1. INTRODUCCIÓN

A través de los años se ha sostenido la infraestructura tecnológica solo con fines de prestar y mantener un servicio a usuarios dando el mejor soporte a ellos, pero en la actualidad esos esfuerzos ya no son suficientes para conservar y preservar de forma segura la información en los entornos institucionales, debido a que la tecnología, el conocimiento y los riesgos se han desarrollado de manera exponencial lo cual ha llevado a las entidades a incrementar las inversiones en elementos, equipos y profesionales para la implementación de sistemas que permitan estar a la vanguardia de los retos que deben ser afrontados como respuesta a la evolución.

2. OBJETIVO

La Empresa de Salud ESE del Municipio de Soacha generara pautas para la prestación de servicios a la comunidad de forma continua e interrumpida.

También con ello se buscar fomentar el uso y apropiación de la Política de Seguridad vigente en los funcionarios y contratistas de la Empresa de Salud ESE del Municipio de Soacha. Para poder reducir las brechas de seguridad, de forma ordenada y guiada por los parámetros dictaminados desde el Ministerio de las TIC's. Estableciendo 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 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 Empresa de Salud ESE del Municipio de Soacha conforme a los dominios del marco de referencia; involucrando y prestando apoyo a todos los usuarios que tengan interacción con los servicios tecnológicos facilitados por la entidad. 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. POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Las Políticas de Seguridad y privacidad de la Información protegen a la Empresa de Salud ESE del Municipio de Soacha de una amplia gama de amenazas, a fin de garantizar la continuidad de los sistemas de información, minimizar los riesgos de daño y asegurar el eficiente cumplimiento de los objetivos de la Empresa de Salud ESE del Municipio de Soacha.
La información se cataloga como un recurso que, como el resto de los activos, tiene valor para la entidad y por consiguiente debe ser debidamente protegida.
Es importante que dicha política se conviertan en una cultura organizacional asegurando así un compromiso manifiesto por el personal de la Empresa.

4.1. Objetivos

A. Proteger los recursos de información de la Empresa de Salud ESE del Municipio de Soacha y la tecnología utilizada para su operación, frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.
B. Asegurar la implementación de las medidas de seguridad comprendidas en esta Política, identificando los recursos y las partidas presupuestarias correspondientes, sin que ello implique necesariamente la asignación de partidas adicionales.
C. Mantener la Política de Seguridad y privacidad de la información, de la Empresa de Salud ESE del Municipio de Soacha actualizada, a efectos de asegurar su vigencia y nivel de eficacia.

4.2 Alcance

Esta Política se aplica en todo el ámbito de la Empresa de Salud ESE del Municipio de Soacha, a sus recursos y a la totalidad de los procesos, ya sean internos o externos vinculados a la entidad a través de contratos o acuerdos con terceros.

4. 3 Nivel de cumplimiento

Todas las personas cubiertas por el alcance y aplicabilidad deberán dar cumplimiento a esta política.
A continuación, se establecen las políticas que soportan el plan de seguridad y privacidad de la información de Empresa de Salud ESE del Municipio de Soacha.

A. La Empresa de Salud ESE del Municipio de Soacha ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, amparado en lineamientos claros alineados a las necesidades de la entidad, y a los requerimientos regulatorios que le aplican a su naturaleza.
B. Las responsabilidades frente a la seguridad de la información serán definidas, compartidas,

publicadas y aceptadas por cada uno de los empleados, contratistas o terceros.

C. La Empresa de Salud ESE del Municipio de Soacha protege la información generada, procesada resguardada por los procesos de la entidad y activos de información que hacen parte de los mismos.
D. La Empresa de Salud ESE del Municipio de Soacha protege la información creada, procesada, transmitida o resguardada por sus 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.
E. La Empresa de Salud ESE del Municipio de Soacha protege su información de las amenazas originadas por parte del personal.
F. La Empresa de Salud ESE del Municipio de Soacha protege las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
G. La Empresa de Salud ESE del Municipio de Soacha controla la operación de sus procesos de la entidad garantizando la seguridad de los recursos tecnológicos y las redes de datos.
H. La Empresa de Salud ESE del Municipio de Soacha implementa controles de acceso a la información, sistemas y recursos de red.
I. La Empresa de Salud ESE del Municipio de Soacha garantiza que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
J. La Empresa de Salud ESE del Municipio de Soacha garantiza 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.
K. La Empresa de Salud ESE del Municipio de Soacha garantiza la disponibilidad de sus procesos de la entidad y la continuidad de su operación basada en el impacto que pueden generar los eventos.

