Política de Seguridad y privacidad de la información

ENERO 2020

Tabla de contenido

INTRODUCCIÓN.

La ESE Hospital San José de La Palma clasifica a la información como un activo de alto valor para la misma, por lo cual se hace necesario definir un sistema de gestión de seguridad de la información que permita garantizar la integridad, confidencialidad y disponibilidad de la información, contra las amenazas constantes y cada vez mayores, que se tienen por la masificación de las nuevas tecnologías, y el aumento de uso fraudulento y desordenado que se tiene, en el conglomerado del estado.

Como acción preponderante se realiza un diagnóstico del estado actual de la entidad en materia de seguridad de la información y las necesidades de la institución en esta materia, lo que permite identificar de primera mano las fortalezas y debilidades que se tienen arrojando como primera Tarea el establecimiento de una política general de seguridad de la información, la cual resume el compromiso de la administración con la implementación de un sistema de gestión de seguridad de la información.

En este documento se define la política general de seguridad y privacidad de la información para el ESE Hospital San José de La Palma, la cual se definió teniendo en cuenta el contexto particular de la institución y las necesidades y regulaciones en esta materia.

1. OBJETIVOS.

Establecer los lineamientos que le permitan al ESE Hospital San José de La Palma, proteger la información y los sistemas de información ante cualquier amenaza que pueda comprometer la disponibilidad, integridad y confidencialidad de la información recolectada, procesada o almacenada por la entidad.

Fomentar en los funcionarios, usuarios y colaboradores de la entidad una cultura de seguridad de la información, que les permita tomar conciencia de sus deberes y responsabilidades frente a la gestión de seguridad de la información, así como de sus beneficios.

Minimizar los incidentes relacionados con seguridad de la información, que afecten el normal funcionamiento de la ESE Hospital San José de La Palma.

Desarrollar un sistema de gestión de riesgos de seguridad de la información que permita generar controles que ayuden a reducir los impactos negativos de los incidentes de seguridad.

2. ALCANCE.

Esta política aplica a toda la entidad, sus funcionarios, contratistas y terceros del ESE Hospital San José de La Palma y la ciudadanía en general.

3. TERMINOS Y DEFINICIONES.

Colaborador: Empleado, contratista, practicante, proveedor y en general cualquier persona que tenga acceso a información del Ministerio de Cultura y tenga un vínculo contractual con el mismo.

Criptografía: Arte o técnica de escribir con clave secreta o de un modo enigmático.

Política: Declaración de alto nivel que describe la posición de la entidad sobre un tema específico.

Procedimiento: Documento que describe la forma específica de llevar a cabo a una actividad o un proceso.

Proceso: Conjunto de actividades mutuamente relacionadas o que interactúan para generar valor y las cuales transforman elementos de entrada en resultados.

Seguridad de la Información: Preservación de la confidencialidad, disponibilidad e integridad de la información (ISO/IEC 27000) independiente de su medio de conservación, transmisión o formato.

Sistema de Gestión de Seguridad de la Información (SGSI): Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

4. MARCO NORMATIVO.

La política de seguridad de la información se encuentra regulada por las siguientes normas

Decreto 2573 de 2014 “Por el cual se establecen los lineamientos generales de la estrategia de gobierno en línea”

Ley Estatutaria 1581 de 2012 “Por la cual se dictan disposiciones generales para la protección de datos personales”

Ley 1915 de 2018 ““Por la cual se modifica la ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos"

Norma Técnica colombiana ISO/IEC 27001 Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un sistema de gestión de la seguridad de la información (SGSI).

5. POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La dirección del ESE Hospital San José de La Palma, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con el

Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad.

Para El ESE Hospital San José de La Palma, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés identificados.

De acuerdo con lo anterior, esta política aplica a la Entidad según como se defina en el alcance, sus funcionarios, terceros, aprendices, practicantes, proveedores y la ciudadanía en general, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del SGSI estarán determinadas por las siguientes premisas:

- Minimizar el riesgo en las funciones más importantes de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de sus usuarios, socios y empleados.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y usuarios del ESE Hospital San José de La Palma
- Garantizar la continuidad del negocio frente a incidentes.

A continuación, mencionamos las políticas específicas que soporten la declaración de la política general.

6. POLITICAS ESPECIFICAS DE SEGURIDAD DE LA INFORMACIÓN

6.1. Recursos tecnológicos.

El uso de los recursos tecnológicos con los que cuenta la entidad y que son asignados a funcionarios del hospital o a tercero estarán sujetos a las siguientes políticas.

