PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

	ELABORÓ	REVISÓ			APROBÓ
FIRMA					
NOMBRE	Roosbelth Gaona López	Johan Andrés Sánchez Ruiz	Dra. Johana Bolívar Cuellar	Dr. Jorge Enrique Pedraza	Dr. Diego Alejandro García Londoño
CARGO	Referente TIC	Referente Planeación	Referente Calidad	Subgerente Administrativo y Financiero	Gerente

TABLA DE CONTENIDO

INTRODUCCIÓN

La Empresa Social del Estado Región de Salud Soacha, a través del área de Tecnologías de Información y Comunicación TIC, busca adherir los procesos por medio de la implementación de mejores prácticas dadas por el Departamento Administrativo de la Función Pública DAFP con la estrategia MIPG y, el ministerio de las Tecnologías de Información y Comunicación en el diagnóstico, planificación, implementación, gestión y mejoramiento continuo, del Modelo de Seguridad y Privacidad de la Información.

El Modelo de Seguridad y Privacidad de la Información, pretende lograr en la institución y sus clientes internos, externos y partes interesadas, confianza en el manejo de la información garantizando la privacidad, continuidad, integralidad y disponibilidad de los datos.

1 CAPITULO 1. GENERALIDADES

1.1 Objetivo

Fortalecer la integridad, confidencialidad y disponibilidad de los activos de información y reducir los riesgos a los que está expuesta la institución hasta niveles aceptables, a partir de la implementación de estrategias de seguridad digital definidas en este documento.

Establecer los lineamientos de buenas prácticas en Seguridad y Privacidad de la información para el uso de los recursos tecnológicos de la Empresa Social del Estado Región de Salud Soacha.

1.1.1 Objetivos Específicos

- Establecer los lineamientos de buenas prácticas en Seguridad y Privacidad de la información para el uso de los recursos tecnológicos de la Empresa Social del Estado Región de Salud Soacha.
- Definir lineamientos internos de seguridad de la información, dando cumplimiento a la normatividad vigente.
- Promover el uso de mejores prácticas de seguridad de la información en de la Empresa Social de Estado Región Salud Soacha.

1.2 Alcance

El Plan de Seguridad y Privacidad de la Información, está dirigido a todos los funcionarios de la Empresa Social del Estado Región de Salud Soacha, a sus recursos, procesos y procedimientos tanto internos como externos, así mismo al personal vinculado a la entidad y terceros, que usen activos de información que sean propiedad de la entidad.

1.3 Control de cambios

FECHA	VERSIÓN	DESCRIPCIÓN
31/01/2023	00	Creación documento, cambio de razón social
31/01/2024	01	Actualización del documento
28/01/2025	02	Actualización del documento

1.4 Definiciones

Confidencialidad: se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.

Integridad: se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.

Disponibilidad: se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

Confiabilidad De La Información: es decir, que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

Información: se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.

Sistema De Información: se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.

Tecnología de la Información: se refiere al hardware y software operado por la institución o por un tercero que procese información, para llevar a cabo una función propia de la Empresa Social del Estado Región de Salud Soacha, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).

Amenazas: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

Ciber Seguridad: Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).

Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

SGSI: Sistema de Gestión de la Seguridad de la Información.

1.5 Normatividad

Constitución Política de Colombia. Artículos 15, 20, 23 y 74.

Ley 23 de 1982. Sobre derechos de autor.

Ley 44 de 1993. Por la cual se modifica y adiciona la Ley 23 de 2082 y se modifica la Ley 29 de 2044 y Decisión Andina 351 de 2015 (Derechos de autor).

Ley 527 de 1999. Por la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales y se establecen las entidades de certificación y se dictan otras disposiciones. Ley 594 de 2000. Por medio de la cual se regula el Derecho Fundamental de Petición y se sustituye un título del Código de Procedimiento Administrativo y de lo Contencioso Administrativo.

Ley 962 de 2005. Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos.

Ley 1221 del 2008. Por la cual se establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones.

Ley 1266 diciembre de 2008. Por la cual se dictan disposiciones generales del habeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

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 1341 del 30 Julio de 2009. Por la cual se definen principios y conceptos sobre la sociedad de la información y organización de las tecnologías de la información y comunicaciones.

