RESUMEN – TRABAJO DE GRADO

AUTORES	KAREN PAOLA SÁNCHEZ JAIME
FACULTAD	FACULTAD DE INGENIERIAS
PLAN DE ESTUDIOS	INGENIERIA DE SISTEMAS
DIRECTOR	EDUARD FABIÁN ÁLVAREZ PACHECO
TÍTULO DE LA TESIS	DISEÑO DEL PLAN DE CONTINUIDAD DEL NEGOCIO PARA LA E.S.E HOSPITAL EMIRO QUINTERO CAÑIZARES DE OCAÑA MEDIANTE EL ESTÁNDAR ISO 27001:2013

RESUMEN

(70 palabras aproximadamente)

EL PRINCIPAL OBJETIVO DE ESTE TRABAJO ES LA REALIZACIÓN DEL PLAN DE CONTINUIDAD DEL NEGOCIO PARA LA E.S.E HOSPITAL EMIRO QUINTERO CAÑIZARES, DETERMINÁNDOSE LA NECESIDAD DE EVALUAR LOS RIESGOS TECNOLÓGICOS, PARA CUAL SE REALIZÓ UNA SERIE DE ENCUESTAS Y VISITAS DONDE SE EVALUÓ Y VALORÓ LA SITUACIÓN ACTUAL EN LA QUE SE ENCUENTRA LA EMPRESA, PARA EL LOGRO DE OBJETIVOS, SE PLANTEÓ EL DISEÑO DE FORMATOS.

CARACTERÍSTICAS

PÁGINAS: 150	PLANOS:	ILUSTRACIONES:	CD-ROM: 1

DISEÑO DEL PLAN DE CONTINUIDAD DEL NEGOCIO PARA LA E.S.E HOSPITAL EMIRO QUINTERO CAÑIZARES DE OCAÑA MEDIANTE EL ESTÁNDAR ISO 27001:2013

KAREN PAOLA SÁNCHEZ JAIME

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA
FACULTAD DE INGENIERIAS
INGENIERIA DE SISTEMAS
OCAÑA
2015

DISEÑO DEL PLAN DE CONTINUIDAD DEL NEGOCIO PARA LA E.S.E HOSPITAL EMIRO QUINTERO CAÑIZARES DE OCAÑA MEDIANTE EL ESTÁNDAR ISO 27001:2013

KAREN PAOLA SÁNCHEZ JAIME

Trabajo de grado bajo la modalidad pasantías presentado para optar el título de Ingeniera de Sistemas

Director
EDUARDO FABIÁN ÁLVAREZ PACHECO

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA
FACULTAD DE INGENIERIAS
INGENIERA DE SISTEMAS
OCAÑA
2015

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

LISTA DE ANEXOS

Pág.

RESUMEN

El principal objetivo de este trabajo es la realización del Plan de Continuidad del Negocio para la E.S.E Hospital Emiro Quintero Cañizares, determinándose la necesidad de evaluar los riesgos tecnológicos, para cual se realizó una serie de encuestas y visitas donde se evaluó y valoró la situación actual en la que se encuentra la empresa.

Para el logro de objetivos, se planteó el diseño de formatos: Seguimiento a las Copias de Seguridad, Seguimiento de las Inscripciones a las Capacitaciones, Seguimiento al Acceso a los Servidores y Creación de las Cuentas de Usuario; Creación de Políticas que ayuden a un mejor manejo interno de la información y control interno: Buen Uso de Hardware, Cuentas de Usuario, Seguridad de la Información y Creación de Contraseñas.

Con el propósito de darle un buen manejo de las tecnologías de la información y de las comunicaciones, se vio la necesidad de elaborar un Plan de Contingencia completo, instrumento que servirá para evitar la posible pérdida, destrucción, robo y otras amenazas de la información para definir las tareas orientadas a reducir dichos riesgos.

El análisis realizado, determinó que no se tiene un orden y protección a la hora de almacenamiento y restauración de los backup (Copias de Seguridad), labor que se efectúa en USB'S y que pone en alto riesgo la información valiosa de la Empresa; por tanto, se recomienda gestionar la compra de un servidor remoto, con el fin de cumplir con eficiencia y eficacia esta función. Así mismo, se hace diseña el Procedimiento de Generacion de Copias de Respaldo y Recuperación de la Información.

Si se tiene en cuenta que cualquier Sistema de Redes de Computadoras (ordenadores, periféricos y accesorios) están expuestos a riesgos y puede ser fuente de problemas. El Hardware, el Software están expuestos a diversos Factores de Riesgo Humano y Físicos. Estos problemas menores y mayores sirven para retroalimentar nuestros procedimientos y planes de seguridad en la información. Pueden originarse pérdidas catastróficas a partir de fallos de componentes críticos (el disco duro), bien por grandes desastres (incendios, terremotos, sabotaje, etc.) o porfallas técnicas (errores humanos, virus informático, etc.) que producen daño físico irreparable, por ende se plantea y se diseña la Matriz, donde estan plasmados los riesgos que aquejan al Hospital y en ella encontramos el grado de impacto, probabilidad de ocurrencia y algunas acciones que deben tenerse en cuenta a la hora de mitigar el riesgo.

INTRODUCCION

El propósito de este informe es la realizacion del trabajo de grado modalidad pasantia, desarrollada en la E.S.E Hospital Emiro Quintero Cañizares, donde se identificó la necesidad de diseñar el Plan de Continuidad del Negocio.

Si se tiene en cuenta que la información es uno de los activos más importantes de la Empresa, y que la infraestructura informática (hardware, software y elementos complementarios) son indispensables para mantener un adecuado almacenamiento de la información o datos críticos para prestar un servicio con calidad a los usuarios, se crea la necesidad de realizar un análisis de los posibles riesgos a los cuales estan expuestos los equipos de cómputo y sistemas de información, con el propósito de elaborar un diagnóstico que nos permita evaluar y valorar los riesgos para la toma de decisiones y/o estrategias técnicas y sistemáticas que nos ayuden a evitar y disminuir los riesgos, o transferirlos a personal especializado que pueda asumirlo.

El Plan de Continuidad del Negocio contribuirá al logro de metas y objetivos de la Empresa y a mejorar la imagen y credibilidad del Hospital Emiro Quintero Cañizares, dado que se promueve la adopción de un enfoque basado en procesos, para establecer, implementar, operar, hacer seguimiento, mantener y mejorar el Sistema de Gestión de Seguirdad de la Información – SGSI en la organización.

1. DISEÑO DEL PLAN DE CONTINUIDAD DEL NEGOCIO PARA LA E.S.E HOSPITAL EMIRO QUINTERO CAÑIZARES DE OCAÑA MEDIANTE EL ESTÁNDAR ISO 27001:2013

1.1. DESCRIPCIÓN DE LA EMPRESA

E.S.E HOSPITAL EMIRO QUINTERO CAÑIZARES (HEQC)

La Empresa Social del Estado Hospital Emiro Quintero Cañizares es una institución de larga trayectoria y experiencia demostrada en toda la Provincia de Ocaña. Se consolida como institución de primer y segundo nivel de complejidad para brindar los servicios de salud a la población vinculada, subsidiada, contributiva y regímenes especiales.
Gracias a su actual infraestructura cuenta con cómodas instalaciones físicas garantizando un ambiente agradable y personal altamente calificado para ofrecer calidad y oportunidad[1].

RESEÑA HISTORICA

Nuevamente al igual que con la fundación de Ocaña, la Ciudad de Pamplona jugó un papel muy importante en materia de salud con la fundación del primer Hospital denominado SAN JUAN DE DIOS, en 1622 en la ciudad de Pamplona, por la comunidad de los hermanos de San Juan de Dios, se hace necesario fundar uno en la Ciudad de Ocaña, es así que desde Pamplona, se trasladan seis (6) religiosos en el año 1645 y fundan un hospital manicomio que además prestaba los servicios en Medicina General, dicho centro hospitalario funcionó poco tiempo en una casa ubicada en el Barrio San Agustín cerca al convento de la capilla de San Sebastián; este Hospital se terminó debido a las guerras de la época y a la expulsión de los religiosos de la Nueva Granada.

Luego a Mediados del siglo XVIII, se fundó una clínica que también funcionó en el barrio San Agustín, más concretamente en la casa de los COLOBON, donde funcionaba la panadería la INSUPERABLE, y quién fuera propietario el controvertido presbítero padre BUZETA.

En el año 1888 llegó a Ocaña, el pavoroso azote de la FIEBRE AMARILLA, dejando la ciudad reducida a menos de su tercera parte; ante esta epidemia y desolación y ante la ausencia de una Institución Hospitalaria, mediante Decreto Eclesiástico No, 203 de 1890 emanado de la Diócesis de Santa Marta se autorizaba al Párroco RAFAEL CELEDÓN de la parroquia de Santa Ana de Ocaña, la creación del Hospital de Caridad SANTA ANA DE OCAÑA, con escritura pública No. 445 del 25 de julio de 1890, el cuál inició labores el 1° de febrero de 1891 en el sitio denominado "El Llano de Echávez".

La Resolución No. 06 del 16 de marzo de 1937 del Consejo Municipal de Ocaña, cambia su

[1]E.S.E Hospital Emiro Quintero Cañizares Ocaña N. De S. Información Corporatica (presenteción [En línea]. <http://www.hospitaleqc.gov.co/plataforma-estrategica/reseña-historica.html> [citrado el 08 de marzo de 2012]

nombre por el del Hospital Civil de Ocaña y faculta al Director del mismo. La Resolución Ejecutiva No.90 del 18 de septiembre de 1939, le concede Personería Jurídica.

Desde diciembre de 1955, ofrece sus servicios en el local donde actualmente funciona, adoptando el nombre de HOSPITAL EMIRO QUINTERO CAÑIZARES, por Resolución No.23 de 1960. El Doctor Emiro Quintero Cañizares, en su condición de Secretario General de Salud hizo posible su construcción y dotación.

El Acuerdo del Concejo Municipal No.27 de 1938 establece los estatutos que posteriormente fueron reformados por la Resolución No. 001 de 1960, emanada de la Junta Directiva y que define claramente su finalidad.

Su nivel de atención se determinó en 1960, cuando Norte de Santander fue tomado como uno de los Departamentos de prueba en la implantación de la regionalización según el plan Piloto estructurado por Minsalud, O.P.S., UNICEF, con el fin de descentralizar las cuatro (4) especialidades básicas: Cirugía, Medicina Interna, Pediatría y Gineco-Obstetricia.
En el año de 1990 se inician los trabajos de remodelación que se terminan a finales de 1995.

Se le da vida jurídica como una empresa social del estado según ordenanza 060 del 29 de diciembre de 1995 emanada de la honorable Asamblea del Norte de Santander.

La ESE Hospital Emiro Quintero Cañizares es actualmente Hospital de II Nivel de atención, es Hospital de referencia para los Municipios de Ocaña, Abrego, Hacarí, La Playa, Teorama, San Calixto, Convención, El Tarra, El Carmen, Cáchira, y la Esperanza en el Departamento Norte de Santander, y de los Municipios de Río de Oro y Gonzáles del Departamento del Cesar.

El Hospital, es el centro asistencial más importante de la provincia de Ocaña ya que tiene una cobertura aproximada de 300.000 mil usuarios tiene como misión la prestación de servicios de salud con atención humanizada, dignidad, eficiencia, integridad y calidad a toda la población de Ocaña y municipios vecinos, que además ofrece servicios de promoción y prevención realizando visitas a diferentes zonas del área rural y puestos de salud.

La ESE Hospital Emiro Quintero Cañizares se encuentra en un momento trascendental e importante en su historia siendo el líder en el sector a través de la prestación de servicios, brindando atenciones en salud a miles de ciudadanos en condiciones de eficiencia, oportunidad y calidad, con buen nivel científico y realizando un aporte significativo al desarrollo de la región.

Como ya es sabido ante la permanente generación de cambios y transformación institucional tan profunda en el sector que se desenvuelven las entidades, ya sea jalonadas por la implementación de nuevas normas, la adopción de correctivos oportunos en cumplimiento de la legislación vigente, es de vital importancia para nosotros como IPS trabajar arduamente en la calidad de la prestación de servicios hacia nuestros clientes como compromiso para

satisfacer la población en sus necesidades de salud en todas las fases.[2]

1.1.1 Misión. Somos una empresa social del Estado que presta servicios de salud de baja, mediana y alta complejidad en la Provincia de Ocaña, con altos estándares de calidad y mejora continua a los usuarios del sistema general de seguridad social en salud en la sede principal y redes integradas; basadas en la participación social, el desarrollo del Talento Humano, la relación docencia – servicio e investigación, con tecnología apropiada y en pro de la sostenibilidad financiera, respetando la dignidad del individuo, con el enfoque diferencial, enfoque de género, enfoque de derechos, logrando satisfacer las necesidades en salud.[3]

1.1.2 Visión. Para el año 2023 la ESE Hospital Emiro Quintero Cañizares quiere ser reconocida en el Nororiente colombiano como una institución líder en salud, en la prestación de servicios, modelo en la atención, acreditada, promoviendo la gestión del conocimiento a través de la atención humanizada para mejorar la salud de los individuos y comunidad, enfocada a la población materno-infantil.[4]

1.1.3 Objetivo de la empresa.

Contribuir al desarrollo social de la región mejorando la calidad de vida, y reduciendo la morbilidad, la mortalidad, la incapacidad y la angustia evitables en la población usuaria, en la medida en que esto esté a su alcance.

Producir servicios de salud eficientes y efectivos, que cumplan con las normas de calidad establecidas de acuerdo con las reglamentaciones que se expida para tal propósito. Garantizar, mediante un manejo Gerencial adecuado, la rentabilidad social y financiera de la empresa.

Ofrecer a las Empresas Promotoras de salud y demás personas naturales o jurídicas que lo demandan, servicios y paquetes de servicios a tarifas competitivas en el mercado. Satisfacer los requerimientos del entorno, adecuando continuamente sus servicios y funcionamiento.

Garantizar los mecanismos de participación ciudadana y comunitaria establecidos por la ley y los reglamentos.

Prestar servicios de salud que satisfagan de manera óptima las necesidades y expectativas de la población en relación con la promoción, el fomento y la conservación de la salud y la prevención, tratamiento y rehabilitación de la enfermedad.
Satisfacer las necesidades esenciales y secundarias de salud de la población usuaria a través de acciones gremiales, organizativas, técnico-científicas y técnico-administrativas.

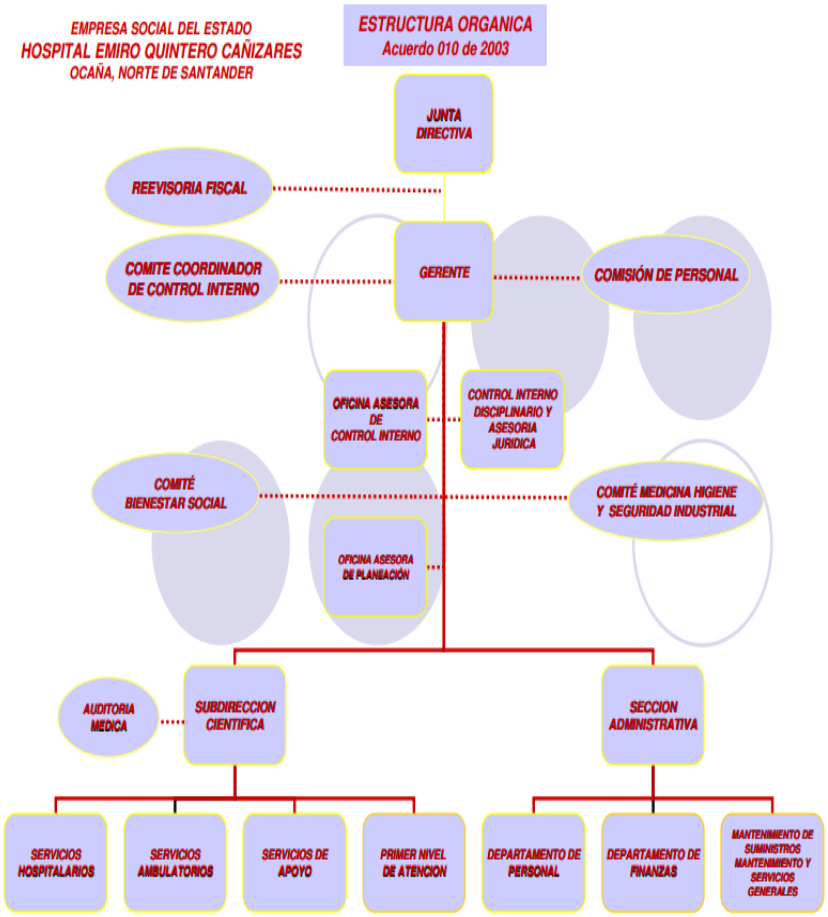
---

[2] ESE Hospital Emiro Quintero Cañizares Ocaña N. De S. Plataforma Estratégica (Reseña histórica) [En línea]. <http://www.hospitaleqc.gov.co/plataforma-estrategica/reseña-historica.html> [citado el 08 de marzo de 2012].
[3] PORTAFOLIO DE SERVICIO ESE Hospital Emiro Quintero Cañizares, 2014 (Misión)
[4] PORTAFOLIO DE SERVICIO ESE Hospital Emiro Quintero Cañizares, 2014 (Visión)

Desarrollar la estructura y capacidad operativa de la Empresa mediante la aplicación de principios y técnicas gerenciales que aseguren su supervivencia, crecimiento, calidad de sus recursos, capacidad de competir en el mercado y rentabilidad social y financiera. [5]

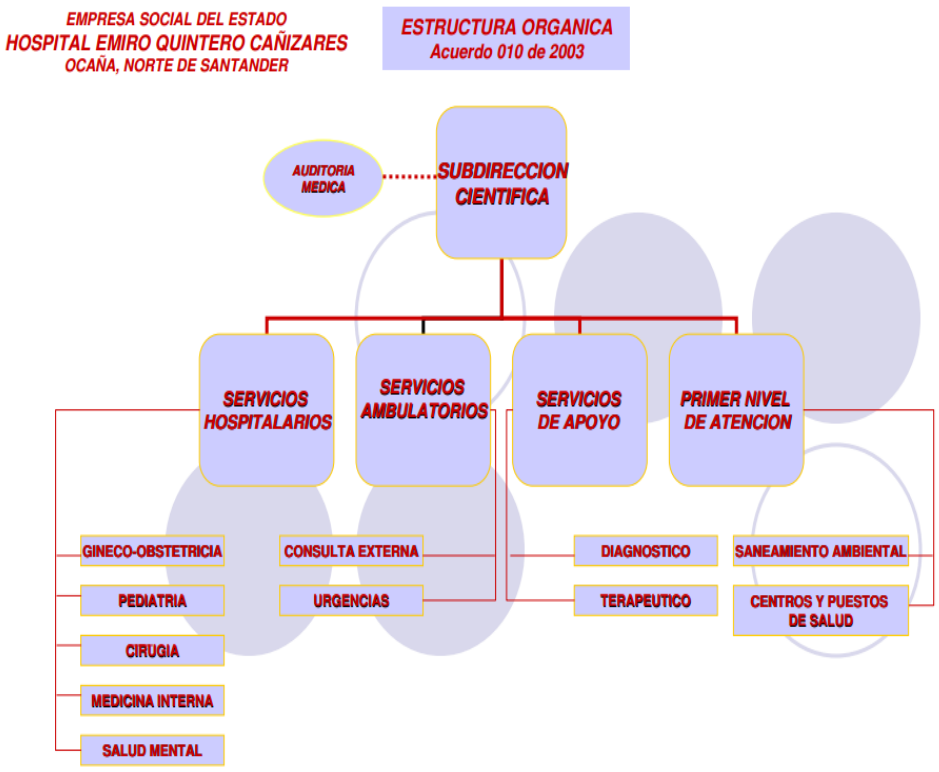
1.1.4 Estructura orgánica del HEQC Ocaña [6]

Figura 1. Estructura Orgánica del HEQC.



[5] ESE Hospital Emiro Quintero Cañizares Ocaña N. De S. Plataforma Estratégica (Objetivos Institucionales) [En línea]. <http://www.hospitaleqc.gov.co/plataforma-estrategica/objetivos.html> [citado el 08 de marzo de 2012].

[6] ESE Hospital Emiro Quintero Cañizares Ocaña N. De S. Información Corporativa (Estructura Orgánica) [En línea]. <http://www.hospitaleqc.gov.co/organigrama.html> [citado el 30 de marzo de 2012].



Fuente: ESE Hospital Emiro Quintero Cañizares Ocaña N. De S. Información Corporativa (Estructura Orgánica) [En línea]. <http://www.hospitaleqc.gov.co/organigrama.html> [citado el 30 de marzo de 2012].

Gerencia. Dirigir, formular y adoptar políticas, planes, programas y proyectos que garanticen la prestación de servicios de salud, tendientes a promover el desarrollo integral.
Oficina Asesoría jurídica. Fortalecer las labores asistenciales de apoyo a los procesos administrativos jurídicos en la ESE.

Oficina Asesora de Control Interno. Proteger los recursos de la organización, buscando su adecuada administración ante posibles riesgos que los afecten, garantizar la eficacia, la eficiencia y economía en todas las operaciones, promoviendo y facilitando la correcta ejecución de las funciones y actividades definidas para el logro de la misión institucional, velar porque todas las actividades y recursos de la organización estén dirigidos al cumplimiento de los objetivos del Hospital.

Subdirección Científica. Organizar y coordinar políticas institucionales de atención en salud, planear y controlas los recursos necesarios para el desarrollo de las políticas de salud, dirigir la prestación del servicio conforme a las competencias asignadas por las normas en salud pública.

Servicios Hospitalarios. Fortalecer los procesos que se realizan en el laboratorio Clínico, fisioterapia, radiología, anestesiología, cirugías, gineco-obstetricia, pediatría, para mejorar la

calidad de la prestación del servicio en la institución.

Servicios de Apoyo. Fortalecer los procesos de sistemas de información, estadística, archivo y procedimientos que se realizan en trabajo social para mejorar la calidad en la prestación del servicio en la institución.

Sección Administrativa. Planear, ejecutar, controlar la prestación de los servicios administrativos y velar por el cumplimiento de las políticas financieras de personal, de recursos físicos e información del Hospital.

Departamento de Personal. Fortalecer los procedimientos de programación, coordinación y supervisión de programas que garanticen el buen funcionamiento y desarrollo del Talento Humano en la institución.

Departamento de finanzas. Fortalecer los procedimientos dando cumplimiento a las normas contables generalmente aceptadas y referentes técnicos de la Contaduría general de la Nación y Entes de Control.

Mantenimiento de Suministros y servicios generales. Fortalecer labores de programación, coordinación y supervisión del área de suministros, almacén y controlar las labores técnicas en la oficina de mantenimiento, lavandería y economato.

Servicios Ambulatorios. Fortalecer los procesos y procedimientos que se realizan en medicina interna, traumatología, ortopedia, otorrinolaringología, psiquiatría, para mejorar la calidad de la prestación del servicio en la institución.

1.1.5 Descripción de la dependencia. La dependencia de sistemas no es un área visiblemente constituida o bien estructurada ya que se encuentra dividida en dos partes, mantenimiento de sistemas que es la encargada de las labores técnicas sistemáticas del hospital y el mantenimiento preventivo de todos los equipos de cómputo con los que cuenta la ESE actualmente; esta área se encuentra ubicada en la dependencia Mantenimiento de Suministros y servicios generales.

Por otra parte existen sistemas de información, encargados de las agendas médicas, asignación de citas y demás procesos de pagos por los servicios prestados, esta actividad está a cargo de la empresa COOTRASMAR CTA que se encuentra en comodato con la ESE HEQC, también es llevado a cabo el proceso de estadísticas vitales encargados del manejo de las estadísticas de nacidos vivos y los fallecimientos en las diferentes áreas dentro de la ESE.

Se hace evidente la participación del área de Auditoria de calidad en el proceso del proyecto a realizar, ya que se ha contado con el apoyo y la disposición de la misma, adecuándonos el espacio de trabajo y los equipos para un buen rendimiento, esta área es la encargada de hacer seguimiento a los procesos sistemáticos documentados y la verificación objetiva, para obtener y evaluar la evidencia de la auditoria, determinando cuales actividades específicas

cumplen con los criterios de auditoría para determinar las medidas en que la atención suministrada logre el equilibrio más favorable de riesgos y beneficios y así comunicar los resultados de estos procesos al cliente.

1.2. DIAGNÓSTICO INICIAL DE LA DEPENDENCIA ASIGNADA

Tabla 1. Diagnóstico de la Dependencia

Fortalezas	Debilidades
• Se cuenta con disposición de la alta gerencia para invertir en pro de mejorar el servicio. • Existencia de moderna dotación de las oficinas con la tecnología adecuada para la ejecución de los procesos (Hardware, software y equipos de telecomunicaciones). • El Hospital tiene a su disposición un excelente equipo orientado a mejorar la prestación del servicio.	• No se cuenta con un Plan de Continuidad del Negocio que soporte y mantenga de forma eficiente la información. • La responsabilidad de la información se encuentra descentralizada. • El Recurso Humano no es suficiente para atender la demanda en la implementacion de nuevos sistemas de información y tecnología. • No se realizan controles a los riesgos tecnológicos (Ver Matriz de Riesgos) identificados dentro de la Empresa. • Demora en los procesos de toma de decisiones y verificación de la información. • Información redundante en los diferentes formatos que se manejan.
Amenazas	**Oportunidades**
• Fácil acceso de personal no autorizado a la información permitiendo que se presenten alteraciones, modificaciones o perdida de la misma. • Desestabilizacion del sistema por ataques informáticos. • Alta dependencia con el Hospital Erasmo Meoz de Cúcuta para la toma de decisiones y aprobación de documentos.	• Implementación de políticas y procedimientos que garanticen la integridad, accesibilidad y disponibilidad de la información. • Competitividad, rentabilidad y buena imagen frente a otras empresas que desempeñen la misma función.

Fuente personal (Entrevista y Observación directa)

1.2.1. Planteamiento del problema. La E.S.E Hospital Emiro Quintero Cañizares presenta falencias en la seguridad de la Información dado a que no ha generado políticas o procedimientos que garanticen la accesibilidad, integridad y disponibilidad de la información, lo que conlleva a generar problemas de alto riesgo no solo para la entidad sino también para los usuarios, a quienes debe preservárseles sus derechos; También ha tenido cese de actividades momentáneas en su sistemas de infraestructura de red en cuanto al soporte a los equipos de cómputo se refiere (hardware), lo cual genera un descontento a sus clientes y la pérdida de tiempo para ambas partes.

Las organizaciones y sus sistemas de información están expuestos a un numero cada vez mas elevado de amenazas que puedes aprovechar cualquiera de las vulnerabilidades existentes para someter activos críticos de información a diversas formas de fraude, espionaje, sabotaje o vandalismo; Así mismo debe considerarse los riesgos de sufrir incidentes de seguridad causados voluntaria e involuntariamente desde dentro de la propia organización o aquellos provocados accidentalmente por catástrofes naturales.[7]

La información, junto con los procesos y sistemas que hacen uso de ella, son activos muy importante de una organización, pueden llegar a ser esenciales para mantener los niveles de competitividad, rentabilidad, conformidad legal e imagen empresarial necesario para lograr los objetivos de la organización y asegurar beneficios económicos.

Es evidente además que la empresa en mención, pese a que no se ha presentado ningún inconveniente de tipo lógico o humano que pudiera poner en riesgo la seguridad de la información, no cuenta con un plan de continuidad del Negocio, por tal razón, es imperiosa la necesidad de implementar una estrategia que permita hacer un diagnóstico sobre el estado actual de sus sistemas de información, sugerir controles para manejar los riesgos de la seguridad de la informacion y establecer objetivos que contribuyan al seguimiento y revisión eficaz de Sistema de Gestion de la Información.

1.3. OBJETIVOS

1.3.1. General

Diseño del plan de continuidad del negocio para la E.S.E Hospital Emiro Quintero Cañizares de Ocaña mediante el estándar ISO 27001:2013.

1.3.2. Específicos

1. Evaluar en la Institución los riesgos tecnológicos a los que está expuesto.

2. Elaborar el Mapa de Riesgos tecnológicos presentes en la E.S.E.

[7] Sistema de Gestión de la Seguridad de la Información. ISO 27001.

3. Diseñar Políticas, Procedimientos que garanticen la integridad, accesibilidad y la disponibilidad de la información.

4. Presentar recomendaciones a la E.S.E Hospital Emiro Quintero Cañizares, acerca de los procedimientos que permitan evitar riesgos tecnológicos que garanticen mantener la seguridad de la Información.

1.4. DESCRIPCIÓN DE LAS ACTIVIDADES A DESARROLLAR.

Tabla 2. Actividades a desarrollar.

Objetivo General	Objetivos Específicos	Actividades a Desarrollar en la empresa para hacer posible el cumplimiento de los Objetivos Específicos
✓ Diseño del plan de continuidad del negocio para la E.S.E Hospital Emiro Quintero Cañizares de Ocaña mediante el estándar ISO 27001:2013.	✓ Analizar y evaluar en la Institución los riesgos tecnológicos a los que están expuestos los Sistemas de Información.	✓ Entrevista con las personas encargadas de hacer la recopilación de información ✓ Recolección de la información mas relevante con respecto a los riesgos mas concurrentes.
	✓ Diseñar Políticas, Procedimientos que garanticen la integridad, accesibilidad y la disponibilidad de la información.	✓ Aplicar la Norma ISO 27001
	✓ Elaborar el Mapa de Riesgos tecnológicos presentes en la E.S.E.	✓ Identificar los Riesgos tecnológicos. ✓ Evaluar peligros o amenazas inminentes mediante la elaboración de la Matriz de Riesgos
	✓ Presentar recomendaciones a la E.S.E Hospital Emiro Quintero Cañizares, acerca de los procedimientos que permitan evitar riesgos tecnológicos que garanticen mantener la seguridad de la Información.	✓ Analizar la informacion recopilada en los procesos de evaluación y valoracion de riesgos para asi presentar las recomendaciones pertinentes

Fuente: Pasante

2. ENFOQUES REFERENCIALES

2.1. ENFOQUE CONCEPTUAL

2.1.1. Información.[8]La información es un conjunto de datos dispuestos de manera que nos permitan adquirir cualquier tipo de conocimiento. Asimismo, es uno de los principales activos de las organizaciones, por lo que salvaguardarla es vital para la continuidad del negocio.

2.1.2. Sistemas de Información[9]**.** Los Sistemas de Información (SI) son conjuntos organizados de elementos que procesan y distribuyen información con el fin de cumplir unos objetivos. No es necesario que estén basados en ordenadores. La utilización de aplicaciones informáticas sobre soportes informáticos da lugar a los Sistemas de Información Automatizados (SIA).

Los Sistemas de Información pretenden proporcionar una información oportuna y exacta para el apoyo en la toma de decisiones de la compañía. Además, garantizan la confiabilidad, la integridad y disponibilidad de la información. El uso de Sistemas de Información automatiza procesos operativos y pretenden conseguir ventajas competitivas en el mercado.

Características de los datos en un sistema de información:

Integridad:

Para la Seguridad de la Información, la integridad es la propiedad que busca mantener a los datos libres de modificaciones no autorizadas.

Confidencialidad:

La confidencialidad es la propiedad de prevenir la divulgación de información a personas o sistemas no autorizados.

Disponibilidad:

La Disponibilidad es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.

[8] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. Information Technology. Security Techniques. Code of Practice for Information Security Management. Geneva:ISOIIEC, 2005, 107 P (ISOIIEC 27002:2005 (E)).
[9] Universidad Carlos III de madrid escuela politecnica superior calidad y seguridad de la información y auditoría informática

2.1.3 Auditoria de Sistemas de información.[10]

La Auditoría de Sistemas de Información es el proceso de recoger y evaluar las evidencias para determinar la seguridad de los sistemas informáticos, la salvaguarda de los activos, la integridad de los datos y conseguir los objetivos de la organización con eficacia y con consumo de recursos eficiente.

Por tanto, la Auditoría de Sistemas de Información mantiene la obtención de los objetivos de la Auditoría tradicional, que tiene como foco la salvaguarda de los activos y la integridad de los datos, y además los objetivos de eficacia y eficiencia. El proceso de la Auditoría de Sistemas de Información se puede concebir como una fuerza que ayuda a las organizaciones a conseguir mejor estos objetivos.

Importancia de realizar auditorías a los sistemas de información:

La Auditoria es de vital importancia para el buen desempeño de los sistemas de información, ya que proporciona los controles necesarios para que los sistemas sean confiables y con un buen nivel de seguridad. Además debe evaluar todo: informática, organización de centros de información, hardware y software.

La Auditoria del Sistema de Información en la empresa, a través de la evaluación y control que realiza, tiene como objetivo fundamental mejorar la rentabilidad, la seguridad y la eficacia del sistema mecanizado de información en que se sustenta.

2.1.4 Auditoría.[11]

La auditoría es un proceso sistemático que se realiza para obtener y evaluar de manera objetiva las evidencias relacionadas con informes presentados sobre acciones que tienen que ver directamente con las actividades que se desarrollan en un área o una organización, sea pública o privada.

La auditoría es un proceso sistemático. Esto quiere decir que en toda auditoría debe existir un conjunto de procedimientos lógicos y organizados que se deben cumplir para la recopilación de la información con el fin de emitir una opinión final.

