RESUMEN – TRABAJO DE GRADO

AUTORES	YAN LEONARD VERGEL SANCHEZ RICHAR MAURICIO MARTINEZ PORTILLO
FACULTAD	FACULTAD DE INGENIERIAS
PLAN DE ESTUDIOS	ESPECIALIZACION EN AUDITORIA DE SISTEMAS
DIRECTOR	YESICA MARÍA PÉREZ PÉREZ
TÍTULO DE LA TESIS	GUÍA PRÁCTICA PARA EL CONTROL DE ACCESO AL SISTEMA DE INFORMACION MY PROCESS DEL HOSPITAL EMIRO QUINTERO CAÑIZARES UTILIZANDO COMO HERRAMIENTA LA IESO /IEC 27001:2005

RESUMEN

(70 PALABRAS APROXIMADAMENTE)

EL PRESENTE TRABAJO TIENE POR OBJETIVO LA CREACIÓN DE UNA HERRAMIENTA QUE BRINDE APOYO PARA PODER PROTEGER LA INFORMACIÓN EN EL HOSPITAL EMIRO QUINTERO CAÑIZARES DE OCAÑA, DE LA MEJOR MANERA Y DE ACUERDO A LA SITUACIÓN ACTUAL; TODA VEZ QUE SI YA SE HA COMENZADO DICHO TRABAJO, SE ORIENTE EN ESE CAMINO, BRINDANDO RECOMENDACIONES, EN FORMA SENCILLA Y ENTENDIBLE, ACERCA DE CÓMO MEJORAR LOS PROCESOS PARA PROTEGER LA INFORMACIÓN.

CARACTERÍSTICAS

PÁGINAS: 84	PLANOS: 0	ILUSTRACIONES: 6	CD-ROM: 1

GUÍA PRÁCTICA PARA EL CONTROL DE ACCESO AL SISTEMA DE INFORMACION MY PROCESS DEL HOSPITAL EMIRO QUINTERO CAÑIZARES UTILIZANDO COMO HERRAMIENTA LA IESO /IEC 27001:2005

YAN LEONARD VERGEL SANCHEZ
RICHAR MAURICIO MARTINEZ PORTILLO

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA
FACULTAD DE INGENIERIAS
ESPECIALIZACION EN AUDITORIA DE SISTEMAS
OCAÑA
2015

GUÍA PRÁCTICA PARA EL CONTROL DE ACCESO AL SISTEMA DE INFORMACION MY PROCESS DEL HOSPITAL EMIRO QUINTERO CAÑIZARES UTILIZANDO COMO HERRAMIENTA LA IESO /IEC 27001:2005

YAN LEONARD VERGEL SANCHEZ
RICHAR MAURICIO MARTINEZ PORTILLO

Proyecto de grado presentado como requisito para optar el título de Especialista de Auditoria en Sistemas

Directora
YESICA MARÍA PÉREZ PÉREZ
Especialista

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA
FACULTAD DE INGENIERIAS
ESPECIALIZACION EN AUDITORIA DE SISTEMAS
OCAÑA
2015

CONTENIDO

LISTA DE IMÁGENES

Pág.

LISTA DE ANEXOS

Pág.

INTRODUCCION

La seguridad en cualquier campo de conocimiento y trabajo resulta ser muy importante, dado que representa confianza y disminuye el grado de incertidumbre. El concepto de seguridad es punto fuerte para el desarrollo de las Tecnologías de Información y de las empresas. De esta manera, para que un sistema de información se defina como seguro, debe cumplir con cuatro características: integridad, confidencialidad, disponibilidad y no repudio.

La integridad significa que la información puede ser modificada solo por personal autorizado; la confidencialidad, se refiere al acceso autorizado; la disponibilidad, implica que se puede acceder a la información cuando se necesite; y no repudio, consiste en que el personal no puede negar su acción sobre la información. En este sentido, las tecnologías de información requieren de una coordinación y control adecuados para lograr la seguridad, que se pretende, siendo relevantes tres elementos clave: la información, equipos que la soportan y los usuarios.

Por lo anterior, el objetivo del trabajo de grado, es crear una herramienta que nos brinde apoyo para poder proteger nuestra información de la mejor manera y de acuerdo a nuestra situación actual; y si ya hemos comenzado dicho trabajo, que nos oriente en ese camino, dándonos recomendaciones acerca de cómo mejorar nuestros procesos para proteger la información. Dicha herramienta debe presentar la información de una manera sencilla y entendible para el usuario; además debe ser de fácil distribución, con el propósito de que llegue a más personas, pero principalmente a los alumnos interesados de la Facultad de Ingeniería de la Universidad Francisco de Paula Santander Ocaña, en seguridad Informática.

1. GUÍA PRÁCTICA PARA EL CONTROL DE ACCESO AL SISTEMA DE INFORMACION MY PROCESS DEL HOSPITAL EMIRO QUINTERO CAÑIZARES UTILIZANDO COMO HERRAMIENTA LA IESO /IEC 27001:2005

1.1 PLANTEAMIENTO DEL PROBLEMA

Actualmente el Hospital Emiro Quintero Cañizares, se encuentra modificando sus sistemas de Administración y Control, por lo cual se genera una necesidad de mejorar los controles de acceso, de lo cual cuenta con una serie de vulnerabilidades a la hora de brindar una seguridad eficaz a la información de suma importancia para el normal desarrollo de las actividades diarias.

Proyectándonos en un muy corto plazo y haciendo estudios del caso presentado en el Hospital Emiro Quintero Cañizares consideramos que la empresa pudiera ser vulnerada correspondiente a las bases de datos y la información de total relevancia para el normal desarrollo de sus actividades.

La solución que nosotros planteamos es implementar las ISO/IEC 27001:2005 Y sus políticas en los controles de acceso y con esto brindar una solución efectiva para la seguridad de la información del Hospital Emiro Quintero Cañizares, logrando proveer un desarrollo eficaz en sus actividades de Administración y Control.

1.2 FORMULACION DEL PROBLEMA

¿Es posible que al implementar las ISO/IEC 27001:2005 como herramienta para los sistemas de información MY PROCESS, el HOSPITAL EMIRO QUINTERO CAÑIZARES pueda garantizar las características fundamentales de los sistemas de información?

1.3 OBJETIVOS DE LA INVESTIGACION

1.3.1 General. Diseñar una guía práctica para el control de acceso de los sistemas de información del Hospital Emiro Quintero Cañizares usando como herramienta las ISO /IEC 27001:2005

1.3.2 Específicos. Reconocimiento de las áreas del Hospital Emiro Quintero Cañizares Ocaña, relacionadas con el sistema de información MY PROCESS.

Identificar los factores que ocasionan riesgos en la integridad, confidencialidad y disponibilidad de la información del sistema MY PROCESS, de acuerdo al dominio control de acceso de la ISO 27001:2013.

Documentar la guía práctica que permitirá orientar los procesos y procedimientos para el control de acceso al sistema MY PROCESS del Hospital Emiro Quintero Cañizares Ocaña.

1.4 JUSTIFICACION

Conveniente a la necesidad que presenta el HOSPITAL EMIRO QUINTERO CAÑIZARES correspondiente a la implementación de un nuevo sistema de información y teniendo en cuenta la gran utilidad que este representa para la institución, del cual recibirán beneficios el personal encargado de manipular dicho sistema, como los usuarios de la institución, debido a la agilidad y veracidad a la hora de trasmitir comunicación interna o externa, debido a la actividad que desempeña la institución y con la nueva implementación se fortalecería la estructura organizacional brindando así cualidades con las cuales la empresa, las utilizaría de forma adecuada para enfocar, dirigir, controlar las labores diarias y programas de expansión de sus servicios, además de incrementar su valor patrimonial.

1.5 HIPÓTESIS

1.5.1 A nivel de la Empresa. El Hospital Emiro Quintero Cañizares se beneficiara en primer lugar en obtener un desarrollo seguro y eficaz de sus actividades diarias, ahorraría tiempo, gastos y precisión de la obtención de informes, igualmente permitiría una máxima movilización en los procesos Administrativos, de igual manera simplificaría, ya que mediante las políticas de control de acceso de las ISO/IEC 27001:2005 la empresa contaría con unos sistemas oportunos y confiables.

1.5.2 A nivel de la Especialización. Aplicar y fomentar el desarrollo de los conocimientos adquiridos durante la Especialización Auditoria de Sistemas y el mejoramiento en las investigaciones, y promover la implementación de las políticas de los controles de acceso de las ISO/IEC 27001:2005.

1.5.3 A nivel Personal. Serviría como herramienta principal para la solución en los controles de acceso de los sistemas del Hospital Emiro Quintero Cañizares y como idea para ayudar por medio de nuestra investigación a las directivas a cumplir con una serie de seguridades para un desarrollo eficiente en sus actividades diarias.

1.6 DELIMITACIONES

1.6.1 Geográficas. El proyecto será ejecutado en las instalaciones del Hospital Emiro Quintero Cañizares de Ocaña, en el área de facturación de la sección de urgencias.

1.6.2 Temporales. La investigación cuenta con un tiempo de tres meses a partir de la aprobación del anteproyecto.

1.6.3 Conceptuales. Correspondiente al tema de un nuevo sistema de Administración y Control al momento de implementación de las políticas de control de acceso de las ISO/IEC 27001:2005 se generaron una serie de incógnitas tendientes a mejorar el direccionamiento de nuestro tema de investigaciones por los cuales nos conceptualizamos en temas de políticas y actualidad tendiente una mejor calidad en los procesos de los sistemas del Hospital Emiro Quintero Cañizares.

2. MARCO REFERENCIAL

2.1 MARCO HISTÓRICO

La norma ISO 27001 cubre a todo tipo de organizaciones, este estándar fue confeccionado para proveer un modelo para el establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora del ISMS, La información actualmente es considerada un activo que representa gran valor para cualquier organización. Por tal motivo, se hace necesario protegerla y darle un manejo adecuado a la misma con el fin de evitar impactos significativos que pueden ser causados por agentes externos o interno que permanentemente se encuentran a esperas para aprovechar las vulnerabilidades o puntos débiles que presentan los sistemas de información en las organizaciones. Cabe aclarar, que los sistemas de información están compuestos por activos que cumplen funciones dentro de los mismos. Estos activos son las personas, el hardware, el software, los procesos, la infraestructura y la misma información, entre otros.[1]

Para este proyecto se consideran activos de información los mencionados anteriormente.

Dichos activos están sujetos a ser atacados por amenazas que de no controlarse pueden causar impactos en la información y en efecto a la organización reflejándose en pérdidas económicas y de imagen. Así de esta manera, la alta dirección de cualquier organización debe ser consciente de que su información siempre se encontrará en riesgo y que debe tomar las medidas necesarias para enfrentarse a este tipo de adversidades.

Hablar de seguridad de la información involucra muchos conceptos en especial el delo que significa el riesgo de TI y la manera de administrarlo o gestionarlo en la organización. Existen muchos estudios donde se aplican los conceptos de gestión de riesgos de tecnologías de la información en las organizaciones. Se habla de procesos, metodologías, planes tratamiento, mapas de riesgo, herramientas tecnológicas para riesgos.

2.1.1 Breves Referencias sobre las normativas ISO/IEC 27001 e ISO/IEC 27002

British Standard BS 7799-2 (origen de las ISO actuales). Publicidad por primera vez en 1998.

Normativa Británica
Se divide en 1: Buenas prácticas y 2: Especificaciones
Casi no se utiliza, ha sido reemplazada por la ISO/IEC 27001 Y 27002

ISO/IEC 27001:2005. Especificaciones para los sistemas de gestión de la seguridad de la información, Es una lista completa de los controles a aplicar. Se certifica en esta ISO, emula la BS 7799 parte 2 pero con 2 nuevos conceptos:

[1] http://www.iso27001standard.com/es/que-es-iso-27001/

Indicadores. Es una medida que provee una estimación o evaluación de un atributo (que es a su vez una propiedad o característica de un objeto tangible o intangible) especificado con respecto a las necesidades de información definidas.

Ej: No tener más de 10 infecciones por virus sobre el total de pc's

Métricas. En la ISO/IEC 27001 en el apartado 4.2.2 d) se comenta la necesidad de disponer en métricas de la efectividad, pero no especifica cuales utilizar= en el borrador de la ISO/IEC 27004 se encuentra más pautas.

Ej: Se ha tenido en un año 11 infecciones por virus sobre el total de pc's

ISO/IEC 27002 (actualización año 2007 de la 17799:2005)[2]. Código o guía de buenas prácticas para la gestión de la seguridad de la información. No se certifica en esta ISO

BSI historia. 1901 Nacimiento del BSI
1910 Creación del primer estándar
1926 Inicio del proceso de certificación de productos
1946 Creación de la ISO por parte de miembros del BSI
1979 Primer estándar para sistemas de gerencia (Bs 5750)
1992 Primer estándar sobre el medio ambiente
1999 Elaboración del estándar sobre seguridad de la información (BS 7799)

BSI historia 2. Desarrollo del estandar BS 7799

1993
Reuniones de un grupo multi- sectorial
Primer borrador de codigo de practicas

1995
Publicacion Oficial BS 7799:1 codigo de buenas practicas

1998
Publicacon oficial BS 7799:2 especificaciones SGSI

1999
Publicidad oficial BS 7799:1999 parte 1 y 2

2002
Publicidad de nueva version BS 7799: 2

ISO/IEC 27002: historia.
2000

[2] http://www.welivesecurity.com/la-es/2013/12/12/iso-iec-27002-2013-cambios-dominios-control/

ISO/IEC 17799:2000 código de buenas practicas

2002
UNE ISO/IEC 17799 código de buenas prácticas

2004
UNE 71502 especificaciones SGSI

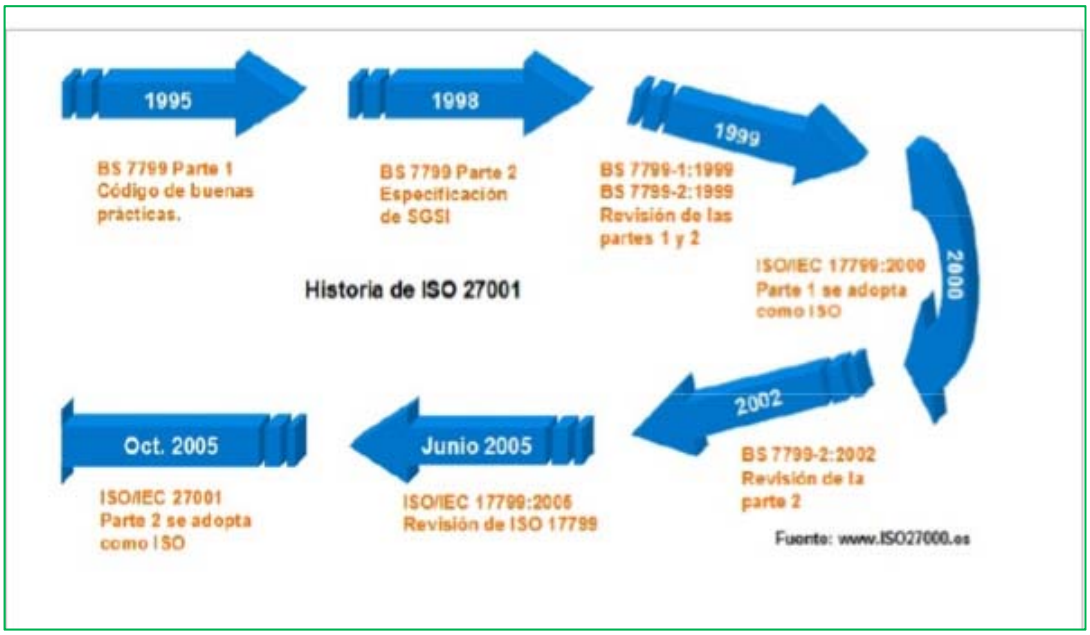
2005
ISO 17799:2005 código de buenas practicas

2005
ISO/IEC 27001 especificaciones SGSI

2007
ISO/IEC 17799 – ISO/IEC 27002

2013
ISO/IEC 27001:2013 borrador final 07/2013, norma a fines de 2013, esta versión tendrá 114 controles en 14 dominios (en la actual versión son 133 controles en 11 dominios)[3]

Imagen 1. Historia de las normas ISO



Fuente: http://www.iso27000.es/iso27000.html

[3] http://www.iso27000.es/iso27000.html

2.2 MARCO CONCEPTUAL

La utilización de controles de acceso evita o controla los riesgos, igualmente ayuda al conocimiento y mejoramiento de la empresa contribuyendo a elevar la productividad y a garantizar la eficiencia y la eficacia en los procesos organizacionales, permitiendo definir estrategias de mejoramiento continuo, brindándole un manejo sistemático adecuado para la entidad.[4]

Teniendo en cuenta que la presente propuesta está enfocada en la administración y disminución de riesgos o vulnerabilidades de la información, también se involucran conceptos relacionados con seguridad de la información.

Integridad: Se considera a la propiedad de salvaguardar la exactitud y estado completo de los activos.

Confidencialidad: Se refiere a la propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

Disponibilidad: Es la propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.

Evento. Presencia o cambio de un conjunto particular de circunstancias.

Consecuencia. Resultado de un evento.

Probabilidad. Oportunidad de que algo suceda.

Amenaza: La fuente de daño potencial o una situación que potencialmente cause Pérdidas.

Causas: Son los medios, las circunstancias y agentes generadores de vulnerabilidades.

Riesgo: Probabilidad de que suceda algún evento que tendrá un impacto sobre los objetivos institucionales o del proceso. Se expresa en términos de probabilidad y consecuencias.

Mejora continua. Acción permanente realizada, con el fin de aumentar la capacidad para cumplir los requisitos y optimizar el desempeño.

2.3 MARCO CONTEXTUAL

ISO/IEC 27001. Basada en la parte 2 del estándar BS 7799.

[4] http://www.codejobs.biz/es/blog/2012/09/07/seguridad-informatica-que-es-una-vulnerabilidad-una-amenaza-y-un-riesgo

Especifica los requerimientos para establecer, implementar y documentar los sistemas de gestión de la seguridad de la información

Indica los controles de seguridad a implementar por las organizaciones dependiendo de sus necesidades

Es certificable.

