emape s.a.

EMPRESA MUNICIPAL
ADMINISTRADORA DE PEAJE DE LIMA

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Versión: 02	Código: GCPS-GSI-001-2018	Fecha: 20-11-2018	N° de Páginas: 50

RUBRO	NOMBRE	CARGO	FIRMA
REVISADO Y APROBADO POR:	ENRIQUE CASTILLO ALVAREZ	GERENTE CENTRAL DE PLANEAMIENTO Y SISTEMAS	

ÍNDICE

1. OBJETIVO

Establecer las 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, funcionarios, personal de planta de las oficinas y gerencias de la empresa, bajo el liderazgo de la Gerencia de Sistemas de Información perteneciente a la Gerencia Central de Planeamiento y Sistemas.

2. ALCANCE

La Seguridad de la Información es aplicable a todo el personal de las oficinas y gerencias de la empresa, para conseguir un adecuado nivel de protección de las características de calidad y Seguridad de la Información, aportando con su participación en la toma de medidas preventivas y correctivas, siendo un punto clave para el logro del objetivo y la finalidad de dicho manual.

3. BASE LEGAL

- 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 27001:2014.Sistemas de Gestión de Seguridad de la Información.
- Resolución Ministerial Nº 246-2007-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.

4. TÉRMINOS Y DEFINICIONES

4.1 CONCEPTOS GENERALES DE LA SEGURIDAD DE LA INFORMACIÓN

- Acceso, es la recuperación o grabación de datos que han sido almacenados en un sistema de computación. Cuando se consulta a una base de datos, los datos son primeramente recuperados hacia la computadora y luego transmitidos a la pantalla del terminal.
- **Amenaza,** cualquier cosa que pueda interferir con el funcionamiento adecuado de una computadora personal, o causar la difusión no autorizada de información

confiada a una computadora. Ejemplo: Fallas de suministro eléctrico, virus, saboteadores o usuarios descuidados.

- **Ataque,** término general usado para cualquier acción o evento que intente interferir con el funcionamiento adecuado de un sistema informático, o intento de obtener de modo no autorizado la información confiada a una computadora.
- **Ataque Activo,** acción iniciada por una persona que amenaza con interferir el funcionamiento adecuado de una computadora, o hace que se difunda de modo no autorizado información confiada a una computadora personal. Ejemplo: El borrado intencional de archivos, la copia no autorizada de datos o la introducción de un virus diseñado para interferir el funcionamiento de la computadora.
- Ataque Pasivo, intento de obtener información o recursos de una computadora personal sin interferir con su funcionamiento, como espionaje electrónico, telefónico o la intercepción de una red. Todo esto puede dar información importante sobre el sistema, así como permitir la aproximación de los datos que contiene.
- **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.

  También puede definirse, como un conjunto de archivos interrelacionados que es creado y manejado por un Sistema de Gestión o de Administración de Base de Datos (Data Base Management System - DBMS).

  Las características que presenta un DBMS son las siguientes:

  - Brinda seguridad e integridad a los datos.
  - Provee lenguajes de consulta (interactivo).
  - Provee una manera de introducir y editar datos en forma interactiva.
  - Existe independencia de los datos, es decir, que los detalles de la organización de los datos no necesitan incorporarse a cada programa de aplicación.
- **Datos,** los datos son hechos y cifras que al ser procesados constituyen una información, sin embargo, muchas veces datos e información se utilizan como sinónimos.

  En su forma más amplia los datos pueden ser cualquier forma de información: campos de datos, registros, archivos y bases de datos, texto (colección de

palabras), hojas de cálculo (datos en forma matricial), imágenes (lista de vectores o cuadros de bits), vídeo (secuencia de tramas), etc.

- **Golpe (Breach)**, es una violación con éxito de las medidas de seguridad, como el robo de información, el borrado de archivos de datos valiosos, el robo de equipos, PC, etc.
- **Incidente,** cuando se produce un ataque o se materializa una amenaza, tenemos un incidente, como por ejemplo las fallas de suministro eléctrico o un intento de borrado de un archivo protegido.
- **Integridad,** se refiere a que los valores de los datos se mantengan tal como fueron puestos intencionalmente en un sistema. Las técnicas de integridad sirven para prevenir que existan valores errados en los datos provocados por el software de la base de datos, por fallas de Programas, del sistema, hardware o errores humanos.

  El concepto de integridad abarca la precisión y la fiabilidad de los datos, así como la discreción que se debe tener con ellos.
- **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, sea accidental o intencionalmente, puedan ser modificados, destruidos o simplemente divulgados.

  En el caso de los datos de una organización, la privacidad y la seguridad guardan estrecha relación, aunque la diferencia entre ambas radica en que la primera se refiere a la distribución autorizada de información, mientras que la segunda, al acceso no autorizado de los datos.
- El acceso a los datos queda restringido mediante el uso de palabras claves, de forma que los usuarios no autorizados no puedan ver o actualizar la información de una base de datos o a subconjuntos de ellos.

4.2 OTROS CONCEPTOS

- **Acción correctiva:** acción tomada para eliminar las causas de una no conformidad detectada u otra situación indeseable, de tal forma que no se vuelva a presentar.

- **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:** Según [ISO/IEC 13335-12004]: Cualquier cosa que tiene valor para la empresa. También se entiende por cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la empresa. Es todo activo que contiene información, la cual posee un valor y es necesaria para realizar los procesos misionales y operativos en EMAPE S.A. Se pueden clasificar de la siguiente manera:
  - **Aplicaciones:** Es todo el software que se utiliza para la gestión de la información. Ejemplo: GEMA, Trámite Documentario, Planilla, entre otros.
  - **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, aquellos que la empresa suministra para el bien de la población.
  - **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, a través de una secuencia de actividades humanas que incluyen evaluación de riesgo, estrategias de desarrollo para manejarlo y mitigación del riesgo utilizando recursos gerenciales. Las estrategias incluyen transferir el riesgo a otra parte, evadir el riesgo, reducir los efectos negativos del riesgo y aceptar algunas o todas las consecuencias de un riesgo particular.

- **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, se basa en un análisis continuo y mejorado del desempeño de todos los activos y recursos gerenciales que tiene la empresa.

  Su objetivo principal es atender y orientar las acciones inmediatas para solucionar cualquier situación que cause una interrupción de los diferentes servicios que presta la empresa, de manera rápida y eficaz. No se limita a la solución de problemas específicos sino a buscar las causas que determinaron el incidente limitando el marco de acción de futuras ocurrencias, su enfoque se base en tres pilares fundamentales:

  - Detectar cualquier alteración en los servicios TI.
  - Registrar y clasificar estas alteraciones.
  - Asignar el personal encargado de restaurar el servicio.

