DS4.8 Recuperación y Reanudación de los Servicios de TI
	DS4.9 Almacenamiento de Respaldos Fuera de las Instalaciones
	DS4.10 Revisión Post Reanudación
Riesgos Asociados	• Al no existir una alternativa que permita la continuidad del desarrollo de los procesos en el módulo de citas médicas, se generan los siguientes riesgos: la suspensión del servicio de citas y de turnos, y la suspensión de solicitudes de historias clínicas. • Este represamiento de información lleva a la acumulación de trabajo afectando el desarrollo dinámico de la asignación de citas
Descripción	
Las auxiliares del módulo de citas médicas no conocen de la existencia de un plan de continuidad o de contingencia de los recursos de TI involucrados en el módulo de citas y en la organización en general.	
Recomendación	
• La oficina de gestión de información a través del administrador del módulo de citas médicas debe brindar capacitaciones que den a conocer a las funcionarias del área de citas la importancia del plan de contingencia de la organización, el contenido de este plan y cuál sería el	

rol de cada funcionaria en el momento de presentarse algún evento que genere alguna contingencia. • Elaborar el plan de continuidad del área de citas médicas, en el que se contemple con exactitud que recursos de TI se ven involucrados, los riesgos a los que se expone el área, los pasos a seguir para controlar la contingencia, los responsables de ejecutar las tareas. El objetivo principal del plan es permitir al área seguir operando bajo condiciones adversas, al implantar estrategias adecuadas, objetivos de recuperación, planes de gestión de crisis y estrategias de gestión de riesgos, facilitando a la Organización de una estructura preparada para mantener la flexibilidad y la capacidad de una efectiva respuesta en la protección de los intereses principales, tales como: información, activos de valor, continuidad de procesos y operaciones.
Causa
• La no existencia de un plan de continuidad para el área de citas, no genera un proceso claro a seguir en el momento que ocurre un fallo en el sistema, impidiendo el desarrollo normal del trabajo de citas médicas. • Los funcionarios de gestión de información consideran que el modulo está en riesgo bajo por lo que no ha sido necesario e importante realizar un plan.
Nivel de riesgo
En cuanto a la probabilidad de ocurrencia está clasificada en alto, y el impacto es alto

HALLAZGO DE OBJETIVO DE LA ORGANIZACIÓN

Tabla 17: Hallazgo 10 HUDN

Tipo de registro: Hallazgos de Auditoria				
Entidad Auditada	Hospital Universitario Departamental de Nariño E.S.E			**Nº Guía: H10**
Área Auditada	Módulo de Citas Medicas	Sistema	Dinámica Gerencial Hospitalaria	
Responsable	Jaydivi Castillo Guerrero			
R/PT:	CUESTIONARIOS/Entrevista: **ENT5_Nº Preg 1, 2, 3** EVIDENCIA EN AUDIO/**EVI_AUDIO_15** **ANEXO No. 7- Ley 100 de 1993** **P10**			

Dominio	Adquirir e Implementar
Procesos	AI1 Identificar Soluciones Automatizadas
Objetivo de Control	AI1.1 Definición y Mantenimiento de los Requerimientos Técnicos y Funcionales del Negocio
Riesgos Asociados	• Al no existir un análisis de requerimientos puede ocasionar riesgos como fallas continuas en el sistema ya que estas no se corrigen. • Al no existir un análisis de requerimientos puede ocasionar riesgos como costos elevados para la organización ya que si el software no cumplió las expectativas de trabajo se debe pensar en otro.
Descripción	
No existe un estudio particular sobre las necesidades o requerimientos de hardware, software y procedimientos del área de citas médicas.	
Recomendación	
Elaborar un estudio de requerimientos del Área de Citas Médicas para conocer que mejoras se deben hacer a los procesos. Este estudio permite profundizar los siguientes aspectos: cómo se lleva el proceso básico, que datos utiliza o produce el área, cuales son los límites impuestos por el tiempo y carga de trabajo, los controles de desempeño que se utilizan.	
Causa	
Los requerimientos del área de citas médicas se basan en la reglamentación de la ley 100 en esta se menciona que las instituciones de salud deben contar con un sistema de información que evite que los pacientes tengan que esperar demasiado tiempo en una ventanilla.	

El sistema Dinámica Gerencial Hospitalaria para los funcionarios ha cumplido con el trabajo básico del hospital
Nivel de riesgo
En cuanto a la probabilidad de ocurrencia está clasificada en alto, y el impacto es alto

HALLAZGO DE USO DEL SOFTWARE

Tabla 18: Hallazgo 11 HUDN

Tipo de registro: Hallazgos de Auditoria				
Entidad Auditada	Hospital Universitario Departamental de Nariño E.S.E			**Nº Guía: H11**
Área Auditada	Módulo de Citas Medicas	Sistema	Dinámica Gerencial Hospitalaria	
Responsable	Jaydivi Castillo			
R/PT:	CUESTIONARIOS/Entrevista: **ENT6_Nº Preg 3** CUESTIONARIOS/Lista de Chequeo: **LC4_NºPreg 3, 4** CUESTIONARIOS/Lista de Chequeo: **LC5_NºPreg 9** EVIDENCIA EN AUDIO/**EVI_AUDIO_16** **ANEXO No. 8- (42571-98054) NUM_CITAS_MEDICAS.NET V 002** **ANEXO No. 9- (83313-33777) 05 Citas Médicas DGH** **ANEXO No. 11- MANUAL DE CAPACITACION Y SOPORTE P11**			

Dominio	Adquirir e Implementar
Procesos	AI4 Facilitar la Operación y Uso
Objetivo de Control	AI4.3 Transferencia de Conocimiento a Usuarios Finales
Riesgos Asociados	Al no capacitar al personal de reemplazo genera riesgo como: ✓ el represamiento del trabajo. ✓ errores en la ejecución del software como por ejemplo ingreso de datos erróneos y por consiguiente incorrecta asignación de citas o de turnos médicos.

Descripción

- Los funcionarios no tienen los manuales de usuario de las aplicaciones instaladas en los equipos del Call Center.

- Al no existir información documental de la aplicación las auxiliares del módulo no tienen una herramienta de consulta.

Recomendación

- La oficina de gestión de información debe elaborar un manual de usuario que facilite el conocimiento sobre:

  ✓ cuáles son los datos del entrada,
  ✓ como se debe obtener los resultados
  ✓ cuáles son los datos de salida
  ✓ como son los formatos de los documentos

✓ en qué momento se debe pedir una operación o una información específica. • El manual de usuario debe ser redactado en forma clara e ir de acuerdo al tipo de usuario que usa el sistema y debe entregarse como parte del entrenamiento de las funcionarias oficiales y del personal de reemplazo.
Causa
• El manual de usuario del aplicativo que tiene la oficina de gestión de Información no es distribuido entre los funcionarios. • La coordinación de gestión de información afirma que la capacitación inicial que se dio a los funcionarios es suficiente para comprender el software. • El manual de usuario que tiene la organización es de autoría del SYAC desarrollador del Sistema Dinámica Gerencial y Hospitalaria, por lo tanto es un manual que no está diferenciado de acuerdo a los perfiles de usuario.
Nivel de riesgo
En cuanto a la probabilidad de ocurrencia está clasificada en alto, y el impacto es alto.

Tabla 19: Hallazgo 12 HUDN

Tipo de registro: Hallazgos de Auditoria				
Entidad Auditada	Hospital Universitario Departamental de Nariño E.S.E			**Nº Guía: H12**
Área Auditada	Módulo de Citas Medicas	Sistema	Dinámica Gerencial Hospitalaria	
Responsable	Jaydivi Castillo			
R/PT:	CUESTIONARIOS/Lista de Chequeo: **LC4_NºPreg 1** **ANEXO No. 8- (42571-98054) NUM_CITAS_MEDICAS.NET V 002** **ANEXO No. 9- (83313-33777) 05 Citas Médicas DGH P12**			

Dominio	Adquirir e Implementar
Procesos	AI4 Facilitar la Operación y Uso
Objetivo de control	AI4.1 Plan para Soluciones de Operación
	AI4.4 Transferencia de Conocimiento de Operaciones y Soporte
Riesgos Asociados	Una incorrecta instalación del software lleva a que el sistema trabaje erróneamente arrojando posibles datos equivocados y por ende el trabajo se puede ver afectado.
Descripción	
• No existe documentación sobre los aspectos técnico del sistema Dinámica Gerencial Hospitalaria.	
Recomendación	
• La coordinación de gestión de información deberá elaborar el documento describiendo cuales son los aspecto en cuanto a software y hardware que se deben tener en cuenta antes de la instalación, así mismo el documento debe detallar los pasos a seguir para la instalación y una sesión de los posibles problemas que se pueden generar en la instalación junto con la forma de solucionarlos.	
Causa	
• Al ser equipos de cómputo nuevos no han surgido problemas de instalación. • el soporte que ofrece la empresa desarrolladora Sistemas y asesoría de Colombia es en línea por lo tanto la organización no ve necesario la realización de un manual. • Las políticas de acceso a usuarios de acuerdo al rol de los funcionarios no	

están definidas ni documentadas. • El administrador del módulo no hacen control ni revisión de los permisos que están asignados en el sistema. • La confianza de la coordinación de gestión de información, de que los empleados no realizaran modificaciones sobre las funcionalidades que no hacen parte del cargo.
Nivel de riesgo
En cuanto a la probabilidad de ocurrencia está clasificada en baja, y el impacto es medio.

