Procedimiento y Plan de Seguridad y Privacidad de la Información

Política General de Seguridad

2021

INDICE

1. DEFINICIONES

Para los propósitos de este documento, se definen los siguientes conceptos:

Administrador del sistema.
Persona responsable de administrar, controlar, supervisar y garantizar la operatividad y funcionalidad de los sistemas. Dicha administración está en cabeza de la Gerencia de informática

Buzón.
También conocido como cuenta de correo, es un receptáculo exclusivo, asignado en el servidor de correo, para almacenar los mensajes y archivos adjuntos enviados por otros usuarios internos o externos a la empresa.

Chat. (Tertulia, conversación, charla).
Comunicación simultánea entre dos o más personas a través de Internet.

Computador.
Es un dispositivo de computación de sobremesa o portátil, que utiliza un microprocesador como su unidad central de procesamiento o CPU.

Contraseña o password.
Conjunto de números, letras y caracteres, utilizados para reservar el acceso a los usuarios que disponen de esta contraseña.

Correo electrónico.
También conocido como E-mail, abreviación de electronic mail. Consiste en el envío de textos, imágenes, videos, audio, programas, etc., de un usuario a otro por medio de una red. El correo electrónico también puede ser enviado automáticamente a varias direcciones.

FTP
File Transfer Protocol (Protocolo de Transferencia de Ficheros) y es el ideal para transferir grandes bloques de datos por la red.

Gusano
Virus o programa auto replicante que no altera los archivos sino que reside en la memoria y se duplica a sí mismo.

Hacker
Expertos relacionados con la informática, para también referirse a cualquier profesional que está en la cúspide de la excelencia en su profesión, ya que en la descripción más pura, un hacker es aquella persona que le apasiona el conocimiento, descubrir o aprender nuevas cosas y entender el funcionamiento de éstas.

Hacking

Es la búsqueda permanente de conocimientos en todo lo relacionado con sistemas informáticos, sus mecanismos de seguridad, las vulnerabilidades de los mismos, la forma de aprovechar estas vulnerabilidades y los mecanismos para protegerse de aquellos que saben hacerlo.

Internet
Es una red de redes a escala mundial de millones de computadoras interconectadas con un conjunto de protocolos, el más destacado, el TCP/IP. También se usa este nombre como sustantivo común y por tanto en minúsculas para designar a cualquier red de redes que use las mismas tecnologías que Internet, independientemente de su extensión o de que sea pública o privada.

Módem
Acrónimo de las palabras modulador/demodulador. El módem actúa como equipo terminal del circuito de datos (ETCD) permitiendo la transmisión de un flujo de datos digitales a través de una señal analógica.

Monitoreo de Cuentas de correo
Vigilancia o seguimiento minucioso de los mensajes de correo que recibe y envía un usuario.

Proxy
Programa o dispositivo que realiza una acción en representación de otro. La finalidad más habitual es la del servidor proxy, que sirve para permitir el acceso a Internet a todos los equipos de una organización.

Red
Se tiene una red, cada vez que se conectan dos o más computadoras de manera que pueden compartir recursos.

Seguridad
Mecanismos de control que evitan el uso no autorizado de recursos.

Servidor
Computadora que comparte recursos con otras computadoras, conectadas con ella a través de una red.

Servidor de correo
Dispositivo especializado en la gestión del tráfico de correo electrónico. Es un servidor perteneciente a la red de Internet, por lo que tiene conexión directa y permanente a la Red Pública. Su misión es la de almacenar, en su disco duro, los mensajes que envía y que reciben los usuarios.

Sistema Operativo
Plataforma operativa, programa o conjunto de programas que permiten administrar los recursos de hardware y software de una computadora.

Software
Todos los componentes no físicos de una PC (Programas).

