TABLA DE CONTENIDO

1. INTRODUCCIÓN 2
2. OBJETIVO 2
3. ALCANCE 2
4. VIGENCIA 3
5. ROLES Y RESPONSABLES 3
6. MARCO NORMATIVO 4
7. REVISIÓN Y EVALUACIÓN 4
8. GLOSARIO 4
9. PROCESO DE GESTIÓN EN TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIONES 8
9.1 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN 8
10. REGLAS DE NEGOCIO 43
11. REGISTROS 48
12. CONTROL DE CAMBIOS 49

ELABORADO	***REVISADO***	***APROBADO***
Participantes del Proceso	*Gerente Soporte Organizacional*	*COMITÉ NORMATIVO No. 139*
Fecha: 15/12/2023	*Fecha: 12/02/2024*	*Fecha: 12/02/2024*

"Este documento es confidencial, puede contener información privilegiada y no puede ser usado ni divulgado por personas distintas a personal de EMSA E.S.P., Está prohibida su retención, copia, grabación, utilización o divulgación con cualquier propósito"

1. INTRODUCCIÓN

Las Políticas de Seguridad de la Información, surgen como una herramienta institucional para sensibilizar a cada uno de los directivos, funcionarios, contratistas y terceros que presten sus servicios o tengan algún tipo de relación con la Electrificadora del Meta S.A. ESP; sobre la importancia de proteger los activos de información y servicios críticos, de tal forma que le permitan desarrollar adecuadamente sus labores y cumplir con su propósito misional.

Este manual describe además las responsabilidades, privilegios y limitaciones del usuario y les informa de la existencia de sanciones por la violación de la política de seguridad.

2. OBJETIVO

Informar de forma clara y coherente a todos los directivos, funcionarios, contratistas, terceros y otros usuarios autorizados, los elementos que conforman la política de seguridad que deben conocer y cumplir con carácter obligatorio para salvaguardar los activos de información, aplicaciones y servicios informáticos contra todo tipo de amenazas, fallas o desastres tecnológicos, garantizando la disponibilidad, seguridad y confidencialidad de la información institucional de la Electrificadora del Meta S.A. ESP. mediante la gestión de las copias de respaldo y su recuperación y, establecer directrices que posibiliten la recuperación de la información en el menor tiempo posible.

Por lo anterior, se definen las pautas, directrices y reglas para generar una adecuada seguridad y protección de la información de los procesos de EMSA, estableciendo dentro del plan estratégico de TI su liderazgo y desarrollo, y certificar la organización en la norma NTC-ISO-27001:2013.

3. ALCANCE

Para el adecuado cumplimiento de sus funciones y para conseguir un adecuado nivel de protección de calidad y seguridad de la información, se deben aplicar las políticas de seguridad a todos los aspectos administrativos y de control, y cumplirse por los directivos, funcionarios, contratistas y terceros que presten sus servicios o tengan algún tipo de relación con la Electrificadora del Meta. Aportando con su participación en la toma de medidas preventivas y correctivas, siendo un punto clave para el logro del objetivo y la finalidad del presente manual.

"Este documento es confidencial, puede contener información privilegiada y no puede ser usado ni divulgado por personas distintas a personal de EMSA E.S.P., Está prohibida su retención, copia, grabación, utilización o divulgación con cualquier propósito"

La aplicación de esta política se extiende a toda la información alojada en servidores físicos y virtuales, equipos de comunicación y estaciones de trabajo que contengan datos, aplicaciones y configuraciones, herramientas y sistemas de información en producción de EMSA; esta garantizará y facilitará la adquisición de ambientes físicos y virtuales, como también licencias para la correcta ejecución de la presente política.

4. VIGENCIA

El manual de políticas de seguridad de la información, lineamientos y reglas de negocio de EMSA estará sujeta a la normatividad vigente, ajustada e implementada de conformidad con las necesidades de la entidad sin omitir o extralimitarse de lo establecido en el marco normativo.

5. ROLES Y RESPONSABLES

Las políticas del SGSI (Sistema de Gestión de la Seguridad de la Información) aplican y son de obligatorio cumplimiento para la alta dirección, gerentes, secretarios, jefes de oficina, líderes, funcionarios, contratistas, y en general a todos los usuarios de la información que permitan el cumplimiento de los propósitos generales de EMSA.

Oficina de las TIC:

Velar por el cumplimiento de la presente política; designar el personal idóneo para definir y gestionar el estándar de respaldo de los servidores y equipos de hardware de EMSA.

a) Coordina, ejecuta y vela por la realización de las copias de respaldo y restauración de estas, utilizando las herramientas pertinentes para tales efectos y validar que la actividad se realice correctamente.
b) Mantiene un inventario de los activos de información sobre los que se realizan copias de respaldo.
c) Realiza pruebas periódicas de recuperación de información a partir de las copias de respaldo.

Áreas que administran sistemas de información: El líder de área o encargado podrá solicitar respaldos o restauración de las copias, según la necesidad que se requiera.

Personal: Da cumplimiento a la presente política y los lineamientos del Sistema de Gestión de Seguridad de la Información.

"Este documento es confidencial, puede contener información privilegiada y no puede ser usado ni divulgado por personas distintas a personal de EMSA E.S.P., Está prohibida su retención, copia, grabación, utilización o divulgación con cualquier propósito"

6. MARCO NORMATIVO

El presente documento se basa en las buenas prácticas, leyes y normas relacionadas con la seguridad de la información: Ley 1273 de 2009 – De la protección de la información y de los datos, ISO/IEC 27001:2013 – Sistemas de Gestión de Seguridad de la Información (SGSI), ISO/IEC 27002:2005 – Código para la práctica de la gestión de la seguridad de la información, ISO 22301:2012 – Seguridad de la Sociedad: Sistemas de Continuidad del Negocio y la Norma Técnica Colombiana NTC- ISO: 9001.

7. REVISIÓN Y EVALUACIÓN

La presente política deberá ser sometida a revisiones anuales posterior al ejercicio de seguimiento, monitoreo y evaluación de su aplicación; frente a lo cual, se harán los ajustes razonables como resultado de planes de mejora anuales, que en todo caso deben ser sometidos al análisis de las instancias correspondientes contando con los conceptos técnicos del área TIC de EMSA, así como con el concepto de adopción o actualización normativa a que haya lugar por parte de la oficina jurídica.

8. GLOSARIO

Activo de información: 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 etc.) que tenga valor para la organización.

Agentes: accesos determinados por las herramientas de backup que deben ser instalados en los equipos objeto de copias de seguridad.

Aplicaciones: Nombre que reciben los programas especializados en tareas concretas y de una cierta complejidad

Backup: Copia idéntica de algo, copia de seguridad o copia respaldo de algo.

Bases de Datos: Es la colección de información, que está organizada de forma tal que su contenido sea fácilmente accedido, administrado y actualizado.

Cintas Magnéticas: Dispositivo de almacenamiento masivo de datos.

"Este documento es confidencial, puede contener información privilegiada y no puede ser usado ni divulgado por personas distintas a personal de EMSA E.S.P., Está prohibida su retención, copia, grabación, utilización o divulgación con cualquier propósito"

Copia de respaldo (backup): es la actividad de resguardar en forma segura la información contenida en un medio de almacenamiento en un medio o ubicación distinta al origen. Es un duplicado de la información más importante, y se realiza para salvaguardar los documentos, archivos, fotos, bases de datos, configuraciones etc.

Copia Incremental: es una tarea de backup donde se copian únicamente los archivos que han sido incorporados o modificados desde la copia de seguridad anterior.

Copia Total: es un proceso donde se copian la totalidad de archivos y directorios seleccionados.

Custodia de Medios: Corresponde al almacenamiento seguro de los medios magnéticos fuera de la entidad, a cargo de un proveedor externo.

Custodia: Se entrega al cuidado de una persona natural o jurídica.

Eliminar de forma segura: se refiere a borrado seguro de información de un dispositivo, con el fin que no se pueda recuperar ni acceder a ella bajo ningún escenario.

Estándar: Regla que especifica una acción o respuesta que se debe seguir a una situación dada. Los estándares son orientaciones obligatorias que buscan hacer cumplir las políticas. Los estándares son diseñados para promover la implementación de las políticas de alto nivel de la entidad antes de crear nuevas políticas.

File Server: servidor que permite a los clientes de la Red acceder a sus recursos de almacenamiento.

OneDrive: almacenamiento en la nube proporcionado por la compañía Microsoft.

Guía: Una guía es una declaración general utilizada para recomendar o sugerir un enfoque para implementar políticas, estándares buenos prácticas. Las guías son esencialmente, recomendaciones que deben considerarse al implementar la seguridad. Aunque no son obligatorias, serán seguidas a menos que existan argumentos documentados y aprobados para no hacerlo.

Incidentes: se cataloga como incidente todo evento que represente un daño significativo sobre la información, o que atente contra los principios fundamentales, como disponibilidad, confidencialidad e integridad.

"Este documento es confidencial, puede contener información privilegiada y no puede ser usado ni divulgado por personas distintas a personal de EMSA E.S.P., Está prohibida su retención, copia, grabación, utilización o divulgación con cualquier propósito"

Librería de cintas de Backups (Tape Library): Dispositivo de Hardware que realiza la rutina de respaldo en cintas de manera automática.

Librería de Cintas: Sistema de Backup robotizado que utiliza como medio de almacenamiento cintas magnéticas. Es el puente de conexión entre la red de datos y las cintas de respaldo.

Líderes de Procesos: Toda persona adscrita al Departamento de Función Pública que tiene a cargo la administración de tecnologías de la información y las comunicaciones tales como: aplicaciones (misionales y/o de apoyo), sistemas de información, servidores, bases de datos, redes y todo aquello que involucre información relacionada con la operación de la entidad en el cumplimiento de sus objetivos mediante herramientas tecnológicas.

Mejor Práctica: Una regla de seguridad específica o una plataforma que es aceptada, a través de la industria al proporcionar el enfoque más efectivo a una implementación de seguridad concreta. Las mejores prácticas son establecidas para asegurar que las características de seguridad de los sistemas utilizados con regularidad estén configurados y administrados de manera uniforme, garantizando un nivel consistente de seguridad a través de la entidad.

Política: Declaración de alto nivel que describe la posición de la entidad sobre un tema específico.

Procedimiento: Los procedimientos, definen específicamente como las políticas, estándares, mejores prácticas y guías que serán implementadas en una situación dada. Los procedimientos son independientes de la tecnología o de los procesos y se refieren a las plataformas, aplicaciones o procesos específicos. Son utilizados para delinear los pasos que deben ser seguidos por una dependencia para implementar la seguridad relacionada con dicho proceso o sistema específico. Generalmente los procedimientos son desarrollados, implementados y supervisados por el dueño del proceso o del sistema, los procedimientos seguirán las políticas de la entidad, los estándares, las mejores prácticas y las guías tan cerca como les sea posible, y a la vez se ajustarán a los requerimientos procedimentales o técnicos establecidos dentro del a dependencia donde ellos se aplican.

Propietario de Activo de Información: Es el nombre del responsable de la producción de la información (propietario): Que corresponde al nombre del área, dependencia o unidad interna, o al nombre de la entidad externa que creó la información. Es el responsable del activo, quien debe velar por el cumplimiento de los requerimientos establecidos frente a las propiedades de disponibilidad,

"Este documento es confidencial, puede contener información privilegiada y no puede ser usado ni divulgado por personas distintas a personal de EMSA E.S.P., Está prohibida su retención, copia, grabación, utilización o divulgación con cualquier propósito"

confidencialidad e integridad.

Recuperación: Hace referencia a las técnicas empleadas para recuperar la información (archivos) a partir de una copia de seguridad (medio externo); esto se aplica para archivos perdidos o eliminados por diferentes causas como daño físico del dispositivo de almacenamiento, borrado accidental, fallos del sistema, ataques de virus y hackers.

Red: enlace de comunicaciones que se puede establecer mediante canales o interfaces cableadas o inalámbricas.

Respaldo: Sinónimo de back up.

Restauración: recuperar la información (archivos) a partir de una copia de seguridad (medio externo).

Restore: tarea relacionada con el back up que consiste en la recuperación de archivos o carpetas eliminadas.

Servidor: computadora de gran capacidad que realiza tareas en beneficio de otras computadoras llamadas clientes, también provee almacenamiento a los equipos cliente, todo esto mediante una conexión de red.

