# POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE EMAPE S.A.

## INDICE

## 1. Titulo

La presente se denominada "**Política de Seguridad de la Información DE EMAPE S.A"**

## 2. OBJETIVO

Establecer los principios que regulan la Política de Seguridad de la Información en EMAPE S.A. y presentar en forma clara y coherente los elementos que conforman esta política que deben conocer, acatar y cumplir todos los colaboradores y funcionarios.
Esta Política de Seguridad será mantenida, actualizada y adecuada a los fines de la organización.
Los tres principios claves del SGSI, que deben respetarse, en base a las dimensiones básicas de la seguridad, son los siguientes:

- **Confidencialidad**: Propiedad por la cual únicamente puede acceder a la información gestionada por EMAPE S.A.
- **Integridad**: propiedad que garantiza la validez, exactitud y completitud de la información gestionada por EMAPE S.A.
- **Disponibilidad**: propiedad de ser accesible y utilizable en los intervalos acordados. La información gestionada por EMAPE S.A. es accesible y utilizable por los usuarios.

## 3. ALCANCE

La Seguridad de la Información es aplicable a todo el personal de las oficinas y gerencias de la empresa de EMAPE S.A., para conseguir un adecuado nivel de protección de la Gestión de Seguridad de la Información.
Este documento se desarrolla con los requisitos exigidos por la Norma ISO/IEC 27001:2013.

## 4. BASES LEGALES

- Ley N° 29733, sobre Protección de Datos Personales y su Reglamento.
- Decreto Supremo N° 043-2003-PCM, Aprueba Texto Único Ordenado de la Ley N° 27806, Ley de Transparencia y Acceso a la Información Pública.
- Resolución Ministerial N° 004-2016-PCM Aprueban el uso obligatorio de la Norma Técnica Peruana ISO/IEC 27001:2013. Sistemas de Gestión de Seguridad de la Información.
- Resolución Ministerial N9246-2007-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana ISO/IEC 17799:2007 Código de buenas prácticas para la gestión de la seguridad de la información.
- Resolución de Gerencia General N°000129-2021-EMAPE/GG, que aprueba la modificación del Reglamento de Organización y Funciones de EMAPE S.A.

## 5. TERMINOS Y DEFINICIONES

- **Acceso**. - es la recuperación o grabación de datos que han sido almacenados en un sistema de computación.
- **Amenaza**. - cualquier cosa que pueda interferir con el funcionamiento adecuado de una computadora personal.
- **Ataque**. - término general usado para cualquier acción o evento que intente interferir con el funcionamiento adecuado de un sistema informático.
- **Ataque Activo**. - acción iniciada por una persona que amenaza con interferir el funcionamiento adecuado de una computadora.
- **Ataque Pasivo**. - intento de obtener información o recursos de una computadora personal sin interferir con su funcionamiento.
- **Base de Datos**. - una base de datos es un conjunto de datos organizados, entre los cuales existe una correlación y que, además están almacenados con criterios independientes de los programas que los utilizan.
- **Datos**. - los datos son hechos y cifras que al ser procesados constituyen una información.
- **Golpe (Breach)**. - es una violación con éxito de las medidas de seguridad.
- **Incidente**. - cuando se produce un ataque o se materializa una amenaza.
- **Integridad**. - se refiere a que los valores de los datos se mantengan tal como fueron puestos intencionalmente en un sistema.
- **Privacidad**. - se define como el derecho que tienen los individuos y organizaciones para determinar, ellos mismos, a quién, cuándo y qué información referente a ellos serán difundidos o transmitidos a otros.
- **Seguridad**. - se refiere a las medidas tomadas con la finalidad de preservar los datos o información que en forma no autorizada.
- **Acción correctiva**. - acción tomada para eliminar las causas de una no conformidad detectada u otra situación indeseable.
- **Acción preventiva**. - Disposición de operaciones que buscan de forma preliminar, que no se presente en su ejecución, desarrollo e implementación una no conformidad.
- **Aceptación del Riesgo**. - Después de revisar las consecuencias que puede acarrear el riesgo, se toma la decisión de afrontarlo.
- **Activo**. - Cualquier cosa que tiene valor para la empresa, Se pueden clasificar de la siguiente manera:

    - ✓ **Aplicaciones**: Es todo el software que se utiliza para la gestión de la información.
    - ✓ **Personal**: Es todo el colaborador o personal de planta de la empresa, que tengan acceso de una manera u otra a los activos de información en la empresa.
    - ✓ **Servicios**: Son tanto los servicios internos, aquellos que una parte de la empresa suministra a otra, como los externos.
    - ✓ **Tecnología**: Son todos los equipos utilizados para gestionar la información y las comunicaciones.

- ✓ **Instalaciones**: Son todos los lugares en los que se alojan los sistemas de información.
- ✓ **Equipamiento auxiliar**: Son todos aquellos activos que dan soporte a los sistemas de información y que no se hallan en ninguno de los tipos anteriormente definidos. Ejemplo: Aire acondicionado, UPS, entre otros.
- ✓ **Administración de riesgos**: Gestión de riesgos, es un enfoque estructurado para manejar la incertidumbre relativa a una amenaza.
- ✓ **Administración de incidentes de seguridad**: Procedimientos, estrategias y herramientas de control, enfocados a una correcta evaluación de las amenazas existentes, en este caso hacia toda la infraestructura de TI.

- **Alerta**. - Una notificación formal de que se ha producido un incidente relacionado con la Seguridad de la Información que puede evolucionar hasta convertirse en desastre.
- **Análisis de riesgos**. - Uso sistemático de la información para identificar fuentes y estimar el riesgo.
- **Auditabilidad**. - Los activos de información deben tener controles que permitan su revisión. Permitir la reconstrucción, revisión y análisis de la secuencia de eventos.
- **Auditor**. - Persona encargada de verificar, de manera independiente, la calidad e integridad del trabajo que se ha realizado en un área particular.
- **Auditoria**. - Proceso planificado y sistemático en el cual un auditor obtiene evidencias objetivas que le permitan emitir un juicio.
- **Autenticidad**. - Proceso que tiene por objetivo asegurar la identificación de una persona o sistema
- **Confiabilidad**. - Se puede definir como la capacidad de un producto de realizar su función de la manera prevista
- **Confidencialidad**. - Acceso a la información por parte únicamente de quienes esté autorizados
- **Control**. - son todas aquellas políticas, procedimientos, prácticas y las estructuras organizativas concebidas para mantener los riesgos de Seguridad de la Información.
- **Evaluación de riesgos**. - proceso de comparar el riesgo estimado contra un criterio de riesgo dado con el objeto de determinar la importancia del riesgo.
- **Evento**. - Suceso identificado en un sistema, servicio o estado de la red que indica una posible brecha en la política de Seguridad de la Información.
- **ISO 27001**. - Estándar para sistemas de gestión de la Seguridad de la Información
- **ISO 27002**. - Código de buenas prácticas en gestión de la Seguridad de la Información.
- **No conformidad grave**. - Ausencia o fallo de uno o varios requerimientos de la ISO 27001.
- **Phishing**. - Tipo de delito encuadrado dentro del ámbito de las estafas.