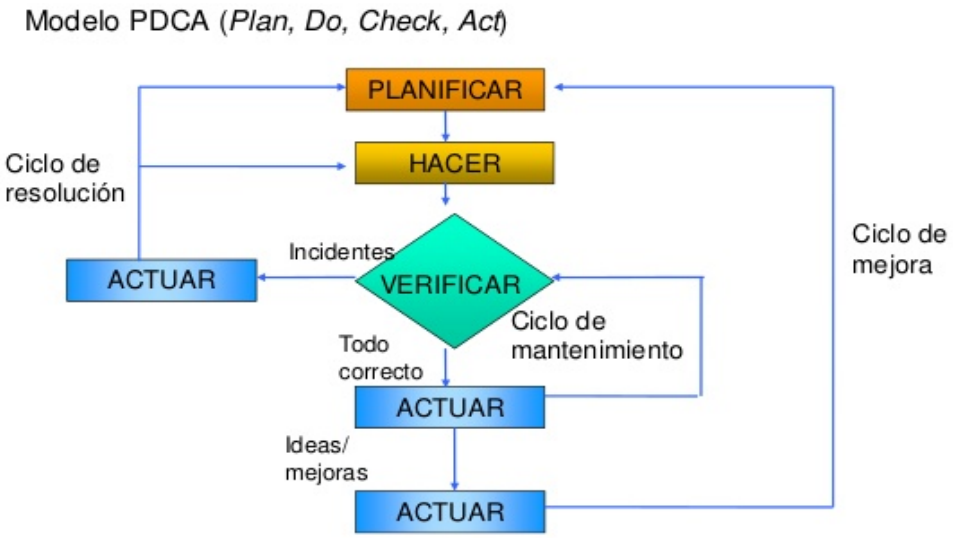
ISO/IEC 27002:2005 SGSI. Como resultado de la implementación de esta normativa se obtiene un sistema de gestión de la seguridad de la información (SGSI)

Una estructura organizativa donde las funciones, responsabilidades, autoridad, etc. De las personas están definidas en procesos y recursos necesarios para lograr los objetivos

Metodología de medida y de evaluación para valorar los resultados frente a los objetivos, incluyendo la realimentación de resultados para planificar las mejoras del sistema

Un proceso de revisión para asegurar que los problemas se detectan y se corrigen, y las oportunidades de mejora se implementan cuando están justificadas.[5]

Imagen 2. Modelo PDCA, ISO/IEC 27002:2005



Fuente: OJEDA PÉREZ, Jorge Eliécer. Delitos informáticos y entorno jurídico vigente en Colombia. (online) [Bogotá] 2010, [citado 23 jun., 2014]. Disponible en: http://www.sci.unal.edu.co/scielo.php?script=sci_arttext&pid=S0123-14722010000200003&lng=es&nrm=iso

[5] OJEDA PÉREZ, Jorge Eliécer. Delitos informáticos y entorno jurídico vigente en Colombia. (online) [Bogotá] 2010, [citado 23 jun., 2014]. Disponible en: http://www.sci.unal.edu.co/scielo.php?script=sci_arttext&pid=S0123-14722010000200003&lng=es&nrm=iso

Imagen 3. Estructura del análisis de riesgos.

Fuente: OJEDA PÉREZ, Jorge Eliécer. Delitos informáticos y entorno jurídico vigente en Colombia. (online) [Bogotá] 2010, [citado 23 jun., 2014]. Disponible en: http://www.sci.unal.edu.co/scielo.php?script=sci_arttext&pid=S0123-14722010000200003&lng=es&nrm=iso

Imagen 4. Visión global de una auditoría.

Fuente: OJEDA PÉREZ, Jorge Eliécer. Delitos informáticos y entorno jurídico vigente en Colombia. (online) [Bogotá] 2010, [citado 23 jun., 2014]. Disponible en: http://www.sci.unal.edu.co/scielo.php?script=sci_arttext&pid=S0123-14722010000200003&lng=es&nrm=iso

2.3.1 Organización de la Seguridad. Objetivo: Definir la estructura de la seguridad de la información dentro de la organización, así como asegurar el nivel de seguridad de la información para las situaciones en las que terceras organizaciones acceden a la información.[6]

Aspectos Destacados. Estructura referente a la seguridad (comités de seguridad)
Seguridad con terceras organizaciones
Gestión de Activos
Objetivo: Mantener el nivel apropiado de seguridad en los activos de la organización
Aspectos Destacados
Inventario de activos
Propietario de los activos
Clasificación de los activos
Manejo de los activos

2.3.2 Seguridad del Personal. Objetivo: Tratar de asegurar que durante todo el ciclo de vida de los trabajadores de la organización, se trata de minimizar los riesgos que puedan provocar estos

Aspectos Destacados. Antes de entrar a trabajar (términos de empleo)
Durante la realización del trabajo (formación, proceso disciplinario)
Finalización de la actividad laboral (retorno de los activos, derechos de acceso)

2.3.3 Seguridad Fisica. Objetivo: Prevenir accesos no autorizados, daños o interferencias en la organización o en los servicios de la misma

Aspectos Destacados. Áreas seguras (controles d entrada)
Protección contra incidentes ambientales
Protección de los equipos
Seguridad del cableado
Eliminación de equipos

2.3.4 Comunicación y Operaciones. Objetivo: Asegurar la correcta realización de las operaciones de la organización así como las comunicaciones que se realicen

Aspectos Destacados. Procedimientos operacionales
Segregación de entornos
Cambios en los sistemas (planificación de capacidades)
Protección contra software malicioso
Copias de seguridad
Gestión de la red
Dispositivos móviles

[6] Ibid., p.3.

Intercambio de información (correo electrónico, comercio electrónico, correo ordinario etc.)
Monitorización (gestión de logs)[7]

2.3.5 Control de Acceso. Objetivo: Controla el acceso a la información de la organización así como los permisos de los usuarios

Aspectos Destacados. Política de control de acceso
Gestión de usuarios (identificadores, privilegios, gestión de contraseñas)
Control de acceso a los servicios de red (enrutado, protección de puertos, segregación de redes, etc.)
Controles de acceso a diferentes niveles (sistema operativo, aplicación, información)
Teletrabajo
Selección de controles
Asegurar que la aplicación de los controles cumple:
Haber identificado los requerimientos de seguridad
Seleccionar los objetivos y los controles
Asegurar el cumplimiento de los requerimientos
Factores y restricciones de aplicabilidad:
Coste de control versus coste del impacto
Disponibilidad del control (tecnología existente y probada)
Implementación y mantenimiento
Controles existentes y planificación

2.3.6 Adquisición, desarrollo y mantenimiento. Objetivo: Asegurar la seguridad de las aplicaciones, prevenir errores, perdidas, modificaciones de las mismas así como de las informaciones que contienen.

Aspectos Destacados. Análisis de requerimientos de seguridad
Control del procesado de la información
Controles criptográficos
Control en el cambio de aplicaciones
Análisis de vulnerabilidades

2.3.7 Gestión de Incidentes. Objetivo: Tratar de asegurar la seguridad y tratar de minimizar el tiempo de respuesta ante los incidentes de seguridad

Aspectos Destacados. Comunicación de incidentes
Resolución de incidentes
Aprender de los incidentes
Recogida de evidencias
Mejoras

[7] Ibid., p.4.

2.3.8 Gestión de continuidad de negocio. Objetivos: Tratar de evitar interrupciones en los servicios de la organización o minimizar el tiempo de recuperación.[8]

Aspectos Destacados. Business Impact
Análisis (BIA)
Desarrollo de los PCN
Pruebas de planes
Mejora de los planes

2.3.9 Base legal. Artículo 39 del decreto n° 4 norma técnico del control interno de la corte de cuentas.

Decreto numero 29 reglamento de normas técnicas de control interno especificas del ministerio de hacienda de la corte de cuentas

Capítulo 7 manual de políticas de control interno del ministerio de hacienda

Articulo 36 definición de políticas y procedimientos de los controles generales de los sistemas de información (NTCIE de ministerio de hacienda)

Los titulares directores y demás jefaturas deben establecer las políticas y procedimientos sobre los controles generales, comunes a todos los sistemas de información como mínimo relativas a la seguridad de la información, planes de contingencia, desarrollo y auditoria, documentación control y licenciamiento de software.

2.3.10 Cumplimiento Legal.[9] Objetivo: Evitar incumplimiento legales, contractuales y con las normativas.

Aspectos Destacados. Propiedad intelectual
Protección de evidencias
Protección de datos
Auditoria de sistemas
Auditorias del sistema de gestión de la seguridad de la información

Implementar controles básicos. Legales
Comunes
LOPD
Política de seguridad
Propiedad intelectual
Responsabilidad de seguridad de la información
Proteger la información empresarial exigible y critica

[8] http://www.dnvba.com/es/Certificacion/Sistemas-de-Gestion/Gestion-de-continuidad-de-negocio/Pages/default.aspx
[9] OJEDA PÉREZ, Jorge Eliécer. Op cit., p.5.

Comunicación y formación
Reporte de incidentes
Planes de contingencia

Factores de éxito. Una seguridad (politica, objetivos, actividades) orientada al negocio.
Implementar la seguridad e consonancia con al cultura de la empresa.
Soporte visible y compromiso de la direcion.
Buen entendimiento de los requerimientos y buena gestion de los riesgos.
Comunicación eficaz a todos los niveles de la organización.
Proveer educación y formación.
Tener un sistema de medicion para evaluar el rendimiento de la gestion de la seguridad, asi como obtener sugerencias de mejora.

Enfoque para una Seguridad pro-activa.[10]

Implementar un SGSI. Especificaciones de la ISO/IEC 27001 – 12 dominios, 39 objetivos, 133 controles

Razones para un SGSI. Externas:

Mejora la confianza con clientes, proveedores partners (imagen corporativa)
Asegurar la conformidad con la legislación y los contratos

Internas:

Reducir impactos de incidentes
Facilitar la mejora continua
Consistencia

Ventajas de Implementar un SGSI. Cumplimiento de la legislación
Conocer los riesgos y poder gestionarlos
Credibilidad, confianza y fiabilidad
Compromiso
Basado en procesos
Adopción de las mejores practicas
Preservar la información

Alcance del SGSI.

Identificar los activos de información SGSI
Organización, localización, activos y tecnología
Categorización, descripción, localización y responsable de los activos

[10] Ibid., p.10.

Categorización de activos de información

Información. BD ficheros, documentación, manuales, contratos, etc.
Tipo soporte: papel electrónico

SW
Aplicaciones, S.O., herramientas de desarrollo, utilidades

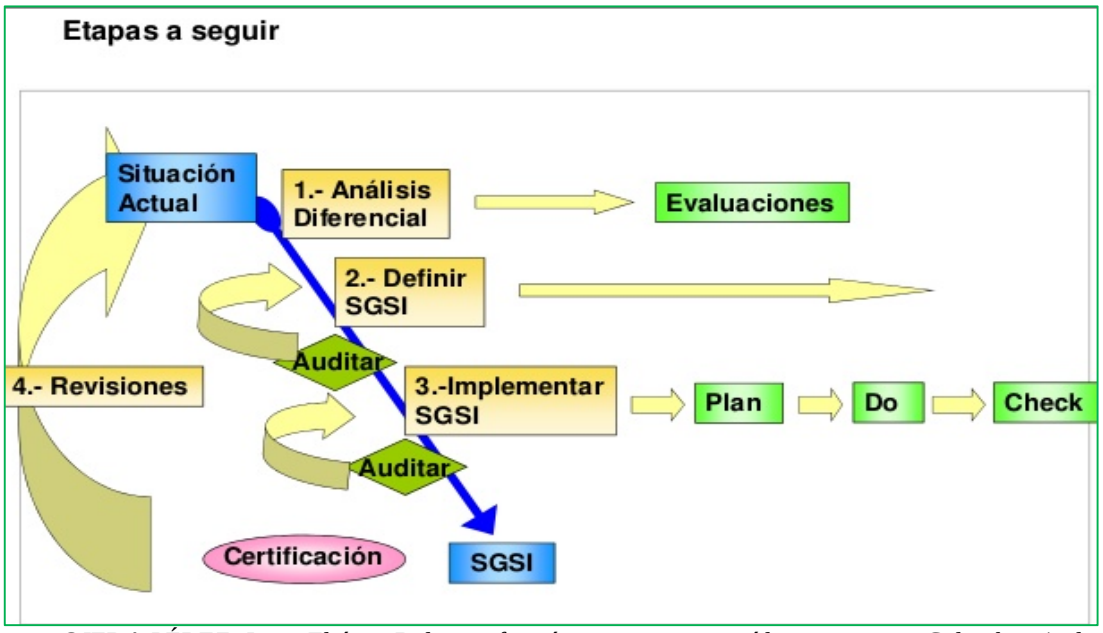
Físicos
Ordenadores, equipos de comunicación (routers, hubs)
Soportes

Servicios
Tratamientos externos, energía, telefonía

Personas
Conocimiento, experiencia

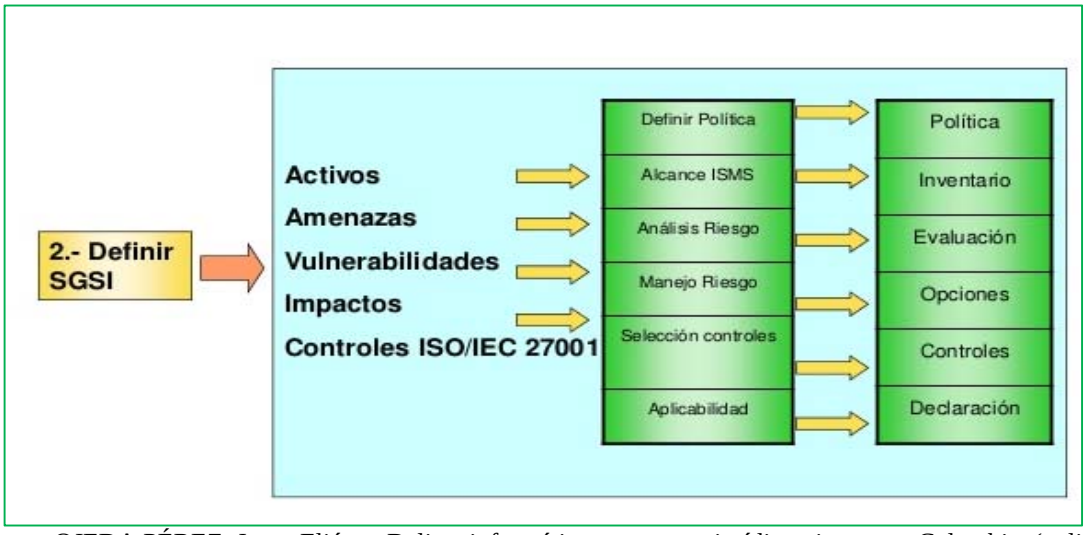
Intangibles

Imagen 5. Etapas a seguir en seguridad pro-activa.



Fuente: OJEDA PÉREZ, Jorge Eliécer. Delitos informáticos y entorno jurídico vigente en Colombia. (online) [Bogotá] 2010, [citado 23 jun., 2014]. Disponible en: http://www.sci.unal.edu.co/scielo.php?script=sci_arttext&pid=S0123-14722010000200003&lng=es&nrm=iso

Imagen 6. Etapas a seguir (punto 2).



Fuente: OJEDA PÉREZ, Jorge Eliécer. Delitos informáticos y entorno jurídico vigente en Colombia. (online) [Bogotá] 2010, [citado 23 jun., 2014]. Disponible en: http://www.sci.unal.edu.co/scielo.php?script=sci_arttext&pid=S0123-14722010000200003&lng=es&nrm=iso

2.3.11 Politica de Seguridad.[11] Es un documento:

Aprobado por la direcion, publicado y comunicado
Revisado periodicamente

Como Minimo

Definicion de la seguridad de la informacon
Declaracion del soporte de la direcion
Explicaciones breves sobre politicas, principios, practicas y cumplimiento de seguridad
Definiciopn de responsabilidades
Referencias a otros documentos

Lineamientos de seguridad

Organización de la seguridad de la información
Gestión de activos
Seguridad de los recursos humanos
Seguridad física y ambiental
Gestión de comunicación y operaciones

[11] MINISTERIO DE LA INFORMATICA Y LAS COMUNICACIONES. Reglamento sobre Seguridad Informática. La Habana. Cuba. 2012. 15h. [en línea]. http://fcmfajardo.sld.cu/seguridad_informatica/resol_y_dispos_del_mic/reglamento_seguridad_informatica.pdf

Control de accesos
Adquisición, desarrollo y mantenimiento de sistemas de información
Gestión de incidentes de seguridad de la información
Gestión de continuidad del negocio
Conformidad

Análisis del Riesgo

Identificar los riesgos de los activos de la información

Las amenazas a los activos
Sus vulnerabilidades
El impacto en la organización
Su probabilidad
El nivel de riesgo

Riesgo de seguridad
Un riesgo de seguridad es la posibilidad que una amenaza dada aproveche una vulnerabilidad para dañar uno a un grupo de activo de información, pudiendo extenderse a toda la organización
Administración del riesgo

Gestionar los riesgos identificados:
Decidir sobre la forma de manejar el riesgo
Identificar y aceptar el riesgo residual

Forma de gestionar el riesgo:

Evitar
Suprimir las causas del riesgo: activo, amenaza, vulnerabilidad
Transferir
Cambiar un riesgo por otro: outsourcing, seguros
Reducir
Reducir la amenaza, vulnerabilidad, impacto
Asumir (statu quo)
Detectar y recuperarse

Declaracion de Aplicabilidad

Declarar sobre la aplicabilidad de los controles de seguridad:

Documentar los resultados finales del marco del SGSI
Aplicar a la normativa ISO/IEC 27001 con: 12 dominios, 39 objetivos, 133 controles
Incluir otros controles propios o especificaciones

Debe incluir:

Los objetivos de los controles (requerimientos)
La descripción de los controles (y las medidas)
La razón de su exclusión[12]

2.4 MARCO LEGAL

La Ley 1273 del 5 de enero de 2009, reconocida en Colombia como la *Ley de Delitos Informáticos*, tuvo sus propios antecedentes jurídicos, además de las condiciones de contexto analizadas en el numeral anterior. El primero de ellos se remite veinte años atrás, cuando mediante el Decreto 1360 de 1989 se reglamenta la inscripción del soporte lógico (software) en el Registro Nacional de Derecho de Autor, que sirvió como fundamento normativo para resolver aquellas reclamaciones por violación de tales derechos, propios de los desarrolladores de software. A partir de esa fecha, se comenzó a tener asidero jurídico para proteger la producción intelectual de estos nuevos creadores de aplicativos y soluciones informáticas.[13]

En este mismo sentido y en el entendido de que el soporte lógico o software es un elemento informático, las conductas delictivas descritas en los Artículos 51 y 52 del Capítulo IV de la Ley 44 de 1993 sobre Derechos de Autor, y el mismo Decreto 1360 de 1989, Reglamentario de la inscripción del soporte lógico (software) en el Registro Nacional del Derecho de Autor, se constituyeron en las primeras normas penalmente sancionatorias de las violaciones a los citados Derechos de Autor. Al mismo tiempo, se tomaron como base para la reforma del año 2000 al Código Penal Colombiano:

Capítulo Único del Título VII que determina los Delitos contra los Derechos de Autor: Artículo 270: Violación a los derechos morales de autor. Artículo 271: Defraudación a los derechos patrimoniales de autor. Artículo 272: Violación a los mecanismos de protección de los derechos patrimoniales de autor y otras defraudaciones.