- **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.
- **Autenticación:** Proceso que tiene por objetivo asegurar la identificación de una persona o sistema.
- **Autenticidad:** Los activos de información solo pueden estar disponibles verificando la identidad de un sujeto o recurso, es la propiedad que garantiza que la identidad de un sujeto o recurso es la que declara y se aplica a entidades tales como usuarios, procesos, sistemas de información.

- **Características de la Información:** las principales características desde enfoque de seguridad de Información son: confidencialidad, disponibilidad e integridad.
- **Checklist:** Lista de apoyo para el auditor con los puntos a auditar, que ayuda a mantener claros los objetivos de la auditoría, sirve de evidencia del plan de auditoría, asegura su continuidad y profundidad y reduce los prejuicios del auditor y su carga de trabajo.
- **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 por debajo del nivel de riesgo asumido, (Nota: Control es también utilizado como sinónimo de salvaguarda).
- **Control correctivo:** Control que corrige un riesgo, error, omisión o acto deliberado antes de que produzca pérdidas. Supone que la amenaza ya se ha materializado pero que se corrige.
- Control detectivo: Control que detecta la aparición de un riesgo, error, omisión o acto deliberado. Supone que la amenaza ya se ha materializado, pero por sí mismo no la corrige.
- **Control disuasorio:** Control que reduce la posibilidad de materialización de una amenaza.
- **Control preventivo:** Control que evita que se produzca un riesgo, error, omisión o acto deliberado. Impide que una amenaza llegue siquiera a materializarse.
- **Denegación de servicios:** Acción iniciada por agentes externos (personas, grupos, organizaciones) con el objetivo de imposibilitar el acceso a los servicios y recursos de una organización durante un período indefinido de tiempo.
- **Desastre:** Cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una organización durante el tiempo suficiente como para verse afectada de manera significativa.
- **Directiva:** descripción que clarifica qué debería ser hecho y cómo, con el propósito de alcanzar los objetivos establecidos en las políticas.
- **Disponibilidad:** característica o propiedad de permanecer accesible y disponible para su uso cuando se requiera.

- **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 o fallo de las salvaguardas, o una situación anterior desconocida que podría ser relevante para la seguridad.
- **Evidencia objetiva:** Información, registro o declaración de hechos, cualitativa o cuantitativa, verificable y basada en observación, medida o test, sobre aspectos relacionados con la confidencialidad, integridad o disponibilidad de un proceso o servicio o con la existencia e implementación de un elemento del sistema de Seguridad de la Información.
- **Gestión de claves:** Controles referidos a la gestión de claves criptográficas.
- **Gestión de riesgos:** Proceso de identificación, control y minimización o eliminación, a un coste aceptable, de los riesgos que afecten a la información de la organización. Incluye la valoración de riesgos y el tratamiento de riesgos.
- **Gusano (Worm):** Es un programa malicioso de computador que tiene la capacidad de duplicarse a sí mismo. A diferencia del virus, no altera información, aunque casi siempre causan problemas de red debido al consumo de ancho de banda y su gran facilidad para mutar.
- **Impacto:** Resultado de un incidente de Seguridad de la Información.
- **Información:** La información constituye un importante activo, esencial para las actividades de una organización y, en consecuencia, necesita una protección adecuada. La información puede existir de muchas maneras, es decir puede estar impresa o escrita en papel, puede estar almacenada electrónicamente, ser transmitida por correo o por medios electrónicos, se la puede mostrar en videos, o exponer oralmente en conversaciones.
- **Ingeniería Social:** Es la manipulación de las personas para conseguir que hagan que algo debilite la seguridad de la red o faciliten información con clasificación confidencial o superior.
- **Inventario de activos:** Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, reputación de la organización, etc.), que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.

- **ISO:** Organización Internacional de Normalización, con sede en Ginebra (Suiza). Es una agrupación de organizaciones nacionales de normalización cuyo objetivo es establecer, promocionar y gestionar estándares.
- **ISO 17799:** Código de buenas prácticas en gestión de la 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.
- **ISO 9000:** Normas de gestión y garantía de calidad definidas por la ISO.
- **ISO/IEC TR 13335-3:** "Information technology. Guidelines for the management of IT Security .Techniques for the management of IT Security." Guía de utilidad en la aplicación de metodologías de evaluación del riesgo.
- **ISO/IEC TR 18044:** "Information technology. Security techniques. Information security incident management". Guía de utilidad para la gestión de incidentes de Seguridad de la Información.
- **ITIL IT Infrastructure Library:** Un marco de gestión de los servicios de tecnologías de la información.
- **Keyloggers:** Son software o aplicaciones que almacenan información digitada mediante el teclado de un computador por un usuario.
- **Legalidad:** El principio de legalidad o Primacía de la ley es un principio fundamental del Derecho público conforme al cual todo ejercicio del poder público debería estar sometido a la voluntad de la ley de su jurisdicción y no a la voluntad de las personas (ej. el Estado sometido a la constitución o al Imperio de la ley). Por esta razón se dice que el principio de legalidad establece la seguridad jurídica, Seguridad de Información, Seguridad informática y garantía de la información.
- **No conformidad:** Situación aislada que, basada en evidencias objetivas, demuestra el incumplimiento de algún aspecto de un requerimiento de control que permita dudar de la adecuación de las medidas para preservar la confidencialidad, integridad o disponibilidad de información sensible, o representa un riesgo menor.
- **No conformidad grave:** Ausencia o fallo de uno o varios requerimientos de la ISO 27001 que, basada en evidencias objetivas, permita dudar seriamente de la

adecuación de las medidas para preservar la confidencialidad, integridad o disponibilidad de información sensible, o representa un riesgo inaceptable.

