PLAN DE SEGURIDAD Y PRIVACIDAD

EMPRESA DE SERVICIOS PUBLICOS DE LA PLATA

EMSERPLA E.S.P.

VIGENCIA 2021

Carrera 3 no. 2-04 La Plata, Huila Colombia
gerencia@emserpla.gov.co
www.emserpla.gov.co
(098) 8370029 - 8470160

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

1- POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

1.1 ALCANCE

1.2 NIVEL DE CUMPLIMIENTO

2. IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

2.1 JUSTIFICACIÓN.

2.2 OBJETIVO.

2.3 ALCANCE.

2.4 ROLES Y RESPONSABILIDADES.

2.5 CUMPLIMIENTO.

2.6 COMUNICACIÓN.

2.7 MONITOREO.

3. DESCRIPCIÓN DE LAS POLÍTICAS

3.1 GESTIÓN DE ACTIVOS.

3.1.1 Política para la identificación, clasificación y control de activos de información.

3.2 CONTROL DE ACCESO.

3.2.1 Política de acceso a redes y recursos de red.

3.2.2 Política de administración de acceso de usuarios.

3.2.3 Políticas de seguridad física.

3.2.4 Política de seguridad para los equipos.

3.2.6 Política de uso adecuado de internet.

4. PRIVACIDAD Y CONFIDENCIALIDAD

4.1 POLÍTICA DE TRATAMIENTO Y PROTECCIÓN DE DATOS.

1- POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

A través del decreto único reglamentario 1078 de 2015, del sector de Tecnologías de Información y las Comunicaciones, define el componente de seguridad y privacidad de la información, como parte integral de la estrategia Gobierno en Línea.

El Modelo de Seguridad y Privacidad de la Información se encuentra alineado con el Marco de Referencia de Arquitectura TI y soporta transversalmente los otros componentes de la Estrategia GEL: TIC para Servicios, TIC para Gobierno Abierto y TIC para Gestión.

La Política de Seguridad y Privacidad de la Información es la declaración general que representa la posición de la Empresa de Servicios Públicos de la Plata (EMSERPLA E.S.P) con respecto a la protección de los activos de información (los funcionarios, contratistas, terceros, la información, los procesos, las tecnologías de información incluido el hardware y el software), que soportan los procesos de la Entidad y apoyan la implementación del Sistema de Gestión de Seguridad de la Información, por medio de la generación y publicación de sus políticas, procedimientos e instructivos, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información.

Las acciones de esta política son acciones encaminadas a:

a) Mitigar los riesgos de la entidad.

b) Cumplir con los principios de seguridad de la información.

c) Cumplir con los principios de la función administrativa.

d) Mantener la confianza de los funcionarios, contratistas y terceros.

e) Apoyar la innovación tecnológica.

f) Implementar el sistema de gestión de seguridad de la información.

g) Proteger los activos de información.

h) Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.

i) Fortalecer la cultura de seguridad de la información en los funcionarios y clientes externos.

j) Garantizar la continuidad del servicio frente a incidentes.

1.1 ALCANCE.

Esta política aplica a toda la entidad, sus funcionarios, contratistas y terceros de la Empresa de Servicios Públicos de la Plata Huila (EMSERPLA E.S.P) y la ciudadanía en general.

1.2 NIVEL DE CUMPLIMIENTO.

Todas las personas cubiertas por el alcance y aplicabilidad deberán dar cumplimiento a esta política. A continuación se establecen las políticas que soportan el plan de seguridad y privacidad de la información de la de la Empresa de Servicios Públicos de la Plata (EMSERPLA E.S.P).

a) Implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, teniendo en cuenta las necesidades de la entidad, y los requerimientos regulatorios que le aplican a su naturaleza.

b) Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, contratistas o terceros.

c) La Empresa de Servicios Públicos de la Plata (EMSERPLA E.S.P) protege la información generada, procesada o resguardada por los procesos de la entidad y activos de información que hacen parte de los mismos.

d) La Empresa de Servicios Públicos de la Plata (EMSERPLA E.S.P) protege la información creada, procesada, transmitida o resguardada por sus procesos de la entidad, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.

e) La Empresa de Servicios Públicos de la Plata (EMSERPLA E.S.P) protege su información de las amenazas originadas por parte del personal.

f) La Empresa de Servicios Públicos de la Plata (EMSERPLA E.S.P) protege las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.