La Empresa de Salud ESE del Municipio de Soacha garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas

4.4 Manual de políticas

La Empresa de Salud ESE del Municipio de Soacha con el propósito de salvaguardar la información de la entidad en todos sus aspectos, garantizando la seguridad de los datos y el cumplimiento de las normas legales, ha establecido realizar un Plan de Seguridad y Privacidad de la información con el ánimo de que no se presenten pérdidas, robos, accesos no autorizados y duplicación de la información en la Empresa de Salud ESE del Municipio de Soacha, igualmente promueve una política de seguridad de la información física y digital de acuerdo a la caracterización de los usuarios tanto internos como externos.

La seguridad de la información se entiende como la preservación de las siguientes características:

A. Confidencialidad: se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la Empresa de Salud ESE del Municipio de Soacha.
B. Integridad: se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.
C. Disponibilidad: se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la Empresa de Salud ESE del Municipio de Soacha, toda vez que lo requieran.

Adicionalmente, debe considerarse los conceptos de:

A. Auditabilidad: define que todos los eventos de un sistema deben poder ser registrados para su control posterior.
B. Protección a la duplicación: consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.
C. No repudio: se refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.
D. Legalidad: referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeto el Organismo.

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.

4.5 Objetivos

Preservar, proteger y administrar de forma eficiente la información de la Empresa de Salud ESE del Municipio de Soacha junto con los medios utilizados para la manipulación o procesamiento, frente a amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de las características de confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.
Mantener la Política de Seguridad de la Información actualizada, vigente, operativa y controlada, enmarcada en el tratamiento de los riesgos de la información de la Empresa de Salud ESE del Municipio de Soacha, para asegurar la sostenibilidad de la Empresa de Salud ESE del Municipio de Soacha y el nivel de eficacia.

4.6 Alcance

Esta política es de aplicación en el conjunto de Secretarias, Departamentos, subsecretarias, oficinas y dependencias que componen la Empresa de Salud ESE del Municipio de Soacha, a sus recursos, a

la totalidad de los procesos internos o externos vinculados a la Administración Pública a través de contratos o convenios con terceros y a todo el personal de la Empresa, independiente de su tipo de vinculación, la dependencia a la cual se encuentre adscrito y el nivel de funciones o labores que ejecute.

4.7 Nivel de Cumplimiento

Todas las personas cubiertas por el alcance y aplicabilidad deberán dar cumplimiento un 100% de la política. A continuación, se establecen los 12 principios de seguridad que soportan el MSPI de LA EMPRESA DE SALUD ESE DEL MUNICIPIO DE SOACHA:

1. LA EMPRESA DE SALUD ESE DEL MUNICIPIO DE SOACHA ha decidido definir, implementar, operar y mejorar de forma continua un Modelo de Seguridad y Privacidad de la Información, soportado en lineamientos claros alineados a las necesidades de la empresa, y a los requerimientos regulatorios que le aplican a su naturaleza.
2. Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de funcionarios provisionales, funcionarios con carrera administrativa, funcionarios con libre nombramiento y contratistas.
3. LA EMPRESA DE SALUD ESE DEL MUNICIPIO DE SOACHA, protegerá la información generada, procesada o resguardada por los procesos de negocio y activos de información que hacen parte de los mismos, incluyendo los datos personales conforme lo define la Ley 1581 de 2012 y las normas que complementen, definen o reglamentan.
4. LA EMPRESA DE SALUD ESE DEL MUNICIPIO DE SOACHA, protegerá la información creada, procesada, transmitida o resguardada por sus procesos de la Empresa, 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.

5. LA EMPRESA DE SALUD ESE DEL MUNICIPIO DE SOACHA, protegerá su información de las amenazas originadas por parte del personal.

6. LA EMPRESA DE SALUD ESE DEL MUNICIPIO DE SOACHA, protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.

7. LA EMPRESA DE SALUD ESE DEL MUNICIPIO DE SOACHA, controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.

8. LA EMPRESA DE SALUD ESE DEL MUNICIPIO DE SOACHA, implementará control de acceso a la información, sistemas y recursos de red. POLÍTICA GENERAL DEL MODELO DE

SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

9. LA EMPRESA DE SALUD ESE DEL MUNICIPIO DE SOACHA, garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

10. LA EMPRESA DE SALUD ESE DEL MUNICIPIO DE SOACHA, 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.

11. LA EMPRESA DE SALUD ESE DEL MUNICIPIO DE SOACHA, garantizará la disponibilidad de sus procesos de la Empresa y la continuidad de su operación basada en el impacto que pueden generar los eventos.