## 6. GESTION DE RIESGOS

La gestión de la Seguridad de la Información en EMAPE S.A. está basada en el riesgo, de conformidad con la Norma internacional ISO/IEC 27001:2013.

Se articula mediante un proceso general de apreciación y tratamiento del riesgo, que potencialmente pueden afectar a la seguridad de la información de los servicios prestados, consistente en:

- Identificar las amenazas, que aprovecharán vulnerabilidades de los Sistemas de Información que soportan, o de los que depende, la seguridad de la información.
- Analizar el riesgo, en base a la consecuencia de materializarse la amenaza y de la probabilidad de ocurrencia.
- Evaluar el riesgo, según un nivel previamente establecido y aprobado de riesgo ampliamente aceptable, tolerable e inaceptable.
- Tratar el riesgo inaceptable, mediante los controles o salvaguardas adecuadas.

Dicho proceso es cíclico y debe llevarse a cabo de forma periódica, como mínimo una vez al año. Para cada riesgo identificado se asignará un propietario, pudiendo recaer múltiples responsabilidades en una misma persona o comité.

## 7. POLÍTICAS, PROCEDIMIENTOS Y CONTROLES

### 7.1 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

#### 7.1.1 POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

De acuerdo a lo mencionado del Riesgos en el punto anterior, se establece que la información es vital para el desarrollo de las actividades de la empresa, de gran importancia para la toma de decisiones, por lo cual preservar los activos de información, su confidencialidad, integridad, disponibilidad, y la continuidad de las operaciones, la administración y/o gestión de riesgos, la creación de cultura y conciencia de seguridad en los usuarios que hagan uso de los activos de información son prioridades en la empresa estableciendo políticas de seguridad tomando como base que la efectividad de estas políticas depende finalmente del comportamiento de los usuarios, (por lo que saben, lo que sienten y de que estén dispuestos a realizar).

Para garantizar la continuidad del negocio y las operaciones de la empresa sobre estos análisis pueden revisarse el documento de gestión de sistemas Plan de Contingencia.

**Objetivo**: Definir las pautas para asegurar una adecuada protección y Seguridad de la Información en EMAPE S.A., de los Sistemas y Tecnología de

la Información, estableciéndose dentro del plan estratégico de sistemas y las desarrollará con los recursos asignados.

**Aplicabilidad**: Estas políticas aplican a la Alta Dirección, Gerencia General, Asesores, funcionarios, jefes de Oficina, y todo usuario de la empresa que permita el cumplimiento de los propósitos generales.

**Directrices**:

**I.** Se debe verificar que se definan, implementen, revisen y actualicen las Políticas de Seguridad de la Información.

**II.** Se debe establecer un programa que permita el fomento continuo de la creación de cultura y conciencia de Seguridad de la Información en los funcionarios, y usuarios de los sistemas de información y telecomunicaciones en EMAPE S.A

**III.** Todos los usuarios de las Unidades Orgánicas y que utilicen los sistemas de información y telecomunicaciones en EMAPE S.A., tienen la responsabilidad y obligación de cumplir con las políticas, normas, procedimientos y buenas prácticas establecidas en la presente Política de Seguridad de la Información.

**IV.** Todas las compras de equipos tecnológicos como computadoras, impresoras, cámaras de seguridad, servidores, discos duros y demás dispositivos y componentes informáticos que se realicen en EMAPE S.A., previamente debe tener un informe de aprobación con las especificaciones técnicas de la Gerencia de Sistemas de Información.

**V.** Todo aplicativo informático o software que sea diseñado, desarrollado o que se busque de adquirir de terceros e implementar en EMAPE S.A. debe tener aprobación y conformidad técnica de la Gerencia de Tecnologías de la Información

**VI.** La empresa debe contar con un firewall o dispositivo de seguridad perimetral para la conexión a Internet.

**VII.** La conexión remota a la red de área local en EMAPE S.A. con las otras sucursales, debe realizarse a través de una conexión VPN segura suministrada por la entidad, la cual debe ser aprobada, registrada y auditada, por la Gerencia de tecnologías de la Información

**VIII.** Los funcionarios o jefes de área deben asegurarse que todos los procedimientos de Seguridad de la Información dentro de su área se realicen correctamente para lograr el cumplimiento de las políticas y estándares de Seguridad de la Información. EMAPE S.A.

### 7.1.2 POLÍTICA DE ESTRUCTURA ORGANIZACIONAL DE SEGURIDAD DE LA INFORMACIÓN

La Gerencia de Tecnologías de la Información creará 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.

**Objetivo**: Definir el programa de Seguridad de la Información con la Gerencia Central de Administración y Finanzas donde se describan roles y responsabilidades para operación, gestión y administración de la protección de la Información.

**Aplicabilidad**: Estas políticas aplican a la Alta Dirección, Gerencia General, Asesores, funcionarios, jefes de Oficina, y todo usuario de la empresa que permita el cumplimiento de los propósitos generales.

**Directrices:**

**I.** Crear el Comité de Seguridad de la Información, y asignar el rol de Oficial de Seguridad de la Información y su equipo de apoyo, junto con los roles, funciones y responsabilidades respectivamente.

**II.** La Gerencia de Sistemas de Información debe establecer los roles, funciones y responsabilidades de operación y administración de los sistemas de información, estos roles, funciones y responsabilidades, deberán estar debidamente documentadas y distribuidas.