g) La Empresa de Servicios Públicos de la Plata (EMSERPLA E.S.P) controla la operación de sus procesos de la entidad garantizando la seguridad de los recursos tecnológicos y las redes de datos.

h) La Empresa de Servicios Públicos de la Plata (EMSERPLA E.S.P) implementa controles de acceso a la información, sistemas y recursos de red.

i) La Empresa de Servicios Públicos de la Plata (EMSERPLA E.S.P) garantiza que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

j) La Empresa de Servicios Públicos de la Plata (EMSERPLA E.S.P) garantiza a través de una adecuada gestión de los eventos de seguridad y las debilidades

asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.

k) La Empresa de Servicios Públicos de la Plata (EMSERPLA E.S.P) garantiza la disponibilidad de sus procesos de la entidad y la continuidad de su operación basada en el impacto que pueden generar los eventos.

l) La Empresa de Servicios Públicos de la Plata (EMSERPLA E.S.P) garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

2. IMPLEMENTACIÓN DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN.

2.1 JUSTIFICACIÓN.

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

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

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

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

Adicionalmente, debe considerarse los conceptos de:

a) Auditabilidad: define que todos los eventos de un sistema deben poder ser registrados para su control posterior.

b) Protección a la duplicación: consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original.

c) No repudio: se refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.

d) Legalidad: referido al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeto el Organismo.

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

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

g) Tecnología de la Información: se refiere al hardware y software operados la entidad o por un tercero que procese información en su nombre, para llevar a cabo una función propia del Organismo, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.

2.2 OBJETIVO.

Se busca definir los mecanismos y todas las medidas necesarias, tanto técnica, lógica, física, legal y ambiental para la protección de los activos de información, los recursos y la tecnología de la entidad, con el propósito de evitar accesos no autorizados, divulgación, duplicación, interrupción de sistemas, modificación, destrucción, pérdida, robo, o mal uso, que se pueda producir de forma intencional o accidental, frente a amenazas internas o externas, asegurando el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

2.3 ALCANCE.

Este Plan de Seguridad y Privacidad de la Información y su política, son aplicables a todos los funcionarios de La Empresa de Servicios Públicos de la Plata (EMSERPLA E.S.P), a sus recursos, procesos y procedimientos tanto internos como externos, así mismo al personal vinculado a la entidad y terceras partes, que usen activos de información que sean propiedad de la entidad.

2.4 ROLES Y RESPONSABILIDADES.

Es responsabilidad del Comité de Seguridad de la Información la implementación, aplicación, seguimiento y autorizaciones de la política del Plan de Seguridad y

Privacidad de la información en las diferentes áreas y procesos de la entidad, además garantiza el apoyo y el uso de la Política de Seguridad de la Información como parte de su herramienta de gestión, la cual debe ser aplicada de forma obligatoria por todos los funcionarios para el cumplimiento de los objetivos.

- Líder del Proyecto.
- Personal de seguridad de la información.
- Un representante del área de Tecnología.
- Un representante del área de Control Interno.
- Un representante del área de Planeación.
- Un representante de sistemas de Gestión de Calidad.
- Un representante de la Oficina de Almacén General.
- Líder de gestión Documental.
- Funcionarios, proveedores, y ciudadanos.

Una de las tareas principales del líder del proyecto es entregar y dar a conocer los perfiles y responsabilidades de cada personaje al grupo de trabajo e identificar las personas idóneas para tomar cada rol.

Es importante resaltar nuevamente la necesidad del compromiso de la Alta dirección de la entidad, de esta forma se presenta la figura No. 01, en la cual se presentan los perfiles de manera genérica el nivel al cual pertenecerían según lo propuesto.

Figura No. 1 – Equipo de Gestión de Seguridad de la Información en las entidades

Responsabilidades del equipo del proyecto:

- Apoyar al líder de proyecto al interior de la entidad.
- Oficiar como consultores de primer nivel en cuanto a las dudas técnicas y de procedimiento que se puedan suscitar en el desarrollo del proyecto.
- Ayudar al líder de proyecto designado, en la gestión de proveedores de tecnología e infraestructura.
- Asistir a las reuniones de seguimiento o de cualquier otra naturaleza planeadas por el líder de proyecto.
- Las que considere el líder del proyecto o el comité de seguridad de la entidad.