- La instalación de cualquier tipo de software o hardware en los equipos de cómputo del ESE Hospital San José de La Palma es responsabilidad del área de tecnología, y por tanto son los únicos autorizados para realizar esta labor. Así mismo, los medios de instalación de software deben ser los proporcionados por el ESE Hospital San José de La Palma a través de 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, entre otros. Estos cambios pueden ser realizados únicamente por el área de TI del Hospital.

- Únicamente los funcionarios y terceros autorizados por el área de TI, previa solicitud por parte de la dependencia que lo requiera, pueden conectarse a la red inalámbrica del ESE Hospital San José de La Palma.

- Sólo personal autorizado puede realizar actividades de administración remota de dispositivos, equipos o servidores de la infraestructura de procesamiento de información del ESE Hospital San José de La Palma. las conexiones establecidas para este fin, deben utilizar los esquemas y herramientas de seguridad y administración definidos por el área de TI.

6.2 Seguridad Del recurso Humano.

Identificado como el eslabón más débil en la cadena de seguridad de la información se deben definir unas políticas particulares que permitan minimizar la ocurrencia de incidentes de seguridad de la información debidos a el recurso humano.

- La entidad debe asegurarse de que los funcionarios y colaboradores entienden sus responsabilidades y están capacitados para el desempeño de sus funciones.

- En los acuerdos contractuales se deben establecer las responsabilidades y obligaciones de los colaboradores para con la entidad en materia de seguridad de la información.

- Debe existir un compromiso de la dirección que exija a los colaboradores cumplir con las políticas en materia de seguridad de la información.

- Es importante desarrollar un plan de sensibilización de los funcionarios con respecto a las bondades de la implementación de un sistema de seguridad de la información, donde se muestren los lineamientos generales y los controles adoptados, pero se haga énfasis en los beneficios del SGSI y las consecuencias negativas de ignorar las responsabilidades en materia de seguridad de la información.

- Todos los funcionarios del ESE Hospital San José de La Palma y/o terceros deben aceptar los acuerdos de confidencialidad definidos por la Institución, los cuales reflejan los compromisos de protección y buen uso de la información de acuerdo con los criterios establecidos en ella.

- Para el caso de contratistas, los respectivos contratos deben incluir una cláusula de confidencialidad, de igual manera cuando se permita el acceso a la información y/o a los recursos del ESE Hospital San José de La Palma a personas o entidades externas.

- Estos acuerdos deben aceptarse por cada uno de ellos como parte del proceso de contratación, razón por la cual dicha cláusula y/o acuerdo de confidencialidad hace parte integral de cada uno de los contratos

.

6.3 Control de Acceso:

Se deben desarrollar políticas que permitan establecer los permisos de acceso a la información y a los sistemas encargados de su captura, procesamiento y almacenamiento, de tal forma que se establezca mantenga y actualice la información de permisos de acceso, su administración gestión y los procedimientos de otorgamiento y remoción de permisos.

- Se deben implementar mecanismos de autenticación acordes que permitan el acceso seguro a los sistemas y aplicaciones. Las credenciales de acceso son responsabilidad de los funcionarios, los cuales deben mantenerlas en secreto, deben ser de uso personal y exclusivo.

- Cualquier usuario interno o externo que requiera acceso remoto a la red y a la infraestructura de procesamiento de información del Hospital sea por Internet, acceso telefónico o por otro medio, siempre debe estar autenticado y sus conexiones deberán utilizar cifrado de datos.

- El acceso a plataformas, aplicaciones, servicios y en general cualquier recurso de información del hospital debe ser asignado de acuerdo a la identificación previa de requerimientos de seguridad y del negocio que se definan por las diferentes dependencias de la Institución, así como normas legales o leyes aplicables a la protección de acceso a la información presente en los sistemas de información.

6.4 Seguridad física y del entorno.

Se deben establecer controles que prevengan el acceso no autorizado a los lugares de procesamiento de información de la ESE Hospital San José de La Palma (datacenters).

- Se deben implementar protecciones físicas contra desastres naturales, ataques maliciosos o accidentes, con el fin de evitar daños por incendios, inundaciones, terremotos, disturbios civiles.

- Se deben implementar controles con el fin de evitar pérdidas, daños o robos de la infraestructura de TI, por lo que los equipos deben estar ubicados en lugares seguros con controles de acceso adecuados, protegidos contra fallas de la energía, y cualquier servicio que pueda afectar de manera física los equipos. El cableado eléctrico y de datos debe estar debidamente protegido contra interceptación interferencia o daños.