El Código Penal colombiano (Ley 599 de 2000) en su Capítulo séptimo del Libro segundo, del Título III: Delitos contra la libertad individual y otras garantías, trata sobre la violación a la intimidad, reserva e interceptación de comunicaciones:

Artículo 192: Violación ilícita de comunicaciones. Artículo 193: Ofrecimiento, venta o compra de instrumento apto para interceptar la comunicación privada entre personas.

Artículo 194: Divulgación y empleo de documentos reservados. Artículo 195: Acceso abusivo a un sistema informático. Artículo 196: Violación ilícita de comunicaciones o

[12] Ibid., p.4.
[13] OJEDA PÉREZ, Jorge Eliécer. Delitos informáticos y entorno jurídico vigente en Colombia. (online) [Bogotá] 2010, [citado 23 jun., 2014]. Disponible en: http://www.sci.unal.edu.co/scielo.php?script=sci_arttext&pid=S0123-14722010000200003&lng=es&nrm=iso

correspondencia de carácter oficial. Artículo 197: Utilización ilícita de equipos transmisores o receptores. Estos artículos son concordantes con el artículo 357: Daño en obras o elementos de los servicios de comunicaciones, energía y combustibles.

Una norma posterior relacionada fue la Ley 679 de 2001, que estableció el Estatuto para prevenir y contrarrestar la explotación, la pornografía y el turismo sexual con niños menores de edad. De igual manera, consagra prohibiciones para los proveedores o servidores, administradores o usuarios de redes globales de información, respecto a alojar imágenes, textos, documentos o archivos audiovisuales que exploten a los menores en actitudes sexuales o pornográficas. Sin embargo, la norma no contiene sanciones penales, sino administrativas (Artículo 10), pues siendo simple prohibición, deja un vacío que quita eficacia a la Ley, cuando se trata de verdaderos delitos informáticos.

Para subsanar lo anterior, el 21 de julio de 2009, se sancionó la Ley 1336, "por medio de la cual se adiciona y robustece la Ley 679 de 2001, de lucha contra la explotación, la pornografía y el turismo sexual, con niños, niñas y adolescentes". En forma específica, en su Capítulo VI, sanciona los "Tipos penales de turismo sexual y almacenamiento e intercambio de pornografía infantil" con penas de prisión de diez (10) a veinte (20) años y multas de ciento cincuenta (150) a mil quinientos (1.500) salarios mínimos legales mensuales vigentes (SMLMV).

La Ley 1273 de 2009 complementa el Código Penal y crea un nuevo bien jurídico tutelado a partir del concepto de la *protección de la información y de los datos*, con el cual se preserva integralmente a los sistemas que utilicen las tecnologías de la información y las comunicaciones. El primer capítulo de los dos en que está dividida la Ley, trata de los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos. El segundo Capítulo se refiere a los atentados informáticos y otras infracciones.

A partir de la Ley 1273 de 2009, se tipificaron los delitos informáticos en Colombia en los siguientes términos: acceso abusivo a un sistema informático (modificado del Código Penal); obstaculización ilegítima del sistema informático o red de telecomunicación; interceptación de datos informáticos; daño informático; uso de software malicioso; hurto por medios informáticos y semejantes; violación de datos personales; suplantación de sitios *web* para capturar datos personales y transferencia no consentida de activos.

Este marco jurídico se ha convertido en una importante contribución y un instrumento efectivo para que las entidades públicas y privadas puedan enfrentar los "delitos informáticos", con definiciones de procedimientos y políticas de seguridad de la información; y, en consecuencia, con las acciones penales que pueden adelantar contra las personas que incurran en las conductas tipificadas en la norma. Con ella, Colombia se ubica al mismo nivel de los países miembros de la Comunidad Económica Europea (CEE), los cuales ampliaron al nivel internacional los acuerdos jurídicos relacionados con la protección de la información y los recursos informáticos de los países, mediante el

Convenio 'Cibercriminalidad', suscrito en Budapest, Hungría, en 2001 y vigente desde julio de 2004.

Con los desarrollos jurídicos hasta ahora logrados acerca de "la protección de la información y de los datos y la preservación integral de los sistemas que utilicen las tecnologías de información y comunicaciones", las organizaciones pueden amparar gran parte de sus sistemas integrados de información: datos, procesos, políticas, personal, entradas, salidas, estrategias, cultura corporativa, recursos de las TIC y el entorno externo (Davenport, 1999), de manera que, además de contribuir a asegurar las características de calidad de la información, se incorpora la administración y el control, en el concepto de protección integral.

3. DISEÑO METODOLÓGICO

3.1 TIPO DE INVESTIGACIÓN

La presente investigación pretende mostrar que el desarrollo de una guía práctica para implementar las ISO/IEC 27001:2005 como herramienta para los sistemas de información, el HOSPITAL EMIRO QUINTERO CAÑIZARES pueda garantizar las características fundamentales de los sistemas de información para tal efecto se hace uso de una metodología cuantitativa con un enfoque descriptivo.

3.2 POBLACIÓN

La población a estudiar está constituida por el personal del Área de sistemas de la empresa HOSPITAL EMIRO QUINTERO CAÑIZARES, los cuales son en total cuatro personas.

3.3 MUESTRA

Por ser tan reducida la población, para la muestra se tomará el 100% de la misma, debido que se encuestarán a los encargados de la instalación y capacitación del personal en cabeza del señor Alexander Becerra. (4 personas).

3.4 TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN DE INFORMACIÓN

Fuentes Primarias: Entre las fuentes primarias de información utilizadas en el estudio investigativo descriptivo se encuentran la asesoría de ingenieros de sistemas y especialistas, docentes de la Universidad Francisco de Paula Santander Seccional Ocaña y demás personas y entidades que provean información base para este estudio; se utilizará la encuesta a los empleados del área objeto de estudio; todo esto con el fin de conocer a fondo las operaciones de la sección para obtener una visión clara de los procedimientos realizados en la misma. En este estudio se emplearán diferentes instrumentos de recolección de información como: la encuesta y observación directa. (Ver anexo A encuesta)

Fuentes Secundarias: Entre las fuentes secundarias de información se cuenta con la información extraída de revistas, libros y textos de clase, información de centro de información y documentación, bibliotecas y consultas virtuales.

3.5 ANALISIS DE LA INFORMACIÓN

Los datos obtenidos mediante la aplicación de los instrumentos de recolección de la información, serán analizados cuantitativamente a través de tablas y gráficas, mediante la interpretación de los datos numéricos y el análisis de cada respuesta para la forma cualitativa.

4. RESULTADOS

4.1 RECONOCIMIENTO DE LAS ÁREAS DEL HOSPITAL EMIRO QUINTERO CAÑIZARES OCAÑA RELACIONADAS CON EL SISTEMA DE INFORMACIÓN MY PROCESS

Con el fin de hacer un reconocimiento de las áreas del Hospital Emiro Quintero Cañizares Ocaña, se realiza un pequeño resumen con el objetivo de conocer el fortalecimiento institucional que proyecta la misión, en cada una de las cinco (5) líneas de direccionamiento estratégico definidas por la Gerencia; dichas líneas son:

Calidad: Desarrollo de una cultura de la calidad y el autocontrol, a partir del sistema integrado de gestión, con Énfasis en Acreditación en Salud.

Participación Social: Fortalecimiento de los mecanismos y espacios de participación de la comunidad en la gestión institucional.

Servicios Integrales de Salud: Prestación de servicios de primer y segundo nivel en los ámbitos intramural y extramural, para contribuir en el mantenimiento de la salud individual, familiar y colectiva.

Coordinación: Unificación y articulación de esfuerzos entre colaboradores del Hospital y, de ésta con otras instituciones para el logro de los objetivos y el impacto en la comunidad.

Sostenibilidad Institucional: Garantía de permanencia y desarrollo del Hospital en el tiempo, a través de intervenciones relacionadas con:

Gestión Estratégica: Posicionamiento y reconocimiento institucional en el sector por la presencia y generación de beneficios a la comunidad objetivo.

Personas: Desarrollo de estrategias y acciones de potencialización de las competencias del talento humano y humanización del servicio, dentro de la política del talento humano.

Recursos Físicos y Tecnológicos: Disposición, actualización y mantenimiento de los recursos físicos y tecnológicos, acordes con las necesidades de prestación de servicios y bienestar del talento humano.

Sostenibilidad Financiera: Gestión permanente de recursos para garantizar el funcionamiento y desarrollo de la institución, dentro de niveles superiores de calidad y acordes con la política de gestión financiera.

Continuando con el reconocimiento del Hospital Emiro Quintero Cañizares Ocaña, en los centros hospitalarios se debe tener en cuenta principalmente la variedad de gente que compone el ambiente típico del hospital - pacientes, personal, vendedores, médicos, visitantes e incluso sus enemigos. La tipología del lugar queda definida por muchos

cuartos, habitaciones, salas, espacios, equipos de alto valor, accesibilidad a las drogas, muchas entradas y salidas. Y siempre valorando todos los aspectos que faciliten el movimiento en el edificio y alrededores.

La seguridad es esencial en este tipo de entornos. Los encargados del hospital basan sus decisiones en la protección y reputación de su entidad.

Las principales amenazas en un ambiente hospitalario son el hurto por parte de empleados o del visitante, vandalismo de personal ajeno al hospital y amenazas contra pacientes o el personal interno.

4.1.1 Áreas del Hospital Emiro Quintero Cañizares Ocaña, relacionadas con el sistema de información MY PROCESS.

Área de Urgencias. Atiende la alteración en la integridad física y/o mental de una persona, causada por un trauma o por una enfermedad de cualquier etiología que genere la demanda de una atención médica inmediata y efectiva, en la búsqueda de disminuir los riesgos de invalidez y muerte.

Hospitalización. El servicio de Régimen Contributivo hace aproximadamente 4 décadas era llamado Pensión, los pacientes que se recibían atención eran particulares, o de entidades como Batallón, Policía Nacional, Maestros y Empleados de CAJANAL y de la salud.

Mediante la ley 100 de 1993 este servicio pasó a llamarse Régimen Contributivo, La E.S.E. H.E.Q.C. lo adaptó en el año 2000, desde entonces se ha venido prestando el servicio a los afiliados del contributivo de la Seguridad Social en Salud.

El Régimen Contributivo ha sido pilar fundamental en la E.S.E. H.E.Q.C; pues también se reciben pacientes de otros regimenes de seguridad social en salud. Contamos con un censo de 8 a 9 pacientes, con calidad en la prestación del servicio y un ánimo constante.

El servicio cuenta con 9 camas disponibles, 1 Jefe de Enfermería que presta el servicio por 4 horas diarias, 5 auxiliares de enfermería que cubren turnos las 24 horas del día. También cuenta con Medicina Especializada para cubrir necesidades que demandan nuestros usuarios, y un Médico interno las 24 horas del día.

Consulta Externa. Es una dependencia que cuenta con un equipo multidisciplinario comprometido con el usuario encaminado a la promoción de la salud y prevención de las enfermedades, trabajando con perseverancia para que la atención y la accesoria faciliten la sensibilización al buen uso y beneficios de los programas de atención en salud.

El acelerado crecimiento poblacional y el aumento de la esperanza de vida nos ha generado la necesidad de ser cada día más partícipes en la atención con calidad apoyándonos en la educación y reducción de la mortalidad en busca de asegurar una existencia digna para todos.

Por esto contamos con el programa de protección específica como atención preventiva en salud oral, planificación familiar en hombres y mujeres; detención temprana como control de crecimiento y desarrollo, control prenatal, adulto joven, adulto mayor, agudeza visual, cáncer de cuello uterino y de seno.

Además contamos con el programa de guías de atención para el manejo de enfermedades de interés en salud pública, psicología, inducción a la demanda, consulta por medicina general, enfermería y especializada.

Presta los siguientes servicios:

Medicina General.
Medicina Especializada.
Cirugía General.
Ortopedia y Traumatología.
Gineco-Obstetricia.
Medicina Interna.
Anestesiologia.
Dermatología.
Otorrinolaringología
Psiquiatría.
Odontología.
Promoción y Prevención.

Cabe destacar que, consulta externa, es uno de los servicios con más información registrada en los sistemas de información del Hospital Emiro Quintero Cañizares.

Quirófanos y salas de parto. Los servicios que se prestan son las urgencias Ginecoobtetricias, atención del parto, complicaciones del embarazo, patologías ginecológicas, procedimientos de ayuda diagnóstica y terapéuticas.

Lo conforman tres quirófanos y dos salas de parto con Anestesiólogo, Cirujano General y Gineco-Obstetra las 24 horas. Cirugía Programada, Urgencias y ambulatoria.

Medicina Interna. Servicio encargado de la atención, diagnóstico, tratamiento y seguimiento de las diferentes enfermedades no quirúrgicas.

Cuenta con tres Internistas, Enfermero Jefe de piso, Auxiliares de enfermería y Médico general.

En piso se hace la toma de Electrocardiogramas.

4.2 FACTORES QUE OCASIONAN RIESGOS EN LA INTEGRIDAD, CONFIDENCIALIDAD Y DISPONIBILIDAD DE LA INFORMACIÓN DEL SISTEMA MY PROCESS, DE ACUERDO AL DOMINIO CONTROL DE ACCESO DE LA ISO 27001:2013

Para lograr sus objetivos, la seguridad informática se fundamenta en tres principios, que debe cumplir todo sistema informático:

Confidencialidad
Integridad
Disponibilidad

CONFIDENCIALIDAD

Se refiere a la privacidad de los elementos de información almacenados y procesados en un sistema informático.

Basándose en este principio, las herramientas de seguridad informática deben proteger al sistema de invasiones, intrusiones y accesos, por parte de personas o programas no autorizados.

Este principio es particularmente importante en sistemas distribuidos, es decir, aquellos en los que usuarios, ordenadores y datos residen en localidades diferentes, pero están física y lógicamente interconectados.

INTEGRIDAD

Se refiere a la validez y consistencia de los elementos de información almacenados y procesados en un sistema informático.

Basándose en este principio, las herramientas de seguridad informática deben asegurar que los procesos de actualización estén sincronizados y no se dupliquen, de forma que todos los elementos del sistema manipulen adecuadamente los mismos datos.

Este principio es particularmente importante en sistemas descentralizados, es decir, aquellos en los que diferentes usuarios, ordenadores y procesos comparten la misma información.

DISPONIBILIDAD

Se refiere a la continuidad de acceso a los elementos de información almacenados y procesados en un sistema informático.

Basándose en este principio, las herramientas de Seguridad Informática deben reforzar la permanencia del sistema informático, en condiciones de actividad adecuadas para que los usuarios accedan a los datos con la frecuencia y dedicación que requieran.

Este principio es particularmente importante en sistemas informáticos cuyo compromiso con el usuario, es prestar servicio permanente.

El Hospital Emiro Quintero Cañizares Ocaña, como todo otro organismo, se encuentra expuesto a riesgos en materia de seguridad de la información.

No existe la seguridad completa, por lo que es necesario conocer cuál es el mapa de riesgos al que se enfrenta el organismo y tomar acciones tendientes a minimizar los posibles efectos negativos de la materialización de dichos riesgos. Es por ello que resulta imprescindible gestionar los riesgos del Organismo, como pilar fundamental para la gestión de seguridad.

Para ello, el Hospital deberá conocer los riesgos a los que se expone el Organismo en materia de seguridad de la información y generar información de utilidad para la toma de decisiones en materia de controles de seguridad.

Responsabilidad. El Comité de Seguridad de la Información será responsable de que se gestionen los riesgos de seguridad de la información, brindando su apoyo para el desarrollo de dicho proceso y su mantenimiento en el tiempo.

El Responsable de Seguridad de la Información junto con los responsables de cada dependencia del Hospital serán responsables del desarrollo del proceso de gestión de riesgos de seguridad de la información.

4.2.1 Evaluación de los riesgos de seguridad. El Hospital evaluará sus riesgos identificándolos, cuantificándolos y priorizándolos en función de los criterios de aceptación de riesgos y de los objetivos de control relevantes para el mismo.

Los resultados guiarán y determinarán la apropiada acción de la dirección y las prioridades para gestionar los riesgos de seguridad de la información y para la implementación de controles seleccionados para protegerse contra estos riesgos.

Se debe efectuar la evaluación de riesgos periódicamente, para tratar con los cambios en los requerimientos de seguridad y en las situaciones de riesgo, por ejemplo: cambios producidos en activos, amenazas, vulnerabilidades, impactos, valoración de riesgos. Asimismo, se debe efectuar la evaluación cada vez que ocurran cambios significativos. Es conveniente que estas evaluaciones de riesgos se lleven a cabo de una manera metódica capaz de producir resultados comparables y reproducibles.