De manera particular se resaltan dos perfiles que deben estar participando de manera activa durante el desarrollo del proyecto, a pesar que el proyecto no es de responsabilidad exclusiva del área de TI su papel es fundamental, y de acuerdo a

la Ley de Protección de Datos Personales se debe tener muy presente el rol de Responsable del tratamiento de los datos personales. Teniendo en cuenta que el responsable del tratamiento de datos personales en la entidad, es quien tiene decisión sobre las bases de datos que contengan este tipo de datos y que el responsable es quien direcciona las actividades de los encargados de los datos personales (quien realiza el tratamiento directamente), como se mencionaba anteriormente, adicional a las responsabilidades arriba citadas se tendrán en cuenta que de acuerdo a la Ley 1581 de 2012 Protección de Datos Personales los deberes y responsabilidades de los responsables y/o encargados del tratamiento de los datos personales son:

- Informar y garantizar el ejercicio de los derechos de los titulares de los datos personales.
- Tramitar las consultas, solicitudes y reclamos.
- Utilizar únicamente los datos personales que hayan sido obtenidos mediante autorización, a menos que los mismos no la requieran.
- Respetar las condiciones de seguridad y privacidad de información del titular.
- Cumplir instrucciones y requerimientos impartidos por la autoridad administrativa competente.

2.5 CUMPLIMIENTO.

El cumplimiento de la Política de Seguridad y Privacidad de la Información es obligatorio. Si los funcionarios de la entidad o terceros violan este plan, la Empresa de Servicios Públicos de la Plata (EMSERPLA E.S.P) se reserva el derecho de tomar las medidas correspondientes.

2.6 COMUNICACIÓN.

Mediante socialización a todos los funcionarios de la se dará a conocer el contenido del documento de las políticas de seguridad, así mismo se deberá informar a los contratistas y/o terceros en el momento que se requiera con el propósito de realizar los ajustes y la retroalimentación necesaria para dar cumplimiento efectivo al plan. Todos los funcionarios, contratistas y/o terceros de la entidad deben conocer la existencia de las políticas, la obligatoriedad de su cumplimiento, la ubicación física del documento estará a cargo del Sistema de Gestión Integrado para que sean consultados en el momento que se requieran, igualmente estarán alojados en la página de la entidad www.emserpla.gov.co.

2.7 MONITOREO.

Se crearán los mecanismos y los indicadores correspondientes a la política de seguridad con el fin de determinar el cumplimiento de las mismas para establecer qué modificaciones o adiciones deben hacerse, este monitoreo debe realizarse como mínimo una vez al año o cuando sea necesario.

3. DESCRIPCIÓN DE LAS POLÍTICAS.

GENERALIDADES.

La Empresa de Servicios Públicos de la Plata (EMSERPLA E.S.P) en todas sus áreas y procesos cuenta con información, reservada, relevante, privilegiada e importante, es decir que esta información es el principal activo de la entidad para el desarrollo de todas sus actividades por lo que se hace necesario y se debe proteger conforme a los criterios y principios de los sistemas de información, como son

integridad, disponibilidad y confidencialidad de la información. De acuerdo a esta Política se divulgan los objetivos y alcances de seguridad de la información de la entidad, que se logran por medio de la aplicación de controles de seguridad, con el fin de mantener y gestionar el riesgo como lo establece la política de riesgos institucional. Este documento tiene el objetivo de garantizar la continuidad de los servicios, minimizar la probabilidad de explotar las amenazas, y asegurar el eficiente cumplimiento de los objetivos institucionales y de las obligaciones legales conforme al ordenamiento jurídico vigente y los requisitos de seguridad destinados a impedir infracciones y violaciones de seguridad.

3.1 GESTIÓN DE ACTIVOS.

3.1.1 Política para la identificación, clasificación y control de activos de información.

El Comité de Seguridad de la Información realizará la supervisión de cada proceso, el cual debe aprobar el inventario de los activos de información que procesa y produce la entidad, estas características del inventario deben establecer la clasificación, valoración, ubicación y acceso de la información, correspondiendo al líder de Gestión Documental brindar herramientas que permitan la administración del inventario por cada área, garantizando la disponibilidad, integridad y confidencialidad de los datos que lo componen.