2.1.4.1 Auditoría a Bases de Datos.[12]

Es el proceso que permite medir, asegurar, demostrar, monitorear y registrar los accesos a la información almacenada en las bases de datos incluyendo la capacidad de determinar:

---

[10] Universidad Carlos III de Madrid escuela politécnica superior calidad y seguridad de la información y auditoría informática

[11] FERNÁNDEZ, Eduardo. CFT soeduc concepto de auditoría Disponible en internet: <www.soeduc.cl/apuntes/concepto%20de%20auditoria.doc>

[12] En Línea http://www.jkmst.com

– Quién accede a los datos.
– Cuándo se accedió a los datos.
– Desde qué tipo de dispositivo/aplicación.
– Desde que ubicación en la Red.
– Cuál fue la sentencia SQL ejecutada.
– Cuál fue el efecto del acceso a la base de datos.

Es uno de los procesos fundamentales para apoyar la responsabilidad delegada a IT por la organización frente a las regulaciones y su entorno de negocios o actividad.

2.1.4.2 Auditoría a Redes de Datos.[13]

Una Auditoria de Redes es, en esencia, una serie de mecanismos mediante los cuales se pone a prueba una red informática, evaluando su desempeño y seguridad, a fin de lograr una utilización más eficiente y segura de la información.

2.1.5 Controles.

Conjunto de disposiciones metódicas, cuyo fin es vigilar las funciones y actitudes de las empresas y para ello permite verificar si todo se realiza conforme a los programas adoptados, órdenes impartidas y principios admitidos.

2.1.5.1 Clasificación general de los controles.

Controles Preventivos.

Son aquellos que reducen la frecuencia con que ocurren las causas del riesgo, permitiendo cierto margen de violaciones.
Ejemplos: Letrero "No fumar" para salvaguardar las instalaciones.

Sistemas de claves de acceso

Controles Detectivos.

Son aquellos que no evitan que ocurran las causas del riesgo sino que los detecta luego de ocurridos. Son los más importantes para el auditor. En cierta forma sirven para evaluar la eficiencia de los controles preventivos.

Ejemplo: Archivos y procesos que sirvan como pistas de auditoría

[13] DEL PESO NAVARRO, EMILIO; DEL PESO, MAR; PIATTINI VELTHUIS, MARIO G. (2008). Auditoría de Tecnologías y Sistemas de Información
. México: Alfaomega Ra-Ma.

Procedimientos de validación

Controles Correctivos

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

2.1.6 Estándar ISO/IEC 27001.[14]

ISO/IEC 27001 es un estándar para la seguridad de la información (Information technology - Security techniques - Information security management systems - Requirements) aprobado y publicado como estándar internacional en octubre de 2005 por International Organization for Standardization y por la comisión International Electrotechnical Commission.

Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un sistema de gestión de la seguridad de la información (SGSI) según el conocido como "Ciclo de Deming":PDCA - acrónimo de Plan, Do, Check, Act (Planificar, Hacer, Verificar, Actuar). Es consistente con las mejores prácticas descritas en ISO/IEC 27002, anteriormente conocida como ISO/IEC 17799, con orígenes en la norma BS 7799-2:2002, desarrollada por la entidad de normalización británica, la British Standards Institution (BSI).

La gestión de la seguridad de la información debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización.

Este proceso es el que constituye un Sistema de Gestión de Seguridad de la Información SGSI, que podría considerarse, por analogía con una norma tan conocida como ISO 9001, como el sistema de calidad para la seguridad de la información.

Garantizar un nivel de protección total es virtualmente imposible, incluso en el caso de disponer de un presupuesto ilimitado. El propósito de un sistema de gestión de la seguridad de la información es, por tanto, garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

[14] Estandar Internacional ISO 27001. Tecnologia de la información – Tecnicas de seguridad –Sistemas de gestión de seguridad de la información- Requerimiento

2.1.6.1 Seguridad de la información.[15]

Según ISO 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización. Así pues, estos tres términos constituyen la base sobre la que se cimienta todo el edificio de la seguridad de la información:

• **Confidencialidad:**

La información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.

• Integridad:

Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

• Disponibilidad:

Acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

2.1.6.2 Cuatro fases del sistema de gestión de seguridad de la información.[16]

La norma ISO 27001 determina cómo gestionar la seguridad de la información a través de un sistema de gestión de seguridad de la información. Un sistema de gestión de este tipo, igual que las normas ISO 9001 o ISO 14001, está formado por cuatro fases que se deben implementar en forma constante para reducir al mínimo los riesgos sobre confidencialidad, integridad y disponibilidad de la información.

Las fases son las siguientes:

La Fase de planificación:

Esta fase sirve para planificar la organización básica y establecer los objetivos de la seguridad de la información y para escoger los controles adecuados de seguridad (la norma contiene un catálogo de 133 posibles controles).

La Fase de implementación:

Esta fase implica la realización de todo lo planificado en la fase anterior.

---

[15] Auditoría de Sistemas de Información. Seguridad informática: Conceptos básicos, Capítulo 1 [en línea] Disponible en Internet: <http://catarina.udlap.mx/u_dl_a/tales/documentos/lis/jerez_l_ca/capitulo1.pdf>

[16] Disponible en línea http://www.iso27001standard.com

La Fase de revisión:

El objetivo de esta fase es monitorear el funcionamiento del SGSI mediante diversos "canales" y verificar si los resultados cumplen los objetivos establecidos.

La Fase de mantenimiento y mejora:

El objetivo de esta fase es mejorar todos los incumplimientos detectados en la fase anterior.

El ciclo de estas cuatro fases nunca termina, todas las actividades deben ser implementadas cíclicamente para mantener la eficacia del SGSI.

2.1.7. Análisis de riesgos informáticos.[17]

El análisis del riesgo es un método sistemático de recopilación, evaluación, registro y difusión de información necesaria para formular recomendaciones orientadas a la adopción de una posición o medidas en respuesta a un peligro determinado. Hay pequeñas variaciones en la terminología utilizada por las tres organizaciones. Sin embargo, las tres organizaciones hermanas consideran el análisis del riesgo como un proceso que consta de cuatro etapas:

Identificación del peligro
Evaluación del riesgo
Gestión del riesgo
Comunicación del riesgo.

La **identificación del peligro** consiste en especificar el acontecimiento adverso que es motivo de preocupación.

En la **evaluación del riesgo** se tiene en cuenta la probabilidad (la probabilidad real y no sólo la posibilidad) de que se produzca el peligro, las consecuencias si ocurre y el grado de incertidumbre que supone. (Obsérvese que esta descripción de la evaluación del riesgo es diferente de la definición que figura en el Acuerdo MSF.)

La **gestión del riesgo** consiste en la identificación y aplicación de la mejor opción para reducir o eliminar la probabilidad de que se produzca el peligro.

La **comunicación del riesgo** consiste en el intercambio abierto de información y opiniones aclaratorias que llevan a una mejor comprensión y adopción de decisiones

[17] Disponible en Linea http://www.wto.org

2.2. ENFOQUE LEGAL.[18]

El presente trabajo tiene como base legal las siguientes normas:

En España, existe la **Ley Orgánica de Protección de Datos de carácter personal** (LOPD) para regular este tipo de información. El objetivo de la Ley Orgánica 15/1999, de 13 de diciembre, se expone en el Título 1 artículo 1 de dicha ley, detallando que se trata de "*garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar*".

Por lo tanto, la LOPD pretende establecer una serie de principios en cuanto al tratamiento de datos de carácter personal y reconoce unos derechos a los titulares de los datos. Asimismo, cabe destacar el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

En el Titulo VI de esta ley ya derogada se creó la Agencia de Protección de Datos regulada en el Real Decreto 428/1993, de 26 de marzo, por el que se aprobó el Estatuto de la **Agencia Española de Protección de Datos** (AEPD). Se rige también por el Título VI de la LOPD.

Las nuevas tecnologías han traído consigo el nacimiento de varias leyes que pretender regular el uso de aquellas. El 11 de julio de 2002 se desarrolló la Ley 34/2002 de **Servicios de la Sociedad de la Información** y de **Comercio Electrónico** (LSSICE). Esta ley regula, entre otras cosas, la celebración de contratos por vía electrónica, establece una serie de obligaciones y responsabilidades para los prestadores de servicios de la sociedad de la información (y de los intermediarios) y protege los intereses de los destinatarios de los servicios.

Finalmente, sin querer adentrarme demasiado en materia legislativa, es de relevancia señalar que en la Constitución Española de diciembre de 1978 ya se alude a la regulación de la informática para proteger los derechos de las personas en el artículo 18 apartado 4 "*La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos*".

2.2.1 Ley 1273 DE 2009.[19]Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado de la protección de la información y de los datos

[18] Universidad Carlos III de madrid escuela politécnica superior seguridad lógica y de accesos y su auditoría *proyecto fin de carrera* ingeniería técnica en informática de gestión

[19] Constitución política de Colombia. De la protección de la información y de los datos, Ley 1273 de 2009 [En Línea] Disponible en internet:
<http://www.dmsjuridica.com/CODIGOS/LEGISLACION/LEYES/2009/LEY_1273_DE_2009.htm>

y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

EL CONGRESO DE COLOMBIA

Decreta:

ARTÍCULO 1°. Adiciónese el Código Penal con un Título VII BIS denominado "De la Protección de la información y de los datos.

De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos

Artículo 269ª: **Acceso abusivo a un sistema informático**.

El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269C: **Interceptación de datos informáticos**.

El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

Artículo 269D: **Daño Informático**.

El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269F: **Violación de datos personales**.

El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

2.2.2. Convenio institucional. Convenio marco de apoyo Inter-institucional para la realización de pasantías y/o prácticas profesionales, celebrado entre la Universidad Francisco de paula Santander seccional Ocaña y la E.S.E Hospital Emiro Quintero Cañizares.

3. INFORME DE CUMPLIMIENTO DE TRABAJO

3.1. PRESENTACIÓN DE RESULTADOS

Con el objeto de realizar el diagnóstico que permita identificar si la E.S.E Hospital Emiro Quintero Cañizares cuenta con un Sistema de Gestión de Seguridad de la información, se hizo necesario elaborar un plan de acción sistemático, que nos ayudara al logro de objetivos.

Para ello se efectuó el siguiente proceso:

3.1.1 Evaluación de la documentación suministrada por la entidad. Realización de entrevistas con las personas encargadas del área de Mantenimiento y el Ingeniero de Sistemas, quienes proporcionaron información necesaria para hacer un análisis minucioso de la situación encontrada en la Empresa.

Se permite utilizar la Filosofía Institucional y el Organigrama de la Empresa, en la elaboración del Plan de Trabajo.

3.1.2. Actividades desarrolladas durante el proceso:

Elaboración de instrumentos de recolección de información:

Las encuestas tuvieron como objetivo, identificar los riesgos inminentes que vulneran y ponen en riesgo la información que se encuentra dentro de la infraestructura tecnológica de la E.S.E Hospital Emiro Quintero Cañizares y priorizar los que tienen mayor afectación de impacto para la Institución. Se realizaron cuatro encuestas orientadas a diferentes áreas:

2. Evaluación de la Seguridad Lógica**.** (ANEXO 1)

3. Evaluar los Elementos de Seguridad Física en el Ambito Informático. (ANEXO 2)

4. Evaluar el Servicio de Mantenimiento de Hardware. (ANEXO 3)

5. Evaluación a la Seguridad Física. (ANEXO 4)

Diseño de la Matriz de Riesgos. (Evaluación de los Riesgos)

- Matriz de Riesgos (ANEXO 5)

Riesgo Tecnológico:[20] Es la probabilidad de que un objeto, material o proceso peligroso, una sustancia tóxica o peligrosa o bien un fenómeno debido a la interacción de estos, ocasione

[20] http://helid.digicollection.org/fr/d/Jcne05/1.1.html

un número determinado de consecuencias a la salud, la economía, el medio ambiente y el desarrollo integral de un sistema

Los riesgos tecnológicos pueden presentarse en una amplia gama de variedades, debe tenerse presente que no hay dos accidentes idénticos. Por ello los riesgos se clasifican según la variedad de la amenaza:

- Riesgo por Incendio o explosión. Presente sobre todo en plantas industriales y áreas de almacenamiento.

- Riesgo por escapes o derrames. Más común en plantas industriales y transporte de materiales peligrosos (sea por medio de tubería o por medio de vehículos automotores).

- Riesgo de intoxicación y exposición a radiaciones ionizantes. En procesos industriales y manejo inadecuado de desechos.

El riesgo tecnológico puede verse desde tres aspectos:

- A nivel de la infraestructura tecnológica (hardware o nivel físico)
- A nivel lógico (riesgos asociados a software, sistemas de información e información)
- Riesgos derivados del mal uso de los anteriores factores, que corresponde al factor humano como un tercer nivel.

Los riesgos identificados en la E.S.E Hospital Emiro Quintero Cañizares corresponden a Riesgos Tecnológicos, dado que las fallas se ubican en los niveles de infraestructura tecnológica, lógico y de riesgos derivados del mal uso de los anteriores factores, sin obviar que también existen riesgos por incendio, explosión o naturales. A continuación se relacionan los priorizados:

Tabla 3. Riesgos Tecnológicos

R I E S G O	**III. VALORACIÓN DE RIESGOS VS. CONTROLES**	
	Valoración Final	
	GRADO DE IMPACTO	**PROBABILIDAD DE OCURRENCIA**
Fallas electricas	6	5
Pérdida de la Información	5	7
Inseguridad en Area de servidores y central telefónica	6	7
Software sin licencia	5	6
Tecnologia obsoleta.	5	6
Daño de Hardware	6	7
Infeccion por Virus Informatico	7	8

Fuente: Pasante

Dentro de los Riesgos hallados, se descubrió que ninguno de ellos tiene controles para la mitigacion de los mismos, esto hace que la información este predispuesta o susceptible a ser afectada o a sufrir pérdidas.

En la Matriz adjunta se analizan cada uno de los riesgos de acuerdo a:

NIVEL DE DECISIÓN: se clasifican en Estratégico, Directivo u Operativo, según el nivel de decisión institucional en el que recaería la administración del Riesgo identificado.

CLASIFICACIÓN DEL RIESGO: Hace relación al origen más representativo del Riesgo identificado. En este caso se ubican en el área Legal, de Seguridad y de TIC's.

FACTOR: En esta columna se describen las principales circunstancias o situaciones que indican la presencia de un Riesgo o que aumenten la Probabilidad de que un Riesgo se materialice.

CLASIFICACIÓN DEL FACTOR: Estos se pueden catalogar en:

Humano, Financiero Presupuestal, Técnico-Administrativo, TIC's, Material, Normativo y Entorno, especificación que se relaciona en el Anexo 15.

POSIBLES EFECTOS DEL RIESGO: En este ítem se describen las consecuencias que, de materializarse el Riesgo identificado, incidirán en el cumplimiento de los objetivos o metas institucionales.

VALORACIÓN INICIAL, GRADO DE IMPACTO Y PROBABILIDAD DE OCURRENCIA: Se asigna una escala de valor de 1 a 10 los cuales se ordenan de acuerdo al grado de impacto y la probabilidad de ocurrencia, como se evidencia en el siguiente tabla:

Tabla 4. Ponderación para la valoración de Riesgos.

Tabla de Ponderaciones para la Valoración de Riesgos					
Probabilidad de Ocurrencia			**Grado de impacto**		
10	**Recurrente**	Probabilidad de ocurrencia Muy Alta	10	**Catastrófico**	Influye directamente en el cumplimiento de la misión, perdida patrimonial incumplimientos normativos, problemas operativos o de impacto ambiental o deterioro de la imagen, dejando además sin funcionar totalmente o por un periodo importante de tiempo los programas o servicios que entrega la institución.
9			9		
8	**Probable**	Probabilidad de ocurrencia Alta	8	**Grave**	Dañaría significativamente el patrimonio, incumplimientos normativos, problemas operativos o impacto ambiental o deterioro de la imagen o logro de objetivos institucionales. Además se referiría una cantidad importante de tiempo de la alta dirección en investigar y corregir los daños.
7			7		
6	**Posible**	Probabilidad de ocurrencia Media	6	**Serio**	Causaría, ya sea una pérdida importante en el patrimonio, incumplimientos normativos, problemas operativos o de impacto ambiental o un deterioro significativo de la imagen. Además se referiría una cantidad importante de tiempo de la alta dirección en investigar y corregir los daños.
5			5		
4	**Inusual**	Probabilidad de ocurrencia Baja	4	**Moderado**	Causa un daño en el patrimonio o imagen, que se puede corregir en el corto tiempo, y no afecta el cumplimiento de los objetivos estratégicos.
3			3		
2	**Remota**	Probabilidad de ocurrencia Muy Baja	2	**Insignificante**	Riesgo que puede tener un pequeño o nulo efecto en la institución.
1			1		

Fuente: Pasante

EVALUACIÓN DE CONTROLES: Los tipos de controles para administrar el Riesgo se clasifican en: Preventivo, Detectivo y Correctivo, vigilancia que no se ejerce en la Entidad, razón por la cual la valoracion inicial es igual a la valoración final, generando en el Mapa de Riesgos una ubicación en el cuadrante de color rojo, porque no existe control alguno.

ESTRATEGIAS PARA ADMINISTRAR EL RIESGO: Finalmente se establecen estratégias para administrar el Riesgo, basadas en la valoración, respecto a los controles, que permitan tomar las decisiones y establecer acciones de control. Como se evidencia en la Matriz se seleccionó la estratégia de Evitar, con el objeto de generar cambios sustanciales por mejora; de Reducir para disminuir las probabilidades de ocurrencia y el impacto y de Transferir cuando el control debe ser efectuado por un tercero que tenga experiencia y especialización necesaria para asumirlo.

Diseño de los diferentes formatos.

- Seguimiento a las Copias de Seguridad (ANEXO 6)
- Seguimiento de las Inscripciones a las Capacitaciones (ANEXO 7)
- Seguimiento al Acceso a los Servidores (ANEXO 8)
- Creacion de las Cuentas de Usuario (ANEXO 9)

Diseño de Politicas.

- Buen Uso de Hardware (ANEXO 10)
- Cuentas de Usuario (ANEXO 11)
- Seguridad de la Información (ANEXO 12)
- Creacion de Contraseñas (ANEXO 13)

Diseño del Plan de Contingencia para la Seguridad de la Información.

- Plan de Contingencia (ANEXO 14)

Procedimiento de Generación de Copias de Respaldo y Recuperación de la Información.

(ANEXO 15)

4. DIAGNOSTICO FINAL

Luego de identificar la carencia en la implementación de un Sistema de Gestión de la Información en la E.S.E. Hospital Emiro Quintero Cañizares, que permita prevenir la vulnerabilidad en lo que respecta a fraude, espionaje, sabotaje o vandalismo dentro de la infraestructura física y lógica, que puedan afectar la integridad, disponibilidad y confidencialidad de la información, se logró sensibilizar a los servidores públicos que apoyaron el Plan de Trabajo, sobre la importancia de conocer los riesgos que pueden perjudicar el funcionamiento de la Empresa, asimilarlos y buscar los mecanismos necesarios para la realización de acciones que promuevan los controles obligatorios para mitigarlos, así mismo, el compromiso de gestionar los recursos que coadyuven en el logro del mejoramiento de la calidad de la prestación del servicio y se mejore la buena imagen de la Empresa.

5. CONCLUSIONES

De acuerdo al diagnóstico realizado a la E.S.E Hospital Emiro Quintero Cañizares, se pudo identificar que no cuenta con un Sistema de Gestión de Seguridad de la Información, situación que lo hace altamente vulnerable, dado que las probabilidades de ocurrencia y la posibilidad de que un evento adverso (externo o interno) obstaculice el logro de objetivos y metas institucionales sea grave; impacto desfavorable para la Empresa, teniendo en cuenta la relevancia de la Institución para la región y el servicio público que presta a la comunidad. Por tal motivo se hace necesario e indispensable realizar controles, que coadyuven a mitigar los riesgos.

El servicio que presta la Entidad es para los usuarios de la zona urbana, rural y Municipios aledaños, dándole un alto grado de responsabilidad con la población, que entre otras, son personas con vulnerabilidad socioeconómica, lo que puede acarrear descontento, si el servicio prestado no es oportuno y se identifican fallas de tipo humano y tecnológico. Las consecuencias para la Institución y los usuarios serían graves, dado que se vería seriamente afectada la imagen de la Empresa, los usuarios perderían tiempo y dinero, generando problemas legales, económicos y financieros a la Institución.

6. RECOMENDACIONES

Socializar al interior del Comité de Dirección, el diagnóstico de los Riesgos identificados en la Empresa E.S.E. Hospital Emiro Quintero Cañizares, en lo que compete a la implementacion del Sistema de Gestión de Seguridad de la Información, con el objeto de que interioricen, la necesidad de implementar un proceso sistematico, documentado y conocido por toda la organización, que permita preservar la confidencialidad, integridad y disponibilidad de la información.

Dar a conocer el diseño de Políticas empleadas para garantizar el Buen Uso del Hardware, Manejo de Cuentas de Usuario, Seguridad en la Información y el Manejo de la Creacion de Contraseñas, así mismo los formatos de Seguimiento a las Copias de Seguridad, Inscripción a las Capacitaciones, Acceso a los Servidores y Creación de Cuentas de Usuario; además del Plan de Contingencia y el Proceso de Generación de Copias de Respaldo y Recuperación de la Informacion, con el propósito de conocerlos, asimilarlos e implementarlos una vez la Direccion se comprometa a liderar el proceso.

Se recomienda hacer seguimiento a la Matriz con el fin de identificar claramente las circunstancias que indican la presencia de los Riesgos, sus efectos, valorar el grado de impacto, evaluar los controles que se ejercen; igualmente la valoración del Riesgo frente a los controles; identificar por cuadrante la Matriz de Riesgos de la Institución y definir las estrategias y acciones para su administracion.

Estudiar la posibilidad de gestionar la asignación de recursos para la compra de una planta eléctrica de mayor capacidad para el suministro de energía en caso de que se presente deficiencia en el fluido eléctrico y evite suspensión de actividades, perdida de la información, la prestacion de servicio y daño en equipos tecnológicos.

Gestionar los recursos para la compra de sistema operativo y software licenciado con el propósito de fomentar la competencia leal y enfrentar las operaciones fiscales. Así mismo permitir actualizaciones permanentes, contar con soporte técnico, evitar ataques informáticos que atenten contra el acceso y la confidencialidad de la información.

Presupuestar la adquisición de un servidor remoto que tenga como función el almacenamiento del backup (Copia de seguridad), que permita guardar periódicamente la información y recuperarlas en diferentes eventos tales como catástrofe informática, natural o ataque, que puedan haberse eliminado accidentalmente, infectado por un virus u otras causas.

Adquisición de antivirus licenciado para la proteccion de los equipos, aplicación imprescindible en la actualidad debido a la gran exposición en la navegacion de las páginas web y la utilización de dispositivos extraíbles como la USB.

Estudiar la posiblidad de crear el Departamento de Sistemas o Informática, dada la capacidad de la Empresa y la relevancia del servicio que presta, como garante de la del Derecho a la Salud en la Región.

BIBLIOGRAFÍA

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. Information Technology. Security Techniques. Code of Practice for Information Security Management. Geneva:ISOIIEC, 2005, 107 P (ISOIIEC 27002:2005 (E)).

DEL PESO NAVARRO, EMILIO; DEL PESO, MAR; PIATTINI VELTHUIS, MARIO G. (2008). Auditoría de Tecnologías y Sistemas de Información México: Alfaomega Ra-Ma.

Estándar Internacional ISO 27001. Tecnología de la información – Técnicas de seguridad – Sistemas de gestión de seguridad de la información- Requerimiento

Ramirez Castro, A. (2014). Memoria TFM: Actualización del Sistema de Gestión de Seguridad de la Información de una empresa a la norma ISO/IEC 27001: 2013.

Ramírez López, L. J. (2014). Manual de seguridad de la información para un organismo del estado colombiano.

Gaspar, J. (2004). Planes de contingencia la continuidad del negocio en las organizaciones. Ediciones Díaz de Santos.

Junttila, J. (2014). A Business continuity management maturity model: the search for an ISO 22301 Compliant BCM Maturity model.

Zawada, B. (2014). La aplicación práctica de la norma ISO 22301. Diario de la continuidad del negocio y la planificación de emergencias , 8 (1), 83-90.

Marañon, G. Á., García, P. P. P., & Bustamante, P. (2004). Seguridad informática para la empresa y particulares. McGraw-Hill.

Gómez Vieites, Á. (2007). Enciclopedia de la seguridad informática. México: Alfa omega Grupo Editor.

Cardona, O. D. (1993). Evaluación de la amenaza, la vulnerabilidad y el riesgo.En: A. Maskrey (ed.) Los desastres no son naturales, 51-74.

Medina, M. (1992). Nuevas tecnologías, evaluación de la innovación tecnológica y gestión de riesgos. J. Sanmartín-SH Cutcliffe-SL Goldman-M. Medina, Estudios sobre ciencia y tecnología, Barcelona, Anthropos, 163-194.

Díaz Muñoz, M. D. L. Á., & Díaz Castillo, C. (2002). El análisis de la vulnerabilidad en la cartografía de riesgos tecnológicos: algunas cuestiones conceptuales y metodológicas.

Fàbrega, J. C. (1999). Análisis del riesgo en instalaciones industriales (Vol. 77). Univ. Politèc. de Catalunya.

Cardona, O. (2001). La necesidad de repensar de manera holística los conceptos de vulnerabilidad y riesgo. Una crítica y una revisión necesaria para la gestión. In Work-Conference on Vulnerability in Disaster Theory and Practice. Wegeningen, Disaster Studies of Wegeningen University and Research Center. Available from< http://www. desenredando. org/public/articulos/2003/rmhcvr/rmhcvr_may-08-2003. pdf.

Palop, F., & Vicente, J. M. (1999). Vigilancia tecnológica e inteligencia competitiva: su potencial para la empresa española. Madrid: Cotec.

Vásquez Paco, K. A. (2010). Sistema de gestión de riesgos tecnológicos AS/NZ 4360: 2004.

REFERENCIAS ELECTRONICAS

ESE Hospital Emiro Quintero Cañizares Ocaña N. de S. Información Corporativa (presentación) [en línea] [citado el 08 de marzo de 2012] Disponible en internet: < http://www.hospitaleqc.gov.co/plataforma-estrategica/resena-historica.html>.

ESE Hospital Emiro Quintero Cañizares Ocaña N. de S. Plataforma Estratégica (Reseña histórica) [en línea] [citado el 08 de marzo de 2012] Disponible en internet: < http://www.hospitaleqc.gov.co/plataforma-estrategica/resena-historica.html>.

ESE Hospital Emiro Quintero Cañizares Ocaña N. de S. Planeación Estratégica (objetivos institucionales) [en línea] [citado el 30 de marzo de 2012] Disponible en internet: < http://www.hospitaleqc.gov.co/plataforma-estrategica/objetivos.html>.

FERNÁNDEZ, Eduardo. CFT soeduc concepto de auditoría Disponible en internet: <www.soeduc.cl/apuntes/concepto%20de%20auditoria.doc>
En Línea http://www.jkmst.com

Auditoría de Sistemas de Información. Seguridad informática: Conceptos básicos, Capítulo [en línea] Disponible en Internet:
<http://catarina.udlap.mx/u_dl_a/tales/documentos/lis/jerez_l_ca/capitulo1.pdf>

Disponible en línea http://www.iso27001standard.com

Disponible en Linea http://www.wto.org
Universidad Carlos III de madrid escuela politécnica superior seguridad lógica y de accesos y su auditoría *proyecto fin de carrera* ingeniería técnica en informática de gestión
Constitución política de Colombia. De la protección de la información y de los datos, Ley 1273 de 2009 [En Línea] Disponible en internet:

<http://www.dmsjuridica.com/CODIGOS/LEGISLACION/LEYES/2009/LEY_1273_DE_2009.html.

http://revista.seguridad.unam.mx/numero-14/riesgo-tecnol%C3%B3gico-y-su-impacto-para-las-organizaciones-parte-i

http://helid.digicollection.org/fr/d/Jcne05/1.1.html

ANEXOS

Anexo 1. Evaluación de la Seguridad Lógica.

EVALUACIÓN MEDIANTE EL ESTÁNDAR ISO 27001 DE LA SEGURIDAD FÍSICA Y LÓGICA DE LA INFRAESTRUCTURA TECNOLÓGICA DE LA E.S.E HOSPITAL EMIRO QUINTERO CAÑIZARES DE LA CIUDAD DE OCAÑA – NORTE DE SANTANDER.

Objetivo: Evaluación a la Seguridad Lógica

1) ¿Qué tipo de control existe para acceder a los equipos de cómputo o a los programas de software?

_____
_____

2) ¿Qué políticas posee La E.S.E. Hospital Emiro Quintero Cañizares para mantener la confidencialidad, integridad y disponibilidad de la información que se genera?

- o No existen
- o Si existen, Cuales? _____

3) ¿Cómo se cumplen estas políticas?

_____
_____

4) ¿Cómo se registra el cumplimiento de estas políticas?

_____
_____

5) ¿Qué mecanismos utiliza El Hospital para generar conciencia en sus empleados de la importancia de proteger la información que manejan?

- o Realizando capacitaciones.
- o No se hace concientización.
- o No hay protección de la información.
- o Otra _____

6) ¿Qué tipo de mecanismo se utiliza para el ingreso a las aplicaciones?

- o Usuario y Contraseña
- o Otro _____

7) ¿Dónde se encuentran las copias de las claves de acceso de los usuarios?

- o USB

- o DISCO DURO
- o CD
- o Otro _____

8) ¿Existen un acuerdo de confidencialidad entre la E.S.E. Hospital Emiro Quintero Cañizares y los empleados para la protección de la información que les ha sido encomendada? ¿Qué establece este acuerdo?

- o SI
- o NO
- o Cuál _____

9) ¿Qué pasa con las claves de acceso de esas personas que han dejado de laborar en la empresa?

- o Se eliminan
- o Permanecen vigentes
- o Otro _____

10) ¿Cómo se lleva a cabo la capacitación periódica a los usuarios en el adecuado manejo de los equipos y de los aplicativos?

- o De 1 a 3 meses
- o 4 a 6 meses
- o 7 a 9 meses
- o 10 a 12 meses
- o No se hace.

11) ¿Cómo hace la empresa para saber si estas capacitaciones fueron exitosas?

_____
_____

12) ¿Cómo se realizan las copias de seguridad de la información que se genera al interior de la E.S.E. Hospital Emiro Quintero Cañizares?

- o Manualmente
- o Automáticamente
- o Otro _____

13) ¿Dónde almacenan estas copias de respaldo?

- o Caja fuerte
- o Mueble con cerradura
- o Otro _____

14) ¿Qué medios utilizan para realizar las copias de la información?

- o CD
- o DVD
- o MEMORIAS USB
- o DISCOS DUROS
- o Otro _____

15) La E.S.E. Hospital Emiro Quintero Cañizares que tipo de programas utiliza para el proceso de recuperación de archivos en caso de fallas en los equipos?

_____
_____

16) ¿En los equipos de la E.S.E. Hospital Emiro Quintero Cañizares que tipo de software existe para la detección de intrusos?

_____
_____

17) ¿Qué software antivirus poseen los equipos de la E.S.E. Hospital Emiro Quintero Cañizares?

_____
_____

18) ¿Cada cuánto las bases de datos de estos antivirus son actualizadas?

_____
_____

19) ¿Cómo los operadores mantienen un registro de los eventos y acciones que realizan a diario?

_____
_____

20) ¿Cuáles son los procedimientos para evitar la ejecución de programas no autorizados?

_____
_____

21) ¿Dónde se archivan las bitácoras del sistema del equipo de cómputo?

_____
_____

22) ¿Cómo se restringe el acceso a los lugares asignados para guardar los dispositivos de almacenamiento?

_____
_____

Anexo 2. Evaluar los Elementos de Seguridad Física en el Ambito Informático.

EVALUACIÓN MEDIANTE EL ESTÁNDAR ISO 27001 DE LA SEGURIDAD FÍSICA Y LÓGICA DE LA INFRAESTRUCTURA TECNOLÓGICA DE LA E.S.E HOSPITAL EMIRO QUINTERO CAÑIZARES DE LA CIUDAD DE OCAÑA – NORTE DE SANTANDER.

Objetivo: Evaluar los elementos de seguridad física en el ámbito informático de la E.S.E. Hospital Emiro Quintero Cañizares

1) ¿Qué mecanismo utiliza/implementa la empresa para la protección física de los equipos de cómputo?

_____
_____

2) ¿Cómo se lleva a cabo en la E.S.E. Hospital Emiro Quintero Cañizares la labor de Mantenimientos preventivos y correctivos a los equipos de cómputo?

_____
_____

3) ¿Con que frecuencia?

- De 1 a 3 meses
- 4 a 6 meses
- 7 a 9 meses
- 10 a 12 meses
- No se hace.

4) ¿De qué manera el responsable del mantenimiento entrega reportes de las tareas ejecutadas?

_____
_____

5) ¿Cómo se lleva a cabo el plan de mantenimiento preventivo de equipos contemplado dentro de las políticas de la empresa? Si existe claro está?