Ley 1438 de 2011. Por medio del cual se reforma el sistema general de Seguridad Social en Salud y se dictan otras disposiciones. Parágrafo "transitorio" del Artículo 112 "La historia clínica única electrónica será de obligatoria aplicación antes del 31 de Diciembre de 2013.

Ley 1581 de 2012, Art 3. Autorización Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales.

Ley 2088 de 2012. Por la cual se regula el trabajo en casa y se dictan otras disposiciones.

Ley 1712 de 2014. Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.

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.

Decreto 1499 de 2017 Se modifica el decreto 1083 de 2015 y se definen los lineamientos del modelo integral de planeación y gestión para el desarrollo administrativo y la gestión de la calidad para la gestión pública.

Directiva 26 de 2020. Diligenciamiento de la información en el índice de transparencia y acceso a la información – ITA – de conformidad con las disposiciones del artículo 23 de la ley 1712 de 2014.

Resolución 500 de 2021. Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital.

Norma Técnica ISO/IEC 27000. Activo En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización.

Guía de Gestión de Riesgos Ministerio de Tecnologías de Información y Comunicación – MINTIC.

2 CAPITULO 2. PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El equipo de colaboradores de la Empresa Social del Estado Región de Salud Soacha se encuentra 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, todo enmarcado en el estricto cumplimiento de las leyes en concordancia con la misión y la visión de la entidad y los procesos establecidos para su operación.

De igual forma estamos comprometidos en satisfacer las expectativas tanto de los usuarios externos como internos de la tal manera que los diferentes procesos adopten buenas prácticas que permitan garantizar la confiabilidad, oportunidad, confidencialidad, seguridad y acceso a la información.

2.1 Seguridad de las Operaciones

La entidad protege la información, los datos y sus activos de información, mediante seguridad interna y externa, la cual es contratada en el inicio del año con proveedores tecnológicos que ofertan opciones seguras, rentables y acordes a las necesidades de la Empresa Social del Estado Región de Salud Soacha.

La Seguridad UTM (gestión unificada de amenazas) protege a la entidad de amenazas externas que deseen ingresar por la red o servicios externos. El antivirus instalado en los equipos de cómputo, cumple con verificar las fuentes seguras en internet, análisis de correos entrantes, bloqueo de dispositivos de almacenamiento, informes y otras opciones de seguridad que permiten identificar virus y amenazas internas.

2.2 Adquisición, Desarrollo Y Mantenimiento de Sistemas de Información

El mantenimiento de los sistemas de información se realiza acorde a las funciones, características, errores, uso y acciones preventivas para cada uno, los cuales se dividen entre mantenimientos preventivos y correctivos. La entidad ha documentado procedimientos donde se describen las acciones de operación para la continuidad del servicio, estos documentos están disponibles en la intranet, mediante la siguiente codificación:

- SIS_FTO_03 CRONOGRAMA MANTENIMIENTO DE EQUIPOS.xlsx
- SIS_FTO_06 CONTROL DE MANTENIMIENTO SISTEMAS.xlsx

2.3 Aspectos de Seguridad de la Información de la Gestión de Continuidad de Negocio

Algunos procesos institucionales cuentan con manuales, planes, procedimientos y formatos que garantizan la continuidad en la prestación de servicios, ante algún desastre o incidente crítico, estos son actualizados e integrados con las demás áreas.

2.4 Fase De Planificación

Para la Empresa Social del Estado Región de Salud Soacha, la protección de la información busca la disminución del impacto generado sobre sus activos en cuanto a su integridad, disponibilidad y confidencialidad de la información además de mitigar los riesgos a los que se puede ver expuesta, con objeto de prevenir amenazas internas o externas que afecten el funcionamiento de la institución.

Integrar el modelo Planificar, Hacer, Verificar y Actuar (PHVA) a los procesos del Sistema de Gestión de la Seguridad (SGSI) planteado en la norma ISO/IEC 27001 para:

- Planificar - Establecer lineamientos, objetivos, procesos y procedimientos de seguridad pertinentes para gestionar el riesgo y mejorar la seguridad de la información, acorde con los objetivos globales de la Institución.
- Hacer - Implementar y operar las buenas prácticas, los controles, procesos y procedimientos del SGSI.
- Verificar - medir y evaluar el desempeño de los procesos y lineamientos, de acuerdo a los resultados realizar planes de acción para la mejora continua.
- Actuar - Emprender acciones correctivas y preventivas con base en los resultados de la auditoría interna del SGSI y la revisión por la dirección, para lograr la mejora continua del SGSI.