Sistema Operativo: Programa o conjunto de programas que actúan como intermediarios entre las aplicaciones de los usuarios (Software) y el equipo físico (Hardware) de la máquina, ocultando las características particulares de este último.

Sistemas de Información: Medios de almacenamiento y procesamiento de los datos de la entidad y que ofrecen algún servicio informático

Tareas de respaldo: Programación de las copias de seguridad que incluyen: la fuente, el destino y la periodicidad.

Ticket: número de caso generado con la herramienta de mesa de ayuda de la entidad, para atención de incidentes y/o solicitudes.

TSM: Tivoli Storage Manager- herramienta tipo software de gestión de backups, que permite programar y realizar de forma automática los backups

"Este documento es confidencial, puede contener información privilegiada y no puede ser usado ni divulgado por personas distintas a personal de EMSA E.S.P., Está prohibida su retención, copia, grabación, utilización o divulgación con cualquier propósito"

Usuario: puede ser un Servidor público y/o Contratista de la USPEC.

9. PROCESO DE GESTIÓN EN TECNOLOGÍA DE LA INFORMACIÓN Y COMUNICACIONES

9.1 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

9.1.1 Estructura organizacional de seguridad de la información

EMSA en cumplimiento al compromiso del Sistema de Gestión de Seguridad de la Información, crea un esquema de seguridad de la información definiendo y estableciendo roles y responsabilidades que involucren las actividades de operación, gestión y administración de la seguridad de la información.

El Área de Tecnologías de la Información y comunicaciones, debe establecer los roles, funciones y responsabilidades de operación y administración de los sistemas de información a los funcionarios asignados en EMSA, estos roles, funciones y responsabilidades, deberán estar debidamente documentadas y distribuidas.

9.1.2 Seguridad para los recursos humanos

EMSA implementa acciones para asegurar que los funcionarios, contratistas y demás colaboradores de la Entidad, las cuales se relacionan a continuación:

- El aspirante previo a la posesión del cargo y el contratista posterior a la firma del contrato deberá diligenciar y firmar el formato de compromiso y reserva.

- Se debe capacitar y sensibilizar a los funcionarios durante la inducción sobre las políticas de seguridad de la información.

- Se debe asegurar que los funcionarios, contratistas y demás colaboradores de EMSA, adopten sus responsabilidades en relación con las políticas de seguridad de la información y actúen de manera consistente frente a las mismas, con el fin de reducir el riesgo de hurto, fraude, filtraciones o uso inadecuado de la información o los equipos empleados para el tratamiento de la información; el conocimiento de las políticas de seguridad de la información se notifican mediante el diligenciamiento y firma del formato de administración de usuarios FO-GSO-TI-06.

- El funcionario o contratista debe entregar los activos de información de acuerdo con el formato de Administración de usuarios por retiro del servicio o separación temporal del cargo FO- GSO-TI-06.

"Este documento es confidencial, puede contener información privilegiada y no puede ser usado ni divulgado por personas distintas a personal de EMSA E.S.P., Está prohibida su retención, copia, grabación, utilización o divulgación con cualquier propósito"

En situaciones de incumplimiento y/o violaciones a las políticas de seguridad de la información se deberá tramitar el cumplimiento del reglamento interno de trabajo y demás normas que reglamenten los procesos disciplinarios para los funcionarios de EMSA.

Actualmente las personas que tienen cuenta de usuario de la organización pueden realizar el cambio de su fotografía para MS-Teams, Intranet y correo electrónico institucional, de tal forma que al realizar la inclusión y/o cambio de fotografía, al ser considerada un dato sensible, "una foto contiene la imagen de una persona, la cual es un dato biométrico", el titular está dando su aprobación, en cuanto al tratamiento de sus datos personales de acuerdo a la Ley estatutaria 1581 de 2012.

9.1.3 Clasificación de la información

Las reglas de como clasificar la información, son liderado por el proceso de Gestión Documental de la organización.

Se considera información toda forma de comunicación o representación de conocimiento o datos digitales, escritos en cualquier medio, ya sea magnético, papel, visual u otro que genere EMSA como, por ejemplo:

- Formularios / comprobantes propios o de terceros.
- Información en los sistemas, equipos informáticos, medios magnéticos/electrónicos o medios físicos como papel.
- Otros soportes magnéticos/electrónicos removibles, móviles o fijos.
- Información transmitida vía oral o por cualquier otro medio de comunicación.

Los usuarios responsables de la información de EMSA, deben identificar los riesgos a los que está expuesta la información de sus áreas, teniendo en cuenta que la información pueda ser copiada, divulgada, modificada o destruida física o digitalmente por personal interno o externo.

Un activo de información es un elemento definible e identificable que almacena registros, datos o información en cualquier tipo de medio y que es reconocida como "Valiosa" para EMSA; Independiente del tipo de activo, se deben considerar las siguientes características:

1) El activo de información es reconocido como valioso para EMSA.

2) No es fácilmente reemplazable sin incurrir en costos, habilidades especiales, tiempo, recursos o la combinación de los anteriores.

"Este documento es confidencial, puede contener información privilegiada y no puede ser usado ni divulgado por personas distintas a personal de EMSA E.S.P., Está prohibida su retención, copia, grabación, utilización o divulgación con cualquier propósito"

3) Forma parte de la identidad de la organización y sin la cual EMSA puede estar en algún nivel de riesgo. (La determinación del nivel de seguridad se observa en el cuadro siguiente).

4) Los niveles de clasificación de la información que se ha establecido son: CRITICA – MEDIA – ALTA – BAJA, como se relaciona a continuación:

NIVEL DE SEGURIDAD	DESCRIPCIÓN	EJEMPLO
CRÍTICA	Este sistema contiene información **confidencial,** información que no puede ser revelada al personal fuera de la organización. Incluso dentro de la organización, el acceso a esta información se proporciona sobre una base "necesita saber", además la información debe estar resguarda para la modificación únicamente por el personal autorizado.	Bases de datos que contiene información confidencial, información de históricos. Routers, Switches, Firewalls, Servidores SCADA.
	El sistema de información debe permanecer **disponible** 7x24 x 365 días del año.	
ALTA	Este sistema contiene información **confidencia**l pero no ejecuta **servicios críticos**, ofrece la posibilidad de acceder a sistemas **críticos** a través de la red interna de la organización.	Departamento de usuario con estaciones de trabajo utilizados para acceder a servidores y aplicaciones.
	El sistema puede sufrir fallos de **disponibilidad** sin suponer un impacto directo a los sistemas **críticos**, La **integridad** de la información almacenada también es requerida.	Estaciones de trabajo de gestión utilizados por los administradores de red y sistemas.
MEDIO	Este sistema no es accesible desde el exterior. Está en un segmento aislado de LAN, no se puede tener acceso a sistemas de niveles **críticos** o **altos**. No contienen información confidencial o realizan servicios **críticos**.	Un sistema de prueba utilizado por diseñadores de sistemas y programadores para desarrollar nuevos sistemas informáticos.
	Puede manejar información de tipo **interno**, la **disponibilidad** de este tipo de sistemas de información no afecta ningún proceso **crítico** de la organización.	

"Este documento es confidencial, puede contener información privilegiada y no puede ser usado ni divulgado por personas distintas a personal de EMSA E.S.P., Está prohibida su retención, copia, grabación, utilización o divulgación con cualquier propósito"

BAJA	Este sistema es accesible desde el exterior. Está aislado de sistemas **crítico y alto** por un firewall. Mientras que realiza servicios necesarios para la organización, no contiene información **confidencia**l. Únicamente maneja información de dominio **público**. La **disponibilidad** del sistema no afecta los servicios críticos de la organización.	Un servidor Web público con información no sensible.

Clasificación de Redes de Área Local

Una LAN se clasifica de acuerdo a los sistemas conectados directamente a él. Por ejemplo, si una LAN contiene un sistema de CRÍTICO y todos los usuarios de la red están sujetos a las mismas restricciones que los usuarios de sistemas de CRÍTICO, una LAN puede asumir la clasificación de seguridad de los sistemas de nivel CRÍTICO.

CATEGORÍA DEL USUARIO	PRIVILEGIOS Y RESPONSABILIDADES
Departamento de Usuarios (Empleados)	Acceso a aplicaciones y bases de datos necesarios para la función de trabajo.
Administradores del Sistema	Acceso a sistemas informáticos, routers, hubs y otra tecnología de infraestructura necesaria para la función de trabajo. Acceso a información confidencial sobre una base "necesita saber" solamente.
Administrador de Seguridad (Analista III)	Tiene el más alto nivel de acceso de seguridad. Permite el acceso a los sistemas informáticos, bases de datos, firewalls y dispositivos de red como sea necesario para la función de su trabajo.
Analistas de Sistemas	Acceso a aplicaciones y bases de datos como sea necesario para la función de trabajo específico. No autorizado al acceso de routers, firewalls u otros dispositivos de red.
Consultores/Contratistas	Acceso a aplicaciones y bases de datos como sea necesario para funciones de trabajo específicas. Acceso a routers y firewall, sólo si es necesario para la función de trabajo. Conocimiento de las políticas de seguridad. Acceso a información de la organización y sistemas, debe ser aprobado por escrito por el Analista Coordinador TIC.

"Este documento es confidencial, puede contener información privilegiada y no puede ser usado ni divulgado por personas distintas a personal de EMSA E.S.P., Está prohibida su retención, copia, grabación, utilización o divulgación con cualquier propósito"

Agencias	Acceso permitido a aplicaciones seleccionadas sólo cuando existe un contrato o acuerdo de acceso interinstitucional en el lugar y es requerido por las leyes aplicables.
Público en General	El acceso es limitado a aplicaciones que se ejecutan en servidores Web públicos. Al público en general no se le permitirá acceso a la información confidencial.

9.1.4 Uso y gestión de activos de información.

La Organización implementa las directrices para lograr y mantener la protección adecuada y uso de los activos de información, mediante la asignación a los usuarios finales que deban administrarlos de acuerdo a sus roles y funciones.

Los usuarios no deben mantener almacenados en los discos duros de las estaciones cliente o discos virtuales de red, archivos de vídeo, música, fotos y cualquier tipo de archivo que no sean de carácter institucional.

Las directrices de uso de activos se encuentran definidas en el **Lineamiento de uso de activos de Información y dispositivos móviles.**

EMSA es el dueño de la propiedad intelectual de los avances tecnológicos e intelectuales desarrollados por los funcionarios y los contratistas de EMSA, derivadas del objeto del cumplimiento de funciones y/o tareas asignadas, como las necesarias para el cumplimiento del objeto del contrato. EMSA es propietario de los activos de información y los administradores de estos activos son los funcionarios, contratistas o demás colaboradores de EMSA (denominados “usuarios”, que estén autorizados y sean responsables por la información de los procesos a su cargo, de los sistemas de información o aplicaciones informáticas, hardware o infraestructura de Tecnología y Sistemas de Información (TIC).
EMSA mantiene un inventario actualizado de sus activos de información, quedando bajo la responsabilidad de cada propietario de información y centralizado por el Área de Tecnologías de la Información y Comunicaciones, el cual se publicará en la intranet sobre el SIG de TIC.

9.1.5 Uso de estaciones de trabajo

EMSA establece reglas que permitan orientar a la seguridad como parte integral de los activos de información y mediante la correcta utilización de estaciones de trabajo por los usuarios finales.

"Este documento es confidencial, puede contener información privilegiada y no puede ser usado ni divulgado por personas distintas a personal de EMSA E.S.P., Está prohibida su retención, copia, grabación, utilización o divulgación con cualquier propósito"

Las Directrices de uso de estaciones cliente se encuentran definidas en el **Lineamiento de uso de servicios de TI.**

9.1.6 Uso de Internet

La Organización permite el acceso a servicio de internet, estableciendo lineamientos que garanticen la navegación segura y el uso adecuado de la red por parte de los usuarios finales, evitando errores, pérdidas, modificaciones no autorizadas o uso inadecuado de la información en las aplicaciones WEB.

El Líder del Área de Tecnologías de la Información y Comunicaciones, administrará y autorizará los cambios solicitados de permisos de navegación a los usuarios de EMSA, previa solicitud del líder de cada una de las dependencias, de acuerdo a Lineamientos de Control de Acceso y formato para solicitud de creación de cuenta de usuario y servicios de tecnología de información.

