Lineamientos de Seguridad de la Información

Seguridad de la Información y Ciberseguridad

Abril, 2024

Versión 1.0

Contenido

1. Control de Cambios y Versiones

La siguiente tabla lleva control del control de versiones de la Política de Seguridad de la Información:

Revisión	Fecha	Descripción
1.0	10 abril de 2024	Desarrollo y aprobación de los Lineamientos de Seguridad.

Las siguientes personas participaron en la elaboración de la Política de Seguridad de la Información:

Elaborado por:	Responsable	Fecha

Revisado por:	Responsable	Fecha
Evelyn Villalobos Aguilar		18-04-2024

Aprobado por:	Responsable	Fecha	Firma

La Política de Seguridad de Información fue comunicada y se encuentra publicada en el siguiente link corporativo:

Ubicación del Documento

2. Propósito de los Lineamientos de Seguridad

ASEJUPS al comprender que la ciberseguridad y seguridad de la información debe ser tomada como un riesgo del negocio para asegurar la continuidad de los servicios y soluciones tecnológicas que ofrece, establece los siguientes requisitos y responsabilidades de seguridad de la información, con el fin de alinear todos los esfuerzos, procesos y tecnología para proteger y asegurar la Confidencialidad, Integridad y Disponibilidad de la información de sus clientes, de los servicios que presta y del aseguramiento de la infraestructura tecnológica.

Por lo tanto, en los presentes Lineamientos de Seguridad se establecen las directrices específicas para garantizar que todos los colaboradores, usuarios, interesados, clientes u otro tercero, realicen un adecuado uso de los servicios que ASEJUPS brinda, así como, las directrices sobre el tratamiento y gestión de la seguridad de la información que la compañía gestione en la prestación de sus servicios.

3. Glosario

Nombre/Siglas	Definición
Activo	Aquello que tiene valor para la organización. Hay muchos tipos de activos, incluyendo: información, software, hardware, servicios, personas e intangibles.
Amenaza	Causa potencial de un incidente no deseado, que puede ocasionar daños a un sistema u organización. (INTE/ISO/IEC 27000:2018).
Confidencialidad	Propiedad de que la información no esté disponible o divulgada a individuos, entidades o procesos no autorizados. (INTE/ISO/IEC 27000:2018).
Continuidad del Negocio	Procesos Capacidad de la organización para continuar suministrando productos o servicios a niveles predefinidos aceptables, posterior a un incidente disruptivo. (INTE/ISO 22301:2015).
Control/Controles	Medida que modifica un riesgo. (INTE/ISO/IEC 27000:2018).

Disponibilidad	Propiedad de ser accesible y utilizable bajo demanda por una entidad autorizada. (INTE/ISO/IEC 27000:2018).
Gobernanza de Seguridad de la Información	Sistema por el cual son dirigidas y controladas las actividades de seguridad de la información de una organización. (INTE/ISO/IEC 27000:2018).
Información	Interpretación que se da a un conjunto de datos, pudiendo residir en medios electromagnéticos, físicos o en el conocimiento de las personas.
Integridad	Propiedad de exactitud y completitud. (INTE/ISO/IEC 27000:2018).
Política	Intenciones y dirección de una organización expresada formalmente por la Alta Dirección. (INTE/ISO/IEC 27000:2018).
Riesgo	Resultado de la incertidumbre sobre los objetivos. (INTE/ISO/IEC 27000:2018).
Seguridad de la Información	Preservación de la confidencialidad, integridad y disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, rendición de cuentas, no repudio y confiabilidad. (INTE/ISO/IEC 27000:2018).
Trazabilidad	Capacidad para seguir el histórico, la aplicación o la localización de un objeto (ISO 9000:2015)
Vulnerabilidad	Debilidad de un activo o control que puede ser explotada por una o más amenazas.

4. Marco Regulatorio

Los siguientes son los marcos, regulaciones, normativas o elementos que aplican a la política:

- Ley N°1 Constitución Política.
- Ley N°2 Código de Trabajo.
- Ley N°4573 Código Penal.