Spam

Correo basura o mensaje basura a los mensajes no solicitados, no deseados o de remitente no conocido

Usuario
Toda persona, funcionario (empleado, contratista, temporal), que utilice los sistemas de información de la empresa debidamente identificado y autorizado a emplear las diferentes aplicaciones habilitadas de acuerdo con sus funciones.

Virus
Programa que se duplica a sí mismo en un sistema informático, incorporándose a otros programas que son utilizados por varios sistemas. Estos programas pueden causar serios problemas a los sistemas infectados. Al igual que los virus en el mundo animal o vegetal, pueden comportarse de muy diversas maneras. (Ejemplos: caballo de Troya y gusano).

Web Site
Un Web Site es equivalente a tener una oficina virtual o tienda en el Internet. Es un sitio en Internet disponible para ser accesado y consultado por todo navegante en la red pública. Un Web Site es un instrumento avanzado y rápido de la comunicación que facilita el suministro de información de productos o entidades. Un Web Site es también considerado como un conjunto de páginas electrónicas las cuales se pueden accesar a través de Internet.

Web Mail
Es una tecnología que permite acceder a una cuenta de Correo Electrónico (E-Mail) a través de un navegador de Internet, de esta forma podrá acceder a su casilla de correo desde cualquier computadora del mundo.

2. MARCO REGULATORIO

Para los propósitos de este documento se consideró la siguiente legislación informática y proyectos de ley en Colombia:

Para los propósitos de este documento se consideró la siguiente legislación informática y proyectos de ley en Colombia:

LEY ESTATUTARIA 1581 DE 2012

Entró en vigencia la Ley 1581 del 17 de octubre 2012 de PROTECCIÓN DE DATOS PERSONALES, sancionada siguiendo los lineamientos establecidos por el Congreso de la República y la Sentencia C-748 de 2011 de la Corte Constitucional.

LEY 603 DE 2000

Esta ley se refiere a la protección de los derechos de autor en Colombia. Recuerde: el software es un activo, además está protegido por el Derecho de Autor y la Ley 603 de 2000 obliga a las empresas a declarar si los problemas de software son o no legales.

LEY 1273 DEL 5 DE ENERO 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

3. LÍNEA BASE DE LA POLÍTICA GENERAL DE LA SEGURIDAD DE LA INFORMACIÓN

3.1. Objetivo

Lograr la preservación de la confidencialidad, disponibilidad e integridad de la información de la institución, estableciendo un esquema de seguridad bajo la gestión del riesgo.

3.2. Alcance

La presente política de seguridad de la información, tiene como finalidad resguardar la información almacenada en los componentes informáticos de la institución y aplica específicamente a los datos sensibles del personal de la institución y los usuarios que utilizan los servicios del hospital.

Cumplimiento

EL cumplimiento de las políticas y estándares de seguridad es obligatorio y debe ser considerado como una parte para la contratación de empleados y terceros y regirse de acuerdo a las normas, estatutos internos y la legislación colombiana.

3.3. Excepciones

Toda excepción debe ser documentada y aprobada por el comité de seguridad y el área de auditoria interna detallando el motivo por el no cumplimiento de la política interna.

3.4. Referencias

[1] ISO 27001:2005. Sistemas de gestión de Seguridad en la Información– Requerimientos

[2] Constitución colombiana

3.5. Principios

Los siguientes principios básicos fundamentan las políticas de seguridad de la información en EMPRESA:

EL HOSPITAL DEPARTAMENTAL MARIO CORREA RENGIFO E.S.EMRC básicamente está compuesto de **activos importantes** que le permiten realizar sus actividades propias del campo de la salud y darle continuidad a su funcionamiento

Particularmente **la información es un activo** que tiene un valor fundamental para el HRC y debe ser protegida de un modo adecuado.

La **seguridad de la información** protege a la información respecto a una amplia gama de amenazas a fin de asegurarle a la organización que los riesgos, los daños y el impacto sean

mínimos.