12. LA EMPRESA DE SALUD ESE DEL MUNICIPIO DE SOACHA, 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 al Gobierno nacional y territorial en cuanto a Seguridad y Privacidad de la Información se refiere.

5. NORMATIVIDAD

5.5.1 Normas que rigen para la estructura organizacional de seguridad de la información

Normas dirigidas a: GERENCIA

A. La gerencia debe definir y establecer los roles y responsabilidades relacionados con la seguridad de la información en niveles directivo y operativo.

B. 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.

C. La gerencia debe revisar y aprobar las Políticas de Seguridad de la Información contenidas en este documento.

D. La gerencia debe promover activamente una cultura de seguridad de la información en la Empresa.

E. 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.

F. La gerencia, deben asignar los recursos, la infraestructura física y el personal necesario para la gestión de la seguridad de la información de la empresa.

Normas dirigidas a: OFICINA DE TECNOLÓGIA

A. La Oficina De Tecnología debe liderar la generación de lineamientos para gestionar la seguridad de la información de la Empresa y el establecimiento de controles técnicos, físicos y administrativos derivados de análisis de riesgos de seguridad.

B. La Oficina De Tecnología debe validar y monitorear de manera periódica la implantación de los controles de seguridad establecidos.

C. La Oficina De Tecnología debe asignar las funciones, roles y responsabilidades, a sus funcionarios para la operación y administración de la plataforma tecnológica de la Empresa. Dichas funciones, roles y responsabilidades deben encontrarse documentadas y apropiadamente segregadas.

Normas dirigidas a: CONTROL INTERNO

A. La Oficina de Control Interno debe planear y ejecutar las auditorías internas al Sistema de Gestión de Seguridad de la Información de la empresa a fin de determinar si las políticas, procesos, procedimientos y controles establecidos están conformes con los requerimientos institucionales, requerimientos de seguridad y regulaciones aplicables.

B. La Oficina de Control Interno debe informar a las áreas responsables los hallazgos de las auditorías.

Normas dirigidas a: TODOS LOS USUARIOS

- Los funcionarios y personal provisto por terceras partes que realicen labores en o para el LA EMPRESA DE SALUD ESE DEL MUNICIPIO DE SOACHA, tienen la responsabilidad de cumplir con las políticas, normas, procedimientos y estándares referentes a la seguridad de la información.

5.5.2 Normas para uso de conexiones remotas

Normas dirigidas a: OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA

A. La Oficina De Tecnología, deben analizar y aprobar los métodos de conexión remota a la plataforma tecnológica de la empresa.

B. La Oficina De Tecnología debe implantar los métodos y controles de seguridad para establecer conexiones remotas hacia la plataforma tecnológica de la empresa.

C. La Oficina De Tecnología debe restringir las conexiones remotas a los recursos de la plataforma tecnológica; únicamente se deben permitir estos accesos a personal autorizado y por periodos de tiempo establecidos, de acuerdo con las labores desempeñadas.

D. La Oficina De Tecnología debe verificar la efectividad de los controles aplicados sobre las conexiones remotas a los recursos de la plataforma tecnológica de la empresa de manera permanente.

Normas dirigidas a: TODOS LOS USUARIOS

A. Los usuarios que realizan conexión remota deben contar con las aprobaciones requeridas para establecer dicha conexión a los dispositivos de la plataforma tecnológica de la empresa y deben acatar las condiciones de uso establecidas para dichas conexiones.

B. Los usuarios únicamente deben establecer conexiones remotas en computadores previamente identificados y, bajo ninguna circunstancia, en computadores públicos.

5.5.4 Normas relacionadas con la vinculación de funcionarios

Normas dirigidas a: SECRETARIA GENERAL - TALENTO HUMANO

A. El Grupo de Talento Humano debe realizar las verificaciones necesarias para confirmar la veracidad de la información suministrada por el personal candidato a ocupar un cargo en La empresa de Salud ESE del Municipio de Soacha, antes de su vinculación definitiva.

B. El Grupo de Talento Humano debe certificar que los funcionarios de la Empresa firmen un Acuerdo y/o Cláusula de Confidencialidad y un documento de Aceptación de Políticas de Seguridad de la Información; estos documentos deben ser anexados a los demás documentos

relacionados con la ocupación del cargo.