- **No repudio:** Los activos de información deben tener la capacidad para probar que una acción o un evento han tenido lugar, de modo que tal evento o acción no pueda ser negado posteriormente.
- **Phishing:** Tipo de delito encuadrado dentro del ámbito de las estafas, que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria), mediante una aparente comunicación oficial electrónica.
- **Plan de continuidad del negocio (Bussines Continuity Plan):** Plan orientado a permitir la continuación de las principales funciones de la empresa en el caso de un evento imprevisto que las ponga en peligro.
- **Plan de tratamiento de riesgos (Risk treatment plan):** Documento de gestión que define las acciones para reducir, prevenir, transferir o asumir los riesgos de Seguridad de la Información inaceptables e implantar los controles necesarios para proteger la misma.
- **Política de seguridad:** Documento que establece el compromiso de la Dirección y el enfoque de la empresa en la gestión de la Seguridad de la Información.
- **Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.
- **Segregación de tareas:** Separar tareas sensibles entre distintos funcionarios o contratistas para reducir el riesgo de un mal uso de los sistemas e informaciones deliberado o 'por negligencia.
- **Seguridad de la Información:** Preservación de la confidencialidad, integridad y disponibilidad de la información; además, otras propiedades como autenticidad, responsabilidad, no repudio, trazabilidad y fiabilidad pueden ser también consideradas.
- **Selección de controles:** Proceso de elección de los controles que aseguren la reducción de los riesgos a un nivel aceptable.
- **Spamming:** Se llama spam, correo basura o sms basura a los mensajes no solicitados, habitualmente de tipo publicitario, enviados en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptor. La

acción de enviar dichos mensajes se denomina spamming. La vía más usada es el correo electrónico.

- **Sniffers:** Programa de captura de las tramas de red. Generalmente se usa para gestionar la red con una finalidad docente o de control, aunque también puede ser utilizado con fines maliciosos.
- **Spoofing:** Falsificación de la identidad origen en una sesión: la identidad es por una dirección IP o Mac Address.
- **Troyano:** Aplicación que aparenta tener un uso legítimo pero que tiene funciones ocultas diseñadas para sobrepasar los sistemas de seguridad.
- **Usuario:** en el presente documento se emplea para referirse a directivos, funcionarios, y otros colaboradores en EMAPE S.A., debidamente autorizados para usar equipos, sistemas o aplicativos informáticos disponibles en la red y a quienes se les otorga un nombre de usuario y una clave de acceso.
- **Valoración de riesgos:** Proceso completo de análisis y evaluación de riesgos.
- **Virus:** Programas informáticos de carácter malicioso, que buscan alterar el normal funcionamiento de una red de sistemas o computador personal, por lo general su acción es transparente al usuario y este tarda tiempo en descubrir su infección; buscan dañar, modificar o destruir archivos o datos almacenados.
- **Vulnerabilidad:** Debilidad en la Seguridad de la Información de una organización que potencialmente permite que una amenaza afecte a un activo.

5. ANÁLISIS DE RIESGOS

Establecer los riesgos a los cuales está propensa EMAPE S.A., de igual manera determinar el nivel o factor de riesgo, que lo clasificaremos en los siguientes **Factores de Riesgo:**

- Bajo
- Muy Bajo
- Alto
- Muy alto
- Medio

Ellos nos determinan nuestra tabla de riesgos y nivel de factores que a continuación detallamos:

RIESGO	Factor de Riesgo				
	Muy Bajo	Bajo	Medio	Alto	Muy Alto
Incendio					X
Inundación		X			
Robo Común					X
Vandalismo, daño de equipos y archivos.					X
Fallas en los equipos, daño de archivos.					X
Equivocaciones, daño de archivos.			X		
Virus, daño de equipos y archivo.				X	
Terremotos, daño de equipos y archivos.				X	
Acceso no autorizado, filtración de info.					X
Robo de datos					X
Fraude, alteración de información.				X	
Desastre Total					X

En base a la tabla anteriormente presentada, concluimos que nuestro análisis de riesgo a modo general, nos hace ver que las posibles contingencias que pudieran presentarse en su mayoría van de un factor de ocurrencia alto y muy alto.

A continuación realizamos un deslinde de las causas por las cuales mayormente se presentan estos tipos de riesgos, para ello realizamos la siguiente lista de preguntas:

a) Con respecto al ***fuego***, que puede destruir los equipos y los archivos

¿La Institución cuenta con protección contra incendios?

¿Se cuenta con sistemas de aspersión automática?

¿Cuenta con diversos extintores?

¿Detectores de humo?

¿Los empleados están preparados para enfrentar un posible incendio?

b) Con respecto al ***robo común***, llevándose los equipos y archivos

¿En qué tipo de vecindario se encuentra la Institución?

¿Hay venta de drogas?

¿Los equipos de cómputo se ven desde la calle?

¿Hay personal de seguridad en la empresa?

¿Cuántos vigilantes hay?

¿Los vigilantes, están ubicados en zonas estratégicas?

¿Se cuenta con un sistema de seguridad para prevenir el ingreso de personas no autorizadas?

¿Se cuenta con cámaras de seguridad dentro como fuera de la empresa?

c) Con respecto al ***vandalismo***, que dañen los equipos y archivos

¿Existe la posibilidad que un ladrón cause daños?

¿Hay la probabilidad que cause algún otro tipo de daño intencionado?

d) Con respecto a ***fallas en los equipos*** que dañen los archivos

¿Los equipos tienen un mantenimiento continuo por parte de personal calificado?

¿Cuáles son las condiciones actuales del hardware?

¿Es posible predecir las fallas a que están expuestos los equipos?

¿Existe una correcta protección eléctrica para los equipos de cómputo?

e) A ***equivocaciones*** que dañen los archivos

¿Cuánto saben los empleados de computadoras o redes?

Los que no conocen del manejo de la computadora, ¿saben a quién pedir ayuda?

Durante el tiempo de vacaciones de los empleados, ¿qué tipo de personal los sustituye y qué tanto saben del manejo de computadoras?

f) Con respecto a la acción de ***virus***, que dañen los archivos

¿Se prueba software en la oficina sin hacerle un examen previo?

¿Está permitido el uso de usb o cd o dvd en la oficina?

¿Todas las máquinas tienen cd o dvd o puertos USB?

¿Se cuentan con procedimientos contra los virus?

g) Con respecto a ***terremotos*** que destruyen los equipos y archivos

¿La empresa se encuentra en una zona sísmica?

Un terremoto, ¿cuánto daño podría causar?

h) Con respecto a ***accesos no autorizados*** filtrándose datos importantes

¿Existe registro de personal autorizado en el Centro de datos de la empresa?

¿Qué probabilidad hay que un colaborador intente hacer un acceso no autorizado?

¿Existe comunicación remota de la red? ¿Qué tipo de servicio se utiliza (Telnet, FTP, VPN, etc)?

¿Se cuenta con Sistemas de Seguridad en el Correo Electrónico o Internet?

i) Con respecto al ***robo de datos***: y la posible difusión de estos.

