AUDITORÍA APLICADA A LA SEGURIDAD DEL SISTEMA DE INFORMACIÓN DINÁMICA GERENCIAL HOSPITALARIA DEL HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO

EDITH FRINEY DÍAZ FUELANTALA
MAIRA ALEJANDRA MORA ENRÍQUEZ

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

AUDITORÍA APLICADA A LA SEGURIDAD DEL SISTEMA DE INFORMACIÓN DINÁMICA GERENCIAL HOSPITALARIA DEL HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO

EDITH FRINEY DÍAZ FUELANTALA
MAIRA ALEJANDRA MORA ENRÍQUEZ

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

Director:
MANUEL BOLAÑOS GONZALEZ I.S.

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 el Trabajo de Grado son responsabilidad exclusiva del autor".

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

"La Universidad de Nariño no se hace responsable de las opiniones o resultados obtenidos en el presente trabajo y para su publicación priman las normas sobre el derecho de autor".

Artículo 13º del Acuerdo Nº. 005 de 2010, emanado del Honorable Concejo Académico de la Universidad de Nariño.

Nota de aceptación:

_____
_____
_____
_____
_____

_____
Firma del Presidente del Jurado

_____
Firma del Jurado

_____
Firma del Jurado

San Juan de Pasto, 26 de julio de 2013

AGRADECIMIENTOS

Brindamos nuestro más sincero agradecimiento a todas aquellas personas que estuvieron detrás de este sueño. En primer lugar a nuestro asesor, ingeniero Manuel Bolaños por todo su apoyo, calidad humana, por instruirnos y guiarnos para culminar este proyecto con gran éxito.

Al los ingenieros Francisco Solarte y Javier Villalba, porque además de ser nuestros jurados nos brindaron su amistad, su apoyo, nos dedicaron tiempo, paciencia y ánimo.

A nuestro compañero ingeniero John Sarmiento, quien siempre estuvo dispuesto a ayudarnos en el desarrollo del proyecto y nos demostró con su carácter que es posible terminar con excelencia lo que un día empezamos.

Además, damos gracias al coordinador del área de sistemas del Hospital Universitario Departamental de Nariño por su valiosa contribución, ya que sin ella no habría sido posible desarrollar y culminar el proyecto.

También queremos agradecer a la Universidad de Nariño, que nos dio la oportunidad y nos brindó todos los espacios para nuestra formación profesional. Además fue nuestro segundo hogar, donde compartimos momentos de felicidad, aprendimos a vencer temores e inseguridades y a mirar el mundo desde otra perspectiva.

Finalmente, agradecemos a nuestros amigos y familiares que de una u otra forma nos dieron el coraje para seguir adelante.

DEDICATORIA

Gracias Señor por tus misericordias que son nuevas cada mañana y porque se ve reflejado tu amor y fidelidad al cumplir uno de mis sueños más grandes, por eso y mucho más, te quiero dedicar el fruto de mi esfuerzo porque sé que sin ti nada es posible.

A mis padres Lidia del Carmen y Luis Eduardo, por darme la oportunidad de capacitarme, y quienes con su amor, apoyo, sabiduría y cuidado me orientaron por un buen camino y me siguen alentando para seguir adelante.

A mis hermanos Edna, Yazmin y Emil Deiby porque además de tolerar mis travesuras también me han enseñado a ser valiente y a esforzarme para conseguir todo lo que me he propuesto. A mi sobrino James que estuvo conmigo durante el desarrollo del proyecto y que con sus detalles me daba fuerzas para continuar.

A Alejandra por su compañía, paciencia y dulzura, porque además de ser mi colega es una gran amiga que siempre está apoyado mis sueños con sinceridad. A Wilson por enseñarme a ver con amor, alegría y serenidad la excelencia. A ellos que con su apoyo incondicional le dieron una pincelada de color a mi vida, con su lealtad a nuestra amistad.

A mis amigos que siempre quisieron que de lo mejor de mí, que me apoyaron sin importar la situación. A ellos gracias porque valoraron lo que soy, por eso los llevo en el corazón.

Edith Friney Díaz Fuelantala.

Al creador de todas las cosas, al que me ha dado fortaleza para continuar, me ha iluminado el camino y me ha regalado un poquito de su sabiduría, por eso dedico primeramente a Él, el fruto de mi esfuerzo y dedicación.

A mis padres Judith y Luis Antonio, por ser mis mejores maestros que con su dedicación, constancia y rectitud lograron hacer de mí una persona responsable, dedicada y entregada. A ellos que son siempre mi apoyo incondicional y me acompañaron con afán, empeño y muchos desvelos en este difícil proceso de mi formación profesional, les dedico este gran triunfo. Gracias por enseñarme que nunca debo dejar de soñar.

A mis hermanas Julie Angélica y Sandra Milena, que siempre han estado junto a mí, que han tenido el mismo sentir en mis logros y dificultades y que con su inmenso amor me alentaron a armarme de paciencia, a no caer en la desesperación, a levantarme y a comenzar de nuevo.

A mis amigos Edith y Wilson con quienes compartí grandes alegrías, tristezas y maravillosas experiencias que han sido significativas y de valor incalculable en mi vida. De quienes aprendí muchas cosas y de quienes recibí la mejor lección de amistad, compañerismo y solidaridad. A ellos les agradezco su cariño, sus palabras de aliento y el abrazo en los momentos más difíciles, por eso y mucho más los llevaré siempre en mi corazón.

Maira Alejandra Mora Enríquez.

RESUMEN

Este proyecto se centra en la realización de una auditoría para evaluar la eficiencia y eficacia de los procedimientos y controles de seguridad lógica que tiene el sistema de información Dinámica Gerencial Hospitalaria DGH, el cual es administrado por el Hospital Universitario Departamental de Nariño.

Para llevarla a cabo, se tomó como marco de referencia al estándar COBIT 4.1 y a la norma ISO/IEC 27002, de donde se seleccionaron diferentes procesos y objetivos de control con el fin de establecer el grado de cumplimiento de los mismos por parte de la entidad auditada.

Una vez analizados y evaluados todos los criterios, se encontraron una serie de hallazgos para los cuales se plantearon algunas recomendaciones que servirán de base para que el personal de sistemas del hospital tome las medidas necesarias y así pueda fortalecer y mejorar la seguridad lógica del sistema DGH.

ABSTRACT

This project focuses on conducting an audit to evaluate the efficiency and effectiveness of logic security procedures and controls performed in Dinámica Gerencial Hospitalaria Information System (DGH system), which is applied in the Hospital Universitario Departamental de Nariño.

To achieve this audit, the ISO / IEC 27002 standard and the COBIT 4.1 framework were taken as an outline to select different processes and control objectives in order to establish the degree of compliance by the entity audited.

The analysis and evaluation of all the criteria allowed to find some findings for which some recommendations were raised that will provide a base for the hospital systems personnel take the necessary steps so they can strengthen and improve the logic security of the DGH system.

CONTENIDO

pág.

LISTA DE TABLAS

pág.

LISTA DE FIGURAS

pág.

LISTA DE ANEXOS

pág.

GLOSARIO

ACCIÓN CORRECTIVA: medida de tipo reactivo orientada a eliminar la causa de una no-conformidad asociada a la implementación y operación del SGSI con el fin de prevenir su repetición.

ACCIÓN PREVENTIVA: medida de tipo pro-activo orientada a prevenir potenciales no-conformidades asociadas a la implementación y operación del SGSI.

ACEPTACIÓN DEL RIESGO: según [ISO/IEC Guía 73:2002]: decisión de asumir un riesgo.

ACTIVO: en relación con la seguridad de la información, se refiere a cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización. Según [ISO/IEC 13335-1:2004]: cualquier cosa que tiene valor para la organización.

ALERTA: una notificación formal de que se ha producido un incidente relacionado con la seguridad de la información que puede evolucionar hasta convertirse en desastre.

AMENAZA: según [ISO/IEC 13335-1:2004]: causa potencial de un incidente no deseado, el cual puede causar daño a un sistema o a la organización.

ANÁLISIS DE RIESGOS: según [ISO/IEC Guía 73:2002]: uso sistemático de información para identificar fuentes y estimar los riesgos.

APLICACIÓN: aunque se suele utilizar indistintamente como sinónimo genérico de 'programa' es necesario señalar que se trata de un tipo de programa específicamente dedicado al proceso de una función concreta dentro de la empresa.

ARCHIVO DE DATOS: cualquier archivo creado dentro de una aplicación, por ejemplo, un documento creado por un procesador de texto, una hoja de cálculo, una base de datos o un gráfico. También se denomina documento.

ARCHIVO LOG: archivo de texto que almacena generalmente datos sobre procesos determinados. Es como el 'diario' de algunos programas donde se graban todas las operaciones que realizan, para posteriormente abrirlo y ver que ha sucedido en cada momento.

ATACANTE: alguien que deliberadamente intenta hacer que un sistema de seguridad falle, encontrando y explotando una vulnerabilidad.

ATAQUE: acción intencional e injustificada. Intento por romper la seguridad de un sistema o de un componente del sistema.

AUDITOR: persona encargada de verificar, de manera independiente, la calidad e integridad del trabajo que se ha realizado en un área particular.

AUDITORÍA: proceso planificado y sistemático en el cual un auditor obtiene evidencias objetivas que le permitan emitir un juicio informando sobre el estado y efectividad del SGSI de una organización.

AUTENTICACIÓN: según [Magerit:1997]: característica de dar y reconocer la autenticidad de los activos del dominio (de tipo información) y/o la identidad de los actores y/o la autorización por parte de los autorizadores, así como la verificación de dichas tres cuestiones.

AUTENTICIDAD: proceso que tiene por objetivo asegurar la identificación de una persona o sistema.

BASE DE DATOS: colección de datos organizada de tal modo que el ordenador pueda acceder rápidamente a ella. Una base de datos relacional es aquella en la que las conexiones entre los distintos elementos que forman la base de datos están almacenadas explícitamente con el fin de ayudar a la manipulación y el acceso a estos.

CIA: acrónimo inglés de confidencialidad, integridad y disponibilidad, los parámetros básicos de la seguridad de la información.

CID: acrónimo español de confidencialidad, integridad y disponibilidad, los parámetros básicos de la seguridad de la información.

COBIT: *Control Objectives for Information and related Technology*. Guía de mejores prácticas, dirigida a la gestión de Tecnología de la Información. Publicado y mantenido por ISACA y el *IT Governance Institute*. 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.

CONFIDENCIALIDAD: según [NTC 5411-1:2006]: propiedad que determina la condición de que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

CONTROL: las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. (Nota: Control es también utilizado como sinónimo de salvaguarda o contramedida).

CONTROL CORRECTIVO: control que corrige un riesgo, error, omisión o acto deliberado antes de que produzca pérdidas. Supone que la amenaza ya se ha materializado pero que se corrige.

CONTROL DETECTIVO: control que detecta la aparición de un riesgo, error, omisión o acto deliberado. Supone que la amenaza ya se ha materializado, pero por sí mismo no la corrige.

CONTROL DISUASORIO: control que reduce la posibilidad de materialización de una amenaza, por ejemplo, por medio de avisos disuasorios.

CONTROL PREVENTIVO: control que evita que se produzca un riesgo, error, omisión o acto deliberado. Impide que una amenaza llegue siquiera a materializarse.

CRIPTOGRAFÍA: ciencia dedicada al estudio de técnicas capaces de conferir seguridad a los datos. El cifrado es fundamental a la hora de enviar datos a través de las redes de telecomunicaciones con el fin de conservar su privacidad.

CHECKLIST: lista de apoyo para el auditor con los puntos a auditar, que ayuda a mantener claros los objetivos de la auditoría, sirve de evidencia del plan de auditoría, asegura su continuidad y profundidad y reduce los prejuicios del auditor y su carga de trabajo. Este tipo de listas también se pueden utilizar durante la implantación del SGSI para facilitar su desarrollo.

DATOS: término general para la información procesada por un computador.

DECLARACIÓN DE APLICABILIDAD: documento que describe los objetivos de control y los controles pertinentes y aplicables para el SGSI de la organización.

DESASTRE: cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una organización durante el tiempo suficiente como para verse la misma afectada de manera significativa.

DISPONIBILIDAD: según [NTC 5411-1:2006]: propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.

EVALUACIÓN DE RIESGOS: según [ISO/IEC Guía 73:2002]: proceso de comparar el riesgo estimado contra un criterio de riesgo dado con el objeto de determinar la importancia del riesgo.

EVENTO: según [ISO/IEC TR 18044:2004]: suceso identificado en un sistema, servicio o estado de la red que indica una posible brecha en la política de seguridad de la información o fallo de las salvaguardas, o una situación anterior desconocida que podría ser relevante para la seguridad.

GESTIÓN DE LOS RIESGOS: según [ISO/IEC Guide 73:2002]: actividades coordinadas para dirigir y controlar una organización con respecto a los riesgos.

HARDWARE: conjunto de dispositivos de los que consiste un sistema. Comprende componentes tales como: teclado, mouse, unidades de disco y el monitor.

IMPACTO: el costo para la empresa de un incidente de la escala que sea, que puede o no ser medido en términos estrictamente financieros. Por ejemplo, pérdida de reputación, implicaciones legales, etc.

INCIDENTE: según [ISO/IEC TR 18044:2004]: evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

INTEGRIDAD: según [ISO/IEC 13335-1:2004]: propiedad de salvaguardar la exactitud y completitud de los activos.

INTERNET: interconexión de redes informáticas que permite a los computadores conectados comunicarse directamente.

INVENTARIO DE ACTIVOS: lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, reputación de la organización, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.

ISACA: *Information Systems Audit and Control Association*. Publica COBIT y emite diversas acreditaciones en el ámbito de la seguridad de la información.

ISO: Organización Internacional de Normalización, con sede en Ginebra (Suiza). Es una agrupación de organizaciones nacionales de normalización cuyo objetivo es establecer, promocionar y gestionar estándares.

ISO 17799: código de buenas prácticas en gestión de la seguridad de la información adoptado por ISO transcribiendo la primera parte de BS7799. A su vez, da lugar a ISO 27002 por cambio de nomenclatura el 1 de Julio de 2007. No es certificable.

ISO 19011: "*Guidelines for quality and/or environmental management systems auditing*". Guía de utilidad para el desarrollo de las funciones de auditor interno para un SGSI.

ISO 27001: estándar para sistemas de gestión de la seguridad de la información adoptado por ISO transcribiendo la segunda parte de BS7799. Es certificable. Primera publicación en 2005.

ISO 27002: código de buenas prácticas en gestión de la seguridad de la información (transcripción de ISO 17799). No es certificable. Cambio oficial de nomenclatura de ISO 17799:2005 a ISO 27002:2005 el 1 de Julio de 2007.

METODOLOGÍA: conjunto de métodos utilizados en la investigación científica.

NO CONFORMIDAD: situación aislada que, basada en evidencias objetivas, demuestra el incumplimiento de algún aspecto de un requerimiento de control que permita dudar de la adecuación de las medidas para preservar la confidencialidad, integridad o disponibilidad de información sensible, o representa un riesgo menor.

NORMA: principio que se impone o se adopta para dirigir la conducta o la correcta realización de una acción o el correcto desarrollo de una actividad.

OBJETIVO: declaración del resultado o fin que se desea lograr mediante la implementación de procedimientos de control en una actividad de TI determinada.

PAPELES DE TRABAJO: registra el planteamiento, naturaleza, oportunidad y alcance de los procedimientos de auditoría aplicados por el auditor y los resultados y conclusiones extraídas de 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.

PASSWORD: conocida también como 'clave de acceso'. Palabra o clave privada utilizada para confirmar una identidad en un sistema remoto, la cual se utiliza para que una persona no pueda usurpar la identidad de otra.

PDCA: *Plan-Do-Check-Act*. Modelo de proceso basado en un ciclo continuo de las actividades de planificar (establecer el SGSI), realizar (implementar y operar el

SGSI), verificar (monitorizar y revisar el SGSI) y actuar (mantener y mejorar el SGSI).

PLAN DE CONTINUIDAD DEL NEGOCIO: plan orientado a permitir la continuación de las principales funciones del negocio en el caso de un evento imprevisto que las ponga en peligro.

PLAN DE TRATAMIENTO DE RIESGOS: documento de gestión que define las acciones para reducir, prevenir, transferir o asumir los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.

POLÍTICA DE SEGURIDAD: documento que establece el compromiso de la Dirección y el enfoque de la organización en la gestión de la seguridad de la información. Según [ISO/IEC 27002:2005]: intención y dirección general expresada formalmente por la Dirección.

PROCEDIMIENTO: método o sistema estructurado para la ejecución de actividades. En computación, una subrutina o subprograma; como idea general, se presenta como un algoritmo separado del algoritmo principal, el cual permite resolver una tarea específica.

PROCESAMIENTO DE DATOS: conjunto de diferentes operaciones en secuencia sistemática sobre el dato, las cuales se basan en la elaboración, manipulación y tratamiento del mismo, mediante máquinas automáticas para producir los resultados esperados.

PROCESO: conjunto de operaciones lógicas y aritméticas ordenadas, cuyo fin es la obtención de resultados.

RECURSOS INFORMÁTICOS: todos aquellos componentes de hardware y programas (software) que son necesarios para el buen funcionamiento y la optimización del trabajo con computadores y periféricos, tanto a nivel individual, como colectivo u organizativo, sin dejar de lado el buen funcionamiento de los mismos.

RED: servicio de comunicación de datos entre computadores. Conocido también por su denominación inglesa "*network"*. Se dice que una red esta débilmente conectada cuando la red no mantiene conexiones permanentes entre los computadores que la forman. Esta estructura es propia de redes no profesionales con el fin de abaratar su mantenimiento.

REPOSITORIO: donde se almacenan los elementos definidos o creados por la herramienta, y cuya gestión se realiza mediante el apoyo de un Sistema de Gestión de Base de Datos (SGBD) o de un sistema de gestión de ficheros.

RIESGO: posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Según [ISO/IEC Guía 73:2002]: combinación de la probabilidad de un evento y sus consecuencias.

RIESGO RESIDUAL: nivel restante de riesgo después del tratamiento del riesgo.

SEGURIDAD DE LA INFORMACIÓN: según [ISO/IEC 17799:2005]: preservación de la confidencialidad, integridad y disponibilidad de la información; otras características también pueden estar involucradas, tales como la autenticidad, responsabilidad, aceptabilidad y confiabilidad.

SELECCIÓN DE CONTROLES: proceso de elección de los controles que aseguren la reducción de los riesgos a un nivel aceptable.

SGSI: Sistema de Gestión de la Seguridad de la Información. Según [ISO/IEC 27001:2005]: la parte de un sistema global de gestión que, basado en el análisis de riesgos, establece, implementa, opera, monitoriza, revisa, mantiene y mejora la seguridad de la información. (Nota: el sistema de gestión incluye una estructura de organización, políticas, planificación de actividades, responsabilidades, procedimientos, procesos y recursos.)

SERVICIOS DE TRATAMIENTO DE INFORMACIÓN: según [ISO/IEC 27002:2005]: cualquier sistema, servicio o infraestructura de tratamiento de información o ubicaciones físicas utilizadas para su alojamiento.

SISTEMA DE INFORMACIÓN: se denomina sistema de información al conjunto de procedimientos manuales y/o automatizados que están orientados a proporcionar información para la toma de decisiones.

SOFTWARE: componentes inmateriales del computador: programas, sistemas operativos, entre otros.

TI: Tecnologías de la Información.

TÉCNICA: es el procedimiento o el conjunto de procedimientos que tienen como objetivo obtener un resultado determinado, ya sea en el campo de la ciencia, de la tecnología, de las artesanías o en otra actividad.

TRATAMIENTO DE RIESGOS: según [ISO/IEC Guía 73:2002]: proceso de selección e implementación de medidas para modificar el riesgo.

VALORACIÓN DE RIESGOS: según [ISO/IEC Guía 73:2002]: proceso completo de análisis y evaluación de riesgos.

VULNERABILIDAD: debilidad en la seguridad de la información de una organización que potencialmente permite que una amenaza afecte a un activo. Según [ISO/IEC 13335-1:2004]: debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza.

INTRODUCCIÓN

En la actualidad, la información se ha convertido en uno de los principales recursos con los que puede contar toda organización, ya que es un factor determinante para el éxito y la continuidad del negocio. Ahora bien, si se desea maximizar la utilidad que posee dicha información, ésta se debe manejar de forma correcta y eficiente, tal y cómo se manejan los demás recursos existentes en la organización.

No obstante, a diario las empresas se ven amenazadas por riesgos que provienen tanto del exterior como del interior de las mismas, los cuales ponen en peligro la integridad de la información y con ello la viabilidad de los negocios. Por esta razón, es preciso que las empresas aseguren sus datos e información valiosa con la ayuda de la implementación de buenos controles de seguridad y con herramientas que permitan conocer, gestionar y minimizar los riesgos que atenten contra la seguridad de la información.

El Hospital Universitario Departamental de Nariño es consciente de la importancia que tiene la información, por ello adquirió un software denominado Dinámica Gerencial Hospitalaria DGH, cuyo objetivo es reducir tiempos de trabajo, ofrecer elementos para la toma de decisiones gerenciales en tiempo real y apoyar el desarrollo de los procesos misionales a través de la gestión de la información dentro de las áreas asistenciales, administrativas y financieras de la institución.

A raíz de ese acontecimiento, el hospital optó por la realización de auditorías externas, ya que permiten revisar y evaluar los controles, sistemas y procedimientos que se llevan a cabo en cualquier área de una organización, entregando como resultado un diagnóstico sobre su utilización y eficiencia junto con algunas recomendaciones que permitan mantener su rendimiento con altos niveles de calidad y/o mejorar las fallas detectadas.

Sin embargo, se ha pasado por alto la revisión de la efectividad de los controles de seguridad existentes en el sistema DGH, dando paso al posible robo de la información o daño del sistema por parte de personas maliciosas, quienes podrían aprovecharse de las vulnerabilidades para realizar su cometido. De ahí surgió la necesidad de realizar ésta auditoría aplicada a la seguridad lógica del software DGH, con el fin de aportar recomendaciones para solucionar o aminorar las

deficiencias del aplicativo, basándose en normas internacionales para la seguridad de la información.

Para describir detalladamente el proceso de auditoría al sistema DGH, este documento se organiza de la siguiente forma: en el primer capítulo se plantea el problema y su sistematización, además de los objetivos que se pretendían alcanzar, la justificación y la factibilidad del proyecto.

En el segundo apartado se despliega información general sobre las auditorías, las diferentes herramientas, técnicas y estándares utilizados para su desarrollo, la seguridad lógica, algunos aspectos legales de seguridad informática y datos sobre la entidad auditada.

Posteriormente, en el tercer capítulo, se describe la metodología a seguir para la ejecución del proyecto e inmediatamente después, se encuentra el desarrollo de la auditoría, el cual está conformado por el archivo permanente, que contiene información referente a la entidad, área y sistema auditado; el archivo corriente, donde se dan a conocer los diferentes criterios a evaluar y también se describen todos los instrumentos utilizados para la recolección de la información necesaria sobre el sistema DGH; el modelo de madurez del sistema; y por último, los informes de auditoría, en los cuales se exponen las fortalezas y falencias detectadas junto con algunas recomendaciones para su corrección.

A continuación, se presentan las conclusiones del trabajo, algunas recomendaciones a tener en cuenta y, finalmente, se muestra la bibliografía utilizada y un apartado de anexos que hacen referencia tanto a la documentación proporcionada por el hospital, como a las pruebas y demás archivos generados por el grupo auditor.

ELEMENTOS DE IDENTIFICACIÓN DEL PROBLEMA

TEMA

Título. AUDITORÍA APLICADA A LA SEGURIDAD DEL SISTEMA DE INFORMACIÓN DINÁMICA GERENCIAL HOSPITALARIA DEL HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO.

Modalidad. El presente proyecto de trabajo de grado corresponde a la modalidad estipulada como: PROYECTO DE APLICACIÓN.

Línea de investigación. El proyecto pertenece a la línea de investigación: GESTIÓN, SEGURIDAD Y CONTROL. Esta línea tiene como objetivo planificar, analizar, diseñar e implantar sistemas de control de información, con el propósito de brindar seguridad de la información en las organizaciones.

Alcance y delimitaciones. Este proyecto de auditoría permitió evaluar el funcionamiento del sistema de información Dinámica Gerencial Hospitalaria del Hospital Universitario Departamental de Nariño, identificando debilidades y fortalezas en cuanto a seguridad lógica y determinando el grado de cumplimiento del sistema de control con el marco de referencia COBIT (*Control Objectives for Information and Related Technology*) y el estándar internacional ISO/IEC 27002.

La evaluación se realizó haciendo uso de una copia del sistema DGH y de la base de datos que previamente se instalaron en el *laptop* del grupo auditor, así como información digital y entrevistas proporcionadas por el coordinador del área de sistemas.

Dentro de la evaluación se tuvo en cuenta la clasificación de datos, la administración de integridad, propiedad de datos, políticas de seguridad, entrenamiento del personal, administración de riesgos, mantenimiento del software, contrato de compra y venta del software, plan de contingencias, procedimientos para el resguardo de la información, autenticación de usuarios, administración de cuentas de usuarios, concienciación sobre seguridad de la información, protección de la tecnología de seguridad, mesa de servicios, configuración de software y procesos de autoevaluación que se llevan a cabo dentro del área. También se evaluaron algunos aspectos generales sobre

seguridad en la red, basándose en entrevistas ya que no fue posible trabajar en las instalaciones del hospital.

Cabe resaltar que no se tuvo en cuenta lo siguiente: seguridad física, seguridad de la base de datos ni seguridad a nivel del sistema operativo.

Los resultados de este proceso fueron plasmados en un informe que se entregó al Hospital, para que tome las medidas pertinentes con base en las recomendaciones y sugerencias realizadas.

DESCRIPCIÓN DEL PROBLEMA

Planteamiento del problema. El Hospital Universitario Departamental de Nariño no había realizado auditorías al sistema de información, por consiguiente no sabía con certeza si los controles de seguridad implementados en dicho sistema eran lo suficientemente efectivos.

El sistema de información Dinámica Gerencial Hospitalaria hace uso de manejadores de base de datos que garantizan la seguridad de la información, contando con un ambiente de seguridad por usuario con su correspondiente clave de acceso, permisos y privilegios; además cuenta con un *log* de transacciones que permite registrar todas las actividades realizadas por los usuarios.

No obstante, estas técnicas de seguridad no son suficientes, pues la información queda expuesta a cualquier tipo de daño o mal uso, debido a la falta de confidencialidad por parte de los usuarios. La confidencialidad implica la privacidad de los elementos de información almacenados y procesados en el sistema informático. Por consiguiente se puede generar inconsistencias en los datos, falta de veracidad, accesos no autorizados, pérdida de información, entre otros inconvenientes.

Además de esto, el hecho de que se cuente con un *log* de transacciones no significa que el sistema esté protegido dado que es necesario el monitoreo y la revisión continua de dichos registros por parte del personal encargado.

Formulación del problema. ¿Cómo la evaluación del sistema de información Dinámica Gerencial Hospitalaria permitirá establecer mejores controles de seguridad lógica que se ajusten a estándares internacionales como la norma ISO/IEC 27002 y COBIT 4.1?

Sistematización del problema

- ¿Qué tipo de controles se aplican actualmente para garantizar la seguridad del sistema de información Dinámica Gerencial Hospitalaria?

- ¿Cómo se puede determinar la efectividad de los controles de seguridad existentes en el sistema?

- ¿Cómo verificar si los perfiles de usuario cuentan con sus correspondientes permisos?

- ¿Qué estándares se aplican para brindar seguridad al sistema de información Dinámica Gerencial Hospitalaria?

OBJETIVOS

Objetivo general. Evaluar la eficiencia y eficacia de los procedimientos y controles de seguridad lógica que tiene el sistema de información Dinámica Gerencial Hospitalaria, teniendo en cuenta sus recursos, políticas y usuarios, mediante la aplicación de técnicas de auditoría.

Objetivos específicos

- Conocer los estándares, modelos y métodos que se utilizan actualmente en la seguridad de la información.

- Identificar y analizar los controles existentes en la seguridad del sistema de información Dinámica Gerencial Hospitalaria.

- Elaborar un diagnóstico general sobre la situación en la que se encuentra el hospital en cuanto a seguridad de la información.

- Establecer el grado de confiabilidad que tiene el sistema y los riesgos a los que se encuentra expuesto.

- Definir y establecer las posibles causas que originan los hallazgos encontrados, así como los recursos de información que pueden verse afectados, con el fin de establecer las recomendaciones necesarias para su mitigación.

- Implementar en un documento final las recomendaciones y el informe de auditoría, a fin de que el personal encargado de administrar la seguridad del sistema de información en el Hospital pueda tomar las medidas correspondientes.

JUSTIFICACIÓN

A través de los servicios de auditoría de seguridad de la información se puede verificar si se está cumpliendo con el objetivo a nivel de seguridad, puesto que permite detectar fortalezas, debilidades, amenazas, riesgos y fallas presentes en los sistemas ayudando a que los datos sean más seguros y fiables.

Por lo tanto, al realizar este proyecto de auditoría, el Hospital Universitario Departamental de Nariño se benefició gracias a que se estableció una metodología de gestión de la seguridad más clara y estructurada, además de reducir el riesgo de pérdida, robo o corrupción de información.

De esta manera, es posible aumentar la confianza de los clientes por la garantía de calidad y confidencialidad, al tener acceso a la información a través de medidas de seguridad, ya que los riesgos y controles fueron revisados, asegurando la continuidad de las operaciones necesarias del negocio tras incidentes de gravedad reduciendo así los costos, protegiendo la inversión e incrementando el valor del sistema de información.

ANTECEDENTES

Existen diferentes proyectos de auditoría que se han enfocado en la seguridad. Entre ellos se pueden citar:

- El proyecto de investigación “DEFINICIÓN DE POLÍTICAS DE SEGURIDAD INFORMÁTICA PARA EL CENTRO DE INFORMÁTICA DE LA UNIVERSIDAD DE NARIÑO” realizado por los ingenieros María Constanza Torres B. y Efraín Fajardo Guevara. Este trabajo consistió en realizar una auditoría orientada a la seguridad del centro de informática de la Universidad de Nariño para, posteriormente, definir políticas de seguridad informática claras que garantizaron la confidencialidad, integridad y disponibilidad de la información, el software y el hardware, logrando aprovechar al máximo los recursos.

- El proyecto de grado “AUDITORÍA DE SISTEMAS APLICADA AL SISTEMA INTEGRAL DE INFORMACIÓN EN LA SECRETARÍA DE PLANEACIÓN MUNICIPAL DE LA ALCALDÍA DE PASTO” desarrollado por el ingeniero Oscar Julián Estrada Obando. Este proyecto consistió en ejecutar una auditoría de sistemas tendiente a identificar las vulnerabilidades de seguridad física y lógica que presentaba el sistema integral de información (SII) en la secretaría de planeación municipal de la alcaldía de Pasto.

- El proyecto “AUDITORÍA DEL MÓDULO DE HISTORIA CLÍNICA ELECTRÓNICA DEL SISTEMA DE INFORMACIÓN EN EL HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO” realizado por las ingenieras Jenny Nayibi Burgos García y María Carolina Domínguez Gómez. Este proyecto consistió en realizar un análisis de riesgos al módulo de historia clínica electrónica e identificar algunas falencias al interior de la organización teniendo en cuenta la misión y visión del hospital.

FACTIBILIDAD DE LA INVESTIGACIÓN

Factibilidad técnica. Para el desarrollo del proyecto se contó con recursos tales como: equipos de cómputo, impresora, cámara digital y grabadora de voz.

Factibilidad operativa. El equipo humano que llevó a cabo el proyecto, estuvo conformado por las estudiantes Edith Friney Díaz Fuelantala y Maira Alejandra Mora Enríquez, con la dirección del Ingeniero Manuel Bolaños González y con el apoyo del Ingeniero Roberto Yánez Constante y del personal administrativo del Hospital Universitario Departamental de Nariño.

Factibilidad económica. La ejecución del presente proyecto de auditoría no requirió de una inversión muy alta, por lo tanto fue financiado por el grupo investigador.

1. MARCO REFERENCIAL

1.1 MARCO CONTEXTUAL

1.1.1 Información general y ubicación. El Hospital Universitario Departamental de Nariño, ubicado en la ciudad de Pasto, es una entidad que funciona desde el año 1975 como la única organización de la red pública de nivel III del suroccidente del país, categoría que alcanzó en 1990 mediante resolución del Ministerio de Salud [1].

A partir de 1994 se constituyó en una Empresa Social del Estado, E.S.E, por ordenanza expedida en la Asamblea Departamental de Nariño, proyectándose con los avances de la ciencia, la tecnología y la gerencia moderna a la comunidad de esta región del país. Luego, en 2004, se constituyó como Hospital Universitario, nivel que conserva hasta hoy [1].

Su sede está ubicada en la calle 22 No. 7-93, parque bolívar. Para más información, las personas pueden comunicarse al PBX 7 33 34 00, al FAX 7 33 34 08 – 7 33 34 09 o al correo electrónico hudn@hosdenar.gov.co [2].

1.1.2 Misión. El Hospital Universitario Departamental de Nariño E.S.E, es una empresa social del estado, con vocación académica, que complementa, con altos estándares de seguridad, a la red departamental de prestadores de servicios de salud, en mediana y alta complejidad. Cree y propicia el crecimiento integral del talento humano, lo cual permite proyectarse e incidir en el mejoramiento de la salud y calidad de vida en la comunidad del sur occidente colombiano [2].

1.1.3 Visión. Durante la vigencia del presente plan de desarrollo el Hospital Universitario Departamental de Nariño E.S.E, dirigirá sus esfuerzos al mejoramiento continuo, se convertirá en una organización centrada en el usuario y fortalecerá la implementación de tecnología, de tal forma que complemente de manera armónica a la red de prestadores de servicios de salud del departamento.

La satisfacción de las necesidades y expectativas de sus grupos de interés será su máxima prioridad y en especial fortalecerá los procesos de gestión clínica, conducentes a garantizar la seguridad de los usuarios [2].

1.1.4 Objetivo. El Hospital Universitario Departamental de Nariño E.S.E, tiene como objeto prestar el servicio público de salud en el tercer y cuarto nivel de atención de conformidad con su capacidad instalada y su declaratoria de requisitos esenciales avalada por la autoridad competente, con preferencia en los servicios médicos – asistenciales y rehabilitación de la salud [3].

1.1.5 Servicios. El Hospital Universitario Departamental de Nariño E.S.E, ofrece los siguientes servicios [2]:

- **Servicios ambulatorios:** consulta externa y atención al usuario.

- **Servicios hospitalarios:** urgencias, hospitalización, habitaciones y suites, unidad de cuidados intensivos y triage.

- **Servicios de apoyo diagnóstico:** imagenología, tomografía axial computarizada de 64 detectores, resonancia nuclear magnética y ecocardiografía.

- **Soporte terapéutico:** banco de sangre, servicio farmacéutico, patología y soporte nutricional.

- **Servicios quirúrgicos:** el Hospital cuenta con quirófanos integrales equipados con tecnología que permite realizar procedimientos quirúrgicos de alta complejidad, sala de recuperación para los pacientes después de cirugía con camas monitorizadas y atención permanente de los médicos anestesiólogos y enfermeras.

- **Servicios ginecológicos y obstétricos:** sala de partos y hospitalización ginecobstétrica y neonatología.

- **Servicios de rehabilitación y medicina física:** medicina física y rehabilitación.

- **Servicios especiales:** planificación computarizada de los tratamientos de radioterapia y unidad de oncología y radioterapia [2].

- **Servicios logísticos y de apoyo:** traslado asistencial básico, traslado asistencial medicalizado, nutrición, esterilización, vigilancia y central de monitoreo, facturación, central de autorizaciones, call center, auditorios con ayudas virtuales, capilla, suministros y almacén, cafetería, lavandería, morgue, gestión ambiental, gestión de emergencias y desastres, mantenimiento, equipamiento biomédico e infraestructura, servicios generales, archivo central de correspondencia y de historias clínicas, central de gases medicinales, central electrógena, servicios administrativos en manejo y control de recursos financieros, recursos humanos,

recursos físicos, recursos de sistemas de gestión de información y asesorías y referenciación en: Auditoría médica, control interno disciplinario, planeación, calidad, jurídica y gestión comunicacional [2].

1.2 MARCO LEGAL

1.2.1 Aspectos legales de seguridad informática

- **Ley 1273 de 2009:** creó nuevos tipos penales relacionados con delitos informáticos y la protección de la información y de los datos con penas que van de 36 a 120 meses de prisión, hasta multas de 100 a 1500 salarios mínimos legales mensuales vigentes, además de la pena de inhabilitación para el ejercicio de profesiones relacionadas con sistemas de información procesados con equipos computacionales. La ley se divide en dos capítulos, a saber: "De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos" y "De los atentados informáticos y otras infracciones" [4].

- **Ley estatutaria 1266 de 2008:** aparte de tener como objetivo, desarrollar el derecho que tienen las personas a conocer, actualizar y rectificar las informaciones contenidas en los bancos de datos, ésta ley busca ofrecer al ciudadano la posibilidad de proteger sus datos y los diferentes usos que a estos se les pueda dar [5].

- **Ley 527 de 1999:** define y reglamenta el acceso y uso de los mensajes de datos (información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, como por ejemplo Internet, el correo electrónico, el telegrama o el telefax), del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones [6].

1.3 MARCO TEÓRICO

1.3.1 Evolución histórica de la auditoría. La introducción de las máquinas de proceso de datos en las empresas se produjo en los años 50. Dichas máquinas se dedicaban principalmente a sustituir a los empleados en tareas repetitivas como el cálculo de nóminas y facturas de clientes. A causa de su utilización como supercalculadoras, debían manejar grandes cantidades de datos de entrada y de salida, por lo que el auditor se limitaba a rectificar los datos de salida frente a los

datos de entrada, ignorando la lógica y el funcionamiento interno de las máquinas. Es así como surge la auditoría alrededor del ordenador [7].

Esta situación se prolongó hasta mediados de la década de los 60, cuando las organizaciones de auditoría promovieron un cambio en el enfoque, con base a los resultados de baja calidad obtenidos en las auditorías de áreas relacionadas con el proceso de datos a través de ordenadores. Este cambio consistía fundamentalmente en la adaptación de criterios para la evaluación del control interno, de los sistemas organizativos, financieros y contables, al centro de proceso de datos y, concretamente, a la sala del ordenador. A esta etapa se la denomina auditoría del ordenador.

Con la introducción de nuevas tecnologías, como las comunicaciones entre ordenadores en tiempo real, pronto se detectaron las limitaciones del enfoque, ya que se producían pérdidas progresivas de las pistas de auditoría y el auditor era incapaz de controlar determinadas actividades. Así, a finales de los años 70, se llega a una tercera etapa: la auditoría a través del ordenador.

Posteriormente, a principios de los años 80, se empieza a aplicar técnicas de tratamiento de la información por medio de ordenadores, como apoyo a la labor de los auditores. El auditor de sistemas de información empieza a ser también experto en el uso de lenguajes informáticos que le sirven para escribir, compilar y ejecutar programas con el fin de conseguir pruebas y obtener evidencias. Surge de este modo la denominada auditoría con el ordenador [7].

En la misma década se empieza a aplicar los principios básicos de la auditoría operativa a la auditoría de los sistemas de información, dando lugar a la auditoría operativa de proceso de datos, que se centra principalmente en la eficacia y eficiencia del tratamiento automático de los datos.

1.3.2 Definición de auditoría. La auditoría es la actividad consistente en la emisión de una opinión profesional sobre si el objeto sometido a análisis presenta adecuadamente la realidad que pretende reflejar y/o cumple las condiciones que le han sido prescritas [8], estableciendo además los cambios que se deberían realizar para la consecución efectiva del mismo [9].

1.3.3 Tipos de auditoría. La rápida evolución de la auditoría ha provocado su especialización según el objeto, destino, técnicas, métodos y herramientas que se utilicen para su ejecución. Es así como surgen los diferentes tipos de auditoría, los cuales se encuentran clasificados de acuerdo a ciertos factores, a saber:

- **Por el origen de quien hace su aplicación**

Externa: la realizan los auditores que son independientes a la empresa, de tal forma que pueden aplicar libremente los métodos, técnicas y herramientas necesarias para evaluar las actividades, operaciones y funciones. Esto, con el fin de determinar el cumplimiento de los objetivos institucionales y emitir un dictamen independiente de carácter externo en donde se exponen los resultados con sus recomendaciones [10].

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 [10].

- **Por el área en donde se hacen**

Financiera: se preocupa por la veracidad de los estados financieros y la preparación de informes de acuerdo a principios contables [11].

Administrativa: analiza el logro de los objetivos de la administración y el desempeño de las funciones administrativas [11].

Operacional: evalúa la eficiencia, eficacia y economía de los métodos y procedimientos que rigen un proceso de una empresa [11].

Gubernamental: verifica que la gestión pública se haya realizado con economía, eficiencia, eficacia y transparencia, conforme a las disposiciones legales aplicables [12].

Integral: es el examen crítico, sistemático y detallado de los sistemas de información financiero, de gestión y legal de una organización [13].

Sistemas: se preocupa por la función informática [11].

Recursos Humanos: es el examen que se hace para evaluar la eficiencia y eficacia en el manejo del personal y los controles que se ejercen con los expedientes, asistencia y puntualidad, nóminas de pago, políticas de atención social y promociones [14].

- **Por área de especialidad**

Fiscal: consiste en verificar el correcto y oportuno pago de los diferentes impuestos y obligaciones fiscales de los contribuyentes desde el punto de vista físico, direcciones o tesorerías de hacienda estatales o tesorerías municipales [15].

Laboral: es el análisis y revisión de la situación laboral de una empresa, mediante el estudio de la documentación e información aportada por la misma, reflejando en un informe el cumplimiento de las obligaciones jurídico-laborales y de seguridad social [16].

Ambiental: es la cuantificación de las operaciones industriales determinando si los efectos de contaminación que produce dicha empresa, están dentro del marco legal de la protección ambiental [17].

Médica: es un procedimiento técnico, evaluativo y preventivo sobre la calidad de atención fundamentada en la aplicación y análisis de indicadores institucionales, la revisión de la historia clínica, los protocolos de atención, el compromiso de gestión, el cumplimiento de la legislación interna y externa, y la satisfacción de los usuarios y prestadores de servicios [18].

Calidad: evalúa métodos, mediciones y controles de los bienes y servicios [11].

Social: revisa la contribución a la sociedad así como la participación en actividades socialmente orientadas [11].