**III.** El Comité de Seguridad de la Información reportará los incidentes de seguridad al Gerente General de EMAPE S.A. permitiendo apoyar la gestión de incidentes de seguridad y la planificación de contingencias.

**IV.** La Gerencia de Tecnologías de la Información asistirá a foros, conversatorios, conferencias de interés especial en Seguridad de la Información.

**V.** Los proyectos desarrollados por la Gerencia de Tecnologías de la Información deberán incorporar dentro de la planeación y desarrollo, el cumplimiento de la política de Seguridad de la Información, valoración de riesgos y los controles a estos.

### 7.1.3 POLÍTICA PARA USO DE DISPOSITIVOS MÓVILES

**Objetivo**: Establecer las directrices de uso y manejo de dispositivos móviles (teléfonos móviles, teléfonos inteligentes, tabletas, entre otros), suministrados por la empresa y personales que hagan uso de los servicios de información y red en EMAPE S.A.

**Aplicabilidad**: Estas políticas aplican a la Alta Dirección, Gerencia General, Asesores, funcionarios, jefes de Oficina, y todo usuario de la empresa que permita el cumplimiento de los propósitos generales.

**Directrices**:

I. Los dispositivos móviles (teléfonos móviles, teléfonos inteligentes (smart phones) tabletas, entre otros), son herramientas de trabajo que se deben utilizar únicamente para facilitar las comunicaciones de los usuarios de la empresa.

II. Los dispositivos móviles asignados por la empresa deben tener la configuración realizada por la Gerencia de Tecnologías de la Información, así mismo tener configurado la cuenta de correo electrónico asignado al usuario por la empresa.

III. Para que los usuarios de dispositivos móviles institucionales y usuarios autorizados se conecten a la red WiFi de la empresa deben entregar el numero MAC del celular.

IV. En el caso del nivel directivo o funcionarios se autoriza el uso de WhatsApp únicamente en dispositivos suministrados por la empresa, no se permite por esta aplicación se transfiera información pública reservada o información pública clasificada con fines personales, salvo que se solicite la autorización por correo electrónico a la Gerencia de Tecnologías de la Información.

V. Los dispositivos móviles deben tener contraseña de ingreso y bloqueo del equipo de manera automática.

VI. Los dispositivos móviles institucionales 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 entidad. Ante la pérdida del equipo, ya sea por extravío o hurto, deberá informar de manera inmediata a la Gerencia de Tecnologías de la Información.

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

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

IX. En caso de requerir instalación de aplicaciones adicionales en el dispositivo móvil institucional se debe solicitar mediante solicitud a la Gerencia de Tecnologías de la Información para su aprobación.

### 7.1.4 POLÍTICA DE SEGURIDAD PARA LOS ACTIVOS DE LA INFORMACIÓN

**Objetivo**: Establecer la forma en que se logra y mantener la protección adecuada de los activos de información.

**Aplicabilidad**: Estas políticas aplican a la Alta Dirección, Gerencia General, Asesores, funcionarios, jefes de Oficina, y todo usuario de la empresa que permita el cumplimiento de los propósitos generales.

**Directrices**:

- Inventario de activos informáticos y sistemas:
  La Gerencia de Tecnología de la Información mantendrá un inventario actualizado de sus activos de informática y sistemas, bajo la responsabilidad de cada propietario de información y centralizado por la Gerencia de Tecnologías de la Información.
  El inventario de los activos informáticos debe realizarse 03 veces al año, uno al comienzo, otro a mitad y final de año La información de dicho inventario debe estar confrontado con la base de datos de la Oficina Patrimonial.

- Propietarios de los activos de información:
  EMAPE S.A. es el dueño de la propiedad intelectual de los avances tecnológicos e intelectuales desarrollados por los funcionarios de la empresa, personal, consultores y contratistas, derivadas del objeto del cumplimiento de funciones y/o tareas asignadas, como las necesarias para el cumplimiento del objeto del contrato. EMAPE S.A. es propietario de los activos de información y los administradores de estos activos son los funcionarios, o demás colaboradores de la empresa 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)

### 7.1.5 POLÍTICA DE USO DE LOS ACTIVOS

**Objetivo**: Lograr y mantener la protección adecuada de los activos de información mediante la asignación a los usuarios finales que deban administrarlos de acuerdo a sus roles y funciones.

**Aplicabilidad:** Estas políticas aplican a la Alta Dirección, Gerencia General, Asesores, funcionarios, jefes de Oficina, y todo usuario de la empresa que permita el cumplimiento de los propósitos generales.

**Directrices:**

**I.** Los activos de información pertenecen a EMAPE S.A. y el uso de los mismos debe emplearse exclusivamente con propósitos laborales.

**II.** Los usuarios deberán utilizar únicamente los programas y equipos autorizados por la Gerencia de Tecnologías de la Información.

**III.** La Gerencia de Tecnologías de la Información proporcionará al usuario, la solicitud debe hacerla por el módulo de Mesa de Servicio, los equipos informáticos y los programas instalados en ellos; los datos/información creados, almacenados y recibidos, serán propiedad de EMAPE S.A.

**IV.** Periódicamente, la Gerencia 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 considera como una violación a las Políticas de Seguridad de la Información de EMAPE S.A.

**V.** Todos los requerimientos de aplicativos, sistemas y equipos informáticos deben ser solicitados por el funcionario o jefe de la dependencia a través del módulo de Mesa de Servicio.

**VI.** Los usuarios no deben realizar intencionalmente actos que impliquen un mal uso de los recursos 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, mal uso del correo electrónico, practica de juegos en línea, uso permanente de redes sociales personales, conexión de periféricos o equipos que causen molestia a compañeros de trabajo, etc.

**VII.** Los usuarios no podrán efectuar ninguna de las siguientes labores sin previa autorización de la Gerencia de Tecnologías de la Información.

- Bajar o descargar software de Internet u otro servicio en línea en cualquier equipo de la empresa.
- Modificar, revisar, transformar o adaptar cualquier software propiedad de la empresa.
- Cambiar la configuración de hardware de propiedad de la empresa.

**VIII.** El usuario será responsable de todas las transacciones o acciones efectuadas con su "cuenta de usuario".

**IX.** Ningún usuario deberá acceder a la red o a los servicios informáticos de EMAPE S.A. utilizando una cuenta de usuario o clave de otro usuario.