Normas dirigidas a: SUPERVISORES DE CONTRATO

- Cada Supervisor de Contrato debe verificar la existencia de Acuerdos y/o Cláusulas de Confidencialidad y de la documentación de Aceptación de Políticas para el personal provisto por terceras partes, antes de otorgar acceso a la información de la Empresa.

Normas dirigidas a: PERSONAL PROVISTOS POR TERCERAS PARTES

A. El personal provisto por terceras partes que realicen labores en o para la empresa, deben firmar un Acuerdo y/o Cláusula de Confidencialidad y un documento de Aceptación de Políticas de Seguridad de la Información, antes de que se les otorgue acceso a las instalaciones y a la plataforma tecnológica.

B. El personal provisto por terceras partes, deben garantizar el cumplimiento de los Acuerdos y/o Cláusulas de Confidencialidad y aceptación de las Políticas de Seguridad de la Información de la empresa.

5.5.6 Normas para la desvinculación, licencias, vacaciones o cambios de labores de los funcionarios y personal provisto por terceros

Normas dirigidas a: SUPERVISORES DE CONTRATO

- Cada Supervisor de Contrato, debe monitorear y reportar de manera inmediata la desvinculación o cambio de labores de los funcionarios o personal provistos por terceras partes a La Oficina De tecnología.

Normas dirigidas a: OFICINA DE TECNOLOGÍA

- La Oficina tecnología debe verificar los reportes de desvinculación o cambio de labores y posteriormente debe realizar la modificación o inhabilitación de usuarios.

5.5.7 Normas uso de periféricos y medios de almacenamiento

Normas dirigidas a: OFICINA DE TECNOLOGÍA

A. La Oficina tecnología debe establecer las condiciones de uso de periféricos y medios de almacenamiento en la plataforma tecnológica de la Empresa.
B. La Oficina tecnología debe implantar los controles que regulen el uso de periféricos y medios de almacenamiento en la plataforma tecnológica de la empresa, de acuerdo con los lineamientos y condiciones establecidas.

C. La Oficina tecnología debe generar y aplicar lineamientos para la disposición segura de los medios de almacenamiento de la empresa, ya sea cuando son dados de baja o re-asignados a un nuevo usuario.

D. La Oficina tecnología debe autorizar el uso de periféricos o medios de almacenamiento en la plataforma tecnológica de la empresa de acuerdo con el perfil del cargo del funcionario solicitante.

Normas dirigidas a: TODOS LOS USUARIOS

A. Los funcionarios y el personal provisto por terceras partes deben acoger las condiciones de uso de los periféricos y medios de almacenamiento establecidos por La Oficina de tecnología.

B. Los funcionarios de la empresa y el personal provisto por terceras partes no deben modificar la configuración de periféricos y medios de almacenamiento establecidos por La Oficina de tecnología.

C. Los funcionarios y personal provisto por terceras partes son responsables por la custodia de los medios de almacenamiento institucionales asignados.

D. Los funcionarios y personal provisto por terceras partes no deben utilizar medios de almacenamiento personales en la plataforma tecnológica de la empresa.

5.5.8 Normas de administración de acceso de usuarios

Normas dirigidas a: LA OFICINA DE TECNOLOGÍA

A. La Oficina de tecnología debe establecer un procedimiento formal para la administración de los usuarios en las redes de datos, los recursos tecnológicos y sistemas de información de la empresa, que contemple la creación, modificación, bloqueo o eliminación de las cuentas de usuario.

B. La Oficina de tecnología, previa solicitud de los Jefes inmediatos y/o Supervisores de los solicitantes de las cuentas de usuario y aprobación tanto de los propietarios de los sistemas de información, debe crear, modificar, bloquear o eliminar cuentas de usuarios sobre las redes de datos, los recursos tecnológicos y los sistemas de información administrados.

C. La Oficina de tecnología 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.

D. La Oficina de tecnología 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.

E. La Oficina de tecnología debe autorizar la creación o modificación de las cuentas de acceso de los recursos tecnológicos y sistemas de información de la empresa.

Normas dirigidas a: PROPIETARIOS DE LOS ACTIVOS DE INFORMACIÓN

A. Es responsabilidad de los Propietarios de los activos de información, definir los perfiles de usuario y autorizar, conjuntamente con La Oficina tecnología, las solicitudes de acceso a dichos recursos de acuerdo con los perfiles establecidos.

B. Los propietarios de los activos de información deben verificar y ratificar periódicamente todas las autorizaciones sobre sus recursos tecnológicos y sistemas de información.