- **Especializadas en sistemas computacionales**

Informática: es la revisión técnica, especializada y exhaustiva que se realiza a los sistemas computacionales, software e información utilizados en una empresa, así como a sus instalaciones, mobiliario, equipos periféricos, telecomunicaciones y demás componentes [19].

Con la computadora: es el examen y evaluación de los archivos de datos en medios magnéticos, con el auxilio del computador y de software de auditoría generalizado y/o a la medida [20].

Sin la computadora: sus métodos, técnicas y procedimientos están orientados únicamente a la evaluación tradicional del comportamiento y validez de las transacciones económicas, administrativas y operacionales de un área de

cómputo, y en sí de todos los aspectos que afectan a las actividades en las que se utilizan sistemas informáticos, pero dicha evaluación se realiza sin el uso de los sistemas computacionales [19].

Gestión informática: su aplicación se enfoca exclusivamente en la revisión de las funciones y actividades de tipo administrativo que se realizan dentro de un centro de cómputo, tales como la planeación, organización, dirección y control de dicho centro [19].

Alrededor de la computadora: concentra sus esfuerzos en la entrada de datos y en la salida de información. Únicamente se verifica la efectividad del sistema de control interno en el ambiente externo de la máquina [20].

Seguridad de sistemas: es la revisión exhaustiva, técnica y especializada que se realiza a todo lo relacionado con la seguridad de un sistema de cómputo, sus áreas y personal, así como a las actividades, funciones y acciones preventivas y correctivas que contribuyan a salvaguardar la seguridad de los equipos computacionales, las bases de datos, redes, instalaciones y usuarios del sistema [19].

Sistemas de redes: es la revisión exhaustiva, específica y especializada que se realiza a los sistemas de redes de una empresa, considerando en la evaluación los tipos de redes, arquitectura, topología, los protocolos de comunicación, las conexiones, accesos, privilegios, administración y demás aspectos que repercuten en su instalación, administración, funcionamiento y aprovechamiento [19].

1.3.4 Auditoría informática. La auditoría informática consiste en recoger, agrupar y evaluar evidencias para determinar si un sistema de información salvaguarda el activo empresarial, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización, utiliza eficientemente los recursos, y cumple con las leyes y regulaciones establecidas. Además, permite detectar los flujos de información dentro de la organización y establecer qué información es crítica para el cumplimiento de su misión y objetivos, identificando necesidades, duplicidades, costos, valor y barreras, que obstaculizan flujos de información eficientes que servirán para una adecuada toma de decisiones [9].

Generalmente, este tipo de auditoría se puede desarrollar en alguna o combinación de áreas como: servicios de entrega y soporte, gobierno corporativo, protección y seguridad, administración del ciclo de vida de los sistemas y planes de continuidad y recuperación de desastres [9].

La necesidad de contar con lineamientos y herramientas estándar para el ejercicio de la auditoría informática ha promovido la creación y desarrollo de mejores prácticas como COBIT, COSO[1] e ITIL[2] [9].

1.3.5 Objetivos generales de la auditoría informática. Los principales objetivos que constituyen a la auditoría Informática, son [21]:

- El control de los sistemas de información y de las tecnologías de la información.
- El análisis de la eficiencia de los de los sistemas de información y de las tecnologías de la información.
- La verificación del cumplimiento de la normativa general de la organización.
- La verificación de los planes, programas y presupuestos de los sistemas informáticos.
- La revisión de la gestión eficaz de los recursos materiales y humanos informáticos.
- La revisión y verificación de controles técnicos, generales y específicos de operatividad.
- La revisión y verificación de la seguridad en: el sistema operativo, el software, las comunicaciones, las bases de datos, los procesos, las aplicaciones y la parte física entre otros.
- El análisis de verificación y de exposición de debilidades y disfunciones.

Además, la auditoría informática sustenta y confirma la consecución de los objetivos tradicionales de la auditoría:

- Objetivos de protección de activos e integridad de datos.
- Objetivos de gestión que abarcan, no solamente los de protección de activos, sino también los de eficacia y eficiencia.

1.3.6 Justificativos para efectuar una auditoría informática. Algunas de las razones más importantes para realizar una auditoría informática pueden ser las siguientes [22]:

- Cuando se presentan signos de descoordinación y desorganización en el área de sistemas.

[1] Acrónimo de *Committee of Sponsoring Organizations of the Treadway Commission*. Es un documento que contiene las principales directivas para la implantación, gestión y control de un sistema de control, orientadas al logro de los objetivos del negocio.

[2] Acrónimo de *Information Technology Infrastructure Library.* Conjunto de conceptos y prácticas para la gestión de servicios de tecnologías de la información, el desarrollo de tecnologías de la información y las operaciones relacionadas con la misma en general.

- Cuando hay insatisfacción, por parte de los usuarios y/o clientes, con respecto al servicio prestado por el personal técnico.
- Cuando existen señales de debilidades económico – financieras.
- Cuando se sospecha inseguridad, ya sea en el campo de la seguridad lógica y/o física o en materia de confidencialidad de datos y continuidad del servicio.
- Descubrimiento de fraudes efectuados con el computador.
- Falta de planificación informática.
- Falta de documentación o documentación incompleta de sistemas.
- Desconocimiento en el nivel directivo de la situación informática de la empresa.
- Aumento considerable e injustificado del departamento de almacenamiento de datos.

Sin embargo, la auditoría no debe realizarse únicamente cuando la empresa presenta problemas o existen indicios de fallos, puesto que es importante que se tenga una visión general de la situación en la que se encuentra la organización de manera constante. Esto con el fin de que se tomen las medidas necesarias para cumplir con los objetivos planteados y de esta manera la empresa se podrá proyectar como una entidad fuerte y de calidad. Además, se verá beneficiada en los siguientes aspectos:

- Se genera confianza en los usuarios sobre la seguridad y control de los servicios de las tecnologías de la información.
- Se optimizan las relaciones internas y el clima de trabajo.
- Se disminuyen los costos de la mala calidad (rechazos, reclamos, entre otros).
- Se genera un balance de los riesgos en las tecnologías de la información.
- Se realiza un control de la inversión en un entorno de tecnologías de la información, a menudo impredecible.

1.3.7 Aspectos que evalúa la auditoría informática

1.3.7.1 Auditoría de la seguridad informática. La auditoría de seguridad informática evalúa y analiza los procesos relacionados únicamente con la seguridad, que puede ser física, lógica y locativa pero siempre orientada a la protección de la información [23].

Procesos de una auditoría de seguridad informática

Los procesos cubren cuatro frentes específicos [23]:

- Auditoría desde internet, identificando las vulnerabilidades a las que se ve expuesto el recurso computacional y el sitio web de la organización desde internet por parte de delincuentes informáticos.

- Auditoría desde la red interna (LAN) de la organización, para la identificación de las vulnerabilidades generadas desde el interior de la organización aprovechando los beneficios de la red de área local.

- Trabajo sobre los equipos, ejecutando herramientas software de identificación de vulnerabilidades, identificación de archivos que contienen software espía, virus informáticos y análisis personales del estado físico, lógico y locativo de cada uno de los equipos.

- Ejecución de entrevistas sobre el manejo de las políticas de seguridad física, lógica y locativa de los miembros de la organización. En este punto es importante hacer la diferencia entre seguridad física y locativa. La seguridad locativa se refiere a las instalaciones y la física al manejo del hardware del equipo.

Los procesos o fases de la auditoría se complementan mutuamente y si se llegara a desarrollar solo algunos de estos, el aumento de la seguridad de la organización no sería considerable [23].

1.3.7.2 Auditoría de la seguridad física. La seguridad física identifica las amenazas, vulnerabilidades y las medidas que pueden ser utilizadas para proteger físicamente los recursos y la información de la organización. Los recursos incluyen al personal, al sitio donde ellos laboran, a los datos, los equipos, los medios con los cuales los empleados interactúan y en general a los activos asociados al mantenimiento y procesamiento de la información, como por ejemplo activos de información, activos de software y activos físicos [25].

Las principales amenazas que se prevén en la seguridad física, son:

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

Por otra parte, los objetivos de la seguridad física se basan en prioridades con el siguiente orden [24]:

1. Edificio
2. Instalaciones

3. Equipamiento y telecomunicaciones
4. Datos
5. Personas

1.3.7.3 Auditoría de 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 autorizadas para hacerlo" [26].

Algunos de los controles más utilizados en la seguridad lógica son [27]:

- Limitar el acceso a determinadas aplicaciones, programas o archivos mediante claves o a través de la criptografía.

- Otorgar los privilegios mínimos a los usuarios del sistema informático. Es decir, sólo se conceden los privilegios que el personal necesita para desempeñar su actividad.

- Garantizar que los archivos, las aplicaciones y programas que se utilizan en la compañía se adapten a las necesidades y se usen de manera adecuada.

- Controlar que la información que entra o sale de la empresa sea íntegra y que sólo esté disponible para los usuarios autorizados.

Propiedades de la seguridad informática

Las propiedades de la seguridad de la información, también conocidas como requisitos ACID (autenticación, confidencialidad, integridad y disponibilidad), son las siguientes [27]:

- **Autenticación**: garantiza que el usuario es “quien dice ser”.

- **Confidencialidad**: la información sólo se revela a los usuarios autorizados para prevenir el acceso no autorizado, ya sea de manera intencional o accidental.

- **Integridad**: la información debe ser siempre exacta y completa, y sólo puede ser modificada por el personal autorizado.

- **Disponibilidad**: la información sólo debe estar disponible cuando se necesite y de la forma que la requieran los usuarios autorizados.

Amenazas lógicas

Entre las amenazas lógicas más frecuentes que pueden dañar los bienes de la empresa se encuentran:

Malware

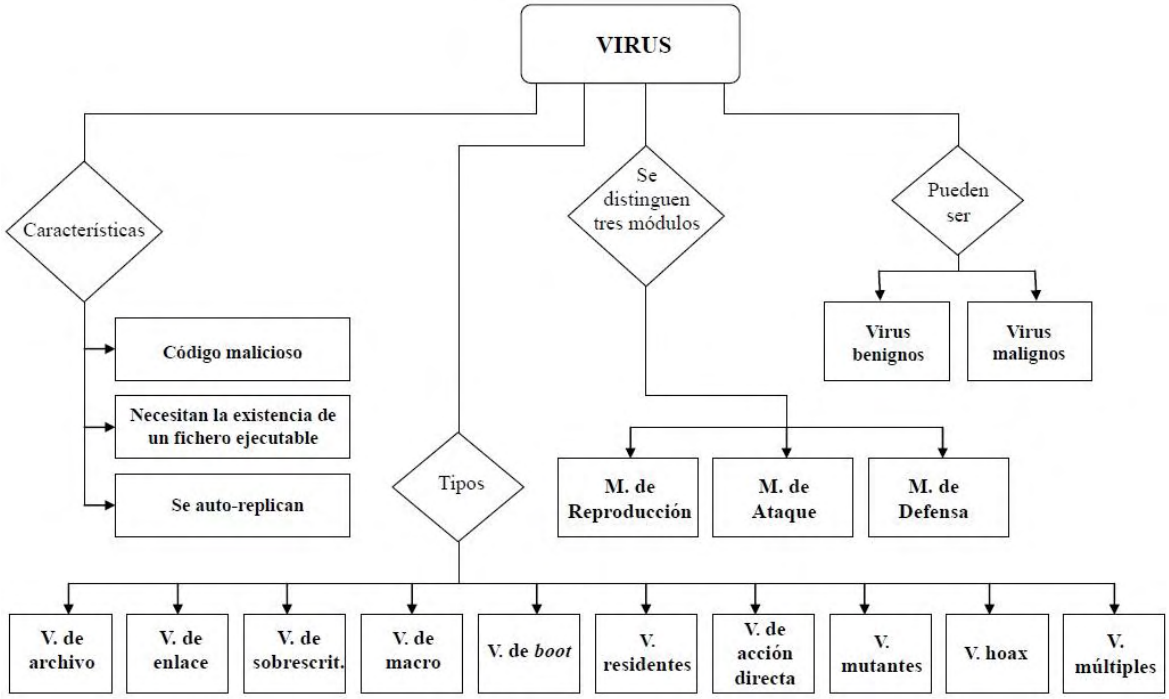
Un *malware* es todo software diseñado para realizar acciones maliciosas sobre el sistema. Los *malware* más relevantes son los siguientes [27]:

1. Virus: es una secuencia de código que se aloja en un fichero ejecutable denominado *hosts* (huésped) de manera que al ejecutar el programa también se ejecuta el virus.

Los virus informáticos son muy habituales en la red y pueden provocar daños irreparables. En algunas ocasiones, borran información necesaria para el correcto funcionamiento del sistema, y esto provoca que el disco duro tenga que ser formateado para reparar el daño. Ocupan poco espacio en disco, característica importante para que el virus pueda pasar inadvertido el máximo tiempo posible. Además, se auto-replican, es decir, se realizan copias de sí mismo para expandirse rápidamente.

La siguiente figura (Figura 1) muestra de manera general los módulos que componen a un virus, algunas de sus características y los diferentes tipos de virus existentes:

Figura 1. Virus



Fuente: MONTE DE PAZ, Marta. Seguridad Lógica y de Accesos y su Auditoría.

2. Gusanos: los gusanos son programas capaces de ejecutarse por sí mismos (a diferencia de los virus que necesitan de la existencia de un fichero ejecutable) y propagarse por la red. Actualmente, constituyen una amenaza habitual en Internet [27].

Se consideran como una subclase de virus informático. Residen en memoria y tienen gran capacidad para replicarse pudiendo incluso, enviar copias de sí mismos a otros equipos por medio de correos electrónicos.

Los gusanos utilizan técnicas para aprovecharse del comportamiento humano y conseguir propagarse. Esto es lo que se denomina ingeniería social. Se utiliza con frecuencia en el caso de gusanos que se envían a través de correos electrónicos [27].

3. Troyanos: un caballo de troya o troyano es un programa que bajo una apariencia inofensiva y útil para el usuario se inserta en un ordenador, y permite que usuarios externos accedan a la información contenida o controlen de forma

remota el equipo. Los troyanos son creados para obtener información privilegiada de la máquina anfitriona. No necesariamente provocan daños en la computadora infectada y, a diferencia de los virus y los gusanos, los troyanos no se reproducen [27].

Los troyanos se componen de dos programas: uno que envía las acciones que deben realizarse en la computadora anfitriona llamado cliente, y otro programa que recibe las acciones del cliente y las realiza en el ordenador infectado denominado servidor.

Los troyanos actuales constituyen una gran amenaza para los usuarios debido a que pasan bastante desapercibidos. Esto se debe a que el programa servidor no consume recursos. Cuando se arranca el equipo, el caballo de Troya se ejecuta automáticamente y reside en memoria. A partir de ahí, puede esperar a que el usuario del ordenador infectado introduzca números de tarjeta de crédito, contraseñas de su correo electrónico, etc.

4. Bombas lógicas: las bombas lógicas son programas que se activan después de cierto tiempo causando daños en el sistema. Pueden realizar diversas acciones, desde mostrar un simple mensaje hasta borrar información importante del disco duro. Además, cabe destacar que muchos virus se ejecutan por medio de bombas lógicas en determinadas fechas.

Las bombas lógicas se activan porque se cumplen algunas de las siguientes condiciones [27]:

- Una fecha concreta.
- Una hora determinada.
- Si un contador interno llega a un número concreto.
- Si se alcanza cierto número de ejecuciones del programa que contiene la bomba lógica.
- Si se cumplen otras características establecidas por el atacante.

Por lo tanto, una bomba lógica puede permanecer inactiva durante un largo periodo de tiempo, de manera que nadie nota ningún comportamiento extraño en el sistema hasta que la bomba se activa. En esta característica, radica el poder dañino de las bombas lógicas.

5. *Adware*: los *adware* son aplicaciones que muestran publicidad o descargas al equipo del usuario cuando éste instala un programa. “Ad” es el diminutivo de *advertisement* que en español significa anuncio [27].

Muchos programas de descarga gratuita contienen *adware*. De esta forma, los creadores del programa consiguen un beneficio económico. El usuario, al instalar el programa, no es consciente de la descarga del *adware*. En ocasiones, pueden remplazar la página de inicio del navegador, aparecer ventanas pop-ups con publicidad o instalarse aplicaciones no deseadas.

6. *Spyware*: el *spyware* o software espía envía información personal del usuario a terceros sin que éste tenga conocimiento sobre lo sucedido. La información enviada puede ser: las páginas web que se visitan o algo más comprometido como contraseñas o números de tarjetas de crédito. Habitualmente las empresas utilizan esa información para enviar publicidad a los usuarios [27].

Al igual que los *adware*, se pueden instalar al descargar un programa y aceptar las condiciones de uso.

7. Puertas traseras: también son conocidas como *backdoors*. Las puertas traseras permiten a su creador o a personas con conocimiento de su existencia, el acceso a una máquina de forma remota sin que el usuario se percate. Son muy difíciles de detectar. La única forma de cerciorarse que un programa no contiene *backdoors* es revisando el código línea a línea [27].

Los atacantes, a través de estas puertas traseras, pueden eliminar ficheros, borrar información del disco duro, acceder a datos confidenciales o abrir puertos de comunicaciones permitiendo que un agente externo controle el ordenador de forma remota, entre otras acciones.

Además, una puerta trasera puede estar integrada en un troyano o en cualquier otra aplicación.

8. Conejo o bacteria: es un programa que no causa daño de forma directa al sistema pero que se reproduce hasta agotar los recursos del ordenador causando una denegación del servicio. Generalmente, estos programas se auto-replican de forma exponencial, por lo tanto, de una copia se generan dos, de dos se crean cuatro, de cuatro se generan ocho y así sucesivamente hasta agotar los recursos del procesador, de la memoria y del disco, entre otros [27].

9. *Rootkit*: es un conjunto de herramientas usadas por agentes externos para acceder sin autorización a un sistema informático. Se esconden a sí mismos al igual que a otros procesos y archivos para encubrir las acciones maliciosas que llevan a cabo los intrusos informáticos. Por ejemplo, si existe alguna puerta trasera, el *rootkit* oculta los puertos abiertos que evidencien la comunicación [27].

10. *Exploit*: para explicar lo que se entiende por *exploit*, es conveniente detallar lo que se conoce como *bug* en el lenguaje informático. Un *bug* es un error o defecto en un elemento de software. En ocasiones esos errores en el software son introducidos de manera intencionada por los programadores sin embargo los *bugs* suelen corregirse según surgen nuevas versiones de un software [27].

En consecuencia, los *exploits* se encargan de aprovechar vulnerabilidades, es decir, aprovechan los *bugs* que contiene el software. Suelen ser programas que explotan los errores de un programa para obtener algún tipo de beneficio o privilegio. Los *exploits* pueden violar las medidas de seguridad para acceder a un sistema sin autorización.

11. *Cookie*: las *cookies* son fragmentos de información acerca de las visitas realizadas a un sitio web que se almacenan en el equipo del usuario. De esta forma, se consigue una navegación más personalizada ajustando el sitio a las preferencias del usuario y, además, permite medir las preferencias del mercado [27].

Las *cookies* surgieron para que los servidores web guardaran y recuperaran información acerca de sus visitantes. El inconveniente de las *cookies* es que pueden vulnerar la intimidad si los datos obtenidos pueden asociarse a un individuo. No obstante, las *cookies* no graban datos personales como el nombre o la dirección de correo electrónico, a menos que se facilite esta información. Además, es importante recalcar que las *cookies* no tienen acceso al disco duro del usuario.

12. *Pharming*: es una técnica que consiste en manipular las direcciones DNS (*Domain Name System*) a las que accede el usuario, permitiendo a un intruso redirigir un nombre de dominio a otra máquina. La manipulación se realiza por algún código malicioso, generalmente un troyano, que se ha introducido en el ordenador. De esta manera, el usuario al intentar acceder al sitio web que desea, accede a otra página creada por el atacante para recabar información confidencial del individuo. La persona no sospecha que se encuentra en una página falsa ya que muestra el mismo aspecto que la original. Esta práctica es muy utilizada en páginas relacionadas con el sector bancario [27].

El cambio de direcciones DNS puede afectar a todos los usuarios que utilicen el servidor o afectar sólo de forma local, es decir, a cada host. Esta última forma, es más peligrosa y se puede llevar a cabo fácilmente en ordenadores que funcionen bajo *Windows* y utilicen el navegador *Internet Explorer*, modificando un archivo denominado "*hosts*".

13. *Spam*: un *spam* o correo basura es un mensaje publicitario enviado al correo electrónico de un gran número de usuarios sin que éstos lo hubiesen solicitado. Sobrecargan los servidores de correo y los usuarios tienen que invertir tiempo en eliminarlos.

Crimeware

Cuando el software malicioso produce pérdidas económicas al usuario del equipo atacado, también se le denomina software criminal o *crimeware*. Por ejemplo, forman parte de esta clasificación [27]:

1. Técnica del salami: consiste en desviar de forma fraudulenta pequeñas cantidades de bienes (habitualmente dinero) de diversas fuentes que posean una gran cuantía de ellos, de manera que sea casi imperceptible el robo de una pequeña cantidad. Se utiliza generalmente en los sectores bancarios.

2. *Carding*: consiste en la utilización ilegal de tarjetas de crédito ajenas. Se utiliza un número de tarjeta perteneciente a otra persona para realizar compras a través de Internet. La persona que comete el fraude puede conseguir el número de la tarjeta a través de:

- **Recogida de información residual**: consiste en aprovechar la información depositada en la papelera que no ha sido destruida. De esta manera, se obtiene acceso a información privilegiada sin autorización para ello. En algunos textos, denominan a esta amenaza lógica *scavenging, trashing* o basureo.

- ***Keyloggers:*** programas que almacenan las teclas pulsadas por el usuario para capturar el número de las tarjetas de crédito y las contraseñas, entre otra información.

- **Troyanos**

3. Scam: la palabra *scam* significa estafa en español. Un *scam* es una técnica que consiste en el envío de correos electrónicos que contienen una propuesta con el fin de estafar económicamente al usuario. Pueden ofrecer grandes sumas de dinero o un trabajo muy bien remunerado para captar la atención de la persona. También se le denomina *scam* a páginas web que ofrecen algún producto o servicio falso con el fin de estafar al usuario.

Ingeniería social

La ingeniería social consiste en la manipulación de las personas para que de manera voluntaria, lleven a cabo actos que de otro modo no realizarían. Es una técnica muy sencilla y desafortunadamente, muy efectiva [27].

Por ejemplo, se utiliza la ingeniería social cuando se descarga un programa de Internet pensando que es un antivirus para el ordenador y, de esta forma, estar a salvo de posibles amenazas. Al ejecutar el programa la computadora es infectada por un troyano.

Los atacantes se aprovechan de los usuarios confiados y de su falta de cultura en medidas de seguridad. El *phishing* es un ejemplo de técnica que utiliza la ingeniería social y el *scam* ya comentado anteriormente.

1. *Phishing*: es una técnica que consiste en la suplantación de identidad de una persona o entidad para obtener datos confidenciales de forma ilícita a través de correos electrónicos. Es considerado como un *malware*, además de como una técnica de ingeniería social [27].

Esta práctica es muy común en el sector bancario. Los estafadores imitan la imagen de la entidad bancaria y solicitan al usuario que confirme determinados datos personales como el número de tarjeta de crédito con alguna excusa.

Ataque de denegación de servicio

Un ataque de denegación de servicio o ataque DoS (*Denial of Service*) es un ataque que imposibilita el acceso a un recurso o servicio por parte de un usuario legítimo [27].

Es una práctica muy utilizada por los *crackers*[3] para provocar la caída de un servidor. El servidor recibe demasiadas peticiones, provocando que se sature y no pueda dar servicio a los usuarios legítimos.

Algunos ejemplos de ataques DoS son [27]:

- ***SYN Flood*:** *flood* significa inundación en español. Se produce una denegación de servicio debido a que el sistema recibe más peticiones de conexión de las que puede atender.

[3] Personas que rompen algún sistema de seguridad.

➢ ***Smurf*:** consiste en enviar a una dirección de *broadcast*[4] una petición de ICMP (protocolo de control y notificación de errores). Se falsifica la dirección de origen (con una técnica denominada *spoofing*) que será la víctima del ataque. Cada *host* mandará una respuesta a la dirección IP de la víctima, provocando así, una denegación de servicio.

➢ ***Ping* de la muerte o *ping of death*:** un atacante podría modificar el tamaño del paquete que envía a otra máquina superando el máximo autorizado (65535 *Bytes*) para producir un desbordamiento de memoria en el *host* atacado causando una denegación de servicio. Actualmente, las máquinas no son vulnerables a este tipo de ataque.

➢ ***Email bombing*:** consiste en enviar gran cantidad de correos electrónicos a los usuarios para saturar los servidores de correo.

Un tipo de ataque de denegación de servicio es DDoS (*Distributed Denial of Service*) o denegación de servicio distribuido. Se instalan varios agentes remotos en diversos equipos denominados *zombies*, controlados por un tercero. Los ordenadores *zombies* son computadoras que han sido infectadas por algún tipo de código malicioso (por ejemplo, un troyano) que permite a una tercera persona controlar las máquinas remotamente. El atacante coordina los equipos para que el ataque sea más efectivo, consiguiendo mayor saturación del recurso. Estos ordenadores solicitan un servicio de manera simultánea, colapsándolo.

Ataque de modificación o daño

Un intruso no autorizado accede al contenido de la información y la altera, de tal forma que los datos que recibe el destinatario difieren de los originales. Este tipo de ataques atentan principalmente, contra la integridad de la información. Algunos ejemplos de este tipo de ataques, son [27]:

1. *Data diddling* o *tampering*: esta práctica consiste en la alteración no consentida de los datos, (modificar datos, borrarlos o introducir datos falsos) o la instalación de software en el sistema.

Algunos ejemplos de esta técnica, son: modificar las calificaciones de un alumno o modificar el nombre de un software malicioso por el nombre de algún programa conocido adhiriéndole un virus. Dentro de esta categoría se incluyen los virus, gusanos, troyanos, bombas lógicas y otras amenazas similares.

[4] Forma de transmisión de información donde un nodo emisor envía información a una multitud de nodos receptores de manera simultánea, sin necesidad de reproducir la misma transmisión nodo por nodo.

2. Borrado de huellas: en los archivos *logs* se almacena información sobre los cambios que se realizan sobre el sistema. Por lo tanto, el borrado de huellas consiste en modificar los *logs* del sistema en los que quedan reflejadas las distintas acciones realizadas para evitar que se detecte su acceso ilícito.

Ataque de suplantación

Los ataques de suplantación (fabricación o impostura) pretenden suplantar a un usuario o una máquina por medio de distintas técnicas para conseguir el acceso a la información. Este tipo de ataques atentan contra la autenticación principalmente [27].

Por lo general, se lleva a cabo obteniendo la contraseña y el identificador de un usuario por medio de distintos mecanismos. Sin embargo, existen ocasiones en las que el atacante pretende hacerse pasar por un usuario o entidad legítima para hacer creer a su víctima que es la persona que dice ser. Este último caso, es lo que realiza la técnica *phishing* ya explicada anteriormente, a través de correos electrónicos.

1. *Spoofing*: se suplanta la identidad de una máquina o usuario legítimo para realizar acciones sobre un sistema. Por ejemplo, el intruso puede conseguir el nombre y contraseña del usuario autorizado y enviar falsos correos electrónicos en nombre de la víctima [27].

Los ataques de *spoofing* se pueden clasificar en función de la tecnología utilizada. Entre ellos se tiene: IP *spoofing*, DNS *spoofing* (resolver una dirección IP falsa a un cierto nombre DNS o viceversa), *mail spoofing* (se suplanta una dirección de correo electrónico) o web *spoofing* (se suplanta una página web), todas con el objetivo común de falsear la identidad de un usuario o máquina y realizar acciones maliciosas.

2. *Hijacking*: *hijacking* (o secuestro en español) hace referencia a cualquier acción ilícita que lleva a cabo un atacante para apropiarse de algo, generalmente de información [27].

En materia informática se pueden destacar el secuestro de sesiones (*session hijacking*), de páginas web (*page hijacking*), de navegadores (*browser hijacking*), de la página de inicio de los navegadores (*home page browser hijacking*) o dominios (*domain hijacking*), entre otros.

Ataque de monitorización

Los ataques de monitorización o intercepción son aquellos en los que una tercera parte no autorizada, busca vulnerabilidades en el sistema para acceder al contenido de la información con el objetivo de apropiarse de ésta pudiendo hacer uso de ella con fines ilícitos. Son ataques que atentan contra la confidencialidad de la información [27].

En este tipo de ataques se incluyen [27]:

- **Señuelos o *decoy*:** programas que imitan la interface de otro original para solicitar el nombre de usuario y la contraseña y guardar esta información para acceder al sistema.

- ***Keyloggers*:** programas que almacenan las teclas pulsadas por el usuario para conocer contraseñas o cualquier información confidencial y realizar acciones maliciosas.

- ***Scanning* o búsqueda:** se escanean los puertos abiertos para explotarlos posteriormente.

1. *Sniffing*: el *sniffing* consiste en capturar cualquier paquete que circula por la red. Se puede realizar *sniffing* por software o por hardware. En este último caso, se conecta un dispositivo a un cable de red para capturar los paquetes que viajen a través del cable [27].

Generalmente, el *sniffing* se realiza por software. Un programa llamado *sniffer* captura la información de la red almacenándola, habitualmente, en un fichero al que accede el atacante. Las tramas que circulan por delante de la máquina en la que se encuentra instalado el *sniffer*, son captadas aunque la información no vaya dirigida a dicha máquina.

El *sniffer* se queda “escuchando” para captar contraseñas, números de tarjeta de crédito, direcciones de correo electrónico o cualquier otra información ya que, en ocasiones, estos datos no viajan cifrados.

Redes sociales

Las redes sociales han surgido en los últimos años para revolucionar la manera de comunicarse vía internet. Estas redes, permiten mostrar y compartir fotos, videos, comentarios, etc. Sin embargo, en ocasiones, suponen una amenaza en la seguridad tanto física como lógica [27].

A través de los mensajes publicados, los vídeos y las fotos, es fácil que los demás usuarios conozcan dónde se encuentra una persona, quiénes son sus amigos y familia y qué hace en cada momento. Estas acciones ponen al usuario en la mira de un atacante.

Relativo a la seguridad lógica, un intruso podría crear un perfil con el nombre y apellidos de un tercero conocido por la víctima. De esta manera, la víctima aceptaría a su supuesto amigo para que ambos pudieran comunicarse a través de la red social. El intruso, haciendo uso de la ingeniería social, podría solicitarle información personal para hacer uso ilícito de ella.

Otra amenaza de la seguridad lógica radica en que estas redes sociales se han convertido en un medio para propagar *malware*.

1.3.8 Metodología de trabajo de la auditoría informática. El proceso de una auditoría informática se puede desglosar en diferentes etapas y actividades que se explican a continuación [27]:

1.3.8.1 Estudio inicial de la auditoría. Es necesario definir de forma clara el objetivo, el alcance y la profundidad de la auditoría. El alcance define el entorno y los límites en que se desarrollará la auditoría informática. Esto es importante, sobre todo, en organizaciones grandes y dispersas. Se definen también las materias, las funciones y las actividades a auditar y las que permanecerán fuera de la auditoría. En el final de esta etapa se determina la viabilidad de la auditoría. Si la auditoría es viable se continúa con el proceso de auditar.

1.3.8.2 Determinación de recursos necesarios. Después del estudio inicial, se determinan los recursos económicos, materiales y humanos, necesarios para la realización de la auditoría. En cuanto a los recursos económicos, existirá un presupuesto que no debe excederse.

Una auditoría requiere una gestión lo más óptima posible. Para ello, es importante conseguir un equilibrio entre el cumplimiento de los objetivos de la auditoría, los plazos y el costo de la auditoría. La prioridad de estos tres factores debe ser el cumplimiento de los objetivos frente al presupuesto y el tiempo.

Los recursos humanos deben ser acordes con la auditoría a realizar. Es decir, la organización del equipo y el número de personas dependerá del entorno de la auditoría y de la formación de éstos. Además, se designa un líder (o líderes) en el equipo humano. El líder del grupo suele ser un auditor con gran experiencia.

En el equipo humano pueden diferenciarse las siguientes funciones:

- Gerente/s
- Jefe/s de equipo
- Auditor/es experimentados
- Auditor/es principiantes

Los recursos materiales serán tanto software como hardware. El equipo de auditores elegidos debe conocer la organización de la empresa auditada. Para ello, el auditor observa entre otras cosas:

- El organigrama de la compañía.
- Las relaciones entre los órganos de la entidad.
- Los departamentos que la componen.
- Los flujos de información.
- Se comprueba que no existen puestos de trabajo distintos que realicen las mismas funciones.
- Se evidencia que el número de personas asignadas a cada puesto es el adecuado.

Además, los auditores informáticos deben poseer un conocimiento previo de: el lugar geográfico donde se sitúan los sistemas, realizar un inventario de forma escrita que contenga la situación de todos los elementos lógicos y físicos que la empresa posee para su operación, la arquitectura hardware y software así como la configuración de los equipos, e informarse sobre las redes de comunicación utilizadas.

En cuanto a las aplicaciones utilizadas por la entidad auditada, se conocerá: la cantidad y complejidad de las aplicaciones, la documentación existente y la metodología utilizada en el desarrollo de las aplicaciones. Además, se obtendrá información sobre las bases de datos y los ficheros.

1.3.8.3 Elaboración del plan de trabajo de auditoría. Se elabora el plan y los programas de trabajo. Para la elaboración del plan de trabajo es necesario conocer si la revisión se realiza por áreas generales, cuya elaboración es más complicada y costosa, o si se realiza por áreas específicas. También se establecen las prioridades de materias que se auditan, se muestran las tareas que debe realizar cada miembro del grupo y se reflejan las ayudas que han de recibir los auditores por parte de los auditados.

El programa de trabajo detalla las actividades que se llevarán a cabo en la auditoría. Los auditores analizan el entorno y obtienen unas evidencias a través

del análisis de información (recabada por el auditor o de otra índole), pruebas, entrevistas, cuestionarios, muestreos u otras técnicas y herramientas.

1.3.8.4 Actividades de la auditoría. Durante la auditoría es importante que exista una buena comunicación entre el auditor y el auditado. Los auditores tienen que recopilar y verificar información, y los auditados pueden servir de ayuda en esta tarea. Para obtener y comprobar la información, los auditores cuentan con diferentes herramientas y técnicas que les facilitan el trabajo.

Las técnicas de auditoría informática tienen distintas finalidades, algunas se centran en comprobar el contenido de los ficheros de datos, otras están enfocadas en comprobar el buen funcionamiento del sistema y realizar pruebas sobre éste.

Algunas técnicas y herramientas que ayudan en la labor de auditar son:

- **Herramientas usadas:** paquetes de auditoría, simuladores, estándares, monitores, cuestionarios *checklist*, cuestionarios generales y matrices de riesgo.

- **Técnicas de trabajo utilizadas por los auditores**: análisis de la información recabada del auditado y de la información propia, muestreo, simulación, entrevistas y pruebas.

Referente a las pruebas que realiza el auditor se puede distinguir entre pruebas de cumplimiento y pruebas sustantivas:

- **Pruebas de cumplimiento:** el auditor evidencia las debilidades existentes en los controles internos de la organización.

- **Pruebas sustantivas:** permiten comprobar la exactitud, validez e integridad de la información mediante la observación, muestreos, entrevistas y revisiones, entre otros.

Durante todo el proceso de auditoría, el auditor elabora una extensa documentación por medio de las técnicas y herramientas utilizadas, y por los procedimientos seguidos. Toda esta documentación recopilada se conoce como los papeles de trabajo del auditor. Estos documentos justifican el trabajo realizado por los auditores.

Entre los requisitos que deben cumplir los papeles de trabajo, se destacan:

- **Claridad:** deben ser fáciles de entender y el auditor evitará los papeles manuscritos siempre que sea posible.

- **Exactitud y completitud:** de manera que puedan documentar los hechos comprobados, los juicios y conclusiones y mostrar la naturaleza y alcance de la auditoría [28].

Asimismo, los papeles de trabajo suponen un vínculo entre el trabajo realizado por el auditor con el informe final que le será entregado al cliente.

1.3.8.5 Informe final. En la última etapa del proceso de la auditoría, se mantiene una reunión de cierre con los responsables de la empresa auditada con el fin de comunicarles los principales hallazgos encontrados durante la auditoría. Después, los auditores comienzan a redactar el borrador del informe, que incluirá todas las evidencias, hallazgos, conclusiones y recomendaciones. El borrador o borradores que se elaboren se discuten con los auditados.

En último lugar, se elabora el informe final. El informe es el resultado por escrito de la evaluación realizada por los auditores sobre la situación de la entidad auditada. Siempre se realiza por escrito.

El informe reflejará fielmente y con imparcialidad los hechos reales descritos, de una forma clara y sencilla, entendible por la persona o personas a las que se dirige el informe. Se incluirá la información objetiva, los descubrimientos y las conclusiones respaldadas en los documentos de trabajo que evidencian los hechos.

Además, contendrá una descripción del trabajo que ha sido realizado y una valoración de la situación de la compañía señalando las debilidades que presenta, los riesgos a los que está expuesta y las posibles mejoras. También puede contener puntos positivos (si existen).

Igualmente, el informe deberá contener la fecha de elaboración y estar firmado por el auditor encargado del trabajo.

El informe consta de las siguientes partes:

- **Inicio del informe:** contiene en primer lugar una introducción en donde se explican los antecedentes. A continuación se incluyen los objetivos, el alcance y la profundidad de la auditoría. Posteriormente, se realiza una descripción del entorno informático, se presentan las conclusiones y finalmente se dan a conocer las limitaciones que hayan existido.

- **Cuerpo del informe:** incluye las metodologías y estándares utilizados. Además, por cada área se tratan los puntos que son objeto de mejora o de incumplimiento y se agrupan aquellos que son muy homogéneos. Cada punto debe llevar consigo una descripción detallada de la deficiencia, la causa y el efecto que tiene en la compañía y una recomendación. Al final del informe se puede adicionar un cuadro que facilite la priorización de los puntos y que facilite a la entidad dónde centrar sus esfuerzos.

- **Anexos:** en este apartado se encuentran las entrevistas realizadas, los cuestionarios utilizados y sus resultados, documentación utilizada y cualquier otro documento escrito o gráfico que pueda desviar la atención de la persona que lea el informe.

1.3.8.6 Carta de introducción del informe final. La carta de introducción o de presentación del informe definitivo resume la auditoría que ha sido realizada. Proporciona una conclusión general mostrando las debilidades más importantes (sin incluir recomendaciones).

Esta carta no sobrepasa las cuatro páginas e incluye la fecha, naturaleza, objetivos y el alcance de la auditoría. El destinatario de la carta será el responsable de la empresa o la persona que encargó la auditoría.

1.3.9 Herramientas y técnicas para la auditoría informática

1.3.9.1 Cuestionarios. Es la recopilación de datos a través de preguntas impresas, las cuales serán respondidas de acuerdo al criterio del encuestado. Posteriormente, el auditor convierte esos datos en información valiosa para realizar su trabajo [29].

Los auditores realizan una serie de cuestionarios a los auditados que, utilizados de forma correcta, pueden explicar cómo ocurren los hechos y las situaciones. Un buen auditor debe elaborar muchas veces sus cuestionarios según el área y la organización que audita [27].

Los cuestionarios deben ser específicos para cada área de la empresa auditada y para cada situación. Además, las preguntas que contiene pueden agruparse por temas [27].

Ventajas:

- Facilitan la recopilación de información y no necesitan muchas explicaciones.
- Permiten la rápida fabulación e interpretación.
- Evitan la dispersión de la información requerida.
- Son fáciles de aplicar y ayudan a recopilar mucha información en poco tiempo.
- Hacen impersonal las respuestas por lo tanto en una auditoría ayuda a recopilar información valiosa.

Desventajas:

- Falta de profundidad en las respuestas y no puede ir más allá del cuestionario.
- Se necesita una buena elección del universo y de la muestra seleccionada.
- Puede provocar la obtención de datos equivocados.
- La interpretación de los datos puede ser muy simple si el cuestionario no está bien estructurado.
- Limita la participación del auditado.

1.3.9.2 Entrevistas. La entrevista es una de las actividades más importantes del auditor, puesto que en ella se recoge más información y mejor matizada, que la proporcionada por las respuestas escritas en los cuestionarios [30].

Antes de realizar una entrevista, el auditor debe haber seleccionado a los funcionarios que va a entrevistar. Éstos pueden ser: directivos, jefes de proyecto, analistas, programadores, usuarios, técnicos de sistemas, administradores de bases de datos, auditores internos (si se trata de una auditoría externa), responsables de seguridad, responsables de desarrollo o cualquier funcionario de la organización que le aporte información relevante. Cualquiera que sea el caso, el auditado debe sentirse lo más cómodo posible y el entrevistador debe inspirar confianza. Además, las preguntas que formule el entrevistador no deben conducir a la respuesta [27].

Por otra parte, los auditores deben tener la capacidad de captar información no verbal, como gestos realizados por el entrevistado, las posturas, los silencios y reacciones del entrevistado ante determinadas preguntas.

Tipos de entrevistas [31]

- **Libres:** son las entrevistas en las que se sigue un guión básico para obtener la información requerida, pero la participación del entrevistado es libre y sin ninguna atadura.

- **Dirigidas:** en estas entrevistas siempre se dirigen las opiniones del entrevistado, forzando sus respuestas dentro de un parámetro o guión preestablecido, sin admitir ni permitir ninguna variación significativa.

- **De exploración:** son entrevistas de carácter libre y pueden ser muy útiles para buscar algún punto de partida para la evaluación. También se hacen con la intención de familiarizar al auditor con los sistemas que va a evaluar.

- **De comprobación:** estas entrevistas se realizan para comprobar la veracidad de la información recopilada durante la evaluación y permiten corroborar y rectificar los datos y percepciones sobre las observaciones encontradas con las pruebas e instrumentos aplicados en la auditoría.

- **De información:** se utiliza este tipo de entrevistas, para que el auditor comente cada una de las desviaciones que reporta en su informe, y con ello obtiene información; además le ayuda a recopilar datos útiles para encontrar las causas y soluciones que complementen sus observaciones.

- **Informales:** ayudan a conocer algún tipo de problemática que sólo se expresa cuando no existe la presión de una entrevista formal.