El Área de Tecnologías de la Información y Comunicaciones implementa herramientas para evitar la descarga de software no autorizado y/o código malicioso en los equipos institucionales, así mismo; controla el acceso a la información contenida en portales de almacenamiento en el internet para prevenir la fuga de información.

Los usuarios de los activos de información del EMSA tienen restringido el acceso a redes sociales, sistemas de mensajería instantánea, acceso a sistemas de almacenamiento en la nube diferentes a las establecidas por la organización y cuentas de correo no institucional. En caso de ser requerido por las funciones del cargo, el jefe inmediato debe remitir la solicitud a Líder del Área de Tecnologías de la información y Comunicaciones, para que sea autorizado por el Administrador de Seguridad.

Las Directrices de uso de Internet se encuentran **definidas en el Lineamiento de uso de servicios de TI.**

9.1.7 Manejo y disposición de información, medios y equipos

La organización establece actividades para evitar la divulgación, la modificación, el retiro o la destrucción no autorizada de información almacenada en los medios proporcionados por EMSA, velando por la disponibilidad y confidencialidad de la información.

Los medios y equipos donde se almacena procesan o comunica la información, deben mantenerse con las medidas de protección físicas y lógicas, que permitan su monitoreo y correcto estado de funcionamiento, para ello se debe realizar los mantenimientos preventivos y correctivos que se requieran.

"Este documento es confidencial, puede contener información privilegiada y no puede ser usado ni divulgado por personas distintas a personal de EMSA E.S.P., Está prohibida su retención, copia, grabación, utilización o divulgación con cualquier propósito"

El servicio de acceso a Internet, Intranet, Sistemas de información, medio de almacenamiento, aplicaciones (Software), cuentas de red, navegadores y equipos de cómputo son propiedad de la organización y deben ser usados únicamente para el cumplimiento de la misión de la misma.

En el **Procedimiento de Borrado Seguro** para dispositivos celulares, se describe el paso a paso para el borrado o eliminación de la información que estos equipos puedan contener cuando se presente la pérdida o hurto de estos.

Se debe realizar el borrado seguro en los equipos de cómputo y demás dispositivos, una vez el funcionario haya sido retirado de la entidad, de acuerdo con lo definido por EMSA.

Está restringida la copia de archivos en medios removibles de almacenamiento, por lo cual se deshabilita la opción de escritura en dispositivos USB, unidades ópticas de grabación en todos los equipos de cómputo institucionales; la autorización de uso de los medios removibles debe ser tramitada a través de la oficina de TIC.

Se debe implementar el procedimiento para la transferencia de medios físicos. Las actividades se definen en el **Procedimiento de Borrado Seguro para equipos y formato de Baja de propiedades, planta y equipo FO-GF-GC-06.**

9.1.8 Establecimiento, uso, protección y control de acceso y claves

La generación de accesos y permisos se enmarca exclusivamente dentro de los términos contractuales establecidos sin exceder los tiempos o fechas establecidos para ello, por lo cual la gerencia financiero-administrativa y el equipo TIC deberán contar con una comunicación eficaz que salvaguarde la seguridad, confiabilidad e integridad de la información. En casos excepcionales, analizarán un plan de contingencia y acciones concretas con carácter de urgente.

EMSA suministrará a los usuarios las claves respectivas para el acceso a los servicios de red y sistemas de información a los que hayan sido autorizados, las claves son de uso personal e intransferible. Ningún usuario deberá acceder a la red o a los servicios TIC de EMSA, utilizando una cuenta de usuario o clave de otro usuario.

"Este documento es confidencial, puede contener información privilegiada y no puede ser usado ni divulgado por personas distintas a personal de EMSA E.S.P., Está prohibida su retención, copia, grabación, utilización o divulgación con cualquier propósito"

El cambio de contraseña solo podrá ser solicitado por el titular de la cuenta, elevando el requerimiento por mesa de ayuda, en donde se llevará a cabo la validación de los datos personales; en caso de ser solicitado el cambio de contraseña para otra persona, debe ser realizada por su jefe inmediato (previa autorización por parte del líder de Área de Tecnologías de Información y Comunicaciones).

Las claves o contraseñas deben tener mínimo ocho (8) caracteres alfanuméricos.

Cada vez que se cambien estas deben ser distintas por lo menos de las últimas cinco anteriores.

La contraseña debe cumplir con tres de los cuatro requisitos:

• Caracteres en mayúsculas
• Caracteres en minúsculas
• Base de 10 dígitos (0 a 9)
• Caracteres no alfabéticos (Ejemplo: ¡$, %,&)

Manejo de contraseñas para administradores de tecnología

Se debe garantizar en las plataformas de tecnología que el ingreso a la administración en lo posible

se realice con la vinculación directamente de las credenciales de los usuarios de directorio activo. Los usuarios súper administradores y sus correspondientes contraseñas a las consolas administrables se dejan en custodia en sobre sellado en el área segura donde designe la entidad, las credenciales allí contenidas deben ser modificadas de manera mensual o cuando amerite.

Las contraseñas referentes a las cuentas “predefinidas” incluidas en los sistemas o aplicaciones adquiridas deben ser desactivadas. De no ser posible su desactivación, las contraseñas deben ser cambiadas después de la instalación del producto.

El personal del Área de Tecnologías de la Información no debe dar a conocer su clave de usuario a terceros de los sistemas de información, sin previa autorización del líder del Área de la Información y Comunicaciones.

Los usuarios y claves de los administradores de sistemas y del personal del Área de Tecnologías de la Información y Comunicaciones son de uso personal e intransferible.

El personal del Área de Tecnologías de la Información y Comunicaciones debe emplear

"Este documento es confidencial, puede contener información privilegiada y no puede ser usado ni divulgado por personas distintas a personal de EMSA E.S.P., Está prohibida su retención, copia, grabación, utilización o divulgación con cualquier propósito"

obligatoriamente las claves o contraseñas con un alto nivel de complejidad y utilizar los servicios de autenticación fuerte que posee la organización de acuerdo al rol asignado.

Los administradores de los sistemas de información deben seguir las políticas de cambio de clave y utilizar procedimiento de salvaguarda o custodia de las claves o contraseñas en un sitio seguro. A este lugar solo debe tener acceso el líder del Área de Tecnologías de Información y Comunicaciones o el Asesor para la de Seguridad de la Información.

Las Directrices de establecimiento, uso y protección de claves de acceso, se encuentran definidas en el documento de **Lineamientos para el control de acceso.**

TIC define las reglas para asegurar un acceso controlado, físico o lógico, a la información y plataforma informática de EMSA, considerándolas como importantes para el SGSI.

La conexión remota a la red de área local de EMSA debe realizarse a través de una conexión VPN segura suministrada por la organización, la cual debe ser aprobada, registrada y auditada, por el área de Tecnologías de información Comunicaciones; el procedimiento para llevar a cabo esta conexión se encuentra en el documento **PROCEDIMIENTO DE CONEXIÓN POR VPN SSL.**

Todo aplicativo informático o software debe ser comprado o aprobado por el área de Tecnologías de información.

Las reglas se encuentran definidas en el **Lineamiento de Control de Acceso.**

9.1.9 Uso de unidades de red o carpetas virtuales

Asegurar la operación correcta y segura de las unidades de red o carpetas virtuales.
Las Directrices de uso de uso de discos de red o carpetas virtuales se encuentran definidas en el documento de Lineamiento de uso de servicios de TI.

9.1.10 Uso de puntos de red de datos y de voz (red de área local – LAN extendida)

Asegurar la operación correcta y segura de los puntos de red.

"Este documento es confidencial, puede contener información privilegiada y no puede ser usado ni divulgado por personas distintas a personal de EMSA E.S.P., Está prohibida su retención, copia, grabación, utilización o divulgación con cualquier propósito"

Las Directrices de uso de puntos de red de datos, se encuentran definidas en el documento de **Lineamiento de uso de servicios de TI.**

9.1.11 Controles criptográficos

Implementar actividades para proteger activos de información clasificada, fortaleciendo la confidencialidad, disponibilidad e integridad, mediante el uso de herramientas criptográficas.

Las Directrices controles criptográficos se encuentran definidas en el Documento de **Lineamientos controles criptográficos.**

9.1.12 Seguridad Física

Implementar el programa de seguridad física para el acceso a las instalaciones que permita fortalecer la confidencialidad, disponibilidad e integridad de la información.

El Área de Tecnologías de la Información y Comunicaciones, debe tener implementadas el sistema de acceso biométrico los centros de datos y de cableado de EMSA.

El Proceso de Logística, debe implementar un sistema de seguridad física para las instalaciones de EMSA en el departamento incluyendo oficinas de atención al cliente y subestaciones.

El Proceso Logística, debe mantener actualizado el programa de seguridad física de las instalaciones, así como el programa de mantenimiento de las barreras de seguridad (Perimetrales e internas) de las instalaciones pertenecientes a las diferentes sedes administrativas, OAC y subestaciones.

TIC informará las debilidades que encuentren a nivel de barreras físicas a la oficina de logística para aprobación y corrección.

9.1.13 Seguridad de los centros de datos y cableado

Asegurar la protección de la información en las redes y la protección de la infraestructura de soporte. En las instalaciones del centro de datos o de los centros de cableado, No está permitido:

- Fumar dentro del Datacenter.

"Este documento es confidencial, puede contener información privilegiada y no puede ser usado ni divulgado por personas distintas a personal de EMSA E.S.P., Está prohibida su retención, copia, grabación, utilización o divulgación con cualquier propósito"

- Introducir alimentos o bebidas al Datacenter
- El porte de armas de fuego, cortopunzantes o similares.
- Mover, desconectar y/o conectar equipo de cómputo sin autorización.
- Modificar la configuración del equipo o intentarlo sin autorización.
- Alterar software instalado en los equipos sin autorización.
- Alterar o dañar las etiquetas de identificación de los servidores, sistemas de información, equipos de protección o sus conexiones físicas.
- Extraer información de los equipos en dispositivos externos.
- Abuso y/o mal uso de los sistemas de información.
- Toda persona debe hacer uso únicamente de los equipos y accesorios que les sean asignados y para los fines que se les autorice.

Los centros de datos cuentan con claves de acceso o tarjeta de proximidad, así como los gabinetes o armarios cuentan con llaves para apertura, las cuales deben permanecer almacenadas en la debida caja de seguridad de doble factor (llave y clave) dispuesta para ello dentro del centro de cómputo.

Las Directrices de seguridad del centro de datos y centros de cableado, se encuentran definidas en el documento de Lineamientos para el control de acceso.

9.1.14 Seguridad de los Equipos

Asegurar la protección de la información en los equipos.

Las Directrices de seguridad de equipos se encuentran definidas en el documento de Lineamientos de seguridad de los Equipos y de las operaciones de TIC.

9.1.15 Escritorio y pantalla limpia

Se definen las pautas generales para reducir el riesgo de acceso no autorizado, pérdida y daño de la información durante y fuera del horario de trabajo normal de los usuarios.

Los funcionarios, contratistas, personas en comisión, pasantes y terceros que tienen algún vínculo con EMSA deben conservar su escritorio libre de información, propia de la entidad, que pueda ser alcanzada, copiada o utilizada por terceros o por personal que no tenga autorización para su uso o

"Este documento es confidencial, puede contener información privilegiada y no puede ser usado ni divulgado por personas distintas a personal de EMSA E.S.P., Está prohibida su retención, copia, grabación, utilización o divulgación con cualquier propósito"

conocimiento.

Los usuarios de los sistemas de información y comunicaciones de EMSA deben bloquear la pantalla de su computador con el protector de pantalla, en los momentos que no esté utilizando el equipo o cuando por cualquier motivo deba dejar su puesto de trabajo (Windows+L).

Los usuarios de los sistemas de información y comunicaciones de EMSA deben cerrar las aplicaciones y servicios de red cuando ya no los necesite.

Al imprimir documentos con información pública reservada y/o pública clasificada (semi-privada o privada), deben ser retirados de la impresora inmediatamente y no se deben dejar en el escritorio sin custodia.

No se debe utilizar fotocopiadoras, escáneres, cámaras digitales, video-proyectores y en general equipos tecnológicos que se encuentren desatendidos.

9.1.16 Seguridad de las Operaciones de TIC

Definir las reglas para asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de EMSA, con el fin de robustecer la continuidad de los sistemas de TIC.

