PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

MYRIAM BEJARANO PULIDO

Gerente

VIGENCIA

2019

CONTENIDO

INTRODUCCIÓN

La información que se genera en el Hospital Roberto Quintero Villa ESE Montenegro, es elemento base y punto crítico de control para su correcto desempeño y cumplimiento de los objetivos organizacionales. Por lo anterior se requieren de procesos de seguridad y privacidad de ésta, como elementos necesarios evitar cualquier posibilidad de alteración, mal uso, pérdida, entre otros eventos, que puedan significar una alteración para el normal desarrollo en la prestación de servicios de salud.

La ESE acoge este documento como un proceso sistemático de confidencialidad, integridad, disponibilidad de la información, permitiendo garantizar la privacidad de los datos, identificación, análisis, evaluación, valoración, y tratamiento de los riesgos; aplicando los controles necesarios para evitar, reducir, compartir, transferir o asumir el riesgo con medidas preventivas o correctivas que deberá generar como resultado minimizar pérdidas, maximizar rendimientos y cuidar la seguridad del paciente.

1. OBJETIVOS

1.1 OBJETIVO GENERAL

Establecer los lineamientos principales de gobierno y gestión de la seguridad de la información para el Hospital Roberto Quintero Villa ESE Montenegro, que permita minimizar los riesgos de pérdida de la información.

1.2 OBJETIVO ESPECIFICO

- Definir los principales activos de información a proteger en el Hospital Roberto Quintero Villa ESE
- Promover el uso de mejores prácticas de seguridad de la información, para ser la base de aplicación del concepto de Seguridad Digital
- Identificar las principales amenazas que afecten la seguridad de la información dentro de la Institución.
- Proponer soluciones para minimizar los riesgos a los que se expone la entidad en cuanto a la pérdida y alteración de la información.
- Evaluar y comparar el riesgo actual de la entidad con el impacto de implementar o no el plan de gestión de la seguridad de la información.

2. ALCANCES Y LIMITACIONES

2.1 ALCANCES

- Compromiso por parte de la institución para realizar la adopción del plan de gestión del riesgo en seguridad informática.
- Capacitar al personal del hospital Roberto Quintero Villa en la implementación del plan de gestión del riesgo en seguridad informática.

2.2 LIMITACIONES

Los recursos financieros de la entidad son insuficientes para la adquisición de equipos y contratación de personal con el cual se puedan apoyar la implementación del plan de gestión del riesgo en seguridad informática.

3. GESTION DE RIESGOS

3.1 IMPORTANCIA DE LA GESTION DEL RIESGO

Los riesgos de seguridad de información deben ser considerados como parte importante para salvar, proteger y custodiar los activos de información de la entidad debido a los avances que han surgido a través de los años en los sistemas de información.

El hospital Roberto Quintero Villa viene desarrollando los lineamientos trazados por el Gobierno Nacional en cumplimiento a la ley de trasparencia 1712 de 2014 y Gobierno digital, con el cual se están ajustando los modelos y estándares que permitirán brindar seguridad a la información generada internamente en la institución.