Tabla 20: Hallazgo 13 HUDN

Tipo de registro: Hallazgos de Auditoria				
Entidad Auditada	Hospital Universitario Departamental de Nariño E.S.E			**Nº Guía: H13**
Área Auditada	Módulo de Citas Medicas	Sistema	Dinámica Gerencial Hospitalaria	
Responsable	Jaydivi Castillo			
R/PT:	CUESTIONARIOS/Lista de Chequeo: **LC1_NºPreg 4,5,6,7,8 ANEXO No. 10- REPORTE DE PERFILES DE USUARIO DEL SISTEMA P13**			

Dominio	Adquirir e Implementar
Procesos	AI4 Facilitar la Operación y Uso
Objetivo de control	AI4.1 Plan para Soluciones de Operación
	AI4.4 Transferencia de Conocimiento de Operaciones y Soporte
Riesgos Asociados	Existe el riesgo de que personas propias o ajenas a la organización introduzcan datos que afecten el procesamiento de la información, por ejemplo el ingreso de datos falsos.
Descripción	
• Las auxiliares del Call Center tienen habilitadas todas las funcionalidades del módulo de citas médicas del aplicativo DGH, a pesar de que algunas de sus funcionalidades no son de su competencia.	
Recomendación	
• La coordinación de gestión de información debe elaborar un documento donde se describa cuáles son los perfiles de usuario que deben funcionar dentro de la institución dicho documento debe ir apoyado por cada uno de los líderes del módulo. • Este documento debe ser distribuido a cada de los administradores de los respectivos módulos para que ellos hagan una revisión continua de los perfiles de usuario configurados en el sistema.	
Causa	
• Las políticas de acceso a usuarios de acuerdo al rol de los funcionarios no están definidas ni documentadas. • El administrador del módulo no hacen control ni revisión de los permisos que están asignados en el sistema.	

• La confianza de la coordinación de gestión de información, de que los empleados no realizaran modificaciones sobre las funcionalidades que no hacen parte del cargo.
Nivel de riesgo
En cuanto a la probabilidad de ocurrencia está clasificada en alto, y el impacto es alto.

HALLAZGO DE AMBIENTE FÍSICO

Tabla 21: Hallazgo 14 HUDN

Tipo de registro: Hallazgos de Auditoria				
Entidad Auditada	Hospital Universitario Departamental de Nariño E.S.E			**Nº Guía: H14**
Área Auditada	Módulo de Citas Medicas	Sistema	Dinámica Gerencial Hospitalaria	
Responsable	Lyda Johana Castro Aguas			
R/PT:	CUESTIONARIOS/Lista de Chequeo: **LC3_Nº Preg 14** EVIDENCIA FOTOGRAFICA**/EVI_FOTO_6** EVIDENCIA FOTOGRAFICA**/EVI_FOTO_13** EVIDENCIA EN VIDEO**/EVI_VIDEO_17** **P14**			

Dominio	Entrega y Soporte
Procesos	DS12 Administración del Ambiente Físico
Objetivo de Control	DS12.1 Selección y Diseño del Centro de Datos
	DS12.2 Medidas de Seguridad Física
	DS12.3 Acceso Físico
	DS12.4 Protección Contra Factores Ambientales
	DS12.5 Administración de Instalaciones Físicas
Riesgos Asociados	• La inadecuada colocación de señales en el lugar de trabajo genera riesgos de lesión en el personal en el momento de que ocurra una desgracia. • Al no haber un extintor en el área puede haber riesgos de pérdidas de vida, aunque exista un extintor cercano es probable que en un momento de emergencia la salida se pueda obstruir.
Descripción	
• El aviso de alarma de evacuación no tiene una correcta visualización ya que sobre él hay una mesa de escritorio. • Dentro del área no existen equipos extintores como tampoco una salida de emergencia. El extintor más cercano se encuentra fuera del Call Center. • El área del Call Center está ubicado en un lugar con demasiado ruido.	
Recomendación	

• Colocar las señales de alarma o de cualquier otro tipo de emergencia en un lugar visible. • Colocar el equipo extintor correspondiente al área y contemplar la construcción de una salida de emergencia por ejemplo en la parte lateral o trasera del Call center. • Colocar una división que separe el Call Center de facturación previniendo de esta manera que se entre el ruido.
Causa
• Una incorrecta planeación del personal encargado de la implementación de los avisos de emergencia.
Nivel de riesgo
En cuanto a la probabilidad de ocurrencia está clasificada en alto, y el impacto es alto

HALLAZGOS DE OPERACIÓN

Tabla 22: Hallazgo 15 HUDN

Tipo de registro: Hallazgos de Auditoria				
Entidad Auditada	Hospital Universitario Departamental de Nariño E.S.E			**Nº Guía: H15**
Área Auditada	Módulo de Citas Medicas	Sistema	Dinámica Gerencial Hospitalaria	
Responsable	Lyda Johana Castro Aguas			
R/PT:	**ANEXO No. 2- JARG SUBPROCESO CITAS MEDICAS POR EPS** **ANEXO No. 10- Manual de funciones** **P15**			

Dominio	Entrega y Soporte
Procesos	DS13 Administración de Operaciones
Objetivo de Control	DS13.1 Procedimientos e intrusiones de operación
Riesgos Asociados	Al no existir coordinación entre quienes dirigen el módulo de citas médicas puede provocar suspensión del servicio de citas, por la confusión de los usuarios.

Descripción

- El diagrama de procesos esta desactualizado.
- Solamente la organización tiene el diagrama de procesos para asignación de citas por EPS y no se tiene el diagrama para asignación de citas a particulares.
- En un principio se dijo que la tarea de asignación de turno era una labor del administrador del módulo de citas médicas en conjunto con la líder del mismo, pero las funcionarias del Call Center también deben hacer esa tarea.
- El encargado de la administración del Módulo de Citas Médicas no ejerce sus funciones porque se cree que no hay problemas dentro del módulo, y por lo tanto quien tiene más conocimiento según el propio administrador del módulo es el coordinador de gestión de información del hospital.

Recomendación

- Actualizar el diagrama de procesos considerando que se pueden asignar citas por EPS y a particulares.
- El coordinador de gestión de información debe controlar que el

administrador del módulo ejerza sus funciones en forma continua y no cuando ocurra un evento inesperado evitando así el desorden en la organización, un administrador permanente facilita la entrega de información más precisa a quienes este interesados en conocer el funcionamiento de los diferentes procesos. • El manual de funciones de la organización debe mejorarse, especificando claramente cada uno de los cargos y las funciones y no debe ir de acuerdo a un departamento en general.
Causa
• El manual de funciones no describe correctamente los cargos y funciones a cumplir. • La falta de control en el módulo de citas médicas lleva a la no actualización del diagrama de procesos.
Nivel de riesgo
En cuanto a la probabilidad de ocurrencia está clasificada en alto, y el impacto es alto

FUNCIONAMIENTO

Tabla 23: Hallazgo 16 HUDN

Tipo de registro: Hallazgos de Auditoria				
Entidad Auditada	Hospital Universitario Departamental de Nariño E.S.E			**Nº Guía: H16**
Área Auditada	Módulo de Citas Medicas	Sistema	Dinámica Gerencial Hospitalaria	
Responsable	Jaydivi Castillo			
R/PT:	EVIDENCIA IMÁGENES/**EVI_IMG_1** EVIDENCIA IMÁGENES/**EVI_IMG_2** CUESTIONARIOS/Lista de Chequeo: **LC1_Nº Preg 20 P16**			

Dominio	Entrega y Soporte
Procesos	DS5 Garantizar la Seguridad de los Sistemas
	DS11 Administración de datos
Objetivo de control	DS5.7 Protección de Tecnología de Seguridad
	DS11.6 Requerimientos de seguridad para la administración de datos
Riesgos Asociados	• La repetición de la contraseña que se asigna por defecto genera el siguiente riesgo: relacionado con que la organización queda expuesta a riesgos relacionados con que los funcionarios puedan llevarse un reporte de datos o información confidencial o reservada.
Descripción	
• La contraseña que asigna por defecto el sistema cuando la restablece se repite en usuarios diferentes ya sea que tengan perfil de administrador o usuario convencional. • Dos funcionalidades: la creación de médico y creación de especialistas se repiten en dos modulo, Historias clínicas y Citas médicas.	
Recomendación	
• La coordinación de gestión de información debe realizar un informe sobre estos errores para luego ser noticiado a los ingenieros de soporte de Sistemas y Asesorías de Colombia para que analicen los errores y hagan las pruebas pertinentes, las analicen y hagan las correcciones necesarias.	
Causa	
• La falta de control de gestión de información y del administrador del módulo de citas médicas sobre las prácticas de seguridad básicas para evitar robo de información, hace que las funcionarias desconozcan las	

normas principales de seguridad.
Nivel de riesgo
En cuanto a la probabilidad de ocurrencia está clasificada en alto, y el impacto es alto.

3.4. GUÍAS DE PRUEBA MODULO DE CITAS MEDICAS

Tabla 24: Guía de Prueba 1

Tipo de registro: Guía de Pruebas				
Entidad Auditada	Hospital Universitario Departamental de Nariño E.S.E			**Nº Guía: P1**
Área Auditada	Módulo de Citas Medicas	Sistema	Dinámica Gerencial Hospitalaria	
R/PT:	CUESTIONARIOS/Lista de Chequeo: **LC2_Nº Preg 1, Preg 6, Preg 8**			

Dominio	Entrega y Soporte
Procesos	DS5 Garantizar la Seguridad de los Sistemas
Objetivo de Control	DS5.2 Plan de Seguridad de TI
	DS5.3 Administración de Identidad
	DS5.4 Administración de Cuentas del Usuario
Riesgos Asociados	• La organización queda expuesta a riesgos de robo de documentación y archivos importantes que son vitales para el hospital. • Al no hacerse un cambio periódico de contraseña el sistema está expuesto a que algún atacante pueda adivinar la contraseña.

No.	**Evidencia**	**Descripción**
1	**Anexo No. 6:** Política de Gestión de Información	No existe una cuenta de usuario para iniciar sesión en el sistema operativo
2		Las auxiliares del módulo no cambian la contraseña del sistema cada 6 meses.
3		La política general de gestión de información no contempla en que situaciones se debe hacer un cambio urgente de contraseña.

Tabla 25: Guía de Prueba 2

Tipo de registro: Guía de Pruebas				
Entidad Auditada	Hospital Universitario Departamental de Nariño E.S.E			**Nº Guía: P2**
Área Auditada	Módulo de Citas Medicas	Sistema	Dinámica Gerencial Hospitalaria	
R/PT:	CUESTIONARIOS/Lista de Chequeo: **LC1_Nº Preg 14, 18, 21** CUESTIONARIOS/Lista de Chequeo: **LC2_Nº Preg 4**			

Dominio	Entrega y Soporte	
Procesos	DS5 Garantizar la Seguridad de los Sistemas	
	DS11 Administración de datos	
Objetivo de Control	DS5.7 Protección de Tecnología de Seguridad	
	DS11.6 Requerimientos de seguridad para la administración de datos	
Riesgos Asociados	La organización queda expuesta a riesgos relacionados con que los funcionarios puedan llevarse un reporte de datos o información confidencial o reservada.	
No.	**Evidencia**	**Descripción**
1	**Anexo No. 6:** Política de Gestión de Información	No se firma, ni renueva el acuerdo de cumplimiento sobre la seguridad y confidencialidad de la información
2		No se hace entrega de un documento que contenga cuáles son sus derechos de acceso de acuerdo a un perfil.
3		No hace revisión periódica de los derechos de acceso establecidos por el sistema.