_____
_____

6) ¿De qué manera se llevan a cabo las prohibiciones formales para el consumo de alimentos o bebidas cerca de los equipos de cómputo al igual que prohibiciones para fumar?

o Por medio de políticas de manejo de hardware.
o No hay prohibición.
o Otro _____

7) ¿En caso de presentarse algún incendio, la E.S.E. Hospital Emiro Quintero Cañizares cuenta con algún mecanismo de alerta y de extinción de fuego?

o SI
o NO
o Cuál _____

8) ¿Dónde está el inventario físico de los equipos de cómputo y dispositivos de comunicación que conforman la red de datos de el Hospital?

_____
_____

9) ¿Cuenta la E.S.E. Hospital Emiro Quintero Cañizares con un circuito cerrado de televisión las 24 horas del día?

o SI
o NO

10) ¿Qué mecanismo de vigilancia interna existe en el Hospital?

_____
_____

11) ¿Qué mecanismo de vigilancia externa existe en el Hospital?

_____
_____

12) ¿Qué tipo de restricciones existen para el ingreso al área de sistemas?

_____
_____

13) ¿Qué mecanismo de identificación utiliza el Hospital para sus empleados en el momento de ingresar a sus instalaciones?

_____
_____

Anexo 3. Evaluar el Servicio de Mantenimiento de Hardware.

EVALUACIÓN MEDIANTE EL ESTÁNDAR ISO 27001 DE LA SEGURIDAD FÍSICA Y LÓGICA DE LA INFRAESTRUCTURA TECNOLÓGICA DE LA E.S.E HOSPITAL EMIRO QUINTERO CAÑIZARES DE LA CIUDAD DE OCAÑA – NORTE DE SANTANDER.

Objetivo: Evaluación del servicio de mantenimiento de hardware

1) Especifique el tipo de contrato de mantenimiento de equipos de cómputo que se tiene en la E.S.E. Hospital Emiro Quintero Cañizares

_____
_____

2) ¿Cómo se lleva a cabo el programa de mantenimiento preventivo para cada dispositivo del sistema de cómputo?

_____
_____

3) ¿Cómo se verifica esta acción?

_____
_____

4) ¿Cómo se dan los tiempos de respuesta y de compostura en caso de fallas en los equipos de cómputo?

_____
_____

5) ¿Si los tiempos de reparación son superiores a los estipulados en el contrato, ¿Qué acciones correctivas se toman para ajustarlos a lo convenido?

_____
_____

6) ¿Cómo se notifican las fallas?

_____
_____

7) ¿Cómo se les da seguimiento?

_____
_____

8) ¿Se cuenta con un inventario de todos los equipos de cómputo que soportan la función informática de el Hospital?

o SI
o NO

9) ¿Con cuanta frecuencia se revisa el inventario?

o De 1 a 3 meses
o 4 a 6 meses
o 7 a 9 meses
o 10 a 12 meses
o No se hace.

10) ¿Qué mecanismo utiliza el área de mantenimiento para registrar las fallas detectadas en los equipos?

_____
_____

11) ¿Se lleva un control de los equipos en garantía, para que a la finalización de ésta, se integren a algún programa de mantenimiento?

_____
_____

12) ¿Se cuenta con servicio de mantenimiento para todos los equipos, incluyendo impresoras?

o SI
o NO

13) ¿Con cuanta frecuencia se realiza mantenimiento a los equipos?

o De 1 a 3 meses
o 4 a 6 meses
o 7 a 9 meses
o 10 a 12 meses
o No se hace.

14) ¿Qué políticas tiene el Hospital para el proceso de adquisición de nuevos equipos?

_____
_____

15) ¿Se tiene inventario actualizado de los equipos y terminales con su localización?

o SI
o NO

16) ¿Se tienen seguros sobre todos los equipos?

- o SI
- o NO

17) ¿Con que compañía?

_____

_____

Anexo 4. Evaluación a la Seguridad Física.

EVALUACIÓN MEDIANTE EL ESTÁNDAR ISO 27001 DE LA SEGURIDAD FÍSICA Y LÓGICA DE LA INFRAESTRUCTURA TECNOLÓGICA DE LA E.S.E HOSPITAL EMIRO QUINTERO CAÑIZARES DE LA CIUDAD DE OCAÑA – NORTE DE SANTANDER.

Objetivo: Evaluación a la Seguridad Física de la E.S.E. Hospital Emiro Quintero Cañizares

1) ¿La red cuenta con un sistema de protección ante descargas eléctricas? ¿Cuál? , ¿Hace cuánto tiempo?, ¿Se ha modificado su estructura?

_____
_____

2) ¿La E.S.E. Hospital Emiro Quintero Cañizares posee algún plan de contingencia que permita el normal desempeño de las actividades, aun cuando se presente algún inconveniente? ¿Cómo se lleva a cabo este plan?

- Inundaciones
- Terremotos
- Corte en el flujo eléctrico
- Daño en los equipos

_____
_____

3) ¿Existe conexión de polo a tierra para las instalaciones de los equipos de cómputo? ¿En qué lugar se encuentra?

_____
_____

4) ¿Con que frecuencia se lleva a cabo del mantenimiento de los aires acondicionado de la E.S.E. Hospital Emiro Quintero Cañizares?

- De 1 a 3 meses
- 4 a 6 meses
- 7 a 9 meses
- 10 a 12 meses
- No se hace.

5) ¿El personal de mantenimiento está capacitado para el mejor desempeño de sus funciones? ¿Quién realiza tal capacitación, si existe claro está?

_____
_____

6) ¿Cada cuánto se realizan estas capacitaciones?

- o De 1 a 3 meses
- o 4 a 6 meses
- o 7 a 9 meses
- o 10 a 12 meses
- o No se hace.

Anexo 5. Matriz de Riesgos

I. EVALUACIÓN RIESGOS																											II. EVALUACIÓN DE CONTROLES														III. VALORACIÓN DE RIESGOS VS. CONTROLES			IV. MAPA DE RIESGOS 2014				V. ESTRATEGIAS Y ACCIONES	
No. de Riesgo	Unidad Administrativa	Alineación a Estrategias, Objetivos, o Metas Institucionales		RIESGO	Nivel de decisión del Riesgo	Clasificación del Riesgo		FACTOR				Posibles efectos del Riesgo	Valoración Inicial			¿Tiene controles?	CONTROL		Determinación de Suficiencia o Deficiencia del Control						Riesgo Controlado Suficientemente	Valoración Final		UBICACIÓN EN CUADRANTES				Estrategia para Administrar el Riesgo	Descripción de la(s) Acción(es)
		Selección	Descripción			Selección	Especificar Otro	No. de Factor	Descripción	Clasificación	Tipo		Grado Impacto	Probabilidad Ocurrencia	Cuadrante		No.	Descripción	Tipo	Está Documentado	Está Formalizado	Se Aplica	Es Efectivo	Resultado de la determinación del Control		Grado de Impacto	Probabilidad de Ocurrencia	I	II	III	IV		
2014_1	area sistemas	Objetivo		Fallas electricas	Directivo	TIC´s		1.1	Contacto de árboles con el cableado eléctrico.	Entorno	Externo	Retraso en la continuidad del negocio o daño en los equipos.	6	5	III	NO									NO	6	5			III		TRANSFERIR EL RIESGO	Gestionar ante la Empresa pública de energía, la adecuación del tendido eléctrico
								1.2	Ausencia de pararrayos	Material	Interno					NO																				Solicitar a CORPONOR autorización para la poda de árboles que evite el corte de
								1.3	Carencia de planta eléctrica de alto poder	Material	Interno					NO																				
2014_2	Area de Sistemas	Estrategia		Pérdida de la Información	Directivo	TIC´s		2.1	Problemas de hardware	Material	Interno	Genera inconvenientes en el proceso de la Empresa.	5	7	II	NO									NO	5	7		II			REDUCIR EL RIESGO	Tener control en el acceso de personal
								2.2	Error humano	Humano	Interno					NO																				Prohibir el uso de USB en los equipos
								2.3	Virus	TIC's	Externo					NO																				Poner seguridad en las puertas de enlace de la red.
2014_3	Area de Sistemas	Meta		Inseguridad en Area de servidores y central telefónica	Directivo	Seguridad		3.1	No hay control en el acceso al area de servidores	Humano	Interno	Perdida de la informacion contenida en los servidores y/o Daño de los equipos.	6	7	I	NO									NO	6	7	I				EVITAR EL RIESGO	Implementar políticas de seguridad para el ingreso de personas ajenas al area de servidores
								3.2	No hay control en el acceso al area de central telefonica	Humano	Interno					NO																				Implementar políticas de seguridad para el ingreso de personas ajenas a la central
2014_4	Area de sistemas	Meta		Software sin licencia	Directivo	Legal		4.1	Caducidad en la licencia.	Humano	Interno	Daño de equipos, posibles sanciones civiles y penales por incumplimiento de normas.	5	6	II	NO									NO	5	6		II			REDUCIR EL RIESGO	Tener software licenciado en su totalidad para un mejor manejo de los equipos
								4.2	El procesamiento del equipo se hace lento	Material	Interno					NO																				
								4.3	Facil acceso de virus al sistema operativo y a los archivos.	TIC's	Interno					NO																				
2014_5	Area de Sistemas	Objetivo		Tecnologia obsoleta.	Directivo	TIC´s		5.1	Poco rendimiento en el proceso.	TIC's	Interno	Falta de credibilidad en la toma de decisiones.	5	6	II	NO									NO	5	6		II			TRANSFERIR EL RIESGO	Actualizar los equipos de computo para mejora en la prestación del servicio
								5.2	Software antiguo	TIC's	Interno					NO																				Gestionar tecnologia de punta y asi obtener una mayor credibilidad en los usuarios
2014_6	Area de sistemas	Meta		Daño de Hardware	Operativo	TIC´s		6.1	Mal uso del Hardware	Humano	Interno	Daño o perdida de la Informacion	6	7	I	NO									NO	6	7	I				EVITAR EL RIESGO	Generar políticas de Uso de Hardware
								6.2	Daño por desastre natural	Entorno	Externo					NO																				Generar un Plan de Contingencia para la seguridad de los mismos
								6.3	Instalacion y desintalacion de programas sin un control pertinente.	Humano	Interno					NO																				Llevar un control y generar restricciones de la red de descargas
2014_7	Area de sistemas	Objetivo		Infeccion por Virus Informatico	Directivo	TIC´s		7.1	Facil infeccion de virus	Humano	Externo	Perdida de laInformacion y esto genera inconvenientes en el proceso de la Empresa.	7	8	I	NO									NO	7	8	I				REDUCIR EL RIESGO	Prohibir el uso de dispositivos que puedan infectar los equipos.
								7.2	Ausencia de antivirus licenciados	Técnico-Administrativo	Interno					NO																				Contratar el servicio de un antivirus licenciado

Anexos 6. Seguimiento a las Copias de Seguridad

E.S.E. HOSPITAL EMIRO QUINTERO CAÑIZARES
OCAÑA NORTE DE SANTANDER

SEGUIMIENTO COPIAS DE SEGURIDAD

Nombre / Apellido	Cargo	Buckups		Fecha	Firma	Observaciones
		Si	No			
				DD/MM/AAAA		
				DD/MM/AAAA		
				DD/MM/AAAA		
				DD/MM/AAAA		
				DD/MM/AAAA		
				DD/MM/AAAA		
				DD/MM/AAAA		
				DD/MM/AAAA		
				DD/MM/AAAA		
				DD/MM/AAAA		
				DD/MM/AAAA		
				DD/MM/AAAA		
				DD/MM/AAAA		
				DD/MM/AAAA		
				DD/MM/AAAA		

Anexo 7. Seguimiento de las Inscripciones a las Capacitaciones

E.S.E. HOSPITAL EMIRO QUINTERO CAÑIZARES
OCAÑA NORTE DE SANTANDER

ACTIVIDAD / OBJETIVO			FECHA	HORA	LUGAR
			DD / MM / AAAA	HH : MM	
REALIZADO POR					
NOMBRE / APELLIDOS	ID	CARGO / SERVICIO	TELÉFONO	E-MAIL	

Anexo 8. Seguimiento al Acceso a los Servidores

<table>
<tr><td colspan="6">E.S.E. HOSPITAL EMIRO QUINTERO CAÑIZARES
OCAÑA NORTE DE SANTANDER</td></tr>
<tr><td colspan="6">REGISTRO DE ACCESO AL ÁREA DE SERVIDORES</td></tr>
<tr><td rowspan="2">Nombre y Apellidos de la persona que solicita acceso</td><td rowspan="2">Funcionario</td><td colspan="2">Interno</td><td></td></tr>
<tr><td></td><td colspan="2">Externo</td><td></td></tr>
<tr><td>Funcionario que autoriza el ingreso</td><td>Cargo</td><td colspan="3">Fecha</td></tr>
<tr><td></td><td></td><td colspan="3">DD / MM / AAAA</td></tr>
<tr><td rowspan="2">Descripción de las actividades a realizar:</td><td>Permanece bajo supervisión</td><td>SI</td><td colspan="2">NO</td></tr>
<tr><td rowspan="5"></td><td colspan="4">Funcionario(s) que realiza(n) la supervisión</td></tr>
<tr><td colspan="4"></td></tr>
<tr><td colspan="4">Cargo(s)</td></tr>
<tr><td colspan="4"></td></tr>
<tr><td>Hora entrada</td><td>Hora salida</td><td colspan="2">Fecha</td></tr>
<tr><td></td><td></td><td></td><td colspan="2">DD / MM / AAAA</td></tr>
<tr><td colspan="6">OBSERVACIONES</td></tr>
<tr><td colspan="2">FUNCIONARIO QUE AUTORIZA EL INGRESO
(En caso de registrar una situación especifica)</td><td colspan="4">FUNCIONARIO QUE INGRESA AL ÁREA
(En caso de registrar una situación específica)</td></tr>
</table>

FORMATO REGISTRO DE ACCESO AL ÁREA DE SERVIDORES

_____ _____

FIRMA
(Funcionario que autoriza el ingreso)

FIRMA
(Funcionario que ingresa)

Anexo 9. Creación de las Cuentas de Usuario

E.S.E. HOSPITAL EMIRO QUINTERO CAÑIZARES
OCAÑA NORTE DE SANTANDER

Solicitud de CUENTA DE USUARIO PARA SISTEMA DE INFORMACIÓN

CREACION ☐ MODIFICACION EL☐INACION ☐

1. Apellido y Nombre completo
   _____
2. Nombre de (Área / Servicio)
   _____
3. Oficina _____
4. Teléfono _____

ROLES: Administrador ☐ Usuario Operativo ☐

5. Sistema de información al que tiene acceso
   _____

_____
_____
(NOMBRE DE SISTEMA DE INFORMACION AL QUE TIENE ACCESO)

6. Email _____@_____

_____ _____
Firma Autorizado
Jefe de Área / Servicio

Firma
Usuario que solicita la cuenta

Para uso interno de la E.S.E Hospital Emiro Quintero Cañizares

Fecha de Solicitud: DD / MM / AAAA. Recibido por:_____

Nombre de usuario:_____

Fecha de Creación: DD / MM / AAAA. Creado por:_____
Fecha de entrega: DD / MM / AAAA. Entregado por:_____
Si el formulario no es retirado dentro de los 30 días y no registra actividad en su cuenta, la misma será dada de baja.

Para el Usuario

Usuario:_____ Password Inicial:_____
Esta clave es sólo para activar la cuenta, es obligatorio el cambio de la misma.
Si el formulario no es retirado dentro de los 30 días y no registra actividad en su cuenta, la misma será dada de baja.

ADMINISTRACIÓN DE CUENTAS DE USUARIOS

Anexo 10. Buen Uso de Hardware

POLITICAS PARA EL BUEN USO DEL HARDWARE

Esta política se refiere al buen uso que debemos darle a los equipos de Cómputo de La E.S.E Hospital Emiro Quintero Cañizares.

1.- POLÍTICAS DE SEGURIDAD PARA EQUIPOS DE COMPUTO

1.1. Los equipos de Cómputo sólo deben usarse en un ambiente seguro. Se considera que un ambiente es seguro cuando se han implementado las medidas de control apropiadas para proteger el software, el hardware y los datos. Esas medidas deben estar acorde a la importancia de los datos y la naturaleza de riesgos previsibles.

1.2. Los equipos sólo deben usarse para actividades de trabajo y no para otros fines, tales como juegos y pasatiempos.

1.3. Debe respetarse y no modificar la configuración de hardware y software establecida por el departamento de sistemas.

1.4. No se permite, comer o beber mientras se esté usando una equipo.

1.5. Deben protegerse los equipos de riesgos del medioambiente (por ejemplo, polvo, incendio y agua).

1.6. Deben usarse protectores contra transitorios de energía eléctrica y en los servidores deben usarse fuentes de poder ininterrumpibles (UPS).

1.7. Cualquier falla en las computadoras o en la red debe reportarse inmediatamente ya que podría causar problemas serios como pérdida de la información o no disponibilidad de los servicios.

1.8. Los equipos deben marcarse para su identificación y control de inventario. Los registros de inventario deben mantenerse actualizados.

1.9. No pueden moverse los equipos o reubicarlos sin permiso. Para llevar un equipo fuera de la ESE se requiere una autorización escrita.

1.10. La pérdida o robo de cualquier componente de hardware o programa de software debe ser reportada inmediatamente.

1.11. Para prevenir el acceso no autorizado, los usuarios deben usar un sistema de contraseñas y además deben configurar el protector de pantalla

para que se active al cabo de 15 minutos de inactividad y que requiera una contraseña al reasumir la actividad.

1.12. No está permitido conectar a la RED computadores portátiles (laptops) de terceros y en caso de ser necesario se debe solicitar la autorización correspondiente y notificar al departamento de sistemas.

1.13. Para prevenir la intrusión de hackers a través de puertas traseras, no está permitido el uso de módems en PCs que tengan también conexión a la red local (LAN), a menos que sea debidamente autorizado. Todas las comunicaciones de datos deben efectuarse a través de la LAN.

1.14. A menos que se indique lo contrario, los usuarios deben asumir que todo el software de la Fundación está protegido por derechos de autor y requiere licencia de uso. Por tal razón es ilegal y está terminantemente prohibido hacer copias o usar ese software para fines personales.

1.15. Debe instalarse y activarse una herramienta antivirus, la cual debe mantenerse actualizada. Si se detecta la presencia de un virus u otro agente potencialmente peligroso, se debe notificar inmediatamente al departamento de Sistemas y poner el equipo en cuarentena hasta que el problema sea resuelto.

1.16. Sólo pueden bajarse archivos de redes externas de acuerdo a los procedimientos establecidos a continuación.

- Solo se pueden bajar archivos que sean estrictamente de trabajo y ubicados en servidores de confianza.
- No se permite descargar música, videos, o programas no autorizados de Internet.
- No se permite hacer transferencia de archivos a través de programas de mensajería como yahoo Messenger, aol instant Messenger, ICQ.
- No se permite descargar archivos y guardarlos localmente desde correos personales como Hotmail, yahoo, etc.
- Debe utilizarse un programa antivirus para examinar todo software que venga de fuera.

1.17. No debe utilizarse software bajado de Internet y en general software que provenga de una fuente no confiable, a menos que haya sido comprobado en forma rigurosa y que esté aprobado su uso por el departamento de Sistemas.

1.18. Para prevenir demandas legales o la introducción de virus informáticos, se prohíbe estrictamente la instalación de software no autorizado, incluyendo el que haya sido adquirido por el propio usuario. Así mismo, no se permite el uso de software de distribución gratuita o shareware, a menos que haya sido previamente aprobado por el departamento de Sistemas.

1.19. Para ayudar a restaurar los programas originales no dañados o infectados, deben hacerse copias de todo el software nuevo antes de su uso, y deben guardarse tales copias en un lugar seguro.

1.20. No deben usarse USB u otros medios de almacenamiento de externos en cualquier computadora a menos que se haya previamente verificado que están libres de virus u otros agentes dañinos.

1.21. Periódicamente debe hacerse el respaldo de los datos guardados en PC's y servidores y las copias de respaldo deben guardarse en un lugar seguro, a prueba de hurto, incendio e inundaciones.

1.22. Es responsabilidad del usuario tener toda su información dentro de una sola carpeta raíz, como Mis Documentos, para facilitar el respaldo de su información.

1.23. La información de carácter personal se deberá almacenar en una carpeta fuera de Mis Documentos y esta no formará parte del respaldo del equipo responsabilidad del departamento de sistemas.

1.24. El conocimiento de las claves de acceso a cuentas de correo, servicios Web y servidores debe limitarse estrictamente a las personas autorizadas (departamento de sistemas y una persona más para emergencias) y en ningún caso deben revelarse a consultores, contratistas y personal temporal.

1.25. Siempre que sea posible, debe eliminarse información confidencial de las computadoras y unidades de disco duro antes de que se les mande a reparar. Si esto no es posible, se debe asegurar que la reparación sea efectuada por empresas responsables, con las cuales se haya firmado un contrato de confidencialidad. Alternativamente, debe efectuarse la reparación bajo la supervisión de un representante.

1.26. Los usuarios deben ser responsables de sus impresiones y por lo tanto asegurarse de recoger sus documentos impresos y revisar que la impresora quede con suficiente papel.

1.27. Los usuarios que tengan impresoras instaladas dentro de su cubículo o en su área de trabajo (conectadas directamente a sus equipos o en Red) son responsables de encender y apagar la(s) impresora(as).

1.28. El personal que utiliza un equipo portátil que contenga información confidencial de la Fundación, no debe dejarla desatendida, sobre todo cuando esté de viaje.

1.29. Los equipos de cómputo deben apagarse por completo durante periodos largos de ausencia (juntas, reuniones, hora de comida) y por supuesto al salir de la oficina, asegurándose de apagar también el monitor.
Anexo 11. Cuentas de Usuario

POLITICAS DE CUENTAS DE USUARIO

Esta política se refiere a la administración de cuentas de usuarios, así como el acceso a los sistemas computacionales de La E.S.E Hospital Emiro Quintero Cañizares.

1.- DECLARACION

Para todo sistema computacional de El Hospital Emiro Quintero Cañizares, el usuario poseerá una cuenta personal que lo identifique unívocamente en relación a las acciones que realice.

Para conectarse a los sistemas computacionales de El Hospital Emiro Quintero Cañizares, el usuario registrará quién es (identificación) y comprobar que es quién dice ser (autenticación).

La identificación se realiza mediante un código o Identificación de Usuario (User Id.). La autenticación se realiza mediante algo que sólo el usuario conoce ("Password" o "Clave").

Las cuentas asignadas a los usuarios tienen el carácter de personal e intransferible.
Cada usuario es responsable único e indelegable de todas las acciones ejecutadas con la cuenta que se le ha asignado.

Los permisos de accesos a los sistemas se asignarán de acuerdo a las necesidades del cargo que desempeña el usuario y deben ser solicitados por su Superior Directo.
Se mantendrá restringido el uso de los usuarios con capacidades especiales (super usuarios), destinados a la administración de los sistemas operativos y generar usuarios con menores capacidades para efectuar las labores de administración necesarias.

2.- AMBITO

Esta política abarca todos los recursos computacionales de El Hospital Emiro Quintero Cañizares que requieran la creación de cuentas de acceso.
Incluye todos los usuarios que accedan a algún recurso computacional, operadores y administradores de El Hospital Emiro Quintero Cañizares.

Incluye usuarios externos que accedan "temporalmente" a algún recurso computacional de El Hospital Emiro Quintero Cañizares.

3.- ROLES Y RESPONSABILIDADES

Oficial de Seguridad:

- Propondrá los esquemas de claves adecuados, cuando la plataforma tecnológica no permita ajustarse a la política.

- Autorizará la creación de cuentas de usuarios externos.
- Validará y autorizará, si corresponde, excepciones de asignación de privilegios de administración a cuentas que no pertenecen al grupo de administradores.

Responsables de Generación de Cuentas de Usuario:

Son responsables de la generación de Cuentas de Usuario las siguientes unidades:

- Departamento de Operaciones/Soporte.
- Departamento de Organización y Calidad.

Departamento de Soporte/Operaciones:

- Crearán Identificadores de Usuario, según su ámbito de responsabilidad.
- Deberán mantener la información referida a la creación de las cuentas de usuario.
- Asignarán una clave expirada en la creación de un Identificador de Usuario nuevo, o cuando se solicita su cambio por olvido o bloqueo de la cuenta.
- Cuando se recibe un nuevo dispositivo bajo su responsabilidad, cambia las claves por omisión, a los estándares de El Hospital Emiro Quintero Cañizares.

Departamento de Organización y Calidad:
- Verificar funciones del cargo con perfiles asignados a sistemas y aplicaciones.

Jefe de Unidad:

- Será responsable de las cuentas de usuarios externos de empresas para las cuales administra su relación.

Supervisor Directo:

- Solicitará la creación de cuentas de usuario de colaboradores bajo su responsabilidad, como así también los cambios justificados en los privilegios de las cuentas de usuario y las eliminaciones de los accesos otorgados cuando el usuario deja de pertenecer a su unidad.

4.- CUERPO

4.1 Tipos de Cuentas de Usuario.

4.1.1 Se mantendrán distintos tipos de cuentas de usuario en relación con los privilegios permitidos, de acuerdo al cargo que desempeña en El Hospital Emiro Quintero Cañizares. Estos tipos de cuenta deberán mantener un perfil propio, los que serán usados como “Perfil Tipo” si no se especifican otras características.

4.2 Creación de Cuentas de Usuario.

4.2.1 Todo nuevo Identificador de Usuario que se cree para cuentas de usuarios, debe ser asignado por el Responsable de la Generación de Cuentas de Usuario.

4.2.2 Se deberá velar por la utilización de un único Identificador de Usuario para una misma persona en diferentes sistemas.

4.2.3 La creación de un nuevo Identificador de Usuario debe ser solicitado por escrito por el Supervisor Directo a la Unidad responsable, indicando claramente:

- La identificación del usuario (Nombre y RUT).
- El motivo de su creación.
- Fecha de expiración en caso de ser temporal.
- Rol o perfil asociado.
- Restricciones o privilegios adicionales relacionadas con la cuenta.

4.2.4 Los Responsables de la Generación de Cuentas de Usuario deben velar por el almacenamiento y actualización de tal información.

4.2.5 El Identificador de Usuario estará compuesto por la primera letra del nombre, seguido del apellido completo, o hasta completar siete caracteres. En caso de duplicidad, se agregarán o modificarán letras hasta lograr la unicidad.

4.2.6 Los cambios de privilegios asignados a una cuenta deben ser solicitados por el Supervisor Directo.

4.3 Cuentas de Administración.

4.3.1 Cuando sea posible, no se usarán las cuentas de administración estándares de los sistemas, sino que se crearán cuentas personalizadas para los administradores con privilegios equivalentes y claves “robustas” (no triviales).

4.3.2. No se permitirá asignar privilegios de administración a cuentas que no pertenezcan al grupo de administradores. Cualquier excepción debe ser validada expresamente por el Oficial de Seguridad.

4.4 Cuentas de Usuarios Externos.

4.4.1 La asignación de Cuentas de Usuario y clave para usuarios externos a El Hospital Emiro Quintero Cañizares, debe ser solicitada formalmente a la Unidad responsable, por el Jefe de la Unidad que administra la relación con la empresa externa, quien debe indicar motivo, horarios de conexión y fecha de expiración. La autorización debe darla el Oficial de Seguridad.

4.4.2 Las cuentas de usuarios externos contarán con atributos restringidos y tendrán accesos exclusivamente a las Aplicaciones o Plataformas necesarias para el desarrollo de la labor que realizarán y poseerán obligatoriamente una fecha de expiración.

4.4.3 El Jefe de la Unidad que administra la relación con la Empresa Externa deberá a lo menos mensualmente, revisar los logs de las aplicaciones que se están accesando por parte de estos usuarios.

4.4.4 La responsabilidad de la vigencia de estas cuentas quedará radicada en el Jefe de la Unidad que administra la relación con la empresa externa.

4.5 Identificación de Usuario y Claves Requeridas.

4.5.1 Antes de tener acceso a cualquier recurso de la red, todos los usuarios serán identificados positivamente mediante su Identificador de Usuario y su Clave.

4.5.2 El Identificador de Usuario y la Clave será de uso estrictamente personal.

4.5.3 Está prohibido el uso de un Identificador de Usuario ajeno o facilitar el Identificador de Usuario y/o su Clave personal a un tercero.

4.6 Información en la Pantalla de Ingreso.

4.6.1 Las pantallas de ingreso sólo deben considerar el ingreso de Identificador de Usuario y Clave y deben advertir que el uso del sistema está restringido a personal autorizado, que registrará las operaciones efectuadas y, en caso de acciones indebidas, el causante se verá expuesto a las sanciones pertinentes.

4.6.2 Estas pantallas de ingreso no deberán entregar información adicional (datos de El Hospital Emiro Quintero Cañizares, sistema operativo, configuración del servidor, identificador de usuario anterior conectado), hasta que el ingreso haya sido autorizado.

4.7 Largo Mínimo y Contenido de Clave.

4.7.1 Toda cuenta de usuario normal, considerará para la clave secreta un largo mínimo de 6 caracteres combinando dígitos numéricos y letras. Se sugiere incluir caracteres especiales y la combinación de minúsculas y mayúsculas.

4.7.2 Para las cuentas con privilegios de administración utilizar un criterio de clave robusta, que considere al menos 10 caracteres, combinando mayúsculas, minúsculas, dígitos numéricos y caracteres especiales.

4.7.3 En el caso que no se puedan utilizar los esquemas de clave señalados anteriormente, el Oficial de Seguridad propondrá el esquema más adecuado según la plataforma tecnológica de que se trate.

4.8 Cambio Periódico de las Claves.

4.8.1 En donde sea posible, se debe establecer el cambio obligatorio de claves a lo más cada 30 días. El cambio deberá ser efectuado por el usuario.

4.9 Uso de Diferentes Claves en el Tiempo.

4.9.1 Los usuarios no deben crear claves que sean idénticas a las 24 anteriormente utilizadas.

4.10 Asignación de Claves Expiradas y Reasignación de Claves.

4.10.1 La clave asignada por los Responsables de la Generación de Cuentas de Usuario, debe estar expirada de modo que obligue al usuario a cambiarla en su primera conexión.

4.10.2 En caso de olvido o bloqueo, el usuario debe solicitar a los Responsables de la Generación de Cuentas de Usuario una nueva clave. Previa identificación positiva, los Responsables de la Generación de Cuentas de Usuario generarán y entregarán al usuario una nueva clave expirada.

4.11 Almacenamiento de Claves.

4.11.1 No incorporar claves en el código fuente de las aplicaciones.

4.11.2 No mantener listados de claves en archivos en texto plano o fácilmente legible.

4.11.3 Los archivos con listas de Identificador de Usuarios y Claves tanto activas como históricas se deben mantener encriptados en todo momento.

4.12 Claves en Dispositivos de Red.

4.12.1 Todos los dispositivos de red (routers, firewalls, etc.) deben tener claves u otro mecanismo de control de acceso. Para evitar el compromiso masivo en caso de ataque a los sistemas de comunicaciones, cada dispositivo debe tener una clave única de acceso.

4.12.2 Si un dispositivo no posee Clave de acceso, se debe permitir el acceso físico, sólo al personal autorizado.
4.13 Claves por Omisión.

4.13.1 Toda clave por omisión (“default”) provista por el fabricante de cualquier sistema, debe ser reemplazada de acuerdo a los estándares de El Hospital Emiro Quintero Cañizares.

4.14 Límite a Intentos Fallidos de Ingreso.

4.14.1 Para prevenir ingresos mediante la prueba de varias posibles claves, se limita la aceptación de intentos consecutivos de ingreso de claves. Después de 3 intentos fallidos, la Cuenta de Usuario debe quedar deshabilitada. Sólo los Responsables de la Generación de Cuentas de Usuario, podrán habilitarla nuevamente, previa verificación de la identidad del usuario.

4.14.2 En caso de usuarios externos la cuenta sólo podrá ser reactivada a solicitud del Jefe de la Unidad que administra la relación con la empresa externa.

4.15 Recordatorio de Claves.

4.15.1 Queda prohibido anotar las claves de acceso en lugares públicos, como por ejemplo, debajo del teclado, en el taco de la agenda, bajo el teléfono, detrás de una fotografía, etc.

Anexo 11. Cuentas de Usuario.

POLITICAS DE CUENTAS DE USUARIO

Esta política se refiere a la administración de cuentas de usuarios, así como el acceso a los sistemas computacionales de La E.S.E Hospital Emiro Quintero Cañizares.

1.- DECLARACION

Para todo sistema computacional de El Hospital Emiro Quintero Cañizares, el usuario poseerá una cuenta personal que lo identifique unívocamente en relación a las acciones que realice.

Para conectarse a los sistemas computacionales de El Hospital Emiro Quintero Cañizares, el usuario registrará quién es (identificación) y comprobar que es quién dice ser (autenticación).

La identificación se realiza mediante un código o Identificación de Usuario (User Id.). La autenticación se realiza mediante algo que sólo el usuario conoce ("Password" o "Clave").

Las cuentas asignadas a los usuarios tienen el carácter de personal e intransferible.
Cada usuario es responsable único e indelegable de todas las acciones ejecutadas con la cuenta que se le ha asignado.