- Ley N°8968 Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales y su reglamento.
- Ley # 7975 Ley de Información No Divulgada.
- Reforma de la Sección VIII, Delitos Informáticos y Conexos, del Título VII del Código Penal.
- Política de Seguridad y Privacidad de Información.

5. Objetivos de la Política

Objetivo General

Definir los lineamientos y directrices que rigen la manera en que los colaboradores, clientes, proveedores, terceros y socios de negocio de ASEJUPS deben seguir para gestionar la información, servicios e infraestructura que se utilice, con el fin de proteger la integridad, disponibilidad y confidencialidad de la información de negocio, de los colaboradores y de los clientes de la empresa.

Objetivo Específicos

- Establecer las responsabilidades y lineamientos específicos de las áreas internas, externas y clientes relacionados a la seguridad de la información.
- Definir los criterios de uso adecuados, confidencialidad, integridad y disponibilidad aplicables a la información, infraestructura y servicios que brinda ASEJUPS
- Gestionar los riesgos de ciberseguridad sobre los activos de información y tecnológicos de ASEJUPS

6. Alcance de la Política

Estos lineamientos aplican y son de acatamiento obligatorio para todo el personal de ASEJUPS, a todos los activos informáticos de la compañía, así como, a todos los procesos, actividades de negocio y servicios que presta la organización.

La política cubre toda la información corporativa, la información sensible de sus colaboradores, así como, la información que se gestione de los clientes de forma

impresa o escrita ya sea en papel, almacenada electrónicamente, trasmitida por correo o usando algún otro medio electrónico.

Por lo tanto, es responsabilidad de todos los colaboradores de ASEJUPS, proveedores y clientes cuando corresponda, conocer, cumplir y hacer valer las disposiciones que se establezcan en estos lineamientos y los controles que deriven de estos.

7. Roles y Responsabilidades

El siguiente apartado establecen las responsabilidades establecidas por ASEJUPS para todos los grupos internos de trabajo:

Gerencia

- Promover en la organización las funciones y responsabilidades en el ámbito de seguridad de la información.
- Facilitar los recursos adecuados para alcanzar los objetivos de seguridad de la información.
- Impulsar la divulgación y la concienciación de los lineamientos de Privacidad y Seguridad de la Información.
- Exigir el cumplimiento de la Política, de la legislación vigente y de los requisitos de los reguladores en el ámbito de la seguridad de la información.
- Impulsar y fortalecer activamente los principios y objetivos de la Seguridad de la Información.
- Considerar los riesgos de seguridad de la información en la toma de decisiones.
- Desarrollar y ejecutar un plan de mejora continua con el fin de asegurar una adecuada gestión de la seguridad de la información.
- Conocer y aplicar los lineamientos de seguridad de la información definidos.
- Asignar los recursos, la infraestructura física y el personal necesario para la gestión de la seguridad de la información.
- Verificar el cumplimiento de la política de seguridad de la información y los lineamientos de seguridad que se generen a partir de esta política.
- Liderar la generación de lineamientos para gestionar la seguridad de la información y el establecimiento de controles técnicos, físicos y administrativos de protección.

- Validar y monitorear de manera periódica la implantación de los controles de seguridad establecidos.
- Asegurar el cumplimiento de la privacidad de datos confidenciales de clientes, proveedores, colaboradores y de información corporativa.
- Conocer y aplicar los lineamientos de seguridad de la información definidos.
- Planear y ejecutar las auditorías internas a fin de determinar si las políticas, procesos, procedimientos y controles establecidos están conformes con los requerimientos institucionales, requerimientos de seguridad, regulaciones y procedimientos aplicables.
- Brindar soluciones que apoyen a la protección, detección y respuesta a los riesgos y a las amenazas de ciberseguridad, a las que se encuentren expuesta la organización, por lo que, deberán afinar los sistemas, infraestructura y procesos, para asegurar la protección de la información de la Corporación y sus servicios.
- Realizar la gestión de riesgos sobre activos de información que no son parte de la infraestructura tecnológica.
- Gestionar riesgos en procesos o actividades específicas de la organización.
- Aprobar y realizar seguimiento a los controles implementados y a los planes de acción para la mitigación de riesgos.
- Llevar a cabo el procedimiento para la gestión de incidentes de seguridad de la información.
- Detectar y analizar los eventos de ciberseguridad que puedan estar afectando la información o los servicios que presta la organización.
- Afinar los Sistemas, infraestructura y procesos constantemente en conjunto con el área de Tecnologías de la Información, para asegurar la protección de la información de la Corporación y sus servicios.
- Desarrollar y ejecutar los planes de respuesta a incidentes de seguridad de la información.
- Implementar los controles, operación e indicadores de cumplimiento de los lineamientos de seguridad de la información definidos.
- Fungir como custodio de la información en conjunto con la Dirección de Tecnologías de la Información.