Tabla 26: Guía de Prueba 3

Tipo de registro: Guía de Pruebas				
Entidad Auditada	Hospital Universitario Departamental de Nariño E.S.E			**Nº Guía: P3**
Área Auditada	Módulo de Citas Medicas	Sistema	Dinámica Gerencial Hospitalaria	
R/PT:	CUESTIONARIOS/Lista de Chequeo: **LC1_Nº Preg 31**			

Dominio	Entrega y Soporte
Procesos	DS5 Garantizar la Seguridad de los Sistemas
Objetivo de Control	DS5.2 Plan de Seguridad de TI DS5.5 Pruebas, Vigilancia y Monitoreo de la Seguridad
Riesgos Asociados	• La distracción interrumpe el desarrollo normal de los procesos en el módulo de citas médicas. **Al estar personas externas en el área:** • La organización queda expuesta a riesgos de robo de documentación y archivos importantes que son vitales para el hospital. • La visualización de información del sistema o de documentos que se encuentren sobre el escritorio que pueden ser críticos para la organización.

No.	Evidencia	Descripción
1	EVIDENCIA FOTOGRAFICA/ EVI_FOTO_4 EVI_FOTO_9	Las personas externas que ingresan al Call center utilizan los equipos para asuntos personales.
2	EVIDENCIA FOTOGRAFICA/ EVI_FOTO_8	Facebook está habilitado en los equipos del Call center

Tabla 27: Guía de Prueba 4

Tipo de registro: Guía de Pruebas				
Entidad Auditada	Hospital Universitario Departamental de Nariño E.S.E			**Nº Guía: P4**
Área Auditada	Módulo de Citas Medicas	Sistema	Dinámica Gerencial Hospitalaria	
R/PT:	CUESTIONARIOS/Lista de Chequeo: **LC3_Nº Preg 6, 8**			

Dominio	Entrega y Soporte
Procesos	DS5 Garantizar la Seguridad de los Sistemas
Objetivo de Control	DS5.2 Plan de Seguridad de TI DS5.5 Pruebas, Vigilancia y Monitoreo de la Seguridad
Riesgos Asociados	• La distracción interrumpe el desarrollo normal de los procesos en el módulo de citas médicas. • El comer en el puesto de trabajo generaría accidentes como: derramar alimento sobre los equipos. **Al estar personas externas en el área:** • La organización queda expuesta a riesgos de robo de documentación y archivos importantes que son vitales para el hospital. • La visualización de información del sistema o de documentos que se encuentren sobre el escritorio que pueden ser críticos para la organización. • Cambios en la configuración del equipo y desinstalación de alguna aplicación

No.	Evidencia	Descripción
1	EVIDENCIA FOTOGRAFICA/ EVI_FOTO_1 EVI_FOTO_2 EVI_FOTO_3 EVI_FOTO_9	Las personas externas al Call center utilizan el teléfono para asuntos personales.
2	EVIDENCIA FOTOGRAFICA/ EVI_FOTO_5 EVI_FOTO_9	El puesto de trabajo es utilizado por las funcionarias y personas externas para almorzar y mirar revistas de catálogo.

3	EVIDENCIA FOTOGRAFICA/ EVI_FOTO_17 EVI_FOTO_18	Las auxiliares del módulo de citas médicas no cierran ni bloquean el sistema al ausentarse por un momento del puesto de trabajo.
4	EVIDENCIA FOTOGRAFICA/ EVI_FOTO_19 **Anexo No. 6:** Política de Gestión de Información	En los equipos utilizados en Call Center no se tiene desactivado el panel de control
5	EVIDENCIA FOTOGRAFICA/ EVI_FOTO_15	Los documentos que se dejan en el escritorio no se retiran al ausentarse del puesto de trabajo.
6	EVIDENCIA FOTOGRAFICA/ EVI_FOTO_11 **Anexo No. 6:** Política de Gestión de Información	Se permite la conexión de dispositivos usb a los equipos del Call center

Tabla 28: Guía de Prueba 5

Tipo de registro: Guía de Pruebas				
Entidad Auditada	Hospital Universitario Departamental de Nariño E.S.E			**Nº Guía: P5**
Área Auditada	Módulo de Citas Medicas	Sistema	Dinámica Gerencial Hospitalaria	
R/PT:	CUESTIONARIOS/Entrevista: **ENT3_Nº Preg 10, 12, 18**			

Dominio	Planeación y Organización
Procesos	PO7 Administrar los Recursos Humanos de TI
Objetivo de Control	PO7.1 Reclutamiento y Retención del Personal
	PO7.2 Competencias del personal
	PO7.4 Entrenamiento del Personal de TI
	PO7.5 Dependencia Sobre los Individuos
	PO7.7 Evaluación del Desempeño del empleado
Riesgos Asociados	• Al no capacitar al personal de reemplazo genera riesgo como: ✓ el represamiento del trabajo. ✓ errores en la ejecución del software como por ejemplo ingreso de datos erróneos y por consiguiente incorrecta asignación de citas o de turnos médicos.

No.	Evidencia	Descripción
1	EVIDENCIA EN AUDIO**/ EVI_AUDIO_16**	No existen planes que eviten las dependencias en los cargos de los funcionarios.
2		No son aprovechados los conocimientos de los empleados al momento de su despido, para ser entregados al nuevo personal.

Tabla 29: Guía de Prueba 6

Tipo de registro: Guía de Pruebas				
Entidad Auditada	Hospital Universitario Departamental de Nariño E.S.E			**Nº Guía: P6**
Área Auditada	Módulo de Citas Medicas	Sistema	Dinámica Gerencial Hospitalaria	
R/PT:	CUESTIONARIOS/Lista de Chequeo:**LC5_Nº Preg 5**			

Dominio	Planeación y Organización
Procesos	PO7 Administrar los Recursos Humanos de TI
Objetivo de Control	PO7.2 Competencias del personal
	PO7.4 Entrenamiento del Personal de TI
	PO7.7 Evaluación del Desempeño del empleado
Riesgos Asociados	✓ Al no existir una alternativa que permita la continuidad del desarrollo de los procesos en el módulo de citas médicas, se generan los siguientes riesgos: la suspensión del servicio de citas y de turnos, y la suspensión de solicitudes de historias clínicas. ✓ Este represamiento de información lleva a la acumulación de trabajo afectando el desarrollo dinámico de la asignación de citas

No.	Evidencia	Descripción
1	EVIDENCIA FOTOGRAFICA/ EVI_FOTO_1 EVI_FOTO_2 EVI_FOTO_3 EVI_FOTO_4 EVI_FOTO_5 EVI_FOTO_9	Se hace caso omiso a las normas y reglamentos establecidos por la Junta Directiva como de la Coordinación de Urgencias, Consulta Externa y Coordinación de Gestión de información.
2	No se programan capacitaciones continuas **Anexo No. 9:** Manual de Capacitación y Soporte	Las capacitaciones y monitoreo a los funcionarios no se hacen de manera continua, solo se realizan para la inducción de los funcionarios y para socializar algún cambio en el módulo.

Tabla 30: Guía de Prueba 7

Tipo de registro: Guía de Pruebas				
Entidad Auditada	Hospital Universitario Departamental de Nariño E.S.E			**Nº Guía: P7**
Área Auditada	Módulo de Citas Medicas	Sistema	Dinámica Gerencial Hospitalaria	
R/PT:	CUESTIONARIOS/Lista de Chequeo: **LC6_Nº Preg 12**			

Dominio	Entrega y Soporte
Procesos	DS4 Garantizar la continuidad del Servicio
Objetivo de Control	DS4.2 Planes de Continuidad de TI
	DS4.3 Recursos Críticos de TI
	DS4.4 Mantenimiento del Plan de continuidad
	DS4.5 Pruebas del Plan de Continuidad de TI
	DS4.6 Entrenamiento del Plan de Continuidad de TI
	DS4.7 Distribución del Plan de Continuidad de TI
	DS4.8 Recuperación y Reanudación de los Servicios de TI
	DS4.9 Almacenamiento de Respaldos Fuera de las Instalaciones
	DS4.10 Revisión Post Reanudación
Riesgos Asociados	Al no existir control sobre las contingencias que se presentan, la administración no sabrá con certeza que problemas se presentan con mayor frecuencia y por lo tanto no habrá una toma correcta de decisiones, ya que no hay un dato de referencia que indique como está el problema en un periodo de tiempo y por lo tanto no se identifica cual es la causa del problema, aumentando los costos para la organización.

No.	Evidencia	Descripción
1	**Anexo No. 4:** Plan de Contingencia Hardware y Software Junio 2009	No se tiene un control estricto del tiempo perdido por el usuario por las interrupciones del servicio.

Tabla 31: Guía de Prueba 8

Tipo de registro: Guía de Pruebas				
Entidad Auditada	Hospital Universitario Departamental de Nariño E.S.E			**Nº Guía: P8**
Área Auditada	Módulo de Citas Medicas	Sistema	Dinámica Gerencial Hospitalaria	
R/PT:	Lista de Chequeo: **LC6_Nº Preg 4, 5, 8, 10, 11 13**			

Dominio	Entrega y Soporte
Procesos	DS4 Garantizar la continuidad del Servicio
Objetivo de Control	DS4.2 Planes de Continuidad de TI
	DS4.3 Recursos Críticos de TI
	DS4.4 Mantenimiento del Plan de continuidad
	DS4.5 Pruebas del Plan de Continuidad de TI
	DS4.6 Entrenamiento del Plan de Continuidad de TI
	DS4.7 Distribución del Plan de Continuidad de TI
	DS4.8 Recuperación y Reanudación de los Servicios de TI
	DS4.9 Almacenamiento de Respaldos Fuera de las Instalaciones
	DS4.10 Revisión Post Reanudación
Riesgos Asociados	• Al no existir una alternativa que permita la continuidad del desarrollo de los procesos en el módulo de citas médicas, se generan los siguientes riesgos: la suspensión del servicio de citas y de turnos, y la suspensión de solicitudes de historias clínicas. • Este represamiento de información lleva a la acumulación de trabajo afectando el desarrollo dinámico de la asignación de citas. • El no probar el plan de recuperación de datos genera riesgo de pérdida total o parcial de datos.

