TABLA DE CONTENIDO

1. INTRODUCCIÓN

La E.S.E. Municipal de Soacha Julio César Peñaloza, reconoce la importancia de la información como uno de los activos más importantes y críticos para el desarrollo de sus funciones. En la gestión de los procesos estratégicos, misionales y de apoyo, continuamente se está procesando, gestionando, almacenando, custodiando, transfiriendo e intercambiando información valiosa que puede ir desde un dato personal de un paciente o usuario cualquiera hasta información secreta de la institución que no deben ser divulgados a personal no autorizado, suceso que puede poner en riesgo la gestión de la E.S.E. Municipal de Soacha Julio César Peñaloza.

En atención a lo anterior, la entidad asumió el reto de implementar el Plan de Seguridad y Privacidad de la Información, siguiendo los lineamientos de la Estrategia de Gobierno en Línea, a su vez reglamentado a través del Decreto 1078 de 2015 para el sector de tecnologías de la información y comunicaciones y el Decreto 2573 de 2014 por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea.

Cuanto mayor es el valor de la información, mayores son los riesgos asociados a su pérdida, deterioro, manipulación indebida o mal intencionada. Plan de Seguridad y Privacidad de la Información de la E.S.E. Municipal de Soacha Julio César Peñaloza adopta como metodología las mejores prácticas existentes para la identificación y valoración de los activos de información, y para la evaluación y tratamiento de los riesgos; siendo éste el medio más eficaz de tratar, gestionar y minimizar los riesgos, considerando el impacto que éstos representan para la entidad y sus partes interesadas.

Así mismo, Plan de Seguridad y Privacidad de la Información de la E.S.E. Municipal de Soacha Julio César Peñaloza define políticas y procedimientos eficaces y coherentes con la estrategia de la entidad, como el desarrollo de los controles que se adoptan para el tratamiento de los riesgos, los cuales están en continuo seguimiento y medición, a través del establecimiento de indicadores que aseguran la eficacia de los controles; apoyado en los programas de seguimiento y control por parte de la dirección, que concluyen en la identificación de oportunidades de mejora. Todo esto se complementa con los programas de formación y transferencia de conocimiento en todo lo referente a la seguridad de la información.

Así pues, la entidad expone a través de este documento el modelo del Plan de Seguridad y Privacidad de la Información que se adopta con el propósito de cumplir con el marco normativo, la misión fijada y la visión trazada, describiendo las disposiciones acogidas por

la entidad para establecer el contexto, las políticas, los objetivos, el alcance, los procedimientos, las metodologías, los roles, las responsabilidades y las autoridades del Plan de Seguridad y Privacidad de la Información que proporciona el esquema para la gestión de riesgos y las mejores prácticas, tales como ISO 27002:2015, ISO 27005:2009, ITIL, entre otras; buscando mejorar el desempeño y la capacidad para prestar un servicio que responda a las necesidades y expectativas de las partes interesadas.

2. OBJETIVOS

2.1 Objetivo general

Presentar el Plan de Seguridad y Privacidad de la Información, el cual es el documento que dirige la implementación de controles de seguridad de la información en la E.S.E. Municipal de Soacha Julio César Peñaloza expone las prioridades de implementación de los controles en relación a seguridad de la información enmarcado en el ciclo de mejoramiento continuo.

2.2 Objetivos específicos

- Comunicar e implementar la estrategia de seguridad de la información.
- Incrementar el nivel de madurez en la gestión de la seguridad de la información.
- Implementar y apropiar el Modelo de Seguridad y Privacidad de la Información con el objetivo de proteger la información y los sistemas de información, de acceso, uso, divulgación, interrupción o destrucción no autorizada.
- Asegurar el uso eficiente y seguro de los recursos de TI (Humano, Físico, Financiero, Tecnológico, etc.), para garantizar la continuidad de la prestación de los servicios.
- Generar pautas para la prestación de servicios a la comunidad de forma continua e interrumpida.
- Fomentar el uso y apropiación de la Política de Seguridad vigente en los funcionarios y contratistas de la E.S.E. Municipal de Soacha Julio César Peñaloza
- Reducir las brechas de seguridad, de forma ordenada y guiada por los parámetros dictaminados desde el Ministerio de las TIC’s.
- Establecer políticas que mejoren los servicios prestados mediante tecnologías de la información, procurando la mejora continua y optimización de los procesos.

3. ALCANCE DEL DOCUMENTO

El Plan de Seguridad y Privacidad de la Información considera los controles de la norma y el análisis de riesgos realizado, en los procesos de la E.S.E. Municipal de Soacha Julio César Peñaloza y los lineamientos del Modelo de Seguridad y Privacidad de la Información con el fin de determinar la estrategia de implementación de los controles de seguridad requeridos.

El presente documento se enfoca en crear una estrategia para el análisis, diseño, ejecución y control de los proyectos gestados desde el área de tecnología, aplicables a la adopción de sistemas de información para mejorar los canales de comunicación, uso y apropiación de los servicios brindados por la E.S.E. Municipal de Soacha Julio César Peñaloza, logrando una comunicación interna eficiente a nivel institucional, mediante el cumplimiento de la normatividad establecida de Gobierno en Línea a través de la mejora continua, teniendo como pilares La **CONFIDENCIALIDAD, DISPONIBILIDAD, INTEGRIDAD, AUTENTICIDAD** de la información.