¿Cuánto valor tienen actualmente las Bases de Datos?

¿Cuánta pérdida podría causar en caso de que se hicieran públicas?

¿Se ha elaborado una lista de los posibles sospechosos que pudieran efectuar el robo?

j) Con respecto al ***fraude***, vía computadora.

¿Cuántas personas se ocupan de la contabilidad de la empresa?

¿Los sistemas son confiables? ¿Pueden copiar datos en archivos?

Las personas que trabajan en las diferentes áreas, ¿qué tipo de antecedentes laborales tienen?

¿Existe acceso a los sistemas desde otros sistemas externos o por personas no autorizadas?

6. POLÍTICAS, PROCEDIMIENTOS Y CONTROLES

6.1 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

6.1.1 POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN.

De acuerdo al Análisis de Riesgos presentados 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 las personas, (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:

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

b. 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

c. 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.

d. 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.

e. 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 Sistemas de Información en concordancia con la política de adquisición de bienes de la empresa.

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

g. 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 Sistemas de Información.

h. Los funcionarios o jefes de área deben asegurarse que todos los procedimientos de Seguridad de la Información dentro de su área de responsabilidad, se realicen correctamente para lograr el cumplimiento de las políticas y estándares de Seguridad de la Información.

i. EMAPE S.A. en caso de tener un servicio de transferencia de archivos deberá realizarlo empleando protocolos seguros. Cuando el origen sea EMAPE S.A. hacia entidades externas, la empresa establecerá los controles necesarios para preservar la Seguridad de la Información; cuando el origen de la transferencia sea una entidad externa, se acordarán las políticas y controles de Seguridad de la Información con esa entidad; en todo caso se deben revisar y proponer controles en concordancia con las políticas de Seguridad de la Información de la empresa; los resultados de la revisión de requerimientos de seguridad se documentarán y preservarán para futuras referencias o para demostrar el cumplimiento con las políticas y con los controles de seguridad de la empresa.

6.1.2 POLÍTICA DE ESTRUCTURA ORGANIZACIONAL DE SEGURIDAD DE LA INFORMACIÓN

La Gerencia de Sistemas de 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:

- 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.
- 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.
- El Comité de Seguridad de la Información reportará los incidentes de seguridad al Director y/o Gerente General de EMAPE S.A. permitiendo apoyar la gestión de incidentes de seguridad y la planificación de contingencias.
- La Gerencia de Sistemas de Información asistirá a foros, conversatorios, conferencias de interés especial en Seguridad de la Información.
- Los proyectos desarrollados por la Gerencia de Sistemas deberá 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.

6.1.3 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:

- 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.
- Los dispositivos móviles asignados por la empresa deben tener la configuración realizada por la oficina de Soporte Técnico perteneciente a la Gerencia de Sistemas de Información, así mismo tener configurado la cuenta de correo electrónico asignado al usuario por la empresa.
- 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.
- 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 Sistemas de Información.
- 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 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 oficina de Soporte Técnico perteneciente a la Gerencia de Sistemas de Información y continuar con el procedimiento administrativo por perdida de elementos establecido por la entidad.
- 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.
- 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.

GERENCIA CENTRAL DE PLANEAMIENTO Y SISTEMAS - GCPS - VºBº - EMAPE S.A.

- Los usuarios no están autorizados a cambiar la configuración, ni a la desinstalación de software de los equipos móviles institucionales posterior a su recibo; únicamente se deben aceptar y aplicar las actualizaciones.
- Los usuarios de dispositivos móviles asignados por la entidad, 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 institucionales no deben conectarlos en computadores y/o puertos USB de uso público *(Restaurantes, café internet, aeropuertos, etc.).*
- Los usuarios de dispositivos móviles institucionales deben mantener desactivados las funciones de redes inalámbricas WiFi, puertos infrarrojos, puerto Bluetooth.
- Los usuarios de dispositivos móviles institucionales NO deben hacer uso de redes inalámbricas públicas.
- En caso de requerir instalación de aplicaciones adicionales en el dispositivo móvil institucional se debe solicitar mediante solicitud a la Gerencia de Sistemas de Información para su aprobación.

6.1.4 POLÍTICA DE SEGURIDAD PARA LOS ACTIVOS DE LA INFORMACIÓN

Objetivo:

Establecer la forma en que se logra y mantiene 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 oficina de Soporte Técnico 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 Sistemas de Información.

El inventario de los activos informáticos deben 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).

6.1.5 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:

- Los activos de información pertenecen a EMAPE S.A. y el uso de los mismos debe emplearse exclusivamente con propósitos laborales.
- Los usuarios deberán utilizar únicamente los programas y equipos autorizados por la Gerencia de Sistemas de Información.
- La oficina de Soporte Técnico perteneciente a la Gerencia de Sistemas de Información proporcionará al usuario, la solicitud debe hacerla por el

módulo de Mesa de Ayuda, los equipos informáticos y los programas instalados en ellos; los datos/información creados, almacenados y recibidos, serán propiedad de EMAPE S.A., los funcionarios solo podrán realizar backup de sus archivos personales o de información pública, para copiar cualquier tipo de información clasificada o reservada debe pedir autorización a su jefe inmediato, su copia, sustracción, daño intencional o utilización para fines distintos a las labores propias de la Institución, serán sancionadas de acuerdo con las normas y legislación vigentes.

- Periódicamente, la Gerencia de Sistemas de Información efectuará la revisión de los programas utilizados en cada dependencia que deben tener la licencia de funcionamiento correspondiente. 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.
- 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 Ayuda.
- Estarán bajo custodia de la oficina de Soporte Técnico perteneciente a la Gerencia de Sistemas de Información los medios magnéticos/electrónicos (CDs, DVDs 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 los *passwords* de administración de los equipos informáticos, sistemas de información o aplicativos.
- En caso de ser necesario, los funcionarios de EMAPE S.A. 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 en EMAPE S.A. 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, para ello debe tener la respectiva autorización.