No.	Evidencia	Descripción
1	**No hay documentación para el modulo en caso de falla en el sistema** **Anexo No. 4:** Plan de Contingencia Hardware y Software	No se hace pruebas de los procedimientos para la recuperación de los datos.
2		El módulo de Citas Médicas no posee alternativas que permitan la continuidad del desarrollo de los procesos luego de una falla total en el sistema.
3		No se ha contemplado un documento que describa cual fue el desastre su causa y acciones que se seguirán después de la recuperación del sistema.

4		Tampoco se han puesto a prueba los planes de continuidad del servicio en el Modulo de Citas Médicas.
5		No se comunican los planes de continuidad del servicio al área de citas médicas.

Tabla 32: Guía de Prueba 9

Tipo de registro: Guía de Pruebas				
Entidad Auditada	Hospital Universitario Departamental de Nariño E.S.E			**Nº Guía: P9**
Área Auditada	Módulo de Citas Medicas	Sistema	Dinámica Gerencial Hospitalaria	
R/PT:	ENTREVISTA: **ENT4 – N° Preg 1**			

Dominio	Entrega y Soporte	
Procesos	DS4 Garantizar la continuidad del Servicio	
Objetivo de Control	DS4.2 Planes de Continuidad de TI	
	DS4.3 Recursos Críticos de TI	
	DS4.4 Mantenimiento del Plan de continuidad	
	DS4.5 Pruebas del Plan de Continuidad de TI	
	DS4.6 Entrenamiento del Plan de Continuidad de TI	
	DS4.7 Distribución del Plan de Continuidad de TI	
	DS4.8 Recuperación y Reanudación de los Servicios de TI	
	DS4.9 Almacenamiento de Respaldos Fuera de las Instalaciones	
	DS4.10 Revisión Post Reanudación	
Riesgos Asociados	• Al no existir una alternativa que permita la continuidad del desarrollo de los procesos en el módulo de citas médicas, se generan los siguientes riesgos: la suspensión del servicio de citas y de turnos, y la suspensión de solicitudes de historias clínicas. • Este represamiento de información lleva a la acumulación de trabajo afectando el desarrollo dinámico de la asignación de citas	
No.	**Evidencia**	**Descripción**
1	**EVI_AUDIO_7**	Las auxiliares o funcionarias del módulo de citas médicas no conocen el plan de contingencia de la organización.

Tabla 33: Guía de Prueba 10

Tipo de registro: Guía de Pruebas				
Entidad Auditada	Hospital Universitario Departamental de Nariño E.S.E			**Nº Guía: P10**
Área Auditada	Módulo de Citas Medicas	Sistema	Dinámica Gerencial Hospitalaria	
R/PT:	CUESTIONARIOS/Entrevista: **ENT5_Nº Preg 1, 2, 3**			

Dominio	Adquirir e Implementar	
Procesos	AI1 Identificar Soluciones Automatizadas	
Objetivo de Control	AI1.1 Definición y Mantenimiento de los Requerimientos Técnicos y Funcionales del Negocio	
Riesgos Asociados	• Al no existir un análisis de requerimientos puede ocasionar riesgos como fallas continuas en el sistema ya que estas no se corrigen. • Al no existir un análisis de requerimientos puede ocasionar riesgos como costos elevados para la organización ya que si el software no cumplió las expectativas de trabajo se debe pensar en otro.	
No.	**Evidencia**	**Descripción**
1	EVIDENCIA EN AUDIO/ EVI_AUDIO_15 **Anexo No. 7:** Ley 100 de 1993	No se cuenta con un estudio de los requerimientos de hardware y software en el área de citas medicas Tampoco plan para el rediseño o modificación de estos requerimientos.

Tabla 34: Guía de Prueba 11

Tipo de registro: Guía de Pruebas				
Entidad Auditada	Hospital Universitario Departamental de Nariño E.S.E			**Nº Guía: P11**
Área Auditada	Módulo de Citas Medicas	Sistema	Dinámica Gerencial Hospitalaria	
R/PT:	CUESTIONARIOS/Entrevista: **ENT6_Nº Preg 3** CUESTIONARIOS/Lista de Chequeo: **LC4_NºPreg 3, 4** CUESTIONARIOS/Lista de Chequeo: **LC5_NºPreg 9**			

Dominio	Adquirir e Implementar
Procesos	AI4 Facilitar la Operación y Uso
Objetivo de Control	AI4.3 Transferencia de Conocimiento a Usuarios Finales
Riesgos Asociados	Al no capacitar al personal de reemplazo genera riesgo como: ✓ el represamiento del trabajo. ✓ errores en la ejecución del software como por ejemplo ingreso de datos erróneos y por consiguiente incorrecta asignación de citas o de turnos médicos.

No.	Evidencia	Descripción
1	EVIDENCIA EN AUDIO/ EVI_AUDIO_16 **Anexo No. 8:** (42571-98054) NUM_CITAS_MEDICAS.NET V 002 **ANEXO No. 9:** (83313-33777) 05 Citas Médicas DGH	No se les presenta la información documentada o manual de usuarios del aplicativo a las auxiliares del módulo de citas médicas.
2	**Anexo No. 11:** Manual de Capacitación y Soporte	No se les realiza capacitaciones o entrenamiento continuo a las auxiliares para la transferencia de conocimiento.

Tabla 35: Guía de Prueba 12

Tipo de registro: Guía de Pruebas				
Entidad Auditada	Hospital Universitario Departamental de Nariño E.S.E			**Nº Guía: P12**
Área Auditada	Módulo de Citas Medicas	Sistema	Dinámica Gerencial Hospitalaria	
R/PT:	CUESTIONARIOS/Lista de Chequeo: **LC4_NºPreg 1**			

Dominio	Adquirir e Implementar
Procesos	AI4 Facilitar la Operación y Uso
Objetivo de Control	AI4.1 Plan para Soluciones de Operación
	AI4.4 Transferencia de Conocimiento de Operaciones y Soporte
Riesgos Asociados	Una incorrecta instalación del software lleva a que el sistema trabaje erróneamente arrojando posibles datos equivocados y por ende el trabajo se puede ver afectado.

No.	Evidencia	Descripción
1	No hay documento técnico del software **Anexo No. 8:** (42571-98054) NUM_CITAS_MEDICAS.NET V 002 **Anexo No. 9:** (83313-33777) 05 Citas Médicas DGH	No se cuenta con documentación donde se identifiquen los aspectos técnicos y capacidad de operación del software.

Tabla 36: Guía de Prueba 13

Tipo de registro: Guía de Pruebas				
Entidad Auditada	Hospital Universitario Departamental de Nariño E.S.E			**Nº Guía: P13**
Área Auditada	Módulo de Citas Medicas	Sistema	Dinámica Gerencial Hospitalaria	
R/PT:	CUESTIONARIOS/Lista de Chequeo: **LC1_NºPreg 4,5,6,7,8**			

Dominio	Adquirir e Implementar
Procesos	AI4 Facilitar la Operación y Uso
Objetivo de Control	AI4.1 Plan para Soluciones de Operación
	AI4.4 Transferencia de Conocimiento de Operaciones y Soporte
Riesgos Asociados	Existe el riesgo de que personas propias o ajenas a la organización introduzcan datos que afecten el procesamiento de la información, por ejemplo el ingreso de datos falsos.

No.	Evidencia	Descripción
1	**Anexo No. 10:** REPORTE DE PERFILES DE USUARIO DEL SISTEMA	Las auxiliares tienen habilitadas todas las funcionalidades del software, aunque algunas de ellas no corresponden a su trabajo

Tabla 37: Guía de Prueba 14

Tipo de registro: Guía de Pruebas				
Entidad Auditada	Hospital Universitario Departamental de Nariño E.S.E			**Nº Guía: P14**
Área Auditada	Módulo de Citas Medicas	Sistema	Dinámica Gerencial Hospitalaria	
R/PT:	CUESTIONARIOS/Lista de Chequeo: **LC3_Nº Preg 14**			

Dominio	Entrega y Soporte
Procesos	DS12 Administración del Ambiente Físico
Objetivo de Control	DS12.1 Selección y Diseño del Centro de Datos
	DS12.2 Medidas de Seguridad Física
	DS12.3 Acceso Físico
	DS12.4 Protección Contra Factores Ambientales
	DS12.5 Administración de Instalaciones Físicas
Riesgos Asociados	• La inadecuada colocación de señales en el lugar de trabajo puede disminuir la productividad porque habría riesgo de lesión en el personal en el momento de que ocurra una desgracia. • Al no haber un extintor en el área puede haber riesgos de pérdidas de vida, aunque exista un extintor cercano es probable que en un momento de emergencia la salida se pueda obstruir.

No.	Evidencia	Descripción
1	EVIDENCIA FOTOGRAFICA**/ EVI_FOTO_6**	El aviso de alarmas de evacuación no se encuentra bien ubicado para que el personal lo visualice.
2	EVIDENCIA FOTOGRAFICA**/ EVI_FOTO_13**	El área no cuenta con salidas de emergencias en caso de una emergencia.
3	EVIDENCIA FOTOGRAFICA**/ EVI_VIDEO_17**	El área de citas médicas no cuenta con extintores y sistemas de irrigación.

Tabla 38: Guía de Prueba 15

Tipo de registro: Guía de Pruebas				
Entidad Auditada	Hospital Universitario Departamental de Nariño E.S.E			**Nº Guía: P15**
Área Auditada	Módulo de Citas Medicas	Sistema	Dinámica Gerencial Hospitalaria	
R/PT:				

Dominio	Entrega y Soporte
Procesos	DS13 Administración de Operaciones
Objetivo de Control	DS13.1 Procedimientos e intrusiones de operación
Riesgos Asociados	Al no existir coordinación entre quienes dirigen el módulo de citas médicas puede provocar suspensión del servicio de citas, por la confusión de los usuarios.