El proceso de TI de la información de la Empresa Social del Estado Región de Salud Soacha, para la vigencia 2025 seguirá implementando lineamientos de Seguridad y Privacidad de la Información.

2.4.1 Gestión De Incidentes De Seguridad De La Información.

La Empresa Social del Estado Región de Salud Soacha promoverá entre los funcionarios, empleados, contratistas de prestación de servicios y personal provisto por terceras partes el reporte de incidentes relacionados con la seguridad de la información y sus medios de procesamiento, incluyendo cualquier tipo de medio de almacenamiento de información, como la plataforma tecnológica, los sistemas de información, los medios físicos de almacenamiento y las personas. Es responsabilidad de los funcionarios, empleados, contratistas de prestación de servicios y personal provisto por terceras partes el reportar cualquier evento o incidente relacionado con la información y/o los recursos tecnológicos con la mayor prontitud posible. En caso de conocer la pérdida o divulgación no autorizada de información clasificada como uso interno, reservada o restringida, deben notificarlo al proceso Administrativo para que se registre y se le dé el trámite necesario.

La Alta Dirección o a quien delegue, son los únicos autorizados para reportar incidentes de seguridad ante las autoridades; así mismo, son los únicos canales de comunicación autorizados para hacer pronunciamientos oficiales ante entidades externas.

2.4.2 Capacitación Y Sensibilización En Seguridad De La Información

El Proceso de Gestión Administrativa debe convocar a los funcionarios, empleados y contratistas a las charlas y eventos programados como parte del programa de formación en seguridad de la información, proveer los recursos para la ejecución de las capacitaciones y controlar la asistencia a dichas charlas y eventos.

Los funcionarios, empleados, contratistas de prestación de servicios y personal provisto por terceras partes que por sus funciones o actividades hagan uso de la información, deben dar cumplimiento a los lineamientos, normas y procedimientos de seguridad de la información, así como asistir a las capacitaciones que sean referentes a la seguridad de la información.

2.5 Gestión de Activos

2.5.1 Identificación, clasificación y control de activos de información

La Empresa Social de Estado Región Salud Soacha a través del Comité de Archivo realizará la supervisión de cada proceso, el cual debe aprobar el inventario de los activos de información que procesa y produce la entidad, estas características del inventario deben establecer la clasificación, valoración, ubicación y acceso de la información, correspondiendo al Proceso de TICS y al Proceso de Gestión Documental brindar herramientas que permitan la administración del inventario por cada área, garantizando la disponibilidad, integridad y confidencialidad de los datos que lo componen.

El Proceso de Recursos Físicos con apoyo técnico operativo del proceso de sistemas es responsable de mantener el inventario actualizado de los recursos de hardware y software de la entidad.

2.6 Control de Acceso

2.6.1 Acceso a redes y recursos de red

El Referente TICS de la Empresa Social de Estado Región de Salud Soacha, como responsable de las redes de datos y los recursos de red de la entidad, debe propender porque dichas redes sean debidamente protegidas contra accesos no autorizados a través de mecanismos de control de acceso lógico.

Pautas para tener en cuenta:

- El proceso Gestión de TICS debe asegurar que las redes inalámbricas de la Empresa Social de Estado Región Salud Soacha cuenten con métodos de autenticación que evite accesos no autorizados.

- El proceso Gestión de TICS debe establecer controles para la identificación y autenticación de los usuarios provistos por terceras partes en las redes o recursos de red de la Empresa Social de Estado Región de Salud Soacha, así como velar por la aceptación de las responsabilidades de dichos terceros. Además, se debe formalizar la aceptación de los lineamientos de Seguridad de la Información por parte de estos.
- Los funcionarios y personal provisto por terceras partes, antes de contar con acceso lógico por primera vez a la red de datos de la Empresa Social de Estado Región de Salud Soacha, deben contar con el formato de creación de cuentas de usuario debidamente autorizado y el acuerdo de Confidencialidad firmado previamente.
- Los equipos de cómputo de usuario final que se conecten o deseen conectarse a las redes de datos de la institución, deben cumplir con todos los requisitos o controles para autenticarse en ellas y únicamente podrán realizar las tareas para las que fueron autorizados.