El alcance de una evaluación de riesgos puede incluir a todo el Organismo, una parte, un sistema de información particular, componentes específicos de un sistema, o servicios.

Resulta recomendable seguir una metodología de evaluación de riesgos para llevar a cabo el proceso.

4.2.2 Tratamiento de riesgos de seguridad. Antes de considerar el tratamiento de un riesgo, el Organismo debe decidir los criterios para determinar si los riesgos pueden, o no, ser aceptados. Los riesgos pueden ser aceptados si por ejemplo: se evaluó que el riesgo es bajo o que el costo del tratamiento no es económicamente viable para la entidad. Tales decisiones deben ser tomadas por las autoridades y debidamente documentadas.

Para cada uno de los riesgos identificados durante la evaluación de riesgos, se necesita tomar una decisión para su tratamiento, como son:

a) Mitigar los riesgos mediante la aplicación de controles apropiados para reducir los riesgos;

b) Aceptar los riesgos de manera objetiva y consciente, siempre y cuando éstos satisfagan claramente la política y los criterios de aceptación de riesgos del Hospital;

c) Evitar los riesgos, eliminando las acciones que dan origen a la ocurrencia de éstos;

d) Transferir los riesgos asociados a otras partes interesadas, por ejemplo: compañías de seguro o proveedores.

Para aquellos riesgos donde la decisión ha sido la mitigación, se buscará reducir los riesgos a un nivel aceptable mediante la implementación de controles, teniendo en cuenta lo siguiente:

a) requerimientos y restricciones de legislaciones y regulaciones nacionales e internacionales;

b) objetivos organizacionales;

c) requerimientos y restricciones operativos;

d) costo de implementación y operación en relación directa a los riesgos reducidos, y proporcionales a los requerimientos y restricciones del Organismo;

e) la necesidad de equilibrar las inversiones en la implementación y operación de los controles contra el daño que podría resultar de las fallas de seguridad.

A continuación se relacionan los diferentes factores que ocasionan riesgos de información, de acuerdo al dominio control de acceso, así:

Factores de riesgo humanos: hurto, adulteración, fraude, modificación, revelación, pérdida, sabotaje, vandalismo, crackers, hackers, falsificación, robo de contraseñas, intrusión, alteración, etc.

Hackers. Los hackers son personas con avanzados conocimientos técnicos en el área informática y que enfocan sus habilidades hacia la invasión de sistemas a los que no tienen acceso autorizado.

En general, los hackers persiguen dos objetivos:

Probar que tienen las competencias para invadir un sistema protegido.
Probar que la seguridad de un sistema tiene fallas.

Crackers. Los crackers son personas con avanzados conocimientos técnicos en el área informática y que enfocan sus habilidades hacia la invasión de sistemas a los que no tienen acceso autorizado.

En general, los crackers persiguen dos objetivos:

Destruir parcial o totalmente el sistema.

Obtener un beneficio personal (tangible o intangible) como consecuencia de sus actividades.

Para éste, se deberá tener en cuenta un control de acceso, de manera que se evite la entrada a cualquier sistema.

Control: Áreas de acceso público, de carga y descarga

Se controlarán las áreas de Recepción y Distribución, las cuales estarán aisladas de las instalaciones de procesamiento de información, a fin de impedir accesos no autorizados.

Para ello se establecerán controles físicos que considerarán los siguientes lineamientos:

a) Limitar el acceso a las áreas de depósito, desde el exterior de la sede del Organismo, sólo al personal previamente identificado y autorizado.

b) Diseñar el área de depósito de manera tal que los suministros puedan ser descargados sin que el personal que realiza la entrega acceda a otros sectores del edificio.

c) Proteger todas las puertas exteriores del depósito cuando se abre la puerta interna.

d) Inspeccionar el material entrante para descartar peligros potenciales antes de ser trasladado desde el área de depósito hasta el lugar de uso.

e) Registrar el material entrante al ingresar al sitio pertinente.

f) Cuando fuese posible, el material entrante debe estar segregado o separado en sus diferentes partes que lo constituyan.

Mapa de riesgos de los procesos informáticos, en el Hospital Emiro Quintero Cañizares (ver Anexo B)

En el anexo C, se encuentra un registro de los riesgos encontrados en el Hospital Emiro Quintero Cañizares, todo ello teniendo en cuenta su calificación de acuerdo a la escala de riesgo.

4.3 DOCUMENTACIÓN DE LA GUÍA PRÁCTICA QUE PERMITA ORIENTAR LOS PROCESOS Y PROCEDIMIENTOS PARA EL CONSTROL DE ACCESO AL SISTEMA MY PROCESS DEL HOSPITAL EMIRO QUINTERO CAÑIZARES OCAÑA

El acceso por medio de un sistema de restricciones y excepciones a la información es la base de todo sistema de seguridad informática. Para impedir el acceso no autorizado a los sistemas de información se deben implementar procedimientos formales para controlar la asignación de derechos de acceso a los sistemas de información, bases de datos y servicios de información, y éstos deben estar claramente documentados, comunicados y controlados en cuanto a su cumplimiento.

Los procedimientos comprenden todas las etapas del ciclo de vida de los accesos de los usuarios de todos los niveles, desde el registro inicial de nuevos usuarios hasta la privación final de derechos de los usuarios que ya no requieren el acceso.

La cooperación de los usuarios es esencial para la eficacia de la seguridad, por lo tanto es necesario concientizar a los mismos acerca de sus responsabilidades por el mantenimiento de controles de acceso eficaces, en particular aquellos relacionados con el uso de contraseñas y la seguridad del equipamiento.

Son sus objetivos:

a) Impedir el acceso no autorizado a los sistemas de información, bases de datos y servicios de información.

b) Implementar seguridad en los accesos de usuarios por medio de técnicas de autenticación y autorización.

c) Controlar la seguridad en la conexión entre la red del Organismo y otras redes públicas o privadas.

d) Registrar y revisar eventos y actividades críticas llevadas a cabo por los usuarios en los sistemas.

e) Concientizar a los usuarios respecto de su responsabilidad frente a la utilización de contraseñas y equipos.
f) Garantizar la seguridad de la información cuando se utiliza computación móvil e instalaciones de trabajo remoto.

4.3.1. Requerimientos para el Control de Acceso. Con el objetivo de impedir el acceso no autorizado a la información se implementarán procedimientos formales para controlar la asignación de derechos de acceso a los sistemas, datos y servicios de información.

Los procedimientos debieran abarcar todas las etapas en el ciclo de vida del acceso del usuario, desde el registro inicial de usuarios nuevos hasta la baja final de los usuarios que ya no requieren acceso a los sistemas y servicios de información.

Registración de Usuarios. El Responsable de Seguridad de la Información definirá un procedimiento formal de registro de usuarios para otorgar y revocar el acceso a todos los sistemas, bases de datos y servicios de información multiusuario, el cual debe comprender:

a) Utilizar identificadores de usuario únicos, de manera que se pueda identificar a los usuarios por sus acciones evitando la existencia de múltiples perfiles de acceso para un mismo empleado. El uso de identificadores grupales sólo debe ser permitido cuando sean convenientes para el trabajo a desarrollar debido a razones operativas.

b) Verificar que el usuario tiene autorización del Propietario de la Información para el uso del sistema, base de datos o servicio de información.

c) Verificar que el nivel de acceso otorgado es adecuado para el propósito de la función del usuario y es coherente con la Política de Seguridad del Organismo, por ejemplo que no compromete la segregación de funciones.

d) Entregar a los usuarios un detalle escrito de sus derechos de acceso.

e) Requerir que los usuarios firmen declaraciones señalando que comprenden y aceptan las condiciones para el acceso.

f) Garantizar que los proveedores de servicios no otorguen acceso hasta que se hayan completado los procedimientos de autorización.

g) Mantener un registro formal de todas las personas registradas para utilizar el servicio.

h) Cancelar inmediatamente los derechos de acceso de los usuarios que cambiaron sus tareas, o de aquellos a los que se les revocó la autorización, se desvincularon del Organismo o sufrieron la pérdida/robo de sus credenciales de acceso.

i) Efectuar revisiones periódicas con el objeto de:

- cancelar identificadores y cuentas de usuario redundantes
- inhabilitar cuentas inactivas por más de..... (Indicar período no mayor a 60 días)
- eliminar cuentas inactivas por más de..... (Indicar período no mayor a 120 días)

En el caso de existir excepciones, deben ser debidamente justificadas y aprobadas.

j) Garantizar que los identificadores de usuario redundantes no se asignen a otros usuarios.

k) Incluir cláusulas en los contratos de personal y de servicios que especifiquen sanciones si el personal o los agentes que prestan un servicio intentan accesos no autorizados.

Gestión de Privilegios. Se limitará y controlará la asignación y uso de privilegios, debido a que el uso inadecuado de los privilegios del sistema resulta frecuentemente en el factor más importante que contribuye a la falla de los sistemas a los que se ha accedido ilegalmente.

Los sistemas multiusuario que requieren protección contra accesos no autorizados, deben prever una asignación de privilegios controlada mediante un proceso de autorización formal. Se deben tener en cuenta los siguientes pasos:

a) Identificar los privilegios asociados a cada producto del sistema, por ejemplo sistema operativo, sistema de administración de bases de datos y aplicaciones, y las categorías de personal a las cuales deben asignarse los productos.

b) Asignar los privilegios a individuos sobre la base de la necesidad de uso y evento por evento, por ejemplo el requerimiento mínimo para su rol funcional.

c) Mantener un proceso de autorización y un registro de todos los privilegios asignados. Los privilegios no deben ser otorgados hasta que se haya completado el proceso formal de autorización.

d) Establecer un período de vigencia para el mantenimiento de los privilegios (en base a la utilización que se le dará a los mismos) luego del cual los mismos serán revocados.

e) Promover el desarrollo y uso de rutinas del sistema para evitar la necesidad de otorgar privilegios a los usuarios.

Los Propietarios de Información serán los encargados de aprobar la asignación de privilegios a usuarios y solicitar su implementación, lo cual será supervisado por el Responsable de Seguridad de la Información.

Gestión de Contraseñas de Usuario. La asignación de contraseñas se controlará a través de un proceso de administración formal, mediante el cual deben respetarse los siguientes pasos:

a) Requerir que los usuarios firmen una declaración por la cual se comprometen a mantener sus contraseñas personales en secreto y las contraseñas de los grupos de trabajo exclusivamente entre los miembros del grupo. Esta declaración bien puede estar incluida en el Compromiso de Confidencialidad.

b) Garantizar que los usuarios cambien las contraseñas iniciales que les han sido asignadas la primera vez que ingresan al sistema. Las contraseñas provisorias, que se asignan cuando los usuarios olvidan su contraseña, sólo debe suministrarse una vez acreditada la identidad del usuario.

c) Generar contraseñas provisorias seguras para otorgar a los usuarios. Se debe evitar la participación de terceros o el uso de mensajes de correo electrónico sin protección (texto claro) en el mecanismo de entrega de la contraseña y los usuarios deben dar acuse de recibo formal cuando la reciban.

d) Almacenar las contraseñas sólo en sistemas informáticos protegidos.

e) Utilizar otras tecnologías de autenticación y autorización de usuarios, como ser la biométrica (por ejemplo verificación de huellas dactilares), verificación de firma, uso de autenticadores de hardware (como las tarjetas de circuito integrado), etc. El uso de esas herramientas se dispondrá cuando la evaluación de riesgos realizada por el Responsable de Seguridad de la Información conjuntamente con el Responsable del Area de Informática y el Propietario de la Información lo determine necesario (o lo justifique).

f) Configurar los sistemas de tal manera que:

- las contraseñas sean del tipo “password fuerte” y tengan ... (especificar cantidad no menor a 8 caracteres) caracteres,
- suspendan o bloqueen permanentemente al usuario luego de ... (especificar cantidad no mayor a 3) intentos de entrar con una contraseña incorrecta (debe pedir la rehabilitación ante quien corresponda),
- solicitar el cambio de la contraseña cada ... (especificar lapso no mayor a 45 días),
- impedir que las últimas .... (especificar cantidad no menor a 12) contraseñas sean reutilizadas,
- establecer un tiempo de vida mínimo de ... (especificar cantidad no mayor a 3) días para las contraseñas.

Administración de Contraseñas Críticas. En los diferentes ambientes de procesamiento existen cuentas de usuarios con las cuales es posible efectuar actividades críticas como ser instalación de plataformas o sistemas, habilitación de servicios, actualización de software, configuración de componentes informáticos, etc. Dichas cuentas no serán de uso habitual (diario), sino que sólo serán utilizadas ante una necesidad específica de realizar alguna tarea que lo requiera y se encontrarán protegidas por contraseñas con un mayor nivel de complejidad que el habitual. El Responsable de Seguridad de la Información definirá

procedimientos para la administración de dichas contraseñas críticas que contemplen lo siguiente:

a) Se definirán las causas que justificarán el uso de contraseñas críticas así como el nivel de autorización requerido.

b) Las contraseñas seleccionadas serán seguras, y su definición será efectuada como mínimo por dos personas, de manera que ninguna de ellas conozca la contraseña completa.

c) Las contraseñas y los nombres de las cuentas críticas a las que pertenecen serán resguardadas debidamente.

d) La utilización de las contraseñas críticas será registrada, documentando las causas que determinaron su uso, así como el responsable de las actividades que se efectúen con la misma.

e) Cada contraseña crítica se renovará una vez utilizada y se definirá un período luego del cual la misma será renovada en caso de que no se la haya utilizado.

f) Se registrarán todas las actividades que se efectúen con las cuentas críticas para luego ser revisadas. Dicho registro será revisado posteriormente por el Responsable de Seguridad de la Información.

Revisión de Derechos de Acceso de Usuarios. A fin de mantener un control eficaz del acceso a los datos y servicios de información, el Propietario de la Información de que se trate llevará a cabo un proceso formal, a intervalos regulares de ..... (indicar periodicidad no mayor a 6 meses), a fin de revisar los derechos de acceso de los usuarios. Se deben contemplar los siguientes controles:

a) Revisar los derechos de acceso de los usuarios a intervalos de ..... (especificar tiempo no mayor a 6 meses).

b) Revisar las autorizaciones de privilegios especiales de derechos de acceso a intervalos de..... (Especificar tiempo no mayor a 3 meses).

c) Revisar las asignaciones de privilegios a intervalos de ..... (especificar tiempo no mayor a 6 meses), a fin de garantizar que no se obtengan privilegios no autorizados.

4.3.2 Responsabilidades del Usuario. Tiene como objetivo, evitar el acceso de usuarios no-autorizados, evitar poner en peligro la información y evitar el robo de información y los medios de procesamiento de la información.

La cooperación de los usuarios autorizados es esencial para una seguridad efectiva. Los usuarios deben estar al tanto de sus responsabilidades para mantener controles de acceso

efectivos, particularmente con relación al uso de claves secretas y la seguridad del equipo del usuario.

Se debe implementar una política de escritorio y pantalla limpios para reducir el riesgo de acceso no autorizado o daño a los papeles, medios y medios de procesamiento de la información.

Uso de Contraseñas. Los usuarios deben seguir buenas prácticas de seguridad en la selección y uso de contraseñas.

Las contraseñas constituyen un medio de validación y autenticación de la identidad de un usuario, y consecuentemente un medio para establecer derechos de acceso a las instalaciones o servicios de procesamiento de información.

Los usuarios deben cumplir las siguientes directivas:

a) Mantener las contraseñas en secreto.

b) Pedir el cambio de la contraseña siempre que exista un posible indicio de compromiso del sistema o de las contraseñas.

c) Seleccionar contraseñas de calidad, de acuerdo a las prescripciones informadas por el Responsable del Activo de Información de que se trate, que:

1. Sean fáciles de recordar.

2. No estén basadas en algún dato que otra persona pueda adivinar u obtener fácilmente mediante información relacionada con la persona, por ejemplo nombres, números de teléfono, fecha de nacimiento, etc.

3. No tengan caracteres idénticos consecutivos o grupos totalmente numéricos o totalmente alfabéticos.

d) Cambiar las contraseñas cada vez que el sistema se lo solicite y evitar reutilizar o reciclar viejas contraseñas.

e) Cambiar las contraseñas provisorias en el primer inicio de sesión (“log on”).

f) Evitar incluir contraseñas en los procesos automatizados de inicio de sesión, por ejemplo, aquellas almacenadas en una tecla de función o macro.

g) Notificar de acuerdo a lo establecido en capítulo 13 (Gestión de Incidentes de Seguridad), cualquier incidente de seguridad relacionado con sus contraseñas: pérdida, robo o indicio de pérdida de confidencialidad.

Si los usuarios necesitan acceder a múltiples servicios o plataformas y se requiere que mantengan múltiples contraseñas, se notificará a los mismos que pueden utilizar una única contraseña para todos los servicios que brinden un nivel adecuado de protección de las contraseñas almacenadas y en tránsito.

Equipos Desatendidos en Áreas de Usuarios. Los usuarios deben garantizar que los equipos desatendidos sean protegidos adecuadamente.

Los equipos instalados en áreas de usuarios, por ejemplo estaciones de trabajo o servidores de archivos, requieren una protección específica contra accesos no autorizados cuando se encuentran desatendidos.

El Responsable de Seguridad de la Información debe coordinar con el Área de Recursos Humanos las tareas de concientización a todos los usuarios y contratistas, acerca de los requerimientos y procedimientos de seguridad, para la protección de equipos desatendidos, así como de sus funciones en relación a la implementación de dicha protección.

Los usuarios cumplirán con las siguientes pautas:

a) Concluir las sesiones activas al finalizar las tareas, a menos que puedan protegerse mediante un mecanismo de bloqueo adecuado, por ejemplo, un protector de pantalla protegido por contraseña.

b) Proteger las PC’s o terminales contra usos no autorizados mediante un bloqueo de seguridad o control equivalente, por ejemplo, contraseña de acceso cuando no se utilizan.

4.3.3 Control de Acceso a la Red.

Objetivo. Evitar el acceso no autorizado a los servicios de la red.

Se debe controlar el acceso a los servicios de redes internas y externas.