4. DEFINICIONES

Caché: es un componente de hardware o software que guarda datos para que las solicitudes futuras de esos datos se puedan atender con mayor rapidez; los datos almacenados en una caché pueden ser el resultado de un cálculo anterior o el duplicado de datos almacenados en otro lugar, generalmente, da velocidad de acceso más rápido.

Cookies: Las cookies son archivos que crean los sitios que visitas. Guardan información de la navegación para hacer que tu experiencia en línea sea más sencilla.

Addons: También conocidos como extensiones, plugins, snap-ins, etc., son programas que sólo funcionan anexados a otro y que sirven para incrementar o complementar sus funcionalidades.

(VPN) Redes Privadas Virtuales: es una tecnología de red de ordenadores que permite una extensión segura de la red de área local (LAN) sobre una red pública o no controlada como Internet. Permite que el ordenador en la red envíe y reciba datos sobre redes compartidas o públicas como si fuera una red privada, con toda la funcionalidad, seguridad y políticas de gestión de una red privada.

Servidor proxy: Los servidores proxy generalmente se usan como un puente entre el

origen y el destino de una solicitud, funciones: Control de acceso, filtrado de contenido, cache.

Firewall: Programa informático que controla el acceso de una computadora a la red y de elementos de la red a la computadora, por motivos de seguridad.

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

Malware: es un término amplio que describe cualquier programa o código malicioso que es dañino para los sistemas

Spyware: puede infectar cualquier dispositivo y dar a los ciber delincuentes acceso completo a información confidencial como contraseñas, datos bancarios o su identidad digital completa.

Rootkits: es un sigiloso y peligroso tipo de malware que permite a los hackers acceder a los equipos sin el conocimiento de la persona.

Armario Ignífugo: son armarios equipados con sistemas de protección contra el fuego para aislar los equipos de cómputo almacenados en su interior.

Time out: Se refiere al momento en que un usuario hace uso de la Red por un período determinado hasta que se agota.

Logs: Registro log o historial de log para referirse a la grabación secuencial en un archivo o en una base de datos de todos los acontecimientos, eventos o acciones que afectan a un proceso particular.

5. POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La Política de Seguridad y Privacidad de la Información es la declaración general que representa la posición de la E.S.E. Municipal de Soacha Julio César Peñaloza con respecto a la protección de los activos de información (los funcionarios, contratistas, terceros. la información, los procesos, las tecnologías de información incluido el hardware y el software), que soportan los procesos de la Entidad y apoyan la implementación del Sistema de Gestión

de Seguridad de la Información, por medio de la generación y publicación de sus políticas, procedimientos e instructivos, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información.

Para asegurar la dirección estratégica de la Entidad, establece la compatibilidad de la política de seguridad de la información y los objetivos de seguridad de la información, estos últimos correspondientes a:

- Minimizar el riesgo de los procesos misionales de la entidad.
- Cumplir con los principios de seguridad de la información
- Mantener la confianza de los funcionarios, contratistas y terceros.
- Apoyar la innovación tecnológica.
- Implementar el sistema de gestión de seguridad de la información.
- Proteger los activos de información.
- 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**.**
- Garantizar la continuidad del negocio frente a incidentes.

5.1. Alcance/Aplicabilidad

- Se aplica a toda la entidad, sus funcionarios, contratistas y terceros y la ciudadanía en general.

5.2. Nivel de cumplimiento

A continuación, se establecen las políticas de seguridad que soportan este documento**:**

- Se define, implementa, opera y mejorar el Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades de la E.S.E. Municipal de Soacha Julio César Peñaloza y a los requerimientos regulatorios que le aplican a su naturaleza.
- Las responsabilidades frente a la seguridad de la información son definidas por el área de tecnología, orientadas, compartidas, publicadas por el área de comunicaciones y posterior aceptadas por cada uno de los empleados, contratistas o terceros.
- Se protegerá la información creada, procesada, transmitida o resguardada por los procesos de la entidad, con el fin de minimizar impactos financieros, operativos o

legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.

- Se protegerá la información de las amenazas originadas por parte del personal.
- Se protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
- Se controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- Se implementará control de acceso a la información, sistemas y recursos de red.
- Se garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
- 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.
- Se garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.
- Se garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

El incumplimiento a la política de Seguridad y Privacidad de la Información, traerá consigo, las consecuencias legales que apliquen a la normativa de la Entidad, incluyendo lo establecido en las normas que competen a la E.S.E. Municipal de Soacha Julio César Peñaloza en cuanto a Seguridad y Privacidad de la Información se refiere.

5.3. Manual de políticas

La política de seguridad de la información, representa la posición de la E.S.E. Municipal de Soacha Julio César Peñaloza con respecto a la protección de los activos de información (los funcionarios, la información, los procesos, las tecnologías de información incluido el hardware y el software) y respecto a la implementación del Sistema de Gestión de Seguridad de la Información y al apoyo, generación y publicación de sus políticas, procedimientos e instructivos.