2.6.2 Administración de acceso de usuarios

La Empresa Social de Estado Región de Salud Soacha, establecerá privilegios para el control de acceso lógico de cada usuario o grupo de usuarios a las redes de datos, los recursos tecnológicos y los sistemas de información de la Entidad. Así mismo, velará porque los funcionarios y el personal provisto por terceras partes tengan acceso únicamente a la información necesaria para el desarrollo de sus labores y porque la asignación de los derechos de acceso esté regulada por normas establecidas para tal fin.

Pautas para tener en cuenta

- El proceso Gestión de TICS, debe definir lineamientos para la configuración de contraseñas que aplicarán sobre la plataforma tecnológica, los servicios de red y los sistemas de información; dichos lineamientos deben considerar aspectos como longitud, complejidad, cambio periódico, control histórico, bloqueo por número de intentos fallidos en la autenticación y cambio de contraseña en el primer acceso, entre otros.
- El proceso Gestión de TICS debe establecer un procedimiento que asegure la eliminación, reasignación o bloqueo de los privilegios de acceso otorgados sobre los recursos tecnológicos, los servicios de red y los sistemas de información de manera oportuna, cuando los funcionarios se desvinculan, toman licencias, vacaciones, son trasladados o cambian de cargo.
- El proceso Gestión de TICS debe asegurarse que los usuarios o perfiles de usuario que tienen asignados por defecto los diferentes recursos de la plataforma tecnológica sean inhabilitados o eliminados.
- Es responsabilidad de los propietarios de los activos de información, definir los perfiles de usuario y autorizar, conjuntamente con el proceso Gestión de TICS, las solicitudes de acceso a dichos recursos de acuerdo con los perfiles establecidos.

2.6.3 Control de acceso a sistemas de información y aplicativos

La Empresa Social de Estado Región de Salud Soacha, como propietario de los sistemas de información y aplicativos que apoyan los procesos, velará por la asignación, modificación y revocación de privilegios de accesos al sistema de información o aplicativos de manera controlada.

El proceso Gestión de TICS, como responsable de la administración de dichos sistemas de información y aplicativos, propende para que estos sean debidamente protegidos contra accesos no autorizados a través de mecanismos de control de acceso lógico. Así mismo, vela porque los desarrolladores, tanto internos como externos, acojan buenas prácticas de desarrollo en los productos generados para controlar el acceso lógico y evitar accesos no autorizados a los sistemas administrados.

Pautas para tener en cuenta

- Los propietarios de los activos de información deben autorizar los accesos a sus sistemas de información o aplicativos, de acuerdo con los perfiles establecidos y las necesidades de uso, acogiendo los procedimientos establecidos. De igual forma se deben monitorear anualmente los perfiles definidos en los sistemas de información y los privilegios asignados a los usuarios que acceden a ellos.
- El proceso Gestión de TICS debe establecer el protocolo y los controles de acceso a los ambientes de producción de los sistemas de información; así mismo, debe asegurarse que los desarrolladores internos o externos, posean acceso limitado y controlado a los datos y archivos que se encuentren en los ambientes de producción.
- El proceso Gestión de TICS debe proporcionar repositorios de archivos fuente de los sistemas de información; estos deben contar con acceso controlado y restricción de privilegios, además de un registro de acceso a dichos archivos.
- Los desarrolladores deben asegurar que los sistemas de información construidos requieran autenticación para todos los recursos y páginas, excepto aquellas específicamente clasificadas como públicas.
- Los desarrolladores deben certificar que no se almacenen contraseñas, cadenas de conexión u otra información sensible en texto claro y que se implementen controles de integridad de dichas contraseñas.

2.7 Seguridad física

La Empresa Social de Estado Región Salud Soacha provee la implantación y vela por la efectividad de los mecanismos de seguridad física y control de acceso que aseguren el perímetro de sus instalaciones en todas sus áreas. Así mismo, controlará las amenazas físicas externas e internas y las condiciones medioambientales de sus oficinas.

Todas las áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, se considera áreas de acceso restringido.

Se debe tener acceso controlado y restringido a donde se encuentra los servidores y el cuarto de comunicaciones. El proceso Gestión de TICS mantiene las normas, controles y registros de acceso a dichas áreas.