El acceso del usuario a las redes y servicios de las redes no deben comprometer la seguridad de los servicios de la red asegurando:

a) que existan las interfaces apropiadas entre la red del Organismo y las redes de otras organizaciones, y redes públicas;

b) se apliquen los mecanismos de autenticación apropiados para los usuarios y el equipo;

c) el control del acceso del usuario a la información sea obligatorio.

Política de Utilización de los Servicios de Red. Las conexiones no seguras a los servicios de red pueden afectar a todo el Organismo, por lo tanto, se controlará el acceso a los servicios de red tanto internos como externos. Esto es necesario para garantizar que los

usuarios que tengan acceso a las redes y a sus servicios, no comprometan la seguridad de los mismos.

El Responsable del Área Informática tendrá a cargo el otorgamiento del acceso a los servicios y recursos de red, únicamente de acuerdo al pedido formal del titular de una Unidad Organizativa que lo solicite para personal de su incumbencia.

Este control es particularmente importante para las conexiones de red a aplicaciones que procesen información clasificada o aplicaciones críticas, o a usuarios que utilicen el acceso desde sitios de alto riesgo, por ejemplo áreas públicas o externas que están fuera de la administración y del control de seguridad del Organismo.

Para ello, se desarrollarán procedimientos para la activación y desactivación de derechos de acceso a las redes, los cuales comprenderán:

a) Identificar las redes y servicios de red a los cuales se permite el acceso.

b) Realizar normas y procedimientos de autorización para determinar las personas y las redes y servicios de red a los cuales se les otorgará el acceso.

c) Establecer controles y procedimientos de gestión para proteger el acceso a las conexiones y servicios de red.

Esta Política será coherente con la Política de Control de Accesos del Organismo .

Camino Forzado. Las redes están diseñadas para permitir el máximo alcance de distribución de recursos y flexibilidad en la elección de la ruta a utilizar. Estas características también pueden ofrecer oportunidades para el acceso no autorizado a las aplicaciones del Organismo, o para el uso no autorizado de servicios de información. Por esto, el camino de las comunicaciones será controlado.

Se limitarán las opciones de elección de la ruta entre la terminal de usuario y los servicios a los cuales el mismo se encuentra autorizado a acceder, mediante la implementación de controles en diferentes puntos de la misma.

A continuación se enumeran algunos ejemplos a considerar en caso de implementar estos controles a los sistemas existentes:

a) Asignar números telefónicos o líneas, en forma dedicada.

b) Establecer la conexión automática de puertos a gateways de seguridad o a sistemas de aplicación específicos.

c) Limitar las opciones de menú y submenú de cada uno de los usuarios.

d) Evitar la navegación ilimitada por la red.

e) Imponer el uso de sistemas de aplicación y/o gateways de seguridad específicos para usuarios externos de la red.

f) Controlar activamente las comunicaciones con origen y destino autorizados a través de un gateway, por ejemplo utilizando firewalls y generando alertas ante eventos no previstos.

g) Restringir el acceso a redes, estableciendo dominios lógicos separados, por ejemplo, redes privadas virtuales para grupos de usuarios dentro o fuera del Organismo.

Los requerimientos relativos a caminos forzados se basarán en la Política de Control de Accesos del Organismo. El Responsable de Seguridad de la Información, conjuntamente con el Propietario de la Información de que se trate, realizará una evaluación de riesgos a fin de determinar los mecanismos de control que corresponda en cada caso.

Autenticación de Usuarios para Conexiones Externas. Las conexiones externas son de gran potencial para accesos no autorizados a la información del Organismo. Por consiguiente, el acceso de usuarios remotos estará sujeto al cumplimiento de procedimientos de autenticación. Existen diferentes métodos de autenticación, algunos de los cuales brindan un mayor nivel de protección que otros. El Responsable de Seguridad de la Información, conjuntamente con el Propietario de la Información de que se trate, realizará una evaluación de riesgos a fin de determinar el mecanismo de autenticación que corresponda en cada caso.

La autenticación de usuarios remotos puede llevarse a cabo utilizando:

a) Un método de autenticación físico (por ejemplo tokens de hardware), para lo que debe implementarse un procedimiento que incluya:

• Asignación de la herramienta de autenticación.
• Registro de los poseedores de autenticadores.
• Mecanismo de rescate al momento de la desvinculación del personal al que se le otorgó.
• Método de revocación de acceso del autenticador, en caso de compromiso de seguridad.

b) Un protocolo de autenticación (por ejemplo desafío/respuesta), para lo que debe implementarse un procedimiento que incluya:

• Establecimiento de las reglas con el usuario.
• Establecimiento de un ciclo de vida de las reglas para su renovación.

c) También pueden utilizarse líneas dedicadas privadas o una herramienta de verificación de la dirección del usuario de red, a fin de constatar el origen de la conexión. Los procedimientos y controles de rellamada, o dial-back, pueden brindar protección contra conexiones no autorizadas a las instalaciones de procesamiento de información del

Organismo. Al aplicar este tipo de control, el Organismo no debe utilizar servicios de red que incluyan desvío de llamadas. Si por alguna causa es preciso mantener el desvío de llamadas, no será posible aplicar el control de rellamada. Asimismo, es importante que el proceso de re-llamada garantice que se produzca a su término, una desconexión real del lado del Organismo.

En caso de utilizarse sistemas de Voz sobre IP, deben ajustarse los controles a fin de que no sean utilizados para efectuar comunicaciones no autorizadas (ej: bloqueo de puertos).

Autenticación de Nodos. Una herramienta de conexión automática a una computadora remota podría brindar un medio para obtener acceso no autorizado a una aplicación del Organismo. Por consiguiente, las conexiones a sistemas informáticos remotos serán autenticadas. Esto es particularmente importante si la conexión utiliza una red que está fuera de control de la gestión de seguridad del Organismo. En el punto anterior se mencionan algunos ejemplos de autenticación y de cómo puede lograrse. La autenticación de nodos puede servir como un medio alternativo de autenticación de grupos de usuarios remotos, cuando éstos están conectados a un servicio informático seguro y compartido.

Protección de los Puertos (Ports) de Diagnóstico Remoto. Muchas computadoras y sistemas de comunicación son instalados y administrados con una herramienta de diagnóstico remoto. Si no están protegidos, estos puertos de diagnóstico proporcionan un medio de acceso no autorizado. Por consiguiente, serán protegidos por un mecanismo de seguridad apropiado, con las mismas características del punto “11.4.3 Control: Autenticación de Usuarios para Conexiones Externas”. También para este caso debe tenerse en cuenta el punto “Control: Camino Forzado”.

Subdivisión de Redes. Para controlar la seguridad en redes extensas, se podrán dividir en dominios lógicos separados.
Para esto se definirán y documentarán los perímetros de seguridad que sean convenientes.

Estos perímetros se implementarán mediante la instalación de “gateways” con funcionalidades de “firewall” o redes privadas virtuales, para filtrar el tráfico entre los dominios y para bloquear el acceso no autorizado de acuerdo a la Política de Control de Accesos.

La subdivisión en dominios de la red tomará en cuenta criterios como los requerimientos de seguridad comunes de grupos de integrantes de la red, la mayor exposición de un grupo a peligros externos, separación física, u otros criterios de aglutinamiento o segregación preexistentes.

Basándose en la Política de Control de Accesos y los requerimientos de acceso (Categoría: Requerimientos para el Control de Acceso), el Responsable del Area Informática evaluará el costo relativo y el impacto en el desempeño que ocasione la implementación de enrutadores o gateways adecuados para subdividir la red. Luego decidirá, junto con el Responsable de Seguridad de la Información, el esquema más apropiado a implementar.

Acceso a Internet. El acceso a Internet será utilizado con propósitos autorizados o con el destino por el cual fue provisto.

El Responsable de Seguridad de la Información definirá procedimientos para solicitar y aprobar accesos a Internet. Los accesos serán autorizados formalmente por el Responsable de la Unidad Organizativa a cargo del personal que lo solicite. Asimismo, se definirán las pautas de utilización de Internet para todos los usuarios.

Se evaluará la conveniencia de generar un registro de los accesos de los usuarios a Internet, con el objeto de realizar revisiones de los accesos efectuados o analizar casos particulares. Dicho control será comunicado a los usuarios de acuerdo a lo establecido en el punto de Acuerdos de confidencialidad. Para ello, el Responsable de Seguridad de la Información junto con el Responsable del Área de Informática analizarán las medidas a ser implementadas para efectivizar dicho control, como ser la instalación de “firewalls”, “proxies”, etc.

Conexión a la Red. Sobre la base de lo definido en el punto “11.1 Categoría: Requerimientos”, se implementarán controles para limitar la capacidad de conexión de los usuarios. Dichos controles se podrán implementar en los “gateways” que separen los diferentes dominios de la red .

Algunos ejemplos de los entornos a las que deben implementarse restricciones son:

a) Correo electrónico.
b) Transferencia de archivos.
c) Acceso interactivo.
d) Acceso a la red fuera del horario laboral.

Ruteo de Red. En las redes compartidas, especialmente aquellas que se extienden fuera de los límites del Organismo, se incorporarán controles de ruteo, para asegurar que las conexiones informáticas y los flujos de información no violen la Política de Control de Accesos. Estos controles contemplarán mínimamente la verificación positiva de direcciones de origen y destino. Adicionalmente, para este objetivo pueden utilizarse diversos métodos incluyendo entre otros autenticación de protocolos de ruteo, ruteo estático, traducción de direcciones y listas de control de acceso.

Seguridad de los Servicios de Red. El Responsable de Seguridad de la Información junto con el Responsable del Área Informática definirán las pautas para garantizar la seguridad de los servicios de red del Organismo, tanto públicos como privados.

Para ello se tendrán en cuenta las siguientes directivas:

- Mantener instalados y habilitados sólo aquellos servicios que sean utilizados.
- Controlar el acceso lógico a los servicios, tanto a su uso como a su administración.

- Configurar cada servicio de manera segura, evitando las vulnerabilidades que pudieran presentar.
- Instalar periódicamente las actualizaciones de seguridad.

Dicha configuración será revisada periódicamente por el Responsable de Seguridad de la Información.

4.3.4 Control de Acceso al Sistema Operativo. Su objetivo es el de evitar el acceso no autorizado a los sistemas operativos.

Se deben utilizar medios de seguridad para restringir el acceso a los sistemas operativos a los usuarios autorizados. Los medios deben tener la capacidad para:

a) autenticar a los usuarios autorizados, en concordancia con una política de control de acceso definida;
b) registrar los intentos exitosos y fallidos de autenticación del sistema;
c) registrar el uso de los privilegios especiales del sistema;
d) emitir alarmas cuando se violan las políticas de seguridad del sistema;
e) proporcionar los medios de autenticación apropiados;
f) cuando sea apropiado, restringir el tiempo de conexión de los usuarios

Identificación Automática de Terminales. El Responsable de Seguridad de la Información junto con el Responsable del Área Informática realizarán una evaluación de riesgos a fin de determinar el método de protección adecuado para el acceso al Sistema Operativo.

Si del análisis realizado surgiera la necesidad de proveer un método de identificación de terminales, se redactará un procedimiento que indique:

a) El método de identificación automática de terminales utilizado.
b) El detalle de transacciones permitidas por terminal o dispositivo.

Procedimientos de Conexión de Terminales. El acceso a los servicios de información sólo será posible a través de un proceso de conexión seguro. El procedimiento de conexión en un sistema informático será diseñado para minimizar la oportunidad de acceso no autorizado.
Este procedimiento, por lo tanto, debe divulgar la mínima información posible acerca del sistema, a fin de evitar proveer de asistencia innecesaria a un usuario no autorizado.

El procedimiento de identificación debe:

a) Mantener en secreto los identificadores de sistemas o aplicaciones hasta tanto se halla llevado a cabo exitosamente el proceso de conexión.

b) Desplegar un aviso general advirtiendo que sólo los usuarios autorizados pueden acceder a la computadora.

c) Evitar dar mensajes de ayuda que pudieran asistir a un usuario no autorizado durante el procedimiento de conexión.

d) Validar la información de la conexión sólo al completarse la totalidad de los datos de entrada.

Si surge una condición de error, el sistema no debe indicar que parte de los datos es correcta o incorrecta.

e) Limitar el número de intentos de conexión no exitosos permitidos y:
• Registrar los intentos no exitosos.
• Impedir otros intentos de identificación, una vez superado el límite permitido.
• Desconectar conexiones de comunicaciones de datos.

f) Limitar el tiempo máximo permitido para el procedimiento de conexión. Si éste es excedido, el sistema debe finalizar la conexión.

g) Desplegar la siguiente información, al completarse una conexión exitosa:
• Fecha y hora de la conexión exitosa anterior.
• Detalles de los intentos de conexión no exitosos desde la última conexión exitosa.

Identificación y Autenticación de los Usuarios. Todos los usuarios (incluido el personal de soporte técnico, como los operadores, administradores de red, programadores de sistemas y administradores de bases de datos) tendrán un identificador único (ID de usuario) solamente para su uso personal exclusivo, de manera que las actividades puedan rastrearse con posterioridad hasta llegar al individuo responsable, a fin de garantizar la trazabilidad de las transacciones. Los identificadores de usuario no darán ningún indicio del nivel de privilegio otorgado.

En circunstancias excepcionales, cuando existe un claro beneficio para el Organismo, podrá utilizarse un identificador compartido para un grupo de usuarios o una tarea específica. Para casos de esta índole, se documentará la justificación y aprobación del Propietario de la Información de que se trate.

Si se utilizará un método de autenticación físico (por ejemplo autenticadores de hardware), debe implementarse un procedimiento que incluya:

a) Asignar la herramienta de autenticación.

b) Registrar los poseedores de autenticadores.

c) Rescatar el autenticador al momento de la desvinculación del personal al que se le otorgó.

d) Revocar el acceso del autenticador, en caso de compromiso de seguridad.

Sistema de Administración de Contraseñas. Las contraseñas constituyen uno de los principales medios de validación de la autoridad de un usuario para acceder a un servicio informático. Los sistemas de administración de contraseñas deben constituir una herramienta eficaz e interactiva que garantice contraseñas de calidad.

El sistema de administración de contraseñas debe:

a) Imponer el uso de contraseñas individuales para determinar responsabilidades.

b) Permitir que los usuarios seleccionen y cambien sus propias contraseñas (luego de cumplido el plazo mínimo de mantenimiento de las mismas) e incluir un procedimiento de confirmación para contemplar los errores de ingreso.

c) Imponer una selección de contraseñas de calidad según lo señalado en el punto “Control: Uso de Contraseñas”.

d) Imponer cambios en las contraseñas en aquellos casos en que los usuarios mantengan sus propias contraseñas, según lo señalado en el punto “Control: Uso de Contraseñas”.

j) Obligar a los usuarios a cambiar las contraseñas provisorias en su primer procedimiento de identificación, en los casos en que ellos seleccionen sus contraseñas.

k) Mantener un registro de las últimas 13 contraseñas utilizadas por el usuario, y evitar la reutilización de las mismas.

l) Evitar mostrar las contraseñas en pantalla, cuando son ingresadas.

m) Almacenar en forma separada los archivos de contraseñas y los datos de sistemas de aplicación.

n) Almacenar las contraseñas en forma cifrada utilizando un algoritmo de cifrado unidireccional.

o) Modificar todas las contraseñas predeterminadas por el vendedor, una vez instalado el software y el hardware (por ejemplo claves de impresoras, hubs, routers, etc.).

p) Garantizar que el medio utilizado para acceder/utilizar el sistema de contraseñas, asegure que no se tenga acceso a información temporal o en tránsito de forma no protegida.

Uso de Utilitarios de Sistema. La mayoría de las instalaciones informáticas tienen uno o más programas utilitarios que podrían tener la capacidad de pasar por alto los controles de sistemas y aplicaciones. Es esencial que su uso sea limitado y minuciosamente controlado. Se deben considerar los siguientes controles:

a) Utilizar procedimientos de autenticación para utilitarios del sistema.
b) Separar entre utilitarios del sistema y software de aplicaciones.
c) Limitar el uso de utilitarios del sistema a la cantidad mínima viable de usuarios fiables y autorizados.
d) Evitar que personas ajenas al Organismo tomen conocimiento de la existencia y modo de uso de los utilitarios instalados en las instalaciones informáticas.
e) Establecer autorizaciones para uso ad hoc de utilitarios de sistema.
f) Limitar la disponibilidad de utilitarios de sistema, por ejemplo durante el transcurso de un cambio autorizado.
g) Registrar todo uso de utilitarios del sistema.
h) Definir y documentar los niveles de autorización para utilitarios del sistema.
i) Remover todo el software basado en utilitarios y software de sistema innecesarios.

Alarmas Silenciosas para la Protección de los Usuarios. Se considerará la provisión de alarmas silenciosas para los usuarios que podrían ser objetos de coerción. La decisión de suministrar una alarma de esta índole se basará en una evaluación de riesgos que realizará el Responsable de Seguridad de la Información junto con el Responsable del Área Informática. En este caso, se definirán y asignarán funciones y procedimientos para responder a la utilización de una alarma silenciosa.

Desconexión de Terminales por Tiempo Muerto. El Responsable de Seguridad de la Información, junto con los Propietarios de la Información de que se trate definirán cuáles se consideran terminales de alto riesgo, por ejemplo áreas públicas o externas fuera del alcance de la gestión de seguridad del Organismo, o que sirven a sistemas de alto riesgo. Las mismas se apagarán después de un período definido de inactividad, tiempo muerto, para evitar el acceso de personas no autorizadas. Esta herramienta de desconexión por tiempo muerto debe limpiar la pantalla de la terminal y debe cerrar tanto la sesión de la aplicación como la de red. El lapso por tiempo muerto responderá a los riesgos de seguridad del área y de la información que maneje la terminal.

Para las estaciones de trabajo, se implementará la desconexión por tiempo muerto, que limpie la pantalla y evite el acceso no autorizado, pero que no cierra las sesiones de aplicación o de red.

Por otro lado, si un agente debe abandonar su puesto de trabajo momentáneamente, activará protectores de pantalla con contraseñas, a los efectos de evitar que terceros puedan ver su trabajo o continuar con la sesión de usuario habilitada.