Las Directrices de uso de seguridad de las operaciones de TIC se encuentran definidas en el documento de Lineamientos de seguridad de los Equipos y de las operaciones de TIC.

9.1.17 Adquisición, desarrollo y mantenimiento de sistemas de información.

Garantizar que la seguridad es parte integral de los sistemas de información.

Las Directrices de adquisición, desarrollo y mantenimiento de sistemas de Información, se encuentran definidas en el documento de Lineamiento de adquisición, desarrollo y mantenimiento de sistemas de información.

9.1.18 Respaldo y restauración de información

El área de TIC proporcionará y garantizará los medios de respaldo adecuados para asegurar que toda la información esencial que reposa en los ambientes productivos de EMSA y el software se pueda recuperar después de una falla, garantizando que la información y la infraestructura de software crítica de la organización, sean respaldadas y puedan ser restauradas en caso de una falla y/o desastre bajo los RTO (Recovery Time Objective) y RPO (Recovery Point Objective) definidos en los acuerdos contractuales.

"Este documento es confidencial, puede contener información privilegiada y no puede ser usado ni divulgado por personas distintas a personal de EMSA E.S.P., Está prohibida su retención, copia, grabación, utilización o divulgación con cualquier propósito"

La restauración de copias de respaldo en ambientes de producción debe estar debidamente aprobada por el propietario de la información y solicitadas a través de la herramienta de gestión de requerimientos establecida por EMSA.

Semanalmente el administrador de plataforma de back up de EMSA, verificará la correcta ejecución de los procesos de back up.

Los administradores de la plataforma de copias de seguridad de la organización deben generar tareas de restauración aleatorias de la información y deben ser documentadas; una vez al mes se realiza la restauración de la copia de seguridad full de las bases de datos de producción y de los servidores definidos como críticos.

Para los cargos de la alta dirección, se realizará la copia de seguridad de manera automática a través del software establecido para ello, en los tiempos no laborales de manera que no interrumpa la sesión de trabajo y dinámica de la entidad.

Se realiza una copia de seguridad diario full de la base de datos en la herramienta de back up de la entidad.

Se realiza una copia de seguridad de los logs, cada 4 horas de las bases de datos clasificadas como críticas.

La copia de seguridad generada de las bases de datos críticas se almacena en una unidad externa de almacenamiento debidamente cifrado.

EMSA proporcionará el espacio de almacenamiento en un servidor para que cada área o proceso gestione sus propios respaldos. Dependiendo de la criticidad del proceso, se realizará diario, semanal o quincenalmente, según las funciones y responsabilidad del cargo.

Las Directrices de respaldo y restauración de Información, se encuentran definidas en el procedimiento copias de seguridad PR-GSO-TI-01.

9.1.19 Realización de copias de seguridad de estaciones de trabajo de usuario final

Se debe asegurar la operación de realización de copias de seguridad de información de estaciones de trabajo de usuario final. Los funcionarios de EMSA son responsables de realizar y actualizar los respaldos de la información que tiene en el equipo asignado mínimo cada 30 días.

"Este documento es confidencial, puede contener información privilegiada y no puede ser usado ni divulgado por personas distintas a personal de EMSA E.S.P., Está prohibida su retención, copia, grabación, utilización o divulgación con cualquier propósito"

El uso de dispositivos de almacenamiento externo (dispositivos móviles, DVD, CD, memorias USB, agendas electrónicas, celulares, etc.), pueden ocasionalmente generar riesgos para la organización al ser conectados a los computadores, ya que son susceptibles de transmisión de virus informáticos o pueden ser utilizados para la extracción de información no autorizada. Para utilizar dispositivos de almacenamiento externo se debe obtener aprobación formal e individual del área TIC.

Bajo ninguna eventualidad ni solicitud se entregará copia de las bases de datos y servidores en dispositivos como discos duros externos, USB, CD, DVD. Salvo por la solicitud escrita de las autoridades judiciales u organismos de control y deberá contar con la aprobación del oficial de seguridad o responsable del equipo TIC de EMSA y jurídico, en tal caso se mantendrá un registro de los archivos copiados a través el agente de cliente DLP (prevención de fuga de información) instalado.

Los medios que vayan a ser eliminados o que cumplan el periodo de retención deben surtir un proceso de borrado seguro y posteriormente serán eliminados o destruidos de forma adecuada.

Todos los mensajes son sujetos a análisis frente a amenazas y ataques dirigidos, y pueden ser conservados, puestos en cuarentena y/o eliminados permanentemente por parte de la organización.

Las Directrices de copias en estaciones de trabajo de usuario final, se encuentran definidas en el documento de **procedimiento de copias de respaldo y restauración PR-GSO-TI-01**.

9.1.20 Registro y seguimiento de eventos de sistemas de información y comunicaciones.

Preservar la integridad, confidencialidad y disponibilidad de los registros de eventos (logs) generados por los sistemas de información y comunicaciones de EMSA.

Las Directrices de registro y seguimiento de eventos de Sistemas de Información y comunicaciones, se encuentran definidas en el documento de Lineamiento para registro y seguimiento de eventos de sistemas de información y comunicaciones.

9.1.21 Control de software operacional de EMSA.

Generar acciones que permitan preservar la integridad de los sistemas operativos pertenecientes de EMSA.

"Este documento es confidencial, puede contener información privilegiada y no puede ser usado ni divulgado por personas distintas a personal de EMSA E.S.P., Está prohibida su retención, copia, grabación, utilización o divulgación con cualquier propósito"

Las Directrices de control de software operacional se encuentran definidas en el documento de Lineamientos de seguridad de los Equipos y de las operaciones de TIC.

9.1.22 Gestión de vulnerabilidades

Evitar la utilización de vulnerabilidades técnicas de los sistemas de información y comunicaciones de EMSA, e implementar los lineamientos para gestión de vulnerabilidades.

Las directrices de gestión de vulnerabilidades se encuentran definidas en el documento de lineamiento para gestión de incidentes y vulnerabilidades de Seguridad de la Información.

9.1.23 Seguridad de las comunicaciones.

Implementar mecanismos de control que permitan mantener la disponibilidad de las redes de datos, sistemas de comunicaciones e instalaciones de procesamiento de EMSA.

Las directrices de seguridad de las comunicaciones se encuentran definidas en el documento de Lineamientos de administración de Red.

9.1.24 Transferencia de Información.

Proteger la información transferida al interior y exterior de EMSA.

El Área de Tecnologías de Información y Comunicaciones, realiza el control del uso de sistemas de transferencia de archivos vía FTP a terceros.

Las directrices para transferencia de información se encuentran definidas en el documento de Lineamientos para acuerdos de transferencia de información.

9.1.25 Uso de correo electrónico.

Se define las pautas generales para asegurar una adecuada protección de la información de EMSA, en el uso del servicio de correo electrónico por parte de los usuarios autorizados.

El personal del área de Tecnologías de la Información y Comunicaciones no debe dar a conocer su clave de usuario de los sistemas de información a terceros, sin previa autorización del Líder del Área de tecnologías de la Información y Comunicaciones.

"Este documento es confidencial, puede contener información privilegiada y no puede ser usado ni divulgado por personas distintas a personal de EMSA E.S.P., Está prohibida su retención, copia, grabación, utilización o divulgación con cualquier propósito"

Los usuarios y claves de los administradores de sistemas y del personal del Área de Tecnologías de la información son de uso personal e intransferible.

El personal del área de Tecnologías de la Información y Comunicaciones debe emplear obligatoriamente las claves o contraseñas con un alto nivel de complejidad y utilizar los servicios de autenticación fuerte que posee la entidad de acuerdo al rol asignado.

Los administradores de los sistemas de información deben seguir las políticas de cambio de clave y utilizar procedimiento de salvaguarda o custodia de las claves o contraseñas en un sitio seguro. A este lugar solo debe tener acceso el líder del Área de Tecnologías de Información y Comunicaciones o el Asesor para la de Seguridad de la Información.

Las directrices de uso de correo electrónico se encuentran definidas en el documento de Lineamientos uso de servicios.

9.1.26 Webmaster

Proteger la integridad del sitio Web institucional, el software y la información contenida.

Las claves de acceso de los responsables de los contenidos de las páginas Web (webmasters), son estrictamente confidenciales, personales e intransferibles.

Las Directrices para web masters se encuentran definidas en el documento de Lineamientos para usuarios y administradores de TI.

9.1.27 Funcionarios y contratistas del Área de Tecnología de la información.

Definir las pautas generales para asegurar una adecuada protección de la información de EMSA por parte de los funcionarios y contratistas de TI de la entidad.

Las directrices se encuentran definidas en el documento de Lineamientos para usuarios y administradores de TI, en protección de Información.

9.1.28 Outsourcing o Tercerización.

Mantener la seguridad de la información y los servicios de procesamiento de información, a los cuales

"Este documento es confidencial, puede contener información privilegiada y no puede ser usado ni divulgado por personas distintas a personal de EMSA E.S.P., Está prohibida su retención, copia, grabación, utilización o divulgación con cualquier propósito"

tienen acceso terceras partes, entidades externas o que son procesados, comunicados o dirigidos por estas.

Se deben establecer criterios de selección que contemplen la experiencia y reputación de terceras partes, certificaciones y recomendaciones de otros clientes, estabilidad financiera de la compañía, seguimiento de estándares de gestión de calidad y de seguridad y otros criterios que resulten de un análisis de riesgos de la selección y los criterios establecidos por la entidad.

Se debe establecer mecanismos de control en las relaciones contractuales, con el objetivo de asegurar que la información a la que tengan acceso o servicios que sean provistos por los proveedores o contratistas, cumplan con las políticas de seguridad de la información de EMSA, las cuales deben ser divulgadas por los funcionarios responsables de la realización y/o firma de contratos o convenios.

En los contratos o acuerdos con los proveedores y/o contratistas se debe incluir una causal de terminación del acuerdo o contrato de servicios, por el no cumplimiento de las políticas de seguridad de la información.

Los contratistas, oferentes y/o proveedores deben aceptar y firmar el acuerdo de confidencialidad establecido por EMSA.

El Área de Tecnologías de Información deberá mitigar los riesgos de seguridad con referencia al acceso de los proveedores y/o contratistas a los sistemas de información de EMSA.

Se debe identificar y monitorear los riesgos relacionados con los contratistas o proveedores en relación con los objetos contractuales, incluyendo la cadena de suministro de los servicios de tecnología y comunicación.

Se deben identificar los riesgos para la información y los servicios de procesamiento de información que involucren partes externas a EMSA.

Los funcionarios de EMSA que fungen como supervisores de contratos relacionados con sistemas de información deberán realizar seguimiento, control y revisión de los servicios suministrados por los proveedores y/o contratistas.

Se deben establecer mecanismos o condiciones con los contratistas o proveedores que permitan realizar la gestión de cambios en los servicios suministrados.

"Este documento es confidencial, puede contener información privilegiada y no puede ser usado ni divulgado por personas distintas a personal de EMSA E.S.P., Está prohibida su retención, copia, grabación, utilización o divulgación con cualquier propósito"

9.1.29 Gestión de los Incidentes de la Seguridad de la Información

Se debe asegurar que los eventos e incidentes de seguridad que se presenten con los activos de información sean comunicados y atendidos oportunamente, empleando los procedimientos definidos, con el fin de tomar oportunamente las acciones correctivas.

Las Directrices de gestión de incidentes de seguridad de la Información, se encuentran definidas en el documento de Lineamiento para gestión de incidentes y vulnerabilidades de Seguridad de la Información.

9.1.30 Uso de mensajería instantánea y redes sociales

EMSA define las pautas generales para asegurar una adecuada protección de la información de la organización, en el uso del servicio de mensajería instantánea y de las redes sociales, por parte de los usuarios autorizados.

La información que se publique o divulgue por cualquier medio de Internet, de cualquier funcionario, contratista o colaborador de EMSA, que sea creado a nombre personal en redes sociales como: twitter®, facebook®, youtube® likedink®, blogs, instagram, etc, se considera fuera del alcance del SGSI y por lo tanto su confiabilidad, integridad, disponibilidad y los daños y perjuicios que pueda llegar a causar serán de completa responsabilidad de la persona que las haya generado.

Toda información distribuida en las redes sociales que sea originada por la organización debe ser autorizada por los líderes de área para ser socializadas y producidas con un vocabulario institucional.