La **información** puede adoptar o estar representada en diversas formas: impresa o escrita (papeles de trabajo, contratos, planificaciones, reportes internos), puede almacenarse electrónicamente (servidores, PC's, memorias, pendrives), magnéticamente (discos rígidos, tarjetas de acceso, disquetes) u ópticamente (CD, DVD), enviarse por correo electrónico, visualizarse en películas o videos, y comunicarse oralmente en una conversación de persona a persona.

Sin importar la forma que posea la información **SIEMPRE debe protegerse adecuadamente**.

3.2.1. Protección de la información

Se establecerán los responsables propietarios de cada archivo o base de datos con información sensible o carácter personal, el responsable será quien deberá promover el establecimiento de controles y medidas para proteger los datos bajo su responsabilidad.

3.2.2. Responsabilidad

La responsabilidad de la seguridad de la información es de la Dirección del HMRC, que empleara los medios adecuados, lo que no excluye a cada empleado o usuario de asumir su parte de responsabilidad respecto a los medios que utiliza, según los puntos que se indican en esta política, en las normas que la desarrollan y en los procedimientos complementarios.

Quienes desempeñen funciones de Seguridad de la Información y otras de administración relacionadas, serán quienes administren la seguridad.

3.2.3. 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. Groso modo, la disponibilidad es el acceso a la información y a los sistemas por personas autorizadas en el momento que así lo requieran.

3.2.4. Integridad

Un principio de seguridad que certifica que los datos y Elementos de Configuración sólo son modificados por personal y Actividades autorizados. La Integridad considera todas las posibles causas de modificación, incluyendo Fallos software y hardware, Eventos medioambientales e intervención humana.

Confianza

La confidencialidad es la propiedad que impide la divulgación de información a personas o sistemas no autorizados. A grandes rasgos, asegura el acceso a la información únicamente a aquellas personas que cuenten con la debida autorización.

3.2.5. **Esfuerzo de Equipo**

4. POLÍTICA GENERAL DE LA SEGURIDAD DE LA INFORMACIÓN

La política de seguridad de información de HOSPITAL DEPARTAMENTAL MARIO CORREA RENGIFO E.S.E

- La gerencia del Hospital Mario Correa Rengifo está comprometida con la preservación de la confidencialidad, disponibilidad e integridad de la información de la institución y con el apoyo de la división de sistemas de información, supervisara la protección de los bienes de la información contra uso, modificación, acceso o destrucción no autorizada.

- ¿**Qué?** la preservación de la C.I.D de la información
- ¿**Quién?** La gerencia y la división de sistemas de información del HOSPITAL DEPARTAMENTAL MARIO CORREA RENGIFO E.S.E
- ¿**Dónde?** Dentro de la institución
- ¿**Cómo?** supervisando la protección de los bienes de la información.
- ¿**Cuándo?** Comuníquese y cúmplase a partir de la fecha
- ¿**Por qué?** para la protección de los bienes de la información.

4.1. Organización de seguridad

Política de Organización de Seguridad
El comité de seguridad de la información definirá la estrategia para la implementación y administración el SGSI dentro del HOSPITAL DEPARTAMENTAL MARIO CORREA RENGIFO E.S.E, definirá acuerdos de confidencialidad en la contratación interna (colaboradores) y externa (servicios), delegará roles y responsabilidades a sus colaboradores frente a la seguridad de la información.

- ¿**Qué?** El SGSI
- ¿**Quién?** El comité de seguridad de la información
- ¿**Dónde?** Dentro del HOSPITAL DEPARTAMENTAL MARIO CORREA RENGIFO E.S.E
- ¿**Cómo?** Definiendo estrategias para la implementación, administración y acuerdos de confidencialidad int y ext. y delegando roles y responsabilidades frente a la seguridad de la información
- ¿**Cuándo?** Comuníquese y cúmplase a partir de la fecha
- ¿**Por qué?** para la protección de los bienes de la información.

