
PLAN DE
DESARROLLO
2020 - 2024
Plan de Seguridad y
Privacidad de la Información
2021
E.S.E HOSPITAL
MARINILLA
¡EL HOSPITAL DE LA GENTE!
hospitalmarinilla
www.hospitalmarinilla.com

INTRODUCCION

La adopción de políticas, normas y procedimientos de seguridad de la información obedece a una decisión estratégica de la ESE Hospital San Juan de Dios de Marinilla, con el fin de definir a través del análisis, diseño e implementación; los objetivos, requisitos de seguridad, procesos, procedimientos y controles.

Se ha definido que las políticas de seguridad de la información deben identificar responsabilidades y establecer los objetivos para una protección apropiada de los activos de información de la entidad. La implementación de las políticas busca reducir el riesgo de que en forma accidental o intencional se divulgue, modifique, destruya o use en forma indebida la información de la entidad.

Todas las entidades en cumplimiento de sus funciones, están sometidos a riesgos que pueden hacer fracasar una gestión; por lo tanto, es necesario tomar las medidas, para identificar las causas y consecuencias de la materialización de dichos riesgos. Por esa razón, la presente guía tiene como objetivo orientar y facilitar la implementación y desarrollo de una eficaz, eficiente y efectiva gestión del riesgo, desde la identificación hasta el monitoreo y control.

Con base en lo anterior se debe integrar a todo el personal de la entidad para que, conozca, participe y cumpla los lineamientos, políticas, procedimientos y demás directrices estipuladas.

OBJETIVOS

GENERAL

Establecer los conceptos básicos y metodológicos que permitan proteger, asegurar y salvaguardar la confidencialidad, integridad y disponibilidad de los activos de información teniendo en cuenta los procesos, la operación, los objetivos de negocio y los requisitos legales vigentes en la entidad.

ESPECIFICOS

- Definir la política de seguridad y privacidad de la información de la ESE Hospital San Juan de Dios de Marinilla.
- Involucrar y comprometer a todos los funcionarios en la formulación e implementación de controles y acciones encaminadas a prevenir y administrar los riesgos de los activos de información de la ESE Hospital San Juan de Dios de Marinilla.
- Implementar políticas de buen manejo y seguridad de la información.
- Definir una estrategia de continuidad de los procesos de la entidad frente a incidentes de seguridad de la Información.

ALCANCE

La ESE Hospital San Juan de Dios de Marinilla propende por la protección de la información física y electrónica que almacena, recolecta, produce y gestiona a través de la implementación de controles físicos y lógicos, gestión de riesgos y la mejora continua, permitiendo incrementar los niveles de confidencialidad, integridad y disponibilidad de la información, apoyándose en los requisitos legales y normativos contribuyendo al cumplimiento misional de la entidad.

La Política de Seguridad y Privacidad de la Información aplica a todos los niveles de la organización, a todos sus funcionarios, contratistas, proveedores, operadores y aquellas personas o terceros, que en razón del cumplimiento de sus funciones y las de la ESE Hospital San Juan de Dios de Marinilla compartan, utilicen, recolecten, procesen, intercambien o consulten su información.

MARCO REGULATORIO Y NORMATIVO

La ESE Hospital San Juan de Dios de Marinilla, como entidad pública, al igual que cualquier organismo del estado, se encuentra cubierta por un marco normativo y regulatorio en todo lo relacionado con la seguridad de la información, como también un marco de referencia de las mejores prácticas para el desarrollo e implementación del Sistema de Gestión de Seguridad de la Información.

Se tiene en cuenta especialmente la nueva Estrategia de Gobierno Digital, que se evidencia en el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones 1078 de 2015, comprende cuatro grandes propósitos: lograr que los ciudadanos cuenten con servicios en línea de muy alta calidad, impulsar el empoderamiento y la colaboración de los ciudadanos con el Gobierno, encontrar diferentes formas para que la gestión en las entidades públicas sea optima gracias al uso estratégico de la tecnología y garantizar la seguridad y la privacidad de la información.