1.3.9.3 *Checklist*. El conjunto de preguntas contenidas en un cuestionario es lo que se conoce como *checklist*. Generalmente, las *checklists* se contestan oralmente. Es importante la manera de formular las preguntas y el modo. El auditado debe responder de forma escueta y clara. El auditor sólo interrumpirá cuando las respuestas no se ajusten a las preguntas o desee una aclaración de la respuesta. Determinadas preguntas de especial trascendencia han de repetirse, formuladas de manera distinta para comprobar si existen contradicciones [27].

Las *checklists* pueden ser [27]:

- ***Checklist* de rango:** las preguntas se puntúan dentro de un rango preestablecido. Por ejemplo, el rango puede comprender los valores desde 1 (como valor más desfavorable) a 5 (como valor más positivo); o de 1 a 10.

- ***Checklist* binaria:** las preguntas tienen como respuesta sí o no, lo que aritméticamente equivale a un 1 o un 0.

1.3.9.4 Trazas y/o huellas. En una traza se comprueba que la ejecución y resultado de un programa es adecuado, haciendo un seguimiento de dicha ejecución y las validaciones de datos llevados a cabo [27].

Una traza es un registro histórico de todos los cambios realizados junto con la información del usuario que realizó la modificación y la fecha. Las trazas no modifican el sistema. Si estas trazas sobrecargan el sistema, se prevé las fechas y horas más apropiadas para utilizarlas [27].

1.3.9.5 Observación. Es la acción de observar, analizar, advertir, estudiar, examinar y mirar detenidamente todo lo relacionado con los sistemas de una empresa. Esta técnica es muy utilizada por los auditores ya que les permite recolectar directamente la información necesaria [29].

1.3.9.6 Inventarios. Esta forma de recopilación de información consiste en hacer un recuento físico de lo que se está auditando a fin de saber la cantidad existente de algún producto en una fecha determinada y compararla con la que debería haber según los documentos en esa misma fecha [29].

1.3.9.7 Flujogramas. Se utilizan para representar gráficamente procesos realizados. Permite plasmar las entradas, las salidas que se producen y los procesos o funciones que recorre [27].

Los diagramas de flujos pueden mostrar controles utilizados en la compañía, las autorizaciones, la segregación de funciones o cualquier proceso que interese reflejar a través de esta herramienta.

1.3.9.8 Muestreo estadístico. Las muestras pueden referirse al control de visitas, a la alteración de documentación, a la revisión de programas y cualquier otra información que probablemente no sea viable analizar al 100% de la “población” por lo que se analiza una muestra representativa [27].

El mayor inconveniente es que el resultado podría diferir si la muestra hubiera sido completa. Se debe encontrar un equilibrio entre el costo o esfuerzo y una fiabilidad aceptable. Además, se puede hacer uso de paquetes estadísticos.

1.3.9.9 CAATs (*Computer Asisted Audit Techniques*) o TAAOs (Técnicas de Auditoría Asistida por Ordenador). Son un conjunto de técnicas que utilizan herramientas informáticas a lo largo de todo el proceso de auditoría. Las que más se utilizan, son: software de auditoría generalizado, software utilitario, los datos de prueba y sistemas expertos de auditoría [27, 32].

Las CAATs se pueden utilizar para realizar varios procedimientos de auditoría incluyendo: prueba de los detalles de operaciones y saldos, procedimientos de revisión analíticos, pruebas de cumplimiento de los controles generales de sistemas de información, pruebas de cumplimiento de los controles de aplicación, entre otros [32].

1.3.9.10 Software especializado en la realización de pruebas. Hoy por hoy existen herramientas extremadamente útiles a la hora de detectar y solucionar fallos en redes y sistemas de información (ver Tabla 1), gracias a que están diseñadas de tal manera que permiten recopilar la información necesaria para asegurar el buen funcionamiento de los servicios implementados en la organización. Sin embargo, hay que resaltar que dichas herramientas pueden ser usadas tanto por analistas de seguridad como por piratas informáticos.

Tabla 1. Herramientas de seguridad más utilizadas

Nombre	Plataformas	Descripción
	Linux Windows Mac OS X	Herramienta libre para la auditoría de redes. Dispone de una amplia gama de técnicas para el escaneo de puertos TCP y UDP con las que se podrán determinar qué equipos se encuentran activos y qué servicios están corriendo.
	Linux Windows	IDS (sistema de detección de intrusos) bajo licencia GPL. Está formado por un motor de detección de ataques que implementa una gran base de datos de filtros que permiten detectar anomalías en la red.
	Windows	Herramienta de recuperación de contraseñas gratuita. Facilita la recuperación de varias clases de contraseñas ya sea escuchando la red, rompiendo contraseñas cifradas, analizando protocolos de enrutamiento, entre otros métodos.
	Linux Windows	Analizador de protocolos de red que permite capturar y navegar de forma interactiva por los contenidos de los paquetes capturados en la red.
	Windows	Herramienta de auditoría y recuperación de contraseñas. Es usada para verificar la debilidad de las contraseñas y algunas veces para recuperar las que se han olvidado o perdido.

Tabla 1. (Continuación)

Nombre	Plataformas	Descripción
	Linux Windows Mac OS X	Escáner de vulnerabilidades. Tiene como características principales la configuración del tipo de auditoría, la velocidad de trabajo, perfiles activos, búsqueda de información sensible y el análisis de vulnerabilidades personalizado. Puede trabajar en cualquier zona de la red.
	Linux	Distribución GNU/Linux, popular en el mundo de la seguridad informática. Está desarrollada por profesionales de seguridad y está dirigida al análisis forense y *Penetration Testing*.
	Linux Windows	Programa de criptografía que aplica fuerza bruta para descifrar contraseñas. Es una herramienta de seguridad muy popular, ya que permite a los administradores de sistemas comprobar que las contraseñas de los usuarios son suficientemente buenas.

Fuente: INTECO (Instituto Nacional de Tecnologías de la Comunicación).

1.3.10 Técnicas avanzadas de auditoría informática. Cuando en una organización se encuentren operando sistemas avanzados de computación, como procesamiento en línea, bases de datos y procesamiento distribuido, se puede evaluar el sistema empleando técnicas avanzadas de auditoría. Estas técnicas requieren de un experto y, por lo tanto, pueden no ser apropiadas si el equipo auditor no cuenta con el entrenamiento adecuado. Sin embargo, cuando se usan apropiadamente, superan todas las expectativas. Entre las técnicas avanzadas más utilizadas se encuentran las siguientes [47]:

- **Pruebas integrales:** consisten en el procesamiento de datos ficticios, comparando estos resultados con resultados predeterminados.

- **Simulación:** consiste en desarrollar programas de aplicación para determinada prueba y comparar los resultados de la simulación con la aplicación real.

- **Revisiones de acceso:** se conserva un registro computarizado de todos los accesos a determinados archivos; por ejemplo, información de la identificación tanto de la terminal como del usuario.

- **Operaciones en paralelo:** consiste en verificar la exactitud de la información sobre los resultados que produce un sistema nuevo que sustituye a uno ya auditado.

- **Evaluación de un sistema con datos de prueba:** consiste en la comparación de los resultados de la aplicación actual con datos de prueba contra los resultados que fueron obtenidos en las pruebas iniciales del programa (solamente aplicable cuando se hacen modificaciones a un sistema).

- **Registros extendidos:** consiste en agregar un campo de control a un registro determinado para controlar parte por parte los resultados de un sistema, como en los siguientes casos:

a. Totales aleatorios de ciertos programas: se consiguen totales en algunas partes del sistema para ir verificando su exactitud en forma parcial.

b. Resultados de ciertos cálculos para comparaciones posteriores: con ellos se puede comparar en el futuro los totales en diferentes fechas.

c. Selección de determinado tipo de transacciones como auxiliar en el análisis de un archivo histórico: por medio de este método se puede analizar en forma parcial el archivo histórico de un sistema.

1.3.11 Estándares utilizados en la auditoría informática

1.3.11.1 COBIT (*Control Objectives for Information and Related Technology*).

COBIT, lanzado en 1996, es una herramienta de gobierno de Tecnologías de la Información que vincula tecnología informática y prácticas de control para consolidar y armonizar estándares de fuentes globales prominentes en un recurso crítico para la gerencia, los profesionales de control y los auditores [33].

COBIT se aplica a los sistemas de información de toda la empresa, incluyendo las computadoras personales, mini computadoras y ambientes distribuidos. Está basado en la filosofía de que los recursos de Tecnologías de la Información necesitan ser administrados por un conjunto de procesos naturalmente agrupados para proveer la información pertinente y confiable que requiere una organización a la hora de lograr sus objetivos [33].

Usuarios

- **La gerencia:** para apoyar sus decisiones de inversión en Tecnologías de la Información y tener control sobre el rendimiento de las mismas, analizando el costo beneficio de dicho 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 Tecnologías de la Información, su impacto en la organización y determinar el control mínimo requerido.

- **Los responsables de Tecnologías de la Información:** para identificar los controles que requieren en sus áreas.

También puede ser utilizado por los encargados de un proceso de negocio y por todos aquellos con responsabilidades en el campo de las Tecnologías de la Información en las empresas [33].

Características [33]

- Orientado al negocio.
- Alineado con estándares y regulaciones "de facto".[5]
- Basado en una revisión crítica y analítica de las tareas y actividades en TI.
- Alineado con estándares de control y auditoría (COSO, IFAC[6], IIA[7], ISACA[8], AICPA[9]).

[5] Normas que se caracterizan por no ser consensuadas ni legitimadas por un organismo de estandarización, pero que generalmente son aceptadas y ampliamente utilizadas por un gran número de interesados.

[6] Acrónimo de *International Federation of Accountants.* Desarrolla y promueve una profesión contable con estándares armonizados, capaces de promover servicios de alta calidad consecuente con el interés público.

[7] Acrónimo de *Institute of Internal Auditors.* Es una asociación internacional dedicada al desarrollo profesional continuado del auditor interno y de la profesión de auditoría interna.

[8] Acrónimo de *Information Systems Audit and Control Association & Foundation.* Es una organización global que establece las pautas para los profesionales de gobernación, control, seguridad y auditoría de información.

[9] Acrónimo de *American Institute of Certified Public Accountants.* Elabora y promueve estándares profesionales para la auditoría del estado de cuentas y otros tipos de auditorías financieras o relacionadas.

Requerimientos de la información del negocio [33]

El enfoque del control en Tecnologías de la Información se lleva a cabo visualizando la información necesaria para dar soporte a los procesos de negocio. Para ello, la información debe satisfacer ciertos criterios:

- Requerimientos de calidad: calidad, costo y entrega.
- Requerimientos fiduciarios: efectividad, eficiencia operacional, confiabilidad de los reportes financieros y cumplimiento de leyes y regulaciones.
- Requerimientos de seguridad: confidencialidad, integridad y disponibilidad.

Recursos de tecnologías de la información [33]

En COBIT se establecen los siguientes recursos en Tecnologías de la Información necesarios para alcanzar los objetivos de negocio:

- **Datos:** son todos los objetos de información. Considera información interna y externa, estructurada o no, gráficas, sonidos, etc.

- **Aplicaciones:** entendido como los sistemas de información, que integran procedimientos manuales y sistematizados.

- **Tecnología:** incluye hardware y software básico, sistemas operativos, sistemas de administración de bases de datos, de redes, telecomunicaciones, multimedia, etc.

- **Instalaciones:** incluye los recursos necesarios para alojar y dar soporte a los sistemas de información.

- **Recurso humano:** por la habilidad, conciencia y productividad del personal para planear, adquirir, prestar servicios, dar soporte y monitorear los sistemas de Información.

Estructura [33]

COBIT se divide en tres niveles:

- **Dominios:** la agrupación natural de procesos, normalmente corresponde a un dominio o una responsabilidad organizacional.

- **Procesos:** conjuntos o series de actividades unidas con delimitación o cortes de control.

- **Actividades:** acciones requeridas para lograr un resultado medible.

Por consiguiente, COBIT define 34 procesos genéricos agrupados en cuatro grandes dominios que se detallan a continuación [33]:

Tabla 2. Dominios y Procesos de COBIT

Dominio	Descripción	Procesos
Planear y Organizar	Este dominio cubre las estrategias y las tácticas, y tiene que ver con identificar la manera en que TI puede contribuir de la mejor manera al logro de los objetivos del negocio. Además, la realización de la visión estratégica requiere ser planeada, comunicada y administrada desde diferentes perspectivas. Finalmente, se debe implementar una estructura organizacional y una estructura tecnológica apropiada.	• PO1 Definir un plan estratégico de TI • PO2 Definir la arquitectura de la información • PO3 Determinar la dirección tecnológica • PO4 Definir los procesos, organización y relaciones de TI • PO5 Administrar la inversión en TI • PO6 Comunicar las aspiraciones y la dirección de la gerencia • PO7 Administrar recursos humanos de TI • PO8 Administrar la calidad • PO9 Evaluar y administrar los riesgos de TI • PO10 Administrar proyectos
Adquirir e Implementar	Para llevar a cabo la estrategia de TI, las soluciones de TI necesitan ser identificadas, desarrolladas o adquiridas así como implementadas e integradas en los procesos del negocio. Además, el cambio y el mantenimiento de los sistemas existentes está cubierto por este dominio para garantizar que las soluciones sigan satisfaciendo los objetivos del negocio.	• AI1 Identificar soluciones automatizadas • AI2 Adquirir y mantener software aplicativo • AI3 Adquirir y mantener infraestructura tecnológica • AI4 Facilitar la operación y el uso • AI5 Adquirir recursos de TI • AI6 Administrar cambios • AI7 Instalar y acreditar soluciones y cambios

Tabla 2. (Continuación)

Dominio	Descripción	Procesos
Entregar y Dar Soporte	Este dominio cubre la entrega en sí de los servicios requeridos, lo que incluye la prestación del servicio, la administración de la seguridad y de la continuidad, el soporte del servicio a los usuarios, la administración de los datos y de las instalaciones operativas.	• Ds1 Definir y administrar los niveles de servicio • Ds2 Administrar los servicios de terceros • Ds3 Administrar el desempeño y la capacidad • Ds4 Garantizar la continuidad del servicio • Ds5 Garantizar la seguridad de los sistemas • Ds6 Identificar y asignar costos • Ds7 Educar y entrenar a los usuarios • Ds8 Administrar la mesa de servicio y los incidentes • Ds9 Administrar la configuración • Ds10 Administrar los problemas • Ds11 Administrar los datos • Ds12 Administrar el ambiente físico • Ds13 Administrar las operaciones
Monitorear y Evaluar	Todos los procesos de una organización necesitan ser evaluados regularmente a través del tiempo para verificar su calidad y suficiencia en cuanto a los requerimientos de control, integridad y confidencialidad.	• M1 Monitorear y evaluar el desempeño de TI • M2 Monitorear y evaluar el control interno • M3 Garantizar el cumplimiento regulatorio • M4 Proporcionar gobierno de TI

Fuente: Normas COBIT 4.1.

1.3.11.2 ISO/IEC 27000. Sistemas de gestión de la seguridad de la información. ISO/IEC 27000 es un conjunto de estándares desarrollados por ISO (*International Organization for Standardization*) e IEC (*International Electrotechnical Commission*), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, ya sea pública o privada, grande o pequeña [34].

A continuación, se resume las distintas normas que componen la serie ISO/IEC 27000:

- **ISO/IEC 27000. Sistemas de gestión de seguridad de la información, generalidades y vocabulario:** publicada en Abril de 2009. En ella se recogen los términos y conceptos relacionados con la seguridad de la información, una visión general de la familia de estándares de esta área, una introducción a los SGSI[10] y una descripción del ciclo de mejora continua [35].

- **ISO/IEC 27001. Sistemas de gestión de la seguridad de la información (SGSI). Requisitos. (ISO/IEC 27001:2005):** publicada en el año 2005. Ésta es la norma fundamental de la familia, ya que contiene los requerimientos del sistema de gestión de seguridad de la información y es la norma con arreglo a la cual serán certificados los SGSI de las organizaciones que lo deseen [35].

- **ISO/IEC 27002. Tecnología de la información. Código de buenas prácticas para la gestión de la seguridad de la información:** publicada en el año 2005. Esta guía de buenas prácticas describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. Fue actualizada desde la ISO/IEC 17799:2005 y renombrada en el 2007 como ISO 27002:2005 [35, 36].

- **ISO/IEC 27003:** guía de implementación de un SGSI e información acerca del uso del modelo PDCA[11] y de los requerimientos de sus diferentes fases [35].

- **ISO/IEC 27004:** estándar para la medición de la efectividad de la implantación de un SGSI y de los controles relacionados [35].

- **ISO/IEC 27005:2008. Gestión del riesgo en la seguridad de la información:** publicada en el año 2008. Esta norma se ajusta a las necesidades de las organizaciones que pretenden realizar su análisis de riesgos en este ámbito y cumplir con los requisitos de la Norma ISO 27001 [35].

- **ISO/IEC 27006. Requisitos para las entidades que suministran servicios de auditoría y certificación de sistemas de gestión de seguridad de la información:** publicada en el año 2007. Recoge los criterios mediante los cuales una organización se puede acreditar para realizar esos servicios [35].

- **ISO/IEC 27007:** guía para la realización de las auditorías de un SGSI [35].

[10] Acrónimo de Sistemas de Gestión de Seguridad de la Información.

[11] Acrónimo de *Plan, Do, Check, Act* (Planificar, Hacer, Verificar, Actuar). Es una estrategia de mejora continua de la calidad.

- **ISO/IEC TR 27008:** proporcionará una guía para auditar los controles de seguridad de la norma ISO 27002:2005 [36].

- **ISO/IEC 27010:** proporcionará una guía específica para el sector de las comunicaciones y sistemas de interconexión de redes de industrias y administraciones, a través de un conjunto de normas más detalladas que comenzarán a partir de la ISO/IEC 27011 [36].

- **ISO/IEC 27011. Directrices para la seguridad de la información en organizaciones de telecomunicaciones utilizando la norma ISO/IEC 27002:** contiene recomendaciones para empresas de este sector, facilitando el cumplimiento de la norma ISO 27001 y conseguir un nivel de seguridad aceptable [35].

- **ISO/IEC 27031:** estará centrada en la continuidad de negocio [36].

- **ISO/IEC 27032:** será una guía para la cyberseguridad [36].

- **ISO/IEC 27033:** sustituirá a la ISO/IEC 18028, norma sobre la seguridad en redes de comunicaciones [36].

- **ISO/IEC 27034:** proporcionará guías para la seguridad en el desarrollo de aplicaciones [36].

- **ISO/IEC 27799. Gestión de la seguridad de la información sanitaria utilizando la norma ISO/IEC 27002 (ISO 27799:2008):** no será estrictamente una parte de la serie ISO 27000 aunque proporcionará una guía para el desarrollo de SGSI para el sector específico de la salud [35].

1.3.11.3 ISO/IEC 27001. Sistemas de gestión de la seguridad de la información. Especifica los requisitos para establecer, implantar, operar, monitorizar, revisar, mantener, documentar y evaluar un sistema de gestión de la seguridad de la información de acuerdo a la norma ISO/IEC 27002 dentro del contexto de los riesgos identificados por la organización [35].

Está basada en un enfoque por procesos y en la mejora continua, por lo tanto es perfectamente compatible e integrable con el resto de sistemas de gestión que ya existan en la organización. La norma asume que la organización identifica y administra cualquier tipo de actividad para funcionar eficientemente. Cualquier actividad que emplea recursos y es administrada para transformar entradas en salidas, puede ser considerada como un proceso. A menudo, estas salidas son aprovechadas nuevamente como entradas, generando una retroalimentación de

los mismos. Estos procesos se someten a revisiones para detectar fallos e identificar mejoras, por lo que se encuentran dentro de un proceso de mejora continua [35].

La norma recoge:

- Los componentes del SGSI o la documentación del sistema: qué documentos mínimos deben formar parte del SGSI, cómo se deben crear, gestionar y mantener y cuáles son los registros que permitirán evidenciar el buen funcionamiento del sistema.
- Cómo se debe diseñar e implantar el SGSI.
- Define los controles de seguridad a considerar.
- Cómo debe realizarse la revisión y mejora del SGSI.

1.3.11.4 ISO/IEC 27002. Sistemas de gestión de la seguridad de la información. ISO/IEC 17799 (denominada actualmente como ISO 27002) es un estándar para la seguridad de la información publicado por primera vez en el año 2000, con el título de *Information technology - Security techniques - Code of practice for information security management*. Tras un periodo de revisión y actualización de los contenidos del estándar, se publicó en el año 2005 el documento actualizado denominado ISO/IEC 17799:2005 [37].

Con la aprobación de la norma ISO/IEC 27001 en octubre de 2005 y la reserva de la numeración 27000 para la seguridad de la información, el estándar ISO/IEC 17799:2005 pasó a ser renombrado como ISO/IEC 27002 en la revisión y actualización de sus contenidos en el 2007 [37].

Alcance

El estándar va orientado a la seguridad de la información en las empresas u organizaciones, de modo que las probabilidades de ser afectadas por robo, daño o pérdida de información se minimicen al máximo [38].

Directrices del estándar

ISO/IEC 27002 proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información. La seguridad de la información se define en el estándar como "la

preservación de la confidencialidad (asegurando que sólo quienes estén autorizados pueden acceder a la información), integridad (asegurando que la información y sus métodos de proceso son exactos y completos) y disponibilidad (asegurando que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran)" [39].

El estándar ISO/IEC 27002 está compuesto por 11 dominios, los cuales se centran en un determinado aspecto de la seguridad de la información y conjuntamente abarcan un total de 133 controles de seguridad. Dichos dominios son los siguientes:

1. Política de seguridad de la información: su objetivo es proporcionar a la gerencia la dirección y soporte para la seguridad de la información conforme con los requerimientos comerciales y las leyes y regulaciones relevantes. Cuenta con dos controles: Documento de Política de seguridad y Revisión del sistema [38,35].

2. Organización de la seguridad de la información: la organización de la seguridad de la información se puede dar de dos formas: organización interna y organización con respecto a terceros [38].

3. Gestión de activos de información: se deben asignar responsabilidades por cada uno de los activos de la organización, así como poseer un inventario actualizado de todos los activos que se tienen, a quien/quienes les pertenecen, el uso que se les debe dar, y la clasificación de todos los activos [38].

4. Seguridad de los recursos humanos: su objetivo es asegurar que los empleados, contratistas y terceros entiendan sus responsabilidades, y sean idóneos para los roles para los cuales son considerados, reduciendo el riesgo de robo, fraude y mal uso de los medios [38].

5. Seguridad física y ambiental: se divide en áreas seguras y seguridad de los equipos [38].

6. Gestión de las comunicaciones y operaciones: su objetivo es asegurar la operación correcta y segura de los medios de procesamiento de la información [38].

7. Control de accesos: se debe contar con una política de control de acceso. Todo acceso no autorizado debe ser evitado y se deben minimizar al máximo las probabilidades de que eso suceda. Todo esto se controla mediante registro de usuarios, gestión de privilegios, autenticación mediante usuarios y contraseñas [38].

8. Adquisición, desarrollo y mantenimiento de sistemas de información: contemplar aspectos de seguridad es requerido al adquirir equipos y sistemas, o al desarrollarlos. No solamente se debe considerar la calidad y el precio, sino la seguridad que ofrecen. Debe existir validación de datos de entrada, control de acceso al código fuente de los programas y control de vulnerabilidades técnicas [38, 35].

9. Gestión de incidentes en la seguridad de la información: la comunicación es fundamental en todo proceso. Por lo tanto, se debe trabajar con reportes de los eventos y debilidades de la seguridad de la información, asegurando una comunicación tal que permita que se realice una acción correctiva oportuna, llevando la información a través de los canales gerenciales apropiados lo más rápidamente posible [38].

10. Gestión de continuidad del negocio: se deben tener planes y medidas para hacerle frente a los incidentes, de modo que el negocio pueda continuar en marcha gracias a medidas alternativas para que un incidente no detenga las operaciones por tiempos prolongados, que no se pierda información, que no se estanquen o detengan las ventas o negocios [38].

11. Cumplimiento: debe darse el debido cumplimiento a los requisitos legales, como derechos de propiedad intelectual, derecho a la confidencialidad de cierta información y control de auditorías [38].

1.3.12 Riesgo informático. El riesgo informático es la incertidumbre existente por la posible realización de un suceso relacionado con la amenaza de daño respecto a los bienes o servicios informáticos (ordenadores, periféricos, instalaciones o programas de cómputo) [44].

Por lo anterior, es importante que toda organización cuente con una herramienta que garantice la correcta evaluación de los riesgos a los cuales están sometidos los procesos y actividades que participan en el área informática, y que por medio de procedimientos de control se pueda evaluar el desempeño del entorno informático. En otras palabras, es vital que las organizaciones recurran al denominado análisis de riesgos [44,45].

El análisis de riesgos tiene como objetivos: identificar los riesgos y lograr establecer el riesgo total y el riesgo residual, ya sea en términos cuantitativos o cualitativos. Cuando se habla de riesgo total se hace referencia a la combinación de los elementos que lo conforman, mientras que el riesgo residual es el riesgo remanente luego de la aplicación de medidas destinadas a mitigar los riesgos

existentes. Dichas medidas son aquellas que generalmente se conocen como controles [45].

Realizar el análisis de riesgos es indispensable para lograr administrar adecuadamente los mismos. Administrar el riesgo se refiere a gestionar los recursos de la organización para lograr un nivel de exposición determinado. Este nivel es generalmente establecido según el tipo de activo, permitiendo una menor exposición en cuanto más crítico sea el activo [45].

Luego de efectuar las tareas referentes al análisis, el ciclo de administración de riesgos se cierra con la determinación de acciones a seguir respecto a los riesgos residuales identificados. Estas acciones pueden ser [45]:

- **Controlar el riesgo:** se fortalecen los controles existentes o se agregan nuevos.
- **Eliminar el riesgo:** se elimina el activo relacionado y por ende el riesgo.
- **Compartir el riesgo:** mediante acuerdos contractuales se traspasa parte del riesgo a un tercero (un ejemplo son los seguros).
- **Aceptar el riesgo:** determinar que el nivel de exposición es adecuado.

Tipos de riesgos

1. Riesgos de integridad: abarcan todos los riesgos asociados con la autorización, completitud y exactitud de la entrada, procesamiento y reportes de las aplicaciones utilizadas en una organización [44].

2. Riesgos de relación: se refieren al uso oportuno de la información creada por una aplicación. Estos riesgos se relacionan directamente con la información utilizada para la toma de decisiones (Información y datos correctos de una persona/proceso/sistema en el tiempo preciso permiten tomar decisiones correctas) [44].

3. Riesgos de acceso: estos riesgos se enfocan al inapropiado acceso a sistemas, datos e información. Estos riesgos abarcan: Los riesgos de segregación inapropiada de trabajo, los riesgos asociados con la integridad de la información de sistemas de bases de datos y los riesgos asociados a la confidencialidad de la información [44].

4. Riesgos de utilidad: estos riesgos se enfocan en tres diferentes niveles de riesgo [44]:

- Los riesgos pueden ser enfrentados por el direccionamiento de sistemas antes de que los problemas ocurran.
- Técnicas de recuperación/restauración usadas para minimizar la ruptura de los sistemas.
- *Backups*[12] y planes de contingencia controlan desastres en el procesamiento de la información.

5. Riesgos de infraestructura: estos riesgos se refieren a que en las organizaciones no existe una estructura de información tecnológica efectiva (hardware, software, redes, personas y procesos) para soportar adecuadamente las necesidades futuras y presentes de los negocios con un costo eficiente. Estos riesgos están asociados con los procesos de la información tecnológica que definen, desarrollan, mantienen y operan un entorno de procesamiento de información y las aplicaciones asociadas (servicio al cliente, pago de cuentas, etc) [44].

6. Riesgos de seguridad general: el estándar IEC 950 es un estándar internacional para seguridad de los equipos de procesamiento de datos o similares. Es así como específica las reglas con relación a la construcción, aislamiento y características de seguridad de los equipos de cómputo con el fin de disminuir riesgos, tales como [44]:

- **Choques eléctricos:** niveles altos de voltaje.
- **Incendios:** inflamabilidad de materiales.
- **Radiaciones:** ondas de ruido, de láser y ultrasónicas.
- **Riesgos mecánicos:** inestabilidad de las piezas eléctricas.

Metodologías de análisis y gestión de riesgos

1. MAGERIT (Metodología de análisis y gestión de riesgos de los sistemas de información): esta metodología interesa a todos aquellos que trabajan con información mecanizada y los sistemas informáticos que la tratan. Si dicha información o los servicios que se prestan gracias a ella son valiosos, esta metodología les permitirá saber cuánto de este valor está en juego y les ayudará a protegerlo [40].

Magerit persigue los siguientes objetivos [40]:

[12] Copias de seguridad. Es la copia total o parcial de información importante del disco duro, CDs, bases de datos u otro medio de almacenamiento. Fundamentalmente se utilizan para dos cosas: para recuperarse de una catástrofe informática y para recuperar una pequeña cantidad de archivos que pueden haberse eliminado accidentalmente o corrompido.

➢ **Directos**

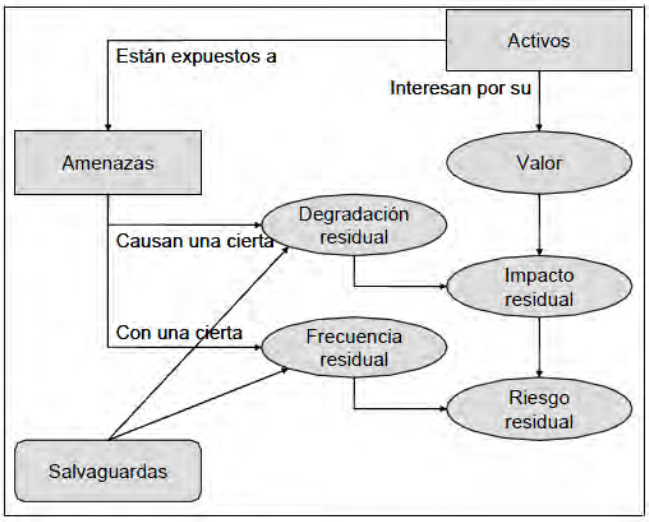
✓ Concienciar a los responsables de los sistemas de información de la existencia de riesgos y de la necesidad de atajarlos a tiempo.
✓ Ofrecer un método sistemático para analizar tales riesgos.
✓ Ayudar a descubrir y planificar las medidas oportunas para mantener los riesgos bajo control.

➢ **Indirectos**

✓ Preparar a la organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

La metodología Magerit se puede resumir gráficamente de la siguiente forma [41]:

Figura 2. Metodología Magerit



Fuente: MATALOBOS VEIGA, Juan Manuel. Análisis de riesgos de seguridad de la información.

2. CRAMM (*CCTA risk analysis and management method*): es la metodología de análisis de riesgos desarrollada por la Agencia Central de Comunicación y Telecomunicación del gobierno británico. Consta de las siguientes 3 etapas [43]:

- La primera recoge la definición global de los objetivos de seguridad entre los que se encuentra la definición del alcance, la identificación y evaluación de los activos físicos y software implicados, la determinación del valor de los datos en cuanto a impacto en el negocio y la identificación.

- En la segunda etapa de la metodología se hace el análisis de riesgos, identificando las amenazas que afectan al sistema, así como las vulnerabilidades que explotan dichas amenazas y por último el cálculo de los riesgos de materialización de las mismas.

- En la tercera etapa, se identifican y seleccionan las medidas de seguridad a aplicar en la entidad obteniendo los riesgos residuales.

3. MECI (Modelo estándar de control interno): es una herramienta de gestión que busca unificar criterios en materia de control interno para el sector público, estableciendo una estructura para el control de la estrategia, la gestión y la evaluación. Surge a partir de la estructura establecida por la Ley 87 de 1993 (Colombia) para el Sistema de Control Interno, el cual está compuesto por una serie de subsistemas, componentes y elementos de control [42].

Entre las principales características del MECI se encuentran las siguientes:

- Se fundamenta en la construcción de una ética institucional.
- Toma como base los modelos internacionales de Control Interno: COSO (Usa), COCO (Canadá), CADBURY (Reino Unido), COBIT (Australia) y GAO (USA Gubernamental).
- Se orienta a la prevención de riesgos.
- Se hace efectivo en una organización por procesos (Gestión de la Calidad).
- Encauza a la entidad hacía un control corporativo permanente.
- Mide la gestión en tiempo real.
- Enfatiza en la generación de información suficiente, pertinente, oportuna, de utilidad organizacional y social, articulada con los sistemas de información existentes.
- Controla la efectividad de los procesos de comunicación pública y rendición de cuentas.
- Fortalece la función de evaluación independiente al control y la gestión.
- Se orienta hacía la estandarización de metodologías y procedimientos de evaluación del sistema de control interno.
- Otorga alto nivel de importancia a los planes de mejoramiento.

1.3.13 Controles. Los controles son acciones y mecanismos definidos para prevenir o reducir el impacto de los eventos no deseados que ponen en riesgo a los activos de una organización. También protege a las organizaciones frente a posibles pérdidas y corrige las desviaciones que se presentan en el desarrollo normal de las actividades [46].

Los controles deben ser suficientes, comprensibles, eficaces, económicos y oportunos y, para ello, es preciso conocer la naturaleza de los riesgos y su frecuencia, así como las consecuencias que implican para que las actividades y los procesos mantengan el rumbo trazado por la organización [46].

De forma genérica, según sea la aplicación de los controles, éstos pueden ser:

- **Voluntarios:** cuando la organización los diseña a fin de mejorar los procesos.
- **Obligatorios:** si son impuestos por autoridades externas o reguladoras.
- **Manuales:** cuando son ejecutados por personas.
- **Automáticos:** si se llevan a cabo a través de sistemas de información.
- **De aplicación:** cuando operan imbricados en el software.

Los controles se clasifican también en preventivos, detectivos y correctivos [46]:

- **Controles preventivos:** actúan sobre la causa de los riesgos con el fin de disminuir su probabilidad de ocurrencia, y constituyen la primera línea de defensa. También actúan para reducir la acción de los agentes generadores de riesgos. Son los más rentables, pues evitan costos de corrección o reproceso.

- **Controles detectivos:** se diseñan para descubrir un evento, irregularidad o resultado no previsto, alertan sobre la presencia de riesgos y permiten tomar medidas inmediatas, pudiendo ser manuales o automáticos. Generalmente, sirven para supervisar la ejecución del proceso y se usan para verificar la eficacia de los controles preventivos. Constituyen la segunda barrera de seguridad y pueden informar y registrar la ocurrencia de los hechos no deseados, accionar alarmas, bloquear la operación de un sistema, monitorizar o alertar a las autoridades.

- **Controles correctivos:** permiten el restablecimiento de la actividad después de ser detectado el evento no deseable y la modificación de las acciones que propiciaron su ocurrencia. Estos controles se establecen cuando los anteriores no operan y permiten mejorar las deficiencias. Por lo general, actúan con los controles detectivos, implican reprocesos y son los más costosos porque actúan cuando ya se han presentado los hechos que implican pérdidas para la organización.

2. METODOLOGÍA

La metodología es una guía que indica qué hacer y cómo actuar de forma ordenada para llevar a cabo cualquier tipo de investigación. Por lo tanto, para el desarrollo de ésta auditoría, es preciso usar una metodología de tipo cualitativo y cuantitativo, ya que se basa en la obtención de información a partir de la cuantificación de datos sobre variables y además se producen registros narrativos a través de las entrevistas y la observación. Asimismo, dicha metodología se divide en varias etapas que son las siguientes:

Etapa 1. Exploración del entorno: Es la etapa en la cual se realiza un estudio previo a la ejecución de la auditoría, a fin de conocer en detalle las características del Hospital Universitario Departamental de Nariño y del Sistema de Información Dinámica Gerencial Hospitalaria, para obtener los elementos necesarios que permitan la adecuada planeación del trabajo a realizar y enfocarlo para que sea coherente con los objetivos previstos. Los resultados de la exploración permiten, además, determinar y priorizar los procesos que se van a auditar.

Durante esta etapa se realizaron varias visitas a las instalaciones del Hospital, con el propósito de recolectar información acerca del funcionamiento del sistema de información y de la organización general del área de sistemas. Para ello se interactuó de manera formal e informal con los funcionarios de dicha dependencia a través de la aplicación de entrevistas abiertas y cuestionarios.

Etapa 2. Planeación de la auditoría: En esta etapa se realiza la planificación de todo el proceso de auditoría, desarrollando las siguientes actividades:

1. Identificar el alcance y los objetivos de la auditoría a realizar.
2. Realizar el estudio inicial en el Hospital, para recolectar datos sobre el funcionamiento del sistema.
3. Determinar los recursos necesarios para realizar la auditoría.
4. Realizar la búsqueda bibliográfica y de Internet sobre seguridad de la información.
5. Elaborar el plan de trabajo.

Etapa 3. Realización de las actividades de auditoría: En esta etapa se ejecutan las actividades planificadas en la etapa anterior, aplicando distintas técnicas y

utilizando herramientas que garanticen el cumplimiento de los objetivos planteados. Se realizan entonces, las siguientes actividades:

1. Elaboración del plan de auditoría, mediante la elección de procesos y objetivos de control de COBIT a evaluar. Dichos procesos deben ser equiparados, además, con los objetivos de control de la norma ISO/IEC 27002.

2. Elaboración de Cuadros de Definición de Fuentes de Conocimiento para cada uno de los procesos COBIT seleccionados, de tal manera que faciliten la identificación de la fuente de obtención de las pruebas.

3. Elaboración de cuestionarios cuantitativos para cada uno de los procesos COBIT seleccionados, partiendo de la información obtenida a través de la aplicación de entrevistas.

4. Recopilación de pruebas que permitan verificar el cumplimiento o incumplimiento de los procesos COBIT seleccionados. Para ello es preciso realizar actividades tales como la revisión de documentos, el uso de medios electrónicos (cámara digital, grabadora de voz) para dar soporte a la evaluación de los procesos y la realización de pruebas de seguridad concernientes al sistema DGH.

5. Análisis de hallazgos, detectando las posibles causas y sus efectos.

6. Elaboración de la matriz de probabilidad e impacto, que permite identificar los riesgos altos que necesitan mitigarse de manera urgente mediante un plan correctivo.

7. Elaboración del modelo de madurez en el cual se encuentra el sistema auditado.

8. Elaboración del informe final.

Etapa 4. Presentación del informe final: En esta etapa se realiza un informe que contiene todos los procesos evaluados con la respectiva descripción de su comportamiento dentro de la empresa. Tal comportamiento puede ser bueno o malo, y en caso de ser malo se dan a conocer los hallazgos encontrados junto con algunas recomendaciones que permitirán mitigarlos.

Este informe se presenta ante el personal encargado de la seguridad del sistema de información en el Hospital, para que tome las medidas pertinentes.

3. DESARROLLO DEL TRABAJO

3.1 ARCHIVO PERMANENTE

3.1.1 Diseño organizacional del Hospital Universitario Departamental de Nariño

3.1.1.1 Reseña histórica. En el mes de marzo de 1967, el Presidente de la República Dr. Carlos Lleras Restrepo, visita la ciudad de Pasto y es enterado de las precarias condiciones funcionales del entonces Hospital Civil de Pasto, y se compromete a facilitar las gestiones conducentes a la creación del Hospital Departamental de Nariño. En el mes de enero de 1970, se inicia el proceso de construcción y el 15 de diciembre de 1975, se da inicio a la prestación de servicios de salud, con la inauguración del servicio de consulta externa. En 1977, se da apertura a los servicios de hospitalización, con las especialidades básicas de medicina interna, cirugía, gineco - obstetricia, y pediatría; y además se ponen en servicio las unidades de apoyo de radiología, laboratorio clínico, patología, rehabilitación, farmacia y nutrición. En 1976, el Hospital se convierte en la sede de la Regional Central No 1 y se coloca bajo su cuidado al Hospital Infantil Los Ángeles y a 18 organismos más de salud de baja complejidad. En el año de 1987, el gobierno de Japón se vincula a la región y al Hospital a través de un proyecto de cooperación internacional, realizando una importante donación de equipos médicos que colocaron al Hospital en ésa época, a la vanguardia de la tecnología biomédica.

Posteriormente, en octubre de 1990, el Hospital 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, con patrimonio propio y autonomía administrativa, según la Ley 100 de 1993. Conforme a esta norma y en concordancia con el Plan Nacional de Desarrollo, el Hospital se ve obligado a mantener su autosostenibilidad financiera, implementando procesos eficientes que le permiten ser competitivo en el mercado del área de influencia, proyectándose con los avances de la ciencia, la tecnología y la gerencia moderna a la comunidad del sur occidente del país.

En el año 2004, la honorable Asamblea del Departamento, modifica los estatutos de la E. S. E y establece una nueva estructura orgánica, y lo transforma en un Hospital de carácter universitario.

Sin lugar a dudas, el proceso de desarrollo que ha venido presentando el Hospital, se ha convertido en una de las obras más significativas para el departamento de Nariño. A finales del año 2003 y por meritocracia, llega a la gerencia el Doctor Bernardo Ocampo Martínez, quien propone en la organización un modelo de gestión integral por calidad, que lleva al Hospital Universitario Departamental de Nariño a su modernización, a la creación de un cultura de calidad corporativa y al cumplimiento de sus objetivos sociales, en un entorno complejo como lo es el Sistema de Seguridad Social en Salud de Colombia. Este modelo de gestión integral por calidad, es una forma de pensamiento gerencial estructurado, que tiene como propósito, que una organización se desarrolle integral y armónicamente, entendiendo por ello, que logre el mayor beneficio y satisfacción para sus usuarios, clientes, empleados, dueños o dolientes y para la sociedad en general.

Durante el período 2003 - 2011, la aplicación del modelo de gestión integral por calidad ha proporcionado cambios significativos, que han asegurado la sostenibilidad de la organización en el tiempo puesto que:

- El presupuesto de la organización desde el año 2003 se ha ido incrementando progresivamente, desde la suma de 23 mil millones de pesos hasta la suma de 89 mil millones proyectados para 2012, proveniente de recursos propios del Hospital, con los cuales se financian los planes de desarrollo de la organización.

- Se ha invertido más de 50 mil millones de pesos en infraestructura durante el período, procedentes de recursos propios del Hospital. Es así como se ha hecho posible la remodelación total del edificio antiguo (12.000.Mt^2) y del servicio de consulta externa (4.000Mt^2), además de la construcción de 8.316 Mt^2 en un nuevo y moderno edificio.

- Se ha invertido más de 20 mil millones en adquisición de tecnología general y biomédica.

- Las ventas durante los últimos 9 años se han incrementado en promedio en un 11.4% anual, pasando de $ 26.833 millones en el año 2003 a $ 76.500 millones en el año 2011.