La E.S.E. Municipal de Soacha Julio César Peñaloza para el cumplimiento de su misión, visión, objetivo estratégico y apegado a sus valores corporativos establece la función de seguridad de la información en la entidad, con el objetivo de:

- Minimizar los riesgos en las funciones más importantes de la entidad
- Cumplir con los principios de la seguridad de la información
- Cumplir con los principios de la función administrativa
- Mantener la confianza de los funcionarios, contratistas y usuarios de la entidad
- Apoyar la innovación tecnológica e implementar el sistema de gestión de seguridad de la información
- Proteger los activos tecnológicos de la entidad
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información
- Consolidar una estrategia orientada a la continuidad del negocio, la administración de riesgos y la consolidación de una cultura de seguridad
- Fortalecer la cultura de seguridad de la información en funcionarios, contratistas, practicantes y usuarios de la institución
- Toda la información que se genere por parte de los funcionarios, contratistas o terceros que tengan relación con el Instituto es propiedad de la E.S.E. Municipal de Soacha Julio César Peñaloza, a menos que se acuerde lo contrario en los contratos escritos y autorizados
- Garantizar la continuidad de operación del Instituto, frente a incidentes de seguridad
- La E.S.E. Municipal de Soacha Julio César Peñaloza, adopta los lineamientos de las Políticas de Seguridad de la Información contenidos en el presente documento y en los documentos relacionados con él, como una herramienta con el fin de mantener la confidencialidad, la integridad y asegurar la disponibilidad de la información, de obligatorio cumplimiento por parte de cada uno de los directivos, funcionarios, contratistas y terceros que presten sus servicios.

5.4 Alcance

Esta política aplica a toda la entidad, sus funcionarios, contratistas, practicantes, proveedores y a la ciudadanía en general.

5.5 Alcance/Aplicabilidad

Nivel de Cumplimiento todas las personas cubiertas por el alcance y aplicabilidad, se espera que se adhieran en un 100% de la política.

6. NORMATIVIDAD

Las normas que rigen la estructura organizacional de seguridad de la información están dirigidas a:

GERENCIA

- La Gerencia debe definir y establecer los roles y responsabilidades relacionados con la seguridad de la información en niveles directivo y operativo
- La Gerencia debe definir y establecer el procedimiento de contacto con las autoridades en caso de ser requerido, así como los responsables para establecer dicho contacto.
- La Gerencia debe revisar y aprobar las Políticas de Seguridad de la Información contenidas en este documento.
- La Gerencia debe promover activamente una cultura de seguridad de la información en la E.S.E. Municipal de Soacha Julio César Peñaloza con el apoyo de sistemas, subgerencias, calidad y planeación
- La Gerencia debe facilitar la divulgación de las Políticas de Seguridad de la Información a todos los funcionarios de la entidad y al personal provisto por terceras partes.
- La Gerencia, deben asignar los recursos, la infraestructura física y el personal necesario para la gestión de la seguridad de la información de la E.S.E. Municipal de Soacha Julio César Peñaloza

Departamento de Tecnología

- El departamento de Tecnología debe liderar la generación de lineamientos para gestionar la seguridad de la información de la E.S.E. Municipal de Soacha Julio César Peñaloza y el establecimiento de controles técnicos, físicos y administrativos derivados de análisis de riesgos de seguridad.
- El departamento de Tecnología está en el deber de validar y monitorear de manera periódica la implantación de los controles de seguridad establecidos.
- El departamento de Tecnología asignará las funciones, roles y responsabilidades, a sus funcionarios para la operación y administración de la plataforma tecnológica de la E.S.E. Municipal de Soacha Julio César Peñaloza. Dichas funciones, roles y responsabilidades deben encontrarse documentadas y apropiadamente segregadas.

CONTROL INTERNO

- La Oficina de Control Interno debe planear y ejecutar las auditorías internas al Sistema de Gestión de Seguridad de la Información de la E.S.E. Municipal de Soacha Julio César Peñaloza a fin de determinar si las políticas, procesos, procedimientos y controles establecidos están conformes con los requerimientos institucionales, requerimientos de seguridad y regulaciones aplicables.
- La Oficina de Control Interno debe informar a las áreas responsables los hallazgos de las auditorías.

USUARIOS EN GENERAL

- Los funcionarios y personal provisto por terceras partes que realicen labores en o para la E.S.E. Municipal de Soacha Julio César Peñaloza, tienen la responsabilidad de cumplir con las políticas, normas, procedimientos y estándares referentes a la seguridad de la información.

6.1. Normas para uso de conexiones remotas

Se considera acceso remoto al realizado desde fuera de las propias instalaciones de la organización, a través de redes de terceros. El acceso desde fuera de las instalaciones de la E.S.E. Municipal de Soacha Julio César Peñaloza conlleva el riesgo de trabajar en entornos de acceso desprotegidos, esto es, sin las barreras de seguridad físicas y lógicas implementadas en las instalaciones de la entidad fuera de este perímetro de seguridad aumentan las v vulnerabilidades y la probabilidad de materialización de las amenazas, por lo que se hace necesario adoptar medidas de seguridad adicionales que aseguren la confidencialidad, autenticidad e integridad de la información.

Además de estas medidas de seguridad de acceso local, la entidad aplica las siguientes medidas:

- Prevención de ataques activos desde el exterior, garantizando que al menos serán detectados y que se activarán los procedimientos previstos de tratamiento del incidente.
- La alteración de la información en tránsito
- La inyección de información espuria

- El secuestro de la sesión por una tercera parte
- Para asegurar la autenticidad del otro extremo de un canal de comunicación antes de intercambiar información es obligatorio el uso de contraseñas acordes a la Política de Contraseñas de la entidad.
- Siempre que sea posible, la autenticación del usuario se realizará en el directorio corporativo de la entidad.
- Cerrar siempre la sesión al terminar de trabajar.
- Bloquear siempre la sesión, ante cualquier ausencia temporal, aunque sea por poco espacio de tiempo.
- Se debe procurar el uso de Redes Privadas Virtuales (VPN) para conexiones externas.

