PLAN DE TRATAMIENTO DE RIESGO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

ÁREA DE SISTEMAS

E.S.E HOSPITAL SAN RAFAEL

2024

Calle 16 Nº 5ª - 46 Salida a Valledupar
Teléfono: 4140124
Código Postal: 472020

ESE Hospital San Rafael Fundación
@ESESANRAFAEL
esehospitalsanrafael

TABLA DE CONTENIDO

INTRODUCCIÓN 3

OBJETIVOS 3

MARCO REFERENCIAL 3

RESPONSABLES 3

ALCANCE 4

DOCUMENTOS DE REFERENCIA 4

GLOSARIO 4

ACTIVOS DE INFORMACIÓN 7

PLAN SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 7

EVALUACIÓN DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 7

MONITOREO DE CONTROLES DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 8

POLÍTICAS 8

- POLÍTICAS DE LA ORGANIZACIÓN 8
- POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN 9
- RESPONSABILIDADES DEL TRABAJADOR 10

1. INTRODUCCIÓN

La E.S.E Hospital San Rafael de Fundación en la búsqueda de la evolución continua digital desea implementar un método lógico y sistemático que permita identificar, analizar, evaluar y monitorear los riesgos asociados al manejo de la información institucional.

Adaptando las necesidades conforme al marco ISO 27001: 2013 para la Política de seguridad y privacidad de la información, en la protección de los datos de la información y los activos, atender las amenazas de forma inmediata y mejoramientos continuos.

2. OBJETIVOS

Brindar al E.S.E Hospital San Rafael de Fundación un guía que proporcione unos planes adecuados para el tratamiento de los riesgos informáticos, responsabilidades de los usuarios con cada activo de información con el fin de minimizar la probabilidad que se materialice una amenaza y posible impacto en la Entidad.

3. MARCO REFERENCIAL

NTC / ISO 27001:2013, Estándar para la seguridad de la información, describe cómo gestionar la seguridad de la información en una empresa.

NTC/ISO 31000:2009, Gestión del Riesgo. Principios y directrices.

4. RESPONSABLES

GERENCIA: Autoriza los esquemas informáticos implantado en la organización.

INGENIERO DE SISTEMAS: responsable del cuidado, vigilancia y verificación de los recursos informáticos.

COORDINADORA DE CALIDAD: Supervisa la ejecución del cuidado, vigilancia y verificación de los recursos informáticos.

5. ALCANCE

Este Manual aplica para todo el personal que se encuentra laborando en el E.S.E Hospital San Rafael de Fundación.

6. DOCUMENTOS DE REFERENCIA

IEC- ISO 2007:2005- SISTEMA DE GESTIÓN INFORMÁTICA – VOCABULARIOS

7. GLOSARIO

Activo: Según [ISO13335]: Cualquier cosa que tiene valor para la organización. También se entiende por cualquier información o sistema relacionado con el tratamiento de esta que tenga valor para la organización. Es todo activo que contiene información, la cual posee un valor y es necesaria para realizar los procesos misionales y operativos.

Almacenamiento: propiedad o capacidad de guardar datos que tiene un dispositivo electrónico. Computadoras, teléfonos celulares, tabletas, televisores y demás dispositivos electrónicos tienen esta propiedad, la cual es muy útil no sólo para guardar datos sino para procesarlos.

Carpeta o recurso compartido: Los recursos compartidos son recursos creados por defecto en la red en todos los sistemas basados en la Tecnología Windows. Estos recursos por defecto comparten cada unidad de disco en el sistema.

Comunicación De La Información: Conjunto de técnicas que permiten la difusión de mensajes escritos o audiovisuales de un informe a una audiencia.

Confidencialidad: Es la propiedad de la información, por la que se garantiza que está accesible únicamente a personal autorizado a acceder a dicha información

Cookies: Las cookies son pequeños archivos usados por los sitios web para almacenar información en tu equipo (como información para iniciar sesión automáticamente y las preferencias de un sitio).

Descarga: se utilizan para referirse a la transferencia de archivos informáticos a un aparato electrónico a través de un canal de comunicación. El término descarga se utiliza frecuentemente para la obtención de contenido a través de una conexión a Internet, donde un servidor remoto recibe los datos que son accedidos por los clientes a través de aplicaciones específicas, tales como navegadores.

Dispositivo electrónico: Un aparato electrónico consiste en una combinación de componentes electrónicos organizados en circuitos, destinados a controlar y aprovechar las señales eléctricas.

Equipo de cómputo: El equipo de cómputo se refiere a los mecanismos y al material de computación que está adjunto a él

Equipo de red: Es el dispositivo que conecta la estación (ordenador u otro equipo de red) con el medio físico

Hardware: Conjunto de elementos físicos o materiales que constituyen una computadora o un sistema informático.