Los permisos de accesos a los sistemas se asignarán de acuerdo a las necesidades del cargo que desempeña el usuario y deben ser solicitados por su Superior Directo.
Se mantendrá restringido el uso de los usuarios con capacidades especiales (super usuarios), destinados a la administración de los sistemas operativos y generar usuarios con menores capacidades para efectuar las labores de administración necesarias.

2.- AMBITO

Esta política abarca todos los recursos computacionales de El Hospital Emiro Quintero Cañizares que requieran la creación de cuentas de acceso.
Incluye todos los usuarios que accedan a algún recurso computacional, operadores y administradores de El Hospital Emiro Quintero Cañizares.

Incluye usuarios externos que accedan "temporalmente" a algún recurso computacional de El Hospital Emiro Quintero Cañizares.

3.- ROLES Y RESPONSABILIDADES

Oficial de Seguridad:

- Propondrá los esquemas de claves adecuados, cuando la plataforma tecnológica no permita ajustarse a la política.
- Autorizará la creación de cuentas de usuarios externos.
- Validará y autorizará, si corresponde, excepciones de asignación de privilegios de administración a cuentas que no pertenecen al grupo de administradores.

Responsables de Generación de Cuentas de Usuario:

Son responsables de la generación de Cuentas de Usuario las siguientes unidades:

- Departamento de Operaciones/Soporte.
- Departamento de Organización y Calidad.

Departamento de Soporte/Operaciones:

- Crearán Identificadores de Usuario, según su ámbito de responsabilidad.
- Deberán mantener la información referida a la creación de las cuentas de usuario.
- Asignarán una clave expirada en la creación de un Identificador de Usuario nuevo, o cuando se solicita su cambio por olvido o bloqueo de la cuenta.
- Cuando se recibe un nuevo dispositivo bajo su responsabilidad, cambia las claves por omisión, a los estándares de El Hospital Emiro Quintero Cañizares.

Departamento de Organización y Calidad:
- Verificar funciones del cargo con perfiles asignados a sistemas y aplicaciones.

Jefe de Unidad:

- Será responsable de las cuentas de usuarios externos de empresas para las cuales administra su relación.

Supervisor Directo:

- Solicitará la creación de cuentas de usuario de colaboradores bajo su responsabilidad, como así también los cambios justificados en los privilegios de las cuentas de usuario y las eliminaciones de los accesos otorgados cuando el usuario deja de pertenecer a su unidad.

4.- CUERPO

4.1 Tipos de Cuentas de Usuario.

4.1.1 Se mantendrán distintos tipos de cuentas de usuario en relación con los privilegios permitidos, de acuerdo al cargo que desempeña en El Hospital Emiro Quintero Cañizares. Estos tipos de cuenta deberán mantener un perfil propio, los que serán usados como "Perfil Tipo" si no se especifican otras características.

4.2 Creación de Cuentas de Usuario.

4.2.1 Todo nuevo Identificador de Usuario que se cree para cuentas de usuarios, debe ser asignado por el Responsable de la Generación de Cuentas de Usuario.

4.2.2 Se deberá velar por la utilización de un único Identificador de Usuario para una misma persona en diferentes sistemas.

4.2.3 La creación de un nuevo Identificador de Usuario debe ser solicitado por escrito por el Supervisor Directo a la Unidad responsable, indicando claramente:

- La identificación del usuario (Nombre y RUT).
- El motivo de su creación.
- Fecha de expiración en caso de ser temporal.
- Rol o perfil asociado.
- Restricciones o privilegios adicionales relacionadas con la cuenta.

4.2.4 Los Responsables de la Generación de Cuentas de Usuario deben velar por el almacenamiento y actualización de tal información.

4.2.5 El Identificador de Usuario estará compuesto por la primera letra del nombre, seguido del apellido completo, o hasta completar siete caracteres. En caso de duplicidad, se agregarán o modificarán letras hasta lograr la unicidad.

4.2.6 Los cambios de privilegios asignados a una cuenta deben ser solicitados por el Supervisor Directo.

4.3 Cuentas de Administración.

4.3.1 Cuando sea posible, no se usarán las cuentas de administración estándares de los sistemas, sino que se crearán cuentas personalizadas para los administradores con privilegios equivalentes y claves "robustas" (no triviales).

4.3.2. No se permitirá asignar privilegios de administración a cuentas que no pertenezcan al grupo de administradores. Cualquier excepción debe ser validada expresamente por el Oficial de Seguridad.

4.4 Cuentas de Usuarios Externos.

4.4.1 La asignación de Cuentas de Usuario y clave para usuarios externos a El Hospital Emiro Quintero Cañizares, debe ser solicitada formalmente a la Unidad responsable, por el Jefe de la Unidad que administra la relación con la empresa externa, quien debe indicar motivo, horarios de conexión y fecha de expiración. La autorización debe darla el Oficial de Seguridad.

4.4.2 Las cuentas de usuarios externos contarán con atributos restringidos y tendrán accesos exclusivamente a las Aplicaciones o Plataformas necesarias para el desarrollo de la labor que realizarán y poseerán obligatoriamente una fecha de expiración.

4.4.3 El Jefe de la Unidad que administra la relación con la Empresa Externa deberá a lo menos mensualmente, revisar los logs de las aplicaciones que se están accesando por parte de estos usuarios.

4.4.4 La responsabilidad de la vigencia de estas cuentas quedará radicada en el Jefe de la Unidad que administra la relación con la empresa externa.

4.5 Identificación de Usuario y Claves Requeridas.

4.5.1 Antes de tener acceso a cualquier recurso de la red, todos los usuarios serán identificados positivamente mediante su Identificador de Usuario y su Clave.

4.5.2 El Identificador de Usuario y la Clave será de uso estrictamente personal.

4.5.3 Está prohibido el uso de un Identificador de Usuario ajeno o facilitar el Identificador de Usuario y/o su Clave personal a un tercero.

4.6 Información en la Pantalla de Ingreso.

4.6.1 Las pantallas de ingreso sólo deben considerar el ingreso de Identificador de Usuario y Clave y deben advertir que el uso del sistema está restringido a personal autorizado, que registrará las operaciones efectuadas y, en caso de acciones indebidas, el causante se verá expuesto a las sanciones pertinentes.

4.6.2 Estas pantallas de ingreso no deberán entregar información adicional (datos de El Hospital Emiro Quintero Cañizares, sistema operativo, configuración del servidor, identificador de usuario anterior conectado), hasta que el ingreso haya sido autorizado.

4.7 Largo Mínimo y Contenido de Clave.

4.7.1 Toda cuenta de usuario normal, considerará para la clave secreta un largo mínimo de 6 caracteres combinando dígitos numéricos y letras. Se sugiere incluir caracteres especiales y la combinación de minúsculas y mayúsculas.

4.7.2 Para las cuentas con privilegios de administración utilizar un criterio de clave robusta, que considere al menos 10 caracteres, combinando mayúsculas, minúsculas, dígitos numéricos y caracteres especiales.

4.7.3 En el caso que no se puedan utilizar los esquemas de clave señalados anteriormente, el Oficial de Seguridad propondrá el esquema más adecuado según la plataforma tecnológica de que se trate.

4.8 Cambio Periódico de las Claves.

4.8.1 En donde sea posible, se debe establecer el cambio obligatorio de claves a lo más cada 30 días. El cambio deberá ser efectuado por el usuario.

4.9 Uso de Diferentes Claves en el Tiempo.

4.9.1 Los usuarios no deben crear claves que sean idénticas a las 24 anteriormente utilizadas.

4.10 Asignación de Claves Expiradas y Reasignación de Claves.

4.10.1 La clave asignada por los Responsables de la Generación de Cuentas de Usuario, debe estar expirada de modo que obligue al usuario a cambiarla en su primera conexión.

4.10.2 En caso de olvido o bloqueo, el usuario debe solicitar a los Responsables de la Generación de Cuentas de Usuario una nueva clave. Previa identificación positiva, los Responsables de la Generación de Cuentas de Usuario generarán y entregarán al usuario una nueva clave expirada.

4.11 Almacenamiento de Claves.

4.11.1 No incorporar claves en el código fuente de las aplicaciones.

4.11.2 No mantener listados de claves en archivos en texto plano o fácilmente legible.

4.11.3 Los archivos con listas de Identificador de Usuarios y Claves tanto activas como históricas se deben mantener encriptados en todo momento.

4.12 Claves en Dispositivos de Red.

4.12.1 Todos los dispositivos de red (routers, firewalls, etc.) deben tener claves u otro mecanismo de control de acceso. Para evitar el compromiso masivo en caso de ataque a los sistemas de comunicaciones, cada dispositivo debe tener una clave única de acceso.

4.12.2 Si un dispositivo no posee Clave de acceso, se debe permitir el acceso físico, sólo al personal autorizado.

4.13 Claves por Omisión.

4.13.1 Toda clave por omisión (“default”) provista por el fabricante de cualquier sistema, debe ser reemplazada de acuerdo a los estándares de El Hospital Emiro Quintero Cañizares.

4.14 Límite a Intentos Fallidos de Ingreso.

4.14.1 Para prevenir ingresos mediante la prueba de varias posibles claves, se limita la aceptación de intentos consecutivos de ingreso de claves. Después de 3 intentos fallidos, la Cuenta de Usuario debe quedar deshabilitada. Sólo los Responsables de la Generación de Cuentas de Usuario, podrán habilitarla nuevamente, previa verificación de la identidad del usuario.

4.14.2 En caso de usuarios externos la cuenta sólo podrá ser reactivada a solicitud del Jefe de la Unidad que administra la relación con la empresa externa.

4.15 Recordatorio de Claves.

4.15.1 Queda prohibido anotar las claves de acceso en lugares públicos, como por ejemplo, debajo del teclado, en el taco de la agenda, bajo el teléfono, detrás de una fotografía, etc.

Anexo 12. Seguridad de la Información

ÍNDICE

1. INTRODUCCIÓN

La información es un recurso que, como el resto de los activos, tiene valor para la E.S.E. Y por consiguiente debe ser debidamente protegida, garantizando la continuidad de los sistemas de información, minimizando los riesgos de daño y contribuyendo de esta manera, a una mejor gestión del Hospital.

Para que estos principios de la Política de Seguridad de la Información sean efectivos, resulta necesaria la implementación de una Política de Seguridad de la Información que forme parte de la cultura organizacional de la E.S.E, lo que implica que debe contarse con el manifiesto

compromiso de todos los funcionarios de una manera u otra vinculados a la institución, para contribuir a la difusión, consolidación y cumplimiento.

Como consecuencia de lo expuesto, la E.S.E. Hospital Emiro Quintero Cañizares, se ha abocado a la tarea de implementar su propia política de seguridad de la información, basándose en las características establecidas en el Modelo de Política de Seguridad de la Información.

2. TÉRMINOS Y DEFINICIONES

Con el objeto de precisar el alcance de los principales conceptos utilizados en este documento, se transcriben las definiciones que sobre los mismos se han incluido en el Modelo de Política de Seguridad de la Información.

2.1. La seguridad de la información se entiende como la preservación de las siguientes características:

• Confidencialidad: se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.
• Integridad: se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.
• Disponibilidad: se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

Adicionalmente, deberán considerarse los conceptos de:

• Autenticidad: busca asegurar la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.
• Auditabilidad: define que todos los eventos de un sistema deben poder ser registrados para su control posterior.
• Protección a la duplicación: consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.
• No repudio: se refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.
• Legalidad: referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeto el Organismo.
• Confiabilidad de la Información: es decir, que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

2.2. Información: Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.

2.3. Sistema de Información: Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.

2.4. Tecnología de la Información: Se refiere al hardware y software operados por el Organismo o por un tercero que procese información en su nombre, para llevar a cabo una función propia de la E.S.E, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.

2.5. Comité de Seguridad de la Información: El Comité de Seguridad de la Información, es un cuerpo integrado por representantes de todas las áreas sustantivas del Organismo, destinado a garantizar el apoyo manifiesto de las autoridades a las iniciativas de seguridad.

2.6. Responsable de Seguridad Informática: Es la persona que cumple la función de supervisar el cumplimiento de la presente Política y de asesorar en materia de seguridad de la información a los integrantes del Organismo que así lo requieran.

3. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

3.1. Objetivos:
a) Proteger los recursos de información de la E.S.E. y la tecnología utilizada para su procesamiento, frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

b) Asegurar la implementación de las medidas de seguridad comprendidas en esta Política, identificando los recursos y las partidas presupuestarias correspondientes, sin que ello implique necesariamente la asignación de partidas adicionales.

c) Mantener la Política de Seguridad de la Información actualizada, a efectos de asegurar su vigencia y nivel de eficacia.

3.2. Sanciones Previstas por Incumplimiento: El incumplimiento de las disposiciones establecidas por las Políticas de Seguridad de la Información tendrá como resultado la aplicación de diversas sanciones, conforme a la magnitud y característica del aspecto no cumplido.

4. ORGANIZACIÓN DE LA SEGURIDAD
Son sus objetivos:

a) Administrar la seguridad de la información dentro de la E.S.E. y establecer un marco gerencial para iniciar y controlar su implementación, así como para la distribución de funciones y responsabilidades.

b) Fomentar la consulta y cooperación con Organismos especializados para la obtención de asesoría en materia de seguridad de la información.

c) Garantizar la aplicación de medidas de seguridad adecuadas en los accesos de terceros a la información de la E.S.E. Hospital Emiro Quintero Cañizares.

4.1. Infraestructura de la Seguridad de la Información

4.1.1. Comité de Seguridad de la Información: Debe ser integrado por representantes de todas las áreas sustantivas de la E.S.E, destinado a garantizar el apoyo manifiesto de las autoridades a las iniciativas de seguridad.

La E.S.E. Hospital Emiro Quintero Cañizares creó el Comité de Seguridad de la Información CSI mediante la Resolución Nº 0497 del 09 de Mayo de 2014, con los siguientes objetivos:

1) Monitorear cambios significativos en los riesgos que afectan a los recursos de la información de la E.S.E. frente a posibles amenazas, sean internas o externas.

2) Tomar conocimiento y supervisar la investigación y monitoreo de los incidentes, relativos a la seguridad, que se produzcan en el ámbito de la E.S.E.

3) Aprobar las principales iniciativas para incrementar la seguridad de la información, de acuerdo a las competencias y responsabilidades asignadas a cada sector, así como acordar y aprobar metodologías y procesos específicos relativos a la seguridad de la información

4) Evaluar y coordinar la implementación de controles específicos de seguridad se la información para los sistemas o servicios de la E.S.E. Sean preexistentes o nuevos.

5) Promover la difusión y apoyo a la seguridad de la información dentro de la E.S.E. como así, coordinar el proceso de administración de la continuidad de las actividades.

4.1.2. Asignación de Responsabilidades en Materia de Seguridad de la Información: El Gerente de la E.S.E. Hospital Emiro Quintero Cañizares deberá asigna las funciones relativas a la Seguridad Informática, en adelante el "Responsable de Seguridad Informática", quien tendrá a cargo las funciones relativas a la seguridad de los sistemas de información de la E.S.E, lo cual incluye la supervisión de todos los aspectos inherentes a seguridad informática tratados en la presente Política.
El Comité de Seguridad de la Información propondrá a la autoridad que corresponda para su aprobación, la definición y asignación de las responsabilidades que surjan de los procesos de seguridad que se detallan a continuación, indicando en cada caso el/los responsable/s del cumplimiento de los aspectos de esta Política aplicables a cada caso:

a) Seguridad del Personal
b) Seguridad Física y Ambiental
c) Seguridad en las Comunicaciones y las Operaciones

d) Control de Accesos
e) Planificación de la Continuidad Operativa

Así mismo, el Comité de Seguridad de la Información propondrá a la autoridad que corresponda para su aprobación, la definición y asignación de las responsabilidades de los propietarios de la información que se definan, quienes serán los responsables de las unidades organizativas a cargo del manejo de la misma.

Cabe aclarar que, si bien los propietarios pueden delegar la administración de sus funciones a personal idóneo a su cargo, conservarán la responsabilidad del cumplimiento de las mismas. La delegación de la administración por parte de los propietarios de la información será documentada por los mismos y proporcionada al Responsable de Seguridad Informática.

4.1.3. Proceso de Autorización para Instalaciones de Procesamiento de Información: Los nuevos recursos de procesamiento de información serán autorizados por los Responsables de las Unidades Organizativas involucradas, considerando su propósito y uso, conjuntamente con el Responsable de Seguridad Informática, a fin de garantizar que se cumplan todas las Políticas y requerimientos de seguridad pertinentes.

Cuando corresponda, se verificará el hardware y software para garantizar su compatibilidad con los componentes de otros sistemas implementados en la E.S.E.

4.1.4. Asesoramiento Especializado en Materia de Seguridad de la Información: El Responsable de Seguridad Informática será el encargado de coordinar los conocimientos y las experiencias disponibles, a fin de brindar ayuda en la toma de decisiones en materia de seguridad. Éste podrá obtener asesoramiento de otros Organismos.

4.1.5. Revisión Independiente de la Seguridad de la Información
La Unidad de Auditoría Interna o en su defecto quien sea propuesto por el Comité de Seguridad de la Información realizará revisiones independientes sobre la vigencia e implementación de la Política de Seguridad de la Información, a efectos de garantizar que las prácticas del Hospital reflejen adecuadamente sus disposiciones.

4.2. Seguridad Frente al Acceso por Parte de Terceros
4.2.1. Identificación de Riesgos del Acceso de Terceras Partes
Cuando exista la necesidad de otorgar acceso a terceras partes a información de la E.S.E, el Responsable de Seguridad Informática y el Propietario de la Información de que se trate, llevarán a cabo y documentarán una evaluación de riesgos para identificar los requerimientos de controles específicos, teniendo en cuenta, entre otros aspectos:

• El tipo de acceso requerido (físico/lógico y a qué recurso).
• Los motivos para los cuales se solicita el acceso.
• El valor de la información.
• Los controles empleados por la tercera parte.
• La incidencia de este acceso en la seguridad de la información.

En todos los contratos cuyo objeto sea la prestación de servicios a título personal bajo cualquier modalidad jurídica que deban desarrollarse dentro de la E.S.E, se establecerán los controles, requerimientos de seguridad y compromisos de confidencialidad aplicables al caso, restringiendo al mínimo necesario, los permisos a otorgar.

En ningún caso se otorgará acceso a terceros a la información, a las instalaciones de procesamiento u otras áreas de servicios críticos, hasta tanto se hayan implementado los controles apropiados y se haya firmado un contrato o acuerdo que defina las condiciones para la conexión o el acceso.

4.2.2. Requerimientos de Seguridad en Contratos o Acuerdos con Terceros
Se revisarán los contratos o acuerdos existentes o que se efectúen con terceros, teniendo en cuenta la necesidad de aplicar los siguientes controles:

a) Cumplimiento de la Política de seguridad de la información de la E.S.E.
b) Protección de los activos de la E.S.E, incluyendo:
• Procedimientos para proteger los bienes del Hospital, abarcando los activos físicos, la información y el software.
• Procedimientos para determinar si ha ocurrido algún evento que comprometa los bienes, por ejemplo, debido a pérdida o modificación de datos.
• Controles para garantizar la recuperación o destrucción de la información y los activos al finalizar el contrato o acuerdo, o en un momento convenido durante la vigencia del mismo.
• Restricciones a la copia y divulgación de información.
c) Descripción de los servicios disponibles.
d) Nivel de servicio esperado y niveles de servicio aceptables.
e) Permiso para la transferencia de personal cuando sea necesario.
f) Obligaciones de las partes emanadas del acuerdo y responsabilidades legales.
g) Existencia de Derechos de Propiedad Intelectual.
h) Definiciones relacionadas con la protección de datos.
i) Acuerdos de control de accesos que contemplen:
• Métodos de acceso permitidos, y el control y uso de identificadores únicos como identificadores de usuario y contraseñas de usuarios.
• Proceso de autorización de accesos y privilegios de usuarios.
• Requerimiento para mantener actualizada una lista de individuos autorizados a utilizar los servicios que han de implementarse y sus derechos y privilegios con respecto a dicho uso.
j) Definición de criterios de desempeño comprobables, de monitoreo y de presentación de informes.
k) Adquisición de derecho a auditar responsabilidades contractuales o surgidas del acuerdo.
l) Establecimiento de un proceso para la resolución de problemas y en caso de corresponder disposiciones con relación a situaciones de contingencia.
m) Responsabilidades relativas a la instalación y al mantenimiento de hardware y software.
n) Estructura de dependencia y del proceso de elaboración y presentación de informes que contemple un acuerdo con respecto a los formatos de los mismos.
o) Proceso claro y detallado de administración de cambios.

p) Controles de protección física requeridos y los mecanismos que aseguren la implementación de los mismos.
q) Métodos y procedimientos de entrenamiento de usuarios y administradores en materia de seguridad.
r) Controles que garanticen la protección contra software malicioso.
s) Elaboración y presentación de informes, notificación e investigación de incidentes y violaciones relativos a la seguridad.
t) Relación entre proveedores y subcontratistas.

4.3. Tercerización
4.3.1. Requerimientos de Seguridad en Contratos de Tercerización
Los contratos o acuerdos de tercerización total o parcial para la administración y control de sistemas de información, redes y/o ambientes de PC del Hospital, contemplarán además de los puntos especificados en ("Requerimientos de Seguridad en Contratos o Acuerdos con Terceros", los siguientes aspectos:

a) Forma en que se cumplirán los requisitos legales aplicables.
b) Medios para garantizar que todas las partes involucradas en la tercerización, incluyendo los subcontratistas, están al corriente de sus responsabilidades en materia de seguridad.
c) Forma en que se mantendrá y comprobará la integridad y confidencialidad de los activos del Hospital.
d) Controles físicos y lógicos que se utilizarán para restringir y delimitar el acceso a la información sensible del Hospital.
e) Forma en que se mantendrá la disponibilidad de los servicios ante la ocurrencia de desastres.
f) Niveles de seguridad física que se asignarán al equipamiento tercerizado.
g) Derecho a la auditoría por parte del Hospital sobre los aspectos tercerizados en forma directa o a través de la contratación de servicios ad hoc.

Se debe prever la factibilidad de ampliar los requerimientos y procedimientos de seguridad con el acuerdo de las partes.

5. CLASIFICACIÓN Y CONTROL DE ACTIVOS
Son sus objetivos:

a) Garantizar que los activos de información reciban un apropiado nivel de protección.
b) Clasificar la información para señalar su sensibilidad y criticidad.
c) Definir niveles de protección y medidas de tratamiento especial acordes a su clasificación.

Esta Política se aplica a toda la información administrada en el Hospital, cualquiera sea el soporte en que se encuentre.

Los propietarios de la información son los encargados de clasificarla de acuerdo con su grado de sensibilidad y criticidad, de documentar y mantener actualizada la clasificación efectuada, y de definir las funciones que deberán tener permisos de acceso a la información.

El Responsable de Seguridad Informática es el encargado de asegurar que los lineamientos para la utilización de los recursos de la tecnología de información contemplen los requerimientos de seguridad establecidos según la criticidad de la información que procesan.

Cada Propietario de la Información supervisará que el proceso de clasificación y rótulo de información de su área de competencia sea cumplimentado de acuerdo a lo establecido en la presente Política.

5.1. Inventario de activos
Se identificarán los activos importantes asociados a cada sistema de información, sus respectivos propietarios y su ubicación, para luego elaborar un inventario con dicha información.

El mismo será actualizado ante cualquier modificación de la información registrada y revisado con una periodicidad no mayor a 6 meses.

El encargado de elaborar el inventario y mantenerlo actualizado es cada Responsable de Unidad Organizativa.

5.2. Clasificación de la información
Para clasificar un Activo de Información, se evaluarán las tres características de la información en las cuales se basa la seguridad:

a) confidencialidad,
b) integridad,
c) disponibilidad.

5.3. Rotulado de la Información
Se definirán procedimientos para el rotulado y manejo de información, de acuerdo al esquema de clasificación definido. Los mismos contemplarán los recursos de información tanto en formatos físicos como electrónicos e incorporarán las siguientes actividades de procesamiento de la información:

-Copia;
-Almacenamiento;
-Transmisión por correo, fax, correo electrónico;
-Transmisión oral (telefonía fija y móvil, correo de voz, contestadores automáticos, etc.).

6. SEGURIDAD DEL PERSONAL
Son sus objetivos:

a) Reducir los riesgos de error humano, comisión de ilícitos, uso inadecuado de instalaciones y recursos, y manejo no autorizado de la información.

b) Explicitar las responsabilidades en materia de seguridad en la etapa de reclutamiento de personal e incluirlas en los acuerdos a firmarse y verificar su cumplimiento durante el desempeño del individuo como empleado.

c) Garantizar que los usuarios estén al corriente de las amenazas e incumbencias en materia de seguridad de la información, y se encuentren capacitados para respaldar la Política de Seguridad de la ESE en el transcurso de sus tareas normales.

d) Establecer Compromisos de Confidencialidad con todo el personal y usuarios externos de las instalaciones de procesamiento de información.

e) Establecer las herramientas y mecanismos necesarios para promover la comunicación de debilidades existentes en materia de seguridad, así como de los incidentes ocurridos, con el objeto de minimizar sus efectos y prevenir su reincidencia.

Esta Política se aplica a todo el personal de la ESE, cualquiera sea su situación de inspección, y al personal externo que efectúe tareas dentro del ámbito del Hospital.

El Responsable del Área de Recursos Humanos incluirá las funciones relativas a la seguridad de la información en las descripciones de puestos de los empleados, informará a todo el personal que ingresa de sus obligaciones respecto del cumplimiento de la Política de Seguridad de la Información, gestionará los Compromisos de Confidencialidad con el personal y coordinará las tareas de capacitación de usuarios respecto de la presente Política.

El Responsable de Seguridad Informática tiene a cargo el seguimiento, documentación y análisis de los incidentes de seguridad reportados así como su comunicación al Comité de Seguridad de la Información, a los propietarios de la información y a la Coordinación de Emergencias en Redes.

El Comité de Seguridad de la Información será responsable de implementar los medios y canales necesarios para que el Responsable de Seguridad Informática maneje los reportes de incidentes y anomalías de los sistemas. Asimismo, dicho Comité, tomará conocimiento, efectuará el seguimiento de la investigación, controlará la evolución e impulsará la resolución de los incidentes relativos a la seguridad.

El Responsable del Área Legal participará en la confección del Compromiso de Confidencialidad a firmar por los empleados y terceros que desarrollen funciones en el organismo, en el asesoramiento sobre las sanciones a ser aplicadas por incumplimiento de la presente Política y en el tratamiento de incidentes de seguridad que requieran de su intervención.

Todo el personal del Hospital es responsable del reporte de debilidades e incidentes de seguridad que oportunamente se detecten.

6.1. Seguridad en la Definición de Puestos de Trabajo y la Asignación de Recursos

6.1.1. Incorporación de la Seguridad en los Puestos de Trabajo
Las funciones y responsabilidades en materia de seguridad serán incorporadas en la descripción de las responsabilidades de los puestos de trabajo. Estas incluirán las responsabilidades generales relacionadas con la implementación y el mantenimiento de las Políticas de Seguridad, y las responsabilidades específicas vinculadas a la protección de cada uno de los activos, o la ejecución de procesos o actividades de seguridad determinadas.

6.1.2. Control y Política del Personal
Se llevarán a cabo controles de verificación del personal en el momento en que se solicita el puesto. Estos controles incluirán todos los aspectos que indiquen las normas que a tal efecto, alcanzan a la ESE.

6.1.3. Compromiso de Confidencialidad
Como parte de sus términos y condiciones iniciales de empleo, los empleados, cualquiera sea su situación laboral, firmarán un Compromiso de Confidencialidad o no divulgación, en lo que respecta al tratamiento de la información de la ESE. La copia firmada del Compromiso deberá ser retenida en forma segura por el Área de Recursos Humanos u otra competente. Asimismo, mediante el Compromiso de Confidencialidad el empleado declarará conocer y aceptar la existencia de determinadas actividades que pueden ser objeto de control y monitoreo. Estas actividades deben ser detalladas a fin de no violar el derecho a la privacidad del empleado.

6.1.4. Términos y Condiciones de Empleo
Los términos y condiciones de empleo establecerán la responsabilidad del empleado en materia de seguridad de la información. Cuando corresponda, los términos y condiciones de empleo establecerán que estas responsabilidades se extienden más allá de los límites de la sede del Organismo y del horario normal de trabajo.

Los derechos y obligaciones del empleado relativos a la seguridad de la información, por ejemplo en relación con las leyes de Propiedad Intelectual o la legislación de protección de datos, se encontrarán aclarados e incluidos en los términos y condiciones de empleo.

6.2. Capacitación del Usuario
6.2.1. Formación y Capacitación en Materia de Seguridad de la Información Todos los empleados de la institución y, cuando sea pertinente, los usuarios externos y los terceros que desempeñen funciones en la ESE, recibirán una adecuada capacitación y actualización periódica en materia de la política, normas y procedimientos del Hospital. Esto comprende los requerimientos de seguridad y las responsabilidades legales, así como la capacitación referida al uso correcto de las instalaciones de procesamiento de información y el uso correcto de los recursos en general, como por ejemplo su estación de trabajo.

6.3. Respuesta a Incidentes y Anomalías en Materia de Seguridad
6.3.1. Comunicación de Incidentes Relativos a la Seguridad
Los incidentes relativos a la seguridad serán comunicados a través de canales apropiados tan pronto como sea posible. Se establecerá un procedimiento formal de comunicación y de

respuesta a incidentes, indicando la acción que ha de emprenderse al recibir un informe sobre incidentes. Dicho procedimiento deberá contemplar que ante la detección de un supuesto incidente o violación de la seguridad, el Responsable de Seguridad Informática sea informado tan pronto como se haya tomado conocimiento. Este indicará los recursos necesarios para la investigación y resolución del incidente, y se encargará de su monitoreo. Asimismo, mantendrá al Comité de Seguridad al tanto de la ocurrencia de incidentes de seguridad.

6.3.2. Comunicación de Debilidades en Materia de Seguridad
Los usuarios de servicios de información, al momento de tomar conocimiento directo o indirectamente acerca de una debilidad de seguridad, son responsables de registrar y comunicar las mismas al Responsable de Seguridad Informática.

6.3.3. Comunicación de Anomalías del Software
Se establecerán procedimientos para la comunicación de anomalías de software, los cuales deberán contemplar:

a) Registrar los síntomas del problema y los mensajes que aparecen en pantalla.
b) Establecer las medidas de aplicación inmediata ante la presencia de una anomalía.
c) Alertar inmediatamente al Responsable de Seguridad Informática o del Activo de que se trate.

La recuperación será realizada por personal experimentado, adecuadamente habilitado.

6.3.4. Aprendiendo de los Incidentes
Se definirá un proceso que permita documentar, cuantificar y monitorear los tipos, volúmenes y costos de los incidentes y anomalías. Esta información se utilizará para identificar aquellos que sean recurrentes o de alto impacto. Esto será evaluado a efectos de establecer la necesidad de mejorar o agregar controles para limitar la frecuencia, daño y costo de casos futuros.

7. SEGURIDAD FÍSICA Y AMBIENTAL
Son sus objetivos:

a) Prevenir e impedir accesos no autorizados, daños e interferencia a las sedes, instalaciones e información de la ESE.
b) Proteger el equipamiento de procesamiento de información crítica de la ESE, ubicándolo en áreas protegidas y resguardadas por un perímetro de seguridad definido, con medidas de seguridad y controles de acceso apropiados. Asimismo, contemplar la protección del mismo en su traslado y permanencia fuera de las áreas protegidas, por motivos de mantenimiento u otros.
c) Controlar los factores ambientales que podrían perjudicar el correcto funcionamiento del equipamiento informático que alberga la información del Hospital.
d) Implementar medidas para proteger la información manejada por el personal en las oficinas, en el marco normal de sus labores habituales.
e) Proporcionar protección proporcional a los riesgos identificados.

Esta Política se aplica a todos los recursos físicos relativos a los sistemas de información de la ESE: instalaciones, equipamiento, cableado, expedientes, medios de almacenamiento, etc.

El Responsable de Seguridad Informática definirá junto con el Responsable del Área Informática y los Propietarios de Información, según corresponda, las medidas de seguridad física y ambiental para el resguardo de los activos críticos, en función a un análisis de riesgos, y controlará su implementación. Asimismo, verificará el cumplimiento de las disposiciones sobre seguridad física y ambiental indicadas en el presente Capítulo.

El Responsable del Área Informática asistirá al Responsable de Seguridad Informática en la definición de las medidas de seguridad a implementar en áreas protegidas, y coordinará su implementación. Asimismo, controlará el mantenimiento del equipamiento informático de acuerdo a las indicaciones de proveedores tanto dentro como fuera de las instalaciones de la ESE.

Los Responsables de Unidades Organizativas definirán los niveles de acceso físico del personal del organismo a las áreas restringidas bajo su responsabilidad. Los Propietarios de la Información autorizarán formalmente el trabajo fuera de las instalaciones con información de su incumbencia a los empleados de la ESE cuando lo crean conveniente.

Todo el personal de la ESE es responsable del cumplimiento de la política de pantallas y escritorios limpios, para la protección de la información relativa al trabajo diario en las oficinas.