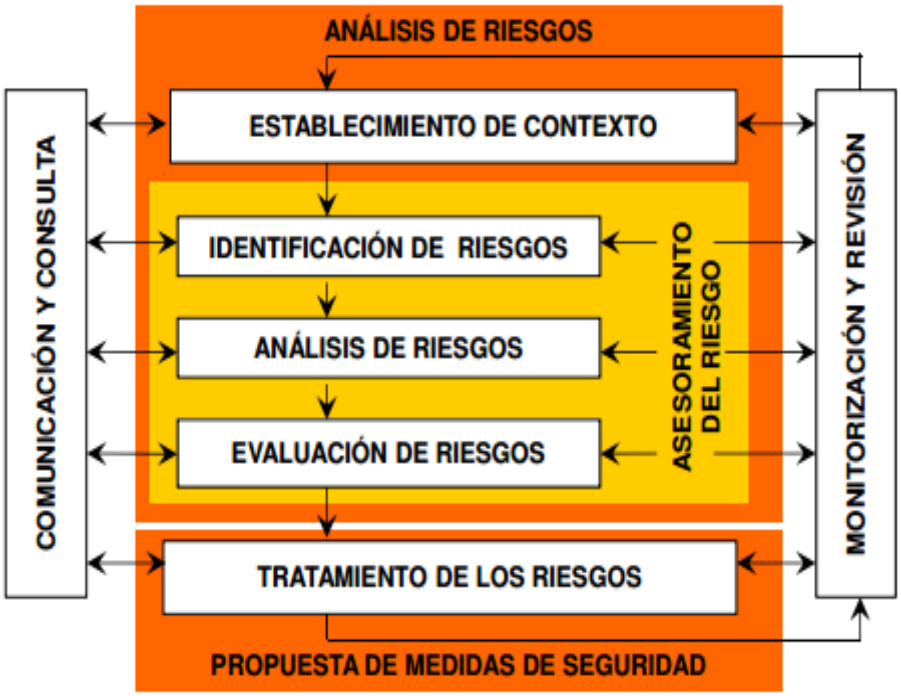
Los riesgos por desastres naturales, riesgos inherentes relacionados con procesos no adecuados en el tratamiento de la misma información, desconocimiento de normas y políticas de seguridad y el no cumplimiento de estas, suelen ser los temas más frecuentes y de mayor impacto presentes en las entidades. Es por tal motivo que se deben tener identificados los riesgos y darles una calificación para poder atacarlos y así poder mitigarlos más fácilmente.

Considerando la situación actual del hospital Roberto Quintero Villa, para reducir los niveles de riesgo, es indispensable diseñar un plan para iniciar las prácticas de las normas y políticas de seguridad e implementar procesos que aseguren la continuidad de los servicios.

3.2 DEFINICION GESTION DEL RIESGO

La definición estandarizada de riesgo proviene de la Organización Internacional de Normalización (ISO), definiéndolo como “la posibilidad de que una amenaza determinada explote las vulnerabilidades de un activo o grupo de activos y por lo tanto causa daño a la organización”.

3.3 VISION GENERAL PARA LA ADMINISTRACIÓN DEL RIESGO DE SEGURIDAD DE LA INFORMACIÓN



3.4 CLASIFICACIÓN DE RIESGOS

- **Riesgos de tecnología**: Están asociado con la capacidad tecnológica de la Institución para satisfacer las necesidades y el cumplimiento de la misión.
- **Riesgos de Cumplimiento**: relacionado con la capacidad de la entidad para cumplir con los requisitos legales, contractuales, de ética pública y en general con su compromiso ante la comunidad y con los entes de control que supervisan el envió de informes.
- **Riesgos Financieros**: Se relacionan con el manejo de los recursos de la entidad que incluyen: la ejecución presupuestal, la elaboración de los estados financieros, los pagos, manejos de excedentes de tesorería y el manejo sobre los bienes.
- **Riesgos Operativos:**son los riesgos provenientes del funcionamiento y operatividad de los sistemas de información de la ESE como son los procesos, la estructura de la entidad y la articulación entre dependencias.

- **Riesgos de Imagen**: Relacionados con la percepción y la confianza por parte de la ciudadanía hacia la institución.

- **Riesgo Estratégico**: Es relacionado con el manejo estratégico de la misión y el cumplimiento de los objetivos institucionales, la clara definición de políticas, diseño y conceptualización de la entidad por parte de la alta gerencia.