Internet: Red informática de nivel mundial que utiliza la línea telefónica para transmitir la información.

Licencia de software: contrato entre el licenciante (autor/titular de los derechos de explotación/distribuidor) y el licenciatario (usuario consumidor/usuario profesional o empresa) del programa informático, para utilizar el software cumpliendo una serie de términos y condiciones establecidas dentro de sus cláusulas

Manual: Documento que contiene las instrucciones a utilizar en seguridad de la información.

Multimedia: Que está destinado a la difusión por varios medios de comunicación combinados, como texto, fotografías, imágenes de video o sonido, generalmente con el propósito de educar o de entretener.

Navegador: Programa que permite navegar por internet u otra red informática de comunicaciones.

Ofimáticos: Conjunto de materiales y programas informáticos que se aplican al trabajo de oficina

Perfiles de usuario: Es una colección de opciones de configuración que hacen que el equipo tenga el aspecto y funcione de la manera que usted desee. Contiene la configuración para fondos de escritorio, protectores de pantalla, preferencias de puntero, configuración de sonido y otras características

Periféricos: Unidad de una computadora que no forma parte de su unidad central.

Política: La política de seguridad es un documento de alto nivel que denota el compromiso de la gerencia con la seguridad de la información. Contiene la definición de la seguridad de la información desde el punto de vista de cierta entidad.

Red corporativa: la red corporativa permite conectar todas las localizaciones de la empresa de una forma permanente, privada, segura y fiable a través de la fibra óptica de R y mediante la tecnología MPLS. El producto red corporativa es una red privada virtual MPLS que permite a la empresa cursar todas sus comunicaciones, ya sean datos, voz, vídeo o imágenes, de un modo rápido, seguro y totalmente gestionado por la red IP/MPLS de R está preparada para dar “calidad de servicio”

Seguridad de la información: La seguridad de la información es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de esta.

Software: Conjunto de programas y rutinas que permiten a la computadora realizar determinadas tareas.

Usuario: Que tiene el derecho de usar de una cosa ajena con unas limitaciones determinadas.

Virus: Programa de computadora confeccionado en el anonimato que tiene la capacidad de reproducirse y transmitirse independientemente de la voluntad del operador y que causa alteraciones más o menos graves en el funcionamiento de la computadora.

8. ACTIVOS DE INFORMACIÓN

En la búsqueda de un sistema de gestión sostenible de la seguridad y privacidad de la información se parte de 4 fases, en esta primera se llevará a cabo un levantamiento de información que nos ayude a tener claro todos los activos de equipos hardware y software de la Entidad, pasarlos a una clasificación por importancia, área, riesgo y cualquier otro dato necesario, por último, se socializará el documento final con la alta gerencia.

9. PLAN SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

En esta fase se hará la identificación de los riesgos dentro de las áreas administrativas, que afecten tanto los equipos, como las redes y gestores de información. Implementar rutas de mejoras y socialización del tratado de los riesgos con la alta gerencia.

10. EVALUACIÓN DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Para la evaluación de riesgos, se hará controles según el análisis y evaluación de los riesgos encontrados en la fase anterior, validar los resueltos y analizarlos conforme a la aplicación del plan de seguridad. Se procede con la priorización de las medidas, definir los responsables de cada uno de los riesgos, las acciones que

deben realizar y las que no, objetivos para cada conflicto o resolución de riesgos y por ultimo las actividades para resolución y prevención de riesgos.

11. MONITOREO DE CONTROLES DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

En esta última fase realizaremos la identificación de las funciones de la Entidad en materia de seguridad de la información, el área de Sistemas se encargará de la gestión de riesgos junto con las oficinas de Subgerencia Administrativa, Planeación, Calidad, Archivo y estadística, encontrados y se definirá las funciones del área para la aplicaciones y gestión de las medidas.

12. POLÍTICAS

Podemos definir Política de Seguridad, como el conjunto de normas y procedimientos establecidos por una organización para regular el uso de la información y de los sistemas que la tratan con el fin de mitigar el riesgo de pérdida, deterioro o acceso no autorizado a la misma.

Políticas de la organización

- Los usuarios no harán parte de los grupos de administrador (ni de server ni locales).
- Se solicitará cambio de contraseñas a los usuarios cada 90 días.
- Se Implementarán cierres automáticos de sesiones abiertas que tengan inactividad de más de 20 minutos, con reinicio de sesión protegido con la contraseña del usuario autenticado.
- Se mantendrán activas las actualizaciones automáticas para poder recibir los parches de seguridad automáticamente cada que estén disponibles.
- El navegador estará configurado para que borre regularmente las cookies.
- Durante los mantenimientos se hará borrado de archivos temporales del sistema operativo y temporales de Internet, descargas e historial de navegación.