**X.** La Gerencia de Tecnologías de la Información, es la gerencia responsable de realizar el aseguramiento de los accesos a internet.

**XI.** Todo archivo o material descargado o recibido a través de medio magnético/electrónico o descarga de Internet o de cualquier red externa, deberá ser revisado para detección de virus y otros programas maliciosos antes de ser instalados en la infraestructura informática de la empresa.

**XII.** Todo cambio a la infraestructura informática deberá estar controlado y será realizado mediante solicitud a la Gerencia de Tecnologías de la Información.

**XIII.** Los funcionarios deberán realizar la devolución de todos los activos físicos y/o electrónicos asignados por la empresa en el proceso de desvinculación, de igual manera deberán documentar y entregar los conocimientos importantes que posee de la labor que ejecutan.

### 7.1.6 POLÍTICA DE SEGURIDAD DE LOS ACTIVOS DE INFORMACIÓN

**Objetivo**: Garantizar que la seguridad es parte integral de los activos de información y la correcta utilización por los usuarios finales.

**Aplicabilidad**: Estas políticas aplican a la Alta Dirección, Gerencia General, Asesores, funcionarios, jefes de Oficina, y todo usuario de la empresa que permita el cumplimiento de los propósitos generales.

**Directrices:**

I. La instalación de software en los computadores suministrados por EMAPE S.A. es una función exclusiva de la Gerencia de Tecnología de la Información el cual mantendrá una lista actualizada del software autorizado para instalar en los computadores.
II. En el Disco C:\de las estaciones cliente se tiene configurado el sistema operativo, aplicaciones y perfil de usuario. El usuario deberá abstenerse de realizar modificaciones a estos archivos.
III. En el Disco D:\los usuarios deberán trabajar todos sus documentos institucionales.
IV. El préstamo de equipos de cómputo, computadores portátiles y vídeo proyectores se debe tramitar a través de la Mesa de Servicio con anticipación y se proveerá de acuerdo a la disponibilidad.
V. Los equipos que ingresan temporalmente a EMAPE S.A. que son de propiedad de terceros: deben ser registrados en los controles de acceso de la entidad para poder realizar su retiro; posteriormente la empresa 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.
VI. La Gerencia de Tecnologías de la Información no prestará servicio de soporte técnico (revisión, mantenimiento, reparación, configuración y manejo e información) a equipos que no sean de la empresa.

### 7.1.7 POLÍTICA NAVEGACIÓN SEGURA

**Objetivo**: Establecer 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.

**Aplicabilidad**: Estas políticas aplican a la Alta Dirección, Gerencia General, Asesores, funcionarios, jefes de Oficina, y todo usuario de la empresa que permita el cumplimiento de los propósitos generales.

**Directrices**:

I. La infraestructura, servicios y tecnologías usados para acceder a internet son propiedad de EMAPE S.A., por lo tanto, se reserva el

derecho de monitorear el tráfico de internet y el acceso la información, solo la de la Gerencia de Tecnología de la Información.

II. La navegación en Internet debe realizarse de forma razonable y con propósitos laborales.

III. No se permite la navegación a sitios con contenidos contrarios a la ley o a las políticas de EMAPE S.A. o que representen peligro para la entidad como: pornografía, terrorismo, segregación racial u otras fuentes definidas por la empresa. El acceso a este tipo de contenidos con propósitos de estudio de seguridad o de investigación, debe contar con la autorización del Jefe o Gerente de la dependencia solicitante hacia la Gerencia de Sistemas de Información

IV. La Gerencia de Sistemas de Información administrará la autorización de navegación a los usuarios de EMAPE S.A., previa solicitud del Gerente o Jefe de la Unidad Orgánica a través de la Mesa de Servicio.

V. La Gerencia de Sistemas de Información implementara herramientas para evitar la descarga de software no autorizado y/o código malicioso en los equipos institucionales.

### 7.1.8 POLÍTICA DE CLASIFICACIÓN DE LA INFORMACIÓN

**Objetivo**: Asegurar que la información recibe el nivel de protección apropiado de acuerdo al tipo de clasificación establecido por la ley.

**Aplicabilidad**: Estas políticas aplican a la Alta Dirección, Gerencia General, Asesores, funcionarios, jefes de Oficina, y todo usuario de la empresa que permita el cumplimiento de los propósitos generales.

**Directrices**:

**I.** 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 la empresa 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.

**II.** Los usuarios responsables de la información en EMAPE S.A., 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.

**III.** 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 la empresa.

### 7.1.9 POLÍTICA DE MANEJO DISPOSICIÓN DE INFORMACIÓN, MEDIOS Y EQUIPOS

**Objetivo**: Contrarrestar las interrupciones en las actividades de EMAPE S.A., proteger sus procesos críticos contra los efectos de fallas importantes en los sistemas de información o contra desastres para su recuperación oportuna, permitiendo la confidencialidad, integridad y disponibilidad de la información.

**Aplicabilidad**: Estas políticas aplican a la Alta Dirección, Gerencia General, Asesores, funcionarios, jefes de Oficina, y todo usuario de la empresa que permita el cumplimiento de los propósitos generales.

**Directrices**:

**I.** 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.

**II.** Está restringido del uso de medios removibles de almacenamiento, por lo cual se deshabilita la funcionalidad de los puertos 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 un correo electrónico a la mesa de servicio con copia a la Gerencia de Tecnologías de la Información especificando la utilización de dichos medio removibles en las Unidades Orgánicas.

### 7.1.10 POLÍTICA DE CONTROL DE ACCESO

**Objetivo**: Definir las pautas generales para asegurar un acceso controlado, físico o lógico, a la información de la plataforma informática de EMAPE S.A., así como el uso de medios de computación móvil.

Aplicabilidad: Estas políticas aplican a la Alta Dirección, Gerencia General, Asesores, funcionarios, jefes de Oficina, y todo usuario de la empresa que permita el cumplimiento de los propósitos generales.

**Directrices**:

**I.** La Gerencia de Tecnologías de la Información establecerá el procedimiento para establecer los niveles de acceso para usuarios de los servicios y sistemas de información en EMAPE S.A.

**II.** La Gerencia de Tecnologías de la Información establecerá las configuraciones de las políticas en los sistemas de tecnología y comunicaciones para el control de acceso a los activos de información.