No se debe utilizar el nombre de la organización en las redes sociales para difamar o afectar la imagen y reputación de los seguidores cuando responden comentarios en contra de la filosofía de la institución.

Las directrices de uso se encuentran definidas en el documento de Lineamientos uso de servicios de TI.

9.1.31 Uso de dispositivos móviles

EMSA establece las directrices de uso y manejo de dispositivos móviles (teléfonos móviles, teléfonos inteligentes “smartphones”, tabletas), entre otros, suministrados por EMSA y personales que hagan uso de los servicios de información de la organización.

"Este documento es confidencial, puede contener información privilegiada y no puede ser usado ni divulgado por personas distintas a personal de EMSA E.S.P., Está prohibida su retención, copia, grabación, utilización o divulgación con cualquier propósito"

Los usuarios no están autorizados a cambiar la configuración, a desinstalar software, formatear o restaurar de fábrica los equipos móviles institucionales, cuando se encuentran a su cargo, únicamente se deben aceptar y aplicar las actualizaciones.

Las Directrices de uso de dispositivos móviles se encuentran definidas en el Lineamiento de uso de activos de Información y dispositivos móviles.

9.1.32 Uso de impresoras y servicio de Impresión

Asegurar la operación correcta y segura de las impresoras y del servicio de impresión.

Las Directrices de uso de impresoras y servicio de impresión, se encuentran definidas en el documento de Lineamiento de uso de servicios de TI.

9.1.33 Política de retención y archivo de datos.

Mantener la integridad y disponibilidad de la información y de los servicios de procesamiento de información.

La política de retención de archivos debe establecer cuánto tiempo se deben mantener almacenados los archivos en EMSA de acuerdo a las tablas de retención documental.

Las reglas y los principios generales que regulan la función archivística se encuentran definidos por la Ley, en sus diferentes niveles, producidos en función de su misión y naturaleza.

La ley prevé el uso de las tecnologías de la información y las comunicaciones en la administración, conservación de archivos y en la elaboración e implantación de programas de gestión de documentos.

9.1.34 LINEAMIENTOS

9.1.35 Lineamientos para gestión y uso de los activos

Los activos de información pertenecen a EMSA y el uso de estos, debe emplearse exclusivamente con propósitos laborales.

Los usuarios deberán utilizar únicamente los programas y equipos autorizados por el Área de Tecnologías de la Información.

"Este documento es confidencial, puede contener información privilegiada y no puede ser usado ni divulgado por personas distintas a personal de EMSA E.S.P., Está prohibida su retención, copia, grabación, utilización o divulgación con cualquier propósito"

EMSA proporcionará al usuario, los equipos informáticos y los programas instalados en ellos; los datos/información creados, almacenados y recibidos, serán propiedad de EMSA, los funcionarios no podrán realizar copias de seguridad de sus archivos personales o de información pública, para copiar cualquier tipo de información clasificada o reservada debe pedir autorización a su jefe inmediato, de acuerdo a las normas sobre clasificación de la información de acuerdo a los niveles de seguridad establecidos por EMSA; su copia, sustracción, daño intencional o utilización para fines distintos a las labores propias de la Organización, serán sancionadas de acuerdo con las normas y legislación vigentes.

Periódicamente, el área de Tecnologías de la Información efectuará la revisión de los programas utilizados en cada dependencia.

La descarga, instalación o uso de aplicativos o programas informáticos NO autorizados será considerada como una violación a las Políticas de Seguridad de la Información de EMSA.

Todos los requerimientos de aplicativos, sistemas y equipos informáticos deben ser solicitados por el Líder de la dependencia a través de la plataforma Help Desk GLPI del área de Tecnologías de Información.

Estarán bajo custodia del área de Tecnologías de la Información los medios magnéticos/electrónicos (memorias USB, CDs u otros) que vengan originalmente con el software y sus respectivos manuales y licencias de uso, adicionalmente las claves para descargar el software de fabricantes de sus páginas web o sitios en internet y las contraseñas de administración de los equipos informáticos, sistemas de información o aplicativos.

En caso de ser necesario y previa autorización del Comité de Seguridad de la Información de EMSA, los funcionarios de EMSA podrán acceder a revisar cualquier tipo de activo de información y material que los usuarios creen, almacenen, envíen o reciban, a través de Internet o de cualquier otra red o medio, en los equipos informáticos a su uso.

Los recursos informáticos de EMSA no podrán ser utilizados, sin previa autorización escrita, para divulgar, propagar o almacenar contenido personal o comercial de publicidad, promociones, ofertas, programas destructivos (virus), propaganda política, material religioso o cualquier otro uso que no esté autorizado.

Los usuarios no deben realizar intencionalmente actos que impliquen un mal uso de los recursos

"Este documento es confidencial, puede contener información privilegiada y no puede ser usado ni divulgado por personas distintas a personal de EMSA E.S.P., Está prohibida su retención, copia, grabación, utilización o divulgación con cualquier propósito"

tecnológicos o que vayan en contravía de las políticas de seguridad de la información entre ellos envíos o reenvíos masivos de correos electrónicos o spam, practica de juegos en línea, uso permanente de redes sociales personales, conexión de periféricos o equipos que causen molestia a compañeros de trabajo, etc.

Los usuarios no podrán efectuar ninguna de las siguientes labores sin previa autorización del Área de Tecnologías de la Información:

1. Instalar software en cualquier equipo de EMSA;
2. Bajar o descargar software de Internet u otro servicio en línea en cualquier equipo de EMSA;
3. Modificar, revisar, transformar o adaptar cualquier software propiedad de EMSA;
4. Descompilar o realizar ingeniería inversa en cualquier software de propiedad de EMSA;
5. Copiar o distribuir cualquier software de propiedad de EMSA;
6. Cambiar la configuración de hardware de propiedad de EMSA;

El usuario deberá informar al área de Tecnologías de Información de EMSA a través de la plataforma de Help Desk GLPI y al Jefe Inmediato, sobre cualquier violación de las políticas de seguridad, uso indebido y debilidades de seguridad de la información de EMSA que tenga conocimiento.

El usuario será responsable de todas las transacciones o acciones efectuadas con su “cuenta de usuario”.

9.1.36 Lineamientos para uso de dispositivos móviles

Los dispositivos móviles (teléfonos móviles, teléfonos inteligentes (smartphones) tabletas, entre otros), son una herramienta de trabajo que se deben utilizar únicamente para facilitar las comunicaciones de los usuarios de la organización.

Los dispositivos móviles corporativos deben estar integrados a una plataforma de administración controlada por el Área de Tecnologías de Información.

Los usuarios de dispositivos móviles corporativos deben tener instaladas únicamente las aplicaciones distribuidas, autorizadas y configuradas por el administrador de la plataforma.

Los dispositivos móviles asignados por EMSA deben tener la configuración realizada por el Área de Tecnologías de Información, así mismo solo podrá configurarse las cuentas de correo electrónico asignadas al usuario por la Organización.

"Este documento es confidencial, puede contener información privilegiada y no puede ser usado ni divulgado por personas distintas a personal de EMSA E.S.P., Está prohibida su retención, copia, grabación, utilización o divulgación con cualquier propósito"

El sistema de mensajería instantánea autorizado para los dispositivos móviles institucionales es Skype empresarial, deberá ser federada por el Área de Tecnologías de Información.

En el caso del nivel directivo se autoriza el uso de WhatsApp únicamente en dispositivos suministrados por EMSA, no se permite por esta aplicación, el envío de fotografías, audios y videos clasificados como información pública reservada o información pública clasificada (privada o semiprivada).

Los sistemas de mensajería instantánea para dispositivos móviles corporativos a implementar en EMSA deben incluir métodos de cifrado de extremo a extremo de la comunicación.

Los dispositivos móviles deben tener contraseña de ingreso y bloqueo del equipo de manera automática y manual, tener activado la función de borrado remoto, cifrar la memoria de almacenamiento.

Los dispositivos móviles corporativos deben tener únicamente la tarjeta sim asignada por la entidad, de igual forma la tarjeta sim únicamente debe instalarse en los equipos asignados por la organización.

Ante la pérdida del equipo, ya sea por extravío o hurto, deberá informar de manera inmediata al Área de Tecnologías de Información, y continuar con el procedimiento administrativo por perdida de elementos establecidos por la entidad.

Los teléfonos móviles y/o teléfonos inteligentes corporativos, debe permanecer encendidos y cargados durante las horas laborales o de acuerdo a la responsabilidad y requerimientos propios del cargo.

Es responsabilidad del usuario hacer buen uso del dispositivo suministrado por EMSA con el fin de realizar actividades propias de su cargo o funciones asignadas en la organización.

Los usuarios no están autorizados a cambiar la configuración, ni a la desinstalación de software de los equipos móviles corporativos posterior a su recibo; únicamente se deben aceptar y aplicar las actualizaciones.

Los usuarios de dispositivos móviles asignados por la organización deben evitar hacer uso de estos en lugares con algún riesgo de seguridad, evitando el extravío o hurto del equipo.

Los usuarios de dispositivos móviles corporativos no deben conectarlos en computadores y/o puertos USB de uso público (Restaurantes, café internet, aeropuertos, etc.).

"Este documento es confidencial, puede contener información privilegiada y no puede ser usado ni divulgado por personas distintas a personal de EMSA E.S.P., Está prohibida su retención, copia, grabación, utilización o divulgación con cualquier propósito"

Los usuarios de dispositivos móviles corporativos deben mantener desactivados las funciones de redes inalámbricas WiFi, puertos infrarrojos, puerto Bluetooth.

Los usuarios de dispositivos móviles corporativos NO deben hacer uso de redes inalámbricas públicas.

En caso de requerir instalación de aplicaciones adicionales en el dispositivo móvil institucional se debe solicitar al Comité de Seguridad de la Información para su aprobación.

9.1.37 Lineamientos de uso de correo electrónico

Creación de correo electrónico:

El correo electrónico corporativo para un usuario debe ser creado de acuerdo a la solicitud de creación de cuenta de usuario, realizada mediante aplicativo Help Desk GLPI, Ver formato para solicitud de creación de cuenta de usuario y servicios de TI FO-GSO-TI-06.

Piemsa/Sistema Integral de Gestión/Documentos/Gestión Soporte Organizacional /Procesos/Gestión TIC/Formatos/FO-GSO-TI-06 Administración de usuarios.pdf

El usuario perteneciente al área de Tecnología de información, responsable de crear la cuenta red y correo electrónico, la define de la siguiente forma:

- Para funcionarios de planta: primernombre.primerapellido@emsa-esp.com.co, si ya existe un usuario con este nombre asignado en la cuenta de red de EMSA, se agrega posterior a primer nombre la inicial del segundo nombre; p.e.carlosm.grisales@emsa-esp.com.co,

- Contratistas: con_primernombreprimerapellido@emsa-esp.com.co,
- Planta temporal: tem_primernombreprimerapellido@emsa-esp.com.co,

Servicio de correo electrónico:

Permite a los usuarios de EMSA, el intercambio de mensajes, a través de una cuenta de correo electrónico corporativa, que facilita el desarrollo de sus funciones.

Principios guía

Los usuarios del correo electrónico corporativo son responsables de evitar prácticas o usos del correo que puedan comprometer la seguridad de la información.

"Este documento es confidencial, puede contener información privilegiada y no puede ser usado ni divulgado por personas distintas a personal de EMSA E.S.P., Está prohibida su retención, copia, grabación, utilización o divulgación con cualquier propósito"

Los servicios de correo electrónico corporativo se emplean para servir a una finalidad operativa y administrativa en relación con la Organización.

Todos los correos electrónicos procesados por los sistemas, redes y demás infraestructura TIC de EMSA se consideran bajo el control de la Organización.

Este servicio debe utilizarse exclusivamente para las tareas propias de la función desarrollada en EMSA y no debe utilizarse para ningún otro fin.

No está autorizado el envío de cadenas de correo, envío de correos masivos con archivos adjuntos de gran tamaño que puedan congestionar la red.

No está autorizado el envío de correos con contenido que atenten contra la integridad y dignidad de las personas y el buen nombre de la entidad. Cuando un funcionario, contratista o colaborador al que le haya sido autorizado el uso de una cuenta de correo electrónico y se retire de EMSA, su cuenta de correo será desactivada.