3.5 SITUACION NO DESEADA

- Perdida de información por ataques de virus informáticos.
- Hurto de equipos de computo de las oficinas y consultorios.
- Robo de información por usuarios del sistema
- Desastres naturales como incendios o generados por terceros.
- Alteración de claves y de información.
- Poca cobertura y velocidad del servicio de internet.
- No entrega de informes a entes de control a tiempo.
- Manipulación indebida de información.
- Acceso a información confidencial por personal no autorizado
- Uso inadecuado de claves de acceso a información institucional

4 ORIGEN DEL PLAN DE GESTION

El Hospital Roberto Quintero Villa cuenta con un área de sistemas el cual viene desarrollando los diferentes planes para poder dar cumplimiento a las normas exigidas por el Gobierno Nacional.

El gobierno nacional y el ministerio de las TIC han abanderado los proyectos de Gobierno en Línea que permite conocer el funcionamiento de las entidades públicas en el país. Es por ello necesario queel Hospital Roberto Quintero Villacumpla con los requisitos de entregaoportuna y eficiente de la información a estas entidades, a la población y a losdiferentes entes de control que vigilan estas normas.

4.1 PROPÓSITO DEL PLAN DE GESTION DE RIESGO DE LA SEGURIDAD DE LA INFORMACIÓN.

Poder realizar un modelo de seguridad de la información al interior de la entidad y que se ajuste a la normatividad vigente.

Descripción de los requisitos de seguridad de la información para un producto un servicio o un mecanismo.

Alcances, límites y organización del proceso de gestión de riesgos en la seguridad de la información.

4.2 IDENTIFICACIÓN DEL RIESGO

Proceso → Objetivo del Proceso → Identificación de Activos → Riesgo

↓

Causas (Amenazas y Vulnerabilidades).

↓

Descripción del Riesgo.

↓

Efectos de la materialización del Riesgo.

4.

5. ANALISIS DE VULNERABILIDADES

5.1 DESCRIPCIÓN DE VULNERABILIDADES

Normalmente los errores cometidos por los usuarios son las amenazas frecuentes en los sistemas de información y en la protección de los datos de cada sistema, pero se describirán algunas otras vulnerabilidades y amenazas que pueden llevar a la perdida de información relevante para la entidad.

- Los puntos de red ubicados en cada oficina no son suficientes y se han dispuesto nuevos según se va presentando la necesidad.
- El hospital tiene conexión WiFi y la señal se torna débil o no llega a algunas oficinas. Debido a que la infraestructura física es amplia, compleja y la señal debe atravesar paredes.
- Algunos cables de energía no están cerca a los escritorios o no son suficientes para la cantidad de equipos que tiene cada oficina, existe riesgo de pérdida de información en el caso que sean desconectados por accidente y la información procesada por el funcionario no alcanza a ser guardada.
- La corriente regulada y la normal con la que cuenta el hospital tiene problemas de alteraciones en los voltajes ya que constantemente se viene quemando fuentes de poder de los equipos de cómputo y otros dispositivos.
- Las políticas y normas de seguridad de la información existentes no han sido socializadas con todo el personal, por eso es muy común identificar el incumplimiento a las reglas básicas del cuidado tanto de los equipos informáticos y como de la información física y digital, algunas son:

  -No ingerir, ni dejar alimentos y/o bebidas cerca y/o encima de los equipos.
  -No fumar ni ubicar ceniceros cerca y/o encima de los equipos.
  -Facilitar la ventilación del equipo, no colocar papeles u otros objetos cerca a las ranuras de ventilación del equipo.
  -La manera de encender y apagar los PC´s, así como su configuración estará a disposición del cliente interno con el fin de evitar daños en el equipo. (Cuidados del computador.)

-No colocar objetos pesados, encima de la unidad central de proceso (CPU), a fin de evitar su deterioro o maltrato.

-Mantener alejados de la CPU, y monitor (Pantalla) todo elemento electromagnético como imanes, teléfonos, radios, etc.

-No colocar la Unidad Central de Proceso (CPU) en el piso o lugares inestables y/o expuestos a ser golpeados involuntariamente.