**III.** La Gerencia de Tecnología de la Información suministrará a los usuarios las claves respectivas para el acceso a los servicios de red y sistemas de información.

**IV.** Es responsabilidad del usuario el manejo apropiado a las claves asignadas.

**V.** Todo trabajo a realizarse en los servidores de la empresa con información de la entidad, por parte de sus funcionarios, se debe realizar en las instalaciones, no se podrá realizar ninguna actividad de tipo remoto sin la debida aprobación de la Gerencia de Tecnologías de la Información.

**VI.** La Gerencia de Tecnologías de la Información debe generar el lineamiento para restringir y auditar el acceso a los códigos fuentes de los programas y elementos asociados como (diseños, especificaciones, librerías de fuentes de programas, planes de verificación y planes de validación.

**VII.** Es muy importante que la Gerencia Central de Administración y Finanzas o la Gerencia que corresponda comunique a la Gerencia de Tecnologías de la Información el término del vínculo laboral del trabajador o funcionario de la empresa para inhabilitar los accesos a los diferentes sistemas.

**VIII.** La conexión remota a la red de área local de EMAPE S.A. debe ser hecha a través de una conexión VPN segura suministrada por la entidad, la cual debe ser aprobada y registrada.

### 7.1.11 POLÍTICA DE ESTABLECIMIENTO, USO Y PROTECCIÓN DE CLAVES DE ACCESO

**Objetivo**: Controlar el acceso a la información.

**Aplicabilidad**: Estas políticas aplican a la Alta Dirección, Gerencia General, Asesores, funcionarios, jefes de Oficina, y todo usuario de la empresa que permita el cumplimiento de los propósitos generales.

**Directrices**:

**I.** Se debe concientizar y controlar a los usuarios para que apliquen buenas prácticas de seguridad en la selección, uso y protección de claves o contraseñas,

**II.** Los usuarios son responsables del uso de las claves o contraseñas de acceso que se le asignen para la utilización de los equipos o servicios informáticos de la empresa.

**III.** La clave de acceso será desbloqueada sólo por la Gerencia de Tecnología de la Información, luego de la solicitud formal por parte del responsable de la cuenta con copia al funcionario de su oficina.

### 7.1.12 POLÍTICA DE USO DE DISCOS DE RED O CARPETAS VIRTUALES

**Objetivo**: Asegurar la operación correcta y segura de los discos de red o carpetas virtuales.

**Aplicabilidad**: Estas políticas aplican a la Alta Dirección, Gerencia General, Asesores, funcionarios, jefes de Oficina, y todo usuario de la empresa que permita el cumplimiento de los propósitos generales.

**Directrices**:

**I.** Para que los usuarios tengan acceso a la información ubicada en los discos de red, el Gerente o jefe inmediato deberá enviar un correo autorizando el acceso y permisos, correspondientes al rol y funciones a desempeñar, de la Gerencia de Tecnologías de la Información.

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

**III.** Está prohibido almacenar archivos con contenido que atente contra la moral y las buenas costumbres de la entidad o las personas, como pornografía, propaganda racista, terrorista o cualquier software ilegal o malicioso, ya sea en medios de almacenamiento de estaciones de trabajo, computadores de escritorio o portátiles, tablets, celulares inteligentes, etc.

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

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

**VI.** La responsabilidad de generar las copias de respaldo de la información de los discos de red, está a cargo la Gerencia de Tecnologías de la Información.

### 7.1.13 POLÍTICA DE USO DE PUNTOS DE RED DE DATOS (RED DE ÁREA LOCAL-LAN)

**Objetivo**: Asegurar la operación correcta y segura de los puntos de red.

**Aplicabilidad**: Estas políticas aplican a la Alta Dirección, Gerencia General, Asesores, funcionarios, jefes de Oficina, y todo usuario de la empresa que permita el cumplimiento de los propósitos generales.

**Directrices**:

**I.** Los usuarios deberán emplear los puntos de red, para la conexión de equipos informáticos Institucionales.

**II.** La Gerencia General y Unidades Orgánicas deberán solicitar la opinión técnica de la Gerencia de Tecnologías de la Información para la ubicación óptima de los puntos de red, computadoras, impresoras, entre otros equipos tecnológicos en la construcción de nuevos ambientes, modificación o eliminación.

**III.** Los equipos de uso personal, que no son de propiedad de EMAPE S.A., solo tendrán acceso a servicios limitados destinados a invitados o visitantes, estos equipos deben ser conectados a los puntos de acceso autorizados y definidos por la Gerencia de Tecnologías de la Información.

**IV.** La instalación, activación y gestión de los puntos de red es responsabilidad de la Gerencia de Tecnologías de la Información.

### 7.1.14 POLÍTICA DE USO DE IMPRESORAS Y DEL SERVICIO DE IMPRESIÓN

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

**Aplicabilidad**: Estas políticas aplican a la Alta Dirección, Gerencia General, Asesores, funcionarios, jefes de Oficina, y todo usuario de la empresa que permita el cumplimiento de los propósitos generales.

**Directrices**:

**I.** Los documentos que se impriman en las impresoras de la empresa deben ser de carácter institucional.

**II.** Es responsabilidad del usuario conocer el adecuado manejo de los equipos de impresión (escáner y fotocopiado) para que no se afecte su correcto funcionamiento.

**III.** Ningún usuario debe realizar labores de reparación o mantenimiento de las impresoras. En caso de presentarse alguna falla, esta se debe reportar a la Gerencia de Tecnologías de la Información.

**IV.** 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.

### 7.1.15 POLÍTICA DE SEGURIDAD FÍSICA

**Objetivo**: Implementar el programa de seguridad física para el acceso a las instalaciones, centros de datos y centros de cableado que permita fortalecer la integridad, disponibilidad e integridad la información.

**Aplicabilidad**: Estas políticas aplican a la Alta Dirección, Gerencia General, Asesores, funcionarios, jefes de Oficina, y todo usuario de la empresa que permita el cumplimiento de los propósitos generales.