Los correos electrónicos deben contener la siguiente nota respecto al manejo del contenido:

Aviso legal - Protección de datos personales: ELECTRIFICADORA DEL META S.A. E.S.P., -en adelante La Empresa - identificada con NIT 892.002.210-6, ubicada en la Calle 41 #32-25, Villavicencio (Meta) y teléfono 661 4000, dando cumplimiento a lo estipulado en la ley 1581 de 2012 y su decreto reglamentario 1377 de 2013, tendiente a la protección de datos personales lo invita a que conozca la política de privacidad en el siguiente enlace: www.electrificadoradelmeta.com.co, la cual establece los derechos que le asisten como titular, el procedimiento para ejercerlos, las finalidades para la cual se tratan los datos, entre otros aspectos. Si usted tiene alguna inquietud frente al manejo de la información, envíe un correo electrónico a pqr@emsa-esp.com.co y con gusto será atendido. Confidencialidad: La información contenida en este mensaje, en los archivos adjuntos son confidenciales. Esta es de uso exclusivo del (de los) destinatario(s) sin la intención de que sea conocida por terceros, por lo tanto, de conformidad con las normas legales vigentes, su interceptación, sustracción, extravío, reproducción o uso no autorizado está prohibido a cualquier persona diferente. Si usted ha recibido este correo por error, equivocación u omisión queda estrictamente prohibido la utilización, copia, reimpresión, reenvió; cualquier acción tomada sobre este correo podrá ser penalizada legalmente. En tal caso, favor notificar en forma inmediata al remitente.

El tamaño del buzón de correo electrónico estará determinado por el rol desempeñado por el usuario en EMSA.

Cada área debe solicitar la creación o ajuste de las cuentas electrónicas para sus funcionarios o

contratistas de acuerdo con el procedimiento solicitud de creación o ajuste de cuenta de usuario y servicios de tecnología de información FO-GSO-TI-06.

El Área de Soporte Organizacional y las dependencias que realizan Contratación son las responsables de solicitar la cancelación de las cuentas electrónicas al Área de Tecnologías de Información de EMSA, por retiro de funcionario o término del contrato.

Las cuentas de correo electrónico son propiedad de EMSA, las cuales son asignadas a personas que tengan algún tipo de vinculación laboral con la Organización, ya sea como personal de planta, en comisión permanente, contratistas, consultores o personal temporal, quienes deben utilizar este servicio única y exclusivamente para las tareas propias de la función desarrollada en la Organización y no debe utilizarse para ningún otro fin.

Cada usuario es responsable del contenido del mensaje enviado y de cualquier otra información adjunta al mismo, de acuerdo a la clasificación de la información establecida por EMSA.
Todos los mensajes son sujetos a análisis frente a amenazas y ataques informáticos dirigidos, y pueden ser conservados, puestos en cuarentena y/o eliminados permanentemente por parte de la Organización.

Todo usuario es responsable por la destrucción de los mensajes cuyo origen sea desconocido y por lo tanto asume la responsabilidad y las consecuencias que puede ocasionar la ejecución de cualquier archivo adjunto. En estos casos no se debe contestar dichos mensajes, ni abrir los archivos adjuntos y se debe reenviar el correo a la cuenta sistemas@emsa-esp.com.co con la frase “correo sospechoso” en el asunto.

El único servicio de correo electrónico autorizado en la entidad es el asignado por el Área de Tecnologías de la Información.

EMSA utilizará herramientas tecnológicas para prevenir el correo no deseado o spam.

9.1.38 Lineamientos para uso de mensajería instantánea y redes sociales

El uso de servicios de mensajería instantánea y el acceso a redes sociales estarán autorizados solo para un grupo reducido de usuarios, teniendo en cuenta sus funciones y para facilitar canales de comunicación con la ciudadanía.

"Este documento es confidencial, puede contener información privilegiada y no puede ser usado ni divulgado por personas distintas a personal de EMSA E.S.P., Está prohibida su retención, copia, grabación, utilización o divulgación con cualquier propósito"

No se permite el envío de mensajes con contenido que atente contra la integridad de las personas o instituciones o cualquier contenido que represente riesgo de código malicioso.

La información que se publique o divulgue por cualquier medio de Internet, de cualquier funcionario, contratista o colaborador de EMSA, que sea creado a nombre personal en redes sociales como: twitter®, facebook®, youtube®, blogs, instagram, etc, se considera fuera del alcance del SGSI y por lo tanto su confiabilidad, integridad y disponibilidad y los daños y perjuicios que pueda llegar a causar serán de completa responsabilidad de la persona que las haya generado.

Toda información distribuida en las redes sociales que sean originadas por la organización debe ser autorizada por los jefes de área para ser socializadas y con un vocabulario institucional.

No se debe utilizar el nombre de la entidad en las redes sociales para difamar o afectar la imagen y reputación de los seguidores cuando responden comentarios en contra de la filosofía de la organización.

9.1.39 Lineamientos para uso de Internet

La infraestructura, servicios y tecnologías usados para acceder a internet son propiedad de EMSA, por lo tanto, se reserva el derecho de monitorear el tráfico de internet y el acceso la información, respetando en todo momento el derecho a la privacidad y a la seguridad de los datos personales consagrados en la Ley 1581 de 2012.

No se permite la navegación a sitios con contenidos contrarios a la ley o a las políticas de EMSA o que representen peligro para la organización como: pornografía, terrorismo, hacktivismo, segregación racial u otras fuentes definidas por EMSA. El acceso a este tipo de contenidos con propósitos de estudio de seguridad o de investigación, debe contar con la autorización expresa del comité de seguridad de la Información de EMSA.

El Líder del Área de Tecnologías de Información autoriza los cambios solicitados de permisos de navegación a los usuarios de EMSA, previa solicitud del Líder de cada una de las dependencias, de acuerdo con Lineamientos de Control de Acceso y formato para solicitud de creación de cuenta de usuario y servicios de tecnología de información FO-GSO-TI-06.

El Área de Tecnologías de Información implementa herramientas para evitar la descarga de software no autorizado y/o código malicioso en los equipos institucionales así mismo controla el acceso a la información contenida en portales de almacenamiento en el internet para prevenir la fuga de información.

"Este documento es confidencial, puede contener información privilegiada y no puede ser usado ni divulgado por personas distintas a personal de EMSA E.S.P., Está prohibida su retención, copia, grabación, utilización o divulgación con cualquier propósito"

La descarga de archivos de Internet debe ser con propósitos laborales y de forma razonable para no afectar el servicio.

Los usuarios de los activos de información de EMSA tienen restringido el acceso a redes sociales, sistemas de mensajería instantánea, acceso a sistemas de almacenamiento en la nube y cuentas de correo no institucional. En caso de ser requerido por las funciones del cargo, el jefe inmediato debe remitir la solicitud a Jefe de Área de Tecnologías de Información, para que sea autorizado por el Comité de Seguridad de la Información y será objeto de auditorías de seguridad mediante los componentes de Seguridad Informática de la Organización.

9.1.40 Lineamientos para uso de estaciones de trabajo

La instalación de software en los computadores suministrados por EMSA, es una función exclusivadel área de Tecnologías y Sistemas de Información el cual mantendrá una lista actualizada del software autorizado en una unidad de almacenamiento virtual para instalar en los computadores.
Se define los perfiles de Administrador local para ingreso a equipos:

1. Administrador local
2. Administrador de soporte
3. Cuentas de servicio

Los usuarios que hagan uso de equipos institucionales en préstamo NO deberán almacenar información en estos dispositivos y deberán borrar aquellos que copien en estos al terminar su uso.

Los usuarios no deben mantener almacenados en los discos duros de las estaciones de trabajo o discos virtuales de red, archivos de vídeo, música, fotos y cualquier tipo de archivo que no sean de carácter institucional.

En el Disco C:\ de las estaciones cliente se tiene configurado el sistema operativo, aplicaciones y perfil de usuario, la persona que haga uso de los equipos deberá abstenerse de realizar modificaciones a estos archivos.

Los usuarios podrán trabajar sus documentos institucionales en borrador en la estación de trabajo asignada por EMSA y deberán ubicar copias y documentos finales en las carpetas virtuales centralizadas (Mi Arbolito) que se establezca para cumplir con las tablas de retención documental TRD de la Organización.

"Este documento es confidencial, puede contener información privilegiada y no puede ser usado ni divulgado por personas distintas a personal de EMSA E.S.P., Está prohibida su retención, copia, grabación, utilización o divulgación con cualquier propósito"

El préstamo de equipos de cómputo, computadores portátiles y vídeo proyectores, se debe tramitar a través de la mesa de ayuda, con solicitud registrada en la herramienta de gestión de solicitudes GLPI y/o correo electrónico remitido a la dirección de correo soporte.tics@emsa-esp.com.co, con anticipación y se proveerá de acuerdo a la disponibilidad.

Los equipos que ingresan temporalmente a EMSA que son de propiedad de terceros: deben ser registrados en los controles de acceso y su retiro de la entidad; posteriormente EMSA no se hará responsable en caso de pérdida o daño de algún equipo informático de uso personal o que haya sido ingresado a sus instalaciones.

El área de Tecnologías de Información no prestará servicio de soporte técnico (revisión, mantenimiento, reparación, configuración y manejo e información) a equipos que no sean de EMSA.

9.1.41 Lineamiento para uso de discos o carpetas virtuales

La aprobación de usuarios para obtener acceso a la información ubicada en los discos de red, la persona responsable de la carpeta virtual o el jefe inmediato del usuario deberá enviar un mensaje de correo electrónico institucional autorizando el acceso y permisos, correspondientes al rol y funciones a desempeñar, mediante la herramienta de gestión de solicitudes del Área de Tecnologías de Información de EMSA.

Los usuarios tendrán permisos de escritura, lectura o modificación de información en los discos de red, dependiendo de la solicitud a las funciones y el rol asignado.

La información institucional que se trabaje en las estaciones cliente de cada usuario debe ser trasladada periódicamente a los discos de red por ser información institucional.

La información almacenada en cualquiera de los discos de red debe ser de carácter institucional.

Está prohibido almacenar archivos que incumplan leyes de derechos de autor, información no relacionada con las funciones asignadas al usuario, información personal calificada como sensible de acuerdo con la ley 1581 de 2012, información de naturaleza intima del usuario.

Archivos que puedan ocasionar o constituir riesgos informáticos, como Software o código malicioso.

Se prohíbe extraer, divulgar o publicar información de cualquiera de los discos de red o estaciones de trabajo, sin expresa autorización de su jefe inmediato.

"Este documento es confidencial, puede contener información privilegiada y no puede ser usado ni divulgado por personas distintas a personal de EMSA E.S.P., Está prohibida su retención, copia, grabación, utilización o divulgación con cualquier propósito"

Se prohíbe el uso de la información de los discos de red con fines publicitarios, de imagen negativa, lucrativa o comercial.

9.1.42 Lineamientos de uso de impresoras y del servicio de Impresión

Los documentos que se impriman en las impresoras de EMSA deben ser de carácter institucional.
Es responsabilidad del usuario conocer el adecuado manejo de los equipos de impresión (escáner y fotocopiado) para que no se afecte su correcto funcionamiento.

Ningún usuario debe realizar labores de reparación o mantenimiento de las impresoras.

En caso de presentarse alguna falla, esta se debe reportar a la mesa de ayuda del Área de Tecnologías de Información.

Los funcionarios en el momento de realizar impresiones de documentos con clasificación pública reservada o información pública clasificada (privada o semiprivada), debe mantener control de la impresora, por lo cual no la deberán dejar desatendida, preservando la confidencialidad de la información.

9.1.43 Lineamientos de controles criptográficos

El Área de Tecnologías y Sistemas de Información debe verificar los sistemas o aplicaciones que realicen y/o permitan la transmisión de información pública reservada o información pública clasificada (privada o semiprivada), lo realicen mediante herramientas de cifrado de datos.

El Área de Tecnologías de Información proveerá la herramienta de encriptación datos a los usuarios, previa solicitud formal.

La asignación de la clave para el cifrado de la información en la herramienta debe ser establecida por el usuario que administra dicha información, teniendo siempre presente que, en caso de olvidar la clave, la información cifrada no es recuperable.

La contraseña de cifrado debe cumplir con la política de establecimiento de contraseñas de EMSA ver Lineamientos para el control de acceso.