No.	Evidencia	Descripción
1	**Anexo No. 2:** Jarg Subproceso Citas Médicas por EPS **Anexo No. 10:** Manual de funciones	El diagrama de procesos esta desactualizado.
2		Solamente la organización tiene el diagrama de procesos para asignación de citas por EPS y no se tiene el diagrama para asignación de citas a particulares.
3		En un principio se dijo que la tarea de asignación de turno era una labor del administrador del módulo de citas médicas en conjunto con la líder del mismo, pero las funcionarias del Call Center también deben hacer esa tarea.
4		El encargado de la administración del Módulo de Citas Médicas no ejerce sus funciones porque se cree que no hay problemas dentro del módulo, y por lo tanto quien tiene más conocimiento según el propio administrador del módulo es el coordinador de gestión de información del hospital.

Tabla 39: Guía de Prueba 16

Tipo de registro: Guía de Pruebas				
Entidad Auditada	Hospital Universitario Departamental de Nariño E.S.E			**Nº Guía: P16**
Área Auditada	Módulo de Citas Medicas	Sistema	Dinámica Gerencial Hospitalaria	
R/PT:	CUESTIONARIOS/Lista de Chequeo: **LC1_Nº Preg 20**			

Dominio	Entrega y Soporte	
Procesos	DS5 Garantizarla Seguridad de los Sistemas	
	DS11 Administración de datos	
Objetivo de Control	DS5.7 Protección de Tecnología de Seguridad	
	DS11.6 Requerimientos de seguridad para la administración de datos	
Riesgos Asociados	La repetición de la contraseña que se asigna por defecto genera el siguiente riesgo: relacionado con que la organización queda expuesta a riesgos relacionados con que los funcionarios puedan llevarse un reporte de datos o información confidencial o reservada.	
No.	**Evidencia**	**Descripción**
1	EVIDENCIA IMÁGENES/ EVI_IMG_1	La contraseña que asigna por defecto el sistema cuando la restablece se repite en usuarios diferentes ya sea que tengan perfil de administrador o usuario convencional.
2	EVIDENCIA IMÁGENES/ EVI_IMG_2	Dos funcionalidades: la creación de médico y creación de especialistas se repiten en dos módulos: Historias clínicas y Citas médicas.

3.5. INFORMES DE LA AUDITORIA

3.5.1. Informe gerencial de auditoría

Doctor
WILSON LARRANIAGA
Gerente Hospital Universitario Departamental de Nariño E.S.E.

Luego de realizar las distintas pruebas y aplicar la metodología de la auditoria, teniendo como objetivo principal: realizar el proceso de auditoría al SISTEMA DE INFORMACION DINAMICA GERENCIAL HOSPITALARIA en el MODULO DE CITAS MEDICAS para el Hospital Universitario Departamental De Nariño con el fin de establecer el grado de confiabilidad y elaborar las recomendaciones necesarias que garanticen el correcto funcionamiento de sus procesos. Se obtuvieron los siguientes resultados.

ALCANCE Y DELIMITACION

La gestión de Citas Medicas es una herramienta para la administración del recurso médico, la optimización y la correcta planeación de citas de cada uno de los profesionales por especialidad que se encuentran vinculados al Hospital Universitario Departamental de Nariño E.S.E, el módulo de citas médicas no solo abarca la acción en sí de la petición de una cita por parte del paciente, sino que comprende también el proceso en que transcurre la cita, y los resultados que de ella salgan. El alcance del proyecto evaluó los siguientes aspectos:

En cuanto a seguridad

Las auxiliares del módulo no cambian la clave de entrada al Sistema Dinámica Gerencial Hospitalaria cada 6 meses, aun las funcionarias no han firmado ni renovado el acuerdo de cumplimiento sobre la seguridad y confidencialidad de la información, tampoco los funcionarios recibieron documentación acerca de los permisos que tienen para manejar el sistema.

Otro de los hechos encontrados es que personas externas al área del Call center usan los teléfonos, los equipos de cómputo para asuntos personales, además esta área es utilizada por personal del hospital para almorzar.

En la seguridad de los datos en el sistema, las auxiliares del módulo olvidan cerrar el sistema y se dejan documentos de citas médicas sobre el escritorio al

ausentarse por un momento del puesto de trabajo, y se permite la conexión de dispositivos USB generando posible robo de información.

Entre las cosas positivas que se pueden destacar en cuanto a seguridad es la existencia de políticas de gestión de información con el fin de ejercer control dentro de la organización y la presencia de cámaras de seguridad.

En cuanto a recursos humanos

Las cosas positivas que se pueden destacar en cuanto a Recursos Humanos es la disposición de las funcionarias del Call Center en brindar la información para llevar el proceso de auditoría. Además existe una clara distribución de los cargos de los funcionarios.

La capacitación del personal de reemplazo de las auxiliares del módulo en el momento que ocurre ausencia temporal de estas funcionarias genera contratiempos debido al tiempo de inducción, al igual que no procura tener en cuenta los conocimientos de las funcionarias encargadas de manejo del módulo, para ser aprovechado posteriormente en la probabilidad de que estas funcionarias abandonen el cargo.

Las auxiliares del módulo de citas médica olvidan las normas y reglamentaciones para el subproceso del Call center ya establecidas por la Junta Directiva como de la Coordinación de Urgencias, Consulta Externa y Coordinación de Gestión de información.

En cuanto a continuidad del servicio

Falta un control sobre el tiempo perdido por el usuario debido a interrupciones en el servicio por razones ajenas a los funcionarios y no se cuenta con un registro sobre los errores más comunes, de la misma forma se debe contemplar un informe que describa las acciones que se tomaron después de recuperado el sistema como tampoco se han puesto a pruebas los planes de continuidad del servicio del módulo de citas médicas.

En caso de una falla total en el sistema principal el módulo de citas médicas debería contar con una alternativa que permita la continuidad del servicio, así mismo aún falta llevar pruebas que demuestren la eficacia del plan de recuperación de datos de toda la organización ante cualquier desastre.

Las auxiliares del módulo de citas médicas desconocen la existencia de un plan de continuidad o de contingencia de los recursos de TI involucrados en el módulo de citas y de la organización en general.

Hay que destacar la existencia de un plan de contingencia de hardware y software que describe el recurso con que cuenta el hospital y los posibles problemas a los cuales se enfrentaría.

En cuanto a objetivos de la organización

Falta un estudio particular sobre las necesidades o requerimientos de hardware, software y procedimientos del área de citas médicas.

Cabe resaltar que la ley 100 de 1993 es una base de cómo debe ser la prestación de servicios de salud.

En cuanto a uso del software

Entre las cosas positivas que se pueden destacar en cuanto a Uso del Software es la existencia de un manual de usuario de la empresa desarrolladora del Sistema Dinámica Gerencial Hospitalaria y el manejo del software no es complicado.

A los funcionarios aún no se les ha distribuido los manuales de usuario de las aplicaciones instaladas en los equipos del Call Center y ni la documentación que especifique que aspectos técnicos tiene sistema Dinámica Gerencial Hospitalaria.

A pesar de que las auxiliares tienen unas funciones definidas en el módulo de citas médicas, el aplicativo Dinámica Gerencial Hospitalaria tiene abiertas todas las funcionalidades del módulo de citas médicas.

En cuanto a ambiente físico

En cuanto al aviso de alarma de evacuación tiene una incorrecta visualización de este, otro inconveniente en el área del call center es la ausencia de equipos extintores como tampoco una salida de emergencia, el extintor más cercano se encuentra fuera del Call Center. Otro aspecto negativo es la ubicación del área del Call Center ya que está en un lugar con demasiado ruido.

Entre las cosas positivas que se pueden destacar en cuanto a ambiente físico es la existencia de un plan contra desastres aunque lamentablemente no fue posible acceder a este para conocerlo a profundidad. De igual manera se destaca la

existencia de detectores de humo y la identificación de la red eléctrica regulada con color naranja.

En cuanto a operación

En un principio se dijo que la tarea de asignación de turno era una labor del administrador del módulo de citas médicas en conjunto con la líder del mismo, pero las funcionarias del Call Center también deben hacer esa tarea.

Otro de los inconvenientes observados es la desactualización del diagrama de procesos además el encargado de la administración del Módulo de Citas Médicas no ejerce sus funciones porque se cree que no hay problemas graves dentro del módulo.

El aspecto positivo a destacar en cuanto a Operación es la inicialización de la actualización del diagrama de procesos.

En cuanto a funcionamiento

En el aplicativo Dinámica Gerencial Hospitalaria se repite en diferentes perfiles la contraseña que asigna por defecto el sistema cuando hay necesidad de restablecerla

Dos funcionalidades: la creación de médico y creación de especialistas se repiten en dos módulos, Historias clínicas y Citas médicas.

Se pueden destacar en cuanto a Funcionamiento la interfaz amigable del Sistema Dinámica Gerencial Hospitalaria y el bloqueo de los usuarios cuando se ingresa de manera errónea la contraseña un determinado número de veces para de esta manera garantizar seguridad.

Además el sistema permite un seguimiento de las acciones que realizan los diferentes usuarios.

De antemano gracias por la atención prestada a este trabajo de auditoria.

Att:

Jaydivi Castillo

Lyda Johana Castro

Joana Narváez O.

3.5.2. Informe general de auditoría

Ingeniero
ROBERTO YANEZ
Coordinador de Gestión de Información del Hospital Universitario Departamental de Nariño E.S.E.

Luego de realizar las distintas pruebas y aplicar la metodología de la auditoria, teniendo como objetivo principal: realizar el proceso de auditoría al SISTEMA DE INFORMACION DINAMICA GERENCIAL HOSPITALARIA en el MODULO DE CITAS MEDICAS para el Hospital Universitario Departamental De Nariño con el fin de establecer el grado de confiabilidad y elaborar las recomendaciones necesarias que garanticen el correcto funcionamiento de sus procesos. Se obtuvieron los siguientes resultados.

Objetivo

Realizar el proceso de auditoría al SISTEMA DE INFORMACION DINAMICA GERENCIAL en el MODULO DE CITAS MEDICAS para el Hospital Universitario Departamental De Nariño con el fin de establecer el grado de confiabilidad y elaborar las recomendaciones necesarias que garanticen el correcto funcionamiento de sus procesos.

Objetivos específicos

- Conocer el funcionamiento del sistema DGH específicamente en el módulo de citas médicas, recolectando información sobre la documentación, el tipo de seguridad del sistema y los usuarios del mismo.

- Planear las actividades que se llevara a cabo dentro de la auditoria dentro de ellas el funcionamiento de los procesos internos de prestación del servicio, la preparación del plan de auditoria, el programa de auditoria y los papeles de trabajo.