Pautas para tener en cuenta

- Las solicitudes de acceso al área donde se encuentra el servidor o los centros de cableado deben ser aprobados por funcionarios que apoyan el proceso Gestión de TICS autorizados; no obstante, los visitantes siempre deberán estar acompañados de un funcionario.
- El proceso Gestión de TICS debe asegurar que las labores de mantenimiento de redes eléctricas, de voz y de datos, sean realizadas por personal idóneo y apropiadamente autorizado e identificado.
- La Gerencia de la Empresa Social de Estado Región Salud Soacha deberá proporcionar los recursos necesarios para ayudar a proteger, regular y velar por el perfecto estado de los controles físicos implantados en las instalaciones del hospital.
- Los ingresos y egresos de personal a las instalaciones de la Empresa Social de Estado Región Salud Soacha en horarios no laborales deben ser registrados; por consiguiente, los funcionarios y personal provisto por terceros deben cumplir completamente con los controles físicos implantados.
- Los funcionarios deben portar el carné que los identifica como tales en un lugar visible mientras se encuentren en las instalaciones de la Empresa Social de Estado Región Salud Soacha; en caso de pérdida del carné, deben reportarlo a la mayor brevedad posible al área de Talento Humano.
- Aquellos funcionarios o personal provisto por terceros para los que aplique, en razón del servicio prestado, deben utilizar prendas distintivas que faciliten su identificación.

2.8 Seguridad para los equipos

La Empresa Social de Estado Región Salud Soacha para evitar la pérdida, robo o exposición al peligro de los recursos de la plataforma tecnológica de la entidad que se encuentren dentro o fuera de sus instalaciones, proveerá los recursos que garanticen la mitigación de riesgos sobre dicha plataforma tecnológica.

Pautas para tener en cuenta

- El proceso Gestión de TICS debe proveer los mecanismos y estrategias necesarios para proteger la confidencialidad, integridad y disponibilidad de los recursos tecnológicos, dentro y fuera de las instalaciones de la Empresa Social de Estado Región Salud Soacha.

- El proceso Gestión de TICS debe realizar soportes técnicos y velar que se efectúen los mantenimientos preventivos y correctivos de los recursos de la plataforma tecnológica de la EMPRESA SOCIAL DE ESTADO REGIÓN SALUD SOACHA.
- El proceso Gestión de TICS en conjunto con el proceso Gestión de Recursos Físicos, debe propender porque las áreas de carga y descarga de equipos de cómputo se encuentren aisladas del área donde se ubica el servidor y otras áreas de procesamiento de información.
- El proceso Gestión de TICS debe generar estándares de configuración segura para los equipos de cómputo de los funcionarios de la entidad y configurar dichos equipos acogiendo los estándares generados.
- El proceso Gestión de TICS debe establecer las condiciones que deben cumplir los equipos de cómputo de personal provisto por terceros, que requieran conectarse a la red de datos de la entidad y verificar el cumplimiento de dichas condiciones antes de conceder a estos equipos acceso a los servicios de red.
- El proceso Gestión de TICS debe generar y aplicar lineamientos para la disposición segura de los equipos de cómputo de los funcionarios de la entidad, ya sea cuando son dados de baja o cambian de usuario.
- El proceso Gestión de Recursos Físicos debe velar porque la entrada y salida de estaciones de trabajo, servidores, equipos portátiles y demás recursos tecnológicos institucionales de las instalaciones de la Empresa Social de Estado Región Salud Soacha revisando que se cuente con la autorización documentada y aprobada previamente por el área.
- El proceso Gestión de Recursos Físicos debe velar porque los equipos que se encuentran sujetos a traslados físicos fuera de la entidad y posean las pólizas de seguro.
- El proceso Gestión de TICS es la única área autorizada para realizar movimientos y asignaciones de recursos tecnológicos; por consiguiente, se encuentra prohibida la disposición que pueda hacer cualquier funcionario de los recursos tecnológicos de la Empresa Social de Estado Región Salud Soacha.
- Las estaciones de trabajo, dispositivos móviles y demás recursos tecnológicos asignados a los funcionarios y personal provisto por terceras partes deben acoger las instrucciones técnicas que proporcione el proceso Gestión de TICS.
- Cuando se presente una falla o problema de hardware o software u otro recurso tecnológico propiedad de la Empresa Social de Estado Región Salud Soacha, el usuario responsable debe informar al proceso Gestión de TICS, con el fin de realizar una asistencia adecuada. El usuario no debe intentar solucionar el problema.
- La instalación, reparación o retiro de cualquier componente de hardware o software de las estaciones de trabajo, dispositivos móviles y demás recursos tecnológicos de la entidad, solo puede ser realizado por el personal asignado al proceso de Gestión de TICS.
- Los equipos de cómputo, bajo ninguna circunstancia, deben ser dejados desatendidos en lugares públicos o a la vista, en el caso de que estén siendo transportados.
- Los equipos de cómputo deben ser transportados con las medidas de seguridad apropiadas, que garanticen su integridad física.
- Los equipos portátiles siempre deben ser llevados como equipaje de mano y se debe tener especial cuidado de no exponerlos a fuertes campos electromagnéticos.