- Durante los últimos 9 años, el Hospital ha demostrado un crecimiento del 62% anual con inversiones en propiedades, planta y equipo.

- El gasto social, que son los recursos donados por el Hospital al estado colombiano por concepto de atención a la población pobre y vulnerable del departamento de Nariño, ha sido aproximadamente de 24 mil millones de pesos en el período.

➢ Se tiene un complemento armónico de la Red de Prestadores de Servicios de Salud del departamento de Nariño, al ser la Institución de máxima complejidad en la región.

➢ Existe transparencia y democracia en la administración pública y un eficiente manejo de los recursos públicos.

➢ Se ha garantizado la salud y la seguridad para los trabajadores gracias a que:

✓ La implementación de nuevas tecnologías en bioseguridad ha permitido reducir los accidentes ocupacionales principalmente por riesgo biológico, pasando del 6,4% en 2003 al 1,7% en 2011.

✓ El Hospital ofrece estabilidad laboral y oportunidades de crecimiento y desarrollo a sus colaboradores, reflejadas en el bajo índice de rotación que equivale a 2,69% en promedio durante este periodo.

✓ El mejoramiento del clima organizacional es una muestra más del fortalecimiento del sentido de pertenencia, liderazgo y reconocimiento del logro en sus colaboradores. El clima organizacional pasó de 1,97% en el año 2003 a 4,02 en el año 2011. (Calificación sobre 5).

Actualmente, la gerencia y representación legal del Hospital se encuentra en manos del Doctor Wilson Larraniaga López.

3.1.1.2 Premios y reconocimientos. En el año 2006, se publica el ranking de instituciones prestadoras de servicios de salud realizado por el Ministerio de la Protección Social y la Universidad Nacional de Colombia, en el cual, el Hospital Universitario Departamental de Nariño es clasificado como el primero a nivel nacional en la categoría de mediana complejidad. Simultáneamente la Presidencia de la República a través del Departamento Administrativo de la Función Pública, considera que en el Hospital existe una experiencia exitosa de gestión y recomienda la inscripción en el banco de éxitos de la función pública la experiencia del Hospital: “El direccionamiento estratégico con enfoque prospectivo para el éxito y la competitividad en las Empresas Sociales del Estado”; y posteriormente en el año 2007 nuevamente se reconoce e inscribe como un proyecto exitoso para el banco de éxitos la experiencia “El programa de administración de seguridad integral hospitalaria, una responsabilidad institucional por la seguridad de nuestros grupos de interés”.

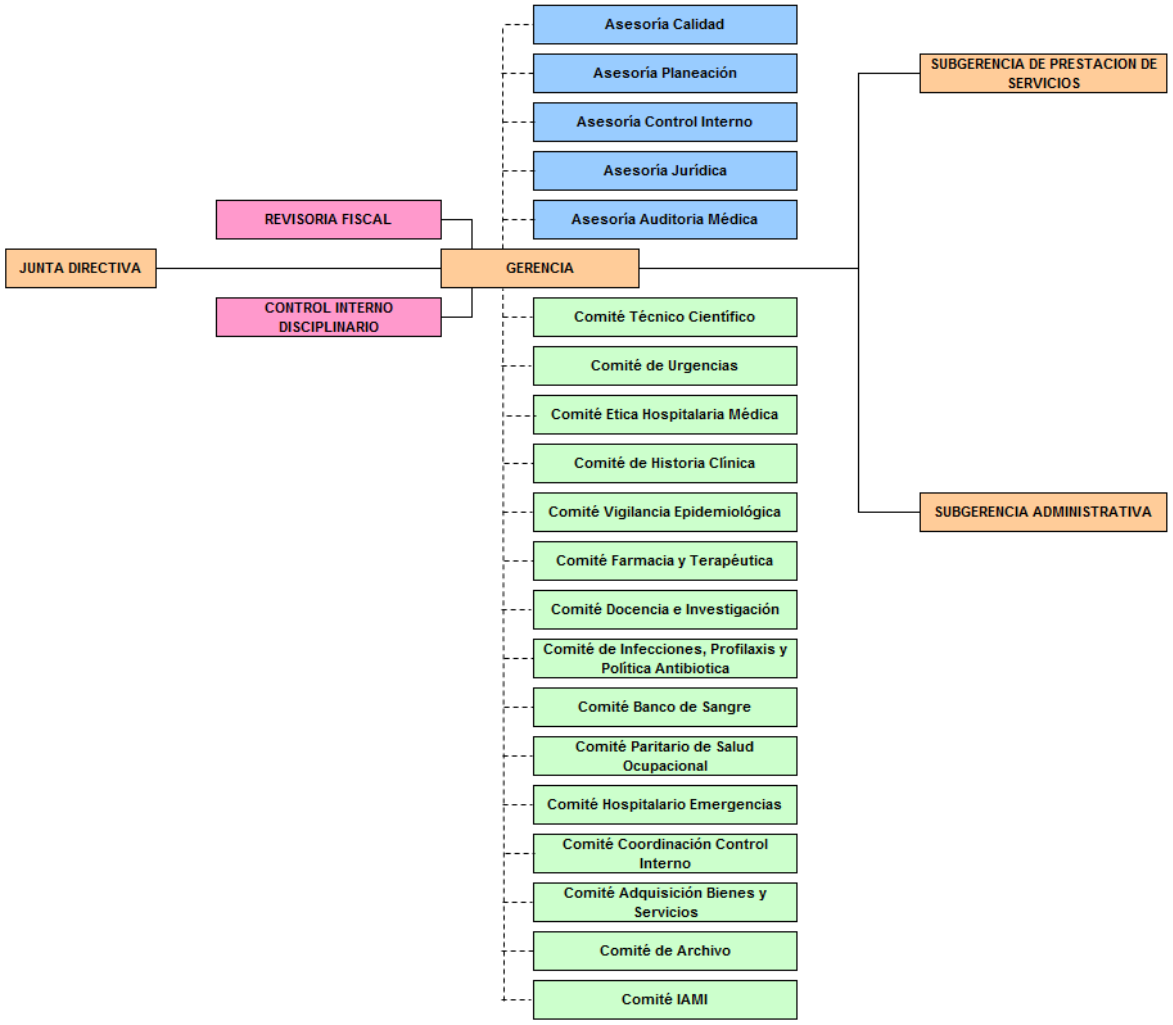
En el año 2007 el Hospital es finalista del premio nacional “Lideres en Acción” en el concurso organizado por la Administradora de Riesgos Profesionales ARP

Colmena; igual mención obtiene en el año 2008 al participar en el Premio “Calidad en Salud Colombia” organizado por el Centro de Gestión Hospitalaria. Pero es, sin lugar a dudas, el año 2010 el de mayores reconocimientos pues se recogen los frutos de años de arduo y acertado trabajo de desarrollo empresarial encaminado al fortalecimiento de una cultura de calidad; es el año donde el lema “Un Hospital seguro para una atención segura” recibe mención de honor en el premio “Galardón Hospital Seguro” organizado por la Asociación Colombiana de Hospitales y Clínicas ACHC y obtiene el premio “Calidad en Salud Colombia, en la categoría “Bronce”, así mismo el organismo acreditador en salud ICONTEC le otorga el certificado de Institución Acreditada en Salud, máximo reconocimiento para las Instituciones Prestadoras de Servicios de Salud Colombianas. Y cierra este exitoso capítulo de la historia, la acreditación como Institución Amiga de la Mujer y de la Infancia IAMI, otorgada por parte del Instituto Departamental de Salud de Nariño IDSN y la UNICEF. En el año 2011 se renueva el certificado de acreditación del Hospital, puesto que se da reconocimiento al Sistema Único de Acreditación por parte de la Sociedad Internacional para la Calidad en Atención de la Salud (ISQUA), incluyendo al logo símbolo creado por el Ministerio de Salud.

En el año 2012, recibe nuevamente la mención de honor en el premio “Galardón Hospital Seguro”, por parte de la Asociación Colombiana de Hospitales y Clínicas ACHC, lo que demuestra el interés por mantener la mejora y el cumplimiento de altos estándares de calidad que lo posicionan como la institución única del municipio de San Juan de Pasto en haber alcanzado tales reconocimientos.

3.1.1.3 Estructura organizacional. El Hospital Universitario Departamental de Nariño E.S.E., cuenta con una estructura organizacional diseñada para facilitar la integración entre los procesos administrativos, asistenciales y de apoyo a través de dos subgerencias, tal como se indica en la siguiente gráfica:

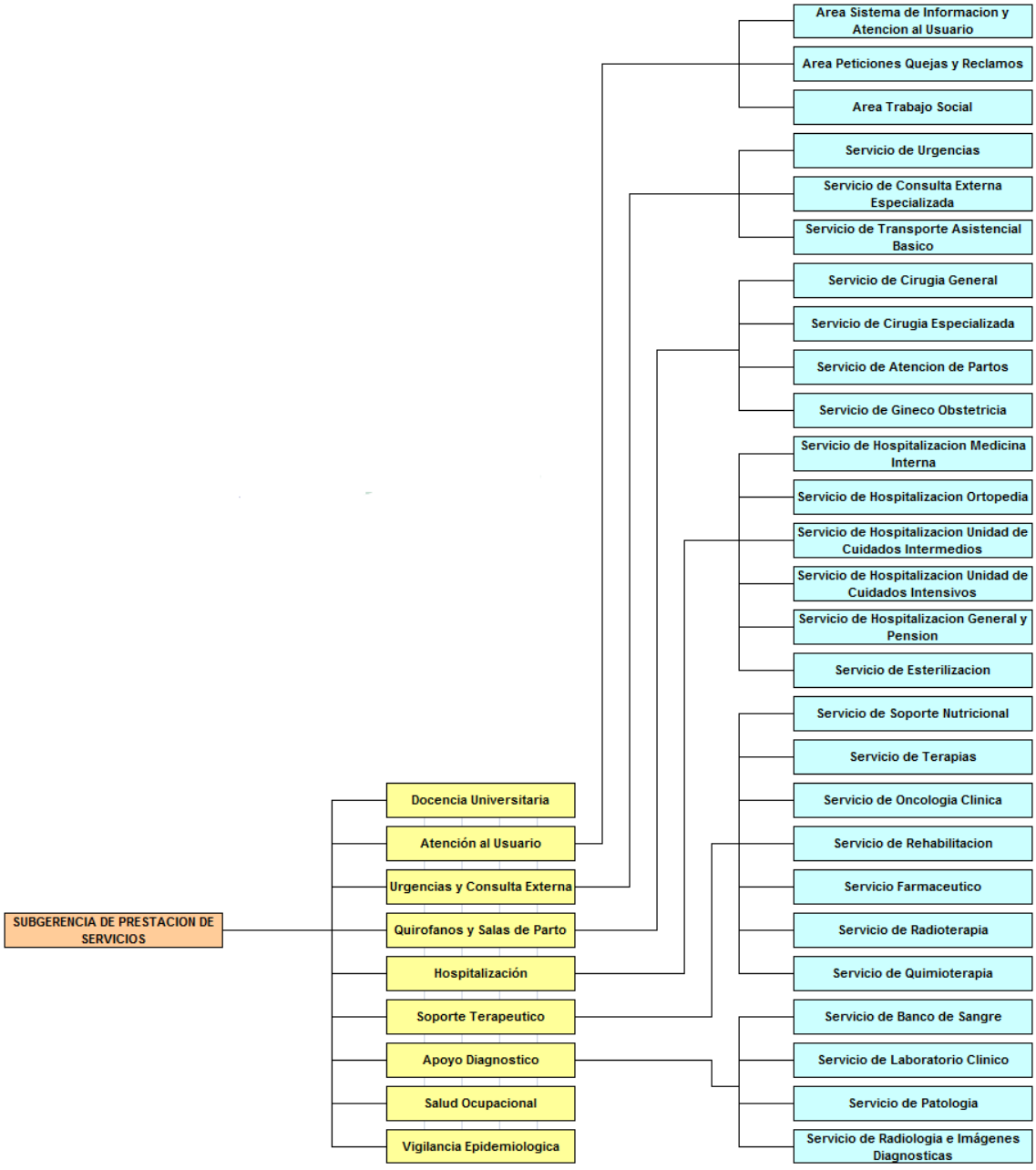
Figura 3. Organigrama HUDN



Fuente: Hospital Universitario Departamental de Nariño E. S. E.

Dentro de la subgerencia de prestación de servicios, la cual está a cargo del Doctor Eduardo Burbano, se tienen las siguientes áreas:

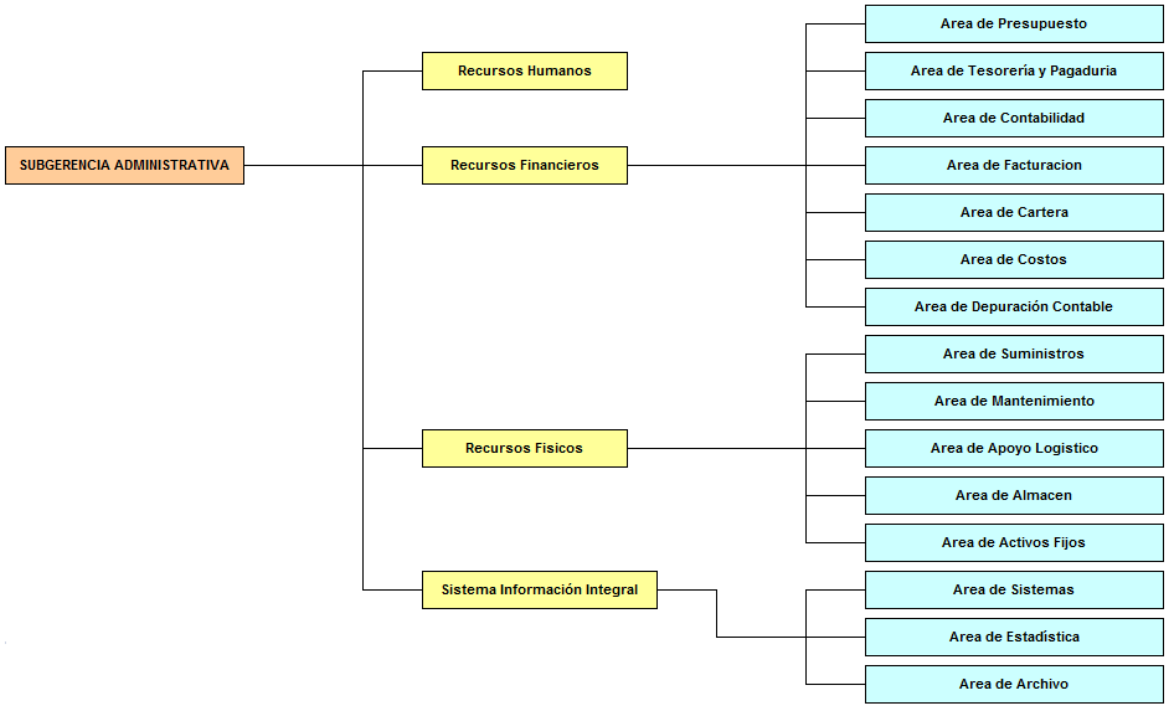
Figura 4. Subgerencia de prestación de servicios HUDN



Fuente: Hospital Universitario Departamental de Nariño E. S. E.

Y dentro de la subgerencia administrativa se puede encontrar las áreas de:

Figura 5. Subgerencia administrativa HUDN



Fuente: Hospital Universitario Departamental de Nariño E. S. E.

Cada dependencia cuenta con un equipo humano cálido, amable, calificado y dispuesto a satisfacer las necesidades de los usuarios, clientes internos, proveedores y la comunidad en general, logrando impactar favorablemente en la salud de los nariñenses.

3.1.1.4 Recursos humanos. El recurso humano del hospital está integrado por funcionarios de planta y de contrato. En esto, hacen parte las empresas: Servicios Multiactivos de Colombia S.A.S, Biolectomedical Service, Compañía de Vigilancia Santafereña, Servivarios la Mejor y Uniservice.

Las siguientes tablas indican la distribución de funcionarios por profesión y el total de empleados:

Tabla 3. Total funcionarios por profesión

DETALLE	TOTAL 2010	TOTAL 2011	TOTAL 2012
Médicos Generales de Planta (4 Horas)	1	1	1
Médicos Generales de Contrato(4 Horas)	0	0	0
Total Médicos Generales (4 Horas)	1	1	1
Médicos Generales de Planta (8 Horas)	13	13	13
Médicos Generales de Contrato(8 Horas)	38	47	54
Total Médicos Generales de Ocho Horas	51	60	67
Médicos Especialistas de Planta(4 Horas)	17	17	20
Médicos Especialistas de Contrato(4 Horas)	19	10	13
Total Médicos Especialistas (4 Horas)	36	27	33
Médicos Especialistas de Planta(8 Horas)	44	44	72
Médicos Especialistas de Contrato(8 Horas)	19	10	13
Total Médicos Especialistas(8 Horas)	63	54	85
Odontólogos Especialistas de Planta	1	1	1
Odontólogos Especialistas de Contrato(MAXILO-FACIAL)	1	1	2
Total Especialistas Odontólogos	2	2	3
Enfermeras de Planta	27	27	28
Enfermeras de Contrato	26	38	39
Total Enfermeras	53	65	67
Auxiliares Área Salud de Planta	104	101	110
Auxiliares Área Salud Contrato	139	158	189
Total Auxiliares Área Salud	243	259	299
Bacteriólogos Planta	6	6	6
Bacteriólogos Contrato	14	11	12
Total Bacteriólogos	20	17	18
Terapistas Planta	5	5	10
Terapistas Contrato	19	23	21
Total Terapistas	24	28	31
Auxiliares Área Laboratorio Planta	3	3	4
Auxiliares Área Laboratorio Contrato	16	15	16
Total Auxiliares Área Laboratorio	19	18	20
Técnicos Área Salud de Planta	3	3	3
Técnicos Área Salud Contrato	7	9	9
Total Técnicos Área Salud	10	12	12
Químicos Farmacéuticos de Planta	0	0	0
Químicos Farmacéuticos de Contrato	1	2	3
Total Químicos Farmacéuticos	1	2	3
Profesional Especializado Área Salud Planta	0	0	9
Total Especializado Área Salud	0	0	9

Fuente: Plan de desarrollo HUDN 2012 – 2016

Tabla 4. Total personal HUDN

DETALLE	2010	2011	2012
Total Personal Asistencial Planta	221	221	257
Total Personal Asistencial Contrato	280	314	358
Total Personal Asistencial	501	535	615
Total Personal Administrativo Planta	83	83	92
Total Personal Administrativo Contrato	154	177	192
Total Personal Administrativo	237	260	257
Total Personal HUDN	738	795	872

Fuente: Plan de desarrollo HUDN 2012 – 2016

Del total del personal de la organización el 32% corresponde a personal administrativo y el personal asistencial es del 68%. El personal asistencial de contrato que presta sus servicios en la organización corresponde al 58%, mientras que el personal de planta es del 42%. Las labores administrativas están distribuidas así: el 68% con personal de contrato y 32% con funcionarios de planta.

3.1.1.5 Recursos informáticos. El hospital cuenta con un total de 376 equipos de cómputo, distribuidos de la siguiente forma:

Tabla 5. Inventario de equipos de cómputo HUDN

Piso	Área	Cantidad de equipos
5	PENSION EST. ENFER	8
	PENSION SEC. CLINICA	1
	FACTURACION	2
	CANAL INSTITUCIONAL	1
4	M. I. EST. ENFERMER	8
	M. I. SEC. CLINICA	1
	ORTOPEDIA EST. ENF	7
	FACTURACION	2
	COOR. HOSPITALIZAC.	1

Tabla 5. (Continuación)

Piso	Área	Cantidad de equipos
4	SEC. COOR. HOSPTAL.	1
	COOR. EPIDEMIOLOGIA	1
	PLANEACION	1
	TERAP. RESPIRATORIA	1
	SISTEMAS COOR.	1
	SISTEMAS	13
	SISTEMAS A. CAPACIT	12
	OFICINA SINDICATO	1
3	GINECO EST. ENFERM.	11
	UCI BASICO	6
	UCI NEONATOS	8
	UCI NEONATOS SECR.	1
	SALA PARTOS	5
	VACUNACION	1
	IAMI	1
	FACTURACION	3
2	QUIRURG. EST. ENFER	7
	QUIRURG. SEC. CLINICA	1
	OFICINA CIRUGIA	1
	FACTURACION	2
	CONSULTA EXTERNA FAC	1
	CON. EXT. CONSULTORIOS	13
	AUDITORIA MEDICA	8
1	URG. EST. ENFERM	12
	URG. CONSULTORIOS	6
	URG. CONT. TRIAGE	1
	URG. FAC CONTRIB.	2
	URG. ADMISIONES	4
	URG. COOR.	1

Tabla 5. (Continuación)

Piso	Área	Cantidad de equipos
1	GERENCIA	1
	URG. CENT.MONIT.UCS	1
	SECRETARIA GERENCIA	1
	SALA DE JUNTAS GERENCIA	1
	SUB GERENCIA PRE. SERVICIO	2
	SUB GERENCIA ADM. Y FIN.	3
	JURIDICA	4
	COORD. REC. HUMANOS	1
	SECRETARIA DE REC. HUMANOS	1
	RECUSOS HUMANOS	5
	COORD FINANZAS	1
	FINANZAS	14
	CENTRAL TELEFONICA	1
	COORD. DE APOYO LOGISTICO	1
	AUDITORIA DE CUENTAS	9
	PATOLOGIA	2
	CONTROL INTERNO	2
	MATENIMIENTO	9
	CONTROL INT. DISCIPLINARIO	1
	ONCOLOGIA	4
	COORD. DE SOP. TEOTERAPIA	1
	ONCOLOGIA SALA DE JUNTAS	1
	ACTIVOS FIJOS	1
	SALUD OCUPACIONAL	2
	CONSULTA EXTERNA	2
	CONSULTA EXTERNA FAC	2
	CONSULTA EXTERNA TRA. SO.	1
	CALL CENTER	2
	CON. EXT. CONSULTORIOS	11

Tabla 5. (Continuación)

Piso	Área	Cantidad de equipos
1	REHABILIACION	8
	ATENCION AL USUARIO	5
	FACTURACION CENTRAL	6
	ARCHIVO	7
	FARMACIA BODEGA	2
	FARMACIA	12
	RAYOS X	3
	RAYOS X IMG.DIAGNO.	1
	RAYOS X ECOGRAFO O	1
	SALA DE LECTURA RX	2
	SERVIDOR RX	2
	RECEPCION RX	1
	LABORATORIO COOR.	1
	LABORATORIO QUIMIK.	1
	LABORATORIO	1
	LABORATORIO FACT.	2
	SISTEMAS SERVIDOR.	7
	AUDITORIO	1
	ARCHIVO CENTRAL	6
	ALMACEN	2
	BIO	1
	NUTRICION	1
	CALIDAD	1
	COORDINACION UNIVERSITARIA	2
	EMERGENCIAS	1
Unidad Complementaria de Servicios		
Piso	**Área**	**Cantidad de equipos**
5	AUDITORIO UCS	3
	PENSION UCS	4

Tabla 5. (Continuación)

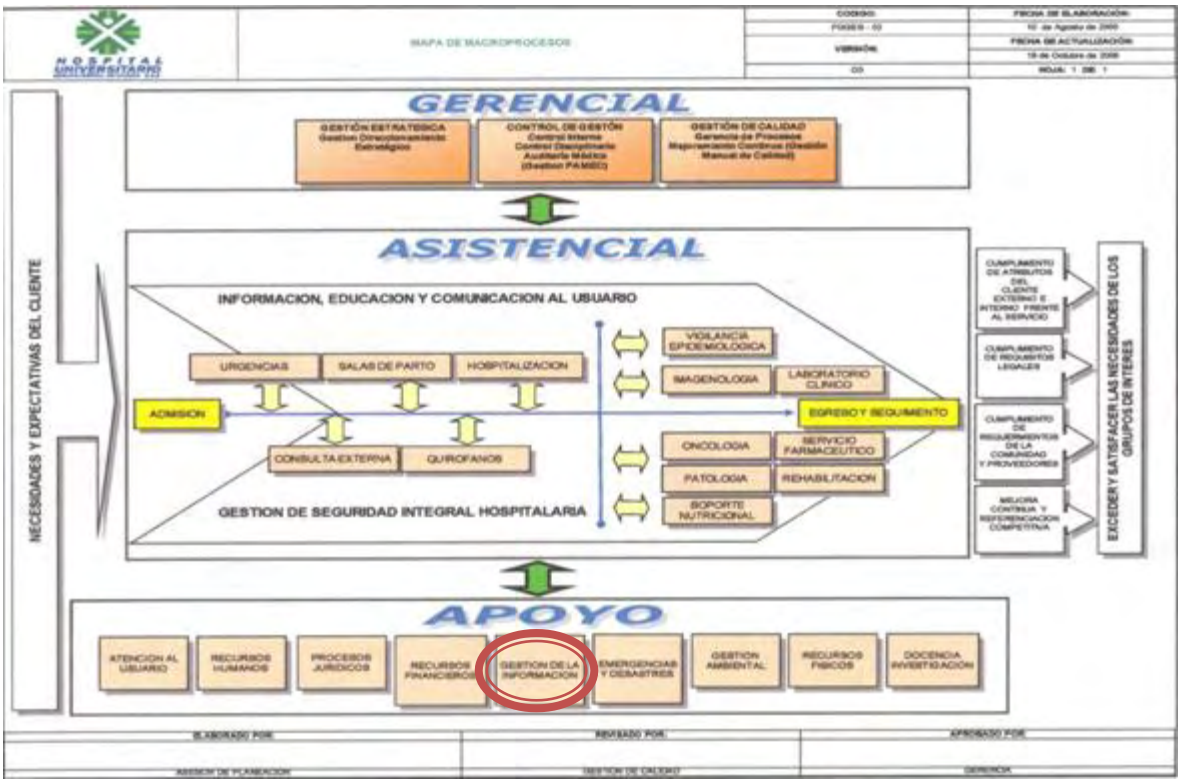
Unidad Complementaria de Servicios		
Piso	**Área**	**Cantidad de equipos**
4	CONTRIB. UCS	8
	CONTRIB. UCS SEC. CLI	1
	CONTRIB. UCS FACT	1
3	UCI UCS	11
	UCI UCS FARMACIA	1
	UCI UCS SEC. CLINICA	1
	UCI-UCS-FACTURACION	1
2	QX EST. ENFERM. UCS	7
	QX ESTAR MEDIC. UCS	1
	QX SALAS UCS	9
	QX CIR. AMBULATORIA	1
	QX URPA UCS	3
	QX FARMAC. UCS	1
	QX FACTURACION UCS	1
	QX COOR. UCS	1

Fuente: Hospital Universitario Departamental de Nariño E. S. E.

Del total de equipos, el 59% tiene instalado el sistema operativo Windows XP mientras que el 38% utiliza Windows 7. Asimismo, el 2% cuenta con Windows Server 2003 y el 1% emplea Windows Vista. Para más información al respecto, consultar el anexo B que se adjunta en formato digital.

3.1.2 Área de información y sistemas. A continuación, se muestra el mapa de macroprocesos existentes en el Hospital, el cual permite identificar el conjunto de acciones coordinadas que la entidad realiza, a fin de cumplir con cada competencia particular asignada, con la misión fijada y con la visión trazada.

Figura 6. Mapa de macroprocesos HUDN



Fuente: Hospital Universitario Departamental de Nariño E. S. E.

Como se puede observar, los macroprocesos de la organización se encuentran agrupados en tres tipos:

Macroprocesos gerenciales: son procesos destinados a definir y controlar las metas de la organización, sus políticas y estrategias, por ello son liderados por la alta dirección. Además proporcionan directrices a los demás macroprocesos, es decir, indican cómo se deben realizar para que se pueda lograr la visión de la empresa.

Macroprocesos asistenciales: son los procesos que tienen contacto directo con el cliente (procesos operativos necesarios para la realización del servicio, a partir de los cuales el cliente percibirá y valorará la calidad en cuanto a planificación del servicio y prestación del mismo).

Macroprocesos de apoyo: son los procesos responsables de proveer a la organización de todos los recursos necesarios en cuanto a personas, maquinaria y materia prima, para poder desarrollar los macroprocesos anteriores.

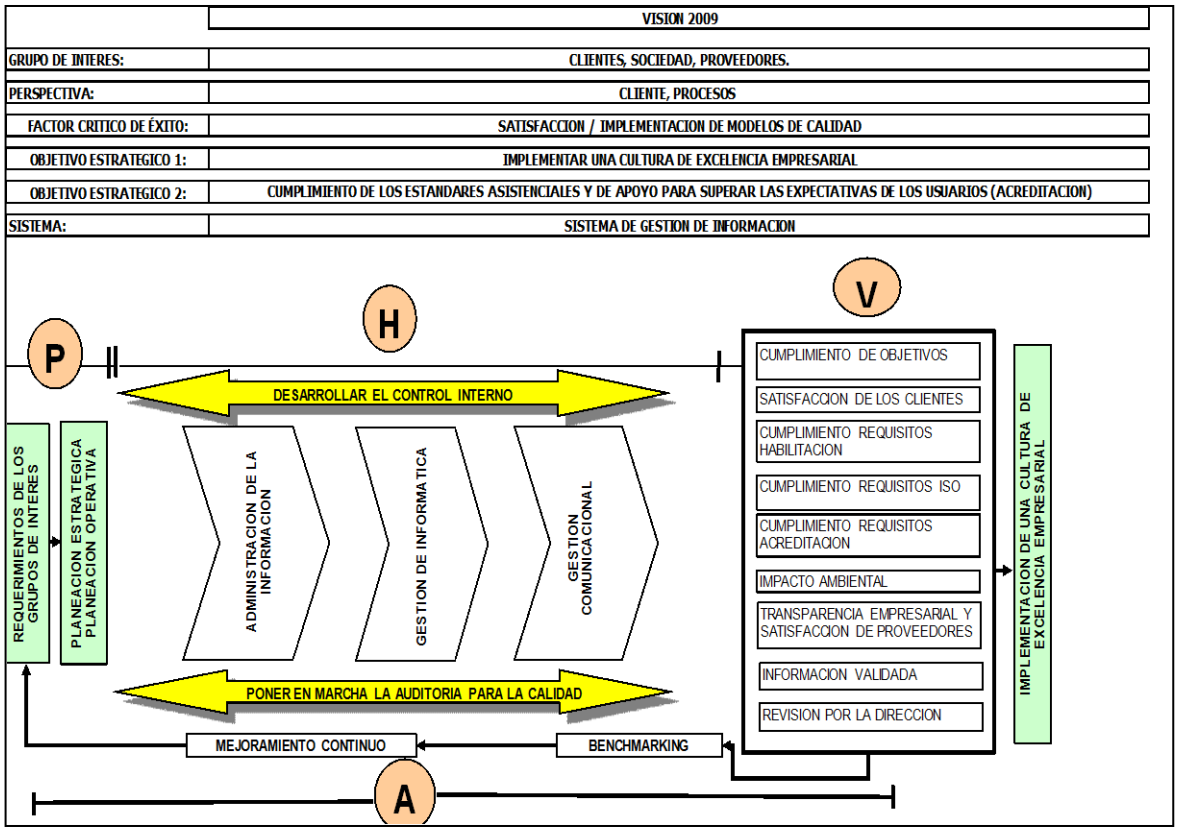
Dentro de los macroprocesos de apoyo existe un proceso llamado gestión de la información, el cual está conformado por las siguientes unidades funcionales:

Figura 7. Organización del área de gestión de información

Fuente: Hospital Universitario Departamental de Nariño E. S. E.

Ahora bien, el área de información y sistemas maneja un sistema de gestión de información compuesto por tres componentes: administración de la información, gestión informática y gestión comunicacional (ver Figura 8).

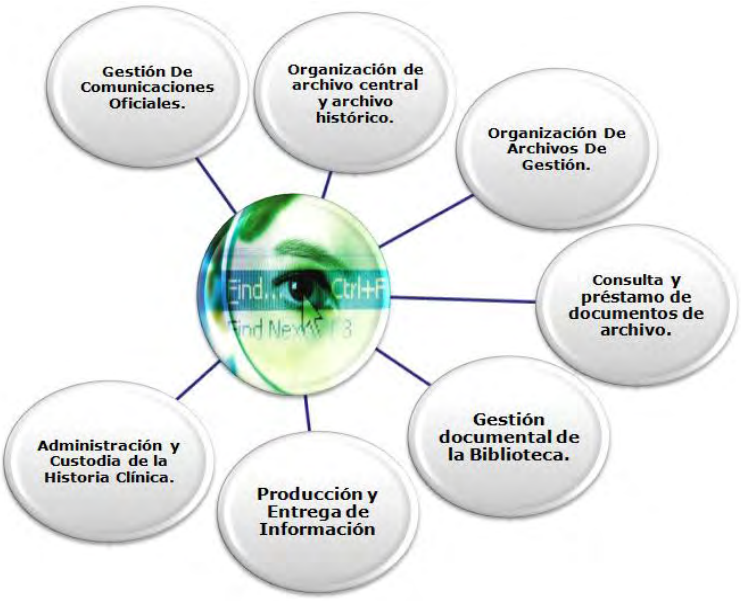
Figura 8. Componentes del área de gestión de información



Fuente: Hospital Universitario Departamental de Nariño E. S. E.

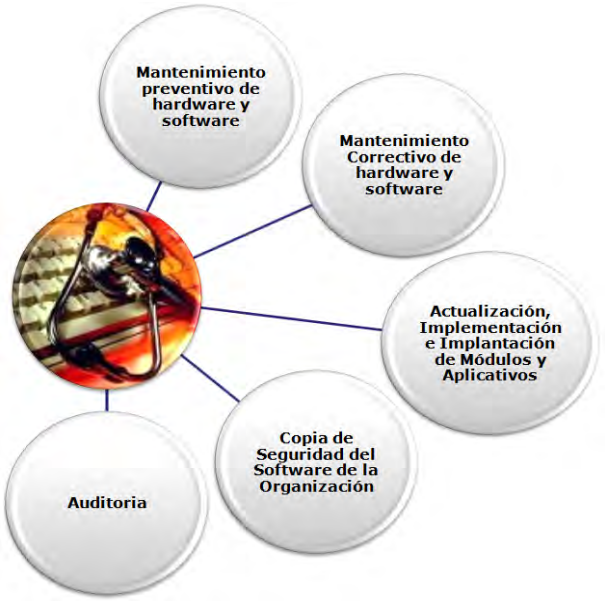
Cada uno de los componentes contiene, a su vez, varios subprocesos tal como se indica en las siguientes figuras:

Figura 9. Subprocesos de administración de la información



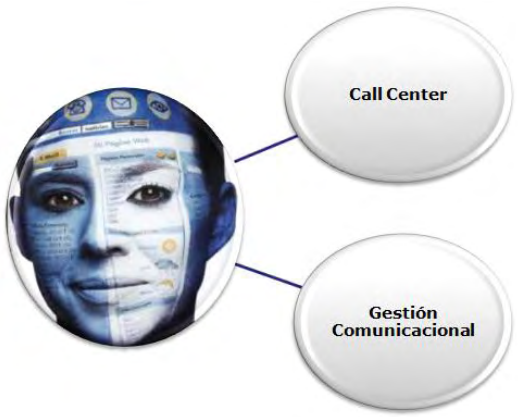
Fuente: Hospital Universitario Departamental de Nariño E. S. E.

Figura 10. Subprocesos de gestión informática



Fuente: Hospital Universitario Departamental de Nariño E. S. E.

Figura 11. Subprocesos de gestión comunicacional



Fuente: Hospital Universitario Departamental de Nariño E. S. E.

3.1.2.1 Misión del área de información y sistemas. El sistema de gestión de información del Hospital Universitario Departamental de Nariño E. S. E., busca satisfacer las necesidades y expectativas de los grupos de interés de la organización con criterios de calidad, eficiencia, seguridad y confidencialidad bajo la normatividad vigente, mediante el buen uso y correcta articulación de: la tecnología, la administración y la comunicación de la información; soportando así la toma de decisiones a los procesos gerenciales, misionales y de apoyo.

3.1.2.2 Cargos y funciones dentro del área de información y sistemas

I.- IDENTIFICACIÓN

NIVEL: PROFESIONAL
DENOMINACIÓN DEL EMPLEO: PROFESIONAL ESPECIALIZADO
CÓDIGO: 222
GRADO: 7
NÚMERO DE CARGOS: 1
DEPENDENCIA: ÁREA SISTEMAS DE INFORMACIÓN
CARGO DEL JEFE INMEDIATO: SUBGERENTE ADMINISTRATIVO Y FINANCIERO

II.- PROPÓSITO PRINCIPAL: El Hospital Universitario Departamental de Nariño, Empresa Social del Estado, dirigirá sus esfuerzos al mejoramiento continuo y se

convertirá en una institución centrada en el usuario. Para alcanzar tales fines implementará un modelo de gestión integral por calidad. Será función esencial de los coordinadores de los grupos de trabajo, desplegar el modelo, las políticas, los objetivos, de la alta dirección, a todos los niveles de su grupo de trabajo, traducirlos a planes operativos, aplicando sistemáticamente el ciclo PHVA.

III.- DESCRIPCIÓN DE FUNCIONES ESENCIALES:

1. Participar activamente en el proceso de direccionamiento estratégico de la organización.
2. Identificar de manera documentada, a los clientes y proveedores internos y externos.
3. Elaborar y documentar el proceso que identifique las necesidades y expectativas de sus clientes, así como el proceso para responder a dichas necesidades.
4. Elaborar y documentar el proceso sistemático para definir y replantear los grandes propósitos institucionales de acuerdo a los cambios del entorno.
5. Participar activamente en la formulación del plan estratégico de la institución.
6. Elaboración en base a políticas y directrices del plan operativo anual de su grupo. dicho plan debe poseer los objetivos y metas en términos medibles, en concordancia con los objetivos estratégicos de la institución.
7. Elaborar el cuadro de indicadores claves, que permitan monitorizar las metas y objetivos propuestos.
8. Presentar mensualmente el informe de su gestión, que incluya cuantitativamente, la gestión realizada.
9. Análisis, evaluación y estandarización del proceso de apoyo de atención al usuario.
10. Construcción de indicadores, evaluación y ciclo de mejora del proceso de apoyo de atención al usuario.
11. Dentro del concepto de gerencia ínter funcional, participar activamente, en el proceso asistencial del sistema único de acreditación y los demás estándares de apoyo del sistema de acreditación.
12. Participar en la elaboración y divulgación de la declaración de los deberes y derechos de los pacientes.
13. Participar en el diseño de las herramientas de seguimiento y evaluación de la aplicación de la declaración de los deberes y derechos de los pacientes por parte del personal a su cargo.
14. Participar o liderar, de acuerdo a su competencia, en el diseño, documentación, prueba, validación, ajuste, socialización e implementación de todos los procesos de los estándares de acreditación de atención al cliente asistencial que se desarrollan en el área o en los cuales ésta interviene.

15. Participar o liderar, de acuerdo a su competencia, en el diseño, documentación, prueba, validación, ajuste, socialización e implementación de todos los procesos de los estándares de acreditación de gerencia que se desarrollan en el área o en los cuales ésta interviene.
16. Elaborar, implementar y evaluar el plan de acción para la monitorización y mejoramiento de la calidad.
17. Participar o liderar, de acuerdo a su competencia, en el diseño, documentación, prueba, validación, ajuste, socialización e implementación de todos los procesos de los estándares de acreditación de gerencia de recursos humanos que se desarrollan en el área o en los cuales ésta interviene.
18. Evaluar el desempeño de todo el personal adscrito a la sección de información y sistemas en coordinación con la oficina de recursos humanos.
19. Apoyar los procesos y programas de la salud ocupacional y seguridad industrial institucional que le competan.
20. Apoyar la evaluación de la satisfacción de los empleados adscritos a su área, que adelante la oficina de recursos humanos.
21. Velar porque en su área los resultados de las actividades del mejoramiento de la calidad sean comunicados.
22. Apoyar la aplicación en su área de los procesos que garanticen el manejo seguro del espacio físico, equipos médicos e insumos, tanto para los trabajadores como para los clientes durante su proceso de atención; y de los procesos para el manejo seguro de desechos.
23. Conocer y cumplir con las actividades que le competa de acuerdo con el plan de emergencias y desastres; y de prevención y respuesta a incendios.
24. Participar en el diseño, documentación, prueba, validación, ajustes, socialización e implementación del plan para mejorar la calidad de los procesos de la gerencia del ambiente físico de su área.
25. Adelantar las acciones que le competan en el diseño e implementación de actividades de mejoramiento dentro de las prioridades seleccionadas en el respectivo plan.
26. Velar porque los resultados de las actividades del mejoramiento de la calidad sean comunicados.
27. Liderar el diseño, documentación, prueba, validación, ajuste, socialización e implementación de todos los procesos de los estándares de acreditación de gerencia de la información que se desarrollan en el área o en los cuales ésta interviene.
28. Identificar las necesidades de información al interior de su área, en especial de aquellas necesidades directamente relacionadas con el proceso de atención a un cliente.
29. Participar en las investigaciones que se realicen cuando el análisis periódico de la información detecte variaciones no esperadas en el desempeño de los procesos o equipos, y en la definición de acciones preventivas y correctivas.

30. Identificar las necesidades de información al interior de cada una de las unidades funcionales, en especial de aquellas necesidades directamente relacionadas con el proceso de atención a un cliente. y en los clientes externos e internos de la institución.
31. Realizar una investigación exhaustiva cuando el análisis periódico de la información detecta variaciones no esperadas en el desempeño de los procesos o equipos, generando acciones preventivas y correctivas.
32. Realizar y controlar procesos para garantizar la seguridad y confidencialidad de la información.
33. Administrar los datos y la información tanto administrativa como asistencial.
34. Consolidar la información asistencial y administrativa.
35. Mejorar la calidad de los procesos de la gerencia de información.
36. Coordinación y administración de la sección de información y sistemas.
37. Administración del sistema de información dinámica gerencial hospitalaria en todos los módulos administrativos y asistenciales.
38. Administración de la red de datos, red eléctrica regulada.
39. Mantenimiento detectivo, preventivo y correctivo del software y hardware (equipos de cómputo).
40. Soporte en cada una de las áreas que manejan el sistema de información.
41. Administración del canal dedicado y del portal empresarial de la institución.
42. Elaborar el plan operativo anual del área.
43. Capacitar en informática, leyes y normatividad vigente.
44. Planear el número y clase de personal que la sección requiera.
45. Orientar a los funcionarios nuevos en sus labores, en la organización del hospital, en sus relaciones con otras áreas y en la confidencialidad de la historia clínica.
46. Dirigir las reuniones del personal para discusión de las actividades, explicaciones de nuevos principios e instrucción sobre nuevos procedimientos.
47. Seleccionar y gestionar equipos y materiales.
48. Colaborar con los diferentes comités en la preparación de los temarios de reuniones, cuando éstos lo soliciten.
49. Colaboración en el establecimiento de normas con respecto al contenido de la historia clínica completa.
50. Establecer con el nivel directivo, jefes de unidades y secciones, las necesidades de información médica y administrativa.
51. Desarrollar procedimientos para establecer el curso que deben seguir los documentos hasta llegar a la historia clínica.
52. Determinar con el personal médico las normas que rijan el registro de diagnóstico exacto y completo.
53. Colaborar en el establecimiento de normas con respecto al contenido de las historias clínicas completas.
54. Desarrollar procedimientos para establecer el curso que deben seguir los documentos hasta llegar a la historia clínica.