6.5. Gestión de medios removibles.

- El uso de medios de almacenamiento removibles (ejemplo: CDs, DVDs, USBs, memorias flash, discos duros externos, Ipods, celulares, cintas) sobre la infraestructura para el procesamiento de la información del ESE Hospital San José de La Palma, estará autorizado para aquellos funcionarios cuyo perfil del cargo y funciones lo requiera.

- El área de TI es responsable de implementar los controles necesarios para asegurar que en los sistemas de información del ESE Hospital San José de La Palma sólo los funcionarios autorizados pueden hacer uso de los medios de almacenamiento removibles.

6.6. Seguridad de las Operaciones

- Se debe realizar un control de cambios en los procesos, organización, instalaciones y sistemas de procesamiento de información que afecten la seguridad de la información.

- El hospital debe implementar controles que permitan la detección, prevención de códigos maliciosos, sumado a la sensibilización de todos los colaboradores para proteger los sistemas informáticos y la información del hospital.

- Se debe asegurar la operación de las instalaciones de procesamiento de información, los procedimientos de operación deben documentarse y quedar a disposición de los usuarios que lo requieran.

- La ESE Hospital San José de La Palma debe realizar copias de seguridad de la información, software e imágenes del sistema, estas copias deben ser probadas periódicamente para comprobar su utilidad, esto de acuerdo a una política establecida de copias de seguridad.

- Se debe controlar las instalaciones y actualizaciones de aplicaciones dentro de los servidores de la entidad.

- Se debe mantener constante supervisión de las vulnerabilidades de los sistemas de información que use la entidad, evaluar la exposición de la entidad a las amenazas que pueden aprovechar estas vulnerabilidades e implementar los controles necesarios para mitigar estas vulnerabilidades.

- El hospital debe controlar la instalación de software en las estaciones de trabajo de los funcionarios, estableciendo que solamente los encargados del área de TI pueden instalar aplicaciones, respetando las normativas en cuanto a licenciamiento y derechos de autor.

6.7 Seguridad de las comunicaciones

- Se debe establecer niveles de seguridad para la información en las redes y las instalaciones de procesamiento de información y hacer cumplir los acuerdos de confidencialidad y de no divulgación del ESE Hospital San José de La Palma.

6.8. Adquisición, desarrollo y mantenimiento de sistemas

- Los sistemas de información deben incluir la seguridad de la información, esto como requisito para la adquisición de nuevos sistemas de información, así como para las futuras actualizaciones de los sistemas de información con los que ya cuenta el hospital.

6.9. Relaciones con los proveedores

- Se deben establecer requisitos de seguridad de la información que permitan mitigar los riesgos para los activos de información a los que tengan acceso o suministren los proveedores

- La prestación de servicios por parte de proveedores debe estar supervisada, revisada y auditada en cuanto a los requisitos de la seguridad de la información.

6.10. Gestión de incidentes de seguridad de la información

- Es necesario establecer las responsabilidades y procedimientos para una respuesta eficaz y eficiente a incidentes de seguridad de la información.

- Los funcionarios deben reportar al área de TI cualquier incidente o sospecha de incidente de seguridad de la información, inmediatamente tengan conocimiento de este.

- Se deben definir los procedimientos post-incidentes con el fin de recolectar y preservar la información de los incidentes que puedan servir como evidencia.

- Es necesario definir un procedimiento que permita recolectar y documentar las experiencias y conocimientos adquiridos durante la respuesta a incidentes con el fin de tomar las acciones pertinentes de mejoramiento de controles y procesos de respuesta a incidentes.

6.11. Continuidad de negocio

- Se deben establecer lineamientos de continuidad de negocio y recuperación ante desastres, la cual debe contener los procesos, procedimientos, controles y requisitos para garantizar la continuidad de negocio en condiciones adversas garantizando los estándares de seguridad de la información.

- Se debe verificar periódicamente que los procedimientos y controles relacionados con continuidad de negocio funcionan de acuerdo a lo planeado.

- Para garantizar la continuidad de negocio y la recuperación ante desastres se debe implementar redundancia de los sistemas de procesamiento de información.

6.12. Acceso a internet.

El internet es una herramienta de trabajo que permite navegar en muchos otros sitios relacionados o no con las actividades propias del negocio de ESE Hospital San José de La Palma, por lo cual el uso adecuado de este recurso se debe controlar, verificar y monitorear, considerando, para todos los casos, los siguientes lineamientos:

NO está permitido:

- 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.