- Ejecutar las pruebas sobre los procesos y el módulo de citas médicas para buscar evidencia que demuestre los hallazgos y confirmen la existencia de riesgos y vulnerabilidades dentro del proceso.

- Elaborar el informe finan de hallazgos y recomendaciones que servirán para ajustar los planes de mejoramiento.

ALCANCE Y DELIMITACION

La gestión de Citas Medicas es una herramienta para la administración del recurso médico, la optimización y la correcta planeación de citas de cada uno de los profesionales por especialidad que se encuentran vinculados al Hospital Universitario Departamental de Nariño E.S.E, el módulo de citas médicas no solo abarca la acción en sí de la petición de una cita por parte del paciente, sino que comprende también el proceso en que transcurre la cita, y los resultados que de ella salgan. Una visión general de la estructura del módulo de citas médicas está compuesta por archivos, procesos, informes, utilidades y unidades. El alcance del proyecto evaluó los siguientes aspectos: Seguridad, recursos humanos, licenciamiento, continuidad del servicio, objetivos de la organización, uso del software, ambiente físico y operaciones.

- En cuanto a la seguridad se evaluó si se cumplen las políticas generales de seguridad de la organización en cuanto a los procedimientos que se llevan a cabo en el módulo de citas médicas.

- En cuanto a recursos humanos se evaluó como se realiza el entrenamiento y desempeño de los funcionarios en el módulo de citas médicas.

- En el licenciamiento se evaluó el cumplimiento de la documentación de adquisición del software DGH

- Se evaluó si existen planes de contingencia para el módulo y que tanto conocen los funcionarios sobre estos planes.

- Se evaluó las necesidades o requerimientos del módulo de Citas Médicas que se tuvieron en cuenta para la adquisición del Software.

- En cuanto al uso del software se revisó el material de apoyo que existe para el personal del módulo, así mismo se valoró la funcionalidad del aplicativo.

- Se evaluó si existen planes de contingencia contra desastre para el módulo y que tanto conocen los funcionarios sobre estos planes.

- Se revisó si están definidos los procedimientos e instrucciones de operación para el módulo de citas médicas.

Para el proceso de auditoría se utilizó el método de auditoría COBIT como un estándar para la buena práctica de la auditoria.

HALLAZGOS MODULO DE CITAS MEDICAS

En seguridad

HALLAZGOS

- Las auxiliares del módulo de citas médicas no tienen una cuenta de usuario para iniciar sesión en el sistema operativo y la documentación que se encuentra en una de las particiones del sistema operativo está expuesta.

- Las auxiliares del módulo no cambian la contraseña del sistema cada 6 meses, desde el punto de vista de las funcionarias no ha sido necesario, aunque este requisito de seguridad si está contemplado dentro del plan general de gestión de información de la institución.

- En la política general de gestión de información no se tienen contempladas en que situaciones se debe hacer un cambio urgente de contraseña.
  - Las auxiliares del módulo como la líder de este no han firmado ni renovado el acuerdo de cumplimiento sobre la seguridad y confidencialidad de la información. Dentro de este punto se incluye la falta de una firma que comprometa a los funcionarios a no revelar la contraseña.

  - A los funcionarios que trabajan en el área de citas médicas no se les hace entrega de un documento que contenga cuáles son sus derechos de acceso de acuerdo a su perfil.

  - Periódicamente la coordinación de gestión de información no hace revisión de los derechos de acceso establecidos por el sistema.

  - Las personas externas que ingresan al Call center utilizan los equipos para asuntos personales.

- Facebook está habilitado en los equipos del Call center, violando la política 5 de gestión de información sobre el manejo de correo electrónico, herramienta y uso del internet:

    - ✓ El uso de Internet estará restringido según políticas de seguridad informática de la organización, desde el área de Gestión de Información se administran todos los accesos a Internet de los funcionarios que lo necesiten, evitando de esta forma colapsar el servicio de Internet.

    - ✓ El correo interno y el uso de Internet deben ser utilizados exclusivamente en las operaciones de la organización.

- Personas ajenas a las funcionarias del Call center utilizan el teléfono para asuntos personales.

- Además el puesto de trabajo es utilizado por las funcionarias y personas externas para almorzar.

- El puesto de trabajo es utilizado por las funcionarias y personas externas para mirar revistas de catálogo.

- Las auxiliares del módulo de citas médicas no cierran ni bloquean el sistema al ausentarse por un momento del puesto de trabajo.

- Los equipos utilizados en Call Center no se tiene desactivado el panel de control.

- Los documentos que se dejan en el escritorio no se retiran al ausentarse del puesto de trabajo.

- Se permite la conexión de dispositivos USB a los equipos del Call center.

- Los anteriores hechos demuestran que las auxiliares del módulo de citas médicas hacen caso omiso a las normas y reglamentaciones establecidas por la Coordinación de Gestión de información como son:

    - ✓ Todos los escritorios o mesas de trabajo deben permanecer limpios para proteger documentos en papel y dispositivos de almacenamiento como CD,s, USB memorykey, disquetes, con fin de reducir los riesgos de acceso no autorizado, perdida y daño de la información durante el horario normal de trabajo y fuera del mismo.

    - ✓ Las unidades de CD, Dvd, USB etc, permanecerá inactivas para la protección de la información contenida en la red corporativa y para evitar la instalación de software no licenciado por la empresa.

    - ✓ Así como las normas establecidas por la Junta Directiva como de la Coordinación de Urgencias, Consulta Externa y Coordinación de Gestión de información como son:

        - ➢ Se encuentra totalmente prohibido hacer uso de los teléfonos del Call Center por personas diferentes a las agentes, ya que esto incrementa el tiempo de espera.

        - ➢ Ninguna persona ajena a nuestra organización podrá ingresar al área de facturación y Call center evitando así el desorden y el tráfico de influencias.

        - ➢ Ninguna persona podrá ingresar al área del Call center, todo tipo de actividades de atención personalizada tendrá que hacerse por la ventanilla. Evitando el tráfico de influencias.

        - ➢ Se encuentra prohibido realizar cualquier tipo de actividades ajenas a las establecidas en los subprocesos de facturación y Call center.

Estas actividades se tendrán que realizar por fuera del sitio de trabajo.

RECOMENDACIONES

- En la política general de gestión de información se debe añadir como política de control de claves de acceso: crear una cuenta de usuario para iniciar sesión en el Sistema Operativo, y la contraseña correspondiente a la cuenta de usuario debe cumplir los mismos parámetros establecidos para el sistema Dinámica Gerencial Hospitalaria como son:

    - ✓ La longitud mínima de la contraseña debe ser como mínimo de cuatro caracteres.

    - ✓ La contraseña debe ser compleja es decir debe contener al menos una letra, un número y un carácter especial y debe ser diferente al nombre del usuario.

- El personal de gestión de información y en concreto el administrador del módulo de citas médicas debe hacer cumplir las políticas de contraseña.

- El personal deber concientizado en las sesiones de capacitación sobre la importancia del cambio de contraseña.

- En la política general de gestión de información se debe añadir como política de contraseña las situaciones o eventos en que se debe cambiar la contraseña por ejemplo: ataque al sistema, cambio de momentáneo de personal, entrada de terceros al sistema.

- La información se considera como uno de los activos principales del negocio por tal razón es recomendable incluir en los contratos laborables acuerdos o anexar pactos de confidencialidad que establezcan claramente las obligaciones de los trabajadores en ese sentido, con estos acuerdos

- Se informó a los funcionarios de las pautas a seguir en el tratamiento de la información confidencial, y se debe renovar estos pactos anualmente para confirmar la obligación de los trabajadores a no revelar ningún tipo de información.

- Elaborar un documento sobre los derechos de acceso de todos los funcionarios del hospital, este documento debe ser redactado de acuerdo a los módulos establecidos en la organización, además debe ser distribuido a los funcionarios de acuerdo a su perfil.

- El coordinador de gestión de información debe hacer cumplir las sanciones establecidas en la política 5 de gestión de información sobre el manejo de correo electrónico, herramienta y uso del internet:

  El usuario que sea sorprendido según el reporte diario del webmaster visitando sitios no autorizados por la empresa, en primera instancia se le hará el llamado de atención, en el segundo intento se le suspenderá el servicio como sanción a lo dispuesto en este documento.

- La oficina de gestión de información debe bloquear las páginas que no están autorizadas.

- Sensibilizar a todo el personal sobre la importancia de la seguridad en el puesto de trabajo.

- La oficina de gestión de información a través del administrador y líder del módulo de citas médicas debe brindar capacitaciones que den a conocer a las funcionarias del área de citas la importancia de seguir las normas ya establecidas para el subproceso del Call center, y hacer control continuo sobre el cumplimiento estas normas.

- De haber incumplimiento se debe tomar cierto tipo de acción correctiva o de sanción a la persona que haga caso omiso a las normas, procurando que la persona entienda que es de vital importancia que las cumpla, evitando el tráfico de influencias, y el incremento en el tiempo de espera en las llamadas.

En recursos humanos

HALLAZGOS

- Aunque existe personal que reemplace a las auxiliares del módulo en el momento que ocurre ausencia temporal de estas funcionarias, esto genera contratiempos porque se debe hacer una inducción al personal de reemplazo sobre el manejo del módulo empezando por lo complejo que es el conocimiento de todos los médicos del Hospital Universitario Departamental de Nariño E.S.E.

- No se tienen en cuenta los conocimientos de las funcionarias encargadas de manejo del módulo de citas médicas, para ser aprovechado posteriormente en la probabilidad de que estas funcionarias abandonen el cargo.

- Las auxiliares del módulo de citas médica hacen caso omiso a las normas y reglamentaciones para el subproceso del Call center ya establecidas por la Junta Directiva como de la Coordinación de Urgencias, Consulta Externa y Coordinación de Gestión de información como son:

    - ✓ Se encuentra totalmente prohibido hacer uso de los teléfonos del Call Center por personas diferentes a las agentes, ya que esto incrementa el tiempo de espera.

    - ✓ Ninguna persona ajena a nuestra organización podrá ingresar al área de facturación y Call center evitando así el desorden y el tráfico de influencias.

    - ✓ Ninguna persona podrá ingresar al área del Call center, todo tipo de actividades de atención personalizada tendrá que hacerse por la ventanilla. Evitando el tráfico de influencias.