- 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.
- Los usuarios no podrán efectuar ninguna de las siguientes labores sin previa autorización de la Gerencia de Sistemas de 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;
  - Descompilar o realizar ingeniería inversa en cualquier software de propiedad de la empresa;
  - Copiar o distribuir cualquier software de propiedad de la empresa.
  - Cambiar la configuración de hardware de propiedad de la empresa.
- El usuario deberá informar al funcionario o Jefe Inmediato de cualquier violación de las políticas de seguridad, uso indebido y debilidades en la Seguridad de la Información a la Gerencia de Sistemas de Información.
- El usuario será responsable de todas las transacciones o acciones efectuadas con su "cuenta de usuario".
- 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.
- Los usuarios no están autorizados para hacer uso de redes externas a través de dispositivos personales en las instalaciones de la entidad (modem USB, router, wifi público, etc), esto compromete la seguridad de los recursos informáticos de EMAPE S.A.
- La Gerencia de Sistemas de Información, es la gerencia responsable de realizar el aseguramiento de los accesos a internet, acceso a redes de terceros y a las redes de la entidad; esta responsabilidad incluye, pero no se limita a prevenir que Intrusos tengan acceso a los recursos informáticos y a prevenir la introducción y propagación de virus.

- 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.
- Todos los archivos provenientes de equipos externos a EMAPE S.A., deben ser revisados para detección de virus antes de su utilización dentro de la red de la empresa.
- Todo cambio a la infraestructura informática deberá estar controlado y será realizado mediante solicitud a la Gerencia de Sistemas de Información.
- Cada vez que se busque construir o implementar una nueva ambiente/área deberá solicitar a la Gerencia de Sistemas de Información su opinión técnica para la mejor distribución de la infraestructura tecnológica.
- La información de la empresa debe ser respaldada de forma frecuente, debe ser almacenada por la Oficina de Soporte Técnico en lugares aproplados en los cuales se pueda garantizar que la información este segura y podrá ser recuperada en caso de un desastre o de incidentes con los equipos de procesamiento.
- 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.

6.1.6 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:

- La instalación de software en los computadores suministrados por EMAPE S.A. es una función exclusiva de la Oficina de Soporte Técnico el cual mantendrá una lista actualizada del software autorizado para instalar en los computadores.
- Se definirán dos (2) perfiles de Administradores locales:
  1. Desarrolladores de aplicaciones.
  2. Usuarios que necesitan utilizar software específico, que por su naturaleza requieren permisos de administrador local para su ejecución.
- Los usuarios de la red EMAPE S.A ingresarán a sus sesiones en los equipos de cómputo a través de usuarios de dominio creados a solicitud del Gerente o Jefe de la Unidad Orgánica.
- Los usuarios no deben mantener almacenados en los discos duros de las estaciones cliente o discos virtuales de red, archivos de vídeo, música y fotos 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. El usuario deberá abstenerse de realizar modificaciones a éstos archivos.
- En el Disco D:\ los usuarios deberán trabajar todos sus documentos institucionales.
- El préstamo de equipos de cómputo, computadores portátiles y vídeo proyectores se debe tramitar a través de la Mesa de Ayuda con anticipación y se proveerá de acuerdo a la disponibilidad.
- 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.
- La Gerencia de Sistemas de Información no prestará servicio de soporte técnico (revisión, mantenimiento, reparación, configuración y manejo e información) a equipos que no sean de la empresa.

6.1.7 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:

- 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.
- La navegación en Internet debe realizarse de forma razonable y con propósitos laborales.
- 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, hacktivismo, 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
- 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 Ayuda. Por ello se contará con un servicio de tres perfiles:
  - **Estándar**, acceso a la intranet páginas institucionales.
  - **Intermedio**, acceso a correos personales comerciales, Hotmail, Gmail.
  - **Total**, acceso exclusivo para Funcionarios o con autorización expresa del Gerente o Jefe a todas las páginas incluyendo redes sociales.

- La Gerencia de Sistemas de Información implementará herramientas para evitar la descarga de software no autorizado y/o código malicioso en los equipos institucionales.
- La descarga de archivos de Internet debe ser con propósitos laborales y de forma razonable para no afectar el servicio, en forma específica el usuario debe cumplir los requerimientos de la política de uso de internet descrita en este manual.
- Los usuarios de los activos de información de EMAPE S.A. tienen prohibido el acceso a redes sociales, sistemas de mensajería instantánea y cuentas de correo no institucional salvo previa autorización salvo el envío de un correo electrónico por parte del Gerente o Jefe de la Unidad Orgánica solicitante a la Oficina de Soporte Técnico.

6.1.8 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:

- 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.
  - Información o conocimiento transmitido de manera verbal o por cualquier otro medio de comunicación.
- 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.

- 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; Independiente del tipo de activo, se deben considerar las siguientes características:

  a) El activo de información es reconocido como valioso para EMAPE S.A.

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

  c) Forma parte de la identidad de la organización y sin el cual la empresa puede estar en algún nivel de riesgo.

  d) Los niveles de clasificación de la información valiosa que se ha establecido son: INFORMACIÓN PÚBLICA RESERVADA, INFORMACIÓN PÚBLICA CLASIFICADA (PRIVADA Y SEMI-PRIVADA) e INFORMACIÓN PÚBLICA.

6.1.9 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:

- Los medios y equipos donde se almacena, procesa 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.

- Se debe realizar la aplicación del procedimiento de borrado seguro definido por la empresa.
- 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 Gerencia de Sistemas de Información o que la Gerencia Central de Administración Finanzas especifique la utilización de dichos medio removibles en las Unidades Orgánicas.

6.1.10 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:

- La Gerencia de Sistemas de Información establecerá el procedimiento para establecer los niveles de acceso para usuarios de los servicios y sistemas de información en EMAPE S.A.
- La Gerencia de Sistemas de Información establecerá las configuraciones de las políticas en los sistemas de tecnología y comunicaciones para el control de acceso a los activos de información.
- La Gerencia Central de Administración y Finanzas proporcionará a los funcionarios, personal en comisión permanente y contratistas (personas naturales) todos los recursos tecnológicos necesarios para que puedan desempeñar las funciones para las cuales fueron contratados, por tal motivo no se permite conectar a la red o instalar dispositivos fijos o

móviles, tales como: computadores portátiles, *tablets*, enrutadores, agendas electrónicas, celulares inteligentes, *access point*, sin el requerimiento expreso a la oficina de Soporte Técnico.