- El intercambio no autorizado de información de propiedad del ESE Hospital San José de La Palma, de sus clientes y/o de sus funcionarios, con terceros.

- 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. La descarga, uso, intercambio y/o instalación de información audiovisual (videos e imágenes) utilizando sitios públicos en Internet debe ser autorizada por el jefe respectivo y la Dirección de Tecnología, 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.

El ESE Hospital San José de La Palma debe realizar monitoreo permanente de tiempos de navegación y páginas visitadas por parte de los funcionarios 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 y terceros, al igual que los empleados o subcontratistas de estos, no pueden asumir en nombre del ESE Hospital San José de La Palma, posiciones personales en encuestas de opinión, foros u otros medios 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 ESE Hospital San José de La Palma.

6.13 Uso del Correo Electrónico.

Los funcionarios y terceros autorizados a quienes El ESE Hospital San José de La Palma les asigne una cuenta de correo deberán seguir los siguientes lineamientos:

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 del ESE Hospital San José de La Palma como punto de contacto en comunidades interactivas de contacto social,

tales como Facebook y/o MySpace, entre otras, o cualquier otro sitio que no tenga que ver con las actividades laborales.

- El envío de archivos que contengan extensiones ejecutables, bajo ninguna circunstancia

- El envío de archivos de música y videos. En caso de requerir hacer un envío de este tipo de archivos deberá ser autorizado por la dirección respectiva y el área de Tecnología.

La cuenta de correo electrónico debe ser usada para el desempeño de las funciones asignadas dentro del ESE Hospital San José de La Palma así mismo podrá ser utilizada para uso personal, siempre y cuando se realice de manera ética, razonable, responsable, no abusiva y sin afectar la productividad.

Los mensajes y la información contenida en los buzones de correo son propiedad del ESE Hospital San José de La Palma, y cada usuario, como responsable de su buzón, debe mantener solamente los mensajes relacionados con el desarrollo de sus funciones.

El tamaño de los buzones de correo es determinado por el área de TI de acuerdo con las restricciones del servicio de Hosting, establecidas de acuerdo a los criterios de presupuesto de la institución.

El envío de información corporativa debe ser realizado exclusivamente desde la cuenta de correo que el ESE Hospital San José de La Palma proporciona. De igual manera, las cuentas de correo genéricas no se deben emplear para uso personal.

Toda información del ESE Hospital San José de La Palma generada con los diferentes programas computacionales (Ej. Office, Citsalud, WordPad, etc.), 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 TI. 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 el ESE Hospital San José de La Palma y deben conservar en todos los casos el mensaje legal corporativo de confidencialidad.

6.14 Segregación de Redes.

La plataforma tecnológica del Hospital que soporta los sistemas de Información debe estar separada en segmentos de red físicos y lógicos e independientes de los segmentos de red inalámbricas y de conexiones con redes con terceros.

6.15. Gestión de contraseña de usuarios.

Todos los recursos de información críticos del Hospital tienen asignados los privilegios de acceso de usuarios con base en los roles y perfiles que cada funcionario requiera para el desarrollo de sus funciones, definidos y aprobados por las áreas de negocio y administrados por el área de TI.

Todo funcionario o tercero que requiera tener acceso a los sistemas de información del Hospital debe estar debidamente autorizado y debe acceder a dichos sistemas haciendo uso como mínimo de un usuario (ID) y contraseña (password) asignado por la organización. El funcionario debe ser responsable por el buen uso de las credenciales de acceso asignadas

6.16. Escritorio y pantalla limpia.

Con el fin de evitar pérdidas, daños o accesos no autorizados a la información, todos los funcionarios del Hospital deben mantener la información restringida o confidencial bajo llave cuando sus puestos de trabajo se encuentren desatendidos

o en horas no laborales. Esto incluye: documentos impresos, CDs, dispositivos de almacenamiento USB y medios removibles en general. Adicionalmente, se requiere que la información sensible que se envía a las impresoras sea recogida manera inmediata.

Todos los usuarios son responsables de bloquear la sesión de su estación de trabajo en el momento en que se retiren del puesto de trabajo, la cual se podrá desbloquear sólo con la contraseña del usuario. Cuando finalicen sus actividades, se deben cerrar todas las aplicaciones y dejar los equipos apagados

Todas las estaciones de trabajo deberán usar el papel tapiz y el protector de pantalla corporativo, el cual se activará automáticamente después de cinco (5) minutos de inactividad y se podrá desbloquear únicamente con la contraseña del usuario.