Colaboradores

- Apoyar la gestión de riesgos en los activos de información a los que tienen acceso y que utilizan.
- Informar de la necesidad de gestionar riesgos sobre los activos de información que tienen a su alcance.
- Informar oportunamente sobre algún evento, amenaza o incidente de seguridad que se presente.
- Cumplir con las directrices que se establecen en los lineamientos establecidos.

Clientes, Proveedores y Terceros

- Clientes, proveedores, fabricantes, socios u otro tercero que tenga acceso a información de la organización, deberán alinearse con las directrices que les correspondan acorde a los lineamientos definidos.

8. Lineamientos de Seguridad de la Información

ASEJUPS a través de la Gerencia establece que los activos de información e infraestructura estratégica son vitales para alcanzar las metas comerciales y lograr los objetivos de negocio, por lo que, con los siguientes lineamientos se establecen las directrices específicas que apoyan a alcanzar los objetivos de seguridad definidos en la política de seguridad de la información para proteger la información corporativa, la información de sus clientes, la información de sus proveedores y la información de sus colaboradores.

Esto define que ASEJUPS mantendrá los esfuerzos necesarios para preservar la privacidad y seguridad de la información de los servicios que brinda, de la infraestructura que utiliza para hacer posible el funcionamiento de estos y de los datos que se gestionen tanto internos como externos de los clientes.

Así mismo, se compromete a establecer una gestión de riesgos de ciberseguridad para la toma de decisiones y definición de controles a implementar, así como, el mejorar continuamente los procesos y conocimientos del personal para aumentar de forma integral la postura de protección y resiliencia cibernética.

Por lo tanto y a continuación, se establecen los siguientes lineamientos de seguridad, que regirán la manera en cómo se dará protección a la información del negocio, de sus colaboradores, clientes y proveedores.:

9.1 Lineamiento de Clasificación de Roles de la Información

La información se ha convertido en uno de los activos más importantes, por lo que, ASEJUPS define los siguientes roles a distribuirse en los colaboradores sin importar su función o método de contratación, para velar por la seguridad de los datos:

9.1.1 Dueño de la Información

ASEJUPS es el dueño de toda la información que es generada por los funcionarios, contratistas o terceros en beneficio y desarrollo de las actividades propias de la empresa, a excepción de la información personal de sus Colaboradores y Asociados, por lo que, velará por el cumplimiento de los siguientes lineamientos:

1. ASEJUPS deberá monitorear el cumplimiento a los lineamientos establecidos y la protección de la información personal de sus Colaboradores y Asociados que tenga acceso.

2. La Gerencia General como representantes de ASEJUPS, será la encargada de aprobar los roles de información que se establezcan en la Organización, así como, aprobar los controles de seguridad que se vayan a aplicar sobre los mismos.

3. La Gerencia General como representantes de ASEJUPS, realizará la gestión requerida para que cada área asigne los recursos necesarios para la implementación de los controles definidos.

4. La Gerencia General como representantes de ASEJUPS, será la responsable de cumplir con los roles y responsabilidades establecidas para el Dueño de la Información.