    - ✓ Se encuentra prohibido realizar cualquier tipo de actividades ajenas a las establecidas en los subprocesos de facturación y Call center.

Estas actividades se tendrán que realizar por fuera del sitio de trabajo.

RECOMENDACIONES

- La capacitación que se brinda en cuanto al software y a la operación del módulo no solo debe involucrar a las funcionarias nombradas sino que debe extenderse también a las auxiliares de consulta externa que son el personal de reemplazo, dicha capacitación debe suministrar los manuales de operación para que en el momento que tenga que ausentarse una funcionaria sea mucho más ágil el proceso de reemplazo.

- Realizar un proceso documentado que permita recoger información sobre el conocimiento que los empleados tienen sobre su puesto de trabajo e ideas que mejoren los procesos operativos, lo que generaría mayor productividad.

- La oficina de gestión de información a través del administrador y líder del módulo de citas médicas debe brindar capacitaciones que den a conocer a las funcionarias del área de citas la importancia de seguir las normas ya establecidas para el subproceso del Call center.

- De no ser así se debe tomar cierto tipo de acción correctivo o de sanción a la persona que haga caso omiso a las normas, procurando que la persona entienda que es de vital importancia que las cumpla, evitando el tráfico de influencias, y el incremento en el tiempo de espera en las llamadas.

En continuidad del servicio

HALLAZGOS

- No se lleva un control sobre el tiempo perdido por el usuario debido a interrupciones en el servicio ocasionadas por factores que afectan a la seguridad del edificio y los que afectan la integridad de los datos.

- No se tiene un registro sobre los errores más comunes que permitan un análisis de probabilidad de ocurrencia de fallas en el área de citas médicas.

- Actualmente el módulo de citas médicas no cuenta con una alternativa que permita la continuidad del desarrollo de los procesos en caso de una falla total en el sistema principal.

- No se han llevado pruebas que demuestren la eficacia del plan de recuperación de datos ante cualquier desastre.

- No se tiene contemplado un informe que describa las acciones que se tomaron después de recuperado el sistema

- No se han puesto a pruebas los planes de continuidad del servicio del módulo de citas médicas para verificar si son efectivos.

- Las auxiliares del módulo de citas médicas no conocen de la existencia de un plan de continuidad o de contingencia de los recursos de TI involucrados en el módulo de citas y en la organización en general.

RECOMENDACIONES

- Elaborar un documento por cada eventualidad que genere interrupción del servicio, dicho documento debe contemplar los siguientes aspectos: contingencia, descripción de la contingencia, recurso afectado, tiempo de suspensión del servicio, firma del administrador de citas médicas. Esta documentación servirá de apoyo al plan de contingencia ya que se puede medir cuales son los eventos más frecuentes que se presentan en el área de citas médicas y que afectan su continuo desarrollo y a su vez este reporte servirá de apoyo a otras dependencias.

- Anexar al plan de contingencia del hospital la documentación correspondiente a las tareas que deben seguirse y los responsables que deben ejecutarlas y capacitar al personal sobre el plan alternos de citas médicas.

- Una vez se tenga este plan realizar las pruebas pertinentes para intentar valorar el impacto real de un posible problema dentro de los escenarios establecidos como posibles.

- Elaborar el formato en el que se pueda hacer un informe del evento que llevo a la recuperación del sistema.

- La oficina de gestión de información a través del administrador del módulo de citas médicas debe brindar capacitaciones que den a conocer a las funcionarias del área de citas la importancia del plan de contingencia de la organización, el contenido de este plan y cuál sería el rol de cada funcionaria en el momento de presentarse algún evento que genere alguna contingencia.

- Elaborar el plan de continuidad del área de citas médicas, en el que se contemple con exactitud que recursos de TI se ven involucrados, los riesgos a los que se expone el área, los pasos a seguir para controlar la contingencia, los responsables de ejecutar las tareas. El objetivo principal del plan es permitir al área seguir operando bajo condiciones adversas, al implantar estrategias adecuadas, objetivos de recuperación, planes de gestión de crisis y estrategias de gestión de riesgos, facilitando a la Organización de una estructura preparada para mantener la flexibilidad y la capacidad de una efectiva respuesta en la protección de los intereses principales, tales como: información, activos de valor, continuidad de procesos y operaciones.

En objetivo de la organización

HALLAZGOS

- No existe un estudio particular sobre las necesidades o requerimientos de hardware, software y procedimientos del área de citas médicas.

RECOMENDACIONES

- Elaborar un estudio de requerimientos del Área de Citas Médicas para conocer que mejoras se deben hacer a los procesos. Este estudio permite profundizar los siguientes aspectos: cómo se lleva el proceso básico, que datos utiliza o produce el área, cuales son los límites impuestos por el tiempo y carga de trabajo, los controles de desempeño que se utilizan.

En uso del software

HALLAZGOS

- Los funcionarios no tienen los manuales de usuario de las aplicaciones instaladas en los equipos del Call Center.

- Al no existir información documental de la aplicación las auxiliares del módulo no tienen una herramienta de consulta.

- No existe documentación sobre los aspectos técnico del sistema Dinámica Gerencial Hospitalaria.

- Las auxiliares del Call Center tienen habilitadas todas las funcionalidades del módulo de citas médicas del aplicativo DGH, a pesar de que algunas de sus funcionalidades no son de su competencia.

- Las auxiliares del Call Center tienen habilitadas todas las funcionalidades del módulo de citas médicas del aplicativo DGH, a pesar de que algunas de sus funcionalidades no son de su competencia.

RECOMENDACIONES

- La oficina de gestión de información debe elaborar un manual de usuario que facilite el conocimiento sobre:

  - ✓ cuáles son los datos del entrada,
  - ✓ como se debe obtener los resultados
  - ✓ cuáles son los datos de salida
  - ✓ como son los formatos de los documentos
  - ✓ en qué momento se debe pedir una operación o una información específica.

- El manual de usuario debe ser redactado en forma clara e ir de acuerdo al tipo de usuario que usa el sistema y debe entregarse como parte del entrenamiento de las funcionarias oficiales y del personal de reemplazo.

- La coordinación de gestión de información deberá elaborar el documento describiendo cuales son los aspecto en cuanto a software y hardware que se deben tener en cuenta antes de la instalación, así mismo el documento debe detallar los pasos a seguir para la instalación y una sesión de los posibles problemas que se pueden generar en la instalación junto con la forma de solucionarlos.

- La coordinación de gestión de información debe elaborar un documento donde se describa cuáles son los perfiles de usuario que deben funcionar dentro de la institución dicho documento debe ir apoyado por cada uno de los líderes del módulo.

- Este documento debe ser distribuido a cada de los administradores de los respectivos módulos para que ellos hagan una revisión continua de los perfiles de usuario configurados en el sistema.

- La coordinación de gestión de información debe elaborar un documento donde se describa cuáles son los perfiles de usuario que deben funcionar dentro de la institución dicho documento debe ir apoyado por cada uno de los líderes del módulo.

- Este documento debe ser distribuido a cada de los administradores de los respectivos módulos para que ellos hagan una revisión continua de los perfiles de usuario configurados en el sistema.

En ambiente físico

HALLAZGOS

- El aviso de alarma de evacuación no tiene una correcta visualización ya que sobre él hay una mesa de escritorio.

- Dentro del área no existen equipos extintores como tampoco una salida de emergencia. El extintor más cercano se encuentra fuera del Call Center.

- El área del Call Center está ubicado en un lugar con demasiado ruido.

RECOMENDACIONES

- Colocar las señales de alarma o de cualquier otro tipo de emergencia en un lugar visible.

- Colocar el equipo extintor correspondiente al área y contemplar la construcción de una salida de emergencia por ejemplo en la parte lateral o trasera del Call center.

- Colocar una división que separe el Call Center de facturación previniendo de esta manera que se entre el ruido.

En operación

HALLAZGOS

- El diagrama de procesos esta desactualizado.

- Solamente la organización tiene el diagrama de procesos para asignación de citas por EPS y no se tiene el diagrama para asignación de citas a particulares.

- En un principio se dijo que la tarea de asignación de turno era una labor del administrador del módulo de citas médicas en conjunto con la líder del mismo, pero las funcionarias del Call Center también deben hacer esa tarea.

- El encargado de la administración del Módulo de Citas Médicas no ejerce sus funciones porque se cree que no hay problemas dentro del módulo, y por lo tanto quien tiene más conocimiento según el propio administrador del módulo es el coordinador de gestión de información del hospital.

RECOMENDACIONES

- Actualizar el diagrama de procesos considerando que se pueden asignar citas por EPS y a particulares.

- El coordinador de gestión de información debe controlar que el administrador del módulo ejerza sus funciones en forma continua y no cuando ocurra un evento inesperado evitando así el desorden en la organización, un administrador permanente facilita la entrega de información más precisa a quienes este interesados en conocer el funcionamiento de los diferentes procesos.

- El manual de funciones de la organización debe mejorarse, especificando claramente cada uno de los cargos y las funciones y no debe ir de acuerdo a un departamento en general.

En funcionamiento

HALLAZGOS

- La contraseña que asigna por defecto el sistema cuando la restablece se repite en usuarios diferentes ya sea que tengan perfil de administrador o usuario convencional.

- Dos funcionalidades: la creación de médico y creación de especialistas se repiten en dos modulo, Historias clínicas y Citas médicas.

RECOMENDACIONES

- La coordinación de gestión de información debe realizar un informe sobre estos errores para luego ser noticiado a los ingenieros de soporte de Sistemas

y Asesorías de Colombia para que analicen los errores y hagan las pruebas pertinentes, las analicen y hagan las correcciones necesarias.

LIMITACIONES

- Al momento las entrevistas la Directora del Módulo no tenía conocimiento de que al Módulo de Citas Médicas se le estuviese realizando la auditoria razón por la cual se opuso a entregarnos algún tipo de información del manejo y funcionamiento del módulo.

- No se contó con una buena disponibilidad tanto del Ingeniero Roberto Yánez como la de las auxiliares del módulo los cuales se negaron en muchas ocasiones a brindarnos información relevante para el desarrollo de la auditoria.

- Cuando pedimos que se nos instalara el sistema en nuestro computador para adquirir conocimiento de cómo es el funcionamiento del módulo y realizar las pruebas necesarias, el sistema quedo mal instalado impidiéndonos que realizar dichas pruebas.