Limitación del Horario de Conexión. Las restricciones al horario de conexión deben suministrar seguridad adicional a las aplicaciones de alto riesgo. La limitación del período

durante el cual se permiten las conexiones de terminales a los servicios informáticos reduce el espectro de oportunidades para el acceso no autorizado. Se implementará un control de esta índole para aplicaciones informáticas sensibles, especialmente aquellas terminales instaladas en ubicaciones de alto riesgo, por ejemplo áreas públicas o externas que estén fuera del alcance de la gestión de seguridad del Organismo.

Entre los controles que se deben aplicar, se enuncian:

a) Utilizar lapsos predeterminados, por ejemplo para transmisiones de archivos en lote, o sesiones interactivas periódicas de corta duración.

b) Limitar los tiempos de conexión al horario normal de oficina, de no existir un requerimiento operativo de horas extras o extensión horaria.

c) Documentar debidamente los agentes que no tienen restricciones horarias y las razones de su autorización. También cuando el Propietario de la Información autorice excepciones para una extensión horaria ocasional.

4.3.5 Control de Acceso a las Aplicaciones. Su objetivo es evitar el acceso no autorizado a la información mantenida en los sistemas de aplicación.

Se deben utilizar medios de seguridad para restringir el acceso a y dentro de los sistemas de aplicación.

El acceso lógico al software de la aplicación y la información se debe limitar a los usuarios autorizados. Los sistemas de aplicación debieran:

a) controlar el acceso del usuario a la información y las funciones del sistema de aplicación, en concordancia con una política de control de acceso definida;

b) proporcionar protección contra un acceso no autorizado de cualquier utilidad, software del sistema de operación y software malicioso que sea capaz de superar o pasar los controles del sistema o la aplicación;

c) no comprometer a otros sistemas con los cuales se comparten recursos de información.

Restricción del Acceso a la Información. Los usuarios de sistemas de aplicación, con inclusión del personal de soporte, tendrán acceso a la información y a las funciones de los sistemas de aplicación de conformidad con la Política de Control de Acceso definida, sobre la base de los requerimientos de cada aplicación, y conforme a la Política del Organismo para el acceso a la información.

Se aplicarán los siguientes controles, para brindar apoyo a los requerimientos de limitación de accesos:

a) Proveer una interfaz para controlar el acceso a las funciones de los sistemas de aplicación.

El Propietario de la Información involucrada será responsable de la adjudicación de accesos a las funciones. En el caso de que las actividades involucradas en el otorgamiento de acceso revistan un carácter técnico elevado, las mismas serán llevadas a cabo por personal del área de sistemas, conforme a una autorización formal emitida por el Propietario de la Información.

b) Restringir el conocimiento de los usuarios acerca de la información o de las funciones de los sistemas de aplicación a las cuales no sean autorizados a acceder, con la adecuada edición de la documentación de usuario.

c) Controlar los derechos de acceso de los usuarios, por ejemplo, lectura, escritura, supresión y ejecución.

d) Garantizar que las salidas de los sistemas de aplicación que administran información sensible, contengan sólo la información que resulte pertinente para el uso de la salida, y que la misma se envíe solamente a las terminales y ubicaciones autorizadas.

e) Revisar periódicamente dichas salidas a fin de garantizar la remoción de la información redundante.

f) Restringir el acceso a la información por fuera del sistema encargado de su procesamiento, es decir, la modificación directa del dato almacenado.

Aislamiento de los Sistemas Sensibles. Los sistemas críticos podrían requerir de un ambiente informático dedicado (aislado). Algunos sistemas de aplicación son suficientemente sensibles a pérdidas potenciales y requieren un tratamiento especial. La sensibilidad puede señalar que el sistema de aplicación debe ejecutarse en una computadora dedicada, que sólo debe compartir recursos con los sistemas de aplicación confiables, o no tener limitaciones. Son aplicables las siguientes consideraciones:

a) Identificar y documentar claramente la sensibilidad de un sistema de aplicación. Esta tarea será llevada a cabo por el administrador de la aplicación.

b) Identificar y acordar con el administrador de la aplicación sensible cuando la aplicación ha de ejecutarse en un ambiente compartido, los sistemas de aplicación con los cuales ésta compartirá los recursos.

c) Coordinar con el Responsable del Area informática, qué servicios estarán disponibles en el entorno donde se ejecutará la aplicación, de acuerdo a los requerimientos de operación y seguridad especificados por el administrador de la aplicación.

d) Considerar la seguridad en la administración de las copias de respaldo de la información que procesan las aplicaciones.

e) Considerar las mismas precauciones de seguridad y privacidad, en la elaboración del plan de continuidad y/o contingencia de la ejecución de la aplicación. Ejemplo: el equipamiento alternativo o las instalaciones de emergencia donde restablecer la aplicación.

4.3.6 Monitoreo del Acceso y Uso de los Sistemas. Su objetivo es el de asegurar que se registren y se evalúen todos los eventos significativos para la seguridad de accesos.

Verificar la existencia de procedimientos para monitorear el uso de las instalaciones de procesamiento de la información.

Registro de Eventos. Se generarán registros de auditoría que contengan excepciones y otros eventos relativos a la seguridad.

Los registros de auditoría deben incluir:

a) Identificación del usuario.
b) Fecha y hora de inicio y terminación.
c) Identidad o ubicación de la terminal, si se hubiera dispuesto identificación automática para la misma.
d) Registros de intentos exitosos y fallidos de acceso al sistema.
e) Registros de intentos exitosos y fallidos de acceso a datos y otros recursos.

En todos los casos, los registros de auditoría serán archivados preferentemente en un equipo diferente al que los genere y conforme los requerimientos de la Política de Retención de Registros.

Los Propietarios de la Información junto con la Unidad de Auditoría Interna o en su defecto quien sea propuesto por el Comité de Seguridad de la Información, definirán un cronograma de depuración de registros en línea en función a normas vigentes y a sus propias necesidades.

Procedimientos y Áreas de Riesgo. Se desarrollarán procedimientos para monitorear el uso de las instalaciones de procesamiento de la información, a fin de garantizar que los usuarios sólo estén desempeñando actividades que hayan sido autorizadas explícitamente.

Todos los empleados deben conocer el alcance preciso del uso adecuado de los recursos informáticos, y se les advertirá que determinadas actividades pueden ser objeto de control y monitoreo.

El alcance de estos procedimientos debe corresponderse a la evaluación de riesgos que realice el Responsable del Area Informática y el Responsable de Seguridad de la Información.

Entre las áreas que deben tenerse en cuenta se enumeran las siguientes:

a) Acceso no autorizado, incluyendo detalles como:
1. Identificación del usuario.
2. Fecha y hora de eventos clave.
3. Tipos de eventos.
4. Archivos a los que se accede.
5. Utilitarios y programas utilizados.

b) Todas las operaciones con privilegio, como:
1. Utilización de cuenta de supervisor.
2. Inicio y cierre del sistema.
3. Conexión y desconexión de dispositivos de Ingreso y Salida de información o que permitan copiar datos.
4. Cambio de fecha/hora.
5. Cambios en la configuración de la seguridad.
6. Alta de servicios.

c) Intentos de acceso no autorizado, como:
1. Intentos fallidos.
2. Violaciones de la Política de Accesos y notificaciones para "gateways" de red y "firewalls".
3. Alertas de sistemas de detección de intrusiones.

d) Alertas o fallas de sistema como:
1. Alertas o mensajes de consola.
2. Excepciones del sistema de registro.
3. Alarmas del sistema de administración de redes.
4. Accesos remotos a los sistemas.

Entre los factores de riesgo que se deben considerar se encuentran:
a) La criticidad de los procesos de aplicaciones.
b) El valor, la sensibilidad o criticidad de la información involucrada.
c) La experiencia acumulada en materia de infiltración y uso inadecuado del sistema.
d) El alcance de la interconexión del sistema (en particular las redes públicas).

Los Propietarios de la Información manifestarán la necesidad de registrar aquellos eventos que consideren críticos para la operatoria que se encuentra bajo su responsabilidad.

Registro y Revisión de Eventos. Se implementará un procedimiento de registro y revisión de los registros de auditoría, orientado a producir un informe de las amenazas detectadas contra los sistemas y los métodos utilizados.

La periodicidad de dichas revisiones será definida por los Propietarios de la Información y el Responsable de Seguridad de la Información, de acuerdo a la evaluación de riesgos efectuada.

Si el volumen de la información contenida en alguno de los registros fuera muy grande, el procedimiento indicará cuáles de los registros más significativos se copiarán automáticamente en registros auxiliares.

Por otra parte, el Responsable del Área Informática, podrá disponer la utilización de herramientas de auditoría o utilitarios adecuados para llevar a cabo el control unificado de los registros.

En la asignación de funciones en materia de seguridad de la información (Ver Control: Asignación de responsabilidades de la seguridad de la información), se debe separar las funciones entre quienes realizan la revisión y aquellos cuyas actividades están siendo monitoreadas.

Las herramientas de registro deben contar con los controles de acceso necesarios, a fin de garantizar que no ocurra:

a) La desactivación de la herramienta de registro.
b) La alteración de mensajes registrados.
c) La edición o supresión de archivos de registro.
d) La saturación de un medio de soporte de archivos de registro.
e) La falla en los registros de los eventos.
f) La sobrescrita de los registros.

La Unidad de Auditoría Interna o en su defecto quien sea propuesto por el Comité de Seguridad de la Información, tendrá acceso a los registros de eventos a fin de colaborar en el control y efectuar recomendaciones sobre modificaciones a los aspectos de seguridad. Adicionalmente podrían evaluar las herramientas de registro, pero no tendrán libre acceso a ellas.

4.3.7 Dispositivos Móviles y Trabajo Remoto. Su objetivo es asegurar la seguridad de la información cuando se utiliza medios de computación y teletrabajo móviles.

La protección requerida se debe conmensurar con los riesgos que causan estas maneras de trabajo específicas. Cuando se utiliza computación móvil, se deben considerar los riesgos de trabajar en un ambiente desprotegido y se debiera aplicar la protección apropiada. En el caso del tele-trabajo, la organización debe aplicar protección al lugar del tele-trabajo y asegurar que se establezcan los arreglos adecuados para esta manera de trabajar.

Computación Móvil. Cuando se utilizan dispositivos informáticos móviles se debe tener especial cuidado en garantizar que no se comprometa la información ni la infraestructura del Organismo.

Se debe tener en cuenta en este sentido, cualquier dispositivo móvil y/o removible, incluyendo:

Notebooks, Laptop o PDA (Asistente Personal Digital), Teléfonos Celulares y sus tarjetas de memoria, Dispositivos de Almacenamiento removibles, tales como CDs, DVDs, Disquetes, Tapes, y cualquier dispositivo de almacenamiento de conexión USB, Tarjetas de identificación personal (control de acceso), dispositivos criptográficos, cámaras digitales, etc.

Esta lista no es taxativa, ya que deben incluirse todos los dispositivos que pudieran contener información confidencial del Organismo y por lo tanto, ser pasibles de sufrir un incidente en el que se comprometa la seguridad del mismo.

Se desarrollarán procedimientos adecuados para estos dispositivos, que abarquen los siguientes conceptos:

a) La protección física necesaria
b) El acceso seguro a los dispositivos
c) La utilización segura de los dispositivos en lugares públicos.
d) El acceso a los sistemas de información y servicios del Organismo a través de dichos dispositivos.
e) Las técnicas criptográficas a utilizar para la transmisión de información clasificada.
f) Los mecanismos de resguardo de la información contenida en los dispositivos.
g) La protección contra software malicioso.

La utilización de dispositivos móviles incrementa la probabilidad de ocurrencia de incidentes del tipo de pérdida, robo o hurto. En consecuencia debe entrenarse especialmente al personal que los utilice. Se desarrollarán normas y procedimientos sobre los cuidados especiales a observar ante la posesión de dispositivos móviles, que contemplarán las siguientes recomendaciones:

a) Permanecer siempre cerca del dispositivo.
b) No dejar desatendidos los equipos.
c) No llamar la atención acerca de portar un equipo valioso.
d) No poner identificaciones del Organismo en el dispositivo, salvo los estrictamente necesarios.
e) No poner datos de contacto técnico en el dispositivo.
f) Mantener cifrada la información clasificada.

Por otra parte, se confeccionarán procedimientos que permitan al propietario del dispositivo reportar rápidamente cualquier incidente sufrido y mitigar los riesgos a los que eventualmente estuvieran expuestos los sistemas de información del Organismo, los que incluirán:

g) Revocación de las credenciales afectadas

h) Notificación a grupos de Trabajo donde potencialmente se pudieran haber comprometido recursos.

Trabajo Remoto. El trabajo remoto utiliza tecnología de comunicaciones para permitir que el personal trabaje en forma remota desde un lugar externo al Organismo.

El trabajo remoto sólo será autorizado por el Responsable de la Unidad Organizativa, o superior jerárquico correspondiente, a la cual pertenezca el usuario solicitante, conjuntamente con el Responsable de Seguridad de la Información, cuando se verifique que son adoptadas todas las medidas que correspondan en materia de seguridad de la información, de modo de cumplir con la política, normas y procedimientos existentes.

Estos casos serán de excepción y serán contemplados en situaciones que justifiquen la imposibilidad de otra forma de acceso y la urgencia, tales como horarios del Organismo, solicitud de las autoridades, etc.

Para ello, se establecerán normas y procedimientos para el trabajo remoto, que consideren los siguientes aspectos:

a) La seguridad física existente en el sitio de trabajo remoto, tomando en cuenta la seguridad física del edificio y del ambiente local.

b) El ambiente de trabajo remoto propuesto.

c) Los requerimientos de seguridad de comunicaciones, tomando en cuenta la necesidad de acceso remoto a los sistemas internos del Organismo, la sensibilidad de la información a la que se accederá y que pasará a través del vínculo de comunicación y la sensibilidad del sistema interno.

d) La amenaza de acceso no autorizado a información o recursos por parte de otras personas que utilizan el lugar, por ejemplo, familia y amigos.

e) Evitar la instalación/desinstalación de software no autorizada por el Organismo.

Los controles y disposiciones comprenden:

a) Proveer de mobiliario para almacenamiento y equipamiento adecuado para las actividades de trabajo remoto.

b) Definir el trabajo permitido, el horario de trabajo, la clasificación de la información que se puede almacenar en el equipo remoto desde el cual se accede a la red del Organismo y los sistemas internos y servicio a los cuales el trabajador remoto está autorizado a acceder.

c) Proveer de un adecuado equipo de comunicación, con inclusión de métodos para asegurar el acceso remoto.

d) Incluir seguridad física.

e) Definir reglas y orientación respecto del acceso de terceros al equipamiento e información.

f) Proveer el hardware y el soporte y mantenimiento del software.

g) Definir los procedimientos de backup y de continuidad de las operaciones.

h) Efectuar auditoría y monitoreo de la seguridad.

i) Realizar la anulación de las autorizaciones, derechos de acceso y devolución del equipo cuando finalicen las actividades remotas.

j) Asegurar el reintegro del equipamiento en las mismas condiciones en que fue entregado, en el caso en que cese la necesidad de trabajar en forma remota.

Se implementarán procesos de auditoría específicos para los casos de accesos remotos, que serán revisados regularmente. Se llevará un registro de incidentes a fin de corregir eventuales fallas en la seguridad de este tipo de accesos.

En los anexos D y E, se encuentran la lista de chequeo y una carta, como herramientas para llevar un mejor control de la seguridad de la información.

4.3.8 Guía práctica para el control de acceso de los sistemas de información del hospital Emiro Quintero Cañizares usando como herramienta las ISO /IEC 27001:2005. Para dar solución al CONTROL DE ACCESO del sistema de información my process daremos a continuación una muy sencilla serie de pasos a tener en cuenta por parte del administrador del sistema del hospital al momento de dar contraseñas y privilegios a los usuarios de la E.S.E.

1. El administrador de los sistemas definirá un procedimiento formal de registro de usuarios para otorgar y revocar el acceso a todos los sistemas, bases de datos y servicios de información multiusuario, el cual debe comprender:

Utilizar los identificadores de usuarios únicos, de manera que se pueda identificar a los usuarios por sus acciones evitando la existencia de múltiples perfiles de acceso para un mismo empleado.

Cancelar inmediatamente los derechos de acceso de los usuarios que cambiaron sus tareas o han sido retirados de la E.S.E.

Incluir cláusulas en los contratos de personal y de servicios que especifique sanciones si el personal que presta el servicio intenta un acceso no autorizado.

2. El administrador identifica a los usuarios, debe tener en cuente la siguiente información:

Los nombres de usuario deben ser únicos.
Evitar crear nombres de usuarios similares.
No debe contener símbolos como: [] <> + - * /. : = , ?.

3. Revisión de derechos de acceso a usuarios.

Debe solicitar por escrito la activación o desactivación de algún usuario, adjunto quien solicita y cargo dentro de la E.S.E.

4. limitar y controlar la asignación y uso de privilegios, debido a que el uso inadecuado de los privilegios del sistema resulta frecuentemente en el factor más importante que contribuye a la falla de los sistemas a los que se accedió ilegalmente.

5. limitar las conexiones de los usuarios y proporcionar a los equipos los permisos para el uso adecuado del internet.

6. Informar por escrito a los usuarios las sanciones correspondientes a las violaciones de los parágrafos anteriores.

7. Revisar periódicamente el manejo de los privilegios para dar soporte y mantenimiento al sistema my process.

8. Controlar por medio de una bitácora el acceso a personal médico de visita a la E.S.E. Que ingrese al sistema para conocer posibles cambios que atenten contra la seguridad de la información.

9. Informar de las irregularidades y eventos relevantes que atenten contra la seguridad de la información.

10. La confidencialidad de la información es completamente es responsabilidad del solicitante.

11. El acceso a la cuenta es personal e intransferible.

12. Queda estrictamente prohibido compartir la cuenta de acceso con otras personas.

13. Es necesario que el usuario cambie la contraseña de acorde a las políticas de seguridad.

14. En caso de que el usuario cambie de funciones o se reubique en otra área administrativa, deberá notificarlo por los medios institucionales a la Gerencia de Informática para realizar las acciones correspondientes en cuanto a claves de acceso.