- La oficina de Soporte Técnico 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, previamente reportado a la Mesa de Ayuda, las claves son de uso personal e intransferible.
- Es responsabilidad del usuario el manejo apropiado a las claves asignadas de los servicios de red y de acceso a la red estas claves de acceso y usuarios son personales e intransferibles.
- Solo la oficina de Soporte Técnico estará autorizado, previa solicitud por correo electrónico, para instalar software y/o hardware en los equipos, servidores e infraestructura de telecomunicaciones de EMAPE S.A, así como el uso de herramientas que permitan realizar tareas de mantenimiento, revisión de software, recuperar datos perdidos, eliminar software maliciosos.
- 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 Sistemas de Información.
- La Gerencia de Sistemas de 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).
- La Gerencia de Sistemas de Información establecerá el procedimiento de registro, cancelación y periodicidad de revisión y ajuste a permisos de acceso a la red y servicios de red, asignados a los usuarios de los sistemas de información y comunicaciones de la empresa, tomando como base los múltiples factores de riesgo existentes en la Seguridad de la Información.
- Es muy importante que la Gerencia Central de Administración y Finanzas o la Gerencia que corresponda comunique a la Gerencia de Sistemas de Información el término del vínculo laboral del trabajador o funcionario de la empresa para inhabilitar los accesos a los diferentes sistemas.

- 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, registrada y auditada.

6.1.11 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:

- 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, las cuales constituyen un medio de validación de la identidad de un usuario y consecuentemente un medio para establecer derechos de acceso a las instalaciones, equipos o servicios informáticos.
- 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.
- Los usuarios deben tener en cuenta los siguientes aspectos:
  - No incluir contraseñas en ningún proceso de registro automatizado, por ejemplo almacenadas en un macro o en una clave de función.
  - El cambio de contraseña solo podrá ser solicitado por el titular de la cuenta o su jefe inmediato.
  - Terminar las sesiones activas cuando finalice, o asegurarlas con el mecanismo de bloqueo cuando no estén en uso.
  - Se bloqueara el acceso a todo usuario que haya intentado el ingreso, sin éxito, a un equipo o sistema informático, en forma consecutiva por cinco veces.
  - La clave de acceso será desbloqueada sólo por la Oficina de Soporte Técnico, luego de la solicitud formal por parte del responsable de la

cuenta. Para todas las cuentas especiales, la reactivación debe ser documentada y comunicada.

Las claves o contraseñas deben:

Poseer algún grado de complejidad y no deben ser palabras comunes que se puedan encontrar en diccionarios, ni tener información personal, ni productos a resaltar de su entidad, evite asociarla con fechas especiales, por ejemplo: fechas de cumpleaños, nombre de los hijos, placas de automóvil, etc.

- Nunca utilice sus contraseñas personales en el entorno laboral.
- Tener mínimo ocho a diez caracteres alfanuméricos.
- Se sugiere que se cambie obligatoriamente la contraseña, la primera vez que el usuario ingrese al sistema.
- Se sugiere que se cambie obligatoriamente cada 30 días, o cuando lo establezca la Gerencia de Sistemas de Información, por medida de seguridad informática.
- Cada vez que se cambien estas deben ser distintas por lo menos de las últimas tres anteriores.
- Cambiar la contraseña si ha estado bajo riesgo o se ha detectado anomalía en la cuenta de usuario.
- No se deben usar caracteres idénticos consecutivos, ni que sean todos numéricos, ni todos alfabéticos.
- No debe ser visible en la pantalla, al momento de ser ingresada o mostrarse o compartirse.
- No ser reveladas a ninguna persona, incluyendo al personal de la Gerencia de Sistemas de Información.
- No regístralas en papel, archivos digitales o dispositivos manuales, a menos que se puedan almacenar de forma segura y el método de almacenamiento este aprobado.
- Bloquear su sesión de trabajo cada vez que abandone su computadora.

6.1.12 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:

- 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, a la oficina de Soporte Técnico de la Gerencia de Sistemas de Información. Los usuarios tendrán permisos de escritura, lectura o modificación de información en los discos de red, dependiendo de sus funciones y su rol.
- La información institucional que se trabaje en las estaciones cliente de cada usuario debe trasladar a las carpeta de red compartida que le corresponda por ser información institucional.
- La información almacenada en cualquiera de los discos de red debe ser de carácter institucional.
- 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. o en los discos de red.
- 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.
- Se prohíbe el uso de la información de los discos de red con fines publicitarios, de imagen negativa, lucrativa o comercial.
- La responsabilidad de generar las copias de respaldo de la información de los discos de red, está a cargo de la Oficina de Soporte Técnico de la Gerencia de Sistemas de Información.

- La responsabilidad de custodiar la información en copias de respaldo controladas, fuera de las instalaciones de EMAPE S.A., estará a cargo de la Oficina de Soporte Técnico de la Gerencia de Sistemas de Información.

6.1.13 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:

- Los usuarios deberán emplear los puntos de red, para la conexión de equipos informáticos Institucionales.
- La Gerencia General y Unidades Orgánicas deberán solicitar la opinión técnica de la Gerencia de Sistemas de 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.
- 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 Oficina de Soporte Técnico de la Gerencia de Sistemas de Información.
- La instalación, activación y gestión de los puntos de red es responsabilidad de Oficina de Soporte Técnico de la Gerencia de Sistemas de Información.

6.1.14 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:

- Los documentos que se impriman en las impresoras de la empresa 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 Oficina de Soporte Técnico de la Gerencia de Sistemas 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.

6.1.15 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:

- La Gerencia de Sistemas de 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.
- La Gerencia de Sistemas de Información deberá implementar alarmas de detección de intrusos a los centros de datos y centros de cableado de la empresa.
- La Gerencia Central de Administración y Finanzas 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.
- La Gerencia Central de Administración y Finanzas deberá apoyar a la Gerencia de Sistemas de Información para mantener libres los pasadizos de los gabinetes así como también los ambientes como se indica en las Normas Técnicas de Seguridad Informática.
- La Gerencia Central de Administración y Finanzas, implementará y mantendrá en operación sistemas de control de incendio, así como planes integrales a las instalaciones para prevenir inundaciones o humedad en los centros de datos y centros de cableado.
- La Gerencia de Sistemas de 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.
- 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, centros de cableados, centros de control.

6.1.16 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 y a terceros que estén encargados de cualquier parte o sistema de la plataforma informática.

Directrices:

- 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.
- La Gerencia de Sistemas de Información debe garantizar que el control de acceso al centro de datos de EMAPE S.A., exija doble autenticación para aprobación de acceso con dispositivos electrónicos.
- La Gerencia de Sistemas de Información deberá garantizar que todos los equipos de los centros de datos cuenten con un sistema alterno de respaldo de energía.
- La limpieza y aseo del centro de datos estará a cargo de la Gerencia Central de Administración y Finanzas y debe efectuarse en presencia de un personal de la Oficina de Soporte Técnico de la Gerencia de Sistemas de Información. El personal de limpieza debe ser ilustrado con respecto a las precauciones mínimas a seguir durante el proceso de limpieza. Debe prohibirse el ingreso de personal de limpieza con maletas o elementos que no sean estrictamente necesarios para su labor de limpieza y aseo.
- 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.
- 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 industrial y de salud ocupacional.
  - Pisos elaborados con materiales no combustibles.