Normas dirigidas a: LOS SUPERVISORES DE CONTRATO

- Los Supervisores deben solicitar la creación, modificación, bloqueo y eliminación de cuentas de usuario, para los funcionarios que laboran en sus áreas, acogiéndose al procedimiento establecidos para tal fin.

5.5.9 Normas de responsabilidades de acceso de los usuarios

Normas dirigidas a: TODOS LOS USUARIOS

A. Los usuarios de las plataformas tecnológicas, los servicios de red y los sistemas de información de la empresa deben hacerse responsables de las acciones realizadas en los mismos, así como del usuario y contraseña asignados para el acceso a estos.

B. Los funcionarios no deben compartir sus cuentas de usuario y contraseñas con otros funcionarios o con personal provisto por terceras partes.

C. Los funcionarios y personal provisto por terceras partes que posean acceso a la plataforma tecnológica, los servicios de red y los sistemas de información de la empresa deben acogerse a lineamientos para la configuración de contraseñas que estén implementados.

5.5.10 Normas de control de acceso a sistemas y aplicativos

Normas dirigidas a: PROPIETARIOS DE LOS ACTIVOS DE INFORMACIÓN

A. 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.

B. Los propietarios de los activos de información deben monitorear periódicamente los perfiles definidos en los sistemas de información y los privilegios asignados a los usuarios que acceden a ellos.

Normas dirigidas a: LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA

A. La Oficina de tecnología debe establecer un procedimiento para la asignación de accesos a los sistemas y aplicativos de la empresa.

B. La Oficina de tecnología debe asegurar, mediante los controles necesarios, que los usuarios utilicen diferentes perfiles para los ambientes de pruebas y producción, y así mismo que los menús muestren los mensajes de identificación apropiados para reducir los riesgos de error.

5.5.11 Normas de seguridad para los equipos institucionales

Normas dirigidas a: LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA

A. La Oficina de tecnología 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.

B. La Oficina de tecnología debe realizar mantenimientos preventivos y correctivos de los recursos de la plataforma tecnológica de la empresa.

C. La Oficina de tecnología debe generar estándares de configuración segura para los equipos de cómputo de los funcionarios de la empresa y configurar dichos equipos acogiendo los estándares generados.

D. La Oficina de tecnología 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 empresa y verificar el cumplimiento de dichas condiciones antes de conceder a estos equipos acceso a los servicios de red.

E. La Oficina de tecnología debe generar y aplicar lineamientos para la disposición segura de los equipos de cómputo de los funcionarios de la empresa, ya sea cuando son dados de baja o cambian de usuario.

Normas dirigidas a: TODOS LOS USUARIOS

A. La Oficina de tecnología 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.

B. 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 de proporcione La Oficina tecnología.

C. Cuando se presente una falla o problema de hardware o software en una estación de trabajo u otro recurso tecnológico propiedad de la empresa el usuario responsable debe informar al área de tecnología donde se atenderá o escalará al interior de La Oficina tecnología, con el fin de realizar una asistencia adecuada. El usuario no debe intentar solucionar el problema.

D. 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 empresa, solo puede ser realizado por los funcionarios de La Oficina de tecnología, o personal de terceras partes autorizado por dicha dirección.

E. Los funcionarios de la empresa y el personal provisto por terceras partes deben bloquear sus estaciones de trabajo en el momento de abandonar su puesto de trabajo.

F. Los funcionarios de la empresa y el personal provisto por terceras partes no deben dejar encendidas las estaciones de trabajo u otros recursos tecnológicos en horas no laborables.

5.5.12 Normas de protección frente a software malicioso

Normas dirigidas a: LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA

A. La Oficina de tecnología debe proveer herramientas tales como antivirus, antimalware, antispam, antispyware, entre otras, que reduzcan el riesgo de contagio de software malicioso y respalden la seguridad de la información contenida y administrada en la plataforma tecnológica de la empresa y los servicios que se ejecutan.

B. La Oficina de tecnología debe asegurar que el software de antivirus, antimalware, antispam y antispyware cuente con las licencias de uso requeridas, certificando así su autenticidad y la posibilidad de actualización periódica de las últimas bases de datos de firmas del proveedor del servicio.

C. La Oficina de tecnología debe certificar que la información almacenada en la plataforma tecnológica sea escaneada por el software de antivirus, incluyendo la información que se encuentra contenida y es transmitida por el servicio de correo electrónico.

D. La Oficina de tecnología, a través de sus funcionarios, debe asegurarse que los usuarios no puedan realizar cambios en la configuración del software de antivirus, antispyware, antispam, antimalware.