- En caso de pérdida o robo de un equipo de cómputo, se debe informar de forma inmediata al líder del proceso para que se inicie el trámite interno y se debe poner la denuncia ante la autoridad competente.
- Los funcionarios de la entidad y el personal provisto por terceros deben asegurar que sus escritorios se encuentran libres de los documentos que son utilizados durante el desarrollo de sus funciones al terminar la jornada laboral y, que estos sean almacenados bajo las protecciones de seguridad necesarias.

2.9 Uso adecuado de internet

La Empresa Social de Estado Región Salud Soacha consciente de la importancia del servicio de Internet como una herramienta para el desempeño de labores, proporcionará los recursos necesarios para asegurar su disponibilidad a los usuarios que así lo requieran para el desarrollo de sus actividades diarias en la entidad.

Pautas para tener en cuenta

- El proceso Gestión de TICS debe proporcionar los recursos necesarios para la implementación, administración y mantenimiento requeridos para la prestación segura del servicio de Internet, bajo las restricciones de los perfiles de acceso establecidos.
- El proceso Gestión de TICS debe diseñar e implementar mecanismos que permitan la continuidad o restablecimiento del servicio de Internet en caso de contingencia interna.
- El proceso Gestión de TICS debe monitorear continuamente el canal o canales del servicio de Internet.
- El proceso Gestión de TICS debe establecer e implementar controles para evitar la descarga de software no autorizado, evitar código malicioso proveniente de Internet y evitar el acceso a sitios catalogados como restringidos.
- El proceso Gestión de TICS debe generar registros de la navegación y los accesos de los usuarios a Internet, así como establecer e implantar el monitoreo sobre la utilización del servicio de Internet.
- Los usuarios del servicio de Internet de la Empresa Social de Estado Región Salud Soacha deben hacer uso del mismo en relación con las actividades laborales que así lo requieran.
- Los usuarios del servicio de Internet deben evitar la descarga de software desde internet, así como su instalación en las estaciones de trabajo o dispositivos móviles asignados para el desempeño de sus labores.
- 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 lineamientos establecidos en este documento.
- Los usuarios del servicio de internet tienen prohibido el acceso y el uso de servicios interactivos o mensajería instantánea como Facebook, Kazaa, MSN, Yahoo, Skype, Net2phome y otros similares, que tengan como objetivo crear comunidades para intercambiar

información, o bien para fines diferentes a las actividades propias de la Empresa Social de Estado Región Salud Soacha.

- No está permitida 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 proceso Gestión de TICS o a quien haya sido delegada de forma explícita para esta función, asociando los procedimientos y controles necesarios para el monitoreo y aseguramiento del buen uso del recurso.
- No está permitido el intercambio no autorizado de información de propiedad de la Empresa Social de Estado Región Salud Soacha, de los funcionarios, con terceros.

2.10 Privacidad Y Confidencialidad.

2.10.1 Tratamiento y protección de datos personales.

En cumplimiento de la de Ley 1581 de 2012 y reglamentada parcialmente por el Decreto Nacional 1377 de 2013, por la cual se dictan disposiciones para la protección de datos personales, la Empresa Social de Estado Región Salud Soacha a través del Comité de Gobierno en Línea, propende por la protección de los datos personales de los usuarios, funcionarios, proveedores y terceros de los cuales reciba y administre información.