- 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 y estas pruebas deberán estar previstas en los procedimientos de mantenimiento y de control.

- 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.

- El cableado de la red debe ser protegido de interferencias por ejemplo usando canaletas que lo protejan.
- Las actividades de soporte y mantenimiento dentro del centro de datos siempre deben ser supervisadas por personal de la oficina de Soporte Técnico.
- 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.
- Cuando se requiera realizar alguna actividad sobre algún armario (*rack*), este debe quedar ordenado, cerrado y con llave, cuando se finalice la actividad.
- Mientras no se encuentre personal dentro de las instalaciones del centro de datos, las luces deben permanecer apagadas.
- Los equipos del centro de datos que lo requieran, deben estar monitoreados para poder detectar las fallas que se puedan presentar.

6.1.17 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:

a) 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 Sistemas de Información.
- 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 EMAPE S.A. 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.

b) 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 Sistemas de Información establecerá un programa de revisiones y/o inspecciones físicas al cableado, con el fin de detectar dispositivos no autorizados.

c) 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.
- Los equipos que requieran salir de las instalaciones de EMAPE S.A. para reparación o mantenimiento, deben estar debidamente autorizados por la Gerencia Central de Administración y Finanzas y se debe garantizar que en dichos elementos no se encuentra información clasificada de acuerdo a 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 entidad, 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 la empresa.
- 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, utilizando herramientas para realizar sobre-escrituras sobre la información existente o la presencia de campos magnéticos de alta intensidad.

d) 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.

6.1.18 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:

- La Gerencia de Sistemas de Información debe elaborar las guías de operación de todos los activos de información, así mismo dejarlas a disposición de los usuarios que los requiera.
- La Gerencia de Sistemas de Información debe generar un programa de seguimiento a la gestión de capacidad de los recursos de red de sistemas de información y comunicaciones, generando proyecciones de crecimiento y expansión asegurando la disponibilidad de los servicios.
- La Gerencia de Sistemas de Información debe implementar el procedimiento para la realización de auditorías técnicas a los sistemas operativos de la empresa, las cuales se deben realizar periódicamente.

6.1.19 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 o por ingresar y a terceros que estén encargados de cualquier parte o sistema de la plataforma informática.

Directrices:

- Asegurar que los sistemas de información o aplicativos informáticos incluyen controles de seguridad y cumplen con las políticas de Seguridad de la Información.
- 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.
- 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.
- La Gerencia de Sistemas de Información desarrollará y/o adquirirá el software requerido; de manera coordinada con el Área que tiene manifieste la necesidad del software, la Gerencia de Sistemas de Información establecerá claramente los requerimientos funcionales, operacionales y especificaciones técnicas para la adquisición o desarrollo de sistemas de información y/o comunicaciones, contemplando requerimientos de Seguridad de la Información.
- 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.
- 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.

- 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.
- La compra de una licencia de un programa permitirá a la oficina de Soporte Técnico realizar una copia de seguridad, para ser utilizada en caso de que el medio se averíe.
- Cualquier otra copia del programa original será considerada como una copia no autorizada y su utilización conlleva a las sanciones administrativas y legales pertinentes.
- La Gerencia de Sistemas de Información será la única dependencia autorizada para realizar copia de seguridad del software original.
- La instalación del software en los activos informáticos de la empresa, se realizará únicamente a través de la oficina de Soporte Técnico de la Gerencia de Sistemas de Información.
- La Gerencia de Sistemas de Información implementará reglas y herramientas que restrinjan la instalación de software no autorizado en los activos de información de la empresa.
- El software proporcionado por la empresa no puede ser copiado o suministrado a terceros.
- En los equipos de la empresa se podrá utilizar el software licenciado por la Gerencia de Sistemas de Información y el adquirido o licenciado por los proyectos o programas que se encuentran en la empresa.
- Para la adquisición y actualización de software, es necesario efectuar la solicitud a la Gerencia de Sistemas de Información con su justificación, quien analizará las propuestas presentadas para su evaluación y aprobación.
- El software que se adquiera a través de proyectos o programas, debe quedar licenciado a nombre de la empresa.
- Se encuentra prohibido el uso e instalación de juegos en los computadores de la empresa.
- Se presentarán para dar de baja el software de acuerdo con los lineamientos dados por la empresa.

- La Gerencia de Sistemas de Información debe implementar actividades para la protección contra códigos maliciosos y de reparación.
- La Gerencia de Sistemas de Información debe implementar métodos y/o técnicas para el desarrollo de software seguro, estas deben incluir definiciones y requerimientos de seguridad, buenas prácticas para desarrollo de software seguro, que le permita a los desarrolladores aplicarlas de manera clara y eficiente.
- La Gerencia de Sistemas de Información debe implementar y aplicar metodologías que permitan proteger las transacciones de los servicios de aplicaciones de la empresa.
- Se debe implementar el procedimiento de control de cambios de los sistemas de información, basados en el ciclo de vida, asegurando la integridad desde las primeras etapas de diseño, pasando por mantenimiento.

6.1.20 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:

- La información de cada sistema debe ser respaldada sobre un medio de almacenamiento como CD, DVD, etc.
- El administrador de los servidores, los sistemas de información o los equipos de comunicaciones, es el responsable de definir la frecuencia de respaldo y los requerimientos de Seguridad de la Información.
- Todas las copias de información crítica deben ser almacenadas en un área adecuada y con control de acceso.
- Las copias de respaldo se guardaran 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.

- Debe ser desarrollado un plan de emergencia para todas las aplicaciones que manejen información crítica; el dueño de la información debe asegurar que el plan es adecuado, frecuentemente actualizado y periódicamente probado y revisado.
- Ningún tipo de información institucional puede ser almacenada en forma exclusiva en los discos duros de las estaciones de trabajo; por lo tanto, es obligación de los usuarios finales realizar las copias en las carpetas destinadas para este fin.
- Deben existir al menos una copia de la información de los discos de red, la cual deberá permanecer fuera de las instalaciones de la empresa.
- La restauración de copias de respaldo en ambientes de producción debe estar debidamente aprobada por el propietario de la información.
- Semanalmente el administrador de infraestructura, verificará la correcta ejecución de los procesos de backup, suministrarán los medios de almacenamiento requeridas para cada trabajo.
- La Gerencia de Sistemas de Información debe mantener un inventario actualizado de las copias de respaldo de la información y los aplicativos o sistemas de la empresa.
- Los medios que vayan a ser eliminados deben surtir un proceso de borrado seguro y posteriormente serán eliminados o destruidos de forma adecuada.
- Es responsabilidad de cada dependencia mantener depurada la información de las carpetas virtuales para la optimización del uso de los recursos de almacenamiento que entrega la empresa a los usuarios.