7.1. Perímetro de Seguridad Física

La protección física se llevará a cabo mediante la creación de diversas barreras o medidas de control físicas alrededor de las sedes del Hospital y de las instalaciones de procesamiento de información.

El Hospital utilizará perímetros de seguridad para proteger las áreas que contienen instalaciones de procesamiento de información, de suministro de energía eléctrica, de aire acondicionado, y cualquier otra área considerada crítica para el correcto funcionamiento de los sistemas de información. Un perímetro de seguridad está delimitado por una barrera, por ejemplo una pared, una puerta de acceso controlado por dispositivo de autenticación o un escritorio u oficina de recepción atendidos por personas. El emplazamiento y la fortaleza de cada barrera estarán definidas por el Responsable del Área Informática con el asesoramiento del Responsable de Seguridad Informática, de acuerdo a la evaluación de riesgos efectuada.

7.2. Controles de Acceso Físico

Las áreas protegidas se resguardarán mediante el empleo de controles de acceso físico, los que serán determinados por el Responsable de Seguridad Informática junto con el responsable del Área Informática, a fin de permitir el acceso sólo al personal autorizado.

7.3. Protección de Oficinas, Recintos e Instalaciones

Para la selección y el diseño de un área protegida se tendrá en cuenta la posibilidad de daño producido por incendio, inundación, explosión, agitación civil, y otras formas de desastres naturales o provocados por el hombre. También se tomarán en cuenta las disposiciones y normas (estándares) en materia de sanidad y seguridad. Asimismo, se considerarán las amenazas a la seguridad que representan los edificios y zonas aledañas.

7.4. Desarrollo de Tareas en Áreas Protegidas
Para incrementar la seguridad de las áreas protegidas, se establecerán controles y lineamientos adicionales, que incluyan controles para el personal que trabaja en el área protegida, así como para las actividades de terceros que tengan lugar allí.

7.5. Aislamiento de las Áreas de Recepción y Distribución
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.

7.6. Ubicación y Protección del Equipamiento y Copias de Seguridad
El equipamiento será ubicado y protegido de tal manera que se reduzcan los riesgos ocasionados por amenazas y peligros ambientales, y las oportunidades de acceso no autorizado,

7.7. Suministros de Energía
El equipamiento estará protegido con respecto a las posibles fallas en el suministro de energía otras anomalías eléctricas. El suministro de energía estará de acuerdo con las especificaciones del fabricante o proveedor de cada equipo.

7.8. Seguridad del Cableado
El cableado de energía eléctrica y de comunicaciones que transporta datos o brinda apoyo a los servicios de información estará protegido contra intercepción o daño.

7.9. Mantenimiento de Equipos
Se realizará el mantenimiento del equipamiento para asegurar su disponibilidad e integridad permanentes, teniendo en cuenta a tal efecto:

a) la realización de tareas de mantenimiento preventivo al equipamiento, de acuerdo con los intervalos de servicio y especificaciones recomendados por el proveedor y con la autorización formal del Responsables del Área Informática.

b) el establecimiento de la práctica de que sólo el personal de mantenimiento autorizado puede brindar mantenimiento y llevar a cabo reparaciones en el equipamiento.
c) la registración de todas las fallas -supuestas y/o reales- y de todo el mantenimiento preventivo y correctivo realizado.

d) la registración del retiro de equipamiento para su mantenimiento de la sede de la ESE.

e) la eliminación de toda información confidencial que contenga cualquier equipamiento que sea necesario retirar, realizándose previamente las respectivas copias de resguardo.

7.10. Seguridad de los Equipos Fuera de las Instalaciones
El uso de equipamiento destinado al procesamiento de información, fuera del ámbito de la ESE será autorizado por el responsable patrimonial. En el caso de que en el mismo se almacene información clasificada, deberá ser aprobado además por el Propietario de la misma. La seguridad provista debe ser equivalente a la suministrada dentro del ámbito de la ESE para un propósito similar, teniendo en cuenta los riesgos de trabajar fuera de la misma.

7.11. Desafectación o Reutilización Segura de los Equipos
La información puede verse comprometida por una desafectación o una reutilización descuidada del equipamiento. Los medios de almacenamiento conteniendo material sensible, por ejemplo discos rígidos no removibles, serán físicamente destruidos o sobrescritos en forma segura en lugar de utilizar las funciones de borrado estándar, según corresponda.

7.12. Políticas de Escritorios y Pantallas Limpias
Se adopta una política de escritorios limpios para proteger documentos en papel y dispositivos de almacenamiento removibles y una política de pantallas limpias en las instalaciones de procesamiento de información, a fin de reducir los riesgos de acceso no autorizado, pérdida y daño de la información, tanto durante el horario normal de trabajo como fuera del mismo.

7.13. Retiro de los Bienes
El equipamiento, la información y el software no serán retirados de la sede del Hospital sin autorización formal. Periódicamente, se llevarán a cabo comprobaciones puntuales para detectar el retiro no autorizado de activos de la institución.

8. GESTIÓN DE COMUNICACIONES Y OPERACIONES
Son sus objetivos:

a) Garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información y comunicaciones.

b) Establecer responsabilidades y procedimientos para su gestión y operación, incluyendo instrucciones operativas, procedimientos para la respuesta a incidentes y separación de funciones.

Cada Propietario de la Información, junto con el Responsable de Seguridad Informática y el Responsable del Área Informática, determinará los requerimientos para resguardar la información por la cual es responsable. Asimismo, aprobará los servicios de mensajería autorizados para transportar la información cuando sea requerido, de acuerdo a su nivel de criticidad.

8.1. Procedimientos y Responsabilidades Operativas

8.1.1. Documentación de los Procedimientos Operativos

Se documentarán y mantendrán actualizados los procedimientos operativos identificados en esta Política y sus cambios serán autorizados por el Responsable de Seguridad Informática.

8.1.2. Control de Cambios en las Operaciones

Se definirán procedimientos para el control de los cambios en el ambiente operativo y de comunicaciones. Todo cambio deberá ser evaluado previamente en aspectos técnicos y de seguridad.

El Responsable de Seguridad Informática controlará que los cambios en los componentes operativos y de comunicaciones no afecten la seguridad de los mismos ni de la información que soportan. El Responsable del Área Informática evaluará el posible impacto operativo de los cambios previstos y verificará su correcta implementación.

8.1.3. Procedimientos de Manejo de Incidentes

Se establecerán funciones y procedimientos de manejo de incidentes garantizando una respuesta rápida, eficaz y sistemática a los incidentes relativos a seguridad.

8.1.4. Separación de Funciones

Se contemplará la separación de la gestión o ejecución de tareas o áreas de responsabilidad, en la medida de que la misma reduzca el riesgo de modificaciones no autorizadas o mal uso de la información o los servicios por falta de independencia en la ejecución de funciones críticas.

En los casos en los que este método de control no se pudiera cumplirse, se implementarán controles tales como el monitoreo de las actividades y/o la elaboración de registros de auditoría y control periódico de los mismos.

8.1.5. Separación entre Instalaciones de Desarrollo e Instalaciones Operativas

Los ambientes de desarrollo, prueba y operaciones, siempre que sea posible, estarán separados preferentemente en forma física, y se definirán y documentarán las reglas para la transferencia de software desde el estado de desarrollo hacia el estado operativo.

8.1.6. Gestión de Instalaciones Externas

En el caso de tercerizar la administración de las instalaciones de procesamiento, se acordarán controles con el proveedor del servicio que se incluirán en el contrato de tercerización.

8.2. Planificación y Aprobación de Sistemas

8.2.1. Planificación de la Capacidad

El Responsable del Área Informática, o el personal que éste designe, efectuará el monitoreo de las necesidades de capacidad de los sistemas en operación y proyectar las futuras demandas, a fin de garantizar un procesamiento y almacenamiento adecuados.

Asimismo, informará las necesidades detectadas a las autoridades competentes para que puedan identificar y evitar potenciales cuellos de botella, que podrían plantear una amenaza a la seguridad o a la continuidad del procesamiento, y puedan planificar una adecuada acción correctiva.

8.2.2. Aprobación del Sistema
El Responsable del Área Informática y el Responsable de Seguridad Informática sugerirán criterios de aprobación para nuevos sistemas de información, actualizaciones y nuevas versiones, solicitando la realización de las pruebas necesarias antes de su aprobación definitiva.

8.3. Protección Contra Software Malicioso
8.3.1. Controles Contra Software Malicioso
El Responsable de Seguridad Informática definirá controles de detección y prevención para la protección contra software malicioso. El Responsable del Área Informática, o el personal designado por éste, implementarán dichos controles.

El Responsable de Seguridad Informática desarrollará procedimientos adecuados de concientización de usuarios en materia de seguridad, controles de acceso al sistema y administración de cambios.

8.4. Mantenimiento
8.4.1. Resguardo de la Información
El Responsable del Área Informática y el de Seguridad Informática junto al Propietarios de Información determinarán los requerimientos para resguardar cada software o dato en función de su criticidad.

En base a ello, se definirá y documentará un esquema de resguardo de la información.

8.4.2. Registro de Actividades del Personal Operativo
El Responsable del Área Informática asegurará el registro de las actividades realizadas en los sistemas, incluyendo según corresponda:

a) Tiempos de inicio y cierre del sistema.
b) Errores del sistema y medidas correctivas tomadas.
c) Intentos de acceso a sistemas, recursos o información crítica o acciones restringidas
d) Ejecución de operaciones críticas
e) Cambios a información crítica

8.4.3. Registro de Fallas

El Responsable del Área Informática desarrollará y verificará el cumplimiento de procedimientos para comunicar las fallas en el procesamiento de la información o los sistemas de comunicaciones, que permita tomar medidas correctivas.

8.5. Administración de la Red

8.5.1. Controles de Redes

El Responsable de Seguridad Informática definirá controles para garantizar la seguridad de los datos y los servicios conectados en las redes del Organismo, contra el acceso no autorizado. El Responsable del Área Informática implementará dichos controles.

8.6. Administración y Seguridad de los Medios de Almacenamiento

8.6.1. Administración de Medios Informáticos Removibles

El Responsable del Área Informática, con la asistencia del Responsable de Seguridad Informática, implementará procedimientos para la administración de medios informáticos removibles, como USB´s, discos e informes impresos.

8.6.2. Eliminación de Medios de Información

El Responsable del Área Informática, junto con el Responsable de Seguridad Informática definirá procedimientos para la eliminación segura de los medios de información respetando la normativa vigente.

8.6.3. Procedimientos de Manejo de la Información

Se definirán procedimientos para el manejo y almacenamiento de la información de acuerdo a lo establecido en el capítulo 5 “Clasificación y Control de Activos”.

8.6.4. Seguridad de la Documentación del Sistema

La documentación del sistema puede contener información sensible, por lo que se considerarán los recaudos para su protección, almacenar la documentación del sistema en forma segura y restringir el acceso a la documentación del sistema al personal estrictamente necesario. Dicho acceso será autorizado por el Propietario de la Información relativa al sistema.

8.7. Intercambios de Información y Software

8.7.1. Acuerdos de Intercambio de Información y Software

Cuando se realicen acuerdos entre organizaciones para el intercambio de información y software, se especificará el grado de sensibilidad de la información del Hospital y las consideraciones de seguridad sobre la misma.

8.7.2. Seguridad de los Medios en Tránsito

Los procedimientos de transporte de medios informáticos entre diferentes puntos (mensajería) deberán contemplar la utilización de medios de transporte o servicios de mensajería confiable, suficiente embalaje para el envío y la adopción de controles especiales, cuando resulte necesario, a fin de proteger la información sensible contra divulgación o modificación no autorizadas.

8.7.3. Seguridad del Correo Electrónico

8.7.3.1. Riesgos de Seguridad
Se implementarán controles para reducir los riesgos de incidentes de seguridad en el correo electrónico, contemplando:

a) La vulnerabilidad de los mensajes al acceso o modificación no autorizados o a la negación de servicio.
b) La posible intercepción y el consecuente acceso a los mensajes en los medios de transferencia que intervienen en la distribución de los mismos.
c) Las posibles vulnerabilidades a errores, por ejemplo, consignación incorrecta de la dirección o dirección errónea, y la confiabilidad y disponibilidad general del servicio.
d) La posible recepción de código malicioso en un mensaje de correo, el cual afecte la seguridad de la terminal receptora o de la red a la que se encuentra conectada.
e) El impacto de un cambio en el medio de comunicación en los procesos del Organismo.
f) Las consideraciones legales, como la necesidad potencial de contar con prueba de origen, envío, entrega y aceptación.
g) Las implicancias de la publicación externa de listados de personal, accesibles al público.
h) El acceso de usuarios remotos a las cuentas de correo electrónico.
i) El uso inadecuado por parte del personal.

8.7.3.2. Política de Correo Electrónico
El Responsable de Seguridad Informática junto con el Responsable del Área Informática definirán y documentarán normas y procedimientos claros con respecto al uso del correo electrónico, que incluya al menos los siguientes aspectos:

a) Protección contra ataques al correo electrónico, por ejemplo virus, intercepción, etc.
b) Protección de archivos adjuntos de correo electrónico.
c) Uso de técnicas criptográficas para proteger la confidencialidad e integridad de los mensajes electrónicos (Ver 10.3. Controles Criptográficos).
d) Retención de mensajes que, si se almacenaran, pudieran ser usados en caso de litigio.
e) Controles adicionales para examinar mensajes electrónicos que no pueden ser autenticados.
f) Aspectos operativos para garantizar el correcto funcionamiento del servicio (ej.: tamaño máximo de información transmitida y recibida, cantidad de destinatarios, tamaño máximo del buzón del usuario, etc.).
g) Definición de los alcances del uso del correo electrónico por parte del personal del Hospital.

8.7.4. Seguridad de los Sistemas Electrónicos de Oficina
Se controlarán los mecanismos de distribución y difusión tales como documentos, computadoras, computación móvil, comunicaciones móviles, correo, correo de voz, comunicaciones de voz en general, multimedia, equipos de fax, etc.

8.7.5. Sistemas de Acceso Público

Se tomarán recaudos para la protección de la integridad de la información publicada electrónicamente, a fin de prevenir la modificación no autorizada.

8.7.6. Otras Formas de Intercambio de Información
Se implementarán normas, procedimientos y controles para proteger el intercambio de información a través de medios de comunicaciones de voz, fax y vídeo.

9. CONTROL DE ACCESOS
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.

9.1. Requerimientos para el Control de Acceso
9.1.1. Política de Control de Accesos
9.1.2. Reglas de Control de Acceso
9.2. Administración de Accesos de Usuarios
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.

9.2.1. Registración de Usuarios
El Responsable de Seguridad Informática 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.

9.2.2. Administración 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.

9.2.3. Administración de Contraseñas de Usuario
La asignación de contraseñas se controlará a través de un proceso de administración formal.

9.2.4. Administración de Contraseñas Críticas
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 Informática definirá procedimientos para la administración de dichas contraseñas críticas.

9.2.5. 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 no más a 6 meses, a fin de revisar los derechos de acceso de los usuarios.

9.3. Responsabilidades del Usuario

9.3.1. 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 directivas que se impartan a tal efecto.

9.3.2. Equipos Desatendidos en Áreas de Usuarios
Los usuarios deberán 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 Informática 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.

9.4. Control de Acceso a la Red

9.4.1. Política de Utilización de los Servicios de Red
Se controlará el acceso a los servicios de red tanto internos como externos. 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.

9.4.2. Camino Forzado

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.

9.4.3. Autenticación de Usuarios para Conexiones Externas
El Responsable de Seguridad Informática, 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.

9.4.4. Autenticación de Nodos
Una herramienta de conexión automática a una computadora remota podría brindar un medio para obtener acceso no autorizado a una aplicación. Por consiguiente, las conexiones a sistemas informáticos remotos serán autenticadas.

9.4.5. Protección de los Puertos (Ports) de Diagnóstico Remoto
Los puertos de diagnóstico proporcionan un medio de acceso no autorizado. Por consiguiente, serán protegidos por un mecanismo de seguridad apropiado

9.4.6. Subdivisión de Redes
Se definirán y documentarán los perímetros de seguridad que sean convenientes, que 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.

9.4.7. 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 Informática 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.

9.4.8. Control de Conexión a la Red
Se podrán implementar controles para limitar la capacidad de conexión de los usuarios, de acuerdo a las políticas que se establecen a tal efecto. Dichos controles se podrán implementar en los "gateways" que separan los diferentes dominios de la red.

9.4.9. Control de Ruteo de Red
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.

9.4.10. Seguridad de los Servicios de Red

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

9.5. Control de Acceso al Sistema Operativo

9.5.1. Identificación Automática de Terminales

El Responsable de Seguridad Informática junto con el Responsable del Área Informática realizará una evaluación de riesgos a fin de determinar el método de protección adecuado para el acceso al Sistema Operativo.

9.5.2. 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.

9.5.3. 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. Los identificadores de usuario no darán ningún indicio del nivel de privilegio otorgado.

9.5.4. Sistema de Administración de Contraseñas

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 “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 “Uso de Contraseñas”.

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

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

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

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

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

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

k) 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.

9.5.5. Uso de Utilidades del Sistema
Existen programas de utilidades que podrían tener la capacidad de pasar por alto los controles de sistemas y aplicaciones. Su uso será limitado y minuciosamente controlado.

9.5.6. Limitación del Horario de Conexión
Se implementará un control de esta índole para aplicaciones informáticas sensibles, especialmente aquellas terminales instaladas en ubicaciones de alto riesgo.

9.6. Control de Acceso a las Aplicaciones

9.6.1. 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 de la ESE HEQC para el acceso a la información

9.6.2. Aislamiento de los Sistemas Sensibles
Los sistemas sensibles podrían requerir de un ambiente informático dedicado (aislado). 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.

9.7. Monitoreo del Acceso y Uso de los Sistemas

9.7.1. Registro de Eventos
Se generarán registros de auditoría que contengan excepciones y otros eventos relativos a la seguridad. Los registros de auditoría deberán incluir la identificación del usuario, la fecha y hora de inicio y terminación, la identidad o ubicación de la terminal, un registro de intentos exitosos y fallidos de acceso al sistema y un registro de intentos exitosos y fallidos de acceso a datos y otros recursos.

9.7.2. Monitoreo del Uso de los Sistemas
9.7.2.1. 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.

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

9.7.2.3. 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 Informática, de acuerdo a la evaluación de riesgos efectuada.

9.7.3. Sincronización de Relojes
A fin de garantizar la exactitud de los registros de auditoría, al menos los equipos que realicen estos registros, deberán tener una correcta configuración de sus relojes. Para ello, se dispondrá de un procedimiento de ajuste de relojes, el cual indicará también la verificación de los relojes contra una fuente externa del dato y la modalidad de corrección ante cualquier variación significativa.

9.8. Computación Móvil y Trabajo Remoto

9.8.1. Computación Móvil
Se desarrollarán procedimientos adecuados para estos dispositivos, que abarquen la protección física necesaria, el acceso seguro a los dispositivos, la utilización de los dispositivos en lugares públicos. El acceso a los sistemas de información y servicios del Organismo a través de dichos dispositivos, las técnicas criptográficas a utilizar para la transmisión de información clasificada, los mecanismos de resguardo de la información contenida en los dispositivos y la protección contra software malicioso.

9.8.2. Trabajo Remoto
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 Informática, 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.

10. ADMINISTRACIÓN DE LA CONTINUIDAD DE LAS ACTIVIDADES DEL ORGANISMO

Son sus objetivos:

a) Minimizar los efectos de las posibles interrupciones de las actividades normales de la ESE HEQC (sean éstas resultado de desastres naturales, accidentes, fallas en el equipamiento, acciones deliberadas u otros hechos) y proteger los procesos críticos mediante una combinación de controles preventivos y acciones de recuperación.
b) Analizar las consecuencias de la interrupción del servicio y tomar las medidas correspondientes para la prevención de hechos similares en el futuro.
c) Maximizar la efectividad de las operaciones de contingencia del Organismo con el establecimiento de planes que incluyan al menos las siguientes etapas:

1) Notificación / Activación: Consistente en la detección y determinación del daño y la activación del plan.
2) Reanudación: Consistente en la restauración temporal de las operaciones y recuperación del daño producido al sistema original.
3) Recuperación: Consistente en la restauración de las capacidades de proceso del sistema a las condiciones de operación normales.
d) Asegurar la coordinación con el personal del Organismo y los contactos externos que participarán en las estrategias de planificación de contingencias. Asignar funciones para cada actividad definida.

El Responsable de Seguridad Informática participará activamente en la definición, documentación, prueba y actualización de los planes de contingencia. Los Propietarios de la Información y el Responsable de Seguridad Informática cumplirán las siguientes funciones:

-Identificar las amenazas que puedan ocasionar interrupciones de los procesos y/o las actividades del Organismo.
-Evaluar los riesgos para determinar el impacto de dichas interrupciones.
-Identificar los controles preventivos.
- Desarrollar un plan estratégico para determinar el enfoque global con el que se abordará la continuidad de las actividades del Organismo.
-Elaborar los planes de contingencia necesarios para garantizar la continuidad de las actividades del Organismo.

10.1. Proceso de la Administración de la Continuidad del Organismo
El Comité de Seguridad de la Información, será el responsable de la coordinación del desarrollo de los procesos que garanticen la continuidad de las actividades del Organismo.

10.2. Continuidad de las Actividades y Análisis de los Impactos
Se establece la necesidad de contar con un Plan de Continuidad de las Actividades de la ESE HEQC que contemple los siguientes puntos:

• Identificar los eventos (amenazas) que puedan ocasionar interrupciones en los procesos de las actividades.
• Evaluar los riesgos para determinar el impacto de dichas interrupciones, tanto en términos de magnitud de daño como del período de recuperación.
• Identificar los controles preventivos. Esta actividad será llevada a cabo con la activa participación de los propietarios de los procesos y recursos de información de que se trate y el Responsable de Seguridad Informática, considerando todos los procesos de las actividades de la ESE HEQC y no limitándose a las instalaciones de procesamiento de la información.

10.3. Elaboración e Implementación de los Planes de Continuidad de las Actividades del Organismo
Los propietarios de procesos y recursos de información, con la asistencia del Responsable de Seguridad Informática, elaborarán los planes de contingencia necesarios para garantizar la

continuidad de las actividades de la ESE HEQC. Estos procesos deberán ser propuestos por el Comité de Seguridad de la Información

10.4. Marco para la Planificación de la Continuidad de las Actividades del Organismo
Se mantendrá un solo marco para los planes de continuidad de las actividades del Organismo, a fin de garantizar que los mismos sean uniformes e identificar prioridades de prueba y mantenimiento.
Cada plan de continuidad especificará claramente las condiciones para su puesta en marcha, así como las personas a cargo de ejecutar cada componente del mismo. Cuando se identifiquen nuevos requerimientos, se modificarán los procedimientos de emergencia establecidos, por ejemplo, los planes de evacuación o los recursos de emergencia existentes.

10.5. Ensayo, Mantenimiento y Reevaluación de los Planes de Continuidad del Organismo

El Comité de Seguridad de la Información establecerá un cronograma de pruebas periódicas de cada uno de los planes de contingencia.

11. CUMPLIMIENTO

Son sus objetivos:

a) Cumplir con las disposiciones normativas y contractuales a fin de evitar sanciones administrativas a la ESE HEQC y/o al empleado o que incurran en responsabilidad civil o penal como resultado de su incumplimiento.
b) Garantizar que los sistemas cumplan con la política, normas y procedimientos de seguridad de la ESE HEQC.
c) Revisar la seguridad de los sistemas de información periódicamente a efectos de garantizar la adecuada aplicación de la política, normas y procedimientos de seguridad, sobre las plataformas tecnológicas y los sistemas de información.
d) Optimizar la eficacia del proceso de auditoría de sistemas y minimizar los problemas que pudiera ocasionar el mismo, o los obstáculos que pudieran afectarlo.
e) Garantizar la existencia de controles que protejan los sistemas en producción y las herramientas de auditoría en el transcurso de las auditorías de sistemas.
f) Determinar los plazos para el mantenimiento de información y para la recolección de evidencia de la ESE HEQC.

11.1. Cumplimiento de Requisitos Legales
11.1.1. Identificación de la Legislación Aplicable
Se definirán y documentarán claramente todos los requisitos normativos y contractuales pertinentes para cada sistema de información. Del mismo modo se definirán y documentarán los controles específicos y las responsabilidades y funciones individuales para cumplir con dichos requisitos.

11.1.2. Derechos de Propiedad Intelectual

Se implementarán procedimientos adecuados para garantizar el cumplimiento de las restricciones legales al uso del material protegido por normas de propiedad intelectual.

11.1.2.1. Derecho de Propiedad Intelectual del Software
El Responsable de Seguridad Informática, con la asistencia del Área Legal, analizará los términos y condiciones de la licencia, e implementará los siguientes controles:

a) Definir normas y procedimientos para el cumplimiento del derecho de propiedad intelectual de software que defina el uso legal de productos de información y de software.
b) Divulgar las políticas de adquisición de software y las disposiciones de la Ley de Propiedad Intelectual, y notificar la determinación de tomar acciones disciplinarias contra el personal que las infrinja.
c) Mantener un adecuado registro de activos.
d) Conservar pruebas y evidencias de propiedad de licencias, discos maestros, manuales, etc.
e) Implementar controles para evitar el exceso del número máximo permitido de usuarios.
f) Verificar que sólo se instalen productos con licencia y software autorizado.
g) Elaborar y divulgar un procedimiento para el mantenimiento de condiciones adecuadas con respecto a las licencias.
h) Elaborar y divulgar un procedimiento relativo a la eliminación o transferencia de software a terceros.
i) Utilizar herramientas de auditoría adecuadas.
j) Cumplir con los términos y condiciones establecidos para obtener software e información en redes públicas.

11.1.3. Protección de los Registros de la ESE Hospital Emiro Quintero Cañizares
Los registros críticos del Organismo se protegerán contra pérdida, destrucción y falsificación. Algunos registros pueden requerir una retención segura para cumplir requisitos legales o normativos, así como para respaldar actividades esenciales de la ESE HEQC.

11.1.4. Protección de Datos y Privacidad de la Información Personal
Todos los empleados deberán conocer las restricciones al tratamiento de los datos y de la información respecto a la cual tengan conocimiento con motivo del ejercicio de sus funciones. La ESE HEQC redactará un “Compromiso de Confidencialidad”, el cual deberá ser suscrito por todos los empleados. La copia firmada del compromiso será retenida en forma segura por la ESE HEQC.

11.1.5. Prevención del Uso Inadecuado de los Recursos de Procesamiento de Información
Los recursos de procesamiento de información del Organismo se suministran con un propósito determinado. Toda utilización de estos recursos con propósitos no autorizados o ajenos al destino por el cual fueron provistos debe ser considerada como uso indebido. Todos los empleados deben conocer el alcance preciso del uso adecuado de los recursos informáticos y deben respetarlo.

11.1.6. Recolección de Evidencia

Es necesario contar con adecuada evidencia para respaldar una acción contra una persona u organización. Siempre que esta acción responda a una medida disciplinaria interna, la evidencia necesaria estará descrita en los procedimientos internos.

11.2. Revisiones de la Política de Seguridad y la Compatibilidad Técnica

11.2.1. Cumplimiento de las Políticas de Seguridad

Cada Responsable de Unidad Organizativa, velará por la correcta implementación y cumplimiento de las normas y procedimientos de seguridad establecidos, dentro de su área de responsabilidad. El Responsable de Seguridad Informática, realizará revisiones periódicas de todas las áreas del Organismo a efectos de garantizar el cumplimiento de la política, normas y procedimientos de seguridad. Entre las áreas a revisar se incluyen las siguientes:

a) Sistemas de información.
b) Proveedores de sistemas.
c) Propietarios de información.
d) Usuarios.

Los Propietarios de la Información brindarán apoyo a la revisión periódica del cumplimiento de la política, normas, procedimientos y otros requisitos de seguridad aplicables.

11.2.2. Verificación de la Compatibilidad Técnica

El Responsable de Seguridad Informática verificará periódicamente que los sistemas de información cumplan con la política, normas y procedimientos de seguridad, las que incluirán la revisión de los sistemas en producción a fin de garantizar que los controles de hardware y software hayan sido correctamente implementados.

11.3. Consideraciones de Auditorías de Sistemas

11.3.1. Controles de Auditoría de Sistemas

Cuando se realicen actividades de auditoría que involucren verificaciones de los sistemas en producción, se tomarán recaudos en la planificación de los requerimientos y tareas, y se acordará con las áreas involucradas a efectos de minimizar el riesgo de interrupciones en las operaciones.

11.3.2. Protección de los Elementos Utilizados por la Auditoría de Sistemas

Se protegerá el acceso a los elementos utilizados en las auditorías de sistemas, o sea archivos de datos o software, a fin de evitar el mal uso o el compromiso de los mismos. Dichas herramientas estarán separadas de los sistemas en producción y de desarrollo, y se les otorgará el nivel de protección requerido. Se tomarán los recaudos necesarios a efectos de cumplimentar las normas de auditoría dispuestas.

11.4. Sanciones Previstas por Incumplimiento

Se sancionará administrativamente a todo aquel que viole lo dispuesto en las presente Políticas de Seguridad conforme a lo dispuesto por las normas estatutarias, escalafonarias y convencionales que rigen al personal y en caso de corresponder, se realizarán las acciones correspondientes ante el o los Organismos pertinentes.

Anexo 13. Creacion de Contraseñas

1. OBJETIVO Y ÁMBITO DE APLICACIÓN

Las contraseñas son un aspecto fundamental de la seguridad de los recursos informáticos, es la primera línea de protección para el usuario. Una contraseña mal elegida o protegida puede resultar en un agujero de seguridad para toda la organización. Por ello, todos los usuarios de la E.S.E. Hospital Emiro Quintero Cañizares (H.E.Q.C.) son responsables de velar por la seguridad de las contraseñas seleccionadas por ellos mismos para el uso de los distintos servicios ofrecidos a la comunidad en general.
La seguridad provista por una contraseña depende de que la misma se mantenga siempre en secreto, todas las directrices suministradas por esta política tienen por objetivo mantener esta característica fundamental en las contraseñas de los recursos del HEQC.
El objetivo fundamental de esta política es establecer un estándar para la creación de contraseñas fuertes, la protección de dichas contraseñas, y el cambio frecuente de las mismas.
El ámbito de esta política incluye a todos aquellos usuarios de los servicios y recursos informáticos de la E.S.E. Hospital Emiro Quintero Cañizares que tienen o son responsables de una cuenta (o cualquier otro tipo de acceso que requiera una contraseña) en cualquiera de los sistemas de la E.S.E. Hospital Emiro Quintero Cañizares.

2. POLÍTICA GENERAL

Todas las contraseñas de cuentas que den acceso a recursos y servicios de la E.S.E. Hospital Emiro Quintero Cañizares. deberán seguir las siguientes directrices generales:

- Todas las contraseñas de sistema (root, administradores, cuentas de administración de aplicaciones, etc…) deben ser cambiados al menos una vez cada seis meses.
- Todas las contraseñas de usuario (cuentas de SI, cuentas de email, cuentas de servicios Web, etc…) deben ser cambiadas al menos una vez cada doce meses. Sin embargo, se recomienda cambiarla con mayor frecuencia y también siempre que el usuario sospeche que la seguridad de su contraseña pueda haber sido comprometida.
- Las cuentas de usuario que tengan privilegios de sistema a través de su pertenencia a grupos o por cualquier otro medio, deben tener contraseñas distintas del resto de cuentas mantenidas por dicho usuario en los servicios y recursos del HEQC.
- Las contraseñas no deben ser incluidas en mensajes de correo electrónico, ni ningún otro medio de comunicación electrónica. Tampoco deben ser comunicadas las contraseñas en conversaciones telefónicas.
- En la medida de lo posible, las contraseñas serán generadas automáticamente con las características recomendadas en esta política y se les comunicará a los usuarios su contraseña siempre en estado “expirado” para obligar al usuario a cambiarla en el primer uso que hagan de la cuenta o servicio.
- Las contraseñas por defecto asociadas a los sistemas o aplicaciones nuevas deberán ser cambiadas antes de poner estos sistemas en producción. También se desactivarán aquellas cuentas “por defecto” que no sean imprescindibles.

- Todas las contraseñas de sistema y de usuario de recursos y servicios del HEQC deben respetar las recomendaciones descritas en la presente política.
- Algunos servicios en los que sea crítico el mantener la seguridad de la contraseña podrán determinar medidas adicionales de protección de la misma.

3. SELECCIÓN Y CUSTODIA DE CONTRASEÑAS

3.1.- Recomendaciones generales para la selección de contraseñas

Las contraseñas son usadas con múltiples propósitos en la E.S.E. Hospital Emiro Quintero Cañizares, como pueden ser las contraseñas de cuentas de usuario para los SI, contraseñas de sistema de los recursos del HEQC, servicios Web, cuentas de correo electrónico, protectores de pantalla en los recursos de los usuarios, administración de dispositivos remotos, etc… Se debe poner especial atención en la selección de contraseñas seguras para la autentificación en todos los recursos y servicios del HEQC.

La seguridad de este tipo de autentificación se basa en dos premisas:

1- La contraseña personal sólo la conoce el usuario.

2- La contraseña es lo suficientemente "fuerte" para no ser descifrada.