-No trasladar ni mover los equipos y/o periféricos de un lugar a otro. En caso de ser necesario el traslado, se deberá contar con la autorización del área de Sistemas de información y Activos Fijos. Cuando se produzca el retorno del equipo, el área de Sistemas de información será la encargada de la supervisión y evaluación del estado del equipo.

-No abrir los equipos de cómputo. Para este caso solo está autorizada el área de sistemas de información.

-En algunas dependencias no hay suficientes equipos para los usuarios teniendo que trabajar con equipos personales y la información es llevada afuera de la institución por estas personas.

-El Datacenter de la entidad requiere de algunas características importantes para cumplir con las normas de funcionamiento (sistemas contra incendios, sistemas de cámaras de vigilancia, alarmas contra incendios, control de temperatura y humedad).

-El área de Sistemas de Información es la responsable de la Instalación y/o desinstalación del software autorizado en la Institución.

-El cliente interno en sus computadores debe tener instalados solo software, aplicativo y/o sistemas autorizados por el área de Sistemas de información en concordancia con las disposiciones de la gerencia de la Institución.

-La información obtenida y desarrollada en el cumplimiento de las funciones es propiedad intelectual de la institución, la cual no deberá ser distribuida, comercializada, ni divulgada.

-Es de carácter obligatorio hacer una revisión de los medios extraíbles de almacenamiento, con el software antivirus del que disponga la institución tales como: Disquete, CD, DVD, memoria USB, en el momento en que se requiera.

-No abrir correos electrónicos de dudosa procedencia, si recibe uno de estos correos debe indicar el inconveniente y remitirlo al responsable del área de Sistemas de información

-Se restringirá automáticamente el acceso a Internet a los clientes internos que naveguen en páginas NO PRODUCTIVAS (Páginas de Adultos, Chat,

etc), ya que estas páginas podrían tener virus que afecten la información de la institución.

5.2 MATRIZ DE VULNERABILIDADES Y MITIGACION DEL RIESGO

IDENTIFICACION DEL RIESGO

Seleciona una clasificación y ubica tu riesgo dentro de una categoría

Nombre del proceso:	OBJETIVO	No. DEL RIESGO	RIESGO	CLASIFICACIÓN	CAUSAS	DESCRIPCION	CONSECUENCIAS POTENCIALES
GESTION DE LA INFORMACION	Gestionar las técnicas y mecanismos para la recolección, clasificación, procesamiento, validación y análisis de la información necesaria para mantener un Sistema de Información que garanticen confiabilidad, validez oportunidad, facilidad de acceso, confidencialidad y seguridad, respondiendo a las necesidades del cliente interno y externo.	R1	Suspensión del funcionamiento del Sistema	TECNOLOGICO	* Problemas con el cableado estructurado * Fallas en los switches * Fallas en la UPS * Problemas con la planta electrica * Ausencia de Mantenimiento Preventivo. *Variaciones en la corriente electrica. . Desastre natural	La ausencia de mantenimiento hospitalario podria ocasionar un mal funcionamineto del sistema de nformacion.	Perdida de informacion No oportunidad en la atencion
		R2	Contaminación del sistema por acción de un virus informático.	TECNOLOGICO	* Ausencia de un paquete de protección antivirus. * Manipulación del servidor por parte de varios usuarios. * Habilitación de puertos en el servidor.. Hackers y por urilizacion de memorias USB externas.	la ausencia de compra de un paquete de antivirus y la no restriccion en los accesos a memorias externas permitira la contaminacion del sistema informatico	Perdida de informacion No oportunidad en la atencion
		R3	Falla en funcionamiento del software institucional	TECNOLOGICO	*Ausencia de mantenimiento preventivo. *Fallas en las baterias. *Fallas en la corriente electrica.. Hackers y por urilizacion de memorias USB externas.	La ausencia de mantenimiento hospitalario podria ocasionar un mal funcionamineto del sistema de nformacion.	No oportunidad en la atencion
		R4	Falla en el Funcionamiento de la UPS	OPERATIVO	* Ausencia de mantenimiento preventivo * Fallas en la red electrica. * Descarga electrica (rayos). . Ausencia de mantenimiento preventivo	La ausencia de mantenimiento hospitalario podria ocasionar un mal funcionamineto del sistema de nformacion.	Perdida de informacion