Cuando la conexión desde el exterior se realice con equipos portátiles corporativos, el usuario tendrá en cuenta:

- Que dichos equipos son para uso exclusivo del trabajador y sólo serán utilizados para fines profesionales.
- No se han de prestar a terceros salvo autorización expresa por parte del líder de sede y de la subgerente administrativa y financiera que incluirá en todo caso la definición de las condiciones de uso.

Si la conexión se realiza desde equipos de trabajo personales que no estén bajo la responsabilidad de la E.S.E. Municipal de Soacha Julio César Peñaloza, los usuarios deben considerar:

- Que los equipos estén configurados con los requisitos de software necesarios que permiten trabajar en los mismos entornos y versiones que requieren los sistemas operativos de la entidad. En cualquier caso, los equipos desde los que se realiza la conexión remota deben disponer de las siguientes medidas de seguridad, estén o no bajo la responsabilidad de E.S.E. Municipal de Soacha Julio César Peñaloza:
- Antivirus instalado y actualizado junto con sus patrones de virus.
- Cortafuegos activados.
- Versión del sistema operativo actualizada con los últimos parches de seguridad.
- Copias de seguridad periódicas de la información contenida en los equipos. Es necesario adoptar las medidas adecuadas para la protección de dichas copias.

Cuando el acceso remoto a los servicios internos de la entidad se realice vía Web, se aplicarán las
siguientes medidas de seguridad:

- Los navegadores utilizados deben estar adecuados a las versiones oficiales que dan cobertura a los sistemas de la E.S.E. Municipal de Soacha Julio César Peñaloza, así como tener los parches de seguridad correspondientes instalados y configurados.
- Una vez finalizada la sesión web, es obligatoria la desconexión con el servidor mediante un proceso que elimine la posibilidad de reutilización de la sesión cerrada.
- Desactivar las características de recordar contraseñas en el navegador.
- Activar la opción de borrado automático al cierre del navegador de la información sensible registrada por el mismo: histórico de navegación, descargas, formularios, caché, cookies, contraseñas y sesiones autenticadas.
- No instalar addons (extensiones) para el navegador que puedan alterar el normal funcionamiento de las aplicaciones.

6.2. Cumplimiento de las normativas internas

Durante la actividad profesional fuera de las instalaciones de la entidad se seguirán las políticas, normativas, procedimientos y recomendaciones internas existentes en la E.S.E. Municipal de Soacha Julio César Peñaloza, atendiendo de manera especial a las siguientes:

- Las contraseñas deberán ser robustas y deben renovarse periódicamente o cuando se sospeche que pueden estar comprometidas.
- El uso de los soportes físicos extraíbles (CD, DVD, memorias USB) debe limitarse. El almacenamiento de la información en soportes físicos extraíbles debe caracterizarse por no ser accesible para usuarios no autorizados. Para ello, es necesario aplicar claves de acceso, cuando la naturaleza de la información así lo aconseje.
- No se desactivarán las herramientas de seguridad habilitadas en los dispositivos móviles (portátiles, móviles, tabletas, etc.) y se mantendrán siempre actualizadas.
- No se descargarán ni se instalarán contenidos no autorizados en los equipos.
- Medidas preventivas y buenas prácticas, cifrar y/o firmar los correos electrónicos con información sensible, confidencial o protegida que vayan a ser transmitidos a través

de correo electrónico o de cualquier otro canal que no proporcione la confidencialidad adecuada.

6.3. Responsabilidades

Todos los usuarios vinculados a la E.S.E. Municipal de Soacha Julio César Peñaloza son responsables de conocer las normas que afectan al desarrollo de sus funciones, así como las consecuencias en que pudieran incurrir en caso de incumplimiento. Todos los usuarios son responsables de cumplir con las directrices de la normativa de acceso local y remoto dispuestas a través del Plan de Seguridad y Privacidad de la Información y el resto de normativas asociadas. Cualquier persona que administre un equipo informático, aplicación o servicio, es responsable de mantener correctamente instalado y actualizado el sistema de protección del equipo como requisito para el acceso a la Red Informática de la entidad.

6.4. Normas uso de periféricos y medios de almacenamiento

El uso de periféricos en los computadores de escritorio, computadores portátiles y demás recursos informáticos (escáner, impresora, mouse, teclado, medios de almacenamiento removibles), debe ser restringido acorde con las funciones realizadas por los empleados de la E.S.E. Municipal de Soacha Julio César Peñaloza.

TODOS LOS USUARIOS

Ningún usuario de la E.S.E. Municipal de Soacha Julio César Peñaloza podrá instalar o conectar al computador de escritorio, computador portátil y demás recursos informáticos asignados, elementos adicionales a los entregados con estos. Dichos elementos, incluyen, pero no se limitan a: cámaras web, cámaras digitales, grabadoras de sonido, impresoras, escáner, reproductores multimedia, puntos de acceso inalámbricos, dispositivos móviles. En caso de requerir el uso de cualquier elemento adicional, deberá solicitar a La Mesa de Ayuda para tal efecto. Los usuarios no deberán usar medios de almacenamiento no autorizados para el manejo de la información, donde se incluyen, pero no se limitan a: disquete, memorias USB, memorias flash directamente o a través de dispositivos móviles, CD, DVD, discos externos, que no sean de propiedad de la E.S.E. Municipal de Soacha Julio César Peñaloza y que no hayan sido entregados con fines y autorización específicos.