Para mantener actualizado el inventario de activos de la información se deben tener en cuenta las siguientes consideraciones:

a) Los usuarios deben acatar los lineamientos guía de clasificación de la Información para el acceso, divulgación, almacenamiento, copia, transmisión,

etiquetado y eliminación de la información contenida en los recursos tecnológicos, así como de la información física de la entidad.

b) La información física y digital de La Empresa de Servicios Públicos de la Plata Huila (EMSERPLA E.S.P) debe tener un periodo de almacenamiento que puede ser dictaminado por requerimientos legales o misionales; este período debe ser indicado en las tablas de retención documental y cuando se cumpla el periodo de conservación, se le debe dar el tratamiento de acuerdo a la disposición final definida por la entidad.

c) Los usuarios deben tener en cuenta estas consideraciones cuando impriman, escaneen, saquen copias y envíen faxes: verificar las áreas adyacentes a impresoras, escáneres, fotocopiadoras y máquinas de fax para asegurarse que no quedaron documentos relacionados o adicionales; asimismo, recoger de las impresoras, escáneres, fotocopiadoras y máquinas de fax, inmediatamente los documentos confidenciales para evitar su divulgación no autorizada o mal intencionada.

d) Tanto los funcionarios como el personal provisto por terceras partes deben asegurarse que en el momento de ausentarse de su puesto de trabajo, sus escritorios se encuentren libres de documentos y medios de almacenamiento, utilizados para el desempeño de sus labores; estos deben contar con las protecciones de seguridad necesarias de acuerdo con su nivel de clasificación.

e) La información que se encuentra en documentos físicos debe ser protegida, a través de controles de acceso físico y las condiciones adecuadas de almacenamiento y resguardo.

3.2 CONTROL DE ACCESO.

3.2.1 Política de acceso a redes y recursos de red.

La Oficina de sistemas a través del encargado (Profesional en Ingeniera de Sistemas o de Redes y Seguridad de La Empresa de Servicios Públicos de la Plata (EMSERPLA E.S.P), como responsable de las redes de datos y los recursos de red de la entidad, debe propender porque dichas redes sean debidamente protegidas contra accesos no autorizados a través de mecanismos de control de acceso lógico. Teniendo en cuenta las siguientes acciones:

a) Las redes inalámbricas deben contar con métodos de autenticación que evite accesos no autorizados.

b) Establecer controles para la identificación y autenticación de los usuarios provistos por terceras partes en las redes o recursos de red, así como velar por la aceptación de las responsabilidades de dichos terceros. Además, se debe formalizar la aceptación de las Políticas de Seguridad de la Información por parte de estos.

c) Los funcionarios y personal provisto por terceras partes, antes de contar con acceso lógico por primera vez a la red de datos, deben contar con el formato de creación de cuentas de usuario debidamente autorizado y el acuerdo de Confidencialidad firmado previamente.

d) Los equipos de cómputo de usuario final que se conecten o deseen conectarse a las redes de datos deben cumplir con todos los requisitos o controles para autenticarse en ellas y únicamente podrán realizar las tareas para las que fueron autorizados.

3.2.2 Política de administración de acceso de usuarios.

La Empresa de Servicios Públicos de la Plata (EMSERPLA E.S.P) establecerá privilegios para el control de acceso lógico de cada usuario o grupo de usuarios a las redes de datos, los recursos tecnológicos y los sistemas de información de la Entidad. Así mismo, velará porque los funcionarios y el personal provisto por terceras partes tengan acceso únicamente a la información necesaria para el desarrollo de sus labores y porque la asignación de los derechos de acceso esté regulada por normas establecidas para tal fin.

Teniendo en cuenta lo siguiente:

a) Definir lineamientos para la configuración de contraseñas que aplicarán sobre la plataforma tecnológica, los servicios de red y los sistemas de información; dichos lineamientos deben considerar aspectos como longitud, complejidad, cambio periódico, control histórico, bloqueo por número de intentos fallidos en la autenticación y cambio de contraseña en el primer acceso, entre otros.

b) Establecer un protocolo que asegure la eliminación, reasignación o bloqueo de los privilegios de acceso otorgados sobre los recursos tecnológicos, los servicios de red y los sistemas de información de manera oportuna, cuando los funcionarios se desvinculan, toman licencias, vacaciones, son trasladados o cambian de cargo.

c) Asegurarse que los usuarios o perfiles de usuario que tienen asignados por defecto los diferentes recursos de la plataforma tecnológica sean inhabilitados o eliminados.