La contraseña para ser considerada "fuerte" (segura) debe poseer las siguientes características:

- Debe tener al menos 8 caracteres.
- Utiliza caracteres de tres de los cuatro grupos siguientes, y SIEMPRE QUE UNO DE ELLOS DEBERÁ SER UN SÍMBOLO:

1. Letras minúsculas.
2. Letras mayúsculas.
3. Números (por ejemplo, 1, 2, 3).
4. Símbolos (por ejemplo, ¡, @, Ñ, =, -, etc.).

- No ser, ni derivarse de una palabra del diccionario, de la jerga o de un dialecto.
- No derivarse del nombre del usuario o de algún pariente cercano.
- No derivarse de información personal (del número de teléfono, número de identificación, fecha de nacimiento, etc…) del usuario o de algún pariente cercano.

Adicionalmente, las contraseñas deben cumplir las siguientes recomendaciones:

- No podrá contener 3 o más caracteres consecutivos del nombre de usuario o del nombre completo de la persona.
- No podrá tener espacios en blanco.

Finalmente, si va a utilizar teclados que no sean españoles, tenga en cuenta que los símbolos que utiliza en su contraseña pueden estar en sitios diferentes del teclado; por ejemplo no use letras 'ñ.

Las contraseñas no deben ser almacenadas por escrito nunca. Intente crear contraseñas que pueda recordar fácilmente. Una forma de recordarlo con facilidad es crear una contraseña basada en una frase fácilmente recordable. Por ejemplo:

La frase: 'Camarero, una de mero'

Me sugiere la contraseña: 'Camarero!,1demero'

3.2.- Recomendaciones para la protección de la contraseña

Cuando sea posible, no utilice las mismas contraseñas en distintas cuentas y servicios del HEQC. Por ejemplo, utilice contraseñas distintas para su usuario a los SI y para su correo electrónico.

No comparta las cuentas y contraseñas con nadie, incluyendo administrativos, secretarias, etc… Todas las contraseñas deben ser tratadas como información sensible y confidencial.

A continuación se presenta una lista de cosas que NO se deben hacer:

- No revele su contraseña por teléfono a NADIE, incluso aunque le hablen en nombre del servicio de informática o de un superior suyo en la organización.
- No revele la contraseña en mensajes de correo electrónico ni a través de cualquier otro medio de comunicación electrónica.
- Nunca escriba la contraseña en papel y lo guarde. Tampoco almacene contraseñas en ficheros de ordenador sin encriptar o proveerlo de algún mecanismo de seguridad.
- No revele su contraseña a sus superiores, ni a sus colaboradores.
- No hable sobre una contraseña delante de otras personas.
- No revele su contraseña en ningún cuestionario o formulario, independientemente de la confianza que le inspire el mismo.
- No comparta la contraseña con familiares.
- No revele la contraseña a sus compañeros cuando se marche de vacaciones.
- No utilice la característica de "Recordar Contraseña" existente en algunas aplicaciones (Outlook, Netscape, Internet Explorer).

Si alguien le pide la contraseña, refiérale a este documento o pídale que se comunique con el Departamento de Sistemas del HEQC. Si sospecha que una cuenta o su contraseña pueden haber sido comprometidas, comuníquelo al Departamento de Sistemas y cambie las contraseñas de todas sus cuentas.
Cambie las contraseñas con la frecuencia recomendada para cada tipo de cuenta y servicio.

4. MEDIDAS A APLICAR

El incumplimiento de la presente Política puede llegar a comprometer la seguridad de la totalidad de la red corporativa de la E.S.E. Hospital Emiro Quintero Cañizares.
Será la dirección de HEQC la que decida las acciones a tomar en el caso de incumplimiento de la presente política una vez establecidas las repercusiones que sobre los recursos y servicios informáticos del Hospital haya podido tener la violación de la misma. Todo ello sin perjuicio de las acciones disciplinarias, administrativas, civiles o penales que en su caso correspondan, a las personas presuntamente implicadas en dicho incumplimiento.

Anexo 14. Plan de Contingencia

PLAN DE CONTINGENCIA

E.S.E. HOSPITAL EMIRO QUINTERO CAÑIZARES

2014

INTRODUCCIÓN

El Plan de Contingencia es el instrumento de gestión para el buen manejo de las Tecnologías de la Información y de las Comunicaciones. Dicho plan contiene las medidas técnicas, humanas y organizativas necesarias para garantizar la continuidad de las operaciones de la institución. Así mismo, este plan de contingencias sigue el conocido "planifica-actúa-comprueba-corrige". Surge de un análisis de riesgos, donde entre otras amenazas, se identifican aquellas que afectan a la continuidad de la operación de la entidad. El plan de contingencias deberá ser revisado semestralmenteme. Así mismo, es revisado/evaluado cuando se materializa una amenaza.

El Plan de Contingencia permitirá mantener la contingencia operativa frente a eventos críticos de la entidad y minimizar el impacto negativo sobre la misma, los usuarios y clientes, deben ser parte integral para evitar interrupciones, estar preparado para fallas potenciales y guiar hacia una solución adecuada.

El Plan de Contingencia debe involucrar a los actores relevantes. Este plan de trabajo considera evaluar las situaciones de riesgo y definir las tareas orientadas a reducir dichos riesgos.

ORGANO RESPONSABLE:
Departamento de Sistemas
I. ETAPAS DEL PLAN

- Análisis de Riesgos
- Plan de Respaldo
- Plan de Recuperación
- Plan de Mantenimiento
- Plan de Entrenamiento

II. DEFINICIÓN:
Es un tipo de plan preventivo, predictivo y reactivo. Presenta una estructura estratégica y operativa que ayudará a controlar una situación de emergencia y a minimizar sus consecuencias negativas.
El plan de contingencia propone una serie de procedimientos alternativos al funcionamiento normal de la organización, cuando alguna de sus funciones usuales se ve perjudicada por una contingencia interna o externa.

Esta clase de plan, por lo tanto, intenta garantizar la continuidad del funcionamiento de la organización frente a cualquier eventualidad, ya sean materiales o personales. Un plan de contingencia incluye cuatro etapas básicas: la evaluación, la planificación, las pruebas de viabilidad y la ejecución.

III. DIAGNOSTICO SITUACIONAL:

Actualmente la E.S.E. Hospital Emiro Quintero Cañizares cuenta con los siguientes Equipos de Cómputo:

A. Hardware:

- 48 UPS
- 293 Computadoras
- 186 Impresoras
- 21 Escaner
- 10 Laptop o Portátiles
- 8 Plantas Eléctricas
- 7 Video Bean
- 24 Cámaras de Seguridad

B. Comunicaciones:

- 5 Router
- 4 Modem
- 16 Switch
- 05 Servidores
- 1 Firewall

IV. NECESIDAD DE REALIZAR EL MANTENIMIENTO

Es necesario por tanto la identificación previa de cuáles de los procesos son críticos y cuáles son los recursos necesarios para garantizar el funcionamiento de las aplicaciones de gestión. Debe contemplar los planes de emergencia, backup, recuperación, comprobación mediante simulaciones y mantenimiento del mismo. Un plan de contingencia adecuado debe ayudar a la institución a recobrar rápidamente el control y capacidades para procesar la información y restablecer la marcha normal de las actividades.

V. FINALIDAD

Tener un Plan de Contingencias lo más completo y global posible. Definir las normas y procedimientos necesarios para afrontar cualquier eventualidad que se produzca en los Sistemas de Información y Comunicación del Hospital, de modo que se asegure la continuidad, seguridad y confiabilidad de los mismos.

VI. OBJETIVO GENERALES

Un Plan de Contingencia y Seguridad de la Información permite prever los riesgos a los que estará sometido el sistema de información que se va a implementar. El objetivo es doble:

Por un lado, tomarlas medidas necesarias para minimizar la probabilidad de que dichos riesgos se conviertan en una realidad y, por otra parte, si esto ocurriera, posibilitar que el sistema pueda responder sin que ello suponga un grave impacto para su integridad.

Este presente Plan de Contingencia y Seguridad, involucra a toda la entidad directa o indirectamente. De este modo, es válido en cuanto se produce con la aprobación de todas las

partes implicadas, con la total asunción de responsabilidad que a cada una pudiera corresponderle.

VII. OBJETIVO ESPECÍFICOS

a) Proteger la vida de las personas inherentes a los servicios informáticos de la entidad.
b) Prevenir o minimizar la pérdida o la corrupción de archivos de datos críticos para la continuidad de las operaciones del Hospital.
c) Proteger la propiedad de la entidad y otros activos.
d) Iniciar un procedimiento de recuperación de los servicios informáticos ante un desastre o posibles fallas ocasionadas.
e) Proteger al sistema de información de pérdidas irreparables de información procesada.
f) Garantizar la continuidad de las operaciones de los elementos considerados críticos que componen los Sistemas de Información y/o infraestructura informática.
g) Alcanzar una alta disponibilidad, es decir, impedir que se produzcan fallas en los sistemas, que dificulten el normal funcionamiento de nuestra Institución.
h) Definir acciones y procedimientos a ejecutar en caso de fallas de los elementos que componen un Sistema de Información y/o infraestructura informática.
i) Impedir que el daño material de cualquier soporte de información, conlleve o no a la pérdida de información: máquinas, instalaciones, líneas de comunicación etc.; además de otros objetivos como establecer las medidas organizativas y técnicas para asegurar la confidencialidad, integridad y disponibilidad de la información y el soporte informático en nuestra entidad.

VIII. LOGRO QUE SE ESPERA ALCANZAR

Brindar un óptimo funcionamiento y proteger toda la información que se procesa día a día la misma que es almacenada en los servidores que utiliza el Hospital.

IX. AMBITO DE APLICACIÓN

E.S.E. Hospital Emiro Quintero Cañizares

X. ACTIVIDADES A REALIZAR

A.- El Plan de Contingencia y Seguridad de la Información

Se elabora desde el Departamento de Sistemas en coordinación con las sedes internas y externas (UBAS) ligadas a la entidad. El Plan de Contingencia está diseñado para ser aplicado tanto en la Sede principal de la entidad como en las Unidades Básicas de atención (UBAS), involucrando al personal y equipos que intervienen en el mantenimiento de la función informática en nuestra institución y contemplen el software base y las aplicaciones informáticas, así como controlar los accesos a áreas de uso restringido y el hardware. Los resultados esperados son establecer los controles necesarios en la función informática y en el uso de las aplicaciones con el fin de garantizar la integridad y confidencialidad de la información y el soporte informático ante cualquier siniestro que pudiera ocurrir.

B.- Esquema General

El Plan de Contingencia implica un análisis de los posibles riesgos a los cuales pueden estar expuestos las instalaciones, equipos de cómputo y la información contenida en los diversos medios de almacenamiento, por lo que en el Plan Contingencia se hará un análisis de los

riesgos (Antes), cómo reducir su posibilidad de ocurrencia y los procedimientos a seguir en caso que se presentara el problema (Durante).
Pese a todas las medidas se seguridad con las que cuenta la institución puede ocurrir un desastre, por tanto es necesario que el Plan de Contingencias incluya un Plan de Recuperación de Desastres (Después).
El cual tendrá como objetivo, restaurar el Servicio de Cómputo en forma rápida, eficiente y con el menor costo y pérdidas posibles. Si bien es cierto que se pueden presentar diferentes niveles de daños, también se hace necesario presuponer que el daño ha sido total, con la finalidad de tener un Plan de Contingencias lo más completo posible.
Comenzaremos por identificar los tipos de riesgos y los factores para proceder a un plan de recuperación de desastres, así como las actividades previas al desastre, durante y después del desastre.
C.- Definiciones de Términos Empleados.
- Contingencia: Interrupción, no planificada, de la disponibilidad de recursos informáticos.
- Plan de Contingencia: Son procedimientos que definen cómo un negocio continuará o recuperará sus funciones críticas en caso de una interrupción no planeada.
- Proceso crítico: Proceso considerado indispensable para la continuidad de las operaciones y servicios de la entidad, y cuya falta o ejecución deficiente puede tener un impacto operacional o de imagen significativo para la institución.
- Impacto: El impacto de una actividad crítica se encuentra clasificado, dependiendo de la importancia dentro de los procesos TI, en:

Impacto Alto: Se considera que una actividad crítica tiene impacto alto sobre las operaciones de la entidad cuando ante una eventualidad en ésta se encuentran imposibilitadas para realizar sus funciones normalmente.
Impacto Medio: Se considera que una actividad crítica tiene un impacto medio cuando la falla de esta, ocasiona una interrupción en las operaciones de la entidad por un tiempo mínimo de tolerancia.
Impacto Bajo: Se considera que una actividad crítica tiene un impacto bajo, cuando la falla de ésta, no tiene un impacto en la continuidad de las operaciones de la entidad.

D.- Análisis e Identificación de Riesgos
En la institución, se ha identificado los siguientes tipos y factores de riesgos:

N°	TIPO DE RIESGO	FACTOR DE RIESGO
	Fallas en el Equipo	Alto
	Acción de Virus	Alto
	Fuego	Medio
	Terremoto	Bajo

a) En caso de Infección por Acción de Virus (Tipo de Riesgo –Medio)
La entidad cuenta con el antivirus Avast para los servidores y para las estaciones de trabajo; asimismo a través de la red se hacen las actualizaciones del antivirus hacia las máquinas correspondientes.

Sin embargo en caso de infección masiva de virus se debe de seguir el siguiente plan de contingencia:

a.1) Si la infección es vía red a los Servidores y PCS, proceder de la siguiente forma:

1. Revisar las alertas que envía el antivirus y ver el tipo de virus que se está propagando detectando el origen del virus. A su vez desconectar de la red el equipo que está infectado y que está reenviando el virus.
2. Comprobar si tiene carpetas compartidas en forma total y proceder a no c compartirlas.
3. Proceder a limpiar los archivos con la opción de: LIMPIAR o CLEAN INFECTED FILES NO CON DELETED por que esta opción podría borra archivos del sistema operativo, quedando inutilizada la máquina.
4. Una vez limpio el equipo, proceder a realizar una copia de Seguridad sólo de la Data.
5. Si no se lograra limpiar en forma satisfactoria, el equipo, porque los archivos del sistema operativo han sido dañados se procederá a formatear el disco reinstalándole el sistema operativo y transfiriendo la data de seguridad, que se tiene en caso de servidores y de los archivos personales en caso de PC y/o Servidor de Archivos si los hubiera; donde se custodia la data de los usuarios.

a.2) Si la infección es por lista de correo proceder de la siguiente forma:

1. Coordinar con los soporte de las unidades de negocio.
2. Entrar al Servidor donde está instalado el Correo a los servicios y deshabilitar el Servicio de Message Transfer Agent para que no siga reenviando los correos.
3. Proceder a eliminar el mensaje que se encuentra en cola y que está infectado.
4. Proceder a pasar el antivirus con las opciones indicadas.

b) En Fallas por tensión (Tipo de Riesgo –Alto) Son fallas que se presentan como parpadeos constantes, de la energía, causando problemas en las instalaciones internas, llegando a malograr equipos de cómputo si no se tiene las siguientes precauciones:

1. Si hubiere fluctuaciones (flickers), constantes y prolongadas, proceder a apagar los equipos, previo aviso a los usuarios. Como medidas de seguridad ante la prevención se deberá contar con UPS, estabilizadores, polo a tierra, etc.
2. Llamar a Servicios Generales para identificar si la falla es del sistema general, o es un problema aislado en el tablero de alimentación. Si la falla es originada en el sistema general, se debe esperar a que se normalice, para proceder a encender los equipos y conectar a los usuarios. Si la falla es originada por algún factor local, deberá, proceder a revisar, los elementos del tablero: fusibles, térmicos, cables flojos, o revisar si existe algún equipo que este ocasionando esta falla; si no se detecta localmente se debe de proceder a revisar la conexiones, en la subestación de donde se está independizando a energía, revisar los bornes flojos u otros.

Si aún no se detecta la falla, ubicar si están realizando algún trabajo con equipos de alto consumo, como son máquinas soldadoras, etc. y que se hayan conectado a la red de los equipos de cómputo por equivocación.

c) Por corte de Energía Imprevisto:

Es el corte intempestivo del suministro de la energía eléctrica, ocasionado por algún factor externo, como son (corte de la línea de transmisión, accidentes, falla en los sistemas de protección, etc.). Esta falla, tanto en el origen como al final (retorno de la energía) pueden

causar daños a los equipos de cómputo por lo que se debe de seguir el siguiente procedimiento:
1. Se activará la luz de emergencia en el equipo correspondiente.
2. Revisar la carga del UPS que alimentan los equipos, para los casos de corte de energía y determinar el tiempo que queda de energía auxiliar.
3. Llamar a Mantenimiento, para identificar si la falla es del sistema general, o es un problema aislado, en el tablero de alimentación.
4. Por seguridad utilizar la energía que se tiene en los UPS para apagar los equipos en forma correcta.
5. Si la falla es originada en el sistema general, se debe esperar a que se normalice, (siempre en coordinación), para proceder a encender los equipos y conectar a los usuarios.
6. Si la falla es originada por algún factor local, deberá, proceder a revisar, los elementos del tablero como son: fusibles, térmicos, cables flojos, o revisar si existe algún equipo que este ocasionando la falla, si no se detecta localmente se debe de proceder a revisar la conexiones, en la subestación de donde se está independizando la energía, revisar los bornes flojos u otros, Si aún no se detecta la falla ubicar si están realizando algún trabajo con equipos de alto consumo, como son máquinas soldadoras, etc., y que hayan conectado a la red ocasionando un corto circuito, y que no permita, restituir la energía, en forma normal.
7. Si la falla es en el sistema interconectado (general) se deberá esperar que restituya la energía, más un tiempo de unos 15 minutos más, aproximadamente para que se estabilicé y se puedan levantar los sistemas.
8. Si la falla es local proceder a la reparación, o reemplazo, de los componentes que causaron la falla, para esto se debe de solicitar el apoyo de Mantenimiento, (se recomienda tener fusibles, y una llave térmica de respaldo de acuerdo a la capacidad de su tablero). Una vez reparada la falla se debe de conectar la energía para ver el comportamiento, de esta y no encender los equipos de cómputo hasta después de 15 minutos aproximadamente después de la restitución de la energía).

d) En caso de Fuego (Tipo de Riesgo –Medio)
La entidad, a pesar de que cuenta con sistemas de protección, contra incendios, como son, extintores manuales, "conexiones alternas de energía" (en algunas áreas), equipos de bajo consumo, vías de acceso y de evacuación, amplias, etc., sin embargo algún incidente involuntario, puede ocasionar, el inicio de un Incendio para lo cual se deberá proceder de la siguiente manera:
1. Si el inicio del incendio se produce en horas de labores, deberá de proceder a dar la alarma a todo el personal de la oficina, colindantes, y a los bomberos.
2. Desconectar las fuentes de alimentación eléctricas (sin riesgo de exponer la vida).
3. Si el tiempo lo permite y si la fuente del siniestro está lejos pero se puede propagar hacia los equipos principales de computo (servidores) deberá retirar los equipos hacia un lugar seguro, discos o ultimas copias que tenga a la mano y (sin que esto signifique riesgo de exponer su vida).
4. Se deberá proceder a sofocar el fuego utilizando el extintor correcto para el tipo de fuego.

E.- Aspecto de Seguridad en las Redes
a) Control de Acceso Físico

1. Solo personal autorizado deberá ingresar a las áreas restringidas donde se encuentra la Sala de Servidores y/o otros lugares donde se encuentren los equipos informáticos; si otras personan ingresan debe ser con autorización y coordinación de la jefatura inmediata y en los tiempos establecidos y/o coordinados.
2. Se recomienda contar con cámaras de seguridad en las áreas consideradas clave y en caso no se encuentre personal en una de esas áreas deberá estar cerrado por motivos de seguridad; y si dicha persona que está a cargo de las llaves se tendría que ausentar por un tiempo considerable, darle a otra persona a fin que se encargará de velar por el mismo.

b) Control de Acceso a la Red Vía PC.
1. Restringir el acceso a las áreas en que están las estaciones de trabajo mediante llaves o bloqueos de las PC.
2. Solicitar clave de ingreso a la red y a los sistemas que están en red.
3. Retirar o inutilizar las unidades de almacenamiento, las PCs y/o Servidores donde se tenga información muy importante que ponga en riesgo la seguridad de la institución.

c) Protección del Servidor
La parte más importante de la red lo conforman los servidores. La concentración de los datos en el servidor, en términos de cantidad e importancia, hace que sea necesario protegerlo de todas las eventualidades. Los controles necesarios serían:
1. La dependencia en donde se encuentre el servidor no debe ser accesible para nadie, excepto para el administrador de la red y/o la persona responsable del mismo.
2. No se debe permitir que personas que no han de utilizar el servidor estén cerca de él.
3. Dada la importancia del servidor y la cantidad de datos que almacenan en él, es necesario efectuar copias de seguridad de los archivos y aplicaciones como configuraciones del servidor. Cabe recordar que las copias de seguridad del servidor de archivos son un elemento especialmente valioso, debiéndose quedar guardados en un lugar cerrado, seguro y con las condiciones ambientales necesarias para su correcto funcionamiento.
4. Un conjunto de copias de seguridad se debe trasladar regularmente a otro lugar seguro (de preferencia otro local).
5. El área donde se encuentran los servidores debe estar con la suficiente ventilación necesaria, con la seguridad e instalación correcta de las redes eléctricas, el orden y limpieza de la infraestructura tecnológica que puede afectar a los servidores o disminuir su tiempo de vida.

XI. ANÁLISIS DE RIESGOS

Para realizar un análisis de los riesgos, se procede a identificar y evaluar los objetos que deben ser protegidos, los daños que éste pueda sufrir, sus posibles fuentes de daño, su impacto dentro de la entidad y su importancia dentro del mecanismo de funcionamiento.
Posteriormente se procede a realizar los pasos necesarios para minimizar o anular la ocurrencia de eventos que posibiliten los daños, y en último término, en caso de ocurrencia de éstos, se procede a fijar un plan de emergencia para su recomposición o minimización de las pérdidas y/o los tiempos de reemplazo o mejoría.

A. Bienes susceptibles de un daño

Se puede identificar los siguientes bienes afectos a riesgos:

- Personal.
- Hardware.
- Software.
- Datos e información.
- Documentación.
- Suministro de energía eléctrica.
- Suministro de telecomunicaciones.

Los posibles daños pueden referirse a:

a) Imposibilidad de acceso a los recursos debido a problemas físicos en las instalaciones donde se encuentran los bienes, sea por causas naturales o por causas humanas.

b) Imposibilidad de acceso a los recursos informáticos por razones lógicas en los sistemas en utilización, sean estos por cambios involuntarios o intencionales, llámese por ejemplo: Cambios de claves de acceso, datos maestros claves, eliminación o borrado físico/lógico de información clave, proceso de información no deseado.

c) Divulgación de información y que afecte su patrimonio estratégico y/o Institucional, sea mediante Robo o Infidencia.

B. Prioridades

La estimación de los daños en los bienes y su impacto, fija una prioridad con relación a la cantidad de tiempo y los recursos necesarios para la reposición de los Servicios que se pierden en dicho acontecimiento. Por lo tanto, los bienes que tienen más alta prioridad serán los primeros a considerarse en el procedimiento de recuperación ante un evento de desastre.

C. Fuentes de daño

Las posibles fuentes de daño que pueden causar la no operación normal de la institución son:

a) Acceso no autorizado

- Por vulneración de los sistemas de seguridad en operación (Ingreso no autorizado a las instalaciones).
- Ruptura de las claves de acceso a los sistemas computacionales.
- Instalación de software de comportamiento errático y/o dañino para la operación de los sistemas computacionales en uso (virus, sabotaje, ejecución de scripts malintencionados)
- Intromisión no calificada a procesos y/o datos de los sistemas, ya sea por curiosidad o malas intenciones.

b) Desastres Naturales

- Movimientos telúricos que afecten directa o indirectamente a las instalaciones físicas de y/o de operación (equipos computacionales y/o servidores).
- Por fallas causadas por la agresividad del ambiente.
- Inundaciones causadas por falla en los suministros de agua.

c) Fallas de Hardware y Equipos de Soporte.

- Falla en el Servidor de Aplicaciones, Servidor Proxy, Servidor Controlador Dominio y Datos, tanto en su(s) disco(s) duro(s) como en el procesador central.
- Falla en los Switches.
- Falla en el Cableado de la Red.
- Falla en el Router.

- Falla en el Firewall.
- Falla en el Aire Acondicionado en la Sala de Servidores.
- Incendios.
- Por fallas de red de energía eléctrica pública por diferentes razones ajenas.
- Por fallas de la comunicación.
- Por fallas en el tendido físico de la red local.
- Por fallas en las telecomunicaciones con instalaciones externas.
- Por fallas de Central Telefónica.
- Por fallas de líneas de fax.

d) Por fallas de Personal Clave.

Se considera personal clave a áquel que cumpla una función vital en el flujo de procesamiento de datos u operación de los Sistemas de Información: Personal de Informática, Unidad Informática, supervisores de Red. Pudiendo existir los siguientes inconvenientes: Enfermedad, accidentes, renuncias, abandono de sus puestos de trabajo, otros imponderables.

D. Expectativa Anual de Daños

Para las pérdidas de información, se deben tomar las medidas precautorias necesarias para que el tiempo de recuperación y puesta en marcha sea menor o igual al necesario para la reposición del equipamiento que lo soporta.

E. Medidas Preventivas:

a) Control de Accesos

Se debe definir medidas efectivas para controlar los diferentes accesos a los activos computacionales:

- Acceso físico de personas no autorizadas.
- Acceso a la Red de PC's y Servidor.
- Acceso restringido a las librerías, programas, datos, logs de auditoria, etc.

b) Previsión de desastres Naturales

La previsión de desastres naturales sólo se puede hacer bajo el punto de vista de minimizar los riesgos innecesarios en la sala de Cómputo y/o servidores correspondientes en la medida de no dejar objetos en una posición tal que ante un movimiento telúrico de cierta magnitud pueda generar mediante su caída y/o destrucción, la interrupción del proceso de operación normal. Además, bajo el punto de vista de respaldo, se debe tener en claro los lugares de resguardo, vías de escape y de la ubicación de los archivos, CD, discos externos, discos con información vital de respaldo de aquellos que se encuentren aún en las instalaciones. Se deberán tener el respaldo en lugares diferentes y con un código de identificación que maneje el personal de sistemas.

c) Adecuado Soporte de Utilitarios

Las fallas de los equipos deberá minimizarse mediante el uso de otros equipos, a los cuales también se les debe controlar periódicamente su buen funcionamiento, nos referimos a:

- UPS de respaldo de actual servidor de Red o de estaciones críticas.
- UPS de respaldo switches y/o HUB's.
- PCs en stock ante cualquier eventualidad que pudiera suceder.

d) Seguridad Física del Personal
Se deberá tomar las medidas para recomendar, incentivar y lograr que el personal comparta sus conocimientos con sus colegas dentro de cada área, en lo referente a la utilización de los software y elementos de soporte relevantes, así como de documentar las incidencias y tener un registro de sus proyectos realizados y plan de trabajo.
Estas acciones permitirán mejorar los niveles de seguridad, permitiendo los reemplazos en caso de desastres, emergencias o períodos de ausencia ya sea por vacaciones o enfermedades.

e) Seguridad de la Información
La información y programas de los Sistemas de Información que se encuentran en el servidor, o de otras estaciones de trabajo críticas deben protegerse mediante claves de acceso y a través de un plan de respaldo adecuado.

XII. Plan de Respaldo
A. Objetivo:
Establecer un procedimiento para la administración de las copias de respaldos de información de los diferentes Sistemas de Información que se encuentran en producción y de los servicios de red de la organización.
El Plan de Respaldo trata de cómo se llevan a cabo las acciones críticas entre la pérdida de un servicio o recurso, y su recuperación o restablecimiento. Todos los nuevos diseños de sistemas, proyectos o ambientes, tendrán sus propios Planes de Respaldo.

B. Respaldo de datos Vitales
Identificar las áreas para realizar respaldos:
a) Sistemas en Red.
b) Sistemas no conectados a Red.
c) Sitio WEB.
d) Correos electrónicos institucionales

C. Alcance.
Este procedimiento es aplicable a todos los sistemas de información en producción y los servicios de red de la organización.

D. Análisis de la Criticidad.
Primeramente se deberá establecer la criticidad de los Sistemas de Información y los Servicios de Red de acuerdo al tipo de información que procesan y almacenan. Esta tarea deberá ser realizada conjuntamente por Soporte técnico y Administración de Sistemas.
Esta tarea deberá ser realizada periódicamente, con el objetivo de revisar la criticidad, al menos dos veces por año o por demanda cuando se pone en producción un nuevo sistema de información o servicio de red y éste debe ser incluido en el plan de respaldos. Este análisis deberá estar enmarcado en los siguientes niveles de criticidad:
Alta: El sistema y/o servicio posee información altamente crítica.
Media: El sistema y/o servicio posee información medianamente crítica.
Baja: El sistema y/o servicio posee información que no es crítica.
E. Toda la Información No es Crítica.

Normalmente cuando uno plantea que va a respaldar los datos de su PC a una persona en una compañía y le pregunta que es crítico respaldar, casi siempre la respuesta es todo. Pero en realidad esto no es así, uno tiene que definir muy bien cuál es la información crítica, por ejemplo la música que guarde un empleado en su PC no es crítica para las actividades de la empresa. En cambio su correo electrónico, proyectos, informes y papeles administrativos si lo suelen ser y tener un respaldo de estos es clave para el funcionamiento de la empresa en caso de cualquier eventualidad. Lo importante de este punto es que NO TODA LA INFORMACIÓN ESCRÍTICA y hay que hacer un levantamiento de la que realmente lo es.
Otro punto importante es que dentro de la información crítica hay varios niveles, no es lo mismo perder los correos de un empleado que perder la información de nómina o de pago de los proveedores y siempre es aconsejable darle niveles de prioridad a la información para tener un mejor manejo de ella. Una vez que definamos que información realmente necesitamos respaldar vamos en buen camino y podemos seguir con nuestro PROCEDIMIENTO DE GENERACIÓN DE COPIAS DE RESPALDO Y RECUPERACION DE DATOS.
Normalmente la data o información que es respaldada por las empresas es:
Archivos creados por aplicaciones, como por ejemplo .doc, .odt, .xls, .mdb, .pdf, .ppt entre otros.

- Archivos de correo electrónico
- Directorios telefónicos y de contactos
- Favoritos de los navegadores como Firefox e Internet Explorer
- Base de datos
- Configuraciones de los equipos
- Archivos de CAD, PSD, XCF, etc.
- Imágenes y Fotografías de proyectos
- Configuraciones de servicios
- Sistemas de la empresa

F. Plan de Respaldo y Responsables
El plan de respaldos contiene información de que sistemas de información y servicios de red serán respaldados, por lo que su periodicidad, tipo de respaldo, etc., estará determinado por la criticidad del sistema de información y/o servicio de red.
Por otro lado se realizarán las tareas de obtención de respaldos tomado en cuenta los horarios en los que el tráfico de datos de la red sea bajo; es decir, cuando no represente una carga excesiva en la red ni represente un trabajo adicional para los servidores de red cuando están trabajando los usuarios (ingresando, operando, realizando transacciones, etc.), por lo que los horarios correctos serán en horas nocturnas donde el tráfico de información es bajo.
El cronograma deberá contemplar claramente los siguientes campos:
Responsable/s: Persona/s quien/es realizo/aron el plan.
Fecha del plan: La fecha en la cual entra en vigencia el plan.
Numero de plan: El número del plan, ejemplo: 001/ Año.
Operador de Respaldos: Nombre y cargo de la persona que asume el rol.
Revisor de Respaldos: Nombre y cargo de la persona que asume el rol.

G. Términos Usados.

a) Nivel de criticidad: Nivel con la cual se ha establecido la criticidad, este puede ser:
Alta: El sistema y/o servicio posee información altamente crítica, por lo que debe ser respaldada al menos de forma diaria y una vez al mes.
Media: El sistema y/o servicio posee información medianamente crítica, por lo que debe ser respaldada al menos una vez por semana y una vez al mes.
Baja: El sistema y/o servicio posee información que no es crítica y por lo que debe ser respaldada al menos una vez por mes.
b) Periodicidad: Es la frecuencia con la que se deberán realizar los respaldos, esta puede ser:
Diario: Realización de la copia de respaldo diariamente a disco duro.
Semanal: Realización de la copia de respaldo semanalmente a disco duro.
Mensual: Realización de la copia de respaldo mensual a cinta con las copias diarias y semanales acumuladas (HISTÓRICO).
A requerimiento: Realización de la copia de respaldo a requerimiento por una sola vez o por un tiempo determinado y puede ser temporal-diario o temporal-mensual normalmente a requerimiento especial, a menudo usado para ambientes de prueba.
c) Tipo: Se refiere al tipo de respaldo.
Total (Full): Es un respaldo completo de toda la información y configuración.
Diferencial (incremental): Es un respaldo de solamente la nueva información comparada con la información que posee el respaldo previo, por lo general a partir de un backup total.
d) Nombre de la tarea: El nombre de la tarea que se ejecutara para obtener el respectivo respaldo.
e) Responsables: El principal responsable es la persona que posee el rol de operador de Respaldos o se puede definir otro responsable exclusivamente en casos muy excepcionales.
f) Horarios: Los horarios se establecerán con el cuidado de no sobrecargar la red y los servidores, normalmente por las noches cuando la carga de interconexión y de procesamiento es muy baja.
g) Sitio: Lugar donde se encuentra el sistema de información y/o servicio de red en producción.
h) Medio: Medio en el cual se obtienen las copias de respaldo (Cintas, Dvds, Discos Duros, etc.), número de copias: Se establecerá el número de copias, normalmente es de una copia de respaldo, pero puede establecerse más copias en algún caso especial (campo opcional).