15. La información contenida en los sistemas es propiedad de Empresa, es responsabilidad del usuario aplicar la confidencialidad de la misma, en caso contrario se procederá jurídicamente según sea el caso.

16. En caso de violar los puntos alguno de los puntos anteriores se hará acreedor a una sanción que determine la Empresa.

17. El uso de esta información es exclusivamente para fines laborales de la institución.

4.3.8.1 Funciones y privilegios del personal del área de urgencias del hospital Emiro Quintero Cañizares. En los centros hospitalarios se debe tener en cuenta principalmente la variedad de gente que compone el ambiente típico del hospital - pacientes, personal, vendedores, médicos, visitantes e incluso sus enemigos. La tipología del lugar queda definida por muchos cuartos, habitaciones, salas, espacios, equipos de alto valor, accesibilidad a las drogas, muchas entradas y salidas. Y siempre valorando todos los aspectos que faciliten el movimiento en el edificio y alrededores.

La seguridad es esencial en este tipo de entornos. Los encargados del hospital basan sus decisiones en la protección y reputación de su entidad.

Las principales amenazas en un ambiente hospitalario son el hurto por parte de empleados o del visitante, vandalismo de personal ajeno al hospital y amenazas contra pacientes o el personal interno.

EL SERVICIO DE URGENCIAS. El servicio de Urgencias de cada hospital, sigue una distribución basada en la funcionalidad y la operatividad. No olvidemos que uno de los lugares por donde el paciente suele ingresar, es el servicio de urgencias, debiendo para ello tener una organización adecuada y funcional, con unas zonas definidas y delimitadas para una correcta atención y que no se produzcan retrasos en la atención al enfermo o una desorganización en cuanto a la atención del mismo. En un servicio de urgencias, tendremos las siguientes áreas o salas:

Admisión de Urgencias.
Sala de Triage.
Primer nivel de atención o críticos.
Segundo nivel o boxes
Salas de espera y observación.

ADMISIÓN DE URGENCIAS: Su objetivo es registrar las entradas y salidas de los pacientes y dirigirlos a la unidad de Triage. En ocasiones actúa como centro de información de pacientes y como servicio general de Admisión en días festivos o fines de semana. Entre sus funciones destacamos:

Registro de entrada de pacientes.
Derivación del paciente al triage.

Custodia de pertenencias en casos excepcionales o a solicitud del enfermo.
Avisar a ambulancias.
Cumplimentar la documentación oportuna (partes al juzgado, etc.)

TRIAGE: Es el lugar físico en el que el profesional de enfermería y el personal médico acogen, clasifican y ubican a los enfermos. En los hospitales este término está empezando a no usarse, sustituyéndolo por R.A.C (Recepción Acogida y Clasificación) dejando la palabra Triage, para catástrofes.

PRIVILEGIOS EN EL SISTEMA MY PROCESS:

Ingresa con su número de cedula.
ingresa número de cedula del paciente.
ingresa los síntomas dados por el paciente y lo remite al área correspondiente.

PRIMER NIVEL DE ATENCIÓN DE CRÍTICOS: Corresponde al área del servicio de Urgencias en el que se tratan a aquellos pacientes cuyo estado de gravedad es grave o muy grave, o bien que sin serlo precisan de una atención inmediata a fin de evitar una situación de mayor gravedad.

SEGUNDO NIVEL O SALA DE BOXES: Es donde los profesionales sanitarios llevan a cabo acciones para mejorar la salud de los pacientes que presentan un riesgo moderado o grave que no compromete su salud.

Salas de espera y observación: Donde estarán los familiares de los enfermos o acompañantes, a la espera de que sean requeridos para información médica. Generalmente se encuentra ubicada al lado de la puerta de entrada de urgencias, junto al servicio de admisión.

La sala de observación, es un lugar habilitado con camas, donde el enfermo estará un máximo de 24 h., para “observar” la evolución de su enfermedad, para posteriormente o bien ingresarlo en la unidad de hospitalización correspondiente, o bien, irse de alta para su domicilio.

LA ATENCION DEL CELADOR EN EL SERVICIO DE URGENCIAS. El celador en este servicio se ocupará de lo siguiente:

Celador de Puerta
Nunca dejará la puerta sin atención.
Recepción y ayuda a los pacientes que vengan en vehículos particulares y ambulancias.
Recepción y ayuda a pacientes ambulantes.
Transporte de los pacientes en sillas de ruedas, camillas, etc.

Trasladar al enfermo al mostrador de Admisión de Urgencias para que el personal administrativo tome datos. En caso de que su estado de salud no le permita esperar, lo pasará directamente a la zona de triage.

Aviso al personal sanitario cuando sea preciso.

Mantener un número suficiente de sillas de ruedas y camillas en la entrada de urgencias.
Vigilancia de las entradas al Área de urgencias, no permitiendo el acceso a sus dependencias más que a las personas autorizadas para ello.

Información general no sanitaria, no administrativa. (EL CELADOR NUNCA INFORMA DEL ESTADO DE UN ENFERMO).

Mantenimiento de las normas de convivencia general (no fumar, buen uso de las instalaciones, etc.

Indicar a los familiares o al paciente que aguarden en la sala de espera de la zona de triage, donde será visto por un facultativo que valorará su situación.

Instalar al paciente en el box.

Controlar que solamente pase a la zona de boxes un acompañante por paciente.

NO TIENE ACCESO NI PRIVILEGIOS AL SISTEMA MY PROCESS.

AUXILIAR DE ENFERMERÍA DE BOXES :(departamento dentro del servicio)

Instalar al paciente en el box, movilizándolo y colocándolo en la posición que le sugiera.
Acompañar o trasladar al paciente a realizar pruebas de diagnóstico en el interior del servicio (TAC, radiografías, ecografías etc.)

Llevar muestras de orina, heces, sangre etc. hasta los laboratorios correspondientes.
Ayudar en punciones lumbares, inyectables y otras pruebas que requieran inmovilización. (Colocando al enfermo en la posición que le solicite)

PRIVILEGIOS EN EL SISTEMA MY PROCESS:

Ingresa con su número de cedula.
Ingresa número de cedula del paciente.
El sistema solo le mostrara los procedimientos y formulación para el suministro de medicamentos del paciente.
Tiene privilegios de solo lectura.

ENFERMERO JEFE DE ÁREAS ESPECÍFICAS DENTRO DEL SERVICIO:

Dentro del servició, existen unos boxes específicos para una atención concreta, entre ellos: Quirofanillo, (lugar de cirugía menor, sutura y limpieza de heridas) sala de yesos (colocación de vendajes y yesos) Box vital o de R.C.P (box acondicionado para reanimaciones, y atenciones vitales de urgencia extrema).

En estas zonas, tendrá las siguientes funciones:

Custodiar la zona quirúrgica de toda persona ajena al área de urgencias.
Pasar a los enfermos de uno en uno (salvo en casos excepcionales)
Mantener la intimidad del paciente.
Ayudar si lo requieren en la colocación de yesos, férulas etc.
Ayudar si lo requieren en la realización por parte del médico de suturas, curas quirúrgicas, etc.

Transporte y control interno de pacientes y familiares.
Ayuda al personal sanitario en general.

Auxilio en aquellas labores propias del celador en las áreas de Yesos y Quirófano de cirugía menor, así como las que sean ordenadas por los médicos, supervisoras o enfermeras.
Transporte y control de documentos, correspondencia u objetos.

Control de personas en el área interna de urgencias.

Ayuda en la higiene de los pacientes en las camas de observación, así como en su movilización.

Atención a la sala de Reanimación Cardiopulmonar.
Transporte de aparatos y mobiliario dentro de la unidad.
Colaboración en la inmovilización y sujeción de enfermos mentales agitados.
Traslado de pacientes a Radiología, y traerlos de vuelta una vez realizada la prueba.

Traslado de documentos, correspondencia u objetos a los laboratorios y servicios o unidades del Hospital.

Traslado de los pacientes a las unidades de Hospitalización y unidades especiales.
Traslado de cadáveres al mortuorio.

PRIVILEGIOS EN EL SISTEMA MY PROCESS:

Ingresa con su número de cedula.
Ingresa número de cedula del paciente.

El sistema le mostrara los procedimientos y formulación para el suministro de medicamentos del paciente.

Tiene privilegios de escritura para ingresar funciones y órdenes dadas por los médicos.
Determina el auxiliar que debe prestar el servicio.
Prescribe los procedimientos y formulas médicas con su respectiva dosificación.

FUNCIONES DEL CAMILLERO EN URGENCIAS:

En el antiguo estatuto de Personal No sanitario, se establecía que los celadores “tendrán a su cargo el traslado de enfermos, tanto dentro de la institución como en el servicio de ambulancias”. Las tareas concretas que el CAMILLERO debe realizar con relación a las ambulancias son:

Trasladar a los pacientes en camilla o silla desde el centro sanitario hasta la puerta de acceso a la ambulancia y viceversa.

Pasar al paciente desde la camilla del hospital hasta la camilla de la ambulancia (esta maniobra se ha de realizar simultáneamente entre varios profesionales) se colocan las camillas juntas, se sujeta la sábana sobre la que descansa el paciente por varios puntos y todos a la vez alzan la sábana pasando al enfermo hacia la otra camilla.

Ayudar al paciente a introducirse en la ambulancia, en caso de que éste no vaya en camilla, sino en silla de ruedas o por sus propios medios.

Ayudar al conductor de la ambulancia en caso de dificultad de maniobra de introducción o salida de la camilla en la ambulancia. Hoy día las ambulancias tienen incorporados sistemas automáticos de entrada-salida de las camillas con patas plegables y desplegables

Acompañar al paciente durante el traslado en la ambulancia si es requerido. El celador irá sentado en el asiento existente al efecto junto al enfermo. Al llegar a destino preparará todo lo necesario para bajarlo.

Dentro de la ambulancia ayudará al personal sanitario en las mismas tareas que le corresponde respecto de los pacientes encamados del hospital (mover a los que lo necesiten).

No tiene acceso ni privilegios al sistema my process.

Los médicos generales y los especialistas tienen los privilegios de ingreso y cambio de información en las historias clínicas de los pacientes. Nunca deben revelar su clave de acceso a ningún otro compañero de trabajo.

5. CONCLUSIONES

Luego de desarrollado el estudio se obtuvo el reconocimiento de las áreas del Hospital Emiro Quintero Cañizares Ocaña, relacionadas con el sistema de información MY PROCESS. En esta empresa se encuentran las áreas de urgencias, hospitalización, consulta externa, consulta interna; en las cuales se maneja una gran cantidad de información que debe estar asegurada.

Al identificar los factores que ocasionan riesgos en la integridad, confidencialidad y disponibilidad de la información del sistema MY PROCESS, de acuerdo al dominio control de acceso de la ISO 27001:2013, se realizó mediante un mapa de riesgos de los procesos informáticos, en el Hospital Emiro Quintero Cañizares. Además, de un registro de los riesgos encontrados en el Hospital Emiro Quintero Cañizares, todo ello teniendo en cuenta su calificación de acuerdo a la escala de riesgo.

Con el fin de documentar la guía práctica que permitirá orientar los procesos y procedimientos para el control de acceso al sistema MY PROCESS del Hospital Emiro Quintero Cañizares Ocaña, se realizó teniendo en cuenta la cláusula gestión de accesos de la ISO 27001, el cual aduce que el acceso por medio de un sistema de restricciones y excepciones a la información es la base de todo sistema de seguridad informática. Para impedir el acceso no autorizado a los sistemas de información se deben implementar procedimientos formales para controlar la asignación de derechos de acceso a los sistemas de información, bases de datos y servicios de información, y éstos deben estar claramente documentados, comunicados y controlados en cuanto a su cumplimiento.

REFERENCIAS DOCUMENTALES ELECTRÓNICAS

http://www.iso27001standard.com/es/que-es-iso-27001/

http://www.iso27000.es/iso27000.html

OJEDA PÉREZ, Jorge Eliécer. Delitos informáticos y entorno jurídico vigente en Colombia. (online) [Bogotá] 2010, [citado 23 jun., 2014]. Disponible en: http://www.sci.unal.edu.co/scielo.php?script=sci_arttext&pid=S0123-14722010000200003&lng=es&nrm=iso

http://www.dnvba.com/es/Certificacion/Sistemas-de-Gestion/Gestion-de-continuidad-de-negocio/Pages/default.aspx

MINISTERIO DE LA INFORMATICA Y LAS COMUNICACIONES. Reglamento sobre Seguridad Informática. La Habana. Cuba. 2012. 15h. [en línea]. http://fcmfajardo.sld.cu/seguridad_informatica/resol_y_dispos_del_mic/reglamento_seguridad_informatica.pdf

http://www.codejobs.biz/es/blog/2012/09/07/seguridad-informatica-que-es-una-vulnerabilidad-una-amenaza-y-un-riesgo

http://www.welivesecurity.com/la-es/2013/12/12/iso-iec-27002-2013-cambios-dominios-control/

ANEXOS

Anexo A. Encuesta al área de facturación y urgencias del Hospital Emiro Quintero Cañizares de Ocaña

Dirigida a: Personal del Área de facturación y urgencias.

CUESTIONARIO CONTROL Y USO DE SOFTWARE			
ENTIDAD:	**ESE HOSPITAL EMIRO QUINTERO CAÑIZARES**		
PROCESO	**ADMINISTRACION DE RECURSOS INFORMATICOS**	**SUBPROCESO**	**SOPORTE**
RESPONSABLE DEL PROCESO AUDITADO:		**ALEXANDER BECERRA**	
LIDER EQUIPO AUDITOR: **YAN LEONAR VERGEL (YV)**		**AUDITOR:** **RICHAR MARTINEZ (RM)**	
PREGUNTAS	**RESPUESTAS**		**EVIDENCIA**
¿el software instalado en los equipos cuenta con las licencias legalmente exigidas?			
¿Cómo detecta el software no autorizado?			
¿Cómo controla que los antimalware estén instalados?			
¿Cómo se lleva el registro de garantía del software instalado?			
Observaciones: Se hará una verificación minuciosa de cada uno de los elementos del centro de cómputo para tener veracidad de las respuestas dadas.			

Anexo B. Mapa de riesgos

NUM	RIESGO	IMPACTO	PROBABILIDAD	CONTROLES EXISTENTES	NIVEL DE RIESGO	CAUSAS	ACCIONES	CRONOGRAMA
1.	PERDIDA DE ARCHIVOS	ALTO	ALTA	REGISTRO DE VISITA DE HISTORIAS CLINICAS LIBRO RADICADOR DE PRESTAMO DE DOCUMENTOS	ALTO	ENTREGA DE HISTORIAS SIN EL DEBIDO PROCESO PERDIDA DE INFORMACION DE HISTORIAS CLINICAS DESORGANIZACION DE ARCHIVO	SISTEMATIZAR EL ARCHIVO CENTRAL MICROFILMACION AMPLIAR PERSONAL GUIA PRACTICA PARA EL CONTROL DE ACESO A MY PROCESS	INICIA DICIEMBRE DE 2014 TERMINA MARZO DE 2015
2.	INFECCCION DE VIRUS INFORMATICO	ALTO	ALTA	ANTIVIRUS BLOQUEO DE PAGINAS DE INTERNET RESTRICCION DE USUARIOS	ALTO	MEMORIAS CONTAMINADAS MALWARE INFORMSTICO DE INTERNET FALTA DE ANTIVIRUS	CONTROL DE ACCESO A INTERNET CONTROL DE ACCESO A MY PROCESS ACTUALIZAR ANTIVIRUS	INICIA DICIEMBRE DE 2014 TERMINA MARZO DE 2015

Anexo C. Registro de riesgos

CÓDIGO	CAUSA	DESCRIPCIÓN DEL RIESGO	REFERENCIA	RELACIÓN	PROBABILIDAD	IMPACTO	P X I	ACCIONES	RESERVAS	SEÑALES	ESTRATEGIA	ESTRATEGIA DE RESPALDO	RESPONSABLE	FECHA
RPO10-01	Administración de proyectos - Planificación -	**Si** los lideres no cuentan con formación y competencias en gestión de proyectos **puede ocasionar** sobrecostos en el proyecto.	punto 01		0,5	0,4	0,20	MITIGAR	Para el tratamiento de los riesgos identificados durante el proyecto se establecerá un 10 % del valor del proyecto. En caso de que estos no requieran inversión económica el dinero debe ser reembolsado a la organización.	Desconocimiento en competencias de proyectos.	Generar un plan de capacitación y formación en competencias de Formulación, evaluación y gestión de proyectos para las personas que lideran proyectos.		Gerente y Jefe RRHH	abr-15
RPO10-02	Adquirir y Mantener Infraestructura Tecnología - Implementación	**Si** la información asociada con el proyecto se encuentra almacenada exclusivamente en un servidor de la empresa y este presenta una falla **puede ocasionar** la perdida de la información generando un impacto económico en la organización.	punto 03		0,5	0,4	0,20	MITIGAR	Para el tratamiento de los riesgos identificados durante el proyecto se establecerá un 10 % del valor del proyecto. En caso de que estos no requieran inversión económica el dinero debe ser reembolsado a la organización.	Presencia de bloqueo de equipo.	Documentar e implementar un procedimiento de respaldo y restauración de información de proyectos.	Implementación de Ciclos de mantenimiento de Servidores	Jefe de TI	ene-15
RPO10-03	Adquirir y Mantener Infraestructura Tecnología - Implementación	**Si** la información asociada con el proyecto se encuentra almacenada exclusivamente en un servidor de la empresa y este presenta una falla **puede ocasionar** la perdida de la información generando retrasos en la entrega de B/S comprometidos.	punto 03		0,5	0,4	0,20	MITIGAR	Para el tratamiento de los riesgos identificados durante el proyecto se establecerá un plazo de 30 días para cumplir con las entregas de B/S comprometidos.	Presencia de bloqueo de equipo.	Documentar e implementar un procedimiento de respaldo y restauración de información de proyectos.	Implementación de Ciclos de mantenimiento de Servidores	Jefe de TI	ene-15