EL DEPARTAMENTO DE TECNOLOGÍA

En su función como asesor y ejecutor de las políticas de seguridad de la información en la E.S.E. Municipal de Soacha Julio César Peñaloza deben adoptar medidas para garantizar que no se conecten a los computadores de escritorio, computadores portátiles y demás recursos informáticos de la entidad, medios de almacenamiento no autorizados, donde se incluyen, pero no se limitan a: disquete, memorias USB, memorias flash directamente o a través de dispositivos móviles, CD, DVD, discos externos, que no sean de propiedad de la E.S.E. Municipal de Soacha Julio César Peñaloza.

6.5. Normas de administración de acceso de usuarios

Los controles de acceso deberán contemplar:

- Requerimientos de seguridad de cada una de las aplicaciones.
- Definir los perfiles o privilegios de acceso de los usuarios a las aplicaciones de acuerdo a su perfil de cargo en la entidad.

- **Administración de Accesos de Usuarios**

La Oficina de Información Pública establece procedimientos para controlar la asignación de derechos de acceso a los sistemas, datos y servicios de información.

- **Creación de Usuarios**

La E.S.E. Municipal de Soacha Julio César Peñaloza, a través del departamento de Tecnología deberá mantener los registros donde cada uno de los lideres responsables de los procesos haya autorizado el acceso a los diferentes sistemas de información de la entidad. Los datos de acceso a los sistemas de información deberán estar compuestos por un ID o nombre de usuario y contraseña que debe ser único por cada servidor o sistema. Cuando se retire o cambie de contrato, se deberá aplicar la eliminación o cambios de privilegios en los sistemas de información a los que el usuario que estaba autorizado. El departamento de Tecnología, deberá realizar revisiones de privilegios de acceso a los diferentes sistemas de información y a los registros de las revisiones y hallazgos.

- **Administración de Contraseñas de Usuario**

Las contraseñas de acceso deberán cumplir con un mínimo de 8 caracteres y la combinación de números, letras mayúsculas, minúsculas y caracteres especiales. Se deberá cambiar su contraseña de acceso a los diferentes sistemas de información con una

frecuencia mínima de cada noventa días, a excepción de aquellos que contengan información confidencial o secreta en cuyo caso el cambio se debe realizar cada treinta días. Los sistemas de información deberán bloquear permanentemente al usuario luego de cinco intentos fallidos de autenticación a excepción de aquellos que contengan información confidencial o secreta en cuyo caso después de tres intentos fallidos de autenticación se realizará el bloqueo.

- **Uso de Contraseñas**

Los usuarios deben cumplir las siguientes normas:

- Mantener los datos de acceso en secreto.
- Contraseñas fáciles de recordar y difíciles de adivinar.
- Que las contraseñas no estén basadas en algún dato que otra persona pueda adivinar u obtener fácilmente mediante información relacionada con la persona, por ejemplo, nombres, números de teléfono, fecha de nacimiento, etc.
- Notificar de acuerdo a lo establecido cualquier incidente de seguridad relacionado con sus contraseñas: pérdida, robo o indicio de pérdida de confidencialidad.

- **Equipos de cómputo de Usuarios**

- Los usuarios deberán garantizar que los equipos de cómputo sean protegidos adecuadamente. Las estaciones de trabajo o servidores de archivos, requieren una protección específica contra accesos no autorizados cuando se encuentran desatendidos.
- Bloquear el equipo de cómputo tras abandonar el puesto de trabajo.
- Bloqueo automático de la sesión en el equipo de cómputo tras inactividad superior a cinco minutos.
- Apagar los equipos de cómputo al finalizar la jornada laboral.

- **Control de Acceso a la Red**

El departamento de Tecnología debe asegurar el bloqueo al acceso de páginas de contenido para adultos, redes sociales, hacking, descargas (FTP), mensajería instantánea y cualquier página que represente riesgo potencial para la Entidad mediante el uso de servidor proxy, firewall o el software que mejor se ajuste a la necesidad. Excepciones de acceso, serán aprobados por la gerencia, según la necesidad del cargo y verificación previa de que las paginas solicitadas no contengan código malicioso con el visto bueno del oficial

de seguridad de la información.

- **Seguridad en los Servicios de Red**

Mantener instalados y habilitados sólo aquellos servicios y puertos que sean utilizados por los sistemas de información y software de la entidad. Controlar el acceso lógico a los servicios, tanto a su uso como a su administración mediante bloqueo de puertos en el firewall de la entidad.

- **Control de Identificación y Autenticación de Usuarios.**

Todos los usuarios (incluido el personal el departamento de Tecnología) tendrán un identificador único (ID de Usuario) solamente para su uso personal exclusivo, de manera que las actividades tengan trazabilidad.

- **Sistema de Administración de Contraseñas**

El sistema de administración de contraseñas debe:

- Obligar el uso de User ID´s y contraseñas individuales para determinar responsabilidades.
- Permitir que los usuarios seleccionen y cambien sus propias contraseñas luego de cumplido el plazo mínimo de mantenimiento de las mismas o cuando consideren que la misma ha sido comprometida e incluir un procedimiento de confirmación para contemplar los errores de ingreso.
- Obligar a los usuarios a cambiar las contraseñas provisionales o que han sido asignadas por el administrador del sistema de información.
- Almacenar las contraseñas en forma cifrada.