55. Determinar con el personal médico las normas que rijan el registro de diagnósticos definitivos exactos y completos.
56. Establecer el tipo de informes periódicos, contenido, indicadores, etc., que permitan satisfacer sus necesidades.
57. Desarrollar instrumentos que permitan la recolección de los datos en las distintas unidades y secciones.
58. Planear y desarrollar métodos sistematizados que permitan guardar oportunamente la información.
59. Planear el sistema de archivo de historias clínicas de tal manera que satisfaga las necesidades del hospital.
60. Recomendar el método más conveniente para la conservación de las historias clínicas, así como la conveniencia de la destrucción de algunas de ellas.
61. Controlar el cumplimiento de las normas para la producción de información, indicadores, plazos, etc.
62. Velar por el buen manejo de la historia clínica de acuerdo a las normas vigentes.
63. Velar por el buen uso de los equipos y materiales de la sección.
64. Organizar y mantener actualizada la sección de información de acuerdo al marco legal vigente de tal manera que sea capaz de presentar respuestas no sólo a las necesidades de información para la atención del paciente, si no para la dinámica de los procesos de decisión y acciones administrativos y científicos.
65. Identificar y definir el tipo de información a captarse, los indicadores mínimos necesarios, los flujos entre los diversos componentes del sistema de información para apoyar los procesos de evaluación, programación e investigación.
66. Analizar periódicamente el funcionamiento del sistema de información del hospital, efectuando las modificaciones necesarias para adaptarlo a los requerimientos y cambios que imponga la normatividad del sistema de seguridad social en salud.
67. Presentar informes estadísticos que sean requeridos por gerencia, subgerencias, jefes de sección y autoridades competentes.
68. Colaborar en el establecimiento de parámetros para el desarrollo, revisión y evaluación técnica de las historias clínicas estableciendo parámetros con respecto a su contenido.
69. Levantar procedimientos para establecer el curso que deben seguir los documentos hasta llegar a la historia clínica.
70. Determinar con el personal médico las normas que rigen el registro de diagnósticos definitivos exactos y completos.
71. Velar por el correcto archivo, conservación, custodia y reserva de las historias clínicas.
72. Las demás funciones asignadas y que sean afines al desarrollo de sus actividades.

IV. CONTRIBUCIONES INDIVIDUALES

1. La realización de las actividades responde a prestación de servicios con criterios de calidad humana y tecnológica.
2. El cumplimiento de las tareas se fortalece y se enfoca en exceder las expectativas de los usuarios que hacen uso de los servicios.
3. Contribuir en el adecuado manejo de los insumos y/o equipos de uso diario en el desarrollo de sus funciones.
4. Reconocer las acciones pertinentes y actuar de acuerdo a ellas dentro del plan de emergencias hospitalarias.

V.- CONOCIMIENTOS BÁSICOS O ESENCIALES:

- Ley 100.
- Decreto 1011 Sistema Obligatorio de Garantía de la Calidad.
- Normas ISO – 9001 / 2000.
- Plan de emergencias hospitalario.
- Normas sobre manejo de información y sistemas.

VI.- REQUISITOS DE ESTUDIO Y EXPERIENCIA:

A. EDUCACIÓN: título profesional en ingeniería de sistemas con su respectiva tarjeta profesional.
B. FORMACIÓN: título de formación avanzada en las áreas relacionadas con el cargo.
C. EXPERIENCIA: dos (2) años de experiencia profesional, uno de los cuales requiere experiencia específica, la cual se entiende como la adquirida en empleos con funciones similares a las del cargo en el Sistema General de Seguridad Social en Salud.

I.- IDENTIFICACIÓN

NIVEL: TÉCNICO
DENOMINACIÓN DEL EMPLEO: TÉCNICO OPERATIVO
CÓDIGO: 314
GRADO: 4
NÚMERO DE CARGOS: 1
DEPENDENCIA: ÁREA SISTEMAS DE INFORMACIÓN
CARGO DEL JEFE INMEDIATO: PROFESIONAL ESPECIALIZADO ÁREA SISTEMAS DE INFORMACIÓN

II.- PROPÒSITO PRINCIPAL: Prestar servicios de apoyo en procesos operativos de ejecución de labores de sistemas, manteniendo buenas relaciones y atendiendo las quejas y solicitudes del personal del hospital para ser trasmitidas a su jefe inmediato.

III.- DESCRIPCIÓN DE FUNCIONES ESENCIALES:

1. Conocer y cumplir, de acuerdo a su competencia, lo establecido en la declaración de los deberes y derechos de los pacientes.
2. Realizar todas las actividades que le competan en los procesos de los estándares de acreditación de atención al cliente asistencial que se desarrollan en el área, o en los cuales ésta interviene.
3. Realizar todas las actividades que le competan en los procesos de los estándares de acreditación de direccionamiento que se desarrollan en el área, o en los cuales ésta interviene.
4. Realizar todas las actividades que le competan en los procesos de los estándares de acreditación de gerencia que se desarrollan en el área, o en los cuales ésta interviene.
5. Realizar todas las actividades que le competan en los procesos de los estándares de acreditación de gerencia de recursos humanos que se desarrollan en el área, o en los cuales ésta interviene.
6. Realizar todas las actividades que le competan en los procesos de los estándares de acreditación de gerencia del ambiente físico que se desarrollan en el área, o en los cuales ésta interviene.
7. Realizar todas las actividades que le competa en los procesos de los estándares de acreditación de gerencia de la información que se desarrollan en el área, o en los cuales ésta interviene.
8. Dar soporte a los módulos de facturación, admisiones, hospitalización, nómina y presupuesto.
9. Dar soporte a las aplicaciones desarrolladas internamente: despacho facturación, conciliación facturación – contabilidad, verificador de derechos y ley 387 y registro de historias clínicas.
10. Prestar soporte a las diferentes secciones en lo relacionado con informes acordes a sus módulos.
11. Análisis - diseño – desarrollo e implementación de herramientas que contribuyan a la administración de información, a nivel de toda la institución, según el plan de trabajo (POA), establecido para cada año.
12. Tener una semana de turno administrativo, durante la cual se da respuesta inmediata a todas las necesidades tanto de software o hardware que demande la institución, además de la verificación de la estabilidad y respaldo del sistema de información (DGH). ésta semana comprende una jornada semanal de 7:00 a.m. – 3:00 p.m., y los fines de semana o festivos de 10:00 a.m. –

12:00 m., y en horario no contemplado en este turno se tendrá disponibilidad inmediata según demanda.
13. Generar informes según demanda de los clientes internos y externos de la institución, de lo relacionado con la atención al paciente.
14. Trabajar en la identificación de problemas cuando la información generada presenta inconsistencias, y colaborar en la corrección de las mismas y en la búsqueda de acciones preventivas y correctivas que prevean este tipo de anomalías.
15. Contribuir en el proceso de recepción de facturas, que busca controlar la generación y despacho de facturación.
16. Colaborar en procesos específicos del manejo de información que sean requeridos de la parte administrativa.
17. Colaborar en el diseño e implementación de procesos sistematizados que permitan generar nuevos niveles de control, para facilitar la toma de decisiones.
18. Contribuir con la implementación e implantación del portal empresarial e intranet en la institución.
19. Realizar jornadas de capacitación de ofimática, a los diferentes funcionarios de la institución.
20. Realizar actualizaciones a nuevas versiones del sistema de información Dinámica Gerencial.
21. Participar en el proceso de acreditación del estándar de la información.
22. Acoger las nuevas funciones relacionadas con el cargo que sean asignadas por el jefe inmediato.
23. Las demás funciones asignadas y que sean afines al desarrollo de sus actividades.

IV.- CONTRIBUCIONES INDIVIDUALES:

1. Adecuada gestión documental.
2. Reconocer las acciones pertinentes y actuar de acuerdo a ellas dentro del plan de emergencias hospitalarias.
3. La realización de las actividades responde a prestación de servicios con criterios de calidad humana y tecnológica.
4. El cumplimiento de las tareas se fortalece y se enfoca en exceder las expectativas de los usuarios que hacen uso de los servicios.
5. Contribuir en el adecuado manejo de los insumos y/o equipos de uso diario en el desarrollo de sus funciones.

V.- CONOCIMIENTOS BÁSICOS O ESENCIALES

- Ley 100.
- Decreto 1011 Sistema Obligatorio de Garantía de la Calidad.
- Normas ISO – 9001 / 2000.
- Plan de emergencias hospitalario.
- Ley 594/2000.
- Informática avanzada.

VI.- REQUISITOS DE ESTUDIO Y EXPERIENCIA

A. EDUCACIÓN: título como tecnólogo en áreas de sistemas o certificación acreditada.
B. FORMACIÓN
C. EXPERIENCIA: un (1) año en cargos relacionados con las funciones.

3.1.2.3 Subprocesos del área de información y sistemas

Tabla 6. Subprocesos área de sistemas

Código	Subproceso	Objetivo	Alcance	Responsable
PRSGI-01	Copia de seguridad del Software de la organización	Garantizar el respaldo de la información registrada en los equipos de cómputo de la institución, con el fin de obtener seguridad y continuidad en los procesos que requieran de la misma.	Toda la organización	Ingeniero Orlando Argoty
PRSGI-02	Producción y entrega de información	Brindar información confiable y oportuna a los clientes externos e internos de la organización que la requieran.	Toda la organización y clientes externos	Ingeniero Orlando García y Ricardo Villota
PRSGI-03	Auditoría de sistemas	Garantizar un sistema de información confiable mediante un proceso de auditoría que permita administrar y controlar, por medio de una evaluación, al proveedor del Sistema de Información y aplicativos desarrollados por el mismo y los implantados por la organización.	Toda la organización	Coordinador gestión de información Roberto Yánez

Tabla 6. (Continuación)

Código	Subproceso	Objetivo	Alcance	Responsable
PRSGI-04	Mantenimiento preventivo de Hardware y Software	Mantener los equipos de cómputo en buenas condiciones de funcionamiento con el fin de garantizar el normal desempeño de los procesos y la vida útil de los equipos.	Toda la organización	Técnicos de sistemas William Solarte y Jhony Meneses
PRSGI-05	Mantenimiento correctivo de Hardware y Software	Obtener tecnología en correcto funcionamiento y acorde a las necesidades de cada área, logrando así la atención oportuna y eficiente de los clientes de la organización.	Toda la organización	Técnicos de sistemas William Solarte y Jhony Meneses
PRSGI-06	Actualización, implementación e implantación de módulos y aplicativos	Dar soluciones informáticas a las áreas de la organización que las requieran, con base en los requerimientos de información de cada una de ellas, con el fin de lograr sistematizar sus procesos obteniendo un adecuado tiempo de respuesta en la atención de sus clientes.	Toda la organización	Técnico Jeider Quintero y Manuel Vinueza

Los diagramas de cada subproceso se encuentran en el anexo A.

3.1.3 Sistema de información Dinámica Gerencial Hospitalaria

3.1.3.1 Información general. Dinámica Gerencial Hospitalaria (DGH) es un software para el sector salud, desarrollado en 1993 por la empresa SYAC S.A., que facilita la gestión de la información dentro de las áreas asistenciales, administrativas y financieras que constituyen a las Instituciones prestadoras de salud (IPS's, ARS's, EPS's, E.S.E.'s, Clínicas, Hospitales, entre otros) [48].

Figura 12. Logotipo del sistema DGH

Fuente: Sistemas y Asesorías de Colombia S.A.

Se trata de un sistema de información 100% web, compuesto por más de 30 módulos que funcionan completamente integrados y que permite, de acuerdo al tamaño de la Institución, instalar los módulos necesarios para satisfacer sus necesidades. Asimismo, puede tener como eje central la historia clínica o la facturación según las condiciones de cada cliente [48].

Actualmente, DGH está desarrollado con herramientas de la más reciente tecnología a nivel mundial, pues se basa en WebServices (Visual Studio – C#), permitiendo usar motores de bases de datos como SQL Server y Oracle.

El objetivo principal de DGH es brindar una herramienta completa que reduzca tiempos de trabajo, ofrezca elementos para la toma de decisiones gerenciales en tiempo real y apoye el desarrollo de los procesos misionales de la entidad, garantizando una mayor productividad y disminución de costos [50].

DGH cumple con todas las normas exigidas por la Ley colombiana para el manejo financiero, de facturación, ley 100 e historia clínica. Además cumple con estándares internacionales como HL7[13], XML, DICOM[14], Telemedicina, entre otros [49].

3.1.3.2 Módulos de la aplicación. Los módulos de la aplicación se encuentran clasificados en 2 grandes grupos, tal como se muestra en la siguiente tabla:

[13] Acrónimo de *Health Level Seven*. Conjunto de estándares para facilitar el intercambio electrónico de información clínica.
[14] Acrónimo *de Digital Imaging and Communication in Medicine*. Estándar reconocido mundialmente para el manejo, almacenamiento, impresión e intercambio de imágenes médicas.

Tabla 7. Módulos del sistema DGH

Grupo	Módulo
Administrativo y financiero	Registro y correspondencia
	Jurídico
	Gestión gerencial
	Contratación
	Control de visitantes
	Archivo central
	Control interno
	Mantenimiento de activos
	Préstamos vivienda
	Generales
	Arrendamientos
	Contabilidad
	Presupuestos
	Tesorería
	Cartera
	Pagos
	Nómina
	Impuestos
	Importaciones
	Mantenimiento de equipos
	Compras
	Producción
	Activos fijos
Operativo y Asistencial	Contratos IPS
	Citas web
	Admisiones
	Hospitalización
	Inventarios
	Historia clínica
	Facturación
	Costos hospitalarios
	Laboratorio
	Promoción y prevención IPS
	Citas médicas
	Programación de cirugías
	Banco de sangre
	Nutrición y dietas
	Esterilización
	Quejas y reclamos
	Telemedicina

Fuente: Sistemas y Asesorías de Colombia S.A.

3.1.3.3 Requerimientos del sistema

Prerrequisitos:

Microsoft .NET Framework 3.5 Service Pack 1. Actualización acumulativa que contiene numerosas características nuevas de .NET Framework 2.0, 3.0 y 3.5, e incluye las actualizaciones acumulativas de .NET Framework 2.0 Service Pack 2 y .NET Framework 3.0 Y 4.0 Service Pack 2 [50].

Requerimientos mínimos:

Los requerimientos técnicos para el buen funcionamiento de DGH, dependen de diferentes aspectos [50]:

- Número de usuarios.
- Número de estaciones.
- Red física.
- Red lógica.
- Software de red.
- Estado de los equipos, entre otros.

Sin embargo se recomienda que los equipos tengan mínimo las siguientes características [50]:

- **Sistemas Operativos compatibles:** Windows Server 2003; Windows Server 2008; Windows Vista; Windows XP.
- **Procesador:** procesador Pentium a 400 MHz o equivalente (mínimo); procesador Pentium a 1 GHz o equivalente (recomendado).
- **RAM:** 1 Giga.
- **Disco Duro:** 10 Gigas.
- **unidad de CD o DVD:** no se necesita.
- **Pantalla:** 1024 x 700, 256 colores (mínimo); color de alta densidad de 1024 x 768, de 32 bits (recomendado).
- **Motor de Base de Datos:** SQL u Oracle.

3.1.4 Manuales y documentos de soporte

- Portafolio de servicios del Hospital Universitario Departamental de Nariño E.S.E
- Planos arquitectónicos del Hospital
- Normograma del Hospital Universitario Departamental de Nariño E.S.E
- Plan de Desarrollo Hospital Universitario Departamental de Nariño E.S.E

- Estatuto de contratación
- Manual de funciones y competencias laborales
- Código de ética y valores del Hospital
- Reconocimientos
- Política del Sistema de Gestión de Información 2011
- Políticas de uso responsable de los sistemas de información y computadores del Hospital Universitario Departamental de Nariño E.S.E
- Inventario a Diciembre de 2012
- *Screenshots* del Sistema de Información Dinámica Gerencial Hospitalaria
- Manual de Generales y Seguridad .NET
- Diccionario de Datos del Módulo General.NET 2.0

Para más información sobre ésta documentación, ver anexo B.

3.2 ARCHIVO CORRIENTE

3.2.1 Memorando de planeación

Tema: auditoría de la seguridad lógica.

Título de la auditoría: auditoría aplicada a la seguridad del sistema de información Dinámica Gerencial Hospitalaria del Hospital Universitario Departamental de Nariño.

Objetivo: evaluar la eficiencia y eficacia de los procedimientos y controles de seguridad lógica que tiene el sistema de información DGH, teniendo en cuenta sus recursos, políticas y usuarios.

Alcance: dentro de la evaluación se tuvo en cuenta la clasificación de datos, la administración de integridad, propiedad de datos, políticas de seguridad, entrenamiento del personal, administración de riesgos, mantenimiento del software, contrato de compra y venta del software, plan de contingencias, procedimientos para el resguardo de la información, autenticación de usuarios, administración de cuentas de usuarios, concienciación sobre seguridad de la información, protección de la tecnología de seguridad, mesa de servicios, configuración de software y procesos de autoevaluación que se llevan a cabo dentro del área. También se evaluaron algunos aspectos generales sobre seguridad en la red, basándose en entrevistas concedidas por el personal del área de sistemas.

Los resultados de este proceso fueron plasmados en un informe que se entregó al Hospital, para que tome las medidas pertinentes con base en las recomendaciones y sugerencias realizadas.

Recursos

➢ Recursos humanos

Por parte de la auditoría:

- ✓ Edith Friney Díaz y Maira Alejandra Mora (Estudiantes).
- ✓ Ing. Manuel Ernesto Bolaños (Asesor).

Por parte del Hospital:

- ✓ Ing. Roberto Yánez Constante (Coordinador área de información y sistemas).
- ✓ Usuarios del sistema DGH.

➢ Recursos administrativos

- ✓ Sistema de gestión de base de datos Microsoft SQL Server 2008 R2.
- ✓ Software Sistemas y Asesorías de Colombia S.A. Dinámica Gerencial, versión 2012 upgrade 11 parche 07.9.

➢ Recursos tecnológicos

Hardware

- ✓ Computador de escritorio con procesador Intel Core i3, 3.07 GHZ, memoria RAM de 2 GB y disco duro de 500 GB.
- ✓ Computador portátil con procesador Intel Core 2 Duo, 1.50 GHZ, memoria RAM de 2 GB y disco duro de 120 GB.
- ✓ Impresora multifuncional.
- ✓ Grabadora de voz.

Software

- ✓ Paquete ofimático.
- ✓ Editores de multimedia en general.

Cronograma

Tabla 8. Cronograma

Actividad	Mes 1				Mes 2				Mes 3				Mes 4				Mes 5				Mes 6			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Estudio preliminar																								
Memorando de planeación																								
Elaboración del programa de auditoría																								
Ejecución de la auditoría																								
Elaboración del informe																								
Sustentación del informe																								

Presupuesto: Para la ejecución de la auditoria se estableció el siguiente presupuesto:

Tabla 9. Presupuesto

Ítem	Valor
Útiles y Papelería	$ 20.000
Medios de almacenamiento de datos (CD, DVD, USB)	$ 30.000
Gastos generales (cafetería, transporte e imprevistos)	$300.000
Total	**$350.000**

3.2.2 Programa de auditoría. Para el desarrollo de la auditoría aplicada a la seguridad del sistema de información Dinámica Gerencial Hospitalaria del Hospital Universitario Departamental de Nariño, se utilizará en primer lugar la metodología COBIT, la cual define un marco de referencia que clasifica los procesos de las unidades de tecnología de información en cuatro dominios; y en segundo lugar, se aplicará la norma ISO/IEC 27002 haciendo una equivalencia entre sus controles y los diferentes objetivos de control existentes en COBIT.

Los criterios a tener en cuenta son los siguientes:

3.2.2.1 Dominio: planear y organizar (PO)

➢ **P02. Definir la arquitectura de la información.** Se debe crear y actualizar de forma regular un modelo de información del negocio y definir los sistemas apropiados para optimizar el uso de esta información. Esto garantiza la entrega de información confiable y segura, y permite racionalizar los recursos de los sistemas de información para igualarse con las estrategias del negocio. Este proceso de TI también es necesario para incrementar la responsabilidad sobre la integridad y seguridad de los datos y para mejorar la efectividad y control de la información compartida a lo largo de las aplicaciones y de las entidades.

1. PO2.3 Esquema de clasificación de datos. Verificar si la organización clasifica y protege la información de acuerdo a su sensibilidad e importancia. Su equivalente en la norma ISO/IEC 27002 es 7.2.1 Directrices de clasificación.

2. PO2.4 Administración de integridad. Evaluar la existencia de procedimientos que permitan garantizar la integridad y consistencia de los datos almacenados en la base de datos del sistema DGH. No existe equivalente en la norma ISO/IEC 27002.

➢ **P04. Definir los procesos, organización y relaciones de TI.** Deben existir procesos, políticas de administración y procedimientos para todas las funciones, con atención específica en el control, el aseguramiento de la calidad, la administración de riesgos, la seguridad de la información, la propiedad de datos y de sistemas y la segregación de funciones, con el fin de garantizar el soporte oportuno de los requerimientos del negocio.

1. PO4.9 Propiedad de datos y de sistemas. Verificar el grado de responsabilidad existente sobre la propiedad de los datos. Su equivalente en la norma ISO/IEC 27002 es 6.1.3 Asignación de responsabilidades relativas a la seguridad de la información.

➢ **P06. Comunicar las aspiraciones y la dirección de la gerencia.** Se deben definir y comunicar políticas, procedimientos, directrices y otra documentación aprobada por la dirección, de forma precisa y entendible. La comunicación apoya el logro de los objetivos de TI y asegura la concientización y el entendimiento de los riesgos de negocio y de TI. Además, éste proceso permite garantizar el cumplimiento de las leyes y reglamentos relevantes.

1. PO6.3 Administración de políticas para TI. Verificar la existencia de políticas de seguridad de la información. Su equivalente en la norma ISO/IEC 27002 es 5.1.1 Documento de política de seguridad de la información.

2. PO6.4 Implantación de políticas de TI. Verificar la adecuada implantación y comunicación de políticas de seguridad para el manejo de información. Su equivalente en la norma ISO/IEC 27002 es 6.1.1 Compromiso de la dirección con la seguridad de la información.

- **P07. Administrar los recursos humanos de TI.** Los empleados deben recibir entrenamiento continuo para conservar conciencia sobre la seguridad de la información al nivel requerido para alcanzar las metas organizacionales. Además, se debe tomar medidas expeditas respecto a los cambios en los puestos de trabajo.

1. PO7.4 Entrenamiento del personal de TI. Verificar si el personal de la organización maneja y aplica conocimientos básicos sobre seguridad de la información. Su equivalente en la norma ISO/IEC 27002 es 8.2.2 Concienciación, formación y capacitación en seguridad de la información.

2. PO7.8 Cambios y terminación de trabajo. Verificar si el personal retirado de la organización es privado de sus privilegios de acceso en el sistema DGH. Su equivalente en la norma ISO/IEC 27002 es 8.3.3 Retirada de los derechos de acceso.

- **P09. Evaluar y administrar los riesgos de TI.** Se debe definir un nivel común y acordado de riesgos de TI, estrategias de mitigación y riesgos residuales acordados. Cualquier impacto potencial sobre las metas de la organización, causado por algún evento no planeado, se debe identificar, analizar y evaluar. Se deben adoptar estrategias de mitigación de riesgos para minimizar los riesgos residuales a un nivel aceptable. El resultado de la evaluación debe ser entendible y se debe expresar en términos financieros, para permitir a los participantes alinear los riesgos a un nivel aceptable de tolerancia.

1. PO9.2 Establecimiento del contexto del riesgo. Verificar la existencia de una metodología para la evaluación de riesgos que garantice resultados apropiados bajo criterios preestablecidos. Su equivalente en la norma ISO/IEC 27002 es 14.1.2 Continuidad del negocio y evaluación de riesgos.

2. PO9.3 Identificación de eventos. Revisar si han sido identificados y registrados los eventos con un impacto potencial negativo sobre las operaciones

de la organización. Su equivalente en la norma ISO/IEC 27002 es 13.1.1 Notificación de los eventos de seguridad de la información.

3. PO9.4 Evaluación de riesgos de TI. Verificar si se evalúa de forma regular la probabilidad de ocurrencia y el impacto de todos los riesgos identificados. Su equivalente en la norma ISO/IEC 27002 es 14.1.2 Continuidad del negocio y evaluación de riesgos.

4. PO9.5 Respuesta a los riesgos. Verificar si el área de sistemas cuenta con un plan de acción contra riesgos, en el cual se definan estrategias para evitar, reducir, compartir o aceptar los riesgos. No existe equivalente en la norma ISO/IEC 27002.

3.2.2.2 Dominio: adquirir e implementar (AI)

- **AI2 Adquirir y mantener software aplicativo.** Las aplicaciones deben estar disponibles de acuerdo a los requerimientos del negocio. Este proceso permite apoyar la operatividad del negocio de forma apropiada con las aplicaciones automatizadas correctas.

1. AI2.3 Control y posibilidad de auditar las aplicaciones. Evaluar el uso y administración de los *logs* de auditoría generados por el sistema DGH. Su equivalente en la norma ISO/IEC 27002 es 10.10.1 Registros de auditoría.

2. AI2.8 Aseguramiento de la calidad del software. Verificar los controles utilizados para asegurar el buen funcionamiento y la calidad del sistema DGH. Su equivalente en la norma ISO/IEC 27002 es 10.3.2 Aceptación del sistema.

3. AI2.10 Mantenimiento de software aplicativo. Evaluar los procedimientos existentes para el mantenimiento y/o actualización de las aplicaciones de software. No existe equivalente en la norma ISO/IEC 27002.

- **AI4 Facilitar la operación y el 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.

1. AI4.3 Transferencia de conocimiento a usuarios finales. Verificar la existencia de un plan de entrenamiento que aborde el entrenamiento inicial y continuo del personal involucrado con el sistema DGH. También se evalúa la

existencia de manuales de usuario y otros materiales de apoyo. No existe equivalente en la norma ISO/IEC 27002.

2. AI4.4 Transferencia de conocimiento al personal de operaciones y soporte. Verificar la existencia de un plan de entrenamiento que aborde el entrenamiento inicial y continuo del personal técnico y de operaciones. También se evalúa la existencia de manuales de procedimientos, manuales de operación y escenarios de atención al usuario. Su equivalente en la norma ISO/IEC 27002 es 10.1.1 Documentación de los procedimientos de operación.

- **AI5 Adquirir recursos de TI.** Se deben suministrar recursos TI, incluyendo personas, hardware, software y servicios. Esto requiere de la definición y ejecución de los procedimientos de adquisición, la selección de proveedores y el ajuste de arreglos contractuales. De esta manera se garantiza que la organización tenga todos los recursos de TI que se requieren de una manera oportuna y rentable.

1. AI5.1 Control de adquisición. Evaluar el proceso de adquisición del software DGH. Su equivalente en la norma ISO/IEC 27002 es 6.1.5 Acuerdos de confidencialidad.

2. AI5.2 Administración de contratos con proveedores. Verificar las cláusulas del contrato de compra y venta del software DGH, donde se especifiquen las responsabilidades y obligaciones legales, financieras, organizacionales, documentales, de desempeño, de seguridad, de propiedad intelectual, de mantenimiento y de conclusión por parte del hospital y del proveedor. Su equivalente en la norma ISO/IEC 27002 es 6.2.3 Tratamiento de la seguridad en contratos con terceros.

3. AI5.4 Adquisición de recursos de TI. Verificar la existencia de controles que garanticen la protección de los intereses del hospital en todos los acuerdos contractuales de adquisición. No existe equivalente en la norma ISO/IEC 27002.

3.2.2.3 Dominio: entregar y dar soporte (DS)

- **DS4 Garantizar la continuidad del servicio.** Es preciso desarrollar, mantener y probar planes de continuidad de TI, almacenar respaldos fuera de las instalaciones y entrenar de forma periódica sobre los planes de continuidad. Esto minimiza la probabilidad y el impacto de interrupciones mayores en los servicios de TI, sobre funciones y procesos claves del negocio.

1. DS4.2 Planes de continuidad de TI. Verificar la existencia de un plan de contingencias orientado a la seguridad de la información, en el cual se definan procedimientos que permitan reducir el impacto de una interrupción mayor de las funciones y los procesos clave del hospital. Su equivalente en la norma ISO/IEC 27002 es 14.1.3 Desarrollo e implantación de planes de continuidad que incluyan la seguridad de la información.

2. DS4.3 Recursos críticos de TI. Verificar si el área de sistemas ha clasificado a los recursos de información de acuerdo a su criticidad, para construir resistencia y establecer prioridades en situaciones de recuperación. Su equivalente en la norma ISO/IEC 27002 es 14.1.1 Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio.

3. DS4.9 Almacenamiento de respaldos fuera de las instalaciones. Verificar si los medios de respaldo son almacenados fuera de las instalaciones del hospital, de tal manera que se garantice su disponibilidad para la recuperación de TI y para los planes de continuidad del negocio. Su equivalente en la norma ISO/IEC 27002 es 10.5.1 Copias de seguridad de la información.

- **DS5 Garantizar la seguridad de los sistemas.** La necesidad de mantener la integridad de la información y de proteger los activos de TI, requiere de un proceso de administración de la seguridad. Este proceso incluye el establecimiento y mantenimiento de roles y responsabilidades de seguridad, políticas, estándares y procedimientos de TI. La administración de la seguridad también incluye realizar monitoreos de seguridad y pruebas periódicas, así como realizar acciones correctivas sobre las debilidades o incidentes 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.

1. DS5.3 Administración de identidad. Verificar los mecanismos de autenticación utilizados por el sistema DGH y la administración de identidades de usuarios. Sus equivalentes en la norma ISO/IEC 27002 son 11.5.2 Identificación y autenticación de usuario y 11.2.3 Gestión de contraseñas de usuario.

2. DS5.4 Administración de cuentas del usuario. Verificar los procedimientos existentes para la gestión de las cuentas de usuario del sistema DGH y los privilegios asociados a ellas. Sus equivalentes en la norma ISO/IEC 27002, son: 11.2.1 Registro de usuario, 11.2.2 Gestión de privilegios y 11.2.4 Revisión de los derechos de acceso de usuario.

3. DS5.5 Pruebas, vigilancia y monitoreo de la seguridad. Verificar si el área de sistemas cuenta con un proceso de monitorización para la detección oportuna de actividades inusuales o anormales dentro del sistema DGH. Su equivalente en la norma ISO/IEC 27002 es 12.6.1 Control de las vulnerabilidades técnicas.

4. DS5.7 Protección de la tecnología de seguridad. Verificar los controles que permiten proteger tanto al entorno de trabajo del sistema como a la red y a la información contenida en los equipos de cómputo. Sus equivalentes en la norma ISO/IEC 27002, son: 10.6.2 Seguridad de los servicios de red, 11.6.1 Restricción del acceso a la información y 12.6.1 Control de las vulnerabilidades técnicas.

5. DS5.9 Prevención, detección y corrección de software malicioso. Verificar la existencia de controles que permitan prevenir, detectar y corregir problemas de *malware* (virus, gusanos, *spyware*) en toda la organización. Su equivalente en la norma ISO/IEC 27002 es 10.4.1 Controles contra el código malicioso.

6. DS5.10 Seguridad de la red. Verificar el uso de técnicas de seguridad y procedimientos de administración asociados (*firewalls*, dispositivos de seguridad y detección de intrusos) para autorizar acceso y controlar los flujos de información desde y hacia la red. Sus equivalentes en la norma ISO/IEC 27002, son: 10.6.1 Controles de red y 10.6.2 Seguridad de los servicios de red.

- **DS7 Educar y entrenar a los usuarios.** Se deben identificar las necesidades de entrenamiento de cada grupo de usuarios. Además de identificar las necesidades, este proceso incluye la definición y ejecución de una estrategia para llevar a cabo un entrenamiento efectivo y para medir los resultados. Un programa efectivo de entrenamiento incrementa el uso efectivo y eficiente de soluciones y aplicaciones tecnológicas al disminuir los errores, incrementando la productividad y el cumplimiento de las políticas y procedimientos.

1. DS7.1 Identificación de necesidades de entrenamiento y educación. Verificar la existencia de programas de entrenamiento sobre la seguridad de información para los usuarios del sistema DGH. Su equivalente en la norma ISO/IEC 27002 es 8.2.2 Concienciación, formación y capacitación en seguridad de la información.

- **DS8 Administrar la mesa de servicio y los incidentes.** Es necesario contar con una mesa de servicio bien diseñada y bien ejecutada, y de un proceso de administración de incidentes. Este proceso incluye la creación de una función de mesa de servicio con registro, escalamiento de incidentes, análisis de tendencia, análisis causa-raíz y resolución. Los beneficios del negocio incluyen el incremento

en la productividad gracias a la resolución rápida de consultas. Además, el negocio puede identificar la causa raíz (tales como un pobre entrenamiento a los usuarios) a través de un proceso de reporte efectivo.

1. DS8.1 Mesa de servicios. Verificar la existencia de procedimientos que permitan atender, analizar y solventar requerimientos de información y/o incidentes reportados por los usuarios del sistema. Su equivalente en la norma ISO/IEC 27002 es 14.1.4 Marco de referencia para la planificación de la continuidad del negocio.

- **DS9 Administrar la configuración.** Para garantizar la integridad de las configuraciones de software se requiere establecer y mantener un repositorio de configuraciones completo y preciso. Este proceso incluye la recolección de información de la configuración inicial, el establecimiento de normas, la verificación y auditoría de la información de la configuración y la actualización del repositorio de configuración conforme se necesite. Una efectiva administración de la configuración facilita una mayor disponibilidad y resuelve los problemas más rápido.

1. DS9.1 Repositorio y línea base de configuración. Verificar la existencia de un repositorio que contenga toda la información referente al software aplicativo que se utiliza en el hospital, desde los elementos necesarios para su configuración hasta detalles de licenciamiento. Su equivalente en la norma ISO/IEC 27002 es 7.1.1 Inventario de activos.

2. DS9.2 Identificación y mantenimiento de elementos de configuración. Verificar los procedimientos existentes para prevenir la inclusión de software no-autorizado en los equipos que cuentan con el aplicativo DGH. Su equivalente en la norma ISO/IEC 27002 es 15.1.5 Prevención del uso indebido de recursos de tratamiento de la información.

3. DS9.3 Revisión de integridad de la configuración. Verificar los controles que permiten revelar la existencia de cualquier software personal o no autorizado. Su equivalente en la norma ISO/IEC 27002 es 10.4.2 Controles contra el código descargado en el cliente.

- **DS11 Administración de datos.** Una efectiva administración de datos requiere de la identificación de requerimientos de datos. Este proceso también incluye el establecimiento de procedimientos efectivos para administrar la librería de medios, el respaldo y la recuperación de datos y la eliminación apropiada de medios. Una

efectiva administración de datos ayuda a garantizar la calidad, oportunidad y disponibilidad de la información del negocio.

1. DS11.3 Sistema de administración de librerías de medios. Verificar la rotulación y existencia de inventarios de copias de seguridad. Sus equivalentes en la norma ISO/IEC 27002, son: 7.2.2 Etiquetado y manipulado de la información; y 7.1.1 Inventario de activos.

2. DS11.5 Respaldo y restauración. Verificar los procedimientos existentes para la realización y administración de *backups* de la base de datos del sistema DGH. Su equivalente en la norma ISO/IEC 27002 es 10.5.1 Copias de seguridad de la información.

3.2.2.4 Dominio: Monitorear y Evaluar (ME)

- **ME1 Monitorear y evaluar el desempeño de TI.** Una efectiva administración del desempeño de TI requiere un proceso de monitoreo. El proceso incluye la definición de indicadores de desempeño relevantes, reportes sistemáticos y oportunos de desempeño y tomar medidas expeditas cuando existan desviaciones. El monitoreo se requiere para garantizar que las cosas correctas se hagan y que estén de acuerdo con el conjunto de direcciones y políticas.

1. ME1.4 Evaluación del desempeño. Verificar la existencia de reportes que permitan dar a conocer la situación actual del hospital en cuanto a seguridad de la información y el grado de cumplimiento de los indicadores establecidos para el área de sistemas. Sus equivalentes en la norma ISO/IEC 27002, son: 15.2.1 Cumplimiento de las políticas y normas de seguridad y 15.2.2 Comprobación del cumplimiento técnico.

- **ME2 Monitorear y evaluar el control interno.** Establecer un programa de control interno efectivo para TI requiere un proceso bien definido de monitoreo. Este proceso incluye el monitoreo y el reporte de las excepciones de control, resultados de las auto-evaluaciones y revisiones por parte de terceros. Un beneficio clave del monitoreo del control interno es proporcionar seguridad respecto a las operaciones eficientes y efectivas y el cumplimiento de las leyes y regulaciones aplicables.

1. ME2.2 Revisiones de auditoría. Verificar los procesos de auditoría que se llevan a cabo dentro del área de sistemas y evaluar su utilidad. Su equivalente en la norma ISO/IEC 27002 es 10.10.2 Supervisión del uso del sistema.

2. ME2.5 Aseguramiento del control interno. Verificar los procedimientos existentes para la designación del personal responsable de efectuar los procesos de auditoría. Su equivalente en la norma ISO/IEC 27002 es 15.3.1 Controles de auditoría de los sistemas de información.

3. ME2.7 Acciones correctivas. Verificar si el área de sistemas cuenta con planes para iniciar medidas correctivas basadas en las evaluaciones y en los reportes de control. No existe equivalente en la norma ISO/IEC 27002.

3.2.3 Diseño de los elementos de auditoría. Para iniciar con la ejecución de la auditoría es necesario contar con diferentes instrumentos de recolección de datos; de ellos depende, en gran medida, la calidad de la información, siendo ésta la base para las etapas subsiguientes y para los resultados.

Al momento de diseñar los instrumentos se tuvieron en cuenta tres aspectos importantes: el objetivo de la auditoría, las características del informante y el tiempo disponible para efectuar la recolección. A continuación, se muestran los formatos que se utilizaron en el desarrollo del trabajo.

3.2.3.1 Cuadro de definición de fuentes de conocimiento. Permite establecer las fuentes de conocimiento (documentación, manual, política o procedimiento) necesarias para la evaluación de un determinado proceso COBIT, además de definir las pruebas de análisis y ejecución que se deben realizar con dicho material.

Para la elaboración de los cuadros de definición de fuentes de conocimiento se empleó el siguiente formato:

Figura 13. Formato cuadro de definición de fuentes de conocimiento

HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO E.S.E.	CUADRO DE DEFINICIÓN DE FUENTES DE CONOCIMIENTO, PRUEBAS DE ANÁLISIS Y PRUEBAS DE AUDITORIA	REF

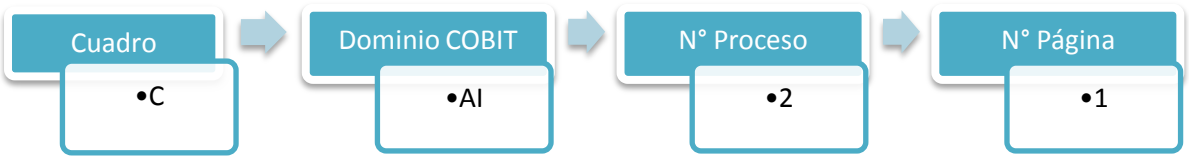
ENTIDAD AUDITADA			
AREA AUDITADA		OBJETO DE ESTUDIO	
RESPONSABLES			
MATERIAL DE SOPORTE		FECHA	
DOMINIO		PROCESO	
DESCRIPCION DE ACTIVIDAD/PRUEBA:			

FUENTES DE CONOCIMIENTO	REPOSITORIO DE PRUEBAS APLICABLES	
	DE ANÁLISIS	DE EJECUCIÓN

Como se puede observar, en la parte superior se encuentra el logo de la empresa auditada y posteriormente existen varios campos que pueden describirse así:

REF: identificación del cuadro. En este campo se utiliza la siguiente nomenclatura:

Figura 14. Identificación del cuadro



ENTIDAD AUDITADA: nombre de la entidad auditada.
ÁREA AUDITADA: nombre del área a la cual se aplica la auditoría.
OBJETO DE ESTUDIO: identificación de la parte a evaluar.
RESPONSABLES: nombre de los auditores.

MATERIAL DE SOPORTE: normas utilizadas para realizar la auditoría (COBIT 4.1 e ISO/IEC 27002)
FECHA: tiempo de duración de la auditoría.
DOMINIO: nombre del dominio de COBIT que se está aplicando.
PROCESO: nombre del proceso específico que hace parte del dominio que se está evaluando.
DESCRIPCIÓN DE ACTIVIDAD/PRUEBA: resumen del objetivo del proceso a evaluar.
FUENTES DE CONOCIMIENTO: espacio que permite identificar las herramientas necesarias para obtener la información. Puede ser a través de entrevistas, manuales, políticas, archivos físicos, reportes, contratos, etc.
REPOSITORIO DE PRUEBAS DE ANÁLISIS: espacio que describe el análisis de cada proceso y de la información obtenida.
REPOSITORIO DE PRUEBAS DE EJECUCIÓN: describe las acciones a realizar para la ejecución de la auditoría, ya sea revisión, verificación, pruebas u obtención de inconsistencias, entre otras.