		R5	Daño masivo de equipos de cómputo	OPERATIVO	* Ausencia de mantenimiento preventivo * Fallas en la red electrica. * Descarga electrica (rayos). . Hackers y por urilizacion de memorias USB externas.	la no renovacion de hardware permitira el daño de los equipos de computo.	Paro en el funcionamiento de los pocesos Perdida de informacion
		R6	No oportunidad en el reporte de informacion	OPERATIVO	* Recepcion tardia de insumos para los informes . Mal funcionamiento de las paginas web de los entes de control	la rotacion de pesonal y la falta de experticia en la elaboracion de informes contribuiria a la no oportunidad en la entrega de los mismos.	Sanciones economicas y disciplinarias

6. PROPUESTA DE SEGURIDAD

- Revisar, organizar y ubicar las conexiones de electricidad según las necesidades propias de las oficinas.
- Revisar las políticas existentes para identificar debilidades y fortalezas, si es necesario se hacen ajustes, teniendo en cuenta que seguridad informática no es igual a seguridad de la información.
- Socializar las políticas de seguridad y privacidad de la información con el personal de la institución.
- Revisar las políticas existentes para identificar debilidades y fortalezas, si es necesario se hacen ajustes, teniendo en cuenta que seguridad informática no es igual a seguridad de la información.

6.1 LINEAMIENTOS DE SEGURIDAD

- Gestión de activos

  Las diferentes áreas con el fin de garantizar la administración y control sobre los activos de la entidad, deben mantener un inventario actualizado de los activos que se encuentran dentro del alcance del modelo de gestión de seguridad de la información y que están cargados a cada procesos, el cual debe estar alineado con el inventario general de activos de información.

  En el inventario se identificará el propietario del activo, quien debe asegurar que la información y los activos asociados con su proceso están clasificados de manera apropiada, así como de establecer controles necesarios para el acceso a éstos de acuerdo con los procedimientos definidos.

  - Uso aceptable de los activos

  La información, archivos físicos, los sistemas, los servicios y los equipos (estaciones de trabajo, portátiles, impresoras, redes, Internet, correo electrónico, herramientas de acceso remoto, aplicaciones, teléfonos y faxes, entre otros) propiedad de la ESE, son activos de la Institución y se

proporcionan a los funcionarios, contratistas y terceros autorizados, para cumplir con los propósitos del negocio.

La ESE podrá monitorear, supervisar y utilizar su información, sistemas, servicios y equipos, de acuerdo con lo establecido en este plan y en cualquier proceso legal que se requiera

El acceso a los documentos físicos y digitales estará determinado por las normas relacionadas con el acceso y las restricciones a los documentos públicos, a la competencia del área o dependencia específica y a los permisos y niveles de acceso de los funcionarios, contratistas y terceros determinadas por la gerencia.

La consulta de expedientes o documentos que reposan en las diferentes oficinas y/o áreas de la ESE se permitirá en días y horas laborales, con la presencia del funcionario o servidor responsable de aquellos

6.1.1 Acceso a Internet:

No está permitido:

o El acceso a páginas relacionadas con pornografía, drogas, alcohol, webproxys, hacking y /o cualquier otra página que vaya en contra de la ética moral, las leyes vigentes o políticas aquí establecidas.

o El acceso y el uso de servicios interactivos o mensajería instantánea que tengan como objetivo crear comunidades para intercambiar información o bien para fines diferentes a las actividades propias del Hospital.

o El Intercambio no autorizado de información de propiedad del Hospital, de sus clientes, usuarios y/o de sus funcionarios, con terceros.