- **Sesiones Inactivas**

Si el usuario debe abandonar la estación de trabajo momentáneamente, activará protectores de pantalla con contraseñas, con el fin de evitar que Terceros puedan ver su trabajo o continuar con la sesión de usuario habilitada. Si los sistemas de información detectan inactividad por un periodo igual o superior a diez minutos, deben automáticamente aplicar,

"timeout" es decir, finalizar la sesión de usuario.

- **Limitación del Tiempo de Conexión**

Las restricciones al horario de conexión deben suministrar seguridad adicional a las aplicaciones de alto riesgo:

Limitar los tiempos de conexión al horario normal de oficina, de no existir un requerimiento operativo de horas extras o extensión horaria.

Documentar los usuarios o contratistas que no tienen restricciones horarias y los motivos y evidencia de la autorización expedida por La Gerencia.

6.6. Normas de protección frente a software malicioso

Existe una gran variedad de especímenes de malware diseñados con la finalidad de realizar acciones maliciosas sobre algún dispositivo electrónico. A día de hoy no solo el malware afecta a los equipos informáticos, y podemos encontrarlos en dispositivos móviles, tablet e incluso televisores. Para combatir y proteger los equipos informáticos y sus derivados en la E.S.E. Municipal de Soacha Julio César Peñaloza se establecen mecanismos contra los efectos del malware.

Existen dos grupos de estas medidas contra el malware:

- **Medidas preventivas:** Tratan de evitar infecciones por malware.
- **Medidas paliativas:** Minimizan el impacto producido por una infección.

Medidas preventivas contra el malware.

Están constituidas por el conjunto de acciones que los usuarios realizan para evitar infecciones por malware. Cuando hablamos de medidas de seguridad activas en general, estamos hablando de técnicas que detectan y previenen un incidente de seguridad. En este punto nos ocuparemos de las herramientas que evitan que los sistemas se infecten con malware, las cuales reciben el nombre de **herramientas antimalware.**

- **Suites de seguridad.**

La medida de protección más conocida entre los usuarios es el antivirus. Se trata de un programa que evita las infecciones por malware y además desinfecta los equipos ya infectados. Una suite, es una evolución de los antivirus que se ha hecho para reconocer otros tipos de malware, como spyware, rootkits, etc.

Estos programas combaten el malware de dos formas:

- **Protegiendo el equipo** contra la instalación del malware.
- **Detectando y eliminando malware** que ya ha sido instalado en el equipo.

- **Cortafuegos**

Diseñado para proteger dicho sistema bloqueando accesos no autorizados y permitiendo solo los que deban ser permitidos solo los que deban ser permitidos. Para permitir o denegar el tráfico, los cortafuegos suelen definir una **política por defecto.** Distinguimos dos tipos de políticas:

- **Políticas permisivas:** Se deniega el acceso a la red.
- **Políticas restrictivas:** Prohibido el acceso a los recursos del sistema.

Además de la política por defecto, la mayoría de cortafuegos definen **reglas** que son un conjunto de condiciones que deben cumplir los mensajes para que el firewall permita o rechace su paso.

- **Tipos de cortafuegos:**

- **Cortafuegos de equipo o de host:** Se instala en el equipo que se desea proteger.
- **Cortafuegos de red o perimetrales:** Actúa como barrera entre la res interna y la externa.

- **Protección ante malware en correos electrónicos.**

Una de las principales formas de propagación utilizadas por el malware es el correo electrónico. En la E.S.E. Municipal de Soacha Julio César Peñaloza consciente de este problema latente ha generado la siguiente normativa para proteger a la entidad contra el

malware en correos electrónicos:

- Instruir al usuario para que actúe con prudencia antes de abrir archivos adjuntos, aunque el emisor sea de confianza.
- Configurar el correo para que el antivirus compruebe los mensajes.
- No reenviar un mensaje sin antes borrar la lista de direcciones de correo electrónico.
- No reenviar mensajes que formen parte de cadenas.
- No hacer clic en las direcciones web que aparecen en un correo electrónico a no ser que el correo sea de confianza.
- Denunciar el correo abusivo o fraudulento informando a la Mesa de Ayuda para que adopte los correctivos necesarios para evitar ataques posteriores con esas mismas características.

- **Medidas paliativas contra el malware.**

Constituyen todo el conjunto de acciones que la E.S.E. Municipal de Soacha Julio César Peñaloza ha adoptado para eliminar malware que ha conseguido infectar al equipo. Conscientes de que no existe una solución mágica ante una infección o incidente de seguridad. Se, deberá estudiar la gravedad y el alcance de la infección para decidirse por una opción u otra.

Copias de seguridad

Guardar una parte o toda la información del sistema para poder recuperarla en el caso de pérdida:

- **Copias de seguridad del sistema:** Permiten restaurar un equipo a un estado operacional después de un desastre.
- **Copias de seguridad de datos:** Permiten restaurar algunos ficheros después de que hayan sido borrados o dañados accidentalmente.

6.7. Normas de copia de seguridad y respaldo de la información

Para la E.S.E. Municipal de Soacha Julio César Peñaloza es vital poder darles continuidad a las operaciones, para ello se han creado las normas para preservar la información sensible a ser dañada o perdida ante una falla puntual de uno o varios equipos, por la negligencia, ignorancia de los procesos por parte de usuarios. Los backup o copias de seguridad se utilizarán como un medio alterno de respaldo de los archivos e información tramitada por medios electrónicos, con el fin de prevenir los riesgos de pérdida total o parcial de

información en un momento determinado, toda vez que facilitan la continuidad de las actividades de una entidad. Sin embargo, este tipo de medios de soporte, por sí solos no garantizan la preservación de la información a largo plazo, lo que implica que la entidad tengan implementadas, de manera continua y sistemática, unas políticas claras de gestión del riesgo, seguridad de la información, de contingencia y de continuidad del negocio.