H. Designación de Responsables
Se deberá designar formalmente a las personas responsables de la obtención de copias de respaldo, es decir, establecer la persona quien tendrá el rol de Operador de Respaldos, así como también el rol de Revisor de Respaldos, ambos roles se describen a continuación:
a) Respaldo Local
El respaldo local puede hacerse de varias formas en varios tipos de dispositivos. Los más comunes son: Servidor de respaldo, con un arreglo RAID (múltiples discos en espejo), este servidor se coloca en red con una aplicación que respalde los datos automáticamente cada cierto tiempo, en estos tiempos el almacenamiento en disco duros es bastante económico y no se necesita que el servidor tenga una gran cantidad de recursos para efectuar esta tarea, casi siempre algún servidor que se haya sacado de circulación o inclusive una PC "vieja" puede hacer el trabajo. Claro hay servidores de alto desempeño para este tipo de tareas y la decisión va a depender del presupuesto con que cuenten.

Disco duro Externo en Red o USB, si la entidad no tiene presupuesto para un servidor y no cuenta con muchas estaciones de trabajo, un disco duro en Red o USB puede hacer las veces de sistema de respaldo, estos disco duros no suelen ser muy costosos y hay de todas las capacidades, lo ideal sería tener dos de estos en espejo en caso de que alguno falle. En caso de ser un disco duro USB se tiene que compartir en Red entre las PC de la empresa.
CDs, DVDs, si el respaldo que va a realizar no es tan periódico (1 o 2 veces al mes) puede utilizar un medio como un CD o DVD, en este caso sólo necesita una unidad capaz de grabar en cualquiera de estos medios y hay varias aplicaciones que permiten hacer el respaldo sin ningún problema. Si quiere utilizar el DVD o CD más de una vez se recomienda comprar los que son regrabables. Estos medios no suelen estar recomendados para respaldos muy periódicos, y casi siempre se utilizan para guardar información histórica de la empresa (como facturas, recibos, proyectos antiguos, etc). Además se tiene que tener en consideración el almacenamiento seguro de estos discos en un contenedor cerrado que sólo tengan acceso personas autorizadas y que esté lejos del sol y la humedad. También se tiene que tener un sistema para catalogar y etiquetar que sea eficiente.
Cintas Magnéticas, este fué el sistema de respaldo preferido por muchos y aún muchas empresas lo utilizan, ahora son un poco difícil de conseguir además que su capacidad de almacenamiento es un poco limitada. Al igual que con los CDs y DVDs hay que tomar en cuenta el almacenamiento (lejos de campos magnéticos), etiquetado correcto y la rotación (de la que hablaremos más adelante) y además son medios que son reutilizables.
Se puede utilizar también una combinación de cualquiera de los métodos que planteamos. Por ejemplo el respaldo del día a día se puede realizar en un servidor o disco duro externo y los históricos con más de un año de antigüedad en CDs y DVDs.
Las desventajas de utilizar un medio de respaldo local es que en caso de desastre o robo se verán igual de afectados que nuestros demás equipos, normalmente la información más crítica se respalda en un medio como un DVD y se puede guardar en una caja fuerte si se tiene alguna en la empresa de esta manera si hay algún incendio o inundación no se verá afectada y tiene menos probabilidades de que sea robada. Aun así el respaldo local es una medida muy importante y es la primera línea de defensa para salvaguardar la información de nuestra empresa.
b) Respaldo Remoto
El respaldo remoto nos ayuda a protegernos contra desastres como incendios e inundaciones, contra robos y otras eventualidades que puedan ocurrir en el sitio principal de nuestra empresa. Este tipo de respaldo se puede realizar de varias formas:
Servidor de Respaldos remotos, si nuestra empresa tiene varias sedes separadas geográficamente podemos colocar uno o varios servidores distribuidos entre las sedes para respaldar nuestra información a través de la red con una conexión segura. Así si pasa una eventualidad en alguna de nuestras sedes podemos recuperar la información fácilmente.
Servicios de Respaldo remoto, hay varias empresas que ofrecen el alquiler de servidores dedicados o servicios de respaldos, con este tipo de servicios no se necesitan tener varias sedes, simplemente se alquila el espacio que necesitemos para nuestro respaldo y se puede ir ampliando a medida que se necesite más. Este es uno de los servicios más populares de los que son llamados servicios de Nube donde una empresa ofrece capacidad y sistemas en demanda en la red. Asegurarse que a la hora de alquilar uno de estos servicios que tenga una fuerte política de seguridad y privacidad y que garanticen la integridad de sus datos, los

proveedores de estos servicios están en la obligación de tener ciertas garantías de sus datos y de explicar cuáles son los mecanismos que utilizan para garantizarlos, si se rehúsan a explicar esto no confíe en el proveedor.
Estos dos son los principales métodos, también hay otra forma que es la de guardar los respaldos realizados en CDs y DVDs en otra localidad, igualmente que en el respaldo local de estos discos es importante un almacenamiento y etiquetado adecuado.
El respaldo remoto trae como ventaja la distancia geográfica que disminuye el riesgo de perder los datos, como desventaja tenemos que si se llega a perder la comunicación por períodos largos de tiempo no se puede realizar el respaldo con regularidad. La mejor solución es utilizar un respaldo local y remoto, así se tienen las ventajas de ambos y se compensan las desventajas de uno con el otro.
Como lo mencionamos anteriormente la información que sea más crítica y con mayor prioridad se puede respaldar en ambos sistemas mientras que la menos crítica se puede hacer solamentelocal, lo cual disminuye los costos de inversión.

I. Uso de los Respaldos
Se establecen dos situaciones:
a) Uso para propósitos de revisión: Los medios antes de ser enviados al custodio, la persona con el rol de Revisor de Copias de Respaldo, podrá solicitar el medio, al Operador de Copias de Respaldo, cuando así lo considere (aleatoriamente) para restaurar en otro ambiente que no sea el de producción, con propósitos de revisión y control y poder certificar el proceso de obtención de copias de respaldo.
b) Uso para restablecer los Sistemas de Información y/o los Servicios de Red: Para la obtención y utilización de los medios donde se encuentra información de respaldo y con el propósito de restaurar los mismos ante posibles incidentes (Administración de Problemas e Incidentes, Administración del Plan de Contingencias, etc.), solo podrán ser solicitados por el responsable de las copias de seguridad y con la aprobación del Jefe de Área correspondiente.

J. Análisis de Impacto de los Procesos
a) Objetivo Principal:
El objetivo principal del Análisis del Impacto de los procesos, es determinar las funciones, procesos e infraestructura de soporte que son críticos para la contingencia operativa de la entidad.
b) Objetivos Específicos:
Para lograr el objetivo principal se definieron los siguientes objetivos específicos:
- Identificar las preocupaciones y prioridades de la Alta Dirección en el caso que exista una indisponibilidad en los sistemas informáticos producida por una contingencia.
- Identificar el tiempo máximo en el que un proceso crítico de la entidad deberá ser restaurado para su normal y eficiente continuidad.
- Identificar el impacto en las aplicaciones que soportan los procesos críticos de la entidad.
- Proporcionar las bases de una estrategia para la contingencia operativa en caso de un desastre.

K. Sistemas de Información de la E.S.E Hospital Emiro Quintero Cañizares
Los principales sistemas existentes en la E.S.E. Hospital Emiro Quintero Cañizares son:

- Sistema de Informacion de facturación en Servicios de Salud (SIFESS).
- Athenea
- Registro Unico de Afiliados RUAF
- TNS
- DELPHY
- Sistema de Información Radiológica SYNAPSE
- Sistema de Vigilancia Alimentaria y Nutrición WIN VAN

L. Principales servicios que deberán ser restablecidos Y/O recuperados.
a) Generales

- Windows
- Correo Electrónico
- Internet.
- Antivirus.
- Herramientas de Microsoft Office.

b) Software Base

- Base de Datos Sql
- Backup de la Información.
- Ejecutables de las aplicaciones.

c) Respaldo de la Información

- Backup de la Base de Datos Sql
- Backup de la Plataforma de Aplicaciones (Sistemas)
- Backup de la WEBSITE
- Backup del Servidor controlador de Dominio.
- Backup del Servidor de Archivos.

XIII. Plan de Recuperación
A. Objetivos del Plan de Recuperación
Los objetivos del plan de Recuperación son:

- Determinación de las políticas y procedimientos para respaldar las aplicaciones y/o los datos.
- Planificar la reactivación dentro de las 5 horas como máximo de producido un desastre, todo el sistema de procesamiento y sus funciones asociadas.
- Permanente mantenimiento y supervisión de los sistemas y aplicaciones.
- Establecimiento de una disciplina de acciones a realizar para garantizar una rápida y oportuna respuesta frente a un desastre.
- Restablecer en el menor tiempo posible el nivel de operación normal del Centro de Procesamiento de la información y/o de los Servidores correspondientes, basándose en los planes de emergencia y de respaldo a los niveles del Centro de Cómputo y de los demás niveles.

B. Lista de Verificación Para el Plan de Recuperación de Desastres

Cuando hablamos de ejecutar una Recuperación de Desastres de nuestra red o de la Continuidad del Negocio, el tiempo y la precisión son de alta importancia. Las metas de una recuperación de desastres y la continuidad del negocio son sensitivos en el tiempo y bastante críticos, por lo que el uso de una Lista de Verificación se convierte en una herramienta ideal cuando nos afrontamos a una situación en donde esos planes son requeridos.

Las siguientes actividades definen una seria de acciones o actividades que deben entrar en juego cuando se requiere ejecutar una recuperación de desastres:

- Detectar una falla y efectos de desastres lo más rápido posible.
- Notificar a los responsables que deben tomar acción.
- Aislar los sistemas afectados para limitar el alcance de las fallas y daños.
- Reparar o reemplazar sistemas críticos, y trabajar hacia una continuidad en las operaciones normales, si es que las circunstancias lo permiten.

El Plan de Recuperación viene de la mano del Plan de Respaldo, pues de la información respaldada se realiza la recuperación en caso de algún inconveniente. La restauración de los datos es el fin por el que hay que luchar a la hora de realizar una buena planificación de copias de seguridad. Los Backus tienen como objetivo hacer frente a cualquier pérdida de datos y poder mantener la continuidad del negocio, por lo que si contamos con una correcta planificación de copias de seguridad, lo único que nos falta para que la organización pueda seguir funcionando es restaurar los datos y volver a la situación previa al desastre o la interrupción en lo que respecta a los sistemas de información.

C. Alcance del plan de recuperación.

La responsabilidad sobre el Plan de Recuperación es de la Unidad de Administración y el Personal de Sistemas con una persona encargada de ejecutarlo, la cual debe considerar la combinación de todo su personal, equipos, datos, sistemas, comunicaciones y suministros.

La duración del plan se determinará de acuerdo a las necesidades que se presenten y la capacidad de los equipos de trabajo para procesar la restauración y recuperación de los sistemas. De igual forma se puede crear un comité entre el mismo personal que tenga conocimientos suficientes para determinar si la recuperación puede realizarse con todas las condiciones favorables.

D. Activación del Plan:

La decisión queda a juicio de la Dirección General, determinando la activación del Plan de Desastres, y además indicar el lugar alternativo de ejecución del Respaldo y/o operación de emergencia, basándose en las recomendaciones indicadas por éste.

E. Duración estimada

Los supervisores de cada área determinarán la duración estimada de la interrupción del servicio, siendo un factor clave que podrá sugerir continuar el procesamiento en el lugar afectado o proceder al traslado del procesamiento a un lugar alternativo.

F. Responsabilidades

- Orden de Ejecución del Plan: Dirección General.
- Supervisión General de Plan: Propia y/o empresa en convenio para Recuperación.

- Supervisión del Plan de Recuperación: Supervisor(es) de Área(s).
- Abastecimiento (HW, SW): Asistente de Administración.
- Tareas de Recuperación: Personal de tareas afines.

G. Aplicación del Plan

Se aplicará el plan siempre que se prevea una pérdida de servicio por un período mayor de 48 horas, en los casos que no sea un fin de mes, y un período mayor a 24 horas durante los fines de mes (durante los cierres contables).

H. Priorizar el Recupero de Recursos.

Listar la prioridad asociada con el recupero de un recurso específico, basado en la caída del impacto y el tiempo de caída aceptable. Usar escalas cuantitativas o cualitativas Alto, Medio, Bajo).

PRIORIZAR EL RECUPERO DE RECURSOS.

N°	RECURSOS	PRIORIDAD DE RECUPERACIÓN
1	PC’s	Alto
2	Impresora	Alto
3	Sistemas de Información	Alto
4	Servidores	Alto
5	Internet	Alto
6	Herramientas de Office (Excel, Word, etc)	Medio
7	Línea telefónica	Medio

Asegurar que la estrategia elegida pueda implementarse de manera eficaz con el Personal y recursos financieros disponibles y se ejecute de manera correcta la continuidad de los procesos y servicios de la entidad.

Se debe determinar un presupuesto de gastos para el planeamiento de contingencias referente a:

- Software y hardware.
- Transporte.
- Pruebas.
- Entrenamiento.
- Materiales.
- Tiempo a incurrir.
- Servicios, etc.

I. Detalla algunas de las causas de la Falla del Servidor.

CASO A: Error Físico de Disco de un Servidor (Sin RAID).

Dado el caso crítico de que el disco presenta fallas, tales que no pueden ser reparadas, se debe tomar las acciones siguientes:

1. Ubicar el disco malogrado.
2. Avisar a los usuarios que deben salir del sistema, utilizar mensajes por red y telefonear a los jefes de área.

3. Deshabilitar la entrada al sistema para que el usuario no reintente su ingreso.
4. Bajar el sistema y apagar el equipo.
5. Retirar el disco malo y reponerlo con otro del mismo tipo, formatearlo y darle partición.
6. Restaurar el último backup en el disco, seguidamente restaurar las modificaciones efectuadas desde esa fecha a la actualidad.
7. Recorrer los sistemas que se encuentran en dicho disco y verificar su buen estado.
8. Habilitar las entradas al sistema para los usuarios.

CASO B: Error de Memoria RAM
En este caso se dan los siguientes síntomas:
1. El servidor no responde correctamente, por lentitud de proceso o por no rendir ante el ingreso masivo de usuarios.
2. Ante procesos mayores se congela el proceso.
3. Arroja errores con mapas de direcciones hexadecimales.
Se debe tomar en cuenta que ningún proceso debe quedar cortado, y se deben tomar las acciones siguientes:
1. Avisar a los usuarios que deben salir del sistema, utilizar mensajes por red y telefonear a los jefes de área.
2. El servidor debe estar apagado, dando un correcto apagado del sistema.
3. Ubicar las memorias malogradas.
4. Retirar las memorias malogradas y reemplazarlas por otras iguales o similares.
5. Retirar la conexión del servidor con el concentrador, ésta se ubica detrás del servidor, ello evitará que al encender el sistema, los usuarios ingresen.
6. Realizar pruebas locales, deshabilitar las entradas, luego conectar el cable hacia el concentrador, habilitar entradas para estaciones en las cuales se realizarán las pruebas.
7. Probar los sistemas que están en red en diferentes estaciones.
8. Finalmente luego de los resultados, habilitar las entradas al sistema para los usuarios.

CASO C: Error Lógico de Datos
La ocurrencia de errores en los sectores del disco duro del servidor puede deberse a una de las siguientes causas:
1. Caída del servidor de archivos por falla de software de red.
2. Falla en el suministro de energía eléctrica por mal funcionamiento del UPS.
3. Bajar incorrectamente el servidor de archivos.
4. Fallas causadas usualmente por un error de chequeo de inconsistencia física.

En caso de producirse alguna de las situaciones descritas anteriormente; se deben realizar las siguientes acciones:
1. Verificar el suministro de energía eléctrica. En caso de estar conforme, proceder con el encendido del servidor de archivos; una vez mostrado el prompt de DOS, cargar el sistema operativo de red.
2. Deshabilitar el ingreso de usuarios al sistema.
3. Descargar todos los volúmenes del servidor, a excepción del volumen raíz. De encontrarse este volumen con problemas, se deberá descargarlo también.

4. Cargar un utilitario que nos permita verificar en forma global el contenido del(os) disco(s) duro(s) del servidor.
5. Al término de la operación de reparación se procederá a habilitar entradas a estaciones para manejo de soporte técnico, se procederá a revisar que los índices en la base de datos estén correctas, para ello se debe empezar a correr los sistemas y así poder determinar si el usuario puede hacer uso de ellos inmediatamente.

J. Consecuencias de la Interrupción del Fluido Eléctrico
A continuación se presenta una tabla donde se listan las consecuencias de interrupción de fluido eléctrico.

CONSECUENCIA/IMPACTO	ÁREAS AFECTADAS
Cierre Inapropiado de la Base de Datos	Todas las áreas
Finalización Incompleta de los Backups	Todas las áreas
Falla de un componente de equipo Servidor	Todas las áreas
Pérdida total o parcial de la operatividad de los Sistemas	Todas las áreas

Se puede presentar lo siguiente:
1. Si fuera corto circuito, el UPS mantendrá activo los servidores, mientras se repare la avería eléctrica.
2. Para el caso de apagón se mantendrá la autonomía de corriente que el UPS nos brinda (corriente de emergencia), hasta que los usuarios completen sus operaciones (para que no corten bruscamente el proceso que tienen en el momento del apagón), hasta que finalmente se realice el By-pass de corriente con el grupo electrógeno, previo aviso y coordinación.
3. Cuando el fluido eléctrico de la calle se ha restablecido se tomarán los mismos cuidados para el paso de grupo electrógeno a corriente normal (o UPS) donde:
- Corriente de emergencia, a la brindada por grupo electrógeno y/o UPS.
- Corriente normal, a la brindada por la compañía eléctrica.

Si se produjera en horas de la noche una interrupción del fluido eléctrico, se podrían paralizar los procesos de cierre y backup de los servidores con motores de base de datos de Sql ,por tal motivo es necesario revisar continuamente el estado de las baterías del UPS. Dichas baterías deben garantizar una autonomía de aproximadamente una hora. Es necesario establecer un procedimiento que permita al personal de seguridad de la entidad avisar al personal de Informática de este hecho. El UPS se caracteriza por emitir una alarma fácil de identificar.

K. Recursos de Contingencia Generales
Se debe tener recursos de contingencia tales como:
- Router (Proveído por el proveedor de Internet y WAN).
- Tarjeta de Red,Conector RJ45,Jack RJ-45,Testeador.
- Servidores y Equipos de Comunicación (Switchs, Antenas, Fibra, etc.).
- Gabinete de Comunicaciones y Servidores.
- Materiales Y herramientas para cableado Estructurado.
- UPS y Equipos de aire acondicionado.

- Backup diario de la información de los Sistemas.
- Instaladores de las aplicaciones, de Software Base, Sistema Operativo, Utilitarios, etc.
- Componente de Remplazo (Memoria, Disco Duro, UPS, etc.).

Si existiere problema en las antenas, puede ser por problema de posición al direccionar las antenas, se recomienda mover las antenas y ver si el equipo se reestablece, en caso extremo contar con un Servidor Vpn que haga de respaldo hasta que se solucione el inconveniente.

L. Impacto de la Caída y tiempos Aceptables de Caída

A continuación se muestra la tabla de impactos y tiempos de caída aceptables:

RECURSO/SERVICIO	IMPACTO	TIEMPO ACEPTABLE DE CAÍDA
Servidores	Alta	1 hora
Internet	Medio	1 hora

LL. Contenido del plan de contingencia para la Coordinación Administrativa de Tecnologías de Información:

1. Listas de notificación, números de teléfono, mapas y direcciones.
2. Prioridades, responsabilidades, relaciones y procedimientos.
3. Información sobre adquisiciones y compras
4. Diagramas de las instalaciones
5. Sistemas, configuraciones y copias de seguridad en cinta o cualquier otro medio.
6. Medios de comunicación como radios, celulares ante cualquier incidencia.

M. Procedimientos para las Pruebas del Plan de Contingencias - Niveles de Prueba

Se recomiendan dos niveles de prueba:

1. Pruebas en pequeñas Unidades Orgánicas.
2. Pruebas en a nivel Gerencial.

La premisa es comenzar la prueba en las Unidades Orgánicas más pequeñas, extendiendo el alcance a nivel Gerencial, para finalmente realizar las pruebas entre sedes o con otras instituciones externas.

N. Métodos para Realizar Pruebas de Planes de Contingencia

- Prueba Específica

Consiste en probar una sola actividad, entrenando al personal en una función específica, basándose en los procedimientos estándar definidos en el Plan de Contingencia. De esta manera el personal tendrá una tarea bien definida y desarrollará la habilidad para cumplirla.

- Prueba de Escritorio

Implica el desarrollo de un plan de pruebas a través de un conjunto de preguntas típicas (ejercicios).

Las características de la prueba de escritorio son:

1. La discusión se basa en un formato preestablecido.
2. Está dirigido al equipo de recuperación de contingencias.
3. Permite probar las habilidades gerenciales del personal que tiene una mayor responsabilidad.

Los ejercicios de escritorio son ejecutados por el encargado de la prueba y el personal responsable de poner el Plan de Contingencia en ejecución, en una situación hipotética de contingencia. Un conjunto de preguntas se pedirán que resuelva el personal. El encargado y el personal utilizarán el Plan de Contingencia para resolver las respuestas a cada situación. El encargado contestará a las preguntas que se relacionan con la disponibilidad del personal entrenado, suficiencia de los recursos, suficiencia de máquinas, y si los requerimientos necesarios están a la mano. Los ajustes serán hechos al plan o al ambiente determinado durante esta fase si cualquier parte del plan no cumple con los objetivos propuestos.

- Simulación en Tiempo Real

Las pruebas de simulación real, en una Unidad, áreas en la entidad están dirigidas a una situación de contingencia por un período de tiempo definido.

1. Las pruebas se hacen en tiempo real.
2. Son usadas para probar partes específicas del plan.

3. Permiten probar las habilidades coordinativas y de trabajo en equipo de los grupos asignados para afrontar contingencias.

O. Preparaciones PRE Prueba

1. Repasar el plan de contingencia.
2. Verificar si se han asignado las respectivas responsabilidades.
3. Verificar que el plan este aprobado por la dirección de la entidad.
4. Entrenar a todo el personal involucrado, incluyendo orientación completa de los objetivos del plan, roles, responsabilidades y la apreciación global del proceso.
5. Establecer la fecha y hora para la ejecución de la prueba.
6. Desarrollar un documento que indique los objetivos, alcances y metas de la prueba y distribuirlo antes de su ejecución.
7. Asegurar la disponibilidad del ambiente donde se hará la prueba y del personal esencial en los días de ejecución de dichas pruebas.
8. No dejar de lado los resultados obtenidos, la meta es aprender y descubrir las vulnerabilidades, no generar fracaso y frustración.
9. La prueba inicial se enfoca principalmente en entrenar al equipo que ejecutará con éxito el plan de contingencias, solucionando el problema y restableciendo a la normalidad las actividades realizadas.
10. Enfocar los procesos críticos que dependen de sistemas específicos o compañías externas donde se asume que hay problemas.
11. Definir el ambiente donde se realizarán las reuniones del equipo de recuperación de contingencias.
12. Distribuir una copia de la parte del Plan de Contingencias a ser ejecutado.

P. Comprobación de Plan de Contingencias

La prueba final debe ser una prueba integrada que involucre secciones múltiples. La capacidad funcional del plan de contingencia radica en el hecho de que tan cerca se encuentren los resultados de la prueba con las metas planteadas.

Si es necesario, el hardware y software necesarios deben activarse o adquirirse, así como ser transportados al sitio alterno; las estrategias básicas para disponer de equipo de reemplazo son:

1. Acuerdos con proveedores: Se establecen acuerdos de nivel de servicios con los proveedores de software, hardware y medios de soporte; se debe especificar el tiempo de respuesta requerido.
2. Inventario de equipos: Los equipos requeridos se compran por adelantado y se almacenan en una instalación segura externa (el sitio alterno).
3. Equipo Compatible Existente:
- Equipo existente en sitios alternativos.
- Comprar los equipos cuando se necesitan puede ser mejor financieramente, pero puede incrementar de manera significativa el tiempo de recuperación.
- Almacenar un equipo sin usar es costoso, pero permite que la recuperación comience más rápidamente.
- Considerar la posibilidad de un desastre extendido que requiere reemplazos masivos de equipos y retrasos del transporte.
- Mantener listas detalladas de necesidades de equipo y especificaciones dentro del
- Plan de Contingencia.

4. Infraestructura del Ambiente Alterno PROPIO: Para este escenario, se requiere acondicionar un ambiente alterno que pueda ser utilizado como sala de servidores en el momento de la contingencia con las dimensiones apropiadas para facilitar la ubicación de los equipos y mobiliario.
El ambiente alterno contaría con los siguientes recursos:
- 1 mesas para monitores y teclados de los servidores principales
- 2 sillas
- Switches 24 Ports (10/100)
- 1 Router para la conexión a internet
- 1 UPS
- 1 Teléfono
- 1 Extinguidor Clase A (Gas Carbónico)
- Utiles de Oficina

XIV. Plan de Mantenimiento
En la mayoría de las organizaciones los cambios ocurren todo el tiempo. Los productos y los servicios cambian continuamente en todos los niveles. El aumento de procesos basados en tecnología, ha incrementado significativamente el nivel general de dependencia sobre la disponibilidad de sistemas e información para que la entidad opere efectivamente.
Es por lo tanto necesario que el Plan de Contingencia, se adecue a esos cambios y se mantenga continuamente actualizado.
Cuando se realizan cambios al Plan de Contingencia se deben probar completamente y hacer las correcciones requeridas. Esto implica el uso de procedimientos formales de control de cambios bajo el manejo de la persona encargada del equipo del Plan de Contingencia.
a) Control de cambios al Plan de Contingencia.
b) Responsabilidad en el mantenimiento de cada parte del plan.
c) Pruebas a todos los cambios del plan.
d) Aviso a persona responsable del mantenimiento.

A. Control de Cambios al Plan

Se recomienda establecer controles formales del cambio para cubrir cualquier modificación que se tenga al Plan de Contingencia.
Esto es necesario debido al nivel de complejidad contenida dentro del plan. Se debe preparar una plantilla para solicitud de cambios y debe ser aprobada previamente.

B. Responsabilidad en el Mantenimiento de Cada Parte del Plan
Cada parte del plan será asignada a un miembro del equipo del Plan de Contingencia o un Supervisor de la entidad, que será responsable de actualizar y mantener el plan.
La persona encargada del equipo de Plan de Contingencia, mantendrá el control completo del Plan de Contingencia, pero los jefes de las unidades necesitarán mantener sus propias secciones al día.

C. Pruebas a todos los cambios del Plan
El equipo del Plan de Contingencia, nombrará una o más personas que serán responsables de coordinar todos los procesos de prueba y asegurar que todo cambio al plan se prueba apropiadamente.
Cuando los cambios se hacen o son propuestos al Plan de Contingencia, se debe notificar al coordinador de pruebas del Plan de Contingencia. Se deberá probar los procedimientos de cambio para asegurar la calidad de los mismos.
Esta sección del Plan de Contingencia, contiene una comunicación del coordinador del Plan de Contingencia a las unidades de la entidad afectadas y contiene información acerca de los cambios que se requieren probar o reexaminar.

XV. Plan de Entrenamiento
Todo el personal del Área de Informática, debe entrenarse en el proceso de Recuperación del Plan de Contingencia. Esto es particularmente importante cuando los procedimientos son significativamente diferentes de las operaciones normales y se requiere un desempeño excelente para garantizar la restauración de los equipos de cómputo.
La capacitación se debe planear detenidamente y debe ser completamente estructurada y coherente acorde con las exigencias de recuperación. El entrenamiento se debe evaluar para verificar que ha logrado sus objetivos.

A. Objetivos del Entrenamiento
- Entrenar todo el personal en los procedimientos particulares a seguir durante el proceso de recuperación del Plan de Contingencia.
- Difusión del Plan de Entrenamiento.

B. Alcance del Entrenamiento
- La capacitación se llevará a cabo de manera exhaustiva para que se llegue a estar familiarizado con todos los aspectos del proceso de recuperación.
- La capacitación cubrirá todos aspectos de la sección de actividades de recuperación del Plan de Contingencia.
- Es importante desarrollar un programa institucional que cubra las partes esenciales requeridas para comunicar los procedimientos del proceso de recuperación de negocio de la entidad.

C. Revisión y Actualización

El seguimiento permanente permite conocer la evolución, los cambios en condiciones actuales, el cumplimiento de metas propuestas y los ajustes requeridos.
La evaluación periódica del Plan de Contingencia se realiza a través de:

- Simulacros
- Simulaciones
- Evaluación del desempeño por evento

D. La simulación y simulacros

Las simulaciones y simulacros son evaluaciones muy importantes, pues entrenan al personal, enfrentándolo en situaciones probables de emergencia o desastres y ponen a prueba la capacidad de la entidad ante los riesgos que pudiera ocasionar.
Los simulacros, llamados también ejercicios de evaluación, constituye la actividad práctica por excelencia en el proceso de preparación del Plan de Contingencia para situaciones ante desastres.
Las simulaciones, son ejercicios de escritorio que se realizan en situaciones ficticias controladas.

F. Guía para simulaciones y simulacros

- Conformar un Comité de emergencia y defina sus funciones.
- Evaluar los riesgos informáticos, y la vulnerabilidad de la entidad
- Realizar un inventario de recursos humanos y materiales.
- Elaborar un plan para la atención de del centro de cómputo y centro de cómputo alterno.
- Difundir el plan a todo el personal de la entidad
- Coordinar con las instituciones que nos prestan servicios y/o asociados.
- Realizar simulaciones o ejercicios de escritorio.

G. Evaluación del Simulacro

Todas las conclusiones deben integrase en un documentos para uso del comité, con la finalidad de facilitar el proceso de ajuste del plan de acuerdo a los resultados.
Los pasos son:

- Reunión con las comisiones o brigadas de las áreas de la entidad.
- Revisión del Plan e integración de las recomendaciones y decisiones adoptadas de acuerdo con las lecciones aprendidas del ejercicio.
- Difusión del documento de evaluación.

H. Errores Frecuentes en la Realización de los Simulacros

- Improvisación y falta de planificación adecuada al simulacro.
- Falta de entrenamiento del personal participante en los procedimientos que se desarrollan.
- Dificultares disciplinarias con los simuladores, que en ocasiones no asumen la ejecución de los ejercidos con la responsabilidad requerida.
- Falta de coordinación entre las diferentes entidades involucradas participantes del simulacro.

I. Comunicación al personal

Una vez se defina la capacitación a ser impartida al personal, es necesario avisarles acerca del programa de capacitación en el que se requiere su asistencia y saber si puede asistir en dichas fechas y horas señaladas.
Se deberá enviar una comunicación separada a los jefes de Unidad y/o Area, encargados del hospital, avisándoles del horario propuesto de entrenamiento para que su personal asista.

J. Evaluación del entrenamiento

- Se debe valorar el programa de capacitación individual del Plan de Contingencia y el Plan de Contingencia Completo, para asegurar su calidad, eficacia y aplicabilidad.
- Esta información se tomará de los entrenadores y también de las personas que toman los entrenamientos. Este proceso se hará con cuestionarios al final, con el propósito de tener retroalimentación.

XVI. RESPONSABLES

Responsables de la elaboración del Plan:

Ing. Esp. Eduard Fabián Álvarez
Ing. Yolimer Arévalo

XVII. ANEXOS

Procedimiento de Apagado y Encendido de Servidores.
a) Pasos a Seguir para el Encendido de Servidores:

- Identificar el botón de encender el equipo servidor y presionar.
- Si el servidor se encuentra encendido se ingresa a esta por medio del acceso remoto.
- Ingresar el usuario y la contraseña del ADMINISTRADOR DE DOMIO.
- Identificar los servicios que se tienen que levantar para su correcto funcionamiento de las aplicaciones Instaladas (Usualmente está configurado el inicio automático de los servicios cuando inicia el sistema Operativo).

b) Lista de Personal de Equipo de Respuesta a Desastres.
Ante un desastre a la hora de ocurrir el problema estas son las personas críticas que deberán ubicar según el problema suscitado, para dar el apoyo ante la emergencia suscitada.

Respaldo de datos Vitales
Identificar las áreas para realizar respaldos:

- Sistemas en Red.
- Sistemas no conectados a Red.
- Sitio WEB.
- Archivos.

Plan de Contingencia en los Sistemas de Información ante los cortes de energía
Ante un posible corte de energía, se deberá realizar el registro manual de los documentos, posteriormente cuando se restablezca el servicio de la energía eléctrica se deberá regularizar los documentos para posteriormente tener los reportes adecuados .Para ello se deberá contar con formatos disponibles para tal caso.
No regularizar la información en el sistema traerá como consecuencia tener reportes estadísticos y/o operativos incompletos así como inconsistencias de información lo que hará que la toma de decisiones no sea la acertada.