Se establece los términos, condiciones y finalidades para las cuales la Empresa Social de Estado Región Salud Soacha, como responsable de los datos personales obtenidos a través de sus distintos canales de atención, tratará la información de todas las personas que en algún momento, por razones de la actividad que desarrolla la entidad, hayan suministrado datos personales. En caso de delegar a un tercero el tratamiento de datos personales, la Empresa Social de Estado Región Salud Soacha, exigirá al tercero la implementación de los lineamientos y procedimientos necesarios para la protección de los datos personales. Así mismo, busca proteger la privacidad de la información personal de sus funcionarios, estableciendo los controles necesarios para preservar aquella información de la entidad conozca y almacene de ellos, velando porque dicha información sea utilizada únicamente para funciones propias de la EMPRESA SOCIAL DE ESTADO REGIÓN SALUD SOACHA. y no sea publicada, revelada o entregada a funcionarios o terceros sin autorización.

Teniendo en cuenta lo anterior, la Empresa Social de Estado Región Salud Soacha, dispone de la Política de Tratamiento de Datos Personales, la que se encuentra publicada en el sitio web de la institución, en la Superintendencia de Industria y Comercio y en la Intranet institucional.

Pautas para tener en cuenta

- Los procesos que gestionan y procesan datos personales de usuarios, funcionarios, proveedores o terceros, deben obtener la autorización para el tratamiento de estos datos con el fin de recolectar, transferir, almacenar, usar, circular, suprimir, compartir, actualizar y transmitir dichos datos personales en el desarrollo de las actividades de la entidad.
- Los procesos que gestionan y procesan datos personales de usuarios, funcionarios, proveedores o terceros, deben asegurar que solo aquellas personas que tengan una relación laboral formal con la Empresa Social de Estado Región de Salud Soacha puedan tener acceso a dichos datos.
- Los procesos que gestionan y procesan datos personales de usuarios, funcionarios, proveedores o terceros, deben establecer condiciones contractuales y de seguridad a las entidades vinculadas o aliadas delegadas para el tratamiento de dichos datos personales.
- Los procesos que gestionan y procesan datos personales de usuarios, funcionarios, proveedores o terceros, deben acoger las directrices técnicas y procedimientos establecidos para el intercambio de estos datos con los terceros delegados para el tratamiento de dichos datos personales.
- Los procesos que gestionan y procesan datos personales de usuarios, funcionarios, proveedores o terceros, deben acoger las directrices técnicas y procedimientos establecidos para enviar a los usuarios, proveedores o terceros mensajes, a través de correo electrónico y/o mensajes de texto.
- El Comité de Gobierno en Línea debe establecer los controles para el tratamiento y protección de los datos personales de los usuarios, funcionarios, proveedores y demás terceros de la Empresa Social de Estado Región Salud Soacha de los cuales reciba y administre información.
- El proceso Gestión de TIC´s debe implantar los controles necesarios para proteger la información personal de los usuarios, 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.
- Los usuarios y funcionarios deben guardar la discreción correspondiente, o la reserva absoluta con respecto a la información de la entidad o de sus funcionarios de cual tengan conocimiento en el ejercicio de sus funciones. Es deber de los usuarios y funcionarios, verificar la identidad de todas aquellas personas, a quienes se les entrega información por teléfono, por correo electrónico o por correo certificado, entre otros.
- Los usuarios de las herramientas informáticas y sistema de información de la EMPRESA SOCIAL DE ESTADO REGIÓN SALUD SOACHA. Hospital Mario Gaitán Yaguas de Soacha deben asumir la responsabilidad individual sobre la clave de acceso a dichas herramientas que se les suministre; así mismo, deben cambiar de manera periódica esta clave de acceso.

2.11 Disponibilidad del Servicio e Información.

La EMPRESA SOCIAL DE ESTADO REGIÓN DE SALUD SOACHA. Hospital Mario Gaitán Yaguas de Soacha con el propósito de garantizar la disponibilidad de la información y mantener los servicios ofrecidos por la entidad, decidió crear una política para proveer el funcionamiento correcto y seguro de la información y medios de comunicación.

2.12 Continuidad, Contingencia y Recuperación de la Información.

La EMPRESA SOCIAL DE ESTADO REGIÓN DE SALUD SOACHA proporcionará los recursos suficientes para facilitar una respuesta efectiva a los funcionarios y para los procesos en caso de contingencia o eventos catastróficos que se presenten en la entidad y que afecten la continuidad de su operación y servicio.