- Se implementarán nuevas políticas de navegación con perfiles restringidos, para la activación de permisos especiales se debe hacer el requerimiento a través de la gerencia general.
- Se hará una restricción de funcionalidades de los puertos de acceso a dispositivos de almacenamiento extraíbles (CD, USB, SD Card, etc.).
- Se replanteará el acceso a carpetas o recursos compartidos en la red local de acuerdo con las áreas y los diferentes perfiles.
- Se restringe el acceso de los dispositivos móviles a la red corporativa
- No se proporcionará ningún tipo de acceso a terceros a la red corporativa.
- Llevar un adecuado control en usuarios y perfiles, estos deben ser personalizados y de uso restringido al funcionario asignado (debe prohibirse el uso de usuarios y claves por parte de personas diferentes a la que asignaron).
- Cumplir con todas las disposiciones determinadas en el manual

Políticas de seguridad de la información.

Mantener una infraestructura tecnológica, soportada en plataformas apropiadas, protegiendo los mecanismos de tratamiento, almacenamiento y comunicación de la información.

Contar con personal competente y comprometido con una cultura de seguridad de la información, generada a través de capacitaciones periódicas al personal, garantizando la aceptación y aplicación de las directrices establecidas.

Así mismo garantiza que:

La información que se administra internamente, es utilizada con fines empresariales; Las herramientas y servicios informáticos asignados a cada usuario, son para uso limitado a la función empresarial; La información digital o digitalizada correspondiente al sistema de información Contable, de Cartera, Facturación e Inventarios y Gestión Humana, las bases de datos de los correos electrónicos corporativos y los archivos ofimáticos de la empresa cuentan con copias de respaldo para garantizar su seguridad.

Los lugares donde se encuentran ubicados los activos asociados al sistema de procesamiento de la información se consideran áreas de acceso restringido, por tal motivo el ingreso y permanencia a estas áreas es controlado y supervisado por el departamento de sistemas.

El acceso no autorizado a los sistemas de información y uso indebido de los recursos informáticos de la empresa está prohibido. Se considera que hay uso indebido de la información y de los recursos, cuando la persona incurre en cualquiera de las siguientes conductas:

Sera Responsabilidades del trabajador

- Suministrar la información a quien no tiene derecho a conocerla.
- Usar la información con el fin de obtener beneficio propio o de terceros.
- Ocultar la información maliciosamente causando cualquier perjuicio.
- Hacer pública la información sin la debida autorización.
- Hurtar software de propiedad de, o licenciado a nombre del E.S.E Hospital San Rafael de Fundación, [copia o reproducción entre usuarios finales].
- Realizar copias no autorizadas de software de propiedad o licenciado a nombre del E.S.E Hospital San Rafael de Fundación dentro y fuera de sus instalaciones.
- Falsificar y duplicar formatos o productos informáticos de propiedad del E.S.E Hospital San Rafael de Fundación.
- Descargar software, a través de Internet sin la debida autorización.
- Intentar modificar, reubicar o sustraer equipos de cómputo o periféricos, software y/o información sin la debida autorización.
- Capturar sin autorización la información de los accesos de otros usuarios a los sistemas.
- Transgredir o burlar los mecanismos de autenticación u otros sistemas de seguridad.
- Utilizar la infraestructura tecnológica del E.S.E Hospital San Rafael de Fundación, [computadores, software, información o redes] para acceder a recursos externos con propósitos ilegales o no autorizados.
- Enviar cualquier comunicación electrónica fraudulenta.

- Adueñarse del trabajo de otros individuos, o de alguna manera apropiarse del trabajo ajeno.
- Usar cualquier medio para dañar o perjudicar de alguna manera los recursos disponibles electrónicamente.
- Lanzar cualquier tipo de virus, gusano, troyano o programa de computador cuya intención sea hostil o destructiva.
- Descargar o publicar material ilegal, con derechos de propiedad o material nocivo usando un recurso del E.S.E Hospital San Rafael de Fundación.
- Descargar o reproducir material multimedia [imágenes, audio, video y animaciones] sin la autorización del Coordinador del área de Informática.
- Uso personal de cualquier recurso informático del E.S.E Hospital San Rafael de Fundación, para acceder, descargar, imprimir, almacenar, redirigir, transmitir o distribuir material pornográfico.

Violar cualquier Ley o Regulación nacional respecto al uso de sistemas de información.