Resultado de la Auditoria

A continuación se presentan los resultados de la auditoría aplicada al Módulo de Citas Médicas del sistema de información Dinámica Gerencial Hospitalaria (DGH) implementado en el Hospital Universitario Departamental de Nariño E.S.E., también se presentan los hallazgos y las recomendaciones de mejoramiento según los dominios y procesos del COBIT auditados.

De antemano gracias por la atención prestada a este trabajo de auditoria.

Att:

_____

Jaydivi Castillo

_____

Lyda Johana Castro

_____

Joana Narváez O.

3.6. EVALUACIÓN DE FUNCIONAMIENTO DEL MÓDULO DE CITAS MÉDICAS SEGÚN EL COBIT (CONTROL OBJECTIVES FOR INFORMATION AND RELATED TECHNOLOGY)

Teniendo como guía el COBIT se pudo concluir que el funcionamiento del Módulo de Citas Médicas en términos generales es bueno, pero hay que tener en cuenta las normas, políticas de seguridad y los planes de contingencia ya que es aquí en estos puntos donde se encontraron la mayoría de las falencias del mismo tales como:

- No siguen o se tienen en cuenta a cabalidad las políticas de seguridad y las normas con las que organización cuenta.

- No se brinda capacitación a los funcionarios del Módulo en cuanto a los planes de contingencia con los que la organización cuenta, razón por la cual en caso de una emergencia o desastre los mismos no sabrían cómo actuar ante tal evento.

3.7. EVALUACIÓN DE FUNCIONAMIENTO DEL MÓDULO DE CITAS MÉDICAS SEGÚN LA LEY 100 DE 1993

De acuerdo a la ley 100 de 1993 se puede decir que el Módulo de citas Médicas cumple pero no a cabalidad ya que a pesar de haberse mejorado la prestación de servicios no es suficiente porque la demanda de citas médicas supera por casi el doble la oferta que el hospital tiene.

4. CONCLUSIONES

COBIT no es una estructura que contiene una serie de pasos formales de cómo debe hacerse una auditoria, COBIT es una guía que sugiere bajo que lineamientos se debe realizar el análisis y la evaluación de los controles existentes en una empresa para las tecnologías de la información.

La auditoría de sistemas y la auditoria informática son las herramientas con la que los ingenieros de sistemas cuentan para evaluar y verificar el funcionamiento de los sistemas de información y los procesos que se llevan a cabo en una organización dentro de estos, un marco de trabajo importante para la evaluación de los mismos es el COBIT que permite verificar que los sistemas están funcionando de forma correcta y que las actividades y procesos son llevados a cabo de una forma eficiente y eficaz.

Realizar una auditoría a una organización tiene como ventajas ayudar a la gerencia o a la administración a evaluar los sistemas de una entidad con el fin de observar de manera objetiva los problemas de una empresa que han pasado desapercibidos y de esta manera poner a disposición de la administración el conocimiento de las operaciones que se realizan en la entidad auditada.

La auditoría permite identificar las amenazas inmediatas y de esta manera reducir los riesgos, favorecer la protección de los recursos de una empresa, mayor comprensión de la información y de los procesos, proporcionar recomendaciones con el ánimo de aportar en la soluciones de los problemas que se presenten.

Entre los aspectos negativos de una auditoria están: el personal de una organización es reacia a entregar información por desconocimiento de lo que es verdaderamente una auditoria, lo que lleva a que el auditor deba interpretar de la mejor manera posible el funcionamiento de los procesos de una entidad con los recursos que se le entregan.

Al aplicar esta auditoria se obtuvo como experiencia: que debe existir buena comunicación entre las personas auditadas y el auditor para poder tener una buena comprensión de lo que está sucediendo en la organización, la aclaración de algunos conceptos aprendidos en el área de auditoria, además nos permitió conocer a una de las entidades de salud más importantes del departamento de Nariño

5. RECOMENDACIONES GENERALES

Crear el documento de requerimientos del Módulo de Citas Médicas en el cual se contemplen todas las necesidades del módulo, incluyendo las que se tuvieron en cuenta a la hora de la adquisición del software, este documento debe también mencionar que artículo de la 100 de 1993 especifica las necesidades que deben cumplir los sistemas de información para las entidades prestadoras de salud.

Aislar el área del Call Center de otras dependencias para crear un mejor ambiente laboral.

Informar y capacitar de manera más responsable a los funcionarios del Módulo de citas Médicas y en general a toda la organización en cuanto a los planes existentes de seguridad en los sistemas y planes de contingencia.

Realizar vigilancia continua a quienes operan en el Módulo de Citas Médicas por parte de la coordinación de gestión de la información y el líder del Módulo con el fin de verificar que si se cumplen las normas establecidas por la institución y hacer seguimiento de las falencias que aparezcan en el módulo.

Actualizar el diagrama de procesos para que el conocimiento específico del módulo sirva de base para un estudio o planificación del área.

Realizar el diagrama de procesos o especificar cuáles es el proceso que se llevan a cabo para la asignación de citas a partículas.

Definir y tener claro cuáles son las tareas y actividades que debe realizar cada uno de los funcionarios del Módulo de Citas Médicas ya que al no tener claridad en este punto las auxiliares tiene sobre cargo de tareas realizando actividades que son pertinentes para ellas y tanto el líder del Módulo como el administrador del mismo deberían tener más conocimiento de todo el proceso que se lleva a cabo en el Modulo.

BIBLIOGRAFIA

Li, David H. Auditoría en centros de cómputo: objetivos, lineamientos y procedimientos. México: Trillas, 1990; 9682432596

Piattini, Mario. Auditoria informática. 2ª ed. Editorial RA-MA, 2000. 700 págs. 9788478974443

Instituto Mexicano de Contadores Públicos A. C. Procedimientos de auditoría en computación. México. 1982; 9686037152

Auditoria Informática, Disponible en: http://www.uaeh.edu.mx/docencia/P_Presentaciones/tlahuelilpan/sistemas/auditoria_informatica/auditoria_informatica.pdf

Auditoria operativa. Disponible en: http://www.gerencie.com/auditoria-operativa.html

Auditoria administrativa. Disponible en: http://www.gerencie.com/auditoria-administrativa.html

Auditoría financiera. Disponible en: http://www.gerencie.com/auditoria-financiera.html

Rossales Natii, Alcance de la auditoria informática (2013). Disponible en: http://www.slideshare.net/NatiiRossalesHidrobo/alcance-de-la-auditora-informtica

http://www.gerencie.com/auditoria

Audiconsystem. Disponible en: http://www.oocities.org/espanol/audiconsystem/auditori.htm

http://www.americanbpm.com/?q=es/resumen-de-las-normas-de-calidad-isoiec-9126-y-isoiec-14598

http://www.hosdenar.gov.co

Alexander Fredy, Gutierrez Lliana, Auditoria de Sistemas. Disponible en: http://www.slideshare.net/fbogota/auditoria-de-sistemas-introduccion-presentation

http://anaranjo.galeon.com/tipos_audi.html

Auditoria administrativa. Disponible en: http://www.gerencie.com/auditoria-informatica.html

Castillo Hector, Seguridad Informatica (2012). Disponible en: http://seguridad-informatica-1-iutll.blogspot.com/2012/11/seguridad-fisica-y-logica.html

Naranjo Alice, Conceptos de auditoria de Sistemas. Disponible en: http://anaranjo.galeon.com/conceptos.htm

Seguridad en el control de aplicaciones. Disponible en: http://www.slideshare.net/oosorioj/seguridad-en-el-control-de-aplicaciones

Naranjo Alice, Objetivos Generales de una Auditoría de Sistemas. Disponible en: http://anaranjo.galeon.com/objetiv_audi.htm

Auditoria de Sistemas. Disponible en: http://www.slideshare.net/VIVIANA1234567890/un3-informe-final-de-la-auditoria-de-sistemas

http://www.gerencie.com/auditoria-tecnicas.html

ANEXOS

Los siguientes anexos se entregan en medio magnético:

- **En la Carpeta EVIDENCIA EN AUDIO**

  Se encuentra las siguientes evidencias en audio:

  EVI_AUDIO_6
  EVI_AUDIO_7
  EVI_AUDIO_13
  EVI_AUDIO_14
  EVI_AUDIO_15
  EVI_AUDIO_16
  EVI_AUDIO_20

- **En la Carpeta EVIDENCIA EN VIDEO**

  Se encuentra la siguiente evidencia en video:

  EVI_VIDEO_17

- **En la Carpeta EVIDENCIA FOTOGRAFICA**

  Se encuentra la evidencia desde EVI_FOTO_1 hasta EVI_FOTO_19

- **En la Carpeta EVIDENCIA IMAGENES**

  Se encuentra la evidencia la **EVI_IMG_1** y la **EVI_IMG_2**

- **En la Carpeta CUESTIONARIOS**

  Se encuentran los archivos Lista de Chequeo y Entrevista

- **ANEXO No. 1-** DATOS ESTADISTICOS2009-2010-2011
- **ANEXO No. 2-** JARG SUBPROCESO CITAS MEDICAS POR EPS
- **ANEXO No. 3-** PLANEACION OPERATIVA DE GESTION UNIFICADO CON DATOS HISTORICOS 2005-2012
- **ANEXO No. 4-** PLAN DE CONTINGENCIA DE HARDWARE Y SOFTWARE JUNIO 2009.

- **ANEXO No. 5-** PLAN GERENCIA DE MEJORAMIENTO ESTANDAR GERENCIA DE LA INFORMACION.
- **ANEXO No. 6-** POLITICA DE GESTION DE INFORMACION
- **ANEXO No. 7-** Ley 100 de 1993
- **ANEXO No. 8-** (42571-98054) MUM_CITAS MEDICAS.NET V 002
- **ANEXO No. 9-** (83313-33777) 05 Citas Médicas DGH
- **ANEXO No. 10-** Manual de Funciones

ANEXO No. 11

REPORTE DE PERFILES DE USUARIO DEL SISTEMA

ANEXO No. 12

MANUAL DE CAPACITACION Y SOPORTE

ANEXO No. 13

PLANILLA DE CITAS

ANEXO No. 14

AUDITORIA DE CITAS

ANEXO No. 15

INFORMACION DEL PACIENTE

ANEXO No. 16

CONTRATO DE PRESTACIÓN DE SERVICIOS OJ 013– 2012