Se utilizarán controles criptográficos en los siguientes casos:

"Este documento es confidencial, puede contener información privilegiada y no puede ser usado ni divulgado por personas distintas a personal de EMSA E.S.P., Está prohibida su retención, copia, grabación, utilización o divulgación con cualquier propósito"

• En la protección de claves de acceso a sistemas, datos y servicios.
• Para la transmisión de información Reservada o Clasificada, fuera de la Organización.
• En la protección de la información a resguardar, cuando así lo establezca el Comité de Seguridad de la Información, el generador de la información o el Administrador de Seguridad de la Información.

Ciclo de vida de llaves criptográficas

La Entidad no establece un lineamiento de ciclo de vida de llaves criptográficas, toda vez que, la asignación de la clave para el cifrado de la información en la herramienta, la establece el usuario que genera o administra la información a cifrar, teniendo siempre presente que, en caso de olvidar la clave, la información cifrada no es recuperable.

9.1.44 Lineamientos de seguridad para los Equipos

- **Instalación de equipos de procesamiento y almacenamiento**

Los equipos de procesamiento y almacenamiento deben ser instalados en las áreas de trabajo seguras definidas por el Área de Tecnologías y de Información.

- **Protecciones en el suministro de energía**

A la red de energía regulada de los puestos de trabajo solo se pueden conectar equipos como computadores, pantallas; los otros elementos deberán conectarse a la red no regulada. Esta labor debe ser revisada por el Área Administrativa.

El Área Administrativa de EMSA debe implementar sistemas redundantes de alimentación eléctrica, como, por ejemplo: plantas generadoras de energía que permita soportar la operación de los sistemas de información durante una falta de suministro de un proveedor de energía.

- **Seguridad del cableado**

Los cables deben estar claramente marcados para identificar fácilmente los elementos conectados y evitar desconexiones erróneas.

Deben existir planos que describan las conexiones del cableado.

El acceso a los centros de cableado (Racks), debe estar protegido.

El área de Tecnologías de Información establece un programa de revisiones y/o inspecciones físicas al cableado, con el fin de detectar dispositivos no autorizados.

"Este documento es confidencial, puede contener información privilegiada y no puede ser usado ni divulgado por personas distintas a personal de EMSA E.S.P., Está prohibida su retención, copia, grabación, utilización o divulgación con cualquier propósito"

- **Mantenimiento de los Equipos**

EMSA debe mantener contratos de soporte y mantenimiento de los equipos críticos.

Las actividades de mantenimiento tanto preventivo como correctivo deben registrarse para cada elemento.

Las actividades de mantenimiento de los servidores, elementos de comunicaciones, energía o cualquiera que pueda ocasionar una suspensión en el servicio, deben ser programadas y realizadas por personal autorizadas por el Área de Tecnologías de Información.

Los equipos que requieran salir de las instalaciones de EMSA para reparación o mantenimiento, deben estar debidamente autorizados por el Área Administrativa y se debe garantizar que en dichos elementos no se encuentra información clasificada de acuerdo con los niveles de clasificación de la información pública reservada o información pública clasificada (privada o semiprivada).

Para que los equipos puedan salir de las instalaciones, se debe suministrar un nivel mínimo de seguridad, que al menos cumpla con los requerimientos internos de la Organización, teniendo en cuenta los diferentes riesgos que se pueden presentar al trabajar en un ambiente que no cuenta con las protecciones ofrecidas en el interior de EMSA.

Los equipos retirados de la entidad deben ser protegidos, no se deben dejar sin vigilancia en lugares públicos, de igual forma se debe continuar con las recomendaciones de uso de los fabricantes de estos y la conexión con los sistemas de información de EMSA debe cumplir con la política de control acceso.

Cuando un dispositivo vaya a ser reasignado o retirado de servicio debe contar con aprobación del Área de Tecnologías de Información, así mismo debe garantizarse la eliminación de toda información residente en los elementos utilizados para el almacenamiento, procesamiento y transporte de la información, utilizando herramientas para realizar sobreescrituras sobre la información existente o la presencia de campos magnéticos de alta intensidad realizando el **Procedimiento de borrado seguro para equiposP-TI-12.**

Este proceso puede además incluir, una vez realizado el proceso anterior, la destrucción física del medio, utilizando impacto, fuerzas o condiciones extremas.

El traslado entre dependencias de EMSA de todo activo de información, está a cargo del Área Administrativa, para el control de inventarios.

"Este documento es confidencial, puede contener información privilegiada y no puede ser usado ni divulgado por personas distintas a personal de EMSA E.S.P., Está prohibida su retención, copia, grabación, utilización o divulgación con cualquier propósito"

- **Ingreso y retiro de activos de información de terceros**

El retiro e ingreso de todo activo de información de propiedad de los usuarios de EMSA, utilizados para fines personales, se realizará mediante los procedimientos establecidos por el sistema de seguridad física.

EMSA no se hace responsable de los bienes o los problemas que se presenten al conectarse a la red eléctrica de la Organización.

El retiro e ingreso de todo activo de información de los visitantes que presten servicios a EMSA (consultores, pasantes, visitantes, proveedores etc.) será registrado e inspeccionado en los controles de accesos de las instalaciones de la Empresa. El personal de seguridad y vigilancia en los controles de acceso verificarán y registrarán las características de identificación del activo de información.

El traslado entre dependencias de EMSA de todo activo de información, está a cargo del área Administrativa, para el control de inventarios.

- **Normas de protección**

Los funcionarios que hagan uso de los equipos de EMSA, no deben dejar desatendidos los equipos de cómputo en sitios públicos y deben transportarlos en lugares visibles bajo medidas que le provean seguridad física.

Los computadores portátiles siempre deben ser transportados como equipaje de mano, evitando golpes, exponerlo a líquidos, y prevenir la perdida y/o hurto.

- **Áreas de despacho y carga de materiales**

Las áreas de despacho y carga de materiales se deben administrar de forma que el personal de despacho no tenga acceso a áreas de procesamiento de información, los materiales que ingresen se deben inspeccionar, para verificar la presencia de materiales peligrosos, todos los materiales que ingresen deben ser registrados de acuerdo a los procedimientos establecidos del Área Administrativa.

9.1.45 Lineamientos para usuarios y administradores de TI.

"Este documento es confidencial, puede contener información privilegiada y no puede ser usado ni divulgado por personas distintas a personal de EMSA E.S.P., Está prohibida su retención, copia, grabación, utilización o divulgación con cualquier propósito"

Directrices:

- El personal del Área de Tecnología de la información no debe dar a conocer su clave de usuario a terceros sin previa autorización del Líder del Área de Tecnología de la información.
- Los usuarios y claves de los administradores de sistemas y del personal del Área de Tecnología de la información son de uso personal e intransferible.
- El personal del Área de Tecnología de la información debe emplear obligatoriamente las claves o contraseñas con un alto nivel de complejidad.
- Los administradores de los sistemas de información deben seguir las políticas de cambio de clave y utilizar procedimiento de salvaguarda o custodia de las claves o contraseñas en un sitio seguro. A este lugar solo debe tener acceso el Líder del Área de Tecnología de la información o el Asesor de Seguridad Informática.
- Los documentos y en general la información de procedimientos, seriales, software etc. deben mantenerse custodiados en todo momento para evitar el acceso a personas no autorizadas.
- Para el cambio o retiro de equipos de funcionarios, se deben seguir políticas de saneamiento, es decir llevar a cabo mejores prácticas para la eliminación de la información de acuerdo al software disponible en la organización. Ej: Formateo seguro, destrucción total de documentos o borrado seguro de equipos electrónicos.
- Los funcionarios encargados de realizar la instalación o distribución de software sólo instalarán productos con licencia y software autorizado.
- Los funcionarios del Área de Tecnología de la información no deben otorgar privilegios especiales a los usuarios sobre las estaciones de trabajo, sin la autorización correspondiente del Líder del Área de Tecnología de la información y el registro en el sistema de la mesa de ayuda.
- Los funcionarios del Área de Tecnología de la información se obligan a no revelar a terceras personas, la información a la que tengan acceso en el ejercicio de sus funciones de acuerdo con la CALIFICACIÓN DE LA INFORMACIÓN DE ACUERDO CON SUS NIVELES DE SEGURIDAD. En consecuencia, se obligan a mantenerla de manera confidencial y privada y a protegerla para evitar su divulgación.
- Los funcionarios del Área de Tecnología de la información no utilizarán la información para fines comerciales o diferentes al ejercicio de sus funciones.
- Toda licencia de software o aplicativo informático y sus medios, se deben guardar y relacionar de tal forma que asegure su protección y disposición en un futuro.
- Las copias licenciadas y registradas del software adquirido deben ser únicamente instaladas en los equipos y servidores de la organización. Se deben hacer copias de seguridad en concordancia con las políticas del proveedor y de la organización.
- La copia de programas o documentación requiere tener la aprobación escrita de EMSA y del proveedor si éste lo exige.

"Este documento es confidencial, puede contener información privilegiada y no puede ser usado ni divulgado por personas distintas a personal de EMSA E.S.P., Está prohibida su retención, copia, grabación, utilización o divulgación con cualquier propósito"

- El personal del Área de Tecnología de la información debe velar por que se cumpla con el registro en la bitácora de acceso al datacenter, de las personas que ingresen y que hayan sido autorizadas previamente por la jefatura del área o por quien esta delegue.
- Por defecto deben ser bloqueados, todos los protocolos y servicios que no se requieran en los servidores; no se debe permitir ninguno de ellos, a menos que sea solicitado y aprobado oficialmente por la organización a través del Comité de Seguridad Informática y Comunicaciones establecido o el Asesor para la Seguridad Informática.
- Aquellos servicios y actividades que no son esenciales para el normal funcionamiento de los sistemas de información deben ser aprobados oficialmente por la organización, a través del Comité de Seguridad Informática y de Comunicaciones, y deben ser asegurados mediante controles que permitan la preservación de la seguridad de la información.
- El acceso a cualquier servicio, servidor o sistema de información debe ser autenticado y autorizado. La generación de accesos y permisos se enmarca exclusivamente dentro de los términos contractuales establecidos sin exceder los tiempos o fechas establecidos para ello, por lo cual la gerencia financiero-administrativa y el equipo TIC deberán contar con una comunicación eficaz que salvaguarde la seguridad, confiabilidad e integridad de la información. En casos excepcionales, analizarán un plan de contingencia y acciones concretas con carácter de urgente.
- Todos los servidores deben ser configurados con el mínimo de servicios necesarios y obligatorios para desarrollar las funciones designadas.
- Las pruebas de laboratorio o piloto deben ser autorizadas por el Comité de Seguridad Informática y de Comunicaciones, para sistemas de información, de software tipo freeware o shareware o de sistemas que necesiten conexión a internet; estas deben ser realizadas sin conexión a la red LAN de la organización y con una conexión separada de internet o en su defecto con una dirección IP diferente a las direcciones públicas de producción.

9.1.46 Lineamientos para la gestión de incidentes de seguridad de la información

EMSA establecerá responsables y procedimientos de gestión para el tratamiento de incidentes de seguridad de la información asegurando una respuesta rápida, eficaz y eficiente, quienes investigarán y solucionarán los incidentes presentados, implementando las acciones necesarias para evitar su repetición, así mismo debe escalar los incidentes de acuerdo con la criticidad de este.

El único canal acreditado para reportar incidentes de seguridad ante las autoridades y el pronunciamiento oficial ante entidades externas de EMSA es el Gerente General o el funcionario que sea delegado EMSA designa al Área de Tecnologías de la Información para responder a los eventos o incidentes de seguridad informática, de acuerdo a las sugerencias, recomendaciones y/o acompañamiento del CSIRT (Computer Security Incident Response) -Equipo de Respuesta a

"Este documento es confidencial, puede contener información privilegiada y no puede ser usado ni divulgado por personas distintas a personal de EMSA E.S.P., Está prohibida su retención, copia, grabación, utilización o divulgación con cualquier propósito"

Incidentes de Seguridad Informática de la Casa Militar; generando el procedimiento de respuesta. Casa Militar será el encargado de coordinar y adelantar las gestiones pertinentes para la atención de los eventos o incidentes de seguridad de la información.