- LEY 1273 DE 2009: “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”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones”.
- LEY 1581 DE 2012: Por la cual se dictan disposiciones generales para la protección de datos personales tiene como objeto “desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma”.
- LEY 1712 DE 2014: “Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública”
- DECRETO 1008 DE 2018: “Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.”

PROPÓSITO

Promover en la ESE Hospital San Juan de Dios de Marinilla el uso de tecnologías de Información y Comunicación – TICs en entornos seguros, mediante normas simples aplicables al usuario del sistema de información, apoyado mediante herramientas que permitan prestar servicios de salud eficientes y confiable.

LINEAMIENTOS ESTRATÉGICOS DE LA POLÍTICA

La protección debe garantizar en primer lugar la confidencialidad, integridad y disponibilidad de los datos, sin embargo existen más requisitos como por ejemplo la autenticidad entre otros.

En la Seguridad de la Información el objetivo de la protección son los datos mismos y tratar de evitar su perdida y modificación no autorizada. La ESE Hospital San Juan de Dios de Marinilla asume el compromiso de implementar el sistema de Gestión de la Seguridad y privacidad de la información para proteger los activos de información de los procesos misionales, comprometiéndose a:

- Realizar una gestión integral de riesgos basada en la implementación de controles físicos y digitales orientados a la prevención de incidentes.
- El fomento de la cultura y toma de conciencia entre el personal (funcionarios, contratistas, proveedores y terceros) sobre la importancia de la seguridad de la información.
- Diseñar e implementar una estrategia que permita proteger la información generada, recolectada, procesada y utilizada en el cumplimiento de la misión de la Entidad.
- El proceso de Gestión de Información establecerá los lineamientos para la identificación, clasificación y buen uso de los activos de información físicos y digitales, para su protección.
- Proteger las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
- Controlar la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- Se garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.

En términos generales la política de seguridad y privacidad de la información, engloba los procedimientos más adecuados para la Gerencia de la información en los diferentes niveles de la organización, tomando como lineamientos principales cuatro criterios, los cuales están soportados en: seguridad organizacional, seguridad física, seguridad lógica y seguridad legal.

Seguridad Organizacional

Dentro de ésta, se establece el marco formal de seguridad que tiene la institución, incluyendo servicios o contrataciones externas a la infraestructura de seguridad, integrando el recurso humano con la tecnología, expresando responsabilidades y actividades complementarias como respuesta ante situaciones anómalas a la seguridad.

Seguridad Física y Lógica

Identifica los límites mínimos que se deben cumplir en cuanto a parámetros de seguridad física y lógica, de forma que se puedan establecer controles de acceso, definición de roles y responsabilidades, perfiles de seguridad, gestión de incidentes, documentación sobre sistemas de información, que van desde el control de cambios en la configuración de los equipos, manejo de incidentes, selección y adquisición de sistemas.

Seguridad Legal

Integra los requerimientos de seguridad que deben cumplir todos los funcionarios y usuarios de la red institucional bajo la reglamentación de la normativa interna de políticas y manuales en cuanto al recurso humano, sanciones aplicables ante faltas cometidas, así como cuestiones relacionadas con la legislación y contrataciones externas.

CLASIFICACION Y FLUJO DE INFORMACION

La clasificación de datos tiene el propósito de garantizar la protección de datos (personales) y significa definir, dependiendo del tipo o grupo de personas internas y externas, los diferentes niveles de autorización de acceso a los datos e informaciones. Considerando el contexto de nuestra misión institucional, tenemos que definir los niveles de clasificación como por ejemplo: confidencial, privado, sensitivo y público. Cada nivel define por lo menos el tipo de persona que tiene derecho de acceder a los datos, el grado y mecanismo de autenticación.

Una vez clasificada la información, tenemos que verificar los diferentes flujos existentes de información internos y externos, para saber quiénes tienen acceso a qué información y datos.