A continuación se muestra como ejemplo, el cuadro de definición de fuentes de conocimiento aplicado en el proceso DS4 Garantizar la continuidad del servicio:

Figura 15. Cuadro de definición de fuentes de conocimiento para el proceso DS4

HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO E.S.E

CUADRO DE DEFINICIÓN DE FUENTES DE CONOCIMIENTO, PRUEBAS DE ANÁLISIS Y PRUEBAS DE AUDITORIA	REF
	C-DS4-1

ENTIDAD AUDITADA	Hospital Universitario Departamental de Nariño E. S. E.		
AREA AUDITADA	Seguridad lógica	**OBJETO DE ESTUDIO**	Sistema de información DGH
RESPONSABLES	Edith Friney Díaz Fuelantala y Maira Alejandra Mora Enríquez		
MATERIAL DE SOPORTE	COBIT e ISO/IEC 27002	**FECHA**	Desde el 22 de Marzo hasta el 18 de Julio de 2013
DOMINIO	Entregar y dar soporte (DS)	**PROCESO**	Garantizar la Continuidad del Servicio (DS4)
DESCRIPCION DE ACTIVIDAD/PRUEBA: Verificar la existencia y administración de planes o procedimientos que garanticen la recuperación de información crítica en caso de daño o pérdida de información.			

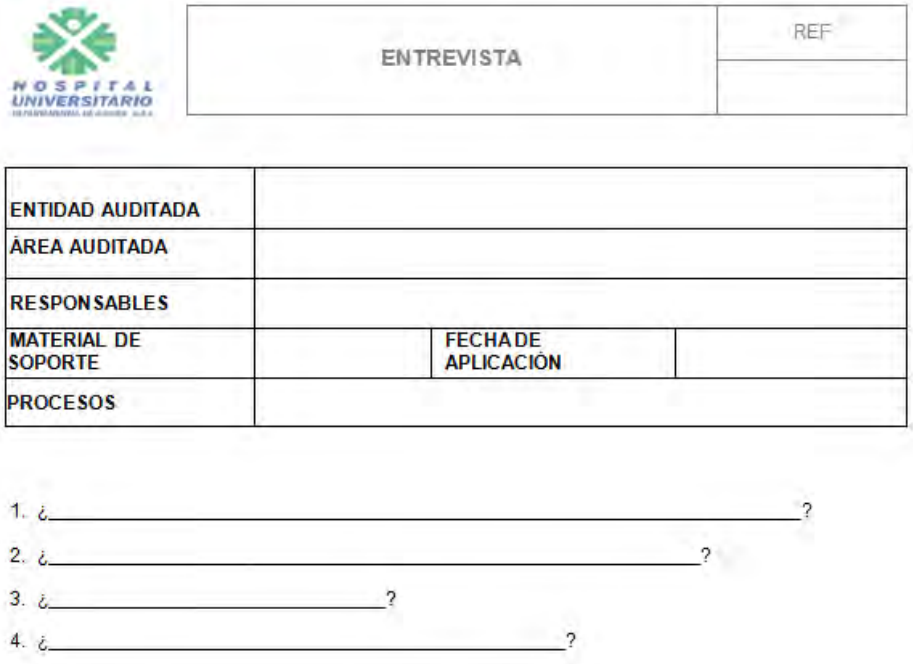
FUENTES DE CONOCIMIENTO	REPOSITORIO DE PRUEBAS APLICABLES	
	DE ANÁLISIS	DE EJECUCIÓN
• Entrevista con el funcionario encargado del área de sistemas. • Entrevista con el funcionario encargado del mantenimiento de los *backups*.	• Analizar la administración de los *backups*. • Analizar el plan de contingencias, en cuanto a seguridad de información, que existe en el hospital	• Verificar la existencia de un plan que permita garantizar la recuperación y estabilidad del funcionamiento del sistema DGH. • Verificar el correcto almacenamiento de los *backups*.

Para observar la totalidad de los cuadros de definición de fuentes de conocimiento utilizados en el desarrollo de la auditoría, ver anexo C.

3.2.3.2 Entrevistas. La entrevista es una técnica eficaz para obtener datos relevantes de alta calidad, que pueden ser probados al detalle con la persona que es entrevistada. Responde al formato de pregunta-respuesta y se utiliza como complemento a los cuestionarios cuantitativos. A través de ella se pueden captar además los gestos, los tonos de voz, los énfasis, etc., que aportan una importante información sobre el tema objeto de auditoría.

Durante el desarrollo del presente trabajo, únicamente se realizaron entrevistas con preguntas abiertas, ya que éstas ponen pocas restricciones a las respuestas del entrevistado permitiéndole expresarse libremente. Para la elaboración de dichas entrevistas, se utilizó el siguiente formato:

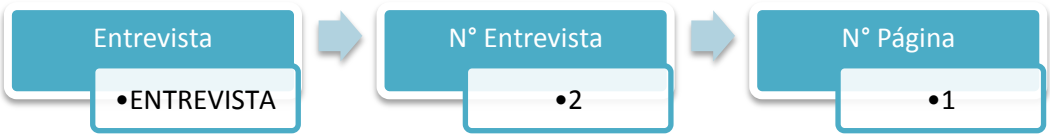
Figura 16. Formato entrevistas



Como se puede observar, el formato contiene varios campos que pueden describirse así:

REF: identificación de la entrevista. En éste campo se utiliza la siguiente nomenclatura:

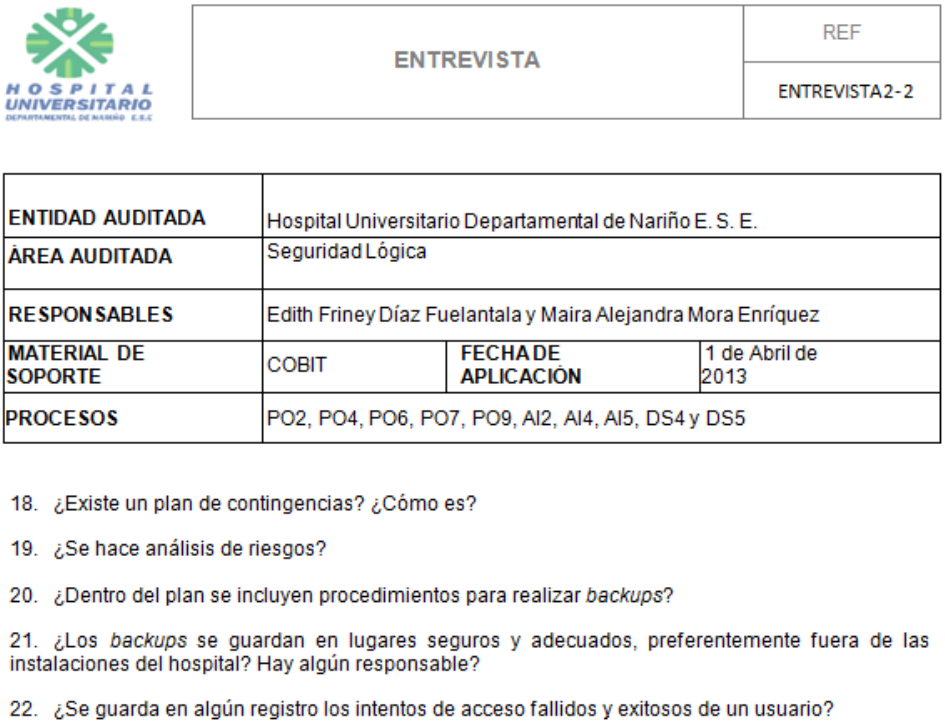
Figura 17. Identificación de entrevistas



ENTIDAD AUDITADA: nombre de la entidad auditada.
ÁREA AUDITADA: nombre del área a la cual se aplica la auditoría.
RESPONSABLES: nombre de los auditores.
MATERIAL DE SOPORTE: normas utilizadas para realizar la auditoría (COBIT 4.1 e ISO/IEC 27002).
FECHA DE APLICACIÓN: día en el que se realizó la entrevista.
PROCESOS: criterios sobre los cuales se está indagando.

A continuación se muestra como ejemplo, una de las primeras entrevistas realizadas para conocer más sobre el cumplimiento del proceso DS4 Garantizar la continuidad del servicio:

Figura 18. Entrevista proceso DS4



HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO E.S.E

ENTREVISTA	REF
	ENTREVISTA2-2

ENTIDAD AUDITADA	Hospital Universitario Departamental de Nariño E. S. E.		
ÁREA AUDITADA	Seguridad Lógica		
RESPONSABLES	Edith Friney Díaz Fuelantala y Maira Alejandra Mora Enríquez		
MATERIAL DE SOPORTE	COBIT	**FECHA DE APLICACIÓN**	1 de Abril de 2013
PROCESOS	PO2, PO4, PO6, PO7, PO9, AI2, AI4, AI5, DS4 y DS5		

18. ¿Existe un plan de contingencias? ¿Cómo es?

19. ¿Se hace análisis de riesgos?

20. ¿Dentro del plan se incluyen procedimientos para realizar *backups*?

21. ¿Los *backups* se guardan en lugares seguros y adecuados, preferentemente fuera de las instalaciones del hospital? Hay algún responsable?

22. ¿Se guarda en algún registro los intentos de acceso fallidos y exitosos de un usuario?

Las entrevistas aplicadas al personal del Hospital Universitario Departamental de Nariño pueden encontrarse en el anexo F.

3.2.3.3 Cuestionario cuantitativo. Contiene una serie de preguntas formuladas a partir del cuadro de definición de fuentes de conocimiento. Dichas preguntas son cerradas, es decir, sólo tienen tres opciones de respuesta: SI, NO y NA (No Aplica).

Con los cuestionarios se pretende conseguir una calificación de cada proceso COBIT a evaluar, por lo tanto, las respuestas a las preguntas se encontrarán en un rango de 1 a 5 (donde 1 es lo más bajo y 5 lo más alto). La puntuación dependerá del nivel de importancia de la pregunta de acuerdo al criterio de los auditores.

El formato utilizado para la elaboración de los cuestionarios contiene una serie de campos que se describen a continuación:

REF: identificación del cuestionario. En éste campo se utiliza la siguiente nomenclatura:

Figura 19. Identificación del cuestionario

ENTIDAD AUDITADA: nombre de la entidad auditada.
ÁREA AUDITADA: nombre del área a la cual se aplica la auditoría.
OBJETO DE ESTUDIO: identificación de la parte a evaluar.
RESPONSABLES: nombre de los auditores.
MATERIAL DE SOPORTE: normas utilizadas para realizar la auditoría (COBIT 4.1 e ISO/IEC 27002).
FECHA: tiempo de duración de la auditoría.
DOMINIO: nombre del dominio COBIT que se está aplicando.
PROCESO: nombre del proceso específico que hace parte del dominio que se está evaluando.
ENTREVISTADO: nombre de la persona a quien se le aplicó el cuestionario.
PREGUNTA: número y descripción de la pregunta.
SI, NO y NA: opciones de respuesta.
OBSERVACIÓN: aclaración sobre las preguntas con respuesta SI, para indicar anomalías.
RPT: referencia a pruebas y hallazgos. En éste campo se pueden encontrar 2 nomenclaturas:

Figura 20. Identificación de pruebas

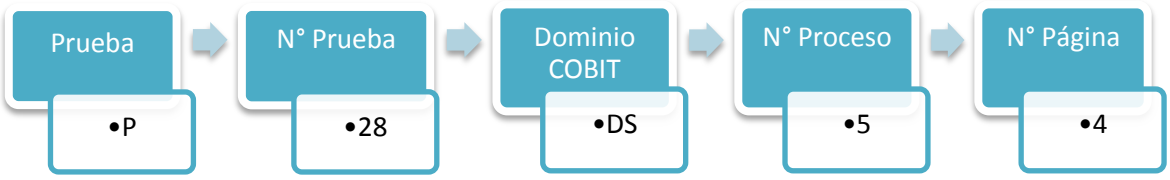
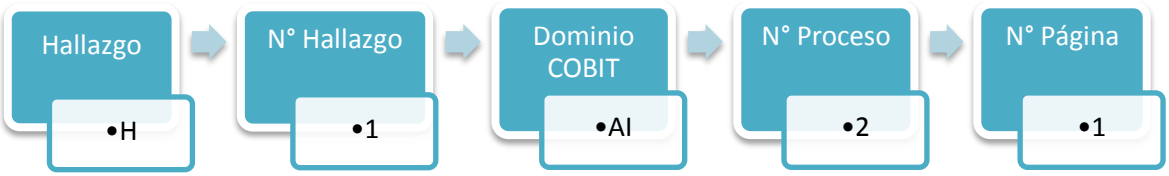


Figura 21. Identificación de hallazgos



TOTALES: calificación de las columnas SI, NO y NA, que se obtiene sumando el puntaje de sus preguntas.
TOTAL CUESTIONARIO: sumatoria del puntaje de todas las preguntas.

Figura 22. Formato cuestionario cuantitativo

HOSPITAL UNIVERSITARIO

CUESTIONARIO CUANTITATIVO	REF

ENTIDAD AUDITADA			
ÀREA AUDITADA		OBJETO DE ESTUDIO	
RESPONSABLES			
MATERIAL DE SOPORTE		FECHA	
DOMINIO		PROCESO	
ENTREVISTADO			

	PREGUNTA	SI	NO	NA	OBSERVACIÓN	RPT
1						
2						
3						
4						
TOTALES						
TOTAL CUESTIONARIO						

El cuestionario cuantitativo, también permite establecer el porcentaje de riesgo y para ello se usa la siguiente fórmula:

$$\%\ \boldsymbol{de\ Riesgo} = \frac{\boldsymbol{Sumatoria\ Columna\ SI} * \mathbf{100}}{\boldsymbol{Total\ Encuesta - Totales\ NA}}$$

Una vez se tenga dicho porcentaje, se determina el nivel de riesgo total, para lo cual se tiene en cuenta la siguiente categorización:

Tabla 10. Niveles de riesgo

Rango	Nivel de Riesgo	Descripción
1% - 30%	Bajo	Deficiencias fáciles de solucionar a largo plazo.
31% - 70%	Medio	Deficiencias que requieren de medidas de solución o mejora a corto plazo.
71% - 100%	Alto	Deficiencias que requieren soluciones inmediatas para reducir el riesgo.

Finalmente se calcula el porcentaje de riesgo total aplicando la fórmula:

$$\%\ \boldsymbol{Riesgo\ Total} = 100 - \%\ de\ Riesgo$$

Con éste resultado se podrá concluir sobre el funcionamiento del proceso evaluado, teniendo como soporte, el conjunto de pruebas que permiten verificar los resultados de la encuesta.

A continuación se muestra como ejemplo, el cuestionario cuantitativo utilizado en la evaluación del proceso DS4 Garantizar la continuidad del servicio:

Figura 23. Cuestionario cuantitativo del proceso DS4

	CUESTIONARIO CUANTITATIVO	REF
HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO E.S.E.		DS4-1

ENTIDAD AUDITADA	Hospital Universitario Departamental de Nariño E. S. E.		
ÁREA AUDITADA	Seguridad Lógica	**OBJETO DE ESTUDIO**	Sistema de información DGH
RESPONSABLES	Edith Friney Díaz Fuelantala y Maira Alejandra Mora Enríquez		
MATERIAL DE SOPORTE	COBIT e ISO/IEC 27002	**FECHA**	Desde el 22 de Marzo hasta el 18 de Julio de 2013
DOMINIO	Entregar y Dar Soporte (DS)	**PROCESO**	Garantizar la Continuidad del Servicio (DS4)
ENTREVISTADO	Coordinador área de gestión de información		

	PREGUNTA	SI	NO	NA	OBSERVACIÓN	RPT
1	¿Existe un plan de contingencias en cuanto a seguridad de la información?		1			H1-(DS4-1)
2	¿Existe procedimientos para realizar *backups*?	5				P1-(DS4-1) P2-(DS4-1)
3	¿Los *backups* se guardan en lugares seguros y adecuados, preferentemente fuera de las instalaciones del hospital?	4				P3-(DS4-1)
4	¿Existe un responsable de administrar los *backups*?	5				P4-(DS4-1)
TOTALES		**14**	**1**	**0**		
TOTAL CUESTIONARIO		**15**				

$$\%\ de\ Riesgo = \frac{14 * 100}{15 - 0} = 93{,}33\%$$

% de Riesgo Total = 100 – 93,33 = 6,67 % (Riesgo Bajo)

AUDITORES RESPONSABLES
EDITH DIAZ
ALEJANDRA MORA

Como se puede observar, cada pregunta con respuesta SI, que no tenga ninguna observación, está soportada por una o varias pruebas que la confirman. Dichas pruebas pueden hacer referencia a un documento, video, audio, imagen o *screenshot*. Para este ejemplo, se tiene lo siguiente:

Tabla 11. Pruebas del proceso DS4

Prueba	Tipo	Descripción	Fuente
P1-(DS4-1) 	Audio	Contiene información referente al proceso de realización de *backups*.	Entrevista aplicada al coordinador del área de sistemas Ing. Roberto Yánez.
P2-(DS4-1) 	Imagen	Diagrama del subproceso copia de seguridad del software de la organización.	Documentación proporcionada por el coordinador del área de sistemas Ing. Roberto Yánez.
P3-(DS4-1) 	*Screenshot*	Disponibilidad de la base de datos en el portal web de la organización.	http://www.hosdenar.gov.co/
P4-(DS4-1) 	Documento	Contiene información sobre actividades, metas, indicadores y responsables de cada subproceso del área de información y sistemas.	Coordinador del área de sistemas Ing. Roberto Yánez.

Las pruebas P2, P3 y P4 pueden visualizarse en el anexo G. Además se encuentran en formato digital, tal como se indica en el anexo E.

En contraste, cada pregunta con respuesta SI, que tenga observaciones, y cada pregunta con respuesta NO conllevan a un hallazgo. Dentro del proceso DS4 únicamente se encontró un hallazgo (H1-(DS4-1)), el cual contiene la siguiente información:

Figura 24. Hallazgo encontrado en el proceso DS4

HALLAZGO	REF
	H1-(DS4-1)

ENTIDAD AUDITADA	Hospital Universitario Departamental de Nariño E. S. E.		
ÁREA AUDITADA	Seguridad Lógica	**OBJETO DE ESTUDIO**	Sistema de información DGH
RESPONSABLES	Edith Friney Díaz Fuelantala y Maira Alejandra Mora Enríquez		
MATERIAL DE SOPORTE	COBIT e ISO/IEC 27002	**FECHA**	Desde el 22 de Marzo hasta el 18 de Julio de 2013
DOMINIO	Entregar y Dar Soporte (DS)	**PROCESO**	Garantizar la Continuidad del Servicio (DS4)

DESCRIPCIÓN
No existe un plan de contingencias en cuanto a seguridad de la información.
CRITERIO
14.1.3 Desarrollo e implantación de planes de continuidad que incluyan la seguridad de la información de la ISO/IEC 27002 y DS4.2 Planes de Continuidad de TI de COBIT 4.1
CAUSA
El plan de contingencias que existe en el hospital sólo contiene un conjunto de normas, procedimientos y acciones básicas de respuesta ante cualquier eventualidad de tipo físico o natural, dejando de lado a los riesgos de tipo lógico.
EFECTO (S)
Al no tener este documento, no se podrá tomar las medidas necesarias para minimizar la probabilidad de que los riesgos a los que está sometido el sistema de información se conviertan en una realidad; y por otra parte el sistema no podría responder eficientemente.
NIVEL DE RIESGO
Alto
RPT
E1-(DS4-1)

AUDITORES RESPONSABLES
EDITH DIAZ
ALEJANDRA MORA

Más adelante, se explicará en detalle cada campo de este formato de hallazgos.

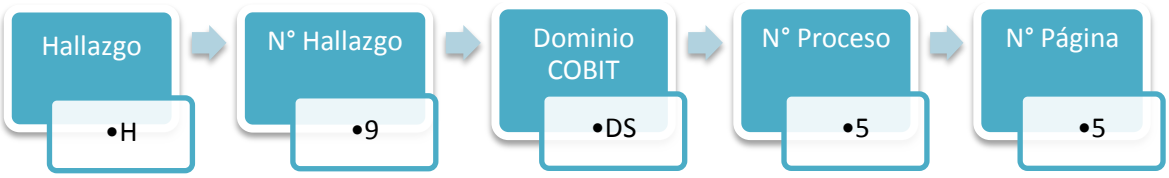
Para observar los cuestionarios cuantitativos empleados en la evaluación de cada criterio de las normas, ver anexo D. Las pruebas y los hallazgos correspondientes pueden encontrarse en el anexo E.

3.2.3.4 Hallazgos. Un hallazgo es la indicación de la inexistencia o inoperancia de un control. Surge como resultado de la comparación que se realiza entre un criterio y la situación actual encontrada por el auditor.

El formato empleado para la descripción de los hallazgos, contiene los siguientes campos:

REF: identificación del hallazgo. En éste campo se utiliza la siguiente nomenclatura:

Figura 25. Identificación del hallazgo



ENTIDAD AUDITADA: nombre de la entidad auditada.
ÁREA AUDITADA: nombre del área a la cual se aplica la auditoría.
OBJETO DE ESTUDIO: identificación de la parte a evaluar.
RESPONSABLES: nombre de los auditores.
MATERIAL DE SOPORTE: normas utilizadas para realizar la auditoría (COBIT 4.1 e ISO/IEC 27002).
FECHA: tiempo en el cual se encontró el hallazgo.
DOMINIO: nombre del dominio COBIT que se está aplicando.
PROCESO: nombre del proceso específico que hace parte del dominio que se está evaluando.
DESCRIPCIÓN (LO QUE ES): aquello que los auditores encontraron o descubrieron.
CRITERIO (LO QUE DEBE SER): marco de referencia utilizado para encontrar la divergencia. En este caso procesos y objetivos de control de las normas COBIT e ISO/IEC 27002.
CAUSA (POR QUÉ): origen de la divergencia encontrada.
EFECTO (LAS CONSECUENCIAS): aquello que se deriva de lo expuesto en la descripción.
NIVEL DE RIESGO: medida de la gravedad de los riesgos identificados en el campo anterior.
RPT: referencia a la evidencia que soporta al hallazgo encontrado. En éste campo se utiliza la siguiente nomenclatura:

Figura 26. Identificación de la evidencia

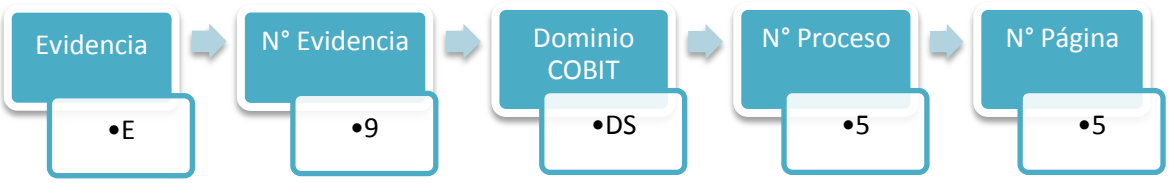


Figura 27. Formato hallazgos

HOSPITAL UNIVERSITARIO	HALLAZGO	REF

ENTIDAD AUDITADA			
ÁREA AUDITADA		OBJETO DE ESTUDIO	
RESPONSABLES			
MATERIAL DE SOPORTE		FECHA	
DOMINIO		PROCESO	

DESCRIPCION
CRITERIO
CAUSA
EFECTO (S)
NIVEL DE RIESGO
RPT

A continuación se retoma como ejemplo, el hallazgo H1-(DS4-1) encontrado en el proceso DS4 Garantizar la continuidad del servicio:

Figura 28. Hallazgo del proceso DS4

HALLAZGO	REF
	H1-(DS4-1)

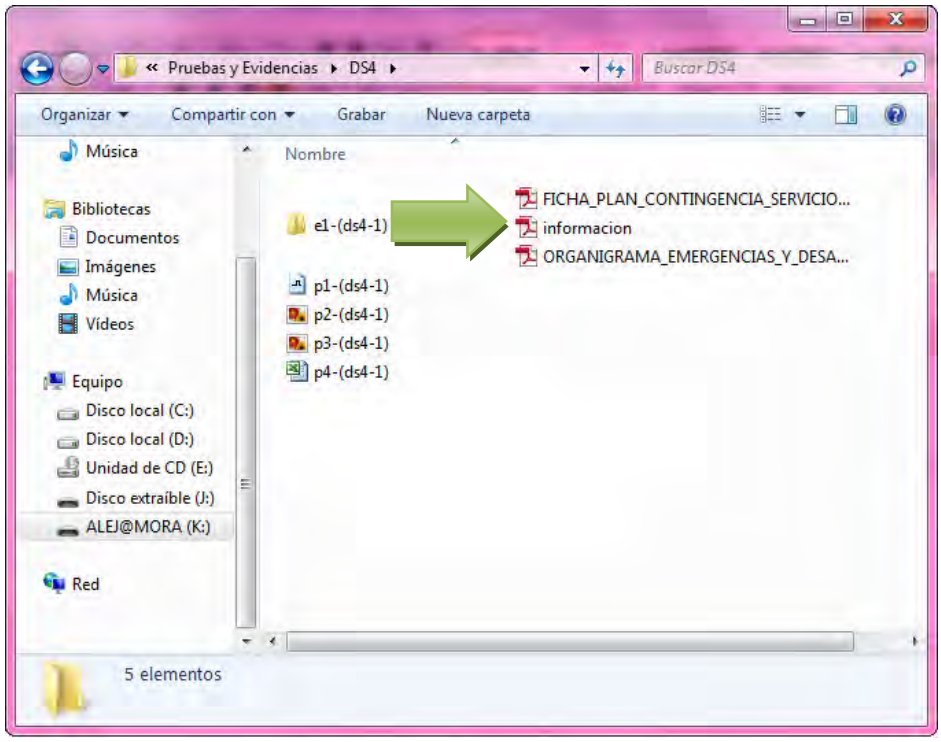
ENTIDAD AUDITADA	Hospital Universitario Departamental de Nariño E. S. E.		
ÁREA AUDITADA	Seguridad Lógica	**OBJETO DE ESTUDIO**	Sistema de información DGH
RESPONSABLES	Edith Friney Díaz Fuelantala y Maira Alejandra Mora Enríquez		
MATERIAL DE SOPORTE	COBIT e ISO/IEC 27002	**FECHA**	Desde el 22 de Marzo hasta el 18 de Julio de 2013
DOMINIO	Entregar y Dar Soporte (DS)	**PROCESO**	Garantizar la Continuidad del Servicio (DS4)

DESCRIPCIÓN
No existe un plan de contingencias en cuanto a seguridad de la información.
CRITERIO
14.1.3 Desarrollo e implantación de planes de continuidad que incluyan la seguridad de la información de la ISO/IEC 27002 y DS4.2 Planes de Continuidad de TI de COBIT 4.1
CAUSA
El plan de contingencias que existe en el hospital sólo contiene un conjunto de normas, procedimientos y acciones básicas de respuesta ante cualquier eventualidad de tipo físico o natural, dejando de lado a los riesgos de tipo lógico.
EFECTO (S)
Al no tener este documento, no se podrá tomar las medidas necesarias para minimizar la probabilidad de que los riesgos a los que está sometido el sistema de información se conviertan en una realidad; y por otra parte el sistema no podría responder eficientemente.
NIVEL DE RIESGO
Alto
RPT
E1-(DS4-1)

AUDITORES RESPONSABLES
EDITH DIAZ
ALEJANDRA MORA

Como se puede observar, el hallazgo está soportado por una evidencia. Las evidencias, al igual que las pruebas, pueden hacer referencia a un documento, video, audio, imagen o *screenshot*. Para este ejemplo, la evidencia E1-(DS4-1) contiene 3 documentos, tal como se indica en la siguiente figura:

Figura 29. Evidencia E1-(DS4-1)



Dichos documentos se adjuntan en el anexo H. Además, están disponibles en formato digital tal como se indica en el anexo E.

➢ **Dominio planear y organizar (PO).** Para ver los hallazgos encontrados en éste dominio y las evidencias que los soportan, ver anexo E.

➢ **Dominio adquirir e implementar (AI).** Para ver los hallazgos encontrados en éste dominio y las evidencias que los soportan, ver anexo E.

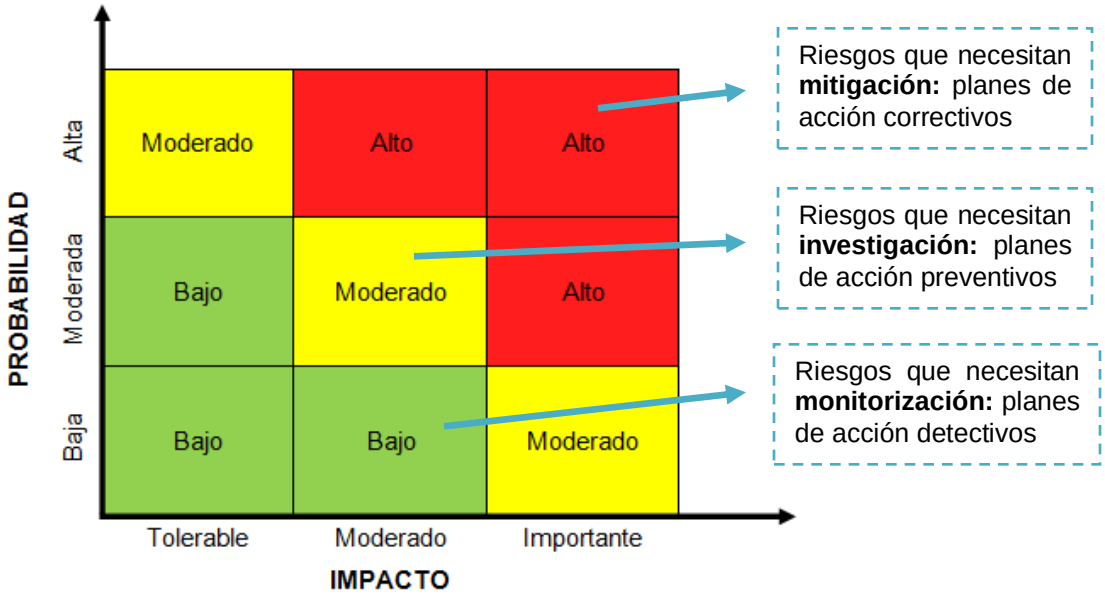
➢ **Dominio entregar y dar soporte (DS).** Para ver los hallazgos encontrados en éste dominio y las evidencias que los soportan, ver anexo E.

➢ **Dominio monitorear y evaluar (ME).** En éste dominio, no se encontraron hallazgos.

3.2.3.5 Matriz de probabilidad e impacto. Es una herramienta de control y gestión que permite visualizar los riesgos a los cuales se enfrenta una organización. Consiste en una gráfica de dos dimensiones (X, Y), en la cual quedan plasmadas las probabilidades de que un evento ocurra, frente a todos los impactos negativos que podría suponer. De ésta forma, los riesgos identificados en cada uno de los procesos COBIT auditados se podrán catalogar como riesgos bajos, moderados o altos.

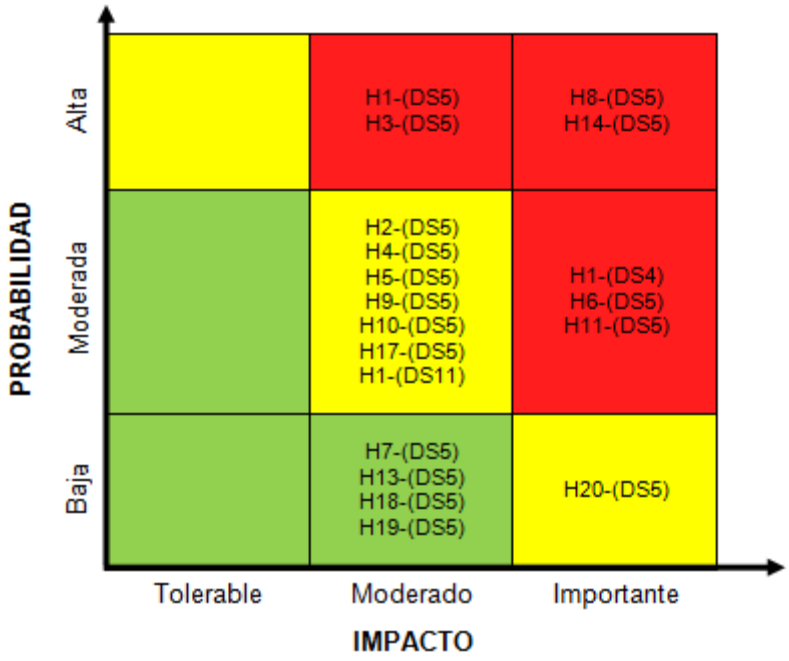
Para la construcción de la matriz, se tuvo en cuenta lo siguiente: el eje X hace referencia al impacto que el riesgo genera; éste puede ser tolerable, moderado o importante. El eje Y representa la probabilidad de ocurrencia del riesgo; dicha probabilidad puede ser baja, moderada o alta.

Figura 30. Matriz de probabilidad e impacto



A continuación se muestra como ejemplo, la matriz de probabilidad e impacto del dominio entregar y dar soporte (DS):

Figura 31. Matriz de probabilidad e impacto del dominio DS



Para observar las matrices de probabilidad e impacto de cada dominio COBIT, ver anexo E. Cabe resaltar que en el dominio Monitorear y Evaluar (ME), no se encontraron riesgos y por lo tanto no se construyó la matriz.

3.2.4 Modelo de madurez del sistema

3.2.4.1 Dominio planear y organizar (PO)

- **Definir la arquitectura de la información (PO2)**

Nivel 4. Administrado y medible. Se da soporte completo al desarrollo e implantación de la arquitectura de información por medio de métodos y técnicas formales. El proceso de definición de la arquitectura de información es proactivo y se enfoca en resolver necesidades futuras del negocio. La organización de administración de datos está activamente involucrada en todos los esfuerzos de desarrollo de las aplicaciones, para garantizar la consistencia. Los sistemas de información ejecutiva y los sistemas de soporte a la toma de decisiones aprovechan la información existente.

- **Definir los procesos, organización y relaciones de TI (PO4)**

Nivel 2. Repetible pero intuitivo. La función de TI está organizada para responder de forma táctica aunque de forma inconsistente, a las necesidades de los clientes. La necesidad de contar con una organización estructurada se comunica, pero las decisiones todavía dependen del conocimiento y habilidades de individuos clave. Surgen técnicas comunes para administrar la organización de TI y las relaciones con los proveedores.

- **Comunicar las aspiraciones y la dirección de la gerencia (PO6)**

Nivel 4. Administrado y medible. La gerencia ha elaborado, documentado y comunicado un ambiente completo de administración de calidad y control de la información, que incluye un marco para las políticas, procedimientos y estándares. El proceso de elaboración de políticas es estructurado, mantenido y conocido por el personal, y las políticas, procedimientos y estándares existentes son razonablemente sólidos y cubren temas clave. Aunque existe un marco general de desarrollo para las políticas y estándares de control, el monitoreo del cumplimiento de estas políticas y estándares es inconsistente.

- **Administrar los recursos humanos de TI (PO7)**

Nivel 2. Repetible pero intuitivo. Existe un enfoque táctico para contratar y administrar al personal de TI, dirigido por necesidades especificas de proyectos, en lugar de hacerlo con base en un equilibrio entendido de disponibilidad interna y externa de personal calificado. Se imparte entrenamiento informal al personal nuevo, quienes después reciben entrenamiento según sea necesario.

- **Evaluar y administrar los riesgos de TI (PO9)**

Nivel 2. Repetible pero intuitivo. Existe un enfoque de evaluación de riesgos en desarrollo. La administración de riesgos se da por lo general a alto nivel y típicamente se aplica sólo como respuesta a problemas. Los procesos de mitigación de riesgos están empezando a ser implementados donde se identifican riesgos.

3.2.4.2 Dominio adquirir e implementar (AI)

- **Adquirir y mantener software aplicativo (AI2)**

Nivel 3. Definido. Existe un proceso claro, definido y de comprensión general para el mantenimiento de software aplicativo. Este proceso va de acuerdo con la estrategia de TI y del negocio. Se intenta aplicar los procesos de manera consistente a través de diferentes aplicaciones y proyectos. Las metodologías son por lo general, inflexibles y difíciles de aplicar en todos los casos, por lo que es muy probable que se salten pasos. Las actividades de mantenimiento se planean, programan y coordinan.

- **Facilitar la operación y el uso (AI4)**

Nivel 4. Administrado y medible. Existe un esquema definido para los procedimientos de mantenimiento y para los materiales de entrenamiento que cuentan con el soporte de la administración de TI. El enfoque considerado para los procedimientos de mantenimiento y los manuales de entrenamiento cubren todos los sistemas y las unidades de negocio, de manera que se pueden observar los procesos desde una perspectiva de negocio. Los procedimientos y materiales de entrenamiento se integran para que contengan interdependencias e interfaces. Existen controles para garantizar que se adhieren los estándares y que se desarrollan y mantienen procedimientos para todos los procesos. Los materiales de documentación y entrenamiento se encuentran generalmente a un buen nivel, predecible, de confiabilidad y disponibilidad. El entrenamiento de negocio y usuario es sensible a las necesidades del negocio.

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

Nivel 5. Optimizado. La administración instituye y da recursos a procesos exhaustivos para la adquisición de TI. La administración impulsa el cumplimiento de las políticas y procedimientos de adquisición de TI. Se toman las medidas en la administración de contratos de adquisiciones, relevantes en casos de negocio para adquisición de TI. Se establece buenas relaciones con el tiempo con la mayoría de los proveedores y socios, y se mide y vigila la calidad de estas relaciones. Se manejan las relaciones en forma estratégica. Los estándares, políticas y procedimientos de TI para la adquisición de recursos TI se manejan estratégicamente y responden a la medición del proceso. La administración del TI comunica la importancia estratégica de tener una administración apropiada de adquisiciones y contratos, a través de la función TI.

3.2.4.3 Dominio entregar y dar soporte (DS)

- **Garantizar la continuidad del servicio (DS4)**

Nivel 3. Definido. La responsabilidad sobre la administración de la continuidad del servicio es clara. Las responsabilidades de la planeación y de las pruebas de la continuidad de los servicios están claramente asignadas y definidas. El plan de continuidad de TI no está documentado. Se han aplicado componentes de alta disponibilidad y redundancia. Se mantiene un inventario de sistemas y componentes críticos.

- **Garantizar la seguridad de los sistemas (DS5)**

Nivel 2. Repetible pero intuitivo. Las responsabilidades y la rendición de cuentas sobre la seguridad, están asignadas a un coordinador de seguridad de TI, pero la autoridad gerencial del coordinador es limitada. Aunque los sistemas producen información relevante respecto a la seguridad, ésta no se analiza. Las políticas de seguridad se han estado desarrollando, pero las herramientas y las habilidades son inadecuadas. La habilitación sobre seguridad está disponible pero depende principalmente de la iniciativa del individuo. La seguridad de TI es vista primordialmente como responsabilidad y disciplina de TI.

- **Educar y entrenar a los usuarios (DS7)**

Nivel 3. Definido. El programa de entrenamiento y educación se institucionaliza y comunica. Los procesos de entrenamiento y educación se estandarizan y documentan. Para soportar el programa de entrenamiento y educación, se establecen presupuestos, recursos, instructores e instalaciones. Se imparten clases formales sobre conducta ética y sobre prácticas de seguridad en los sistemas. El análisis sobre problemas de entrenamiento y educación solo se aplica de forma ocasional.

- **Administrar la mesa de servicio y los incidentes (DS8)**

Nivel 4. Administrado y medible. En todos los niveles de la organización hay un total entendimiento de los beneficios de un proceso de administración de incidentes y la función de mesa de servicio se ha establecido en las unidades organizacionales apropiadas. Las responsabilidades son claras y se monitorea su efectividad. Los procedimientos para comunicar, escalar y resolver incidentes han

sido establecidos y comunicados. El personal de la mesa de servicio está habilitado.

- **Administrar la configuración (DS9)**

Nivel 4. Administrado y medible. En todos los niveles de la organización se reconoce la necesidad de administrar la configuración y las buenas prácticas siguen evolucionando. Se utilizan herramientas automatizadas para fomentar el uso de estándares y mejorar la estabilidad. Los sistemas de administración de configuraciones cubren la mayoría de los activos de TI.

- **Administración de datos (DS11)**

Nivel 5. Optimizado. Se entiende y acepta dentro de la organización la necesidad de realizar todas las actividades requeridas para la administración de datos. Las necesidades y los requerimientos futuros son explorados de manera proactiva. Las responsabilidades sobre la propiedad de los datos y la administración de los mismos están establecidas de forma clara, se conocen ampliamente a lo largo de la organización y se actualizan periódicamente. Los procedimientos se formalizan y se conocen ampliamente. Se utilizan herramientas sofisticadas con un máximo de automatización de la administración de los datos. Se exploran constantemente oportunidades de mejora. El entrenamiento para el personal de administración de datos se institucionaliza.

3.2.4.4 Dominio Monitorear y Evaluar (ME)

- **Monitorear y Evaluar el Desempeño de TI (ME1)**

Nivel 5. Optimizado. Un proceso de mejora continua de la calidad se ha desarrollado para actualizar los estándares y las políticas de monitoreo a nivel organizacional incorporando mejores prácticas de la industria. Todos los procesos de monitoreo están optimizados y dan soporte a los objetivos de toda la organización. Las métricas impulsadas por el negocio se usan de forma rutinaria para medir el desempeño, y están integradas en los marcos de trabajo estratégicos. El monitoreo de los procesos y el rediseño continuo son consistentes con los planes de mejora de los procesos de negocio en toda la organización.

- **Monitorear y Evaluar el Control Interno (ME2)**

Nivel 4. Administrado y medible. La gerencia tiene implantado un marco de trabajo para el monitoreo del control interno de TI. Se ha establecido una función formal para el control interno de TI, con profesionales especializados y certificados que utilizan un marco de trabajo de control formal avalado por la alta dirección. Un equipo calificado de TI participa de forma rutinaria en las evaluaciones de control interno.

3.2.5 Informe general de auditoría

San Juan de Pasto, Julio de 2013

Ingeniero
Roberto Yánez
Ingeniero de sistemas
Coordinador área de sistemas Hospital Universitario Departamental de Nariño
Ciudad

Cordial saludo,

El presente documento es el informe general de la auditoría aplicada a la seguridad del sistema de información Dinámica Gerencial Hospitalaria DGH, cuyo objetivo fue evaluar la eficiencia y eficacia de los procedimientos y controles de seguridad lógica que tiene el sistema, teniendo en cuenta sus recursos, políticas y usuarios.

Para alcanzar el objetivo, el grupo auditor tuvo que identificar y analizar los controles existentes en la seguridad del sistema DGH y comparar dichos controles, procesos y procedimientos con las normas internacionales COBIT 4.1 e ISO/IEC 27002. Una vez hecho lo anterior, se procedió a elaborar un diagnóstico detallado sobre los riesgos a los que se encuentra expuesto el sistema y sus efectos a corto o largo plazo. De esta forma se logró aportar información que permitirá al hospital implementar las medidas necesarias para garantizar seguridad, confiabilidad, confidencialidad e integridad en los datos procesados por el sistema DGH.