3.2.3 Política de control de acceso a sistemas de información y aplicativos.

La Empresa de Servicios Públicos de la Plata (EMSERPLA E.S.P) velara por todos los sistemas de información y aplicativos que apoyan los procesos y áreas, en

cuanto a la asignación, modificación y revocación de privilegios de accesos a sus sistemas o aplicativos de manera controlada. La Oficina de Sistemas, como responsable de la administración de dichos sistemas de información y aplicativos, propende para que estos sean debidamente protegidos contra accesos no autorizados a través de mecanismos de control de acceso lógico. Así mismo, vela porque los administradores y personal de apoyo, tanto internos como externos, acojan buenas prácticas de soporte en los productos generados para controlar el acceso lógico y evitar accesos no autorizados a los sistemas administrados.

a) Los propietarios de los activos de información deben autorizar los accesos a sus sistemas de información o aplicativos, de acuerdo con los perfiles establecidos y las necesidades de uso, acogiendo los procedimientos establecidos.

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

c) Se debe establecer un protocolo para la asignación de accesos a los sistemas y aplicativos.

d) Establecer el protocolo y los controles de acceso a los ambientes de producción de los sistemas de información; así mismo, debe asegurarse que los funcionarios internos o externos, posean acceso limitado y controlado a los datos y archivos que se encuentren en los ambientes de producción.

3.2.4 Políticas de seguridad física.

La Empresa de Servicios Públicos de la Plata (EMSERPLA E.S.P) vela por la efectividad de los mecanismos de seguridad física y control de acceso que aseguren

el perímetro de sus instalaciones en todas sus áreas. Así mismo, controlará las amenazas físicas externas e internas y las condiciones medioambientales de sus oficinas. Todas las áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, se considera áreas de acceso restringido. Se debe tener acceso controlado y restringido a donde se encuentra los servidores y el cuarto de comunicaciones.

Se deben tener en cuenta las siguientes consideraciones:

a) Las solicitudes de acceso al área donde se encuentra el servidor o los centros de cableado deben ser aprobadas por el Gerente(a) de la oficina de EMSERPLA E.S.P; no obstante, los visitantes siempre deberán estar acompañados de un funcionario asignado para el acceso.

b) La Oficina de Sistemas debe asegurar que las labores de mantenimiento de redes eléctricas, de voz y de datos, sean realizadas por personal idóneo y apropiadamente autorizado e identificado

c) La Empresa de Servicios Públicos de la Plata (EMSERPLA E.S.P) debe proveer los recursos necesarios para ayudar a proteger, regular y velar por el perfecto estado de los controles físicos implantados en las sus instalaciones.

d) Se deben identificar mejoras a los mecanismos implantados y de ser necesario, la implementación de nuevos mecanismos, con el fin de proveer la seguridad física de las instalaciones de la entidad.

e) Los ingresos y egresos de personal a las instalaciones de La Empresa de Servicios Públicos de la Plata (EMSERPLA E.S.P) en horarios no laborales deben

ser registrados; por consiguiente, los funcionarios y personal provisto por terceras partes deben cumplir completamente con los controles físicos implantados.

f) Los funcionarios deben portar el carné que los identifica como tales en un lugar visible mientras se encuentren en las instalaciones de La Empresa de Servicios Públicos de la Plata (EMSERPLA E.S.P); en caso de pérdida del carné, deben reportarlo a la mayor brevedad posible al área u oficina correspondiente.

g) Aquellos funcionarios o personal provisto por terceras partes para los que aplique, en razón del servicio prestado, deben utilizar prendas distintivas que faciliten su identificación.

3.2.5 Política de seguridad para los equipos.

Para evitar la pérdida, robo o exposición al peligro de los recursos de la plataforma tecnológica de la entidad que se encuentren dentro o fuera de sus instalaciones, La Empresa de Servicios Públicos de la Plata (EMSERPLA E.S.P) proveerá los recursos que garanticen la mitigación de riesgos sobre dicha plataforma tecnológica.

a) La Oficina de Almacén debe proveer los mecanismos y estrategias necesarios para proteger la confidencialidad, integridad y disponibilidad de los recursos tecnológicos, dentro y fuera de las instalaciones.

b) La Oficina de Sistemas debe establecer las condiciones que deben cumplir los equipos de cómputo que requieran conectarse a la red de datos de la entidad y verificar el cumplimiento de dichas condiciones antes de conceder a estos equipos acceso a los servicios de red.

c) Aplicar lineamientos para la disposición segura de los equipos de cómputo de los funcionarios de la entidad, ya sea cuando son dados de baja o cambian de usuario.