o La descarga, uso, intercambio y/o instalación de juegos, música, películas, protectores y fondos de pantalla, software de libre distribución, información y/o productos que de alguna forma atenten contra la propiedad intelectual de sus autores, o que contengan archivos ejecutables y/o herramientas que atenten contra la integridad, disponibilidad y/o confidencialidad de la infraestructura tecnológica (hacking), entre otros.

o La descarga, uso, intercambio y/o instalación de información audiovisual (videos e imágenes) utilizando sitios públicos en Internet debe ser autorizada por el Líder respectivo y la Líder de los estándares de

Gerencia de la Información, o a quienes ellos deleguen de forma explícita para esta función, asociando los procedimientos y controles necesarios para el monitoreo y aseguramiento del buen uso del recurso.

 La ESE debe realizar monitoreo permanente de tiempos de navegación y páginas visitadas por parte de los funcionarios, contratistas y/o terceros. Así mismo, puede inspeccionar, registrar y evaluar las actividades realizadas durante la navegación, de acuerdo a la legislación nacional vigente.

 Cada uno de los usuarios es responsable de dar un uso adecuado a este recurso y en ningún momento puede ser usado para realizar prácticas ilícitas o mal intencionadas que atenten contra terceros, la legislación vigente y los lineamientos de seguridad de la información, entre otros.

 Los funcionarios, contratistas y terceros, al igual que los empleados o subcontratistas de estos, no pueden asumir en nombre del Hospital, posiciones personales en encuestas de opinión, foros u otros medios de comunicación externos similares.

 El uso de Internet no considerado dentro de las restricciones anteriores, es permitido siempre y cuando se realice de manera ética, razonable, responsable, no abusiva y sin afectar la productividad ni la protección de la información de la ESE.

6.1.2 Correo electrónico:

 El correo electrónico corporativo es una herramienta de comunicación o intercambio de información oficial entre personal o instituciones, no es una herramienta de difusión indiscriminada de información.

 La cuenta de correo electrónico debe ser usada para el desempeño de las funciones asignadas dentro de la ESE.

 Los mensajes y la información contenida en los buzones de correo son propiedad de la ESE y cada usuario, como responsable de su buzón, debe

mantener solamente los mensajes relacionados con el desarrollo de sus funciones.

El tamaño de envío y recepción de mensajes, sus contenidos y demás características propios de estos deberán ser definidos e implementados por el área de Sistemas de la ESE.

 El envío de información corporativa debe ser realizado exclusivamente desde la cuenta de correo que la ESE proporciona. De igual manera, las cuentas de correo genéricas no se deben emplear para uso personal dentro de la institución.

 Toda información de la ESE generada con los diferentes programas computacionales (Office, Project, Access, Wordpad, ect.), que requiera ser enviada fuera de la entidad, y que por sus características de confidencialidad e integridad deba ser protegida, debe estar en formatos no editables, utilizando las características de seguridad que brindan las herramientas proporcionadas por el área de Sistemas. La información puede ser enviada en el formato original bajo la responsabilidad del usuario y únicamente cuando el receptor requiera hacer modificaciones a dicha información.

 Todos los mensajes enviados deben respetar el estándar de formato e imagen corporativa definido por la ESE y deben conservar en todos los casos el mensaje legar corporativo de confidencialidad.

 Los archivos que se adjuntan en los mensajes de correo en lo posible deben comprimirse para evitar la saturación en las diferentes cuentas de correos.

 El usuario que tiene asignada una cuenta de correo electrónico es el único y directo responsable de todas las acciones y mensajes que se lleven a cabo en su nombre, por lo tanto el Hospital no se hace responsable por lo que diga o haga. Esta información se incluirá en todos los mensajes que se envíen.
 El correo electrónico corporativo es la única vía de remisión o envío de documentos de carácter administrativo interno en el hospital.
se cuenta con un total de 20 cuentas de correo institucional para los principales procesos, los demás que se crean son manejados a través de una cuenta de gmail creadas por el administrador del sistema.