4.2. Clasificación y control de activos

El comité de seguridad de la información desarrollara mecanismos que permitan la adecuada identificación y clasificación de los activos de la información conociendo su propietario, ubicación y criticidad dentro de la institución, para gestionar su adecuada protección.

- **¿Qué?** Los activos de información
- **¿Quién?** El comité de seguridad de la información
- **¿Dónde?** Dentro del HOSPITAL DEPARTAMENTAL MARIO CORREA RENGIFO E.S.E
- **¿Cómo?** Desarrollando mecanismos que permitan la adecuada identificación y clasificación, conociendo su propietario, ubicación y criticidad
- **¿Cuándo?** Comuníquese y cúmplase a partir de la fecha
- **¿Por qué?** para gestionar su adecuada protección teniendo en cuenta la criticidad que representan.

4.3. Seguridad con personal

El comité de seguridad de la información apoyado en la unidad funcional de talento humano y la oficina asesora Jurídica definirán un plan estratégico que permita asignar y sensibilizar a todo el

personal del HOSPITAL DEPARTAMENTAL MARIO CORREA RENGIFO E.S.E en sus responsabilidades frente a la seguridad de la información

- **¿Qué?** Sensibilización del personal frente a sus roles en seguridad de la información
- **¿Quién?** El comité de seguridad de la información, la unidad funcional de talento humano y la oficina asesora Jurídica
- **¿Dónde?** Dentro del HOSPITAL DEPARTAMENTAL MARIO CORREA RENGIFO E.S.E
- ¿**Cómo?** Definiendo un marco estratégico para sensibilizar al personal
- ¿Cuándo? Comuníquese y cúmplase a partir de la fecha
- ¿**Por qué** – para la adecuada protección de los activos por parte del personal

4.4. Seguridad física

El comité de la seguridad de la información junto con la unidad funcional de ambiente físico implementara controles físicos para la adecuada protección de los activos de la información del HOSPITAL DEPARTAMENTAL MARIO CORREA RENGIFO E.S.E

- **¿Qué?** Protección de los activos
- **¿Quién?** El comité de seguridad de la información y la unidad funcional de ambiente físico
- **¿Dónde**? Dentro del HOSPITAL DEPARTAMENTAL MARIO CORREA RENGIFO E.S.E
- **¿Cómo?** Implementando controles físicos para adecuada protección
- **¿Cuándo?** Comuníquese y cúmplase a partir de la fecha
- **¿Por qué?** para la adecuada protección física de los activos por parte del personal

4.5. Administración de redes y computadores

La unidad funcional sistemas de información del hospital Mario Correa Rengifo, mantiene en óptima operación los sistemas de información y de comunicación de la institución dando disponibilidad a los usuarios autorizados e implementando procedimientos para la adecuada administración de cada uno de los elementos que la conforman.

- ¿**Qué?** mantiene en optima operación los sistemas de información y de comunicación
- ¿**Quién?** La unidad funcional sistemas de información
- ¿**Dónde?** Dentro del HOSPITAL DEPARTAMENTAL MARIO CORREA RENGIFO E.S.E
- ¿**Cómo?** implementando procedimientos para la adecuada administración de cada uno de los elementos que la conforman.
- ¿**Cuándo?** Comuníquese y cúmplase a partir de la fecha
- ¿**Por qué?** para dar disponibilidad a los usuarios autorizados

4.6. Control de acceso

La unidad funcional sistemas de información, del hospital Mario Correa Rengifo, preserva la fuga y/o modificación de la información e implementa controles de acceso adecuados a sus sistemas de información por medio de procedimientos de autorizaciones establecidos al personal que labora en la institución.