Se realizarán copias de respaldo que permitan recuperar datos perdidos accidental o intencionadamente con una antigüedad determinada. Las copias de respaldo disfrutarán de la misma seguridad que los datos originales en lo que se refiere a integridad, confidencialidad, autenticidad y trazabilidad. En particular, se considerará la conveniencia o necesidad de que las copias de seguridad estén cifradas para garantizar la confidencialidad.

- **Las copias de respaldo deberán abarcar:**

✓ Información de trabajo de la organización.
✓ Aplicaciones en explotación, incluyendo los sistemas operativos.
✓ Datos de configuración, servicios, aplicaciones, equipos, u otros de naturaleza análoga.
✓ Claves utilizadas para preservar la confidencialidad de la información.

- **Recuperación de información por medio de los respaldos**

Para garantizar la continuidad de los servicios, en la E.S.E. Municipal de Soacha Julio César Peñaloza todos los datos almacenados en los servidores y dispositivos de almacenamiento se deben copiar de manera regular. De esta forma, se establecen los mecanismos necesarios para garantizar la continuidad de los servicios en caso de pérdida de datos.

✓ Todos los datos del ámbito de aplicación serán periódicamente respaldados en soportes de backup.
✓ El departamento de Tecnología como responsables de la Información y los Servicios, establecerán los ciclos de copia más adecuados para cada tipo de información.
✓ Las copias de respaldo deben abarcar toda la información necesaria para recuperar el servicio en caso de corrupción o pérdida de datos.
✓ Las copias de seguridad estarán guardadas en un lugar seguro con medidas de seguridad físicas, de forma que el personal no autorizado no tenga acceso. Deben estar identificadas y etiquetadas con la información útil que se considere necesaria.
✓ Siempre debe existir una copia adicional almacenada en un armario ignífugo o procedimiento alternativo como medida de recuperación ante desastres y

dependiendo del nivel de seguridad de la información y los servicios prestados, se debe mantener un segundo juego de copias offside, en otro edificio y en armario ignífugo.

- ✓ El traslado de los volúmenes de las copias se debe realizar conforme a la Normativa de intercambio de información y uso de soportes. Se debe definir un procedimiento de recuperación de las copias de seguridad, de forma que incluya las pautas para los diferentes sistemas operativos.

En la E.S.E. Municipal de Soacha Julio César Peñaloza se dispondrá de un procedimiento de copias de respaldo que incluirá, al menos, estos elementos:

- ✓ Nivel de seguridad de la información
- ✓ Periodicidad de las copias de respaldo acorde al tipo de dato o servicio.
- ✓ Ventana de backup más adecuada.
- ✓ Periodos de retención de las copias.
- ✓ Ubicación de los soportes de respaldo.
- ✓ Procedimientos de recuperación de la información.
- ✓ Procedimientos de restauración de los servicios y verificación de la integridad de la información respaldada.
- ✓ Procedimientos de inventario y gestión de soportes para backup
- ✓ Procedimiento de revisión de logs de copias de seguridad.

- **Copia de respaldo de los equipos de usuario**

El departamento de Tecnología es el responsable de la realización de copias de respaldo periódicas de la información en los puestos de trabajo de los usuarios de la entidad, especialmente cuando haya cambios significativos en la información que manejan.

- ✓ En ningún caso se deberán almacenar copias de respaldo en dependencias de terceros ajenas a la entidad si no existe un acuerdo institucional previamente suscrito con el tercero en el que se expliquen las cautelas debidas respecto de la custodia de la información almacenada.
- ✓ Si el usuario trata información corporativa en su puesto de trabajo, El departamento de Tecnología deberán asegurarse de que los empleados a su cargo salvaguardan dicha información de forma satisfactoria dentro de las dependencias de la entidad de acuerdo a los recursos disponibles.
- ✓ En caso de uso de ordenadores portátiles corporativos, el usuario se atendrá a la "Normativa de uso de portátiles corporativos de la E.S.E. Municipal de Soacha

Julio César Peñaloza

- **Tipos de copias de respaldo**

En función del tipo de información, como parte de la estrategia de copias de seguridad, se podrán utilizar los siguientes tipos de copias de respaldo:

- **Copia completa**

✓ Copia completa o FULL copia completa de todos los datos principales, ficheros y bases de datos.
✓ Requiere mayor espacio de almacenamiento y ventana de backup
✓ Ofrece la seguridad de tener una imagen de los datos en el momento de la copia.

- **Copia incremental**

✓ Copia de los datos modificados desde la anterior copia completa o incremental.
✓ Siempre se debe partir de una copia total o completa inicial.
✓ Si se realiza con frecuencia, el proceso no consumirá un tiempo excesivo, debido al bajo volumen de datos a copiar.

- **La restauración completa**

La restauración completa es lenta se requiere recuperar una copia completa y todas las incrementales realizadas hasta el momento en el cual se quiera restaurar el sistema.

- **Copia diferencial**

Copia de los datos que hayan sido modificados respecto a una copia completa anterior.

✓ Requiere menor espacio de almacenamiento y ventana de backup
✓ Se ejecutará con mayor rapidez en función de la frecuencia con que se realice.

- **Restauración diferencial**

Suele ser más rápida que la incremental, ya que basta con recuperar una copia completa y una copia diferencial.