Plan de Contingencia de los Equipos informáticos ante los cortes de energía

Como todo componente electrónico el computador puede sufrir desperfectos ante con un corte de electricidad, un aumento de energía o una baja, esto incluye cualquiera de sus partes como el disco duro, placa base, memorias, procesador, etc.

El hecho de que se tenga un regulador de voltaje no te salva del todo, el regulador te protege en un cierto porcentaje más no en todo, el conjunto es lo que hace la diferencia, por ejemplo: Un computador con un buen regulador de voltaje pero con una fuente de poder baja o de mala calidad está más propenso a una muerte por un alza eléctrica que uno que tenga una buena fuente de poder. La placa también es importante, quizás el componente más importante. La tierra eléctrica es muy importante, sin este el regulador está ahí solo de adorno.

Con respecto al sistema si es factible que puedan fallar algunos programas y o archivos para lo cual se deberán contar con el backup de los instaladores correspondientes y últimos archivos, y así ejecutar programas de recuperación si el caso lo amerita.

A menos que se tenga un notebook, cuando hay un corte de luz, tu PC se apagará y todo el trabajo que no se haya guardado se perderá. Pero, a veces, cuando restauran la energía eléctrica, la PC no vuelve a encender más porque se quemó la fuente.

¿Por qué se quema la fuente?

Cuando vuelve la luz, en el mejor de los casos, y por suerte el más frecuente, sólo se te quema la fuente.

Esto sucede porque, cuando restauran la energía eléctrica, el voltaje que viene es un algo mayor a los 220V y los circuitos internos de la fuente no lo soportan y se queman.

En el peor de los casos, puede suceder que parte de esa corriente llegue al motherboard, quemando varios de sus circuitos.

¿Cómo Protegerse?

Para protegerse de la sobre-carga de tensión eléctrica, se tiene dos opciones:

a) Estabilizador de tensión

- La corriente eléctrica que nos proporcionan (Ej. Luz del sur), nunca tiene 220V o 110V constantes. Siempre tiene fluctuaciones en unos 2 o 3 voltios.
- Lo que este dispositivo hace, como dice su nombre, estabiliza la tensión de la corriente eléctrica.
- Recibe la tensión como viene y entrega SIEMPRE 220V o 110V constantes.
- Si tu PC está conectado a un estabilizador de tensión, siempre va a recibir 220V, ni más ni menos.
- Aunque tengas una baja de tensión, tu PC recibirá 220V.

- Ventajas:
  1. Siempre entrega la tensión estabilizada.
  2. Es económico.
  3. Necesita poco y nada de mantenimiento.
- Desventajas:

1. Si hay un corte de luz, tu PC se apaga.

b) UPS o Sistema de Energía Ininterrumpida

- La UPS es como el estabilizador, con la diferencia de que tiene una batería, que provee de energía en caso de un corte de luz.
- La mayoría de las UPS, te entrega la energía estabilizada, como el estabilizador de tensión.
- Cuando hay un corte de luz, cambia a modo de batería en unos pocos milisegundos, y comienza a entregar energía desde la batería.
- De este modo, puedes seguir trabajando unos minutos más, guardar tu trabajo y apagar correctamente la PC.
- Algunas UPS, incluso traen un programa para que apaga la PC, en caso de que haya un corte de luz cuando uno no se encuentra en la oficina.
- La batería te provee de energía por unos 10 a 15 minutos, suficiente para que guardes todo tu trabajo y apagues la PC.

- Ventajas:

1. En caso de un corte de luz, puedes seguir trabajando unos minutos más.
2. Te entrega siempre la corriente estabilizada.
3. Algunas UPS vienen con un programa que te apaga la PC automáticamente.
4. Necesita poco mantenimiento. Sólo necesitas drenar la batería cada 6 meses.

- Desventajas:

1. Son más caras que los estabilizadores de tensión.
2. Son bastante pesadas, debido a la batería. Igualmente, no es grave, ya que estarán en el piso y no la vas a estar moviendo de un lado a otro constantemente.

Formato de Cambios del Plan de Contingencia
PLAN DE CONTINGENCIA FORMATO DE CAMBIOS
Cambio N°
Descripción del Cambio
Justificación del Cambio
Fecha efectiva
Alternativas consideradas o eliminadas
Proceso(s) de las instituciones impactada(s)
Cronograma de Pruebas
Entrenamiento Ajustado al Cambio
Solicitado por: Responsable del Plan

Nombre: _____
Fecha: AA / MM / AAAA
Firma
Aprobado por:

Nombre: _____
Fecha: AA / MM / AAAA
Firma
Completado por: NOMBRE Fecha: AA / MM / AAAA
Revisado por: NOMBRE Fecha: AA / MM / AAAA

.

XVIII. Conclusiones

El presente Plan de Contingencia, tiene como fundamental objetivo el salvaguardar la infraestructura de la Red y Sistemas de Información de la E.S.E Hospital Emiero Quintero Cañizares, extremando las medidas de seguridad para protegernos y estar preparados a una contingencia de cualquier tipo.

Las principales actividades requeridas para la implementación del Plan de Contingencia son: Identificación de Riesgos, Evaluación de riesgos, Asignación de prioridades a las aplicaciones, Establecimiento de los requerimientos de recuperación, Elaboración de la documentación, Verificación e implementación del plan, Distribución y mantenimiento del plan.

El plan de Contingencia de la entidad está sujeto a la infraestructura física y las funciones que realiza en Centro de Procesamiento de Datos más conocido como Sala de Servidores.

Lo único que realmente permitirá a entidad reaccionar adecuadamente ante procesos críticos, es mediante la elaboración, prueba y mantenimiento de un Plan de Contingencia.

XVII. Recomendaciones

Se enuncian las siguientes recomendaciones:

a) Programar las actividades propuestas en el presente Plan de Contingencias.

b) Hacer de conocimiento general el contenido del presente Plan de Contingencia, con la finalidad de instruir adecuadamente al personal de de la entidad.

c) Adicionalmente al Plan de Contingencia se debe desarrollar reglas de control y pruebas para verificar la efectividad de las acciones en caso de la ocurrencia de los problemas y tener la seguridad de que se cuenta con un método seguro.

d) Se debe tener una adecuada seguridad orientada a proteger todos los recursos informáticos desde el dato más simple hasta lo más valioso que es el talento humano; pero no se puede caer en excesos diseñando tantos controles y medidas que desvirtúen el propio sentido de la seguridad, por consiguiente, se debe hacer un análisis de costo/beneficio evaluando las consecuencias que pueda acarrear la pérdida de información y demás recursos informáticos, así como analizar los factores que afectan negativamente la productividad de la entidad.

e) Autorizar el manejo de la información por perfiles y a los usuarios correspondientes. Dar niveles de acceso a la información.

f) Tener componentes de reserva y/o en stock para poder reemplazar los equipos en el momento adecuado, como componentes de servidor como discos duros, lectoras, router, etc. que se puede necesitar ante cualquier eventualidad.

g) En el caso de las antenas que comunicaban sedes, si estas dejasen de funcionar es recomendable tener otra vía de comunicación como un enlace VPN, para ello se requiere un aceptable ancho de banda.

h) Hacer los backups correspondientes de información según prioridad como contingencia de eventos imprevistos que afectasen la información.

Anexo 15. Procedimiento de Generación de Copias de Respaldo y Recuperación de la Información.

PROCEDIMIENTO DE GENERACIÓN DE COPIAS DE RESPALDO Y RECUPERACIÓN DE LA INFORMACIÓN

1. OBJETO

El objeto del presente documento es la definición del Procedimiento aplicable a la Generación de Copias de Respaldo y Recuperación de la Información manejada por la E.S.E. Hospital Emiro Quintero Cañizares. Se implantará el presente Procedimiento atendiendo al nivel de seguridad de la información y los servicios prestados, y la categoría de los sistemas.

2. ÁMBITO DE APLICACIÓN

- El presente Procedimiento es de aplicación y de obligado cumplimiento para todo el personal que, de manera permanente o eventual, preste sus servicios en la E.S.E. Hospital Emiro Quintero Cañizares, especialmente, los responsables de los Sistemas de Información y los propios usuarios, en sus respectivas competencias, de la generación de copias de respaldo y su posterior recuperación, incluyendo, en su caso, el personal de proveedores externos, cuando proceda y sean usuarios de los Sistemas de Información del Hospital.
- En el ámbito del presente Procedimiento, se entiende por usuario cualquier empleado perteneciente al Hospital, así como personal de organizaciones privadas externas, entidades colaboradoras o cualquier otro con algún tipo de vinculación con el Hospital y que utilice o posea acceso a los Sistemas de Información.

3. VIGENCIA

- El presente Procedimiento ha sido aprobado por el departamento de sistemas de la E.S.E. Hospital Emiro Quintero Cañizares, contribuyendo al establecimiento de las directrices generales para el uso adecuado de los recursos de tratamiento de información que el Hospital pone a disposición de sus usuarios para el ejercicio de sus funciones y que, correlativamente, cuando proceda, asumen las obligaciones descritas, comprometiéndose a cumplir con lo dispuesto en los siguientes epígrafes.
- Cualquier modificación posterior entrará en vigor inmediatamente después de su publicación por parte de la E.S.E. Hospital Emiro Quintero Cañizares.

4. REVISIÓN Y EVALUACIÓN

- La gestión de este Procedimiento corresponde al Departamento de Sistemas, que es competente para:
  - Interpretar las dudas que puedan surgir en su aplicación.
  - Proceder a su revisión, cuando sea necesario para actualizar su contenido o se cumplan los plazos máximos establecidos para ello.
  - Verificar su efectividad y grado de cumplimiento.

• Anualmente (o siempre que existen circunstancias que así lo aconsejen), El Departamento de Sistemas revisará el presente Procedimiento, que se someterá, de haber modificaciones, a la aprobación por parte del mismo.
• La revisión se orientará tanto a la identificación de oportunidades de mejora en la gestión de la seguridad de la información, como a la adaptación a los cambios habidos en el marco legal, infraestructura tecnológica, organización general, etc.
• Será el Responsable de Seguridad la persona encargada de la custodia y divulgación de la versión aprobada de este documento.

5. REFERENCIAS
• Las referencias tenidas en cuenta para la redacción de este Procedimiento han sido:
o ISO 27001:05; SGSI Sistemas de Gestión de Seguridad de la Información.
o ISO 27002; Estándar para la seguridad de la información.
o Ley 1581 del 2012; Habeas Data, derecho que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.
o Ley 23 de 1982; Sobre derechos de Autor.

6. ROLES Y RESPONSABILIDADES
Las responsabilidades personales derivadas de las actividades descritas en el presente Procedimiento son las siguientes:

ROLES RESPONSABILIDADES
Personal del área del Departamento de
Sistemas de la E.S.E Hospital Emiro Quintero Cañizares. o Gestionar las copias de respaldo de los activos
o Recogidos en el alcance del Procedimiento, siguiendo las directrices señaladas.
o Custodiar los soportes de almacenamiento extraíbles donde se almacenan las copias de respaldo.
o Garantizar la correcta ejecución de las operaciones periódicas de copia de respaldo.
o Ejecutar las comprobaciones periódicas de los
o procedimientos de restauración.
o Aprobar las solicitudes de inclusión de activos en la(s) copia(s) de respaldo solicitadas por los Responsables de los Activos.
o Aprobar las solicitudes de recuperación de activos a partir de copias de respaldo, solicitadas por los Responsables de los Activos.
Responsables de los Activos o Tramitar las solicitudes de inclusión de activos en la(s) copia(s) de respaldo.
o Tramitar las solicitudes de recuperación de activos alterados, dañados o destruidos desde la realización de la(s) copia(s) de respaldo.
o Validar las operaciones de restauración de activos gestionadas por el personal del área del Departamento de Sistemas
7. CUESTIONES GENERALES

7.1. Las Copias de Respaldo

- Toda la información de la E.S.E. Hospital Emiro Quintero Cañizares, del ámbito de aplicación será periódicamente respaldada en soportes de backup.
- Los Responsables de la Información y de los Servicios establecerán los ciclos de copia más adecuados para cada tipo de información.
- Las copias de respaldo deben abarcar toda la información necesaria para recuperar el servicio en caso de corrupción o pérdida de la información. Tal información puede incluir datos, programas, ficheros de configuración e, incluso, la imagen del sistema operativo.
- Para todos los sistemas relevantes se definirán los estándares de respaldo, que incluirán, al menos, la siguiente información:
  - Periodicidad de las copias de respaldo.
  - Periodos de retención de las copias.
  - Ubicación de los soportes de respaldo.
  - Procedimientos de recuperación de la información.
  - Procedimientos de restauración y verificación de la integridad de la información respaldada.
  - Procedimientos de inventario y gestión de soportes.

7.2 Tipos de Copias de Respaldo

TIPO DESCRIPCIÓN

Completa Se efectúa una copia de seguridad completa de todos los ficheros y bases de datos. Puede consumir bastante tiempo si el volumen de datos a salvaguardar es elevado. La ventaja derivada de este tipo de copia es que se tiene la seguridad de tener una imagen completa de los datos en el momento de la salvaguarda

Incremental Se copian los datos modificados desde la anterior copia incremental. Siempre se debe partir de una salvaguarda completa inicial. Si se realiza con frecuencia, el proceso no consumirá un tiempo excesivo, debido al bajo volumen de datos a copiar. Por el contrario, la restauración es lenta, toda vez que requiere restaurar una copia completa y todas las copias incrementales realizadas hasta el momento al que se quiera restaurar el sistema.

Diferencial Se copian los datos modificados desde la última copia completa. Se ejecutará con mayor o menor rapidez en función de la frecuencia con que se realice. La restauración suele ser más rápida que la incremental, ya que basta con recuperar una copia completa y una copia diferencia

7.3. Ordenadores Portátiles

- Todos los usuarios de ordenadores portátiles deberán realizar copias de respaldo de sus datos con la regularidad que se especifique.
- Para la realización de estas copias de respaldo deberá utilizarse la herramienta que, a tal propósito, se defina a nivel corporativo.

7.4. Cifrado de soportes almacenados externamente

- Toda la información de copias de respaldo que el Hospital almacene fuera de sus instalaciones debe estar cifrada, según los procedimientos definidos a tal efecto.
- El procedimiento de envío y recepción de soportes permitirá asegurar que éstos no son extraviados ni han sido manipulados durante su transporte.

7.5. Copia de respaldo de información de usuarios

- Los usuarios son responsables de la realización de copias de respaldo con la frecuencia definida y siempre que haya cambios significativos en la información que manejan, para lo que utilizarán las carpetas de red que a tal efecto les sean habilitadas.
- En ningún caso se deberán almacenar copias de respaldo en el domicilio del usuario o en dependencias de terceros ajenas a la E.S.E. Hospital Emiro Quintero Cañizares si no existe un acuerdo previamente suscrito con el tercero en el que se prevea tal posibilidad y se expliciten las cautelas debidas respecto de la custodia de la información almacenada.
- Los responsables de las unidades administrativas de la E.S.E. Hospital Emiro Quintero Cañizares deberán asegurarse de que la información de los empleados a su cargo se salvaguarda de forma satisfactoria.

7.5. Retención de información

- Los documentos originales y los ficheros en formato electrónico deben ser retenidos durante el tiempo que en cada caso el ordenamiento jurídico prescriba.
- Además de lo anterior, hay que tener en cuenta que puede haber requerimientos para retener datos, tales como "logs para auditorías", de cara a la realización de acciones administrativas, disciplinarias, civiles o penales, por lo que habrán de definirse los procedimientos pertinentes para custodiar este tipo de información. Además, se implantarán los medios necesarios para poder revisar las actividades de los usuarios que manejan este tipo de información.
- El Asesor Jurídica de la E.S.E. Hospital Emiro Quintero Cañizares, con la colaboración del resto de Áreas involucradas, especialmente los Responsables de la Información, los Servicios y de Seguridad, se encargará de definir los periodos de retención de la información en función de la naturaleza de la misma y del ordenamiento jurídico vigente en cada momento.
- Cuando la información de E.S.E. Hospital Emiro Quintero Cañizares deje de ser necesaria, deberá ser destruida o eliminada de manera segura. Para dar soporte a este requisito, los responsables de las unidades administrativas del Hospital deberán revisar, de forma periódica, el valor y la utilidad de la información almacenada.
- Todos los datos almacenados en soportes de información que se desechen serán eliminados según un procedimiento definido a tal efecto, que asegure los objetivos de seguridad para la información de los citados soportes. En este sentido, se deberá tener especial cuidado con respecto a la información almacenada en servidores o estaciones de trabajo, el software licenciado o desarrollado a medida y los elementos que recibirán mantenimiento dentro del Hospital por usuarios que no tengan permiso permanente de acceso a los mismos.

7.6. Identificación de información crítica

Los responsables de las unidades administrativas de E.S.E. Hospital Emiro Quintero Cañizares serán los encargados de identificar y mantener una relación actualizada de aquella información que sus áreas necesitan para recuperar la operativa de sus procesos, durante eventuales operaciones de restauración. Se deberá adoptar especial cuidado con aquella

información que proporcione evidencia de la existencia de un hecho, responsabilidad u obligación contractual.

7.7. Prueba de Soporte Informático

La información del ámbito de aplicación, almacenada en un medio informático durante un período prolongado de tiempo, deberá ser verificada al menos una vez al año, para asegurar que la información es recuperable.

7.8. Periodicidad de las copias de respaldo

- La realización de copias de respaldo de forma periódica permitirá al Hospital disponer de su información en caso de destrucción de los equipos o errores producidos en los datos y/o aplicaciones.
- Las copias de respaldo de software, ficheros de datos y bases de datos se deberán realizar regularmente. La frecuencia con la que se deben realizar los back-ups se definirá en función de la sensibilidad de las aplicaciones o datos y de su impacto en el adecuado desarrollo de las competencias atribuías. Por ello, tal periodicidad deberá determinarse sobre la base de las consecuencias que la pérdida de la información tendría para E.S.E. Hospital Emiro Quintero Cañizares.
- Respecto de los ficheros que contengan datos de carácter personal, habrá de tenerse en cuenta lo siguiente:

o Se deben crear procedimientos para la realización de, al menos, una copia de respaldo semanal, si en tal periodo se hubiere producido alteración o modificación de los datos.

o Cuando las pruebas anteriores a la implantación o modificación de los sistemas de información, traten ficheros con datos reales de carácter personal, se deberá realizar previamente una copia de seguridad de los datos.

7.9. Almacenamiento de las Copias de Respaldo en dependencias externas

- Suele ser frecuente el almacenamiento de la última copia de seguridad en una ubicación externa, lo que minimiza el riesgo de pérdida de datos en caso de producirse una contingencia.
- Deberán adoptarse las siguientes cautelas, especialmente cuando se traten ficheros que contengan datos de carácter personal o con información sensible.

o La última copia de seguridad, junto con los procedimientos de recuperación, deberá ubicarse en edificios distintos. A ser posible, en un centro externo.

o Deberá existir un registro con el contenido de las copias de respaldo (Formato de seguimiento a copias de seguridad), lo que facilitará un control efectivo en su gestión.

o Deberá llevarse un registro de las copias de respaldo ubicadas, tanto en las dependencias del Hospital, como en las sedes de almacenamiento alternativas.

7.10. Protección de las Copias de Respaldo

- La adecuada protección de las copias de respaldo permitirá tanto su correcta conservación, como un control de acceso efectivo a los datos almacenados.
- La protección de las copias de respaldo alcanzará tanto a archivos de información como a librerías de aplicaciones. El almacenamiento de los soportes se hará efectivo ubicando las copias en armarios, bajo llave y restringiendo el acceso a personal previamente autorizado.

7.11. Automatización del sistema de Backup

- La automatización de los procedimientos de backup reducirán la posibilidad de omitir ciclos de respaldo o que éstos sean erróneos.
- La programación periódica de las copias de respaldo se debe efectuar a través de un sistema de administración de soportes.

7.12. Descripción del contenido de las Copias de Respaldo

- La documentación del contenido de las copias de seguridad facilitará su identificación.
- En las correspondientes etiquetas se deberá identificar la fecha a que corresponde. En el inventario de copias de respaldo se detallará los archivos de los cuales se hace backup

7.13. Control de entrada y salida de las Copias de Respaldo

- La existencia de un registro que controle las entradas y salidas de copias de respaldo proporciona fiabilidad al inventario de copias de seguridad.
- Debe quedar registrado el flujo de entradas y salidas de los soportes fuera de las instalaciones, dejando constancia del solicitante de cada petición y de los motivos.
- En cuanto a los ficheros que contengan datos de carácter personal (o especialmente sensibles), se deberá tener en cuenta que las copias de seguridad que contengan datos de carácter personal sólo deberán salir con autorización del Responsable y llevándose a cabo bajo su última responsabilidad.

7.14. Transporte de las Copias de Respaldo

- El transporte de las copias de respaldo deberá contar con las adecuadas medidas de seguridad que garanticen la no alteración, robo o destrucción de los datos durante su transporte.
- El transporte de las copias de respaldo con información sensible se deberá realizar utilizando maletas provistas de mecanismos de apertura operados bajo llave y/o mecanismos de cifrado, y cuyas llaves o claves se encontrarán bajo custodia. La responsabilidad de la destrucción o pérdida de información durante el transporte o almacenamiento recaerá sobre el personal / unidad administrativa / personas jurídicas responsables de su gestión.

7.15. Pruebas de realización y restauración de las Copias de Respaldo

- La realización de las pruebas de restauración de las copias de respaldo confirmará el funcionamiento correcto del proceso de recuperación de copias de datos, y garantizará la integridad de los datos que contienen. Se establecerán pruebas respecto a la restauración de las copias de respaldo, de forma rotativa y con una periodicidad previamente establecida.
- Las pruebas y los resultados deberán estar convenientemente documentados y, como consecuencia de las mismas, se subsanarán las incidencias que se hayan puesto de manifiesto durante su desarrollo.
- Además, cuando se traten ficheros que contengan datos de carácter personal, el Responsable deberá verificar semestralmente la correcta definición, funcionamiento y aplicación de los procedimientos de realización de copias de respaldo y recuperación.

7.16. Periodo de existencia de las Copias de Respaldo y su eventual destrucción

- El establecimiento de un período de existencia de las copias de respaldo, de acuerdo con el ordenamiento jurídico vigente en cada momento y lo dispuesto en la Política de Seguridad, facilitará la salvaguarda de las mismas, el cumplimiento legal y el uso eficiente del espacio físico disponible para el almacenamiento.
- Se deberá establecer el período de existencia para las copias de seguridad y los procedimientos a seguir para proceder a su destrucción definitiva una vez concluido tal periodo.

8. HERRAMIENTAS PARA LA GENERACIÓN DE COPIAS DE RESPALDO

El Departamento de Sistemas de la E.S.E. Hospital Emiro Quintero Cañizares contará con un conjunto de herramientas para la generación de copias de respaldo, que le permitirá realizar copias de seguridad de los activos y sistemas de información del Hospital sujetos al ámbito de aplicación.

9. GENERACIÓN DE COPIAS DE RESPALDO

9.1 INCLUSIÓN DE ACTIVOS EN LA COPIA DE RESPALDO

- La operación de inclusión de activos en la copia de respaldo se iniciará a petición del Responsable del Activo y deberá ser previamente aprobada por el Departamento de Sistemas.
- Para solicitar la inclusión, el Responsable del Activo solicitara la Inclusión del activo.
- Al Departamento de sistema le competente:

o Aprobará la petición, y asignará la incidencia al responsable.

o Rechazará la petición, cerrando la incidencia y detallando los motivos que provocan tal rechazo.

9.2 PROCEDIMIENTO DE GENERACIÓN DE COPIAS DE RESPALDO

- La generación de copias de respaldo de los activos del Hospital se soporta en los procedimientos y herramientas de copia del Departamento de Sistemas.
- Las operaciones de copia de respaldo de los activos del Hospital recogidos dentro del alcance se gestionarán de forma programada en fechas y horas concretas, a través de las herramientas de copia del Departamento de Sistemas.
- El Departamento de Sistemas del Hospital mantendrá un inventario de los activos sobre los que se realiza copia de seguridad en el Registro de Activos sujetos a Copia de Respaldo.

9.3 PROCEDIMIENTO DE VERIFICACIÓN DE COPIAS DE RESPALDO

- El Departamento de Sistemas comprobará el registro del sistema, al objeto de garantizar la correcta ejecución de las operaciones de copia de respaldo.
- En caso de detectar un fallo en el proceso de generación, el Departamento de Sistemas investigará y resolverá la incidencia y relanzará la tarea de copia.

9.4 GESTIÓN DE SOPORTES

La E.S.E. Hospital Emiro Quintero Cañizares mantendrá un inventario de los soportes empleados en las operaciones de generación de copias de respaldo en el Registro de Soportes.

10. RECUPERACIÓN DE ACTIVOS A PARTIR DE COPIAS DE RESPALDO

10.1 SOLICITUD DE RECUPERACIÓN DE ACTIVOS

- La operación de recuperación de activos a partir de copias de respaldo se iniciará a petición del Responsable del Activo y deberá ser previamente aprobada por el departamento de Sistemas.
- Para solicitar una recuperación, el Responsable del Activo abrirá una incidencia en el a la que adjuntará la Solicitud de Recuperación de Activos. Un modelo de esta solicitud.
- Al Departamento de Sistemas le competente:
  - Aprobará la petición y señalará la incidencia.
  - Rechazará la petición, cerrando la incidencia y detallando los motivos que provocan tal rechazo.

10.2 RECUPERACIÓN DE ACTIVOS

- El Departamento de Sistemas accederá al soporte físico en el que reside la copia de respaldo del activo a recuperar y lo cargará en la unidad de lectura de la herramienta de generación de copias de respaldo.
- El personal del Departamento de Sistemas responsable de la recuperación del activo, accederá al soporte y, empleando las herramientas de copia, restaurará el activo en una ubicación temporal a la que sólo tendrá privilegios de acceso su responsable, y actualizará la incidencia informándole de la ubicación donde puede localizar el activo.
- El Responsable del Activo accederá a la ubicación temporal y:
  - Validará la recuperación del activo, expresando su conformidad en el registro de la incidencia, autorizando de esta forma su restauración a partir de la copia en su ubicación original.
  - La rechazará, solicitando en el campo comentarios de la incidencia una nueva recuperación a partir de una copia de respaldo alternativa.
- Una vez validada la restauración, el Responsable del Activo:
  - Recuperará el activo en su ubicación original.
  - Eliminará de su ubicación temporal el activo recuperado desde la copia de respaldo.
- Por su parte, el Departamento de:
  - Retirará el soporte físico de la unidad de lectura de la herramienta de generación de copias y lo devolverá al lugar donde se almacenan los soportes.
  - Almacenará el log de la generación de copias con el resultado de la operación de restauración en el registro de operaciones de restauración.

11. COMPROBACIÓN PERIÓDICA DE LOS PROCEDIMIENTOS DE RESTAURACIÓN

• Para garantizar la eficacia de los procedimientos de restauración y la capacidad para recuperar activos desde las copias de respaldo, se establecerá el procedimiento de comprobación periódica.

11.1 PROCEDIMIENTO DE COMPROBACIÓN

• Periódicamente, el Departamento de Sistemas:

o Seleccionará al azar un activo de información almacenado en la copia de respaldo.

o Ejecutará una restauración del activo sobre una ubicación temporal, comprobará la restauración del activo y lo eliminará posteriormente.

o Almacenará el log de la herramienta de generación de copias con el resultado de la operación de restauración en el registro de operaciones de comprobación periódicas.

13. SOPORTE Y MODELOS

13.1 SOPORTE

• A continuación se detallan los elementos de soporte necesarios para la implantación del presente Procedimiento.

o Herramientas de generación de copias de respaldo.

o Soportes de almacenamiento.

o Armario.

13.2 MODELOS

A continuación se detallan los modelos a emplear para la implantación del presente Procedimiento.

13.2.1. Modelo de solicitud de inclusión de activos en la copia de respaldo

Modelo para la solicitud de inclusión de activos en la copia de respaldo.

ACTIVO SISTEMA PERIODO RETENCIÓN TIPO (A / C) CONTENIDOS COMENTARIOS

(Sistema de información que alberga el activo a incluir en la copia de Respaldo.) (Tipo de activo a incluir en la copia de respaldo:

A: Activo de información,

C: Sistema de Información ompleto.) Únicamente para activos de tipo Activo de información, listado completo con el detalle de contenidos, incluyendo directorios y archivos sobre los que generar copia de respaldo.)

13.2.2. Modelo de registro de herramientas para la generación de copias de respaldo

Modelo para el registro de herramientas para la generación de copias de respaldo.

Nombre Tipo (HE / SW) Fabricante Versión Responsable

Tipo de herramienta:
HW: Hardware,
SW: Software.

13.2.3. Modelo de registro de soporte extraíbles
Modelo para el registro de soportes para la generación de copias de respaldo.
Etiqueta Contenido Formato Capacidad Responsable

13.2.4. Modelo de solicitud de recuperación de activos
Modelo para la solicitud de recuperación de activos desde la copia de respaldo.
Activo a Recuperar Sistemas Tipo (A / C) Fecha Recuperación Tamaño EstimadoComentarios
(Sistema de
Información que alberga el activo a recuperar.) (Tipo de activo a recuperar desde la copia de respaldo:
A: Activo de
información,
C: Sistema de información completo.) (Fecha estimada en la que el activo se encontrará disponible.)
DD/MM/AAA

13.2.5. Modelo de registro de activos sujetos a copia de respaldo modelo para el registro de activos de los que se realiza copia.
Activo Tipo Copia (C/I/D) Periodicidad
(D/S/M/A/
BD) Periodo
retención Contenido Responsable Soporte
(C/D)Tipo Activo
(A/C)Comentarios
(Tipo de copia de respaldo:
C: Completa,
I: Incremental, D: Diferencial.) (Periodicidad de la copia:
D: Diaria,
S: Semanal,
M: Mensual,
A: Anual,
BD: Bajo
Demanda.) (Tipo de
soporte en el que se almacena la copia:
C:Cinta,
D: Disco) (Tipo de
activo:
A: Activo de inf.
C: Sistema de info.
completo

Anexo 16. Informe auditoria

INFORME TECNICO

Con el objeto de hacer un diagnóstico del funcionamiento del área de sistemas de la E.S.E, se consideró necesario la realización de encuentas que nos ayudara a analizar y evaluar los riesgos inminentes que vulneran y ponen en riesgo la información que se encuentra dentro de la infraestructura tecnológica de la E.S.E Hospital Emiro Quintero Cañizares; para lo cual se hizo el siguiente procedimiento:

1. Observacion directa participativa de los procesos, elemento fundamental para la investigación.

2. Elaboración de cuatro (4) encuestas para evaluar los siguientes aspectos:

- Seguridad Lógica.
- Elementos de Seguridad Física en el Ambito Informático.
- Servicio de Mantenimiento de Hardware.
- Seguridad Física.

3. Revisión y Aprobación del modelo de la encuesta.

4. Socialización del Instrumento a los encargados de aplicarla en el Área.

5. Diligenciamiento de la Encuesta, con la debida asesoría de la pasante cuando se requirió.

6. Análisis de la Encuesta, donde se priorizaron los riesgos de mayor impacto negativo en la Institución.

Con el resultado de esta información se diligenció la Matriz donde se logró calificar mediante un puntaje el grado impacto negativo y probabilidad de ocurrencia dentro de cada proceso y que finalmente nos refleja una valoración del estado en el que se encuentra la Institución.

Los riesgos encontrados en la Institución son los siguientes:

Fallas eléctricas
Pérdida de la Información
Inseguridad en Area de servidores y central telefónica
Software sin licencia
Tecnología obsoleta.
Daño de Hardware
Infección por Virus Informático

Dentro de los Riesgos hallados, se descubrió que ninguno de ellos tiene controles para la mitigacion de los mismos, esto hace que la información este predispuesta o susceptible a ser afectada o a sufrir pérdidas.

Posteriormente se procedió al diseño de los diferentes de formatos que se detallan a continuación y necesarios para mitigar riesgos, los cuales fueron revisados y corregidos por los funcionarios responsables en la Institución:

- Seguimiento a las Copias de Seguridad
- Seguimiento de las Inscripciones a las Capacitaciones
- Seguimiento al Acceso a los Servidores
- Creacion de las Cuentas de Usuario

Con el propósito de validar y obtener documentos soportes de consulta que coadyuven al mejoramiento continuo de los procesos de la Empresa, se construyeron polítcas del Buen Uso de Hardware, Cuentas de Usuario, Seguridad en la Información y Creación de Contraseñas teniendo como soporte el estandar ISO 27001 y que están sustentadas en el Plan de Contingencia que contiene las medidas técnicas, humanas y organizativas necesarias para garantizar la continuidad de las operaciones.

Finalmente se dejan recomendaciones específicas de forma escrita que contribuirán con la implementación del Sistema de Gestion de la Seguridad de la Información en la ESE Hospital Emiro Quintero Cañizares, indispensable para prestar un servicio con calidad, mejorar las condiciones de vida de los usuarios y garantizar los derechos de la población altamente vulnerable de la ciudad de Ocaña y sus al rededores.

KAREN PAOLA SANCHEZ JAIME
Pasante