- ¿**Qué?** controles de acceso adecuados a sistemas de información
- ¿**Quién?** La unidad funcional sistemas de información
- ¿**Dónde?** Dentro del HOSPITAL DEPARTAMENTAL MARIO CORREA RENGIFO E.S.E
- ¿**Cómo?** por medio de procedimientos de autorizaciones
- **¿Cuándo?** Comuníquese y cúmplase a partir de la fecha
- ¿**Por qué?** para preservar la fuga y/o modificación de la información

4.7. Mantenimiento y desarrollo de sistemas

La unidad funcional de sistemas de información, establecerá los criterios que deben cumplir los procesos de adquisición, desarrollo y mantenimiento de sistemas de información, mediante la previa identificación, justificación, aceptación y documentación de requisitos de seguridad, para garantizar la preservación de la CID de la información del HOSPITAL DEPARTAMENTAL MARIO CORREA RENGIFO E.S.E que soportan los sistemas de información

- ¿**Qué?** establecerá los criterios que deben cumplir los procesos de adquisición, desarrollo y mantenimiento de sistemas de información.
- ¿**Quién?** La unidad funcional sistemas de información
- ¿**Dónde?** Dentro del HOSPITAL DEPARTAMENTAL MARIO CORREA RENGIFO E.S.E
- ¿**Cómo?** mediante la previa identificación, justificación, aceptación y documentación de requisitos de seguridad
- ¿Cuándo**?** Comuníquese y cúmplase a partir de la fecha
- ¿**Por qué?** para garantizar la CID de la información en los sistemas de información del HOSPITAL DEPARTAMENTAL MARIO CORREA RENGIFO E.S.E

4.8. Plan de continuidad del negocio

La unidad funcional de sistemas de información y el comité de seguridad de la información Establecerá los lineamientos generales para que se lleven a cabo las acciones necesarias que garanticen que la organización esté adecuadamente preparada para enfrentar eventos que afecten la infraestructura y recursos de toda índole. Evitando interrupciones de los procesos críticos del negocio como consecuencia de desastres.

- ¿**Qué?** la organización esté adecuadamente preparada para enfrentar eventos que afecten la infraestructura y recursos de toda índole. Evitar interrupciones a los procesos críticos del negocio como consecuencia de desastres.
- ¿**Quién?** La unidad funcional de sistemas de información y el comité de seguridad de la información
- ¿**Dónde?** Dentro del HOSPITAL DEPARTAMENTAL MARIO CORREA RENGIFO E.S.E
- ¿**Cómo?** Establecerá los lineamientos generales para que se lleven a cabo las acciones necesarias
- ¿Cuándo**?** Comuníquese y cúmplase a partir de la fecha
- ¿**Por qué?** para evitar interrupciones de los procesos críticos del negocio como consecuencia de desastres.

4.9. Cumplimiento de Políticas y normatividad legal

Conscientes de la importancia del cumplimiento de los requisitos legales el comité de seguridad con el apoyo de la oficina asesora jurídica establecerá mecanismos que permitan la validación del cumplimiento de la normatividad legal vigente aplicable al HMRC, mitigando riesgos de sanciones disciplinarias, fiscales y penales.

- ¿**Qué?** cumplimiento de los requisitos legales
- ¿**Quién?** La unidad funcional de sistemas de información y el comité de seguridad de la información
- ¿**Dónde?** Dentro del HOSPITAL DEPARTAMENTAL MARIO CORREA RENGIFO E.S.E
- ¿**Cómo?** establecerá mecanismos que permitan la validación del cumplimiento.

- ¿**Por qué?** mitigando riesgos de sanciones disciplinarias, fiscales y penales.

4.10. Aprobación de Políticas

La gerencia del HOSPITAL DEPARTAMENTAL MARIO CORREA RENGIFO E.S.E ha aprobado las políticas de seguridad de la información, que se aplica a todos los sistemas de Tecnologías de la Información y de la Comunicación (TIC), con el objetivo de maximizar la calidad de los servicios, asegurar la confidencialidad e integridad de la información, y reducir y mitigar los riesgos mediante la mejora continua de los procesos y servicios.

JUAN CARLOS MARTINEZ GUTIERREZ
Gerente
Proyectó y Elaboró: Mario González