- **Verificación y comprobación de las copias**

Se deben comprobar los registros de logs de las copias de seguridad de forma que, ante una incidencia, sea posible relanzar de nuevo la copia de seguridad. El departamento de Tecnología debe realizar pruebas periódicas de restauración de las copias realizadas, de forma que se garantice la integridad de las mismas. La información del ámbito de aplicación de la entidad, almacenada en un medio informático durante un período prolongado de tiempo, deberá ser verificada al menos una vez al año, para asegurar que la información es recuperable.

- **Responsabilidades**

Todos y cada uno de los involucrados en la Gestión de la Seguridad de la Información en la entidad, velará por el cumplimiento de esta normativa y revisará su correcto cumplimiento, asegurándose de la existencia de un procedimiento de copias de respaldo y recuperación y su implantación efectiva.

6.8. Normas de cumplimiento con requisitos legales y contractuales

Normas dirigidas a:

OFICINA ASESORA JURÍDICA

- La Oficina Asesora Jurídica debe identificar, documentar y mantener actualizados los requisitos legales, reglamentarios o contractuales aplicables a la E.S.E. Municipal de Soacha Julio César Peñaloza y relacionados con seguridad de la información.

EL DEPARTAMNETO DE TECNOLOGIA

- El departamento de Tecnología debe certificar que todo el software que se ejecuta en la E.S.E. Municipal de Soacha Julio César Peñaloza esté protegido por derechos de autor y requiera licencia de uso o, en su lugar sea software de libre distribución y uso.
- Debe establecer un inventario con el software y sistemas de información que se

encuentran permitidos en las estaciones de trabajo o equipos móviles de E.S.E. Municipal de Soacha Julio César Peñaloza para el desarrollo de las actividades laborales, así como verificar periódicamente que el software instalado en dichas estaciones de trabajo corresponda únicamente al permitido.

TODOS LOS USUARIOS

- Los usuarios no deben instalar software o sistemas de información en sus estaciones de trabajo o equipos móviles suministrados para el desarrollo de sus actividades.
- Los usuarios deben cumplir con las leyes de derechos de autor y acuerdos de licenciamiento de software.
- Es ilegal duplicar software o su documentación sin la autorización del propietario de los derechos de autor y, su reproducción no autorizada es una violación de ley; no obstante, puede distribuirse un número de copias bajo una licencia otorgada.

6.9. Normas de privacidad y protección de datos personales

PRINCIPIOS

En todo tratamiento de datos personales que realice la E.S.E. Municipal de Soacha Julio César Peñaloza se aplicarán, los principios consagrados en el Régimen General de Protección de Datos Personales Colombiano, en especial los siguientes:

- Principio de legalidad del tratamiento de datos, para el tratamiento de datos personales realizado por la entidad, se aplican las normas del ordenamiento jurídico colombiano relativas al Régimen General de Tratamiento de Datos Personales y las contenidas en la presente normativa.
- Principio de finalidad, el tratamiento dado a los datos personales que trata, obedecen a las finalidades establecidas en la presente normativa, las cuales están en armonía con el ordenamiento jurídico colombiano. En lo no regulado en la presente política se aplicarán las nomas de carácter superior que la reglamenten, adicionen, modifiquen o deroguen.
- Principio de libertad, el tratamiento que se realice a los datos personales, lo hace de acuerdo a la autorización previa, expresa y consentida del titular de los datos personales.
- Principio de veracidad o calidad, la información sujeta a tratamiento debe ser veraz, completa, actualizada, comprobable y comprensible.

- Principio de transparencia, se debe garantizar que el titular de los datos personales puede obtener información sobre sus datos en cualquier momento y sin restricciones de acuerdo a los procedimientos descritos en la presente normativa.
- Principio de acceso y circulación restringida, se garantiza que el tratamiento de los datos personales dado a las bases de datos de la entidad, se realiza por personas autorizadas por el titular y/o las demás personas permitidas por la ley.
- Principio de seguridad, se implementarán todas las medidas técnicas, humanas y administrativas necesarias para proteger los datos personales tratados en sus bases de datos evitando el uso, la adulteración, la perdida y la consulta no autorizada o no deseada.
- Principio de confidencialidad, el tratamiento dado a los datos personales de bases de datos de la E.S.E. Municipal de Soacha Julio César Peñaloza se realizará con estricta confidencialidad y reserva, de acuerdo a las finalidades descritas en la presente normativa.

Normas dirigidas a:

EL DEPARTAMENTO DE TECNOLOGIA

- El departamento de Tecnología debe establecer los controles para el tratamiento y protección de los datos personales de los beneficiarios, funcionarios, proveedores y demás terceros de la E.S.E. Municipal de Soacha Julio César Peñaloza de los cuales reciba y administre información.
- El departamento de Tecnología debe implantar los controles necesarios para proteger la información personal de los beneficiarios, funcionarios, proveedores u otras terceras partes almacenada en bases de datos o cualquier otro repositorio y evitar su divulgación, alteración o eliminación sin la autorización requerida.

TODOS LOS USUARIOS

- Los usuarios deben guardar la discreción correspondiente, o la reserva absoluta con respecto a la información de la E.S.E. Municipal de Soacha Julio César Peñaloza o de sus funcionarios de cual tengan conocimiento en el ejercicio de sus funciones.
- Es deber de los usuarios, verificar la identidad de todas aquellas personas, a quienes se les entrega información por teléfono, por correo electrónico o por correo certificado, entre otros.