**Directrices**:

**I.** La Gerencia de Tecnologías de la Información con el apoyo de la Gerencia Central de Administración y Finanzas deberán implementar barreras y sistemas de control de acceso a las instalaciones, centros de datos y centros de cableado de la empresa, así como la asignación de niveles de acceso**.**

**II.** La Gerencia de Tecnologías de la Información deberá implementar alarmas de detección de intrusos a los centros de datos y centros de cableado de la empresa.

**III.** La Gerencia de Tecnologías de la Información 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 la empresa.

**IV.** La Gerencia Central de Administración y Finanzas deberá apoyar a la Gerencia de Tecnologías de la Información para mantener libres los pasadizos de los gabinetes, así como también los ambientes como se indica en las Normas Técnicas de Seguridad Informática.

**V.** La Gerencia de Tecnologías de la Información, deberá implementar protecciones que eviten o mitiguen daños causados por incendios, inundaciones y otros desastres naturales o generados por el hombre a los centros de datos y centros de cableado.

**VI.** No está permitido el uso de equipo fotográfico, de video, de audio u otro dispositivo de grabación de audio o video al interior de los centros de datos y centros de cableados.

### 7.1.16 POLÍTICAS DE SEGURIDAD DEL CENTRO DE DATOS Y CENTROS DE CABLEADO

**Objetivo**: Asegurar la protección de la información en las redes y la protección de la infraestructura de soporte.

**Aplicabilidad**: Estas políticas aplican a los funcionarios, contratistas, colaboradores de la empresa actuales o por ingresar a terceros que estén encargados de cualquier parte o sistema de la plataforma informática.

**Directrices**:

**I.** No se permite el ingreso al centro de datos, al personal que no esté expresamente autorizado. Se debe llevar un control de ingreso y salida del personal que visita el centro de datos. En el centro de datos debe disponerse de una planilla para el registro, la cual debe

ser diligenciada en lapicero de tinta al iniciar y finalizar la actividad a realizar.

**II.** La Gerencia de Tecnologías de la Información debe garantizar que el control de acceso al centro de datos de EMAPE S.A.

**III.** La Gerencia de Tecnologías de la Información deberá garantizar que todos los equipos de los centros de datos cuenten con un sistema alterno de respaldo de energía.

**IV.** En las instalaciones del centro de datos o de los centros de cableado, no se debe fumar, comer o beber; de igual forma se debe eliminar la permanencia de papelería y materiales inflamables o combustibles que generen riesgo de propagación de fuego, así como mantener el orden y limpieza en todos los equipos y elementos que se encuentren en este espacio.

**V.** El centro de datos debe estar provisto de:

- Señalización adecuada de todos y cada uno de los diferentes equipos y elementos, así como luces de emergencia y de evacuación, cumpliendo las normas de seguridad
- Sistema de refrigeración por aire acondicionado de precisión. Este equipo debe ser redundante para que en caso de falla se pueda continuar con la refrigeración.
- Unidades de potencia ininterrumpida UPS, que proporcionen respaldo al mismo, con el fin de garantizar el servicio de energía eléctrica durante una falla momentánea del fluido eléctrico de la red pública.
- Alarmas de detección de humo y sistemas automáticos de extinción de fuego, conectada a un sistema central. Los detectores deberán ser probados de acuerdo a las recomendaciones del fabricante o al menos una vez cada 6 meses.
- Extintores de incendios o un sistema contra incendios debidamente probados y con la capacidad de detener el fuego generado por equipo eléctrico, papel o químicos especiales.

**VI.** El cableado de la red debe ser protegido de interferencias por ejemplo usando canaletas que lo protejan.

**VII.** Las actividades de soporte y mantenimiento dentro del centro de datos siempre deben ser supervisadas por personal de la Gerencia de Tecnología de la Información

**VIII.** Las puertas del centro de datos deben permanecer cerradas. Si por alguna circunstancia se requiere ingresar y salir del centro de datos, el personal responsable de la actividad se ubicará dentro del centro de datos.

**IX.** Cuando se requiera realizar alguna actividad sobre algún armario (rack), este debe quedar ordenado, cerrado y con llave, cuando se finalice la actividad.

**X.** Los equipos del centro de datos que lo requieran, deben estar monitoreados para poder detectar las fallas que se puedan presentar.

### 7.1.17 POLÍTICAS DE SEGURIDAD DE LOS EQUIPOS

**Objetivo**: Asegurar la protección de la información en los equipos.

**Aplicabilidad**: Estas políticas aplican a los funcionarios, contratistas, colaboradores de la empresa actuales o por ingresar y a terceros que estén encargados de cualquier parte o sistema de la plataforma informática.

**Directrices:**

**I.** Instalación de equipos de procesamiento y almacenamiento

- Los equipos de procesamiento y almacenamiento deben ser instalados en las áreas de trabajo seguras definidas por la Gerencia de Tecnologías de la Información.

**II.** 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.
- La Gerencia de Tecnologías de la Información establecerá un programa de revisiones y/o inspecciones físicas al cableado, con el fin de detectar dispositivos no autorizados.

**III.** Mantenimiento de los Equipos

- 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 realizadas y programadas.
- 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 entidad.
- 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 la empresa debe cumplir con la política de control acceso.

- Cuando un dispositivo vaya a ser reasignado o retirado de servicio debe contar con aprobación de la Gerencia de Sistemas 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.

**IV.** Normas de protección

- Los funcionarios que hagan uso de los equipos de EMAPE S.A., 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.

### 7.1.18 POLÍTICA DE SEGURIDAD DE LAS OPERACIONES DE TIC.

**Objetivo**: Definir las reglas para asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de la empresa, con el fin de robustecer la continuidad de los sistemas de información y comunicación.

**Aplicabilidad**: Estas políticas aplican a los funcionarios, contratistas, colaboradores de la empresa actuales o por ingresar y a terceros que estén encargados de cualquier parte o sistema de la plataforma informática.

**Directrices**:

**I.** La Gerencia de Tecnologías de la Información debe elaborar las guías de operación de todos los activos de información, así mismo dejarlas a disposición de los usuarios que los requiera.

**II.** La Gerencia de Tecnologías de la Información debe generar un programa de seguimiento a la gestión de capacidad de los recursos de red de sistemas de información y comunicaciones.

**III.** La Gerencia de Tecnologías de la Información debe implementar el procedimiento para la realización de auditorías técnicas a los sistemas operativos de la empresa, las cuales se deben realizar periódicamente.