Se debe establecer la implementación de lecciones aprendidas al término del análisis y solución de incidentes de seguridad de la información, estos deben ser socializados a los interesados conservando la confidencialidad de estas, de igual manera, serán utilizadas como herramienta para la toma de decisiones y revisiones de la política de seguridad. El CSIRT (Computer Security Incident Response) Equipo de respuesta a incidentes de seguridad informática de Casa Militar debe establecer el procedimiento para la recolección de evidencia digital, siguiendo los lineamientos jurídicos vigentes en Colombia y estándares internacionales.

En el caso que se presente un evento de Seguridad de la Información en el cual sea necesaria la verificación de la participación de algún funcionario de EMSA, debe ser reportado a la Oficina de Control Interno Disciplinario, mediante comunicación remitida por Sistema de Gestión Documental.
Si lo requiere, la Oficina de Control Interno Disciplinario, puede solicitar el apoyo por parte del CSIRT (Computer Security Incident Response) Equipo de respuesta a incidentes de seguridad informática de la Casa Militar, y al Área de Tecnologías de la Información.

9.1.47 Lineamiento para la gestión de vulnerabilidades

El Análisis de vulnerabilidades tiene como objetivo evaluar las debilidades que puedan existir en un determinado software, aplicación o sistema que pudiera afectar su integridad durante su vida útil en EMSA.

Se llevarán a cabo pruebas periódicas de análisis de vulnerabilidades cada 2 años, estas pruebas deben estar consensuadas y aprobadas por el comité de ciberseguridad, de forma que existan “limitaciones” legales, debido al riesgo al que se somete la organización en la realización de este tipo de pruebas.

El objetivo principal se centra en identificar todos los puertos abiertos, servicios en ejecución y vulnerabilidades ya conocidas sobre sistemas o aplicaciones. Con la premisa de generar un informe de las vulnerabilidades encontradas y como puede llegar a afectar estas vulnerabilidades a la continuidad de negocio. Para posteriormente solucionar o mitigar estas vulnerabilidades trazando un plan de actuación y así evitar sufrir ciberataques que repercutan en las tecnologías utilizadas y en los datos privados de la organización.

"Este documento es confidencial, puede contener información privilegiada y no puede ser usado ni divulgado por personas distintas a personal de EMSA E.S.P., Está prohibida su retención, copia, grabación, utilización o divulgación con cualquier propósito"

Este análisis de vulnerabilidades se efectuará con la ejecución de 2 técnicas:

- Pentesting que está enfocado a la realización de pruebas de penetración de forma ofensiva, atacando a los sistemas de información o a la propia organización, poniendo a prueba la concienciación de los trabajadores, haciendo uso de técnicas de ingeniería social.

- Ethical Hacking que simula el comportamiento de un atacante real, con el objetivo de comprometer la organización en su totalidad. Utilizando técnicas propias de bandas cibercriminales organizadas, haciendo uso de vectores de ataques poco conocidos e incluso ideando nuevos vectores de ataque que ponen a prueba las defensas de la organización.

"Este documento es confidencial, puede contener información privilegiada y no puede ser usado ni divulgado por personas distintas a personal de EMSA E.S.P., Está prohibida su retención, copia, grabación, utilización o divulgación con cualquier propósito"

10. REGLAS E NEGOCIO

ACTIVIDAD DEL PROCESO	CICLO PHVA	REGLA DE NEGOCIO	SUPERVISA	APLICA
Elaborar y/o actualizar el Plan Estratégico de Tecnologías de la Información - PETI	**P**	Elaborar y/o actualizar el Plan de Tecnologías de la Información (PETI), este plan debe tener una vigencia máxima de 6 años.	Líder del proceso	Participantes del proceso
Definir, actualizar y aprobar las políticas internas para garantizar la adecuada operación, control y seguridad de la información.	**P**	Diseñar/actualizar y divulgar el manual de políticas de seguridad de la información, así como, la integridad, disponibilidad, confidencialidad y seguimiento de los servicios de TIC's.	Líder del proceso	Participantes del proceso
laborar el Plan de acción del proceso de tecnologías de la Información	**P**	Elaborar y/o actualizar el Plan de Acción del proceso de Tecnologías de la Información con base en las necesidades corporativas identificadas, definiendo las actividades, responsables, metas e indicadores relacionados con los objetivos corporativos para un periodo de un año, Actividades principales: ✓ Ejecución y monitoreo de proyectos de TI propios y de las áreas. ✓ Plan y ejecución de mantenimiento preventivo de servidores, equipos de cómputo, escáneres, UPS, fibra óptica propia y de terceros.	Líder del proceso	Participantes del proceso

"Este documento es confidencial, puede contener información privilegiada y no puede ser usado ni divulgado por personas distintas a personal de EMSA E.S.P., Está prohibida su retención, copia, grabación, utilización o divulgación con cualquier propósito"

		✓ Arrendamiento de impresoras Operación radioteléfonos Dig. Trunking. Mantenimiento y soporte de licencias de ofimática, ERP, SCADA y sistemas de información técnica.		
Identificar y analizar la plataforma y el recurso humano para ejecutar los requerimientos de tecnología informática	P	La decisión de adquirir o desarrollar con recursos propios un requerimiento de tecnología debe ser responsabilidad del dueño del proceso.	Líder del proceso	Participantes del proceso
		La decisión de adquisición o desarrollo de tecnología debe estar soportada por un estudio de factibilidad y mercadeo.	Líder del proceso	Participantes del proceso
Administrar las BD, controlar y mantener cuentas y permisos de usuarios	H	Cualquier creación, permiso, cambio, actualización, mantenimiento, eliminación en la base de datos debe estar soportada por oficio y realizada únicamente por el administrador de la base de datos.	Líder del proceso	Participantes del proceso
		Se debe realizar por solicitud en escrito o vía e-mail, de parte de los dueños de procesos y se les asigna el nombre y se crean en la base de datos correspondiente.	Líder del proceso	Participantes del proceso
		Se debe asignar únicamente a los usuarios del sistema comercial y el financiero y la solicitud debe ser por el dueño del proceso y se lleva a cabo por escrito o copia del correo electrónico.	Líder del proceso	Participantes del proceso

"Este documento es confidencial, puede contener información privilegiada y no puede ser usado ni divulgado por personas distintas a personal de EMSA E.S.P., Está prohibida su retención, copia, grabación, utilización o divulgación con cualquier propósito"

		Se debe mantener el buen funcionamiento de las BD cuando se presenta algún error en algún proceso sobre la BD que la bloquee, se debe identificar el error o el proceso que está interfiriendo con el normal funcionamiento de la BD al igual se debe revisar el espacio de almacenamiento con que cuenta cada BD y si es necesario reubicar archivos o solicitar discos nuevos, si no se puede efectuar estas actividades se borra información no necesaria de las BD.	Líder del proceso	Participantes del proceso
Administrar la red LAN y WAN	**H**	Para crear usuarios de red, correo, acceso internet administración, intranet y aplicativos, debe realizarse por oficio y validación del dueño del proceso que lo solicita.	Líder del proceso	Participantes del proceso
		Se debe verificar diariamente el comportamiento de la red y la comunicación remota.		
		La asignación de perfiles y el monitoreo debe realizarlo el administrador de la DBA.		
Administrar la red LAN y WAN	**H**	Ningún periférico ni software debe ser instalado o estar en funcionamiento si no es propiedad o está licenciado.	Líder del proceso	Participantes del proceso
		La administración y monitoreo de la infraestructura tecnológica será realizada por asistentes y analistas.		
		La infraestructura tecnológica debe ser rastreada diariamente.		

"Este documento es confidencial, puede contener información privilegiada y no puede ser usado ni divulgado por personas distintas a personal de EMSA E.S.P., Está prohibida su retención, copia, grabación, utilización o divulgación con cualquier propósito"

		Los casos reportados se elevarán única y exclusivamente por medio de la mesa de ayuda (plataforma GLPI) y serán atendidos según la categoría asignada y el ANS específico, para los requerimientos de ingreso, modificación o retiro de usuarios se debe diligenciar y anexar el formato Administración y gestión de usuarios FO-GSO-TI-06.	Líder y Analistas de TIC	Participantes del proceso
Registrar novedades de los componentes de TI	H	Todo hardware y software debe tener su documentación, historial.	Líder del proceso	Participantes del proceso
		El inventario de hardware y software debe permanecer actualizado por cualquier novedad o requerimiento realizado a la oficina de tecnología de información (Help Desk).		
		A todo ajuste de la topología de la intranet debe ser actualizado el plano de puntos.		
Actualizar y definir objetivos y alcances de los requerimientos	H	El estudio de requerimientos funcionales de un aplicativo y el análisis de efectividad debe ser responsabilidad del dueño del proceso y validado por el dueño del proceso que realizo la solicitud.	Líder del proceso	Participantes del proceso
Actualizar el portal de la Web	H	La actualización y generación de enlaces en la página web de la EMSA debe ser realizada por el administrador de Red.	Líder del proceso	Participantes del proceso
		Todo requerimiento efectuado para actualizar o incluir información en la Web debe ser soportada mediante oficio del dueño del proceso.	Líder del proceso	Participantes del proceso

"Este documento es confidencial, puede contener información privilegiada y no puede ser usado ni divulgado por personas distintas a personal de EMSA E.S.P., Está prohibida su retención, copia, grabación, utilización o divulgación con cualquier propósito"

Realizar copias de seguridad	H	Las copias de seguridad se deben realizar diariamente de manera incremental y semanalmente backup completo a las bases de datos de los sistemas de información y a las carpetas de red, estas son ejecutadas por el DBA según el Procedimiento Copias de Seguridad.pdf PR-GSO-TI-01, y registradas en Bitacora ejec. Procesos Backup de FO-GSO-TI-04.	Analista coordinador DBA	Participantes del proceso
		Los usuarios de TI, deben realizar semanalmente el respaldo y verificación de los documentos almacenados en la carpeta establecida en su estación de trabajo a través del agente de copia en la nube (onedrive); según lo establece el Procedimiento Copias de Seguridad PR-GSO-TI-01.	Participantes del proceso	Todos los usuarios de TI
Verificar y actualizar las cuentas de usuarios de SAP y SIEC	V A	Con una periodicidad de 3 meses se ejecutará el procedimiento de chequeo y actualización de cuentas de usuario para el ERP SAP y el sistema de información comercial SIEC, con el objeto de controlar accesos no autorizados por funcionarios retirados, trasladados o con conflictos de segregación de funciones en estos sistemas críticos de EMSA.	Analistas III de TIC	Todos los usuarios de SAP y SIEC
Verificar y actualizar los privilegios de las cuentas de usuarios con permisos de administrador	V A	Con una periodicidad de 3 meses se ejecutará la verificación de excepciones en las de cuentas de usuario que por su trabajo diario requieran permisos de administrador sobre el equipo de cómputo en el dominio de EMSA, con este reporte se ejecutará la actualización en el DA de cada cambio de privilegios por usuario a que haya lugar.	Analista coordinador de TIC	Todos los usuarios pertenecientes al dominio EMSA.local

"Este documento es confidencial, puede contener información privilegiada y no puede ser usado ni divulgado por personas distintas a personal de EMSA E.S.P., Está prohibida su retención, copia, grabación, utilización o divulgación con cualquier propósito"

11. REGISTROS

ITEM	FORMATOS
01	FO-GSO-TI-01 Control de acceso y funcionamiento datacenter.
02	FO-GSO-TI-02 Bitácora servidores.
03	FO-GSO-TI-03 Bitácora funcionamiento diario de los sistemas.
04	FO-GSO-TI-04 Bitácora ejecución de procesos de Backup.
05	FO-GSO-TI-05 Bitácora funcionamiento diario de telecomunicaciones.
06	FO-GSO-TI-06 Administración de usuarios.

12. CONTROL DE CAMBIOS

VERSION	FECHA	MODIFICACIÓN
01	10/11/2023	• Definición de nuevo documento.
02	12/02/2024	• Se modifica el lineamiento para la gestión vulnerabilidades toda vez que se establece la periodicidad de ejecutar este análisis cada 2 años por parte de control interno y TIC de forma intercalada.

"Este documento es confidencial, puede contener información privilegiada y no puede ser usado ni divulgado por personas distintas a personal de EMSA E.S.P., Está prohibida su retención, copia, grabación, utilización o divulgación con cualquier propósito"

"Este documento es confidencial, puede contener información privilegiada y no puede ser usado ni divulgado por personas distintas a personal de EMSA E.S.P., Está prohibida su retención, copia, grabación, utilización o divulgación con cualquier propósito"