No está permitido:

 Enviar cadenas de correo, mensajes con contenido religioso, político, racista, sexista, pornográfico, publicitario no corporativo o cualquier otro tipo de mensajes que atenten contra la dignidad y la productividad de las personas o el normal desempeño del servicio de correo electrónico en la Institución, mensajes mal intencionados que puedan afectar los sistemas internos o de terceros, mensajes que vayan en contra de las leyes, la moral y las buenas costumbres y mensajes que inciten a realizar prácticas ilícitas o promuevan actividades ilegales.

 Utilizar la dirección de correo electrónico de la ESE como punto de contacto en comunidades interactivas de contacto social, tales como Facebook, Instagram, entre otras, o cualquier otro sitio que no tenga que ver con las actividades laborales.

6.1.3 Recursos tecnológicos:

 La instalación de cualquier tipo de software o hardware en los equipos de cómputo se la ESE es responsabilidad del área de Sistemas, y por tanto son los únicos autorizados para realizar esta labor. Así mismo, los medios de instalación de software deben ser los proporcionados por esta área.

 Los usuarios no deben realizar cambios en las estaciones de trabajo relacionados con la configuración del equipo, tales como conexiones de red, usuarios locales de la máquina, papel tapiz y protector de pantalla corporativo, entre otros. Estos cambios son realizados únicamente por el área de Sistemas.

 El área de Sistemas definirá y actualizará, de manera periódica, la lista de software y aplicaciones de trabajo de los usuarios. Así mismo, realizar el control y verificación de cumplimiento del licenciamiento del respectivo software y aplicaciones instaladas y administradas por el Hospital.

 Los funcionarios serán conectados a la red de a ESE con previa solicitud escrita y autorizada por el Líder del área. Los terceros y/o contratistas se conectarán a la red, bajo los lineamientos del área de Sistemas.

 Los usuarios que requieren acceder a la infraestructura tecnológica dela ESE desde redes externas, deben utilizar una conexión bajo los esquemas y herramientas de seguridad autorizados y establecidos por el área de Sistemas. Además, deberán informar previamente a la misma área para autorizar el acceso y brindar los permisos respectivos para la protección de la información, de acuerdo a lo definido por el área de sistemas.

 La sincronización de dispositivos móviles, tales como PDAs, smartphones, celulares u otros dispositivos electrónicos sobre los que se puedan realizar intercambios de información con cualquier recurso de la Organización, debe ser autorizado de forma explícita por el líder de la dependencia respectiva

 Las estaciones de trabajo y en general cualquier recurso de la organización no debe ser empleado para actividades recreativas, entre otras, jugar o grabar música.

 Ningún funcionario contratista o tercero podrá copiar para uso personal archivos o programas de propios del Hospital.

6.1.4 Seguridad de los talento humano

 Todos los funcionarios de la ESE, contratistas y terceros que tengan la posibilidad de acceder a la información de la organización y a la infraestructura para su procesamiento, son responsables de conocer y cumplir con las políticas y procedimientos establecidos en el Modelo de Gestión de Seguridad de la Información de la ESE. De igual forma, son responsables de reportar por medio de los canales apropiados, el incumplimiento de las políticas y procedimientos establecidos.

 Todos los funcionarios deben ser cuidadosos de no divulgar información confidencial en lugares públicos, en conversaciones o situaciones que pongan en riesgo la seguridad y el buen nombre de la organización.

6.2 PLAN SEGURO PARA EL ACOPIO DE COPIAS DE SEGURIDAD

Se debe tener en cuenta que la entidad puede sufrir un incidente que afecte su continuidad y, dependiendo de la forma en que se gestionen dichos incidentes, las consecuencias pueden ser más o menos graves. Debemos tener en cuenta que la información requiere ser protegida y se debe trabajar sobre los tres pilares fundamentales: confidencialidad, integridad y disponibilidad.