6.1.21 POLÍTICA DE GESTIÓN CENTRALIZADA PROTECCION DE RED

Objetivo:

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 oficina de Soporte Técnico.

Directrices:

- La Gerencia de Sistemas de Información en coordinación con la oficina de Soporte Técnico, deberán desarrollar una "Directiva de seguridad ante la presencia de virus informático", incluyendo en estas lineamientos para poder salvaguardar la información ante nuevos virus (por ejemplo, políticas de bloqueo de virus y filtrado de contenido).
- La Gerencia de Sistemas de 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.
- La Gerencia de Sistemas de Información en coordinación con la oficina de Soporte Técnico deberá informar a los usuarios la utilización y configuración del antivirus de manera correcta.
- La empresa deberá contar con una solución antivirus centralizada corporativa de antivirus debidamente licenciada y de versión vigente.
- La oficina de Soporte Técnico deberá mantener actualizada la protección antivirus en toda la institución sin intervención del usuario final, mediante actualizaciones automáticas y calendarizadas.
- La oficina de Soporte Técnico deberá mantener el control de las alertas recibidas de las estaciones de trabajo y servidor.
- La oficina de Soporte Técnico, deberá tener herramientas que les permitan analizar cada e-mail entrante y saliente por el contenido que se desea bloquear en su cabecera, cuerpo o attachment. La herramienta deberá permitir filtrar potencialmente los contenidos maliciosos al proporcionar algunos filtros significativos que detectan el contenido de correos electrónicos como puede ser el remitente, al asunto, el cuerpo del mensaje y el anexo.
- La Oficina de Soporte Técnico, 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 Java, VB Script y

Active X. De esta manera, el sistema del usuario quedará protegido al entrar a Internet.

- Cualquier acción que contravenga a la presente Directiva, ameritará la aplicación de la sanción correspondiente, de parte de la Secretaría de Administración u el órgano correspondiente conforme a Ley.

6.1.22 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:

- La Gerencia de Sistemas de Información debe implementar medidas para asegurar la disponibilidad de los recursos y servicios de red de EMAPE S.A.
- La Gerencia de Sistemas de Información debe crear los estándares técnicos de configuración de la Red de EMAPE S.A. y configuración de seguridad y de dispositivos de seguridad.
- La Gerencia de Sistemas de Información debe interconectar las instalaciones bajo el cumplimiento los estándares de técnicos de configuración y de seguridad de las redes y servicios de la empresa.
- La Gerencia de Sistemas de Información debe implementar sistemas de protección entre las redes de la empresa y las redes externas no administradas por la entidad.
- La Gerencia de Sistemas de 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.
- La Gerencia de Sistemas de Información debe segmentar la red, de modo que permita separar los grupos de servicios de información.

6.1.23 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 y uso 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:

- 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.
- Los funcionarios de la empresa deberán hacer uso del correo electrónico institucional suministrado por la Gerencia de Sistemas de Información, para desarrollar las actividades oficiales inherentes al cargo asignado.
- 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 Sistemas de Información.

Sobre el servicio de correo electrónico:

- Permite a los usuarios de EMAPE S.A., el intercambio de mensajes, a través de una cuenta de correo electrónico institucional, que facilita el desarrollo de sus funciones.
- Los usuarios del correo electrónico corporativo son responsables de evitar prácticas o usos del correo que puedan comprometer la Seguridad de la Información.
- 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.
- Este servicio debe utilizarse exclusivamente para las tareas propias de la función desarrollada 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, o colaborador al que le haya sido autorizado el uso de una cuenta de correo electrónico y se retire de la empresa, su cuenta de correo será desactivada.
- El tamaño del buzón de correo electrónico estará determinado por el rol desempeñado por el usuario en la empresa.
- Las cuentas de correo electrónico son propiedad de EMAPE S.A., las cuales son asignadas a personas que tengan algún tipo de vinculación laboral con la entidad, ya sea como personal de planta, en comisión permanente, o personal temporal, quienes deben utilizar este servicio única y exclusivamente para las tareas propias de la función desarrollada en la Entidad 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 la empresa.
- Todos los mensajes pueden ser sujetos a análisis y conservación permanente por parte de la empresa.
- Todo usuario es responsable por la destrucción de los mensajes cuyo origen sea desconocido y por lo tanto asumirá 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 soporte01@emape.gob.pe con la frase "correo sospechoso" en el asunto.
- El único servicio de correo electrónico autorizado en la entidad es el asignado por la Gerencia de Sistemas de Información.

6.1.24 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 y a terceros que estén encargados de cualquier parte o sistema de la plataforma informática.

Directrices:

- El personal de Soporte Técnico 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.
- Los usuarios y claves de los administradores de sistemas y del personal de Gerencia de Sistemas de Información son de uso personal e intransferible.
- El personal de la Gerencia de Sistemas de Información 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.
- 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 entidad. 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.

- El personal de Soporte Técnico no deben otorgar privilegios especiales a los usuarios sobre las estaciones de trabajo, sin la autorización correspondiente del Gerente de Sistemas de Información.
- El personal de la Gerencia de Sistemas de 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 guía de clasificación de la información según sus niveles de seguridad. En consecuencia, se obligan a mantenerla de manera confidencial y privada y a protegerla para evitar su divulgación.
- El personal de la Gerencia de Sistemas de Información no utilizará 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 entidad. Se deben hacer copias de seguridad en concordancia con las políticas del proveedor y de la entidad.
- El personal de la Gerencia de Sistemas de 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 ésta 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 por el Jefe inmediato.
- Aquellos servicios y actividades que no son esenciales para el normal funcionamiento de los sistemas de información, deben ser aprobados oficialmente por la entidad.
- El acceso a cualquier servicio, servidor o sistema de información debe ser autenticado y autorizado.
- Todos los servidores deben ser configurados con el mínimo de servicios necesarios y obligatorios para desarrollar las funciones designadas.