d) La Oficina de Almacén debe velar porque la entrada y salida de estaciones de trabajo, servidores, equipos portátiles y demás recursos tecnológicos institucionales de las instalaciones cuente con la autorización documentada y aprobada previamente por el área.

e) La Oficina de Almacén es la única área autorizada para realizar movimientos y asignaciones de recursos tecnológicos; por consiguiente, se encuentra prohibida la disposición que pueda hacer cualquier funcionario de los recursos tecnológicos de La Empresa de Servicios Públicos de la Plata (EMSERPLA E.S.P).

f) Las estaciones de trabajo, dispositivos móviles y demás recursos tecnológicos asignados a los funcionarios y personal provisto deben acoger las instrucciones técnicas que proporcione la Oficina de Sistemas.

g) Cuando se presente una falla o problema de hardware o software u otro recurso tecnológico propiedad de La Empresa de Servicios Públicos de la Plata (EMSERPLA E.S.P), el usuario responsable debe informar a la Oficina de Sistemas, con el fin de realizar una asistencia adecuada. El usuario no debe intentar solucionar el problema.

h) La instalación, reparación o retiro de cualquier componente de hardware o software de estaciones de trabajo, dispositivos móviles y demás recursos tecnológicos de la entidad, solo puede ser realizado por los funcionarios de apoyo a la oficina de sistemas.

i) Los equipos de cómputo, bajo ninguna circunstancia, no deben ser dejados desatendidos en lugares públicos o a la vista, en el caso de que estén siendo transportados.

j) Los equipos de cómputo deben ser transportados con las medidas de seguridad apropiadas, que garanticen su integridad física.

k) Los equipos portátiles siempre deben ser llevados como equipaje de mano y se debe tener especial cuidado de no exponerlos a fuertes campos electromagnéticos.

l) En caso de pérdida o robo de un equipo de cómputo, se debe informar de forma inmediata al líder del proceso de la Oficina de Almacén, para que se inicie el trámite interno y se debe poner la denuncia ante la autoridad competente.

3.2.6 Política de uso adecuado de internet.

El servicio de Internet es una herramienta para el desempeño de labores, La Empresa de Servicios Públicos de la Plata (EMSERPLA E.S.P) proporcionará los recursos necesarios para asegurar su disponibilidad a los usuarios que así lo requieran para el desarrollo de sus actividades diarias en la entidad. De acuerdo a ello la Oficina de Sistemas en coordinación con el proveedor de este servicio debe proporcionar los recursos necesarios para la implementación, administración y mantenimiento requeridos para la prestación segura del mismo, bajo las restricciones de los perfiles de acceso establecidos.

Se deben tener en cuenta todos los mecanismos que permitan la continuidad o restablecimiento del servicio de Internet en caso de contingencia interna, así como el monitoreo continuo del canal o canales del servicio de Internet.

Para el control de acceso y uso de adecuado del servicio de internet, la Oficina de Sistemas debe realizar las siguientes acciones:

- implementar controles para evitar la descarga de software no autorizado, evitar código malicioso proveniente de Internet y evitar el acceso a sitios catalogados como restringidos.
- Generar registros de la navegación y los accesos de los usuarios a Internet, así como establecer e implantar el monitoreo sobre la utilización del servicio de Internet.
- Los usuarios del servicio de Internet de La Empresa de Servicios Públicos de la Plata (EMSERPLA E.S.P) deben hacer uso del mismo en relación con las actividades laborales que así lo requieran.
- Los usuarios del servicio de Internet deben evitar la descarga de software desde internet, así como su instalación en las estaciones de trabajo o dispositivos móviles asignados para el desempeño de sus labores.
- No está permitido el acceso a páginas relacionadas con pornografía, drogas, alcohol, webproxys, hacking y/o cualquier otra página que vaya en contra de la ética moral, las leyes vigentes o políticas establecidas en este documento.
- El uso de redes sociales como Facebook, instagram, twiter entre otras, debe corresponder a labores propias de La Empresa de Servicios Públicos de la Plata (EMSERPLA E.S.P) y estas serán limitadas cuando se observe una utilización desmedida y contraproducente con las actividades diarias de los funcionarios en el horario laboral establecido.
- No está permitido la descarga, uso, intercambio y/o instalación de juegos, música, películas, protectores y fondos de pantalla, software de libre distribución, información y/o productos que de alguna forma atenten contra la propiedad

intelectual de sus autores, o que contengan archivos ejecutables y/o herramientas que atenten contra la integridad, disponibilidad y/o confidencialidad de la infraestructura tecnológica (hacking), entre otros.