### 7.1.19 POLÍTICA DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

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

**Aplicabilidad**: Estas políticas aplican a los funcionarios, contratistas, colaboradores de la empresa actuales y a terceros que estén encargados de cualquier parte o sistema de la plataforma informática.

**Directrices**:

- **I.** Asegurar que los sistemas de información o aplicativos informáticos incluyen controles de seguridad y cumplen con las políticas de Seguridad de la Información.
- **II.** En caso de desarrollos propios de la Gerencia de Sistemas de Información debe separar los ambientes de desarrollo, prueba y producción, en diferentes procesadores y dominios.
- **III.** La Gerencia de Sistemas de Información deberá realizar pruebas de funcionamiento y de seguridad a los nuevos sistemas, actualizaciones y/o aplicaciones en ambiente de pruebas, para validar la necesidad y operatividad de estos, previo a la aprobación e implementación.
- **IV.** Se debe verificar que los desarrollos de la entidad estén completamente documentados, igualmente todas las versiones de los desarrollos se deben preservar adecuadamente en varios medios y guardar copia de respaldo externa a la entidad.
- **V.** Desarrollar estrategias para analizar la seguridad en los sistemas de información, como no usar datos sensibles en ambientes de prueba y usar diferentes perfiles para pruebas y producción.
- **VI.** Todo nuevo hardware y software que se vaya a adquirir y conectar a la plataforma tecnológica de EMAPE S.A., por cualquier dependencia o proyecto, deberá ser gestionado por la Gerencia de Sistemas de Información para su correcto funcionamiento.
- **VII.** La Gerencia de Sistemas de Información será la única dependencia autorizada para realizar copia de seguridad del software original.
- **VIII.** La instalación del software en los activos informáticos de la empresa, se realizará únicamente a través de la Gerencia de Tecnologías de la Información.
- **IX.** La Gerencia de Tecnologías de la Información debe implementar actividades para la protección contra códigos maliciosos y de reparación.

### 7.1.20 POLÍTICA DE RESPALDO Y RESTAURACIÓN DE INFORMACIÓN

**Objetivo**: Proporcionar medios de respaldo adecuados para asegurar que toda la información esencial y el software, se pueda recuperar después de una falla.

**Aplicabilidad**: Estas políticas aplican a los funcionarios, contratistas, colaboradores de la empresa actuales o por ingresar y a terceros que estén encargados de cualquier parte o sistema de la plataforma informática.

**Directrices**:

- **I.** Las copias de respaldo se guardarán únicamente con el objetivo de restaurar el sistema luego de la infección de un virus informático,
- **II.** Las copias de respaldo se guardarán únicamente con el objetivo de restaurar el sistema luego de la infección de un virus informático, defectos en los discos de almacenamiento, problemas de los servidores o computadores, materialización de amenazas, catástrofes y por requerimiento legal.
- **III.** La restauración de copias de respaldo en ambientes de producción debe estar debidamente aprobada por el propietario de la información.
- **IV.** Semanalmente el administrador de infraestructura, verificará la correcta ejecución de los procesos de backup. (Dependiendo de la disponibilidad del servidor)
- **V.** La Gerencia de Tecnologías de la Información debe mantener un inventario actualizado de las copias de respaldo de la información y los aplicativos o sistemas de la empresa.
- **VI.** Es responsabilidad de cada dependencia mantener depurada la información de las carpetas para la optimización del uso de los recursos de almacenamiento que entrega la empresa a los usuarios.

### 7.1.21 POLÍTICA DE GESTIÓN DE CENTRALIZADA PROTECCIÓN DE RED

**0bjetivo**: Analizar los riesgos existentes relacionados a la presencia de virus informático y establecer las acciones necesarias para su reducción o eliminación.

**Aplicabilidad**: Estas políticas aplican a los funcionarios, colaboradores y usuarios de la empresa que hagan uso de la red y equipos de cómputo de la empresa con la supervisión de la Gerencia de Tecnología de la Información.

**Directrices**

- **I.** La Gerencia de Tecnologías de la Información, deberán desarrollar una "Directiva de seguridad ante la presencia de virus informático", incluyendo en estos lineamientos para poder salvaguardar la información ante nuevos virus.
- **II.** La Gerencia de Tecnologías de la Información es la encargada de la educación de los usuarios sobre cómo protegerse frente a los virus informáticos y cómo actuar si un virus informático infecta sus equipos

**III.** La empresa deberá contar con una solución antivirus centralizada corporativa de antivirus debidamente licenciada y de versión vigente.

**IV.** La Gerencia de Tecnología de la Información deberá mantener actualizada la protección antivirus en toda la institución sin intervención del usuario final, mediante actualizaciones automáticas y calendarizadas.

**V.** La Gerencia de Tecnología de la Información, deberá realizar configuraciones a los equipos de seguridad que permitan la detección de códigos contaminados introducidos por SMTP, HTTP y FTP, así como códigos en lava, VB Script y Active X. De esta manera, el sistema del usuario quedará protegido al entrar a Internet.

### 7.1.22 POLÍTICA DE SEGURIDAD DE LAS COMUNICACIONES

**Objetivo**:
Implementar mecanismos de control que permitan mantener la disponibilidad de las redes de datos, sistemas de comunicaciones e instalaciones de procesamiento de la empresa.

**Aplicabilidad**: Estas políticas aplican a los funcionarios, contratistas, colaboradores de la empresa actuales o por ingresar y a terceros que estén encargados de cualquier parte o sistema de la plataforma informática.

**Directrices**:

**I.** La Gerencia de Tecnologías de la Información debe implementar medidas para asegurar la disponibilidad de los recursos y servicios de red de EMAPE S.A

**II.** La Gerencia de Tecnologías de la Información debe implementar sistemas de protección entre las redes de la empresa y las redes externas no administradas por la entidad.

**III.** La Gerencia de Tecnologías de la Información debe identificar y documentar los servicios, protocolos y puertos autorizados en las redes de datos e inhabilitar o eliminar los servicios, protocolos y puertos no utilizados.

### 7.1.23 POLÍTICA DE USO DE CORREO ELECTRÓNICO

**Objetivo**: Definir las pautas generales para asegurar una adecuada protección de la información de la empresa, en el servicio yuso del servicio de correo electrónico por parte de los usuarios autorizados.