2.13 Copias de Seguridad.

Toda información que pertenezca a los activos de información institucional, sistema de información o que sea de interés para un proceso operativo o misional de carácter crítico, debe ser respaldada por copias de seguridad tomadas de acuerdo a los procedimientos documentados por el Comité de Gobierno en línea. Dicho procedimiento debe incluir las actividades de almacenamiento de las copias en sitios seguros.
Los procesos de la Empresa Social De Estado Región Salud Soacha deben realizar pruebas controladas para asegurar que las copias de seguridad pueden ser correctamente leídas y restauradas.
Los registros de copias de seguridad deben ser guardados en una base de datos creada para tal fin. El proceso Gestión de TIC´s debe proveer las herramientas para que las dependencias puedan administra la información y registros de copias de seguridad.
La creación de copias de seguridad de archivos usados, custodiados o producidos por usuarios individuales es responsabilidad exclusiva de dichos usuarios.

Pautas para tener en cuenta

- El Comité de Gobierno en Línea, debe reconocer las situaciones que serán identificadas como emergencia o desastre para la entidad, los procesos o las áreas y determinar cómo se debe actuar sobre las mismas.
- El Comité de Gobierno en Línea, debe liderar los temas relacionados con la continuidad de la entidad y la recuperación ante desastres.
- El Comité de Gobierno en Línea debe realizar los análisis de impacto en la entidad y los análisis de riesgos de continuidad para, posteriormente proponer posibles estrategias de recuperación en caso de activarse el plan de contingencia o continuidad, con las consideraciones de seguridad de la información a que haya lugar.

- El Comité de Gobierno en Línea debe validar que los procedimientos de contingencia, recuperación y retorno a la normalidad incluyan consideraciones de seguridad de la información.
- El Comité de Gobierno en Línea, debe asegurar la realización de pruebas periódicas del plan de recuperación ante desastres y/o continuidad de entidad, verificando la seguridad de la información durante su realización y la documentación de dichas pruebas.

2.14 Anexos:

- ✓ SIS_FTO_03 CRONOGRAMA MANTENIMIENTO DE EQUIPOS.xlsx
- ✓ SIS_FTO_03 CRONOGRAMA PLAN DE SEGURIDAD Y PRIVACIDAD INFORMACION.xlsx
- ✓ SIS_FTO_06 CONTROL DE MANTENIMIENTO SISTEMAS.xlsx

2.15 Cronogramas Plan De Seguridad Y Privacidad De La Información

ACTIVIDADES		TRIMESTRE I						TRIMESTRE II						TRIMESTRE III						TRIMESTRE IV					
		ENE		FEB		MAR		ABR		MAY		JUN		JUL		AGO		SEP		OCT		NOV		DIC	
ÁREA	ACTIVIDAD	P	E	P	E	P	E	P	E	P	E	P	E	P	E	P	E	P	E	P	E	P	E	P	E
TECNOLOGIAS DE INFORMACIÓN Y COMUNICACIÓN	1. Entrega de Actividades del Plan de Seguridad y Privacidad de la información (En cumplimiento a el Plan 12 del Decreto 612 MIPG).																							P	
	2. Desarrollo de MSPI para identifica estado actual en cumplimiento a ISO 27001 y programar actividades en cumplimiento a las guías entregadas por MINTIC.											P												P	
	3. Conformación de comité de SGSI definiendo roles y responsabilidades para el desarrollo de controles en la vigencia 2024.											P												P	

2.16 Cronograma Mantenimiento Equipos De Computo

ACTIVIDADES		TRIMESTRE I						TRIMESTRE II						TRIMESTRE III						TRIMESTRE IV					
		ENE		FEB		MAR		ABR		MAY		JUN		JUL		AGO		SEP		OCT		NOV		DIC	
ÁREA	ACTIVIDAD	P	E	P	E	P	E	P	E	P	E	P	E	P	E	P	E	P	E	P	E	P	E	P	E
TECNOLOGIAS DE INFORMACIÓN Y COMUNICACIÓN	1. Limpieza de cache y desfragmentacion de disco									P														P	
	2. Actualizacion de Sistemas operativo Windows									P														P	
	3. Comprobacion de Sectores de Disco duro; un estado viable superior a 80%									P														P	
	4. Mantimiento preventivo y correctivo de equipos de cómputo.									P														P	
	5. Cambio de Pantallla, Teclado, mouse en caso de fortuido cambio total de equipo									P														P	