RPO10-04	Identificar Soluciones Automatizadas - Análisis	Si no se realiza un análisis antes de la creación de las aplicaciones **puede ocasionar** retrasos en los entregables.	punto 04	punto 01	0,9	0,2	0,18	MITIGAR	Para el tratamiento de los riesgos identificados durante el proyecto se establecerá un plazo de 30 días para cumplir con las entregas de B/S comprometidos.	Insatisfacción de los usuarios por incumpliendo de los requerimientos funcionales	Definir un procedimiento para el desarrollo de software que incluya detalladamente cada una de las etapas a efectuar en el desarrollo de aplicaciones	Implementación de registros para evidenciar las etapas en la creación de aplicaciones.	Jefe de TI	ene-15
RPO10-05	Administración de proyectos - Planificación	Si los proyectos no se alinean con los objetivos de la Organización **puede ocasionar** un impacto económico debido a proyectos sin concluir o abandonados.	punto 05	punto 01 y punto 02	0,5	0,4	0,20	MITIGAR	Para el tratamiento de los riesgos identificados durante el proyecto se establecerá un 10 % del valor del proyecto. En caso de que estos no requieran inversión económica el dinero debe ser reembolsado a la organización.	Desinterés del personal en la ejecución del proyecto.	Implementación de Auditorias internas al finalizar cada etapa del proyecto.		Gerencia	Duración del Proyecto
RAI2-01	Administración de proyectos - Planificación -	**Si** los lideres no cuentan con formación y competencias en gestión de proyectos **puede ocasionar** problema en la definición del alcance del proyecto.	punto 01		0,5	0,2	0,10	MITIGAR	Para el tratamiento de los riesgos identificados durante el proyecto se establecerá un 10 % del valor del proyecto y un plazo de 30 días para cumplir con las entregas de B/S comprometidos. En caso de que estos no requieran inversión económica el dinero debe ser reembolsado a la organización.	Desconocimiento en competencias de proyectos.	Generar un plan de capacitación y formación en competencias de Formulación, evaluación y gestión de proyectos para las personas que lideran proyectos.		Gerente y Jefe RRHH	abr-15

RAI2-02	Administración de proyectos - Planificación -	**Si** los lideres no cuentan con formación y competencias en gestión de proyectos **puede ocasionar** retrasos en los B/S comprometidos.	punto 01		0,5	0,2	0,10	MITIGAR	Para el tratamiento de los riesgos identificados durante el proyecto se establecerá un plazo de 30 días para cumplir con las entregas de B/S comprometidos.	Desconocimiento en competencias de proyectos.	Generar un plan de capacitación y formación en competencias de Formulación, evaluación y gestión de proyectos para las personas que lideran proyectos.		Gerente y Jefe RRHH	abr-15
RAI1-01	Administración de proyectos - Planificación -	**Si** no se cuenta con una metodología estándar de administración de proyectos **puede ocasionar** retrasos en el proyecto al no aprovechar lecciones aprendidas	punto 02	punto 01	0,5	0,1	0,05	MITIGAR	Para el tratamiento de los riesgos identificados durante el proyecto se establecerá un plazo de 30 días para cumplir con las entregas de B/S comprometidos.	Todos los proyectos no realizan la misma secuencia de etapas.	Establecer una metodología estándar de acuerdo al tipo de proyecto.		Lideres de Proyectos	ene-15
RAI1-02	Identificar Soluciones Automatizadas - Análisis	Si no se realiza un análisis antes de la creación de las aplicaciones **puede ocasionar** sobre costos por la inclusión de nuevos módulos que originalmente no se habían previstos.	punto 04	punto 01	0,5	0,2	0,10	MITIGAR	Para el tratamiento de los riesgos identificados durante el proyecto se establecerá un 10 % del valor del proyecto. En caso de que estos no requieran inversión económica el dinero debe ser reembolsado a la organización.	Insatisfacción de los usuarios por incumpliendo de los requerimientos funcionales	Definir un procedimiento para el desarrollo de software que incluya detalladamente cada una de las etapas a efectuar en el desarrollo de aplicaciones	Implementación de registros para evidenciar las etapas en la creación de aplicaciones.	Jefe de TI	ene-15
PO10-3	Identificar Soluciones Automatizadas - Viabilidad Tecnológica	**Si** no se realiza una revisión de viabilidad técnica del proyecto **Puede ocasionar** retraso en el B/S comprometido.	punto 06		0,5	0,1	0,05	MITIGAR	Para el tratamiento de los riesgos identificados durante el proyecto se establecerá un plazo de 30 días para cumplir con las entregas de B/S comprometidos.	Retrasos durante la fase de ejecución técnica del proyecto.	Realizar estudio de viabilidad técnica de los proyectos.	Realizar pruebas técnicas a los proyectos.	Jefe de TI	Durante la evaluación de viabilidad técnica del proyecto.

RAI1-03	Facilitar la operación y el uso de nuevos sistemas que se encuentren disponibles - Documentación	**Si** los manuales de usuarios de las aplicaciones desarrolladas no contemplan todas las funcionalidades, o están desactualizados o no son de fácil acceso **puede ocasionar** sobre costos por prestación de servicios del personal de soporte para atender las necesidades de los usuarios.	punto 07		0,9	0,1	0,09	MITIGAR	Para el tratamiento de los riesgos identificados durante el proyecto se establecerá un 10 % del valor del proyecto. En caso de que estos no requieran inversión económica el dinero debe ser reembolsado a la organización.	Aumento en la prestación de soporte técnico.	Establecer el lineamiento de control dentro del área de TI, que todos los manuales de usuarios deben ser revisados y autorizados por el Jefe de TI, para su posterior sensibilización y publicación.		Jefe de TI	dic-14
RAI4-01	Facilitar la operación y el uso de nuevos sistemas que se encuentren disponibles - Documentación	**Si** no se cuenta con manuales de instalación de las aplicaciones desarrolladas en los proyectos **puede ocasionar** sobre costos por la prestación de servicios de personal de soporte para atender fallas por desconfiguración del sistema.	punto 08	punto 07	0,9	0,1	0,09	MITIGAR	Para el tratamiento de los riesgos identificados durante el proyecto se establecerá un 10 % del valor del proyecto. En caso de que estos no requieran inversión económica el dinero debe ser reembolsado a la organización.	Aumento en la prestación de soporte técnico.	Establecer el lineamiento de control dentro del área de TI, que todos los manuales de instalación deben ser revisados y autorizados por el Jefe de TI, para su posterior sensibilización y publicación.		Jefe de TI	dic-14
RAI4-02	Recursos de TI - Selección y contratación	Si la organización no cuenta con un procedimiento documentado para la selección, contratación, registros de evaluación y re-evaluación de proveedores para los proyectos **puede ocasionar** retrasos en los entregables de B/S comprometidos.	punto 09	punto 01	0,5	0,2	0,10	MITIGAR	Para el tratamiento de los riesgos identificados durante el proyecto se establecerá un plazo de 30 días para cumplir con las entregas de B/S comprometidos.	*Demoras en los pedidos *Aumento en los reclamos y solicitudes de garantía	Documentar e implementar un procedimiento de selección, contratación, registros de evaluación y re-evaluación de proveedores para los proyectos.	Implementación de registros para evidenciar el proceso de selección y contratación de proveedores.	Gerencia - Jurídica - directores de proyecto	mar-15

RAI5-01	Recursos de TI - Selección y contratación	Si la organización no cuenta con un procedimiento documentado para la selección, contratación, registros de evaluación y re-evaluación de proveedores para los proyectos **puede ocasionar** deficiencia en la calidad de los B/S comprometidos.	punto 09	punto 01	0,5	0,2	0,10	MITIGAR	Para el tratamiento de los riesgos identificados durante el proyecto se establecerá un 10 % del valor del proyecto. En caso de que estos no requieran inversión económica el dinero debe ser reembolsado a la organización.	*Demoras en los pedidos *Aumento en los reclamos y solicitudes de garantía	Documentar e implementar un procedimiento de selección, contratación, registros de evaluación y re-evaluación de proveedores para los proyectos.	Implementación de registros para evidenciar el proceso de selección y contratación de proveedores.	Gerencia - Jurídica - directores de proyecto	mar-15
RAI5-02	Administración de proyectos - Planificación -	**Si** no se cuenta con una metodología estándar de administración de proyectos **puede ocasionar** sobrecostos en el proyecto al no aprovechar lecciones aprendidas	punto 02	punto 01	0,3	0,1	0,03	MITIGAR	Para el tratamiento de los riesgos identificados durante el proyecto se establecerá un 10 % del valor del proyecto. En caso de que estos no requieran inversión económica el dinero debe ser reembolsado a la organización.	Todos los proyectos no realizan la misma secuencia de etapas.	Establecer una metodología estándar de acuerdo al tipo de proyecto.		Lideres de Proyectos	ene-15

Anexo D. Lista de chequeo

LISTA DE CHEQUEO

AUDITORIA SEGURIDAD DE LA INFORMACION

1	**Los empleados de la empresa tienen legalizado el acuerdo de confidencialidad?** Mostrar evidencia Observaciones	SI ___	NO ___
2	**Ha ingreado personal nuevo a la empresa?**	SI ___	NO ___
3	**Se mantiene la politica de selección de personal?**	SI ___	NO ___
4	**Qué documentos fueron solicitados para el ingreso de los ultimos trabajadores?** a.Certificado Judicial Actualizado b. Copia de la cédula - Libreta Militar c. Referencias laborales d. Motorizados: Pase-Soat-Tarjeta de Propiedad		
5	**Los usuarios han sido creados de acuerdo al procedimiento establecido?**	SI ___	NO ___
6	**Se mantiene actualizada la matriz de perfiles de usuarios**	SI ___	NO ___
7	**Mostrar evidencia de los soportes de creación de los últimos usuarios creados**	SI ___	NO ___
8	**Se mantienen registros de Logs de seguridad de los sistemas operativos** Qué aspectos se auditan?	SI ___	NO ___

9	**Se mantiene actualizada la clasificación de la información de Distrienvios?** Mostrar listado de evidencia	SI ___	NO ___
10	**Se mantiene actualizado el inventario de los recursos informaticos de la empresa?**	SI ___	NO ___
11	**Se mantiene un listado de los programas propietarios y licenciados de la empresa?** Mostrar evidencia	SI ___	NO ___
12	**Se mantiene el control del ingreso del personal autorizado al área de sistemas?** Mostrar evidencia de la bitácora	SI ___	NO ___

13	**Se mantiene el programa de escritorio limpio?** Dpto _____ Check list de escitorio limpio		
	a. Mantiene objetos innecesario en el puesto de trabajo?	SI ___	NO ___
	b. Tiene activado el protector de pantalla del monitor?	SI ___	NO ___
	c. Mantiene resguardada la información confidencial y/o restringida?	SI ___	NO ___
	d. Mantiene archivadores y/o gavetas que contiene información sensitiva bajo llave?	SI ___	NO ___
	e. Destruye el papel desechado en la forma correcta?	SI ___	NO ___
14	**Se mantiene el control del Ingreso de visitantes?** Mostrar evidencia	SI ___	NO ___
15	**Se mantiene el control del ingreso de funcionarios en horarios no habiles** Mostrar evidencia	SI ___	NO ___
16	**cada cuánto se realiza la revisión de estos controles de acceso?** Mostrar evidencia	_____	
17	**Se mantiene la función de los sistemas de alarmas?**	SI ___	NO ___

18	**Se mantiene un listado del personal con acceso a áreas críticas aparte del data center como las bodegas ?** Mostrar listado	SI	NO
19	**Se aplica la política de configuración de password?**	SI	NO
20	**Qué tiempo de cambios de password está parametrizado en el sistema?**		
21	**Qué versión de antivirus se maneja actualmente?**		
22	**Cada cuánto se actualiza el antivirus?**		
23	**Se lleva a cabo el procedimiento de backups?**	SI	NO
24	**Cada cuánto se realiza el backup de la información?** Mostrar evidencia		
25	**Se está almacenando la copia del backups en un lugar alterno?**	SI	NO

Verificar si la información sensible es cifrada antes de ser enviada por canales inseguros

Revisión de Logs de los Usuarios con privilegios

Revisar periodicamente las instalacions físicas de la empresa

Revisar el cumplimiento de la identificación de la información

Revisar el cumplimiento del procedimiento de retención de registros

Verificar Fondos de Pantallas y Conexión a Internet

Se mantine capacitacion constante al comité paritario - Asesoria ARP

Verificar si se imparte capacitación al personal nuevo sobre políticas de seguridad

Capacitación periódica para reforzar temas de políticas de seguridad

Verificar cumplimiento de las políticas en las sucursales

Realizar Reportes a Gerencia de las inconsistencias para sanciones pertinentes

Anexo E. Carta de control de acceso

En su carácter de Usuario designado, le hago entrega de la cuenta de acceso a Empresa

Nombre: Nombre Apellido Puesto: Consultor de Seguridad e infraestructura.
Departamento: Seguridad e infraestructura Área: Gerencia de Informática
Cuenta de usuario: Correo electrónico:

Acepto la responsabilidad por el uso de Cuenta de usuario de acuerdo a los permisos que se otorgan en mi perfil, así como a las responsabilidades en que pudiera incurrir en materia de responsabilidad del Control de Accesos por el uso de la información, incluso aquella considerada como confidencial, de conformidad con lo establecido en las leyes y normatividad vigente aplicable para tal efecto.

- La confidencialidad de la información es completamente es responsabilidad del solicitante.
- El acceso a la cuenta es personal e intransferible.
- Queda estrictamente prohibido compartir la cuenta de acceso con otras personas.
- Es necesario que el usuario cambie la contraseña de acorde a las políticas de seguridad.
- En caso de que el usuario cambie de funciones o se reubique en otra área administrativa, deberá notificarlo por los medios institucionales a la Gerencia de Informática para realizar las acciones correspondientes en cuanto a claves de acceso.
- La información contenida en los sistemas es propiedad de Empresa, es responsabilidad del usuario aplicar la confidencialidad de la misma, en caso contrario se procederá jurídicamente según sea el caso.
- En caso de violar los puntos alguno de los puntos anteriores se hará acreedor a una sanción que determine la Empresa.
- El uso de esta información es exclusivamente para fines laborales de la institución.

Quedando de enterado de los estatutos mencionados usted firma de conformidad a lo establecido por la Gerencia de Informática.

Autorizó Vo. Bo. Aceptó

Director o Gerente del Área Jefe Inmediato Usuario

Asegurar que se aplica un nivel de protección adecuado a la información.

Se debería clasificar la información para indicar la necesidad, prioridades y nivel de protección previsto para su tratamiento.

La información tiene diversos grados de sensibilidad y criticidad. Algunos ítems podrían requerir niveles de protección adicionales o de un tratamiento especial. Debería utilizarse un esquema de clasificación de la información para definir el conjunto adecuado de niveles de protección y comunicar la necesidad de medidas especiales para el tratamiento.

Consejos de implantación

¡Mantenga la sencillez! Distinga los requisitos de seguridad básicos (globales) de los avanzados, de acuerdo con el riesgo.

Comience quizás con la confidencialidad, pero no olvide los requisitos de integridad y disponibilidad.

Métrica. Porcentaje de activos de información en cada categoría de clasificación (incluida la de "aún sin clasificar").

Evitar incumplimientos de cualquier ley, estatuto, regulación u obligación contractual y de cualquier requisito de seguridad.

El diseño, operación, uso y gestión de los sistemas de información pueden ser objeto de requisitos estatutarios, reguladores y de seguridad contractuales.

Los requisitos legales específicos deberían ser advertidos por los asesores legales de la organización o por profesionales adecuadamente calificados.

Los requisitos que marca la legislación cambian de un país a otro y pueden variar para la información que se genera en un país y se transmite a otro país distinto (por ej., flujos de datos entre fronteras).

Obtenga asesoramiento legal competente, especialmente si la organización opera o tiene clientes en múltiples jurisdicciones.

Métrica. Número de cuestiones o recomendaciones de cumplimiento legal, agrupadas y analizadas por su estado (cerradas, abiertas, nuevas, retrasadas) e importancia o nivel de riesgo (alto, medio o bajo).

Porcentaje de requisitos externos clave que, mediante auditorías objetivas o de otra forma admisible, han sido considerados conformes.}

Debería existir un procedimiento formal de alta y baja de usuarios con objeto de garantizar y cancelar los accesos a todos los sistemas y servicios de información.

Anexo F. Gobierno de TI

1. MONITOREO DE ASIGNACIÓN DE PRIVILEGIOS POR PARTE DE UN GOBIERNO DE TI.

COMITÉ DE GOBIERNO DE TI	AUDITOR	JEFE DE SISTEMAS
1. Establece la orden de monitoreo. 5. Recibe el informe 6. Si hay irregularidades informa al jefe de sistemas y pide el descargo. 9. Recibe el informe y analiza la sanción.	2. Recibe la orden 3. Monitorea los privilegios de los usuarios. 4. Informa a gobierno de TI	7. Realiza el descargo 8. Informa al gobierno de TI. 10. Recibe la sanción.

2. MONITOREO DE ASIGNACION DE PRIVILEGIOS.

COMITÉ DE GOBIERNO DE TI	JEFE DE SISTEMAS	USUARIO
1. Solicita el monitoreo de asignación de privilegios 6. Recibe el informe 7. Analiza los sucesos 8. Amerita sanción	2. Recibe solicitud 3.Monitorea asignaciones 4. Si hubo vulnerabilidad de asignaciones. 5. Emite informe sobre la asignación de privilegios.	9. Recibe la sanción.

3. MONITOREO DE ACCESO DE DERECHOS POR USUARIO

USUARIO	COMITÉ DE GOBIERNO DE TI	AREA ADMINISTRATIVA	JEFE DE SISTEMAS
	1. Solicita monitoreo de acceso por usuario		2. Recibe la solicitud 3. Monitorea los accesos 4. Verifica que cumpla las normas 5. Emite informe para autorizar los accesos
		6. Recibe informe 7. Verifica informe 8. Emite informe y lo almacena	
	9. Verifica informe		
		10. Emite respuesta acerca de accesos	
11. Se comunica al usuario			

Anexo G. Pantallazos de la seguridad del myProcess