Sin embargo, durante el desarrollo de la auditoría se encontraron varios factores limitantes, uno de los más importantes fue que el área de sistemas no suministró información suficiente, pues los funcionarios no tenían autorización para dar esta clase de información. En consecuencia, el diagnóstico realizado sobre el sistema DGH se basa en información digital, entrevistas proporcionadas por el coordinador del área y el software DGH. Cabe resaltar que no se realizaron pruebas sobre el sistema en tiempo real, dado que se instaló el aplicativo y la base de datos en el *laptop* del grupo auditor. Esto, permitió desarrollar la auditoría con normalidad ya que fue la fuente principal de conocimiento y análisis.

Teniendo en cuenta todo lo anterior, a continuación se presentan los resultados de la auditoría realizada entre el 22 de marzo y el 18 de julio de 2013, junto con las recomendaciones que el grupo auditor considera convenientes, basadas en las normas COBIT 4.1 e ISO/IEC 27002.

➢ DOMINIO PLANEAR Y ORGANIZAR (PO)

✓ Proceso COBIT PO4: definir los procesos, organización y relaciones de TI

- **Hallazgo.** No existe un documento en el cual se establezcan las responsabilidades de cada funcionario encargado de cada módulo del sistema DGH.

- **Recomendación.** El área de sistemas podría llevar un manual bien estructurado donde se definan claramente las actividades que debe realizar cada funcionario encargado de cada módulo, permitiendo así manejar un mayor control de los procesos y procedimientos que realizan los usuarios en el sistema DGH.

✓ Proceso COBIT PO7: administrar los recursos humanos de TI

- **Hallazgos**

1. Al instalar el sistema DGH en el *laptop* del usuario, no se percatan de la inseguridad generada al tener datos confidenciales en ellos.

2. No existe en los empleados completa conciencia sobre la importancia de la seguridad de la información.

3. Los usuarios del sistema DGH no conocen totalmente las políticas o normas de seguridad que maneja el hospital.

- **Recomendaciones**

1. Llevar un tipo de control a los usuarios para que se responsabilicen de la información y de lo importante que sería para el hospital, que dicha información no cayera en manos de extraños.

2. Si es posible, el hospital debería adquirir más *laptops* para evitar la instalación del software en los *laptops* de los usuarios y así no correr el riesgo del robo de información.

3. Se recomienda que el área de sistemas programe una capacitación semestral sobre la importancia de la seguridad de la información, con el fin de que el personal del hospital adquiera conciencia.

4. Se recomienda que el área de sistemas evalúe periódicamente el conocimiento de los usuarios del sistema DGH sobre las políticas de seguridad a través de encuestas aleatorias.

✓ **Proceso COBIT PO9: evaluar y administrar los riesgos**

- **Hallazgos**

1. No se ha realizado un estudio sobre las contingencias que son irrelevantes para el hospital.

2. No se ha realizado un estudio formal sobre las contingencias que ocurren con más frecuencia.

- **Recomendaciones**

1. El área de sistemas podría analizar y comparar con otras entidades que han sido víctimas de las contingencias que en el hospital son consideradas irrelevantes por ejemplo el hackeo*, Denial Of Service* y espionajes; con el fin de dar a conocer los posibles daños y concienciar al personal sobre el riesgo que correría el hospital ya que dichos ataques son aleatorios.

2. Se sugiere al hospital realizar un registro de soluciones cada vez que se presente un problema relacionado con el sistema para agilizar los trámites en una futura eventualidad.

➢ **DOMINIO ADQUIRIR E IMPLEMENTAR (AI)**

✓ **Proceso COBIT AI2: administrar los recursos humanos de TI**

- **Hallazgos**

1. No es suficiente la información que se muestra en los *logs* generados por el sistema DGH, ya que a pesar de que se muestra información básica como la fecha, hora, usuario, módulo, OID, doc/consec, acción y detalle, hacen falta datos como por ejemplo: origen de evento (terminal), *login* exitoso, *login* fallido y cambios de contraseña exitosos con sus respectivas fechas de cambio.

2. No se documenta la instalación y/o actualización del software que se instala en los equipos del hospital.

3. Los *logs* no se almacenan externamente.

4. No se genera una estadística y/o un análisis antes de borrar los *logs*.

- **Recomendaciones.**

1. Realizar consultas nuevas de la base de datos para generar nuevos reportes que contengan más información, brindando mayor utilidad en caso de un error o falla realizada por un usuario.

2. En los nuevos reportes deberían existir campos como: identificador de usuario, tipo, fecha de conexión, hora, fecha de desconexión, dirección IP, eventos realizados, módulo al que se accede, menú, submenú, y el ítem de acceso.

3. Realizar un documento de instalación y/o actualización que permita llevar una lista del software necesario para el normal desarrollo de las actividades de los usuarios, conteniendo el nombre de la aplicación, versión, configuración y su respectiva actualización si la tiene, ya que esto permitiría administrar eficientemente los recursos tanto del software como del hardware.

4. Sería conveniente que los *logs* fueran almacenados externamente porque ayudarían a recuperar información de manera rápida y eficiente en caso de que los *logs* almacenados internamente sufran algún daño.

5. Se recomienda llevar un control en los *logs* almacenados antes de su eliminación para obtener un conteo estadístico de los errores más comunes que

cometen los usuarios en el sistema, a fin de mirar si es necesario dar una capacitación al personal.

➢ DOMINIO ENTREGAR Y DAR SOPORTE (DS)

✓ Proceso COBIT DS4: garantizar la continuidad del servicio

- **Hallazgo.** No existe un plan de contingencias en cuanto a seguridad de la información.

- **Recomendaciones**

1. Se recomienda que en el plan de contingencias exista un conjunto de normas, procedimientos y acciones básicas de respuesta que se deberían tomar para afrontar de manera oportuna, adecuada y efectiva, cualquier eventualidad de tipo lógico, que se produzca en el sistema de información, de modo que asegure la continuidad, seguridad y confiabilidad del mismo.

2. El plan de contingencias debería contener detalladamente las etapas del plan, objetivos, metas, análisis de riesgos, plan de respaldo, plan de recuperación, plan de mantenimiento, plan de entrenamiento y responsables.

✓ Proceso COBIT DS5: garantizar la seguridad de los sistemas

- **Hallazgos**

1. No se establece un periodo de tiempo máximo para cambiar la contraseña del sistema.
2. El sistema DGH permite que la contraseña contenga el nombre del usuario o empresa.
3. Si un usuario deja de entrar al sistema DGH, la cuenta no pasa al estado inactivo.
4. No se revisan los *logs* de auditoría para buscar pistas de intentos de intrusión.
5. No se utiliza ningún tipo de *firewall* de hardware.
6. No se monitorea el tráfico de red para detectar intentos de intrusión.
7. Si en un determinado tiempo el usuario no responde, la sesión no se termina.
8. El escaneo de virus en los equipos es realizado por los usuarios y no por el encargado de sistemas.
9. No existe ningún procedimiento para definir el mínimo y máximo de caracteres en la contraseña del sistema.

10. No se deshabilitan los puertos que no son necesarios.
11. No se han realizado pruebas de autohackeo (*White Hacking*).
12. Algunos de los usuarios no pueden cambiar la contraseña sin intervención de un administrador.
13. No se hace ningún chequeo periódico de la red y sus permisos.
14. El usuario puede tener varias sesiones en un mismo equipo.
15. Se puede copiar información digital haciendo uso del puerto USB, SD y lectora CD.
16. Se utiliza un proxy en lugar de un *firewall* de software.
17. No se ha verificado si los datos de autenticación se transfieren encriptados hasta el servidor encargado de autenticar.

- **Recomendaciones**

1. Las contraseñas hay que cambiarlas con una cierta regularidad y, a la vez, hay que procurar no generar reglas secuenciales de cambio. Por ejemplo, crear una nueva contraseña mediante un incremento secuencial del valor en relación a la última contraseña. Por ejemplo: pasar de “01Juitnx” a “02Juitnx”.

2. El área de sistemas puede solicitar validación de contraseñas en el sistema DGH para que no contengan el nombre del usuario o empresa.

3. Solicitar al proveedor el cambio de estado activo a inactivo de forma automática de acuerdo a un tiempo límite en el que un usuario deja de entrar a su cuenta.

4. Se recomienda revisar los l*ogs* de auditoría para buscar posibles intentos de intrusión, con el fin de conocer con certeza si existe algún intento de acceder al sistema del hospital y tomar las medidas pertinentes para prevenirlos.

5. Se recomienda adquirir algún *firewall* de hardware para prevenir posibles ataques externos y aumentar la seguridad de los equipos locales.

6. Se recomienda buscar e instalar un software de monitoreo de red que mejor se adapte a las condiciones del hospital, para disminuir el riesgo y además mejorar la calidad y el funcionamiento de la red.

7. Se recomienda que el área de sistemas solicite crear una función que permita cerrar la sesión del sistema después de un determinado tiempo de inactividad.

8. El escaneo de equipos debe realizarse por un funcionario del área de sistemas al menos cada 20 días para asegurar la limpieza de cualquier amenaza que pueda afectar el funcionamiento o el rendimiento normal de los equipos.

9. Se recomienda que las contraseñas tengan más de 8 caracteres. Para que las contraseñas sean de una longitud adecuada y además sencillas de recordar, se pueden utilizar frases completas que pertenezcan a canciones, poemas o similares, que el usuario sea capaz de evocar fácilmente y que, aunque complejas, le resulten familiares.

10. Se recomienda realizar un escaneo de los puertos en los equipos para identificar los que no son necesarios y bloquearlos, de tal manera que los intrusos no puedan acceder a la red con el fin de robar información o espiar.

11. Se recomienda al hospital realizar pruebas de autohackeo diseñadas de tal manera que permitan poner en evidencia las posibles fallas o errores que pueden existir en el sistema, para de esta forma poder corregirlos oportunamente. Con esto se logra una disminución en las debilidades del sistema y en el riesgo de hackeo por parte de personas malintencionadas.

12. El área de sistemas debería solicitar al proveedor del software la verificación del proceso de cambio de contraseña en algunos roles, ya que usuarios pertenecientes al rol de sicología, atención al usuario, coordinador(a) de área, entre otros, no pueden modificar la contraseña y si un administrador la restablece, quedaría por defecto “123” sin posibilidad de cambio.

13. Se recomienda realizar chequeos periódicos de la red a nivel físico y lógico para poder corroborar que todo esté funcionando de manera eficiente y eficaz y así obtener mejores resultados en todos los trabajos y funciones que se realizan mediante el uso de la red. Además se recomienda revisar los permisos de red para tener una mejor distribución de funciones sobre la red y mejorar la seguridad.

14. Se recomienda crear una regla de control de sesiones para informar al usuario sobre ventajas e inconvenientes que podrían presentarse si no hay cuidado en este proceso.

15. El área de sistemas deberá establecer una norma de control para la copia y uso de información mediante los dispositivos extraíbles como memorias USB, SD, micro SD, CD, DVD.

16. Se recomienda adquirir un *firewall* de software además del proxy existente para aumentar el nivel de seguridad en la red. Por otra parte se debe crear un estándar de configuración para el *firewall*, en el cual se incluyan todas las reglas necesarias para garantizar la máxima utilidad del aplicativo. Dentro de dichas reglas se podría considerar lo siguiente: añadir comentarios a las reglas del *firewall*, mantener actualizado el *firmware* del *firewall*, no utilizar el parámetro *ANY* en ninguna regla específica del *firewall*, deshabilitar los servicios de Telnet o FTP,

habilitar el servicio de registro de eventos con su correspondiente huella de tiempo, entre otras.

17. Se recomienda usar un *sniffer* como *Wireshark* para verificar que los datos de autenticación estén viajando encriptados.

✓ **Proceso COBIT DS11: administración de datos**

- **Hallazgo.** Se verifica la funcionalidad de los *backups* de forma aleatoria.

- **Recomendación.** Se recomienda establecer un horario definido semanalmente para la realización de las pruebas y llevar un registro de las copias funcionales.

➢ **DOMINIO MONITOREAR Y EVALUAR (ME)**

En este dominio, no se encontraron hallazgos.

Esperamos que esta información sirva de apoyo para lograr dar cumplimiento a la misión y visión que esta entidad hospitalaria se ha trazado y mejorar la calidad del servicio prestado a los usuarios.

Agradecemos la colaboración prestada por usted para el desarrollo de este proyecto de auditoría, que fue de gran importancia para nosotras.

Atentamente:

Edith Friney Díaz Fuelantala
Maira Alejandra Mora Enríquez

Auditoras

3.2.6 Informe ejecutivo de auditoría

San Juan de Pasto, Julio de 2013

Señores
Junta directiva
Hospital Universitario Departamental de Nariño
Ciudad

Cordial saludo,

A continuación se dan a conocer los resultados de la auditoría aplicada a la seguridad del sistema de información Dinámica Gerencial Hospitalaria DGH entre el 22 de marzo y el 18 de julio de 2013, cuyo objetivo era evaluar la eficiencia y eficacia de los procedimientos y controles de seguridad lógica existentes en el sistema, teniendo en cuenta sus recursos, políticas y usuarios.

Con respecto a la evaluación de la seguridad del sistema, se observó que la norma para crear contraseñas es adecuada ya que permite incluir números, letras mayúsculas, minúsculas y símbolos dando así la posibilidad de crear contraseñas robustas y menos vulnerables. Sin embargo se debe poner atención a la longitud o número de caracteres pues algunos usuarios usan contraseñas demasiado cortas, por esta razón sería recomendable que exista una restricción para que al menos se manejen a partir de 8 caracteres. Así mismo se recomienda que cada usuario cambie la contraseña periódicamente, y que al momento de restablecerla, ésta se genere aleatoriamente para así poder garantizar que cada usuario cambie su contraseña posteriormente.

Por otra parte, en la evaluación de la continuidad del negocio, se encontró que el hospital cuenta con un plan de contingencias muy bien detallado en caso de que ocurra un atentado o catástrofe natural que afecte las instalaciones, no obstante, para eventos o desastres de tipo lógico como virus, intentos de intrusión, robo de información y mala configuración del sistema, no existen procedimientos

informáticos que garanticen la adecuada recuperación de la información. Por ende sería bueno que el área de sistemas elabore un plan de contingencias para el buen manejo de las tecnologías de información y de las comunicaciones donde se incluya análisis de riesgos informáticos, plan de respaldo, plan de recuperación, plan de mantenimiento, plan de entrenamiento y responsables.

En cuanto a la seguridad de la red, el área de sistemas cuenta con personal calificado dispuesto a mantener la infraestructura física y lógica de la red y para su gestión se utiliza una herramienta llamada directorio activo la cual permite controlar el acceso a la información y compartir recursos de manera segura. Sin embargo existen varias falencias entre las cuales están las siguientes: en primer lugar no se maneja un aplicativo para el control y monitoreo continuo de la red dando como resultado posibles caídas del sistema y vulnerabilidad de la información. En consecuencia, se aconseja disponer de un programa como *Wireshark*, el cual permite analizar y dar solución a problemas en redes de comunicaciones; contiene una interfaz gráfica y muchas opciones de organización y filtrado de información. Además proporciona una vista de todo el tráfico que pasa a través de la red. En segundo lugar no existe un aplicativo *firewall* que ayude a incrementar la seguridad de la red, puesto que este se encarga de controlar las entradas y salidas hacia el exterior e interior de la red, por eso se recomienda adquirir este software. No estaría de más que el hospital permita el desarrollo de una auditoría enfocada a la red existente para poner de manifiesto las fallas y así poder ejecutar acciones preventivas y correctivas que permitan mejorar la calidad y eficiencia de la misma.

Con referencia a la evaluación del conocimiento que maneja el personal sobre seguridad de la información, se encontró que el área de sistemas brinda capacitación al usuario sobre el funcionamiento del sistema DGH durante los primeros días de su vinculación, pero en realidad no existe un dominio y conciencia del tema, por ello el área de sistemas podría crear una programación semestral para capacitar al personal sobre la importancia de la seguridad de la información, con el fin de que adquiera conciencia y se forme un clima organizacional lo suficientemente fuerte como para evitar que los usuarios sean víctimas de las diferentes técnicas de robo de información que se emplean actualmente, como son: la ingeniería social, donde los delincuentes se aprovechan de la inocencia de las personas aplicando fuerza persuasiva; el hackeo, que permite entrar de manera forzada a un sistema de cómputo o a una red; o el *malware,* que es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora o sistema de información. Además se sugiere evaluar periódicamente al personal respecto a las políticas de seguridad existentes en el

hospital a través de encuestas aleatorias para que, de acuerdo a los resultados, se ejecute un plan de acción que permita solventar las deficiencias.

Se espera que esta información haya sido de gran importancia para que el Hospital tome las medidas necesarias y así se asegure la calidad del servicio prestado por el área de sistemas de la empresa.

Atentamente:

Edith Friney Díaz Fuelantala
Maira Alejandra Mora Enríquez

Auditoras

4. CONCLUSIONES

Las normas ISO/IEC 27002 y COBIT brindan un buen modelo a seguir durante un proceso de auditoría de la seguridad lógica de sistemas, debido a que contemplan aspectos como la gestión de activos de información, la protección contra códigos maliciosos, el control de acceso y la gestión de la continuidad del negocio, que son de gran importancia para garantizar una buena gestión de la seguridad de la información.

El sistema de información Dinámica Gerencial Hospitalaria DGH cuenta con controles que permiten gestionar usuarios, roles, permisos y *logs* a través del módulo de Generales y además, existe una utilidad en el sistema operativo llamada Directorio Activo, con la cual se restringen las actividades que el usuario puede hacer en el equipo. Sin embargo, el área de sistemas no documenta las funciones de cada líder de los módulos del sistema y no ha organizado la red de datos corporativa.

El diagnóstico general arrojó como resultado que el Sistema DGH se encuentra en una buena situación en cuanto a seguridad de la información. Sin embargo, existen ciertas deficiencias como: la conciencia del personal y de los usuarios es inadecuada y la red no se administra correctamente; por lo tanto es factible que se presente el robo de información.

El sistema DGH es una buena herramienta ya que permite gestionar las actividades del hospital de forma integral, ordenada y rápida, pero no se aprovechan todas las ventajas por falta de conocimiento y mal manejo del aplicativo, debido a que el personal en su mayoría no tiene experiencia en el manejo de las nuevas herramientas tecnológicas.

Luego de haber realizado un análisis detallado de los criterios no cumplidos, se pudo encontrar que las principales causas fueron las siguientes: El sistema DGH no realiza algunos procesos que ya deberían estar, como por ejemplo validar la longitud de contraseñas, cambios automáticos de estado de cuentas de usuario y cierre de sesiones; el área de sistemas ha presentado negligencia ante la red corporativa; algunos servicios que tiene el sistema no son tomados en cuenta como los reportes de auditoría en el módulo de Generales y los *logs*; no existe documentación respecto a procedimientos cotidianos como instalación y/o

actualización de software, manual de funciones para cada responsable de cada módulo, plan de contingencias basado en los riesgos de tipo lógico y finalmente los usuarios no tiene conciencia de la seguridad de la información.

La correcta aplicación de una auditaría puede dar a conocer detalladamente las fortalezas y vulnerabilidades de un sistema, apoyando el proceso sobre estándares y normas internacionales, las cuales permiten observar cada tarea, actividad y procedimiento, permitiendo así diagnosticar y evaluar el sistema en su entorno y contexto real.

Para realizar una buena auditoría, el grupo auditor debe ser cuidadoso a la hora de elegir los procedimientos y objetivos de control que se van a evaluar, porque dependiendo del área o sistema a auditar, se puede llegar a elegir más procesos o más objetivos de control de los que se requiere, o también elegir algunos que no tienen relación con lo que se debe evaluar.

5. RECOMENDACIONES

Hacer seguimiento de los hallazgos encontrados, para minimizar los riesgos y aumentar el nivel de seguridad lógica.

Tener en cuenta que la seguridad abarca aspectos como: la base de datos, la red, el sistema operativo, la seguridad física y la seguridad lógica. Este proyecto evaluó únicamente la seguridad lógica, por lo tanto se recomienda que se evalúen los demás aspectos para garantizar una verdadera seguridad.

Impartir formación frecuente y obligatoria a todos los empleados relativa a la concienciación en seguridad de la información.

Instalar herramientas de red pasivas para detectar la frecuencia de intentos de acceso remoto y sondeos externos. Esto ayudará a los responsables a obtener un conocimiento profundo sobre las vulnerabilidades que pueden estar expuestas en la red.

Participar activamente en el desarrollo de auditorías externas, para que la evaluación pueda ser profunda y detallada.

REFERENCIAS BIBLIOGRÁFICAS

[1] Construcciones de Salud: Materiales & Sistemas. Bogotá, D.C. Abril, 2010, no. 2. ISSN 21454965.

[2] HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO. Hospital Universitario Departamental de Nariño E.S.E [en línea]. <http://www.hosdenar.gov.co/> [citado en 23 de julio de 2012].

[3] COLOMBIA. HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO. Resolución 0376 (31, mayo, 2010). Por la cual se actualiza el Código de Ética y Valores del Hospital Universitario Departamental de Nariño E.S.E. Pasto, 2010. 8 p. [en línea] <http://www.hosdenar.gov.co/archivos/pdf/codigoetica.pdf> [citado en 23 de julio de 2012].

[4] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 1273. (5, enero, 2009). Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. Diario Oficial. Bogotá, D.C., 2009. no. 47223. p. 1 - 4.

[5] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley estatutaria 1266. (31, diciembre, 2008). Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. Diario Oficial. Bogotá, D.C., 2008. no. 47219. p. 1 - 17.

[6] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 527. (18, agosto, 1999). Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones. Diario Oficial. Bogotá, D.C., 1999. no. 43673. p. 1 - 17.

[7] Introducción a la auditoría de sistemas de información [en línea]. <http://www.escet.urjc.es/~ai/T2Apuntes.pdf > [citado en 23 de julio de 2012].

[8] AYALA Magno. Controles generales [en línea]. <http://www.monografias.com/trabajos11/codif/codif.shtml> [citado en 23 de julio de 2012]

[9] WALES, Jimmy y SANGER, Larry. Auditoría Informática [en línea]. <http://es.wikipedia.org/wiki/Auditor%C3%ADa_inform%C3%A1tica> [citado en 23 de julio de 2012]

[10] SCRIBD. Tipos de Auditorías y Conceptos Básicos [en línea]. <http://es.scribd.com/doc/22224605/2-Tipos-de-Auditoria> [citado en 23 de julio de 2012]

[11] HISPAVISTA. Tipos de Auditoría [en línea]. <http://anaranjo.galeon.com/tipos_audi.htm> [citado en 23 de julio de 2012]

[12] ELIZONDO PANIAGUA, Christian, *et al*. Auditoría gubernamental [en línea]. <http://www.monografias.com/trabajos71/auditoria-gubernamental/auditoria-gubernamental.shtml> [citado en 23 de julio de 2012]

[13] TRIPOD. Auditoría Integral [en línea]. <http://members.tripod.com/~Guillermo_Cuellar_M/integral.html> [citado en 23 de julio de 2012]

[14] HURTADO FLORES, Pablo Emilio. Curso elemental de auditoría [en línea]. <http://www.emagister.com/curso-elemental-auditoria/clasificacion-auditoria> [citado en 23 de julio de 2012]

[15] QUINTERO, Oscar. Auditoría [en línea]. <http://www.monografias.com/trabajos17/auditoria/auditoria.shtml> [citado en 23 de julio de 2012]

[16] RODRÍGUEZ, Juan Manuel. Auditoría laboral [en línea]. <http://www.elergonomista.com/14en01.html> [citado en 23 de julio de 2012]

[17] GESTIÓN Y ADMINISTRACIÓN. ¿Qué es la auditoría ambiental? [en línea]. <http://www.gestionyadministracion.com/auditoria/auditoria-ambiental.html> [citado en 23 de julio de 2012]

[18] IRIARTE SÁNCHEZ, María Julia. Auditoría Médica [en línea]. <http://www.univalle.edu/publicaciones/revista_salud/revista05/pagina11.htm> [citado en 23 de julio de 2012]

[19] SCRIBD. Auditoría de Sistemas [en línea]. <http://es.scribd.com/doc/17449458/Clasificacion-Detallada-de-Auditorias> [citado en 23 de julio de 2012]

[20] VARGAS AVILÉS, Julio Rito. Conceptos Básicos de Auditoría Informática [en línea]. <http://jrvargas.files.wordpress.com/2009/03/conceptos-basicos-de-auditoria-informatica.pdf> [citado en 23 de julio de 2012]

[21] MOYASEVICH B, Iván Dimitrie. Auditoría y Control de Sistemas e Informática [en línea]. <http://perso.wanadoo.es/idmb/a_ing/temas/auditoria_informatica.htm> [citado en 24 de julio de 2012]

[22] JARA GUEVARA, Germán. Auditoría de Sistemas [en línea]. <http://www.oocities.org/espanol/audiconsystem/auditori.htm> [citado en 24 de julio de 2012]

[23] MARTÍNEZ, John Edinson y GIRARLDO, Carlos Andrés. Auditoría de seguridad informática [en línea]. <http://artemisa.unicauca.edu.co/~ecaldon/docs/audit/ponencia_PASSWORD_siti2004.pdf> [citado en 25 de julio de 2012]

[24] SÁNCHEZ, Juan. Auditoría de la seguridad física [en línea]. <http://auditoria3.obolog.com/auditoria-seguridad-fisica-876557> [citado en 25 de julio de 2012]

[25] SISTESEG. Estrategias de seguridad física [en línea]. <http://www.sisteseg.com/fisica.html > [citado en 25 de julio de 2012]

[26] BORGHELLO, Cristian. Seguridad lógica [en línea]. <http://www.segu-info.com.ar/logica/seguridadlogica.htm > [citado en 25 de julio de 2012]

[27] MONTE DE PAZ, Marta. Seguridad Lógica y de Accesos y su Auditoría [en línea]. <http://e-archivo.uc3m.es/bitstream/10016/10653/1/PFC%20Seguridad%20Logica%20y%20de%20Accesos%20y%20su%20Auditoria.pdf> [citado en 25 de julio de 2012]

[28] MINISTERIO DE HACIENDA. Organización de los papeles de trabajo [en línea]. <http://www.igae.pap.minhap.gob.es/sitios/igae/esES/ClnControlGasto Publico/Documents/Norma_organizacion_de_papeles_trabajo.pdf> [citado en 28 de agosto de 2012]

[29] GUZMAN, José. Instrumento de recopilación de información de una auditoría de sistema [en línea]. <simulaciondigigal-practicafinal.blogspot.com> [citado en 25 de julio de 2012]

[30] ROSALES, Omar. Técnicas y Herramientas de Auditoría Informática [en línea]. <http://thaudinfor.blogspot.com/2010/10/herramientas-para-la-auditoria.html> [citado en 2 de agosto de 2012]

[31] CARDONA HERNANDEZ, Gustavo. Entrevista [en línea]. <http://entrevista grupo13.blogspot.com/2010/11/gerg.html>[citado en 2 de agosto de 2012]

[32] CARRANZA, Jeicol. Técnicas de auditoría asistidas por computadora [en línea]. <http://es.scribd.com/doc/49852466/TECNICAS-DE-AUDITORIAS-ASISTIDAS-POR-COMPUTADORAS> [citado en 3 de Agosto de 2012]

[33] ROJAS CÓRSICO, Ivana Soledad. Trabajo de Auditoría: Normas COBIT [en línea]. <http://www.monografias.com/trabajos14/auditoriasistemas/auditoriasistemas.shtml> [citado en 8 de agosto de 2012]

[34] LÓPEZ NEIRA, Agustín y RUÍZ SPOHR, Javier. ISO 27000 [en línea]. <http://www.iso27000.es/iso27000.html> [citado en 3 de agosto de 2012]

[35] INTECO-CERT. Curso de sistemas de gestión de la seguridad de la información según la norma UNE/ISO-IEC 27000 [en línea]. <http://es.scribd.com/doc/33892096/Sgsi-La-Norma-Une-Iso-Iec-27000-Series-Gestion-de-la-Seguridad-de-la-Informacion> [citado en 3 de agosto de 2012]

[36] GUTIERRES SORIA, Carlos, *et al.* Manual de Normas y Políticas de Seguridad Informática [en línea]. <http://ebookbrowse.com/iso-27000-04-po-isc-pit-e-pdf-d28664738> [citado en 3 de agosto de 2012]

[37] COLOME, Reynaldo. ISO/IEC 17799 [en línea]. <http://es.scribd.com/doc/98913591/ISO-17799> [citado en 3 de agosto de 2012]

[38] MONTOYA, Jaime. Estándar internacional ISO/IEC 27002 [en línea]. <http://www.monografias.com/trabajos67/estandarinternacional/estandarinternacional2.shtml> [citado en 3 de agosto de 2012]

[39] WALES, Jimmy y SANGER, Larry. ISO/IEC 17799 [en línea]. <http://es.wikipedia.org/wiki/ISO/IEC_17799> [citado en 3 de agosto de 2012]

[40] SCRIBD. MAGERIT – versión 2 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información: I – Método [en línea]. <http://es.scribd.com/doc/35980867/Metodo-v11-Final> [citado en 15 de agosto de 2012]

[41] MATALOBOS VEIGA, Juan Manuel. Análisis de riesgos de seguridad de la información [en línea]. <http://oa.upm.es/1646/1/PFC_JUAN_MANUEL_MATALOBOS_VEIGAa.pdf> [citado en 15 de agosto de 2012]

[42] CAROLINA DEL PRÍNCIPE. ¿Qué es el MECI? [en línea]. <http://carolinadelprincipe-antioquia.gov.co/apc-aa-files/62623337316331356333623663626436/QUE_ES_EL_MECI.pdf> [citado en 15 de agosto de 2012]

[43] SECURITY ARTWORK. Introducción al análisis de riesgos – Metodologías (I) [en línea]. <http://www.securityartwork.es/2012/03/30/introduccion-al-analisis-de-riesgos-metodologias-i/> [citado en 15 de agosto de 2012]

[44] HISPAVISTA. Riesgos Informáticos [en línea]. <http://auditoriadesistemas.galeon.com/productos2223863.html> [citado en 20 de septiembre de 2012]

[45] SENA, Leonardo y TENZER, Simón Mario. Introducción a Riesgo Informático [en línea]. <http://www.ccee.edu.uy/ensenian/catcomp/material/riesgo.pdf> [citado en 20 de septiembre de 2012]

[46] BALLESTER FERNÁNDEZ, José Manuel. Control y Seguridad [en línea]. <http://www.borrmart.es/articulo_redseguridad.php?id=1374> [citado en 22 de septiembre de 2012]

[47] UNIVERSIDAD CATÓLICA BOLIVIANA SAN PABLO. Capítulo N. 1: Concepto de auditoría en informática y diversos tipos de auditoría [en línea]. <auditoriasistemasucb.pbworks.com/f/Resumencapitulo1.docx> [citado en 22 de septiembre de 2012]

[48] SISTEMAS Y ASESORÍAS DE COLOMBIA S.A. Dinámica Gerencial Hospitalaria [en línea]. <http://pinpoint.microsoft.com/es-co/applications/dinamica-gerencial-hospitalaria-4295016102> [citado en 4 de octubre de 2012]

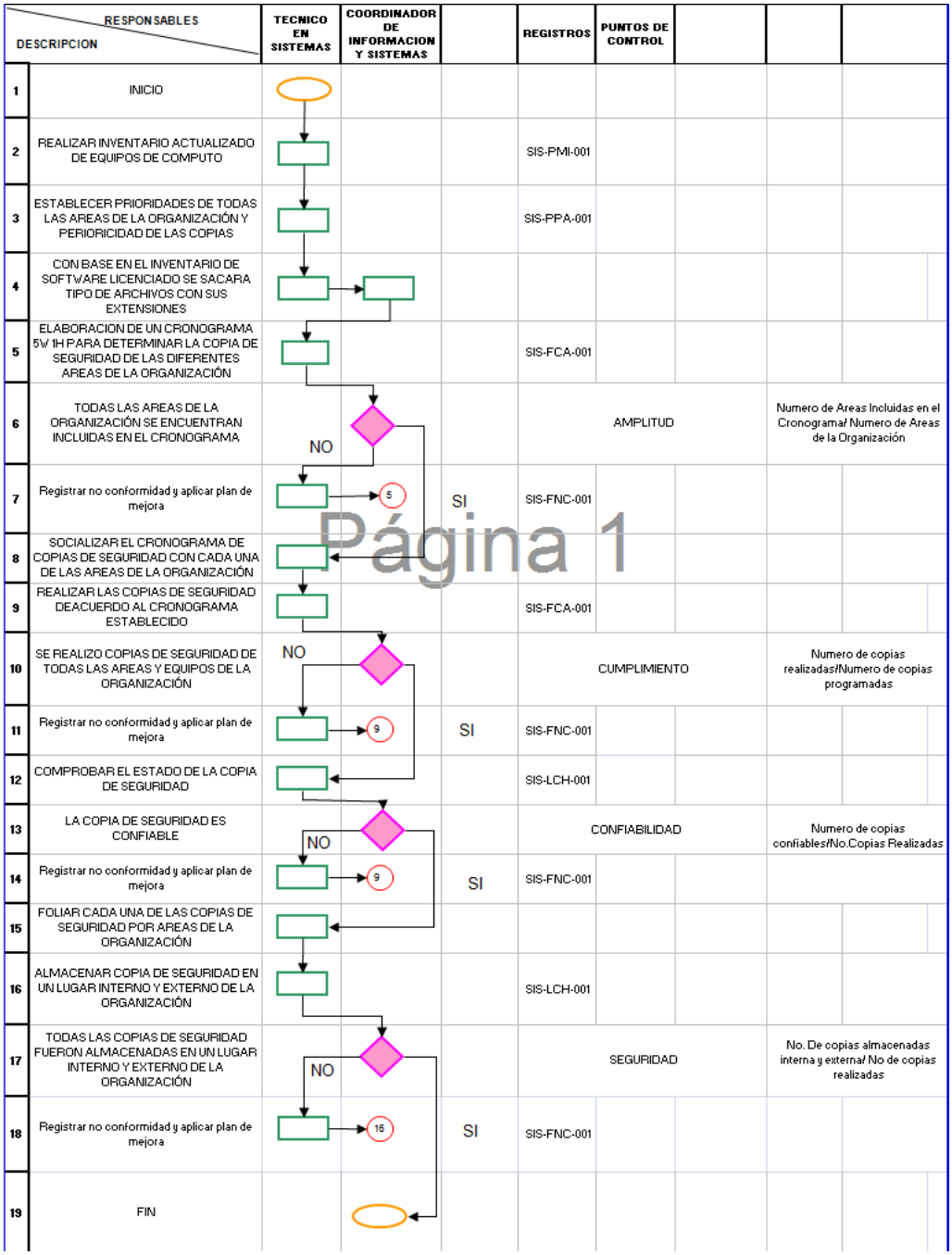
[49] SALAZAR URREA, César Augusto. Dinámica Gerencial Hospitalaria – DGH [en línea]. <http://www.catalogodesoftware.com/producto-dinamica-gerencial-hospitalaria-dgh-669> [citado en 4 de octubre de 2012]

[50] SISTEMAS Y ASESORÍAS DE COLOMBIA S.A. Dinámica Gerencial: Manual de Generales y Seguridad .NET. Colombia, 2011. 48 p.

ANEXOS

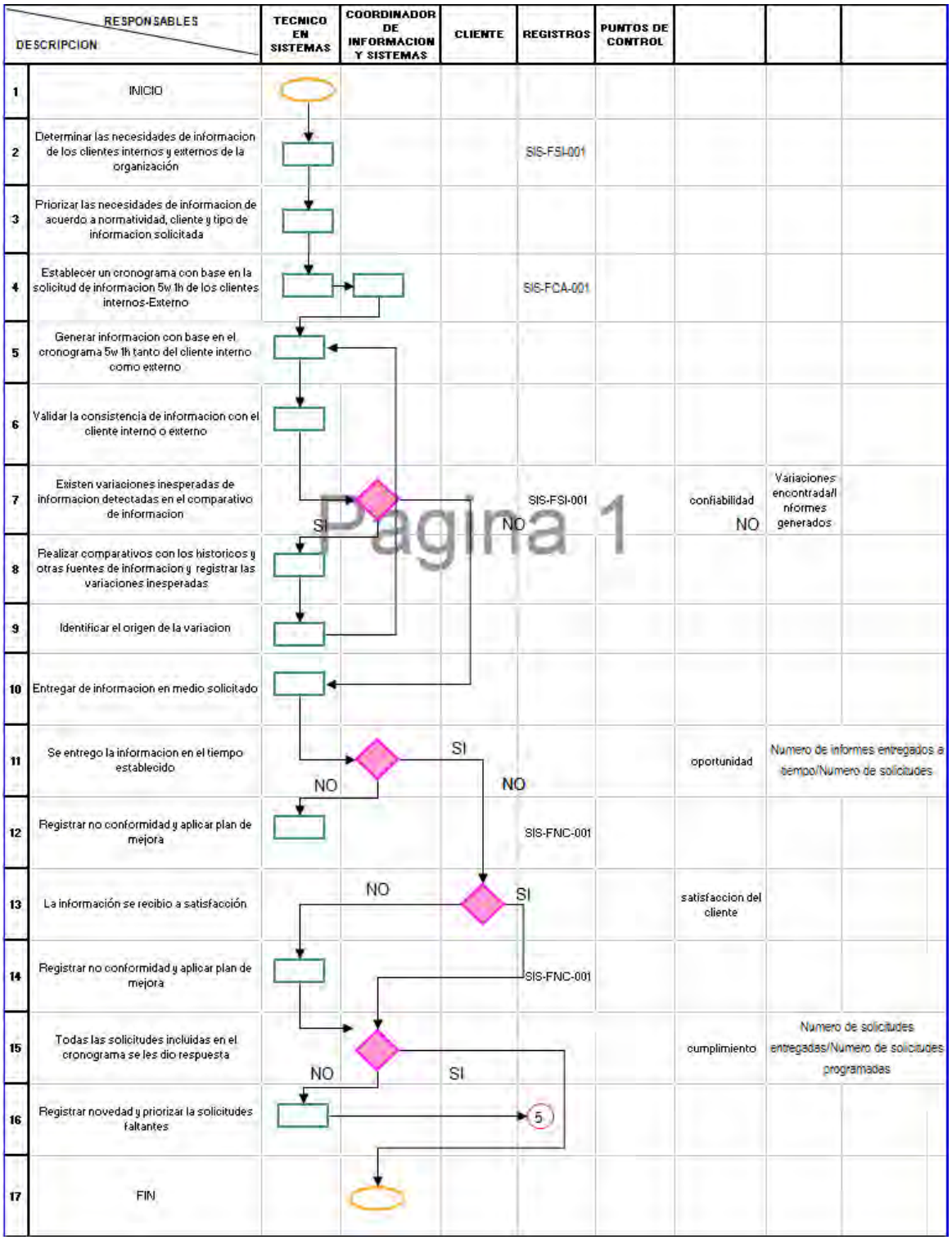
ANEXO A
(Diagrama general de subprocesos del área de información y sistemas)

Subproceso copia de seguridad del software

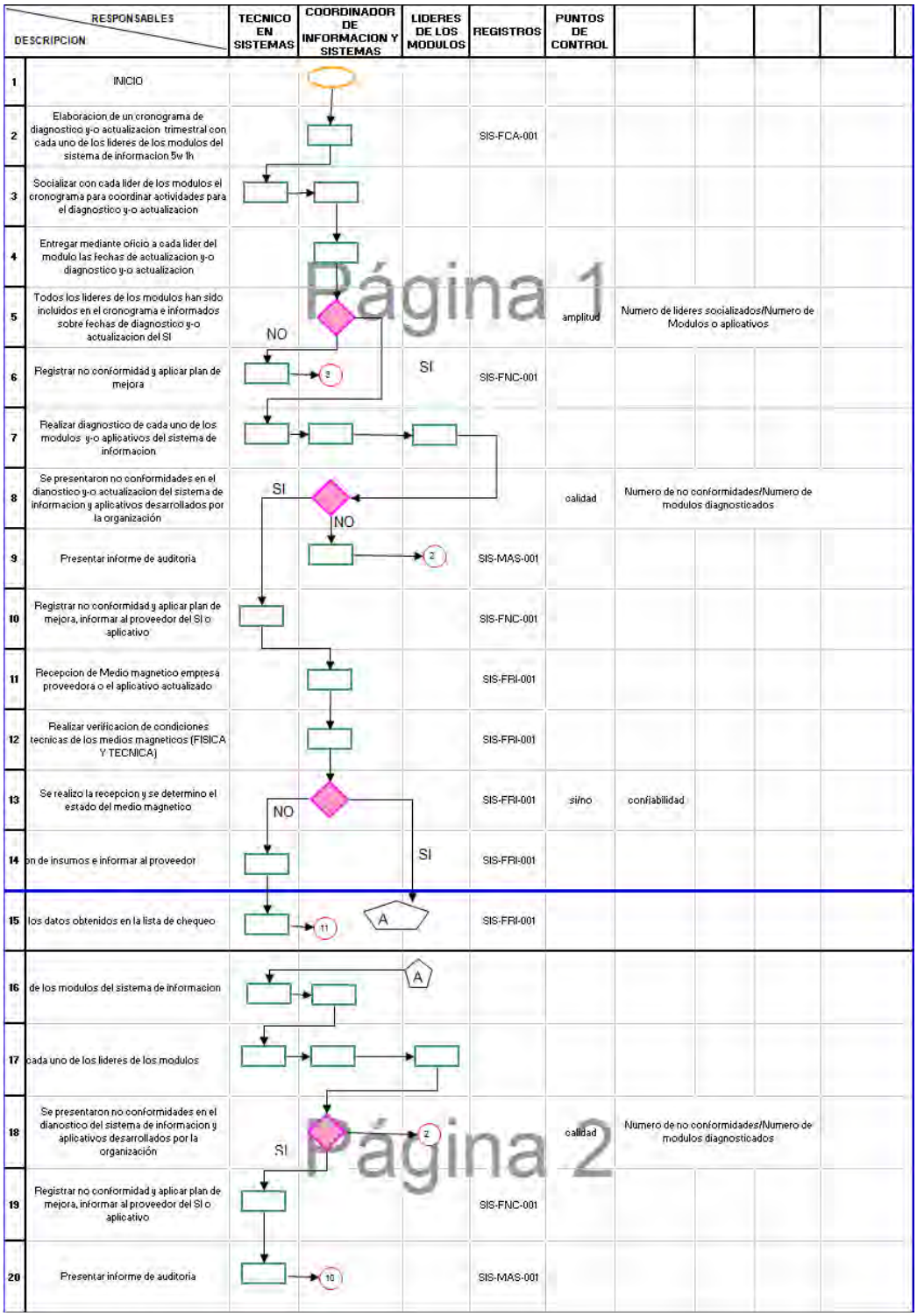


	DESCRIPCION / RESPONSABLES	TECNICO EN SISTEMAS	COORDINADOR DE INFORMACION Y SISTEMAS		REGISTROS	PUNTOS DE CONTROL			
1	INICIO								
2	REALIZAR INVENTARIO ACTUALIZADO DE EQUIPOS DE COMPUTO				SIS-PMI-001				
3	ESTABLECER PRIORIDADES DE TODAS LAS AREAS DE LA ORGANIZACIÓN Y PERIORICIDAD DE LAS COPIAS				SIS-PPA-001				
4	CON BASE EN EL INVENTARIO DE SOFTWARE LICENCIADO SE SACARA TIPO DE ARCHIVOS CON SUS EXTENSIONES								
5	ELABORACION DE UN CRONOGRAMA 5W 1H PARA DETERMINAR LA COPIA DE SEGURIDAD DE LAS DIFERENTES AREAS DE LA ORGANIZACIÓN				SIS-FCA-001				
6	TODAS LAS AREAS DE LA ORGANIZACIÓN SE ENCUENTRAN INCLUIDAS EN EL CRONOGRAMA				AMPLITUD			Numero de Areas Incluidas en el Cronograma/ Numero de Areas de la Organización	
7	Registrar no conformidad y aplicar plan de mejora			SI	SIS-FNC-001				
8	SOCIALIZAR EL CRONOGRAMA DE COPIAS DE SEGURIDAD CON CADA UNA DE LAS AREAS DE LA ORGANIZACIÓN								
9	REALIZAR LAS COPIAS DE SEGURIDAD DEACUERDO AL CRONOGRAMA ESTABLECIDO				SIS-FCA-001				
10	SE REALIZO COPIAS DE SEGURIDAD DE TODAS LAS AREAS Y EQUIPOS DE LA ORGANIZACIÓN				CUMPLIMIENTO			Numero de copias realizadas/Numero de copias programadas	
11	Registrar no conformidad y aplicar plan de mejora			SI	SIS-FNC-001				
12	COMPROBAR EL ESTADO DE LA COPIA DE SEGURIDAD				SIS-LCH-001				
13	LA COPIA DE SEGURIDAD ES CONFIABLE				CONFIABILIDAD			Numero de copias confiables/No.Copias Realizadas	
14	Registrar no conformidad y aplicar plan de mejora			SI	SIS-FNC-001				
15	FOLIAR CADA UNA DE LAS COPIAS DE SEGURIDAD POR AREAS DE LA ORGANIZACIÓN								
16	ALMACENAR COPIA DE SEGURIDAD EN UN LUGAR INTERNO Y EXTERNO DE LA ORGANIZACIÓN				SIS-LCH-001				
17	TODAS LAS COPIAS DE SEGURIDAD FUERON ALMACENADAS EN UN LUGAR INTERNO Y EXTERNO DE LA ORGANIZACIÓN				SEGURIDAD			No. De copias almacenadas interna y externa/ No de copias realizadas	
18	Registrar no conformidad y aplicar plan de mejora			SI	SIS-FNC-001				
19	FIN								