Clasificar los datos y analizar el flujo de la información a nivel interno y externo es importante, porque ambas cosas influyen directamente en el resultado del análisis de riesgo y las consecuentes medidas de protección. Porque solo si sabemos quiénes tienen acceso a qué datos y su respectiva clasificación, podemos determinar el riesgo de los datos, al sufrir un daño causado por un acceso no autorizado.

ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION

En esta política se definen los roles y responsabilidades de la seguridad de la información, específicamente con respecto a la protección de los activos de información. Esta política se aplica a todos los funcionarios, contratistas y terceros de la entidad sin excepción, en donde cada uno de los cuales cumple un rol en la administración de la seguridad de la información.

Todos los funcionarios, contratistas y terceros de la entidad son responsables de mantener un ambiente seguro, en tanto que se debe monitorear el cumplimiento de las políticas de seguridad definidas y realizar las actualizaciones que sean necesarias. Las políticas deben ser revisadas mínimamente una vez por año o cuando se produzca un cambio relevante en la operación que implique realizar ajustes o producto de los cambios en el entorno tecnológico y/o de las necesidades de la operación.

Políticas de Seguridad.

- Conocer y aplicar las políticas y procedimientos apropiados con relación al manejo de la información y de los sistemas informáticos.
- No divulgar información confidencial del Hospital a personas no autorizadas.
- No permitir y no facilitar el uso de los sistemas informáticos del Hospital a personas no autorizadas.
- No utilizar los recursos informáticos (hardware, software o datos) y de telecomunicaciones (teléfono, servidores) para otras actividades que no estén directamente relacionadas con el trabajo.
- Proteger meticulosamente su contraseña, por ningún motivo revelársela a nadie y evitar que sea vista por otros en forma inadvertida.
- Seleccionar una contraseña robusta (mínimo 8 dígitos) y que no tenga relación obvia con el usuario, sus familiares, el grupo de trabajo, y otras asociaciones parecidas.
- La navegación en Internet para fines personales no debe hacerse a expensas del tiempo y los recursos d del Hospital y en tal sentido deben usarse en las horas no laborables.
- Los mensajes que ya no se necesitan deben ser eliminados periódicamente de su área de almacenamiento. Con esto se reducen los riesgos de que otros puedan acceder a esa información y además se libera espacio en disco.
- Los equipos del Hospital sólo deben usarse para actividades de trabajo y no para otros fines, tales como juegos y pasatiempos.
- Debe respetarse y no modificar la configuración de hardware y software establecida por el Área de sistemas.
- No se permite fumar, comer o beber mientras se está usando un PC.
- Deben protegerse los equipos de riesgos del medioambiente (polvo, incendio, agua, etc.).
- Cualquier falla en los computadores o en la red debe reportarse inmediatamente ya que podría causar problemas serios como pérdida de la información o indisponibilidad de los servicios.
- No pueden moverse los equipos o reubicarlos sin permiso. Para cambiar de lugar y/o llevar un equipo fuera de alguna sede del Hospital, se requiere del Área de sistemas.
- La pérdida o robo de cualquier componente de hardware o programa de software debe ser reportada inmediatamente a la administración o Directivos del Hospital.
- Los datos confidenciales que aparezcan en la pantalla deben protegerse de ser vistos por otras personas. Cuando ya no se necesiten o no sean de utilidad, los datos confidenciales se deben borrar. Ejemplo: un mensaje de correo electrónico cuyo objetivo es transmitir o comunicar información confidencial.
- No se debe llevar al sitio de trabajo computadores portátiles (Laptops, NoteBooks, tablet) y en caso de ser necesario se requiere solicitar la autorización correspondiente.
- A menos que se indique lo contrario, los usuarios deben asumir que todo el software del Hospital está protegido por derechos de autor y requiere licencia de uso. Por tal razón es ilegal hacer copias o usar ese software para fines personales.
- Los usuarios no deben copiar a un medio removible (CD, USB, etc.), el software o los datos residentes en las computadoras del Hospital, sin la aprobación previa.