**Aplicabilidad**: Estas políticas aplican a los funcionarios, contratistas, colaboradores de la empresa actuales o por ingresar y a terceros que estén encargados de cualquier parte o sistema de la plataforma informática.

**Directrices**:

- **I.** Esta política define y distingue el uso de correo electrónico aceptable/apropiado e inaceptable/inapropiado y establece las directrices para el uso seguro del servicio.
- **II.** Los funcionarios de la empresa deberán hacer uso del correo electrónico institucional suministrado por la Gerencia de Tecnologías de la Información, para desarrollar las actividades oficiales inherentes al cargo asignado.
- **III.** La cuenta de correo oficial para el cumplimiento de las funciones desempeñadas para la empresa, es la cuenta de correo electrónico institucional suministrado por la Gerencia de Tecnologías de la Información.
- **IV.** Los usuarios del correo electrónico corporativo son responsables de evitar prácticas o usos del correo que puedan comprometer la Seguridad de la Información.
- **V.** Los servicios de correo electrónico corporativo se emplean para servir a una finalidad operativa y administrativa en relación con la entidad. Todos los correos electrónicos procesados por los sistemas, redes y demás infraestructura TIC de la empresa se consideran bajo el control de la entidad.
- **VI.** Este servicio debe utilizarse exclusivamente para las tareas propias de la función desarrollada y no debe utilizarse para ningún otro fin
- **VII.** El tamaño del buzón de correo electrónico estará determinado por el rol desempeñado por el usuario en la empresa.

### 7.1.24 POLÍTICAS ESPECÍFICAS PARA FUNCIONARIOS Y CONTRATISTAS DE LA GERENCIA DE SISTEMAS DE INFORMACIÓN

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

**Aplicabilidad**:

Estas políticas aplican a los funcionarios, contratistas, colaboradores de la empresa actuales o por ingresar ya terceros que estén encargados de cualquier parte o sistema de la plataforma informática**.**

**Directrices**:

- **I.** El personal de la Gerencia de Tecnología de la Información no debe dar a conocer su clave de usuario a terceros de los sistemas de información, sin una solicitud previa además de una autorización previa del Gerente de Sistemas de Información.
- **II.** Los usuarios y claves de los administradores de sistemas y del personal de Gerencia de Sistemas de Información son de uso personal e intransferible.

**III.** 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.

**IV.** El personal de la Gerencia de Tecnología de la Información no debe otorgar privilegios especiales sin la autorización correspondiente del Gerente de Sistemas de Información.

**V.** 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.

### 7.1.25 POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN EN EL TELETRABAJO

**Objetivo**: Definir las pautas generales para asegurar una adecuada protección de la información de la empresa por parte de los funcionarios y usuarios de la entidad.

**Aplicabilidad**: Estas políticas aplican a los funcionarios, contratistas, colaboradores de la empresa con la finalidad de establecer medidas que apoyen a la seguridad de la información a la que accedan.

**Directrices**:

**I.** El equipo del teletrabajador debe estar protegido, actualizado y monitoreado.

**II.** Bloquear puertos USB del equipo para periféricos de almacenamiento externos. Es importante mencionar que en caso de excepciones previamente autorizadas podrán ser habilitados para tal efecto en forma temporal.

**III.** Cuando no es posible utilizar la red doméstica para teletrabajar o cualquier otra red considerada segura como alternativa, utilizar la red de datos móvil 4G o 5G siempre evitando la conexión a redes wifi públicas.

**IV.** Autorizar el acceso remoto al personal responsable de la administración de los sistemas de información, base de datos, servidores o cualquier otro componente de la infraestructura tecnológica de la Empresa, para realizar actividades en el marco del cumplimiento de sus funciones.

**V.** Asegurar que el acceso remoto por el personal autorizado; a los sistemas de información, base de datos, servidores u otros, se realice a través de una Red Privada Virtual (VPN).

**VI.** El usuario debe realizar actividades estrictamente relacionadas con sus funciones por las cuales fue autorizado.

**VII.** Implementar controles de seguridad adicionales en función de la clasificación de la información a la cual tendrá acceso el personal autorizado.

### 7.1.26 POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES

**Objetivo**: Definir las pautas generales para garantizar la seguridad de los datos personales, mediante medidas de seguridad que protejan a los bancos de datos personales.

**Aplicabilidad**: Estas políticas aplican a los funcionarios, contratistas, colaboradores de la empresa con la finalidad de establecer medidas que apoyen a la seguridad de los datos personales.

**I.** Emape S. A. debe asignar a un encargado para los Bancos de Datos Personales, quien debe efectuar el tratamiento de datos personales contenidos en los mencionados bancos.

**II.** La Gerencia de Tecnologías de la información adecuará los sistemas de gestión existente, a efectos de proteger la información contenida en los bancos de Datos Personales evitando el uso no apropiado de estos.

**III.** Los funcionarios serán responsables de cumplir con los requisitos efectuados por el encargado de los bancos de datos personales.

### 7.1.27 Política de Ciberseguridad

**Objetivo:** Definir las pautas generales para garantizar la seguridad de los datos personales, mediante medidas de seguridad que protejan a los bancos de datos personales.

**Aplicabilidad:** Estas políticas aplican a los funcionarios, contratistas, colaboradores de la empresa con la finalidad de establecer medidas que apoyen a la seguridad de los datos personales.

**I.** Brindar capacitación especializada en seguridad de la información y ampliar las líneas de investigación en materia de ciberseguridad dentro de la organización.

**II.** Desarrollar un Plan de sensibilización y capacitación a todos los ciudadanos respecto a la Ciberseguridad.

**III.** Realizar evaluaciones de las amenazas y vulnerabilidades relativas a la información y a las instalaciones de procesamiento de la misma.

## 8. DISPOSICIONES ESPECÍFICAS

La Gerencia de Tecnologías de la Información es la unidad orgánica encargada de desarrollar, implementar y gestionar los sistemas de información, la infraestructura tecnológica y las telecomunicaciones que brindan soporte a las unidades orgánicas de EMAPE S.A., de acuerdo a las políticas y objetivos estratégicos institucionales.

## 9. DISPOSICIONES FINALES

**PRIMERA. –** La Política de Seguridad de la Información, tiene la clasificación de prioridad muy alta.