Una de las principales características que debe poseer la entidad es buscar cómo establecer un Sistema de seguridad enfocado por procesos, resaltando la importancia que tienen las actividades de monitoreo y la correcta configuración para disminuir los riesgos y realizar tratamiento de las diferentes y constantes vulnerabilidades, para lo cual se deberán tener en cuenta los hallazgos y recomendaciones identificadas, cuyo propósito se encamine a mitigar los riesgos encontrados.

Se deben tener las siguientes opciones para dar mayor seguridad y accesibilidad a la información:

Adquirir un sistema de almacenamiento interno donde se pueda acceder más fácilmente de forma rápida y segura (disco duro conectado a la red).

Obtener una nube dedicada a la información compartida por los procesos y para tener un respaldo de información compartida y generada por el servidor.

6.3 PLAN DE CONTINUIDAD DEL NEGOCIO

- Socializar con la alta gerencia y los líderes de procesos la importancia del Plan de Continuidad de Negocio, para hacer frente a incidentes graves de seguridad en la Entidad, resumiendo de forma clara y sencilla cada una de las actividades a desarrollar dentro del plan.
- Tener una lista de chequeo para realizar auditorías periódicas con la finalidad de verificar los controles que se manejan en la entidad están siendo efectivos.
- Adoptar enfoques que nos puedan minimizar las ocurrencias o efectos colaterales sobre la red

- Diseñar un Plan de Contingencia teniendo en cuenta que la continuidad en el negocio dependerá de los riesgos y amenazas potenciales.

6.4 IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD PARA LA INFORMACIÓN

El análisis permitió identificar que se desconocen y poco se cumplen las políticas de seguridad dentro de la institución; por lo cual debe quedar integrado con el documento actual. Se recomienda entre otros tener en cuenta:

- Socializar y capacitar al personal frente al tema de seguridad de la información.
- Tener un ambiente de seguridad adecuada en la institución.
- Sistema de respaldo para mantener un soporte de la información más relevante en casa de eventuales catástrofes naturales o humanas.

6.5 PLAN DE CAPACITACION

Contar con un plan de capacitación para el personal encargado de la seguridad de la información, aspectos a fortalecer como:

- Detectar requerimientos tecnológicos.
- Determinar objetivos de capacitación para el personal.
- Evaluar resultados de las evaluaciones y monitorear el sistema de seguridad.
- Elaborar un programa de capacitación en temas de ciberseguridad y políticas de seguridad de la información para todos los funcionarios de la entidad.
- Evaluar resultados de cada actividad.

6.6 PLAN DE TRANSICIÓN DE IPV4 A IPV6

Se debe establecer un plan para hacer la transición de las direcciones IPv4 existente actualmente por la IPv6 debido a que algunos equipos informáticos del

Hospital Roberto Quintero Villa ESE Montenegro no soportan la nueva versión de IP.

7 MECANISMOS DE SEGUIMIENTO Y VERIFICACIÓN

Los atributos establecidos para valorar el desempeño de la gestión de riesgos es una parte de la evaluación global de la institución y de la medición del desempeño de las áreas y de las personas.

Por lo menos cada responsable de proceso realizará una autoevaluación a la gestión del riesgo, determinando la efectividad de sus controles para minimizar el riesgo, a su vez la Oficina de Control Interno realizará su propio informe de evaluación de riesgos y controles de segundo orden.

JORGE IVAN MEJIA VILLANUEVA

Ingeniero de sistemas

BIBLIOGRAFÍA

Guía 7 gestión de riegos. Modelo de Seguridad y Privacidad de la Información. Ministerio de Tecnologías de la Información y las Comunicaciones, estrategia de Gobierno en Línea.

Guía 8 controles de seguridad y privacidad de la información. Modelo de Seguridad y Privacidad de la Información. Ministerio de Tecnologías de la Información y las Comunicaciones, estrategia de Gobierno en Línea