- La descarga, uso, intercambio y/o instalación de información audiovisual (videos e imágenes) utilizando sitios públicos en Internet debe ser autorizada por el funcionario responsable de la Oficina de Sistemas.
- No está permitido el intercambio no autorizado de información de propiedad La Empresa de Servicios Públicos de la Plata (EMSERPLA E.S.P), de los funcionarios, con terceros.

4. PRIVACIDAD Y CONFIDENCIALIDAD.

4.1 Política de tratamiento y protección de datos.

En cumplimiento de la de Ley 1581 de 2012 y reglamentada parcialmente por el Decreto Nacional 1377 de 2013, por la cual se dictan disposiciones para la protección de datos personales, La Empresa de Servicios Públicos de la Plata (EMSERPLA E.S.P) a través del Comité de Seguridad de la Información, propende por la protección de los datos personales de sus beneficiarios, proveedores y demás terceros de los cuales reciba y administre información. Se establece los términos, condiciones y finalidades para las cuales La Empresa de Servicios Públicos de la Plata (EMSERPLA E.S.P) como responsable de los datos personales obtenidos a través de sus distintos canales de atención, tratará la información de todas las personas que en algún momento, por razones de la actividad que desarrolla la entidad, hayan suministrado datos personales. En caso de delegar a un tercero el tratamiento de datos personales, se exigirá al tercero la implementación de los lineamientos y procedimientos necesarios para la protección de los datos

personales. Así mismo, se busca proteger la privacidad de la información personal de sus funcionarios, estableciendo los controles necesarios para preservar aquella información que la entidad conozca y almacene de ellos, velando porque dicha información sea utilizada únicamente para funciones propias de la entidad y no sea publicada, revelada o entregada a funcionarios o terceras partes sin autorización.

La Empresa de Servicios Públicos de la Plata (EMSERPLA E.S.P) aplicara las siguientes políticas para la protección de datos personales:

- Las Oficinas que recepcionen o procesan datos personales de beneficiarios, funcionarios, proveedores u otras terceras partes deben obtener la autorización para el tratamiento de estos datos con el fin de recolectar, transferir, almacenar, usar, circular, suprimir, compartir, actualizar y transmitir dichos datos personales en el desarrollo de las actividades de la entidad.
- Las Oficinas que recepcionen o procesan datos personales de beneficiarios, funcionarios, proveedores u otras terceras partes deben asegurar que solo aquellas personas que tengan una necesidad laboral legítima puedan tener acceso a dichos datos.
- Las Oficinas que recepcionen o procesen datos personales de beneficiarios, funcionarios, proveedores u otras terceras partes deben establecer condiciones contractuales y de seguridad a las entidades vinculadas o aliadas delegadas para el tratamiento de dichos datos personales.
- Las oficinas que procesan datos personales de beneficiarios, funcionarios, proveedores u otras terceras partes deben acoger las directrices técnicas y procedimientos establecidos para el intercambio de estos datos con los terceros delegados para el tratamiento de dichos datos personales.

- Las oficinas que procesan datos personales de beneficiarios, proveedores u otras terceras partes deben acoger las directrices técnicas y procedimientos establecidos para enviar a los beneficiarios, proveedores u otros terceros mensajes, a través de correo electrónico y/o mensajes de texto.
- El comité de seguridad de la información debe establecer los controles para el tratamiento y protección de los datos personales de los beneficiarios, funcionarios, proveedores y demás terceros de La Empresa de Servicios Públicos de la Plata (EMSERPLA E.S.P) de los cuales reciba y administre información.
- El comité de seguridad debe establecer todos los controles necesarios para proteger la información personal de los beneficiarios, funcionarios, proveedores u otras terceras partes almacenada en bases de datos o cualquier otro repositorio y evitar su divulgación, alteración o eliminación sin la autorización requerida.
- Los usuarios y funcionarios deben guardar la discreción correspondiente, o la reserva absoluta con respecto a la información de la entidad o de sus funcionarios de cual tengan conocimiento en el ejercicio de sus funciones.

ANDRES EDUARDO HERNANDEZ TEJADA
Gerente

Elaboro: Jhon Faiber Cerquera Sánchez
Ingeniero de Sistemas
Fecha: 27-01-2021