- Si se detecta la presencia de un virus u otro agente potencialmente peligroso, se debe notificar inmediatamente al Área de Sistemas y poner el computador en cuarentena hasta que el problema sea resuelto.
- Para prevenir demandas legales o la introducción de virus informáticos, no debe instalarse software no autorizado, incluyendo el que haya sido adquirido por el propio usuario. Así mismo, no se permite el uso de software de distribución freeware o shareware, a menos que haya sido previamente aprobado por el Área de Sistemas.
- No deben usarse usb u otros medios de almacenamiento en cualquier computadora a menos que se haya previamente verificado que están libres de virus u otros agentes dañinos.
- No deben dejarse las impresoras desatendidas, sobre todo si se está imprimiendo (o se va a imprimir) información confidencial del Hospital.
- La información almacenada en los puestos de trabajo por cada usuario es responsabilidad de cada uno, de esta información no se genera copia de seguridad.

Políticas de Contraseñas y el control de acceso

- El usuario no debe guardar su contraseña en una forma legible en archivos en disco, tampoco debe escribirla en papel y dejarla en sitios donde pueda ser encontrada. Si hay razón para creer que una contraseña ha sido comprometida, debe cambiarla inmediatamente.
- La contraseña inicial emitida a un nuevo usuario sólo debe ser válida para la primera sesión. En ese momento, el usuario debe escoger otra contraseña.
- Los usuarios no deben intentar violar los sistemas de seguridad y de control de acceso. Acciones de esta naturaleza se consideran violatorias de las políticas del Hospital, pudiendo ser causal incluso de despido.

Políticas para uso de Cuentas usuarios

- Cuando un usuario recibe una nueva cuenta, debe firmar un documento donde declara conocer las políticas y procedimientos de seguridad, y acepta sus responsabilidades con relación al uso de esa cuenta.
- No debe concederse una cuenta a personas que no sean empleados del Hospital a menos que estén debidamente autorizados, en cuyo caso la cuenta debe expirar automáticamente al cabo de un lapso de 30 días.
- Privilegios especiales, tal como la posibilidad de modificar o borrar los archivos de otros usuarios, sólo deben otorgarse a aquellos directamente responsables de la administración o de la seguridad de los sistemas.
- No deben otorgarse cuentas a técnicos de mantenimiento ni permitir su acceso remoto a menos que la Gerencia determine que es necesario. En todo caso esta facilidad sólo debe habilitarse para el periodo de tiempo requerido para efectuar el trabajo (como por ejemplo, el mantenimiento remoto).
- Cuando un empleado es despedido o renuncia al Hospital, debe desactivarse sus cuentas (Sistema de información CNT, chat interno, turneros) antes de firmar el paz y salvo de retiro.

Acuerdos de Confidencialidad.

Todos los funcionarios, contratistas, proveedores y terceros, que deban realizar labores dentro de la ESE Hospital San Juan de Dios de Marinilla, ya sea por medios lógicos o físicos que involucren el manejo de información, deben conocer, entender, firmar y aceptar el correspondiente acuerdo de confidencialidad de la información.

Este acuerdo se debe revisar a intervalos de tiempo regulares (el texto), avalando que reflejan las necesidades de la entidad para la protección y seguridad de la información.

Revisión del Plan

El proceso de gestión de información debe revisar el plan a intervalos planificados, (por lo menos una por año), para asegurar su conveniencia, suficiencia y eficacia. Esta revisión debe incluir la evaluación de las oportunidades de mejora y la necesidad de cambios, incluidos la política de seguridad y los objetivos de seguridad. Los resultados de las revisiones se deben documentar claramente y se deben llevar registros.

De la misma manera, las políticas de seguridad de la información, normas, procedimientos, estándares, controles, formatos y procedimientos, deben ser revisados y actualizados sistemáticamente, de forma periódica y planificada (mínimo una vez por año o cada vez que ocurra un cambio sustancial en los activos de información), por parte del proceso de gestión de información o en su defecto si se requiere una revisión independiente; se debe realizar por un organismo, empresa o consultor externo especializado.