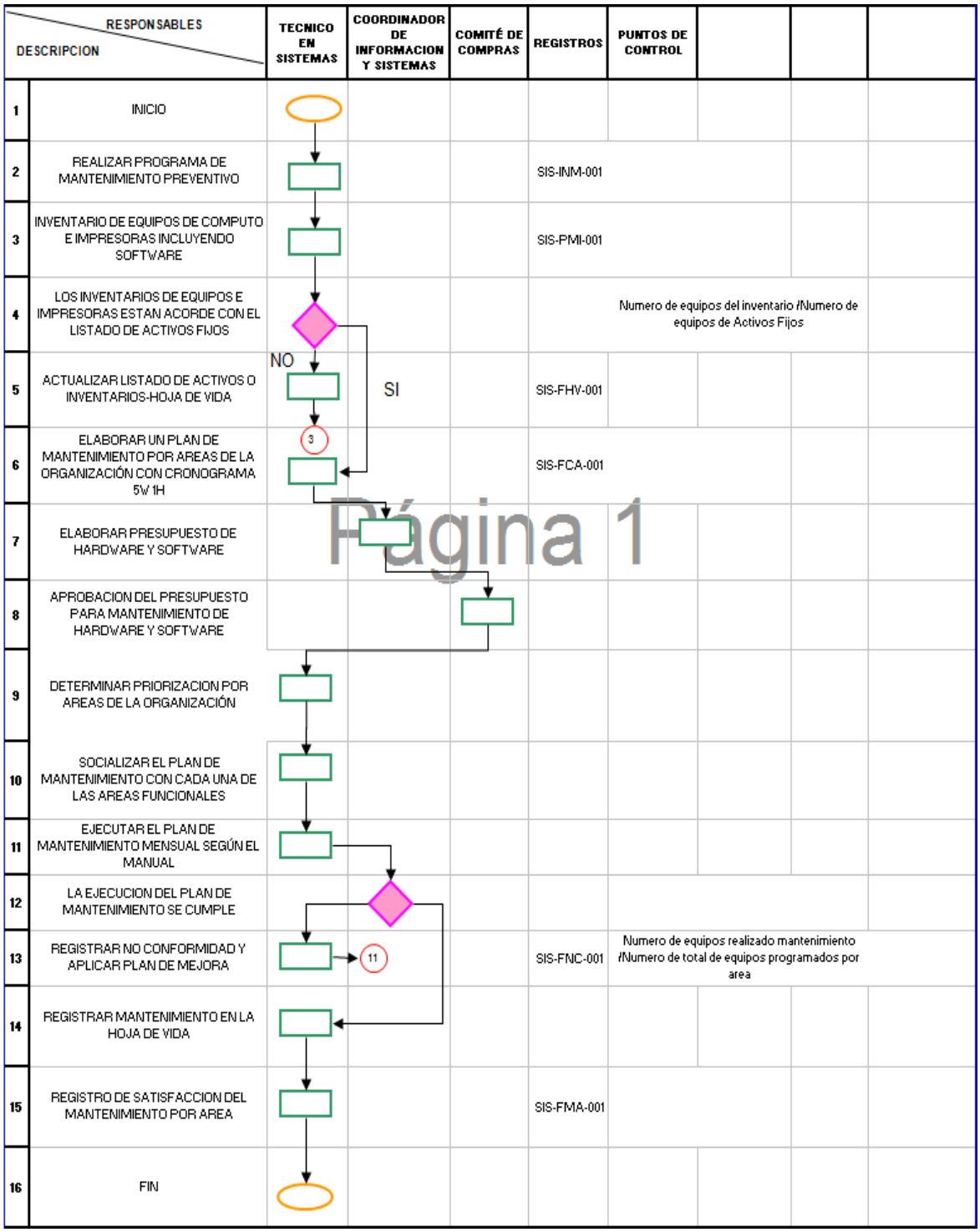
Subproceso producción y entrega de información



Subproceso auditoría de sistemas

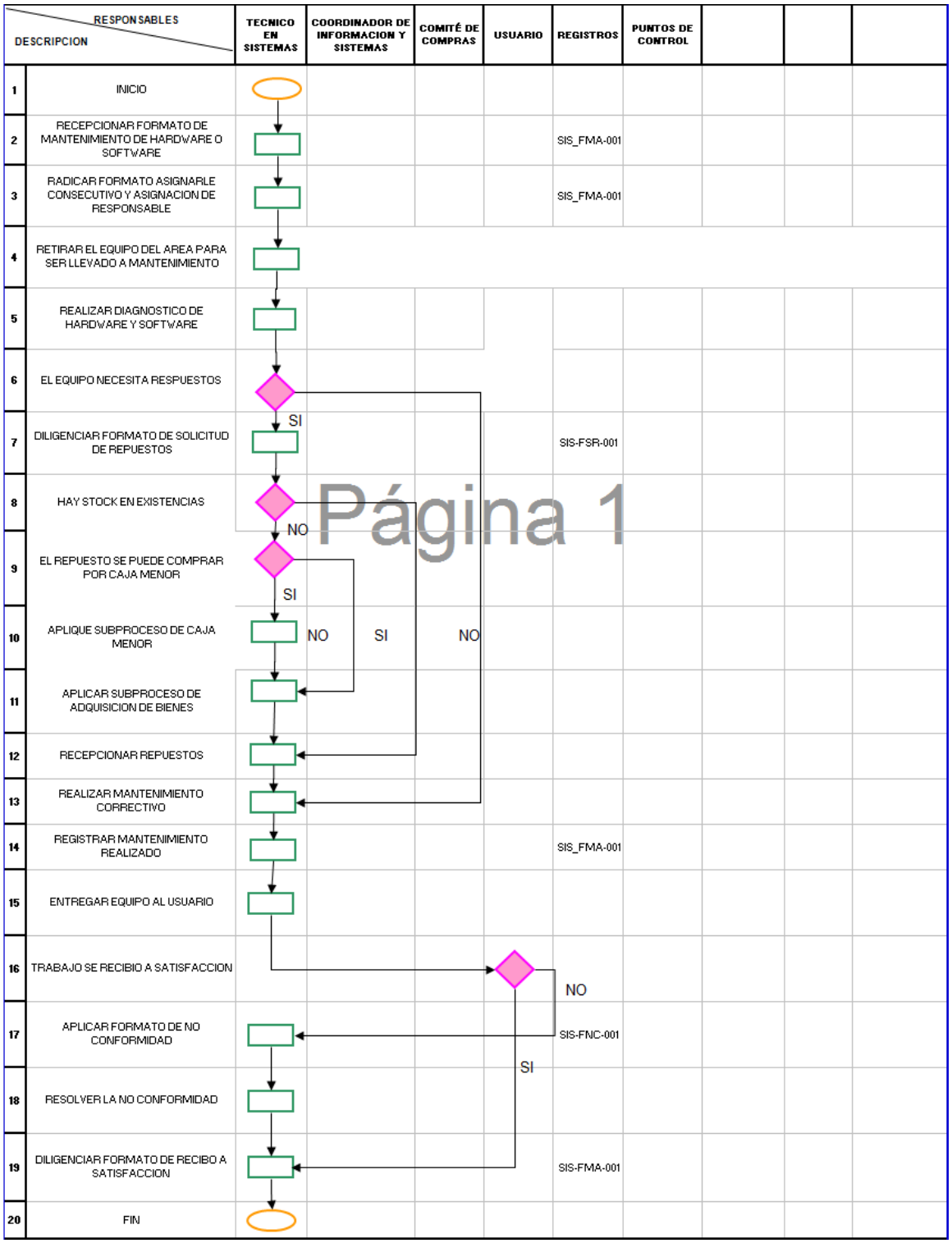


Subproceso mantenimiento preventivo

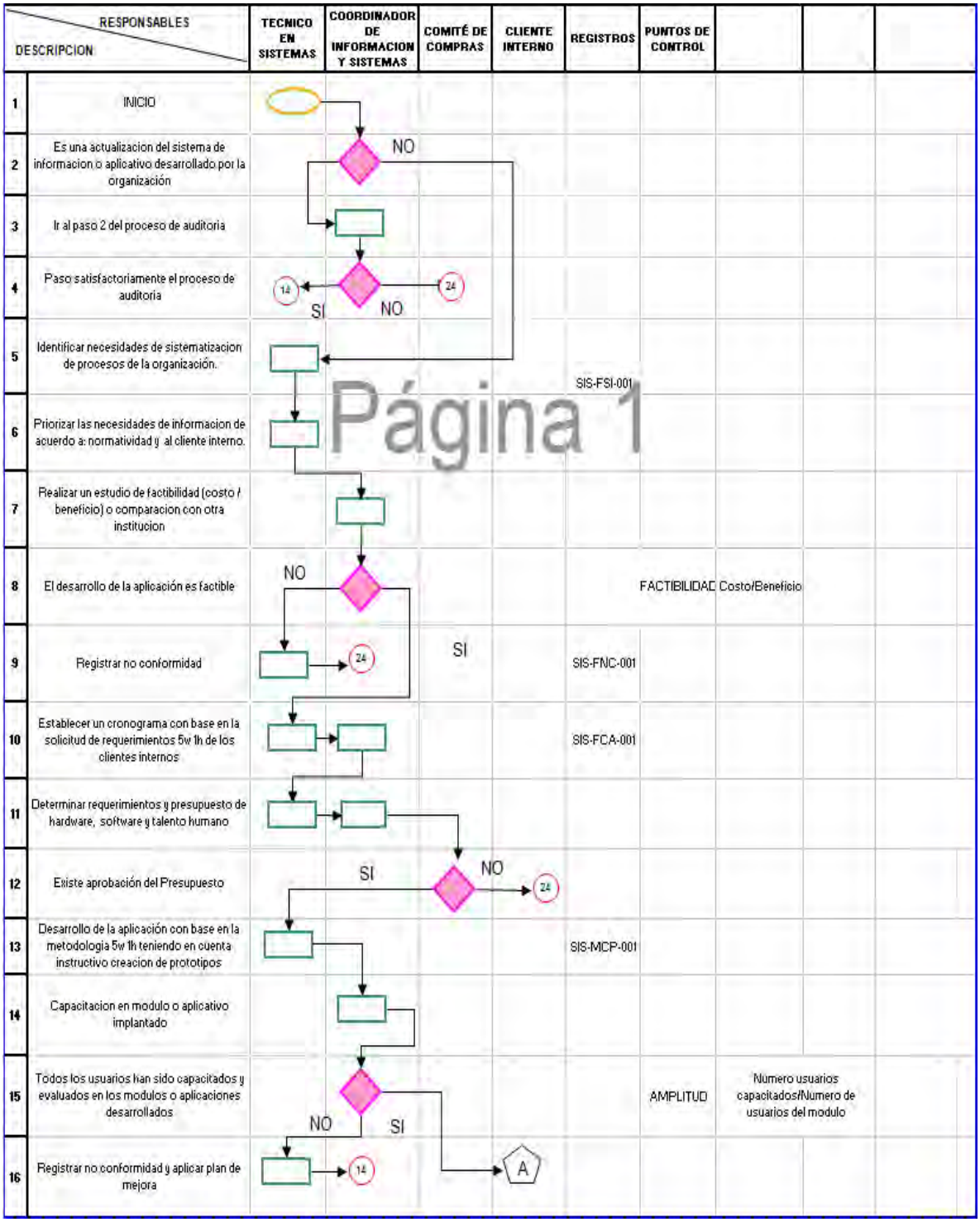


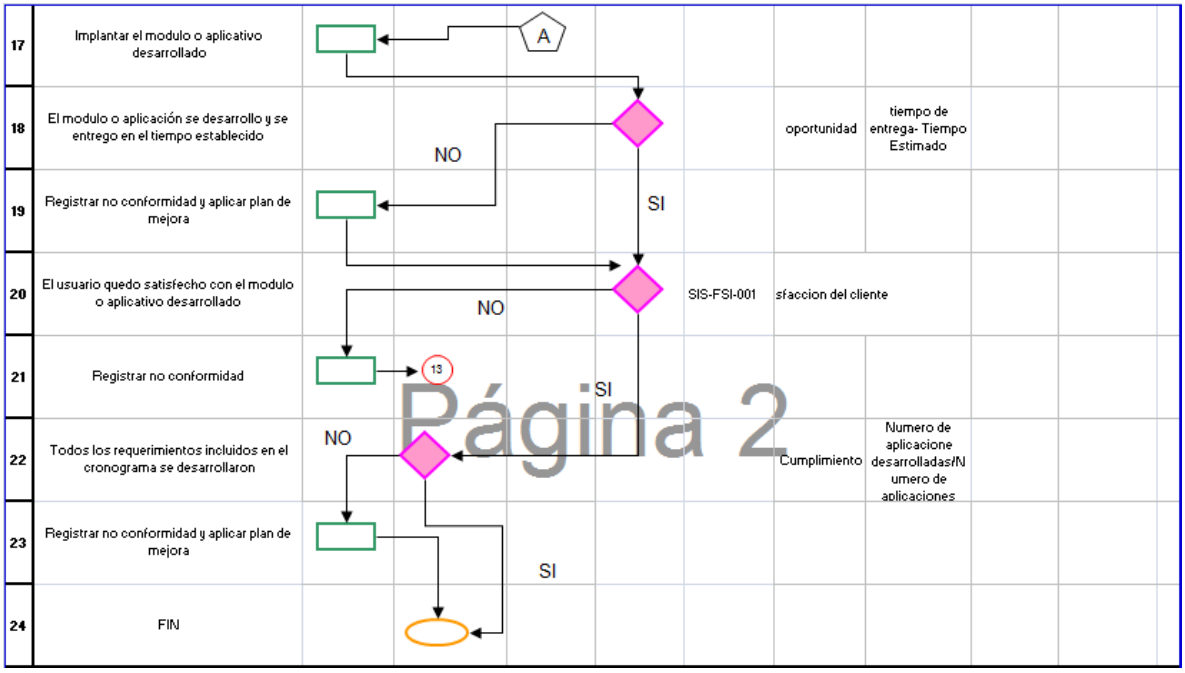
	DESCRIPCION / RESPONSABLES	TECNICO EN SISTEMAS	COORDINADOR DE INFORMACION Y SISTEMAS	COMITÉ DE COMPRAS	REGISTROS	PUNTOS DE CONTROL
1	INICIO					
2	REALIZAR PROGRAMA DE MANTENIMIENTO PREVENTIVO				SIS-INM-001	
3	INVENTARIO DE EQUIPOS DE COMPUTO E IMPRESORAS INCLUYENDO SOFTWARE				SIS-PMI-001	
4	LOS INVENTARIOS DE EQUIPOS E IMPRESORAS ESTAN ACORDE CON EL LISTADO DE ACTIVOS FIJOS					Numero de equipos del inventario /Numero de equipos de Activos Fijos
5	ACTUALIZAR LISTADO DE ACTIVOS O INVENTARIOS-HOJA DE VIDA	NO / SI			SIS-FHV-001	
6	ELABORAR UN PLAN DE MANTENIMIENTO POR AREAS DE LA ORGANIZACIÓN CON CRONOGRAMA 5W 1H	3			SIS-FCA-001	
7	ELABORAR PRESUPUESTO DE HARDWARE Y SOFTWARE					
8	APROBACION DEL PRESUPUESTO PARA MANTENIMIENTO DE HARDWARE Y SOFTWARE					
9	DETERMINAR PRIORIZACION POR AREAS DE LA ORGANIZACIÓN					
10	SOCIALIZAR EL PLAN DE MANTENIMIENTO CON CADA UNA DE LAS AREAS FUNCIONALES					
11	EJECUTAR EL PLAN DE MANTENIMIENTO MENSUAL SEGÚN EL MANUAL					
12	LA EJECUCION DEL PLAN DE MANTENIMIENTO SE CUMPLE					
13	REGISTRAR NO CONFORMIDAD Y APLICAR PLAN DE MEJORA	11			SIS-FNC-001	Numero de equipos realizado mantenimiento /Numero de total de equipos programados por area
14	REGISTRAR MANTENIMIENTO EN LA HOJA DE VIDA					
15	REGISTRO DE SATISFACCION DEL MANTENIMIENTO POR AREA				SIS-FMA-001	
16	FIN					

Subproceso mantenimiento correctivo



Subproceso actualización, implementación e implantación de módulos y aplicativos




17
Implantar el modulo o aplicativo desarrollado
A
18
El modulo o aplicación se desarrollo y se entrego en el tiempo establecido
oportunidad
tiempo de entrega- Tiempo Estimado
NO
SI
19
Registrar no conformidad y aplicar plan de mejora
20
El usuario quedo satisfecho con el modulo o aplicativo desarrollado
SIS-FSI-001
sfaccion del cliente
NO
21
Registrar no conformidad
13
SI
22
Todos los requerimientos incluidos en el cronograma se desarrollaron
NO
Cumplimiento
Numero de aplicacione desarrolladas/Numero de aplicaciones
23
Registrar no conformidad y aplicar plan de mejora
SI
24
FIN

ANEXO B
(Archivo permanente)

Información proporcionada por el Hospital. Dicha información se encuentra en formato digital, organizada en un DVD tal como se indica a continuación:

- *Screenshots* del sistema DGH.
- Código Ética.
- Estatutos de contratación.
- Informe para gerencia.
- Inventario a diciembre del 2012-1.
- Lideres 2012.
- Manual de funciones 2.
- Manual generales y seguridad .net V003.
- Normograma final HUDN.
- Plan de desarrollo definitivo aprobado y publicado.
- Planeación operativa de gestión unificado con datos históricos 2005-2012.
- Planos HUDN.
- Poas 2213 consolidado.
- Política de gestión de información 2011.
- Política en HYS.
- Portafolio HUDN.
- Procesos área de sistemas OK.
- Reconocimientos.
- RPDiccio 2012 (Diccionario de datos, módulo generales).

ANEXO C
(Cuadros de definición de fuentes de conocimiento)

Los cuadros de definición de fuentes de conocimiento contienen las diferentes fuentes de información utilizadas para la evaluación de los criterios seleccionados. Se encuentran en formato digital, organizados en un DVD tal como se indica a continuación:

- AI2
- AI4
- AI5
- DS4
- DS5
- DS7
- DS8
- DS9
- DS11
- ME1
- ME2
- PO2
- PO4
- PO6
- PO7
- PO9

ANEXO D
(Cuestionarios cuantitativos)

Cuestionarios utilizados en la evaluación de los criterios seleccionados. Se encuentran en formato digital, organizados en un DVD tal como se indica a continuación:

- AI2
- AI4
- AI5
- DS4
- DS5
- DS7
- DS8
- DS9
- DS11
- ME1
- ME2
- PO2
- PO4
- PO6
- PO7
- PO9

ANEXO E
(Hallazgos – Pruebas y Evidencias – Matrices)

Contiene los hallazgos encontrados en los criterios evaluados, así como también las diferentes pruebas y evidencias que respaldan el trabajo del grupo auditor. Además, se encuentra la matriz de probabilidad e impacto de cada dominio COBIT evaluado, exceptuando al dominio ME, ya que en él no se identificó ningún riesgo.

Los hallazgos, las pruebas y evidencias de soporte y las matrices se encuentran en formato digital, organizadas en un DVD tal como se indica a continuación:

- Hallazgos – Dominio PO
  - ✓ PO4
  - ✓ PO7
  - ✓ PO9
- Hallazgos – Dominio AI
  - ✓ AI2
- Hallazgos – Dominio DS
  - ✓ DS4
  - ✓ DS5
  - ✓ DS11
- Pruebas y Evidencias
  - ✓ AI2
  - ✓ AI4
  - ✓ AI5
  - ✓ DS4
  - ✓ DS5
  - ✓ DS7
  - ✓ DS8
  - ✓ DS9
  - ✓ DS11
  - ✓ ME1
  - ✓ ME2
  - ✓ PO2
  - ✓ PO4

- ✓ PO6
- ✓ PO7
- ✓ PO9
- ✓ Contraseñas
- ✓ Error_cambio_contraseña_larga
- ✓ *Screenshots* y reportes DGH

- Matriz – AI
- Matriz – DS
- Matriz – PO

ANEXO F
(Entrevistas)

Contiene las diferentes entrevistas realizadas por el grupo auditor. Dichas entrevistas se encuentran en formato digital, organizadas en un DVD tal como se indica a continuación:

- Conociendo Hospital Parte 1
- Conociendo Hospital Parte 2
- Entrevista 1-Audio
- Entrevista 1-Formato
- Entrevista 2-Audio
- Entrevista 2-Formato
- Entrevista 3-Audio
- Entrevista 3-Formato
- Entrevista 4-Audio
- Entrevista 4-Formato
- Entrevista 5-Audio
- Entrevista 5-Formato

ANEXO G
(Pruebas del proceso DS4)

Prueba P2-(DS4-1). Existencia de procedimientos para la realización de *backups.*

HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO E.S.E	PROCESO: GESTION DE INFORMACION	CODIGO:	FECHA DE ELABORACIÓN:
		PRSGI-01	8 DE MAYO DEL 2006
	SUBPROCESO: COPIA DE SEGURIDAD DEL SOFTWARE DE LA ORGANIZACION		FECHA DE ACTUALIZACIÓN:
		VERSIÓN:	8 DE MAYO DEL 2006
		00	HOJA: 1 DE: 2

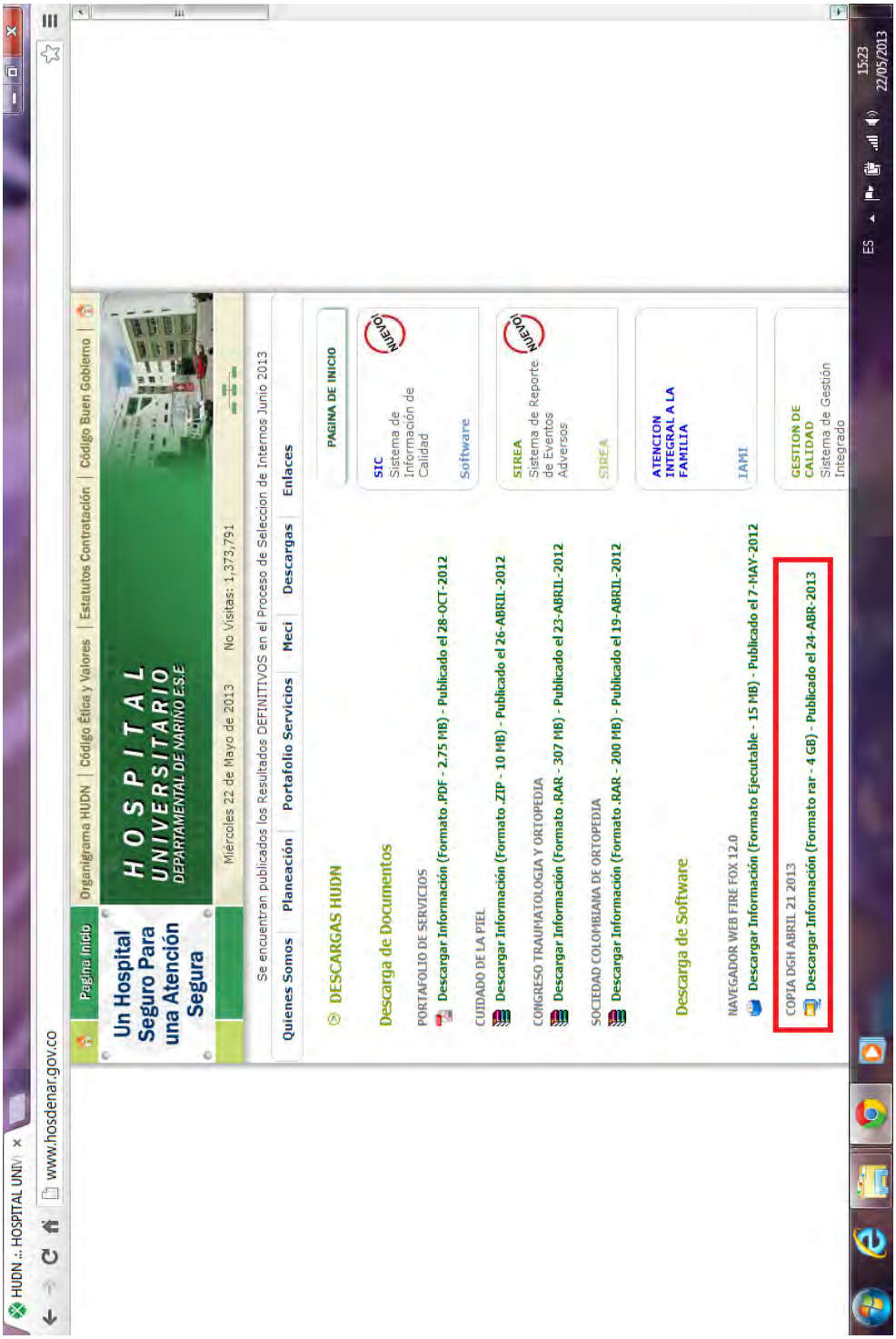
OBJETIVO: Garantizar el respaldo de la informacion registrada en los equipos de computo de la institucion con el fin de obtener seguridad y continuidad en los procesos que requieran de la misma.

ALCANCE: Toda la organización

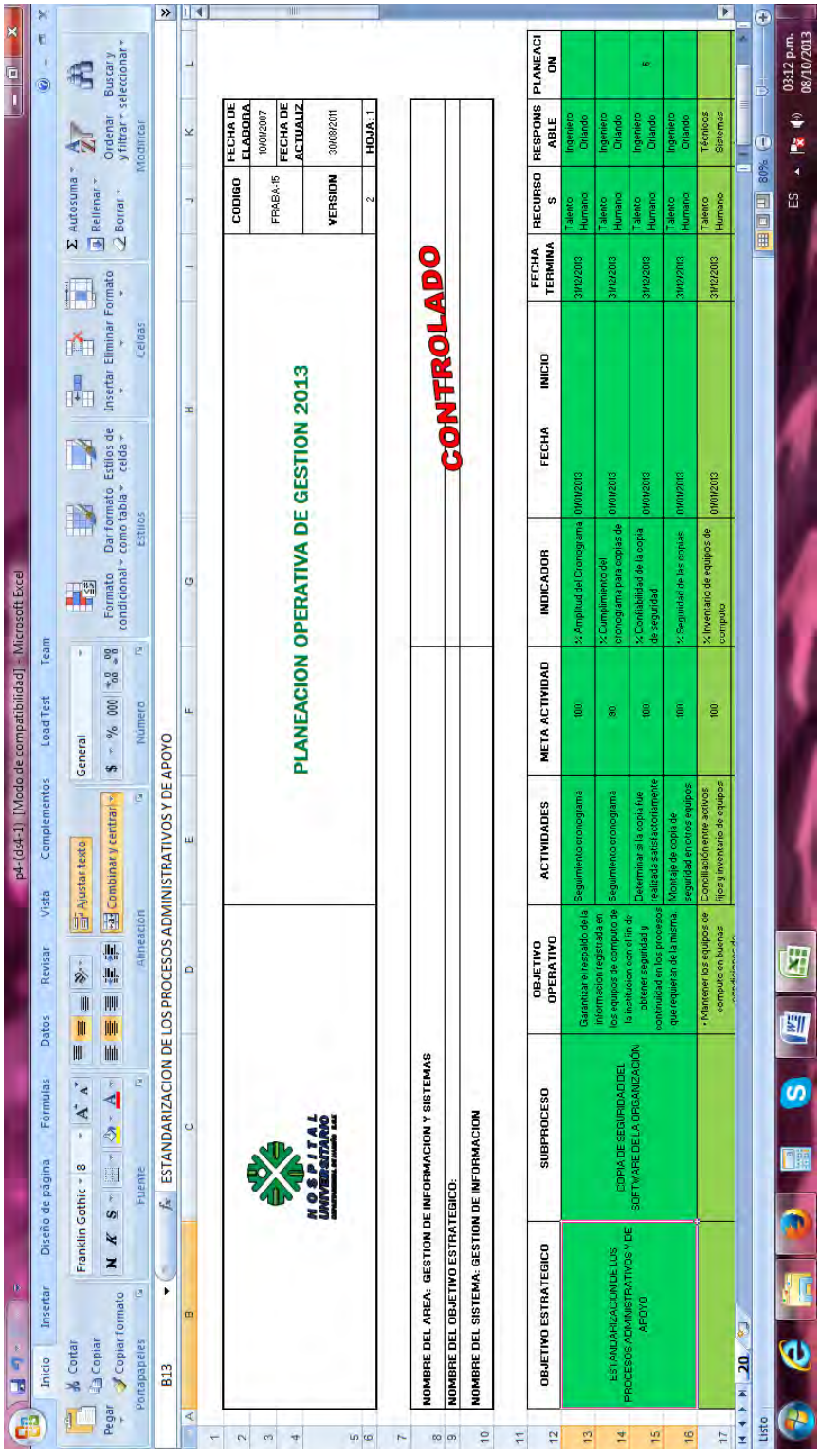
RESPONSABLE: Coordinador de Informacion y sistemas - Tecnicos en Sistemas

	DESCRIPCION / RESPONSABLES	TECNICO EN SISTEMAS	COORDINADOR DE INFORMACION Y	REGISTROS	PUNTOS DE CONTROL		
1	INICIO						
2	REALIZAR INVENTARIO ACTUALIZADO DE EQUIPOS DE COMPUTO			SIS-PMI-001			
3	ESTABLECER PRIORIDADES DE TODAS LAS AREAS DE LA ORGANIZACIÓN Y PERIORICIDAD DE LAS COPIAS			SIS-PPA-001			
4	CON BASE EN EL INVENTARIO DE SOFTWARE LICENCIADO SE SACARA TIPO DE ARCHIVOS CON SUS EXTENSIONES						
5	ELABORACION DE UN CRONOGRAMA 5W 1H PARA DETERMINAR LA COPIA DE SEGURIDAD DE LAS DIFERENTES AREAS DE LA ORGANIZACIÓN			SIS-FCA-001			
6	TODAS LAS AREAS DE LA ORGANIZACIÓN SE ENCUENTRAN INCLUIDAS EN EL CRONOGRAMA	NO		AMPLITUD			Numero de Areas Incluidas en el Cronograma/ Numero de Areas de la Organización
7	Registrar no conformidad y aplicar plan de mejora	5	SI	SIS-FNC-001			
8	SOCIALIZAR EL CRONOGRAMA DE COPIAS DE SEGURIDAD CON CADA UNA DE LAS AREAS DE LA ORGANIZACIÓN						
9	REALIZAR LAS COPIAS DE SEGURIDAD DEACUERDO AL CRONOGRAMA ESTABLECIDO			SIS-FCA-001			
10	SE REALIZO COPIAS DE SEGURIDAD DE TODAS LAS AREAS Y EQUIPOS DE LA ORGANIZACIÓN	NO		CUMPLIMIENTO			Numero de copias realizadas/Numero de copias programadas
11	Registrar no conformidad y aplicar plan de mejora	9	SI	SIS-FNC-001			
12	COMPROBAR EL ESTADO DE LA COPIA DE SEGURIDAD			SIS-LCH-001			
13	LA COPIA DE SEGURIDAD ES CONFIABLE	NO		CONFIABILIDAD			Numero de copias confiables/No.Copias Realizadas
14	Registrar no conformidad y aplicar plan de mejora	9	SI	SIS-FNC-001			
15	FOLIAR CADA UNA DE LAS COPIAS DE SEGURIDAD POR AREAS DE LA ORGANIZACIÓN						
16	ALMACENAR COPIA DE SEGURIDAD EN UN LUGAR INTERNO Y EXTERNO DE LA ORGANIZACIÓN			SIS-LCH-001			
17	TODAS LAS COPIAS DE SEGURIDAD FUERON ALMACENADAS EN UN LUGAR INTERNO Y EXTERNO DE LA ORGANIZACIÓN	NO		SEGURIDAD			No. De copias almacenadas interna y externa/ No de copias realizadas
18	Registrar no conformidad y aplicar plan de mejora	16	SI	SIS-FNC-001			
19	FIN						

Prueba P3-(DS4-1). *Backup* disponible en el portal web de la organización.



Prueba P4-(DS4-1). Existencia del responsable de administrar los *backups*.



p4-(ds4-1) [Modo de compatibilidad] - Microsoft Excel

ESTANDARIZACION DE LOS PROCESOS ADMINISTRATIVOS Y DE APOYO

HOSPITAL UNIVERSITARIO

PLANEACION OPERATIVA DE GESTION 2013

CODIGO	FECHA DE ELABORA
FRABA-I5	10/09/2007
	FECHA DE ACTUALIZ
VERSION	30/08/2011
2	HOJA 1

CONTROLADO

NOMBRE DEL AREA: GESTION DE INFORMACION Y SISTEMAS

NOMBRE DEL OBJETIVO ESTRATEGICO:

NOMBRE DEL SISTEMA: GESTION DE INFORMACION

OBJETIVO ESTRATEGICO	SUBPROCESO	OBJETIVO OPERATIVO	ACTIVIDADES	META ACTIVIDAD	INDICADOR	FECHA INICIO	FECHA TERMINA	RECURSOS	RESPONSABLE	PLANEACION
ESTANDARIZACION DE LOS PROCESOS ADMINISTRATIVOS Y DE APOYO	COPIA DE SEGURIDAD DEL SOFTWARE DE LA ORGANIZACION	Garantizar el respaldo de la informacion registrada en los equipos de computo de la institucion con el fin de obtener seguridad y continuidad en los procesos que requiera de la misma.	Seguimiento cronograma	100	% Amplitud del Cronograma	01/01/2013	31/12/2013	Talento Humano	Ingeniero Orlando	
			Seguimiento cronograma	80	% Cumplimiento del cronograma para copias de	01/01/2013	31/12/2013	Talento Humano	Ingeniero Orlando	
			Determinar si la copia fue realizada satisfactoriamente	100	% Confiabilidad de la copia de seguridad	01/01/2013	31/12/2013	Talento Humano	Ingeniero Orlando	5
			Montaje de copia de seguridad en otros equipos	100	% Seguridad de las copias	01/01/2013	31/12/2013	Talento Humano	Ingeniero Orlando	
		- Mantener los equipos de computo en buenas	Conciliación entre activos fijos y inventario de equipos	100	% Inventario de equipos de computo	01/01/2013	31/12/2013	Talento Humano	Técnicos Sistemas	

ANEXO H
(Evidencia del hallazgo H1-(DS4-1))

En esta sección, se demuestra que la organización cuenta con un plan de contingencias específicamente diseñado para desastres y emergencias de tipo físico.

Ficha plan contingencias servicios 2012.

HOSPITAL UNIVERSITARIO DEPARTAMENTAL DE NARIÑO E.S.E	FICHA PLAN DE CONTINGENCIA DE LOS SERVICIOS ASISTENCIALES Y DEPENDENCIAS ADMINISTRATIVAS	CÓDIGO: FR- 38	FECHA DE ELABORACIÓN: 12 de Enero de 2007	ACREDITACIÓN EN SALUD
		VERSIÓN : 01	FECHA ACTUALIZACIÓN: 15 de enero de 2010	
			HOJA: 10 DE: 77	

RECOMENDACIONES GENERALES ANTE MOVIMIENTOS SÍSMICOS

- Haga que las personas permanezcan dentro del perímetro del hospital; háblele fuerte y calmado.
- Busque refugio bajo o cerca de un elementos no estructural resistente, cama o cerca de una columna, retírese y/o manténgase alejado de las ventanas.
- Si existen evidentes indicios de daño en la estructura (paredes, techos, columnas, etc.), tome la decisión de evacuar y dirija a su grupo al punto de reunión correspondiente.
- Haga que las personas utilicen la salida más próxima.
- Bloquee la entrada al área afectada, e impida que las personas se regresen.
- Si en la vía de salida existe un riesgo inminente, desvíe el tráfico de personas a otra salida, de tal forma que no se vayan a ver afectadas en su integridad por el evento.
- Vaya hasta el sitio de reunión final y verifique la salida del grupo. En caso de alguna anomalía, notifique al Jefe de Emergencias.
- Repórtese al Coordinador de evacuación en el punto de reunión e informe al Puesto de Mando Unificado.
- Espere instrucciones de la organización de emergencias transmítalas al Grupo cuando ello sea procedente.
- Revise que la tubería del alcantarillado esté bien antes de usar los baños o abrir llaves de agua.
- No toque los cables de energía eléctrica derribados ni los objetos que estén en contacto con estos cables. Llame lo antes posible al personal de mantenimiento
- Limpie lo antes posible las medicinas, líquidos inflamables, y cualquier otro material que se haya derramado.
- Mantenga las líneas del teléfono libres a menos que tenga que reportar una emergencia. Verifique que todos los teléfonos estén colgados (es posible que la sacudida los haya descolgado).
- Aléjese de las zonas afectadas. Su presencia podría dificultar la labor de rescate y usted mismo podría ponerse en peligro.
- No utilice el ascensor.

RECOMENDACIONES GENERALES ANTE UN INCENDIO ESTRUCTURAL

- Activar plan hospitalario de emergencia y evacuación.
- Informar de inmediato al Cuerpo de Bomberos.
- Accionar los mecanismos mecánicos y manuales de contra incendio.
- Utilizar los elementos de protección personal.
- Instalar el Puesto de Mando Unificado.
- Apréndase las salidas y los planes de evacuación colocados en sitios visibles cada piso.
- Apréndase la ubicación de todas las salidas del edificio, inclusive a oscuras.
- Asegúrese de que las salidas de incendio no estén bajo llave y estén libres de escombros.
- Asegúrese saber cómo suena la alarma.

Información general sobre gestión de emergencias y desastres

HOSPITAL UNIVERSITARIO

Gestión de Emergencias y Desastres

La **GESTIÓN DE EMERGENCIAS Y DESASTRES** del Hospital Universitario Departamental de Nariño compromete el aseguramiento y desarrollo integral del ser humano y la protección de la infraestructura hospitalaria, mediante la identificación de los factores de riesgo, su mitigación, control y gestión en referencia a salvaguardar la VIDA de los funcionarios, personal medico y paramédico, contratistas, docentes, estudiantes, pacientes hospitalizados, familiares y usuarios flotantes de los servicios esenciales.

Para ello se cuenta con la participación activa del personal interno y con el apoyo externo de diferentes entidades de acuerdo a las necesidades particulares, aplicando valores de solidaridad, humanidad, compromiso y sentido de pertenencia.

VISIÓN

Durante la vigencia del presente Plan de Desarrollo el Hospital Universitario Departamental de Nariño E.S.E, dirigirá sus esfuerzos al mejoramiento continuo, se convertirá en una organización centrada en el usuario, y fortalecerá la implementación de tecnología, de tal manera que complemente de manera armónica la Red de Prestadores de Servicios de Salud del Departamento.

La satisfacción de las necesidades y expectativas de sus grupos de interés será su máxima prioridad y en especial fortalecerá los procesos de gestión clínica, conducentes a garantizar la seguridad de nuestros usuarios.

MISIÓN

El Hospital Departamental de Nariño, es una Empresa Social del Estado, con vocación académica, que complementa, con altos estándares de seguridad a la Red Departamental de Prestadores de Servicios de Salud, en mediana y alta complejidad. Creemos y propiciamos el crecimiento integral de nuestro Talento Humano, lo cual nos permite proyectarnos e incidir en el mejoramiento de la salud y calidad de vida de la comunidad del Sur Occidente Colombiano.

Organigrama Emergencia y Desastres