E. La Oficina de tecnología, a través de sus funcionarios, debe certificar que el software de antivirus, antispyware, antispam, antimalware, posea las últimas actualizaciones y parches de seguridad, para mitigar las vulnerabilidades de la plataforma tecnológica.

5.5.13 Normas de copias de respaldo de la información

Normas dirigidas a: LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA

A. La Oficina de tecnología, a través de sus funcionarios, debe generar y adoptar los procedimientos para la generación, restauración, almacenamiento y tratamiento para las copias de respaldo de la

información, velando por su integridad y disponibilidad.

B. La Oficina de tecnología debe disponer de los recursos necesarios para permitir la identificación de los medios de almacenamiento, la información contenida en ellos y la ubicación física de los mismos para permitir un rápido y eficiente acceso a los medios que contienen la información resguardada.

C. La Oficina de tecnología, a través de sus funcionarios, debe llevar a cabo los procedimientos para realizar pruebas de recuperación a las copias de respaldo, para así comprobar su integridad y posibilidad de uso en caso de ser necesario.

D. La Oficina de tecnología debe definir las condiciones de transporte o transmisión y custodia de las copias de respaldo de la información que son almacenadas externamente.

E. La Oficina de tecnología debe proporcionar apoyo para la definición de las estrategias de generación, retención y rotación de las copias de respaldo de la los activos información de la empresa.

Normas dirigidas a: PROPIETARIOS DE LOS ACTIVOS DE INFORMACIÓN

- Los propietarios de los recursos tecnológicos y sistemas de información deben definir, en conjunto con La Oficina de tecnología, las estrategias para la generación, retención y rotación de las copias de respaldo de los activos de información.

Normas dirigidas a: TODOS LOS USUARIOS

- Es responsabilidad de los usuarios de la plataforma tecnológica de la empresa identificar la información crítica que debe ser respaldada y almacenarla de acuerdo con su nivel de clasificación.

5.5.14 Normas de cumplimiento con requisitos legales y contractuales

Normas dirigidas a: OFICINA ASESORA JURÍDICA Y LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA

- La Oficina Asesora Jurídica y La Oficina de tecnología deben identificar, documentar y mantener actualizados los requisitos legales, reglamentarios o contractuales aplicables a la empresa y relacionados con seguridad de la información.

Normas dirigidas a: LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA

A. La Oficina de tecnología debe certificar que todo el software que se ejecuta en la empresa esté protegido por derechos de autor y requiera licencia de uso o, en su lugar sea software de libre distribución y uso.

B. La Oficina de tecnología debe establecer un inventario con el software y sistemas de información que se encuentran permitidos en las estaciones de trabajo o equipos móviles de la empresa para el desarrollo de las actividades laborales, así como verificar periódicamente que el software instalado en dichas estaciones de trabajo corresponda únicamente al permitido.

Normas dirigidas a: TODOS LOS USUARIOS

A. 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.

B. 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.

5.5.15 Normas de privacidad y protección de datos personales

Normas dirigidas a: ÁREAS QUE PROCESAN DATOS PERSONALES

A. Las áreas que procesan datos personales de beneficiarios, funcionarios, proveedores u otras terceras partes 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 empresa.

B. Las áreas que procesan datos personales de beneficiarios, funcionarios, proveedores u otras terceras partes deben asegurar que solo aquellas personas que tengan una necesidad laboral legítima puedan tener acceso a dichos datos.

C. Las áreas que procesan datos personales de beneficiarios, funcionarios, proveedores u otras terceras partes deben establecer condiciones contractuales y de seguridad a las entidades vinculadas o aliadas delegadas para el tratamiento de dichos datos personales.

D. Las áreas que procesan datos personales de beneficiarios, funcionarios, proveedores u otras terceras partes 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.

E. Las áreas que procesan datos personales de beneficiarios, proveedores u otras terceras partes deben acoger las directrices técnicas y procedimientos establecidos para enviar a los beneficiarios, proveedores u otros terceros mensajes, a través de correo electrónico y/o mensajes de texto.

Normas dirigidas a: LA OFICINA DE GESTIÓN TECNOLÓGICA E INFORMÁTICA

A. La Oficina 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 empresa de los cuales reciba y administre información.

B. La Oficina 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.

Normas dirigidas a: TODOS LOS USUARIOS

A. Los usuarios deben guardar la discreción correspondiente, o la reserva absoluta con respecto a la información de la empresa o de sus funcionarios de cual tengan conocimiento en el ejercicio de sus funciones.
B. 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.