5. La Gerencia General será el enlace para entidades externas, judiciales o legales.

9.1.2 Custodios de la Información

Los custodios de la información son los colaboradores, áreas de negocio o proveedores responsables de aplicar las medidas de seguridad establecidas por los Responsables de la Información, para la protección adecuada de la confidencialidad, integridad y disponibilidad de cada unidad de negocio. Las responsabilidades del custodio son:

1. Comunicación permanente con el Responsable de la Información respectivo para reportes de los resultados de la aplicación de los controles.

2. Responsable de la administración diaria de la seguridad en los sistemas de información y el monitoreo del cumplimiento de los lineamientos de seguridad en los sistemas que se encuentran bajo su administración.

3. Administrar el acceso a nivel de red, base de datos, respaldos, accesos físicos o lógicos de la información que custodia según lo definido por el Responsable de la Información.

4. Desarrollar los procedimientos de autorización y autenticación, en conjunto con el Responsable de la Información.

5. Monitorear el cumplimiento de la política y lineamientos de seguridad en los activos de información que custodia.

6. Asistir y administrar los procedimientos de backup, recuperación y plan de continuidad de sistemas de información utilizados por ASEJUPS

7. Reportar de forma inmediato a los Responsables de la Información los incidentes de seguridad de la información que se presenten.

8. Efectuar la eliminación segura de la información, a través de los mecanismos necesarios en la plataforma tecnológica, ya sea cuando son dados de baja o cambian de usuario.

9. Los custodios de información son los proveedores que brinden servicios de tecnologías de información, asistentes administrativas, personas que custodien información de forma física o virtual en sus dispositivos, sistemas de información u otra plataforma.

9.1.3 Usuarios de la Información

Los usuarios de la información son los colaboradores, áreas de negocio, proveedores o asociados que tienen acceso o interactúan con la información de ASEJUPS, según lo necesario para su labor o actividad comercial. Las responsabilidades de los usuarios de información son:

1. Mantener la confidencialidad, integridad y disponibilidad de la información y servicios a los que tenga acceso.

2. Utilizar la información e infraestructura tecnológica de ASEJUPS únicamente para los propósitos autorizados.

3. Verificar el cumplimiento de la política de seguridad de la información y los lineamientos de seguridad que se generen a partir de esta política.

4. Liderar la generación de lineamientos para gestionar la seguridad de la información de ASEJUPS y el establecimiento de controles técnicos, físicos y administrativos de protección.

5. Validar y monitorear de manera periódica la implantación de los controles de seguridad establecidos.

6. Acatar los lineamientos de la 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.

9.2 Lineamiento de Clasificación de la Información

ASEJUPS consiente de la necesidad de asegurar que la información reciba el nivel de protección apropiado, define las siguientes reglas de como clasificar la información.

El Responsable de la Información será el encargado de la clasificación de esta, la cual deberá ser documentada y seguir la siguiente metodología:

9.2.1 Identificar las Fuentes de Información

Es necesario conocer a la perfección de qué tipo de información se gestiona en ASEJUPS, así como, quién es el responsable de esta para poder darle protección según su clasificación. Para esto, la información puede existir en distintos formatos y medios, como, por ejemplo:

- Los documentos de carácter electrónico o documentos en formato papel.
- Bases de datos.
- Correos electrónicos.

Por lo que, se debe contar con un inventariado de información antes de poder clasificar y agrupar la misma para aplicarle medidas de seguridad.

Es por esta razón que ASEJUPS, ha establecido la siguiente plantilla que deberá ser utilizada por los Responsables de la Información para identificar cada fuente y tipos de información que se gestionan en sus unidades de negocio, para posteriormente clasificarla:

- Plantilla de Clasificación de la Información.

9.2.2 Clasificar la Información Identificada

La información se clasificará acorde a tres criterios de acceso, basados en el atributo de confidencialidad. La clasificación de la información puede ser:

Clasificación	Definición	Ejemplos	Posibles Impactos
Confidencial	Información que debe únicamente tener acceso por los interesados reales, aprobados y autorizados para tener acceso a la misma, ya que es crítica para nuestro negocio, otras empresas pueden estar interesadas en esta, protegida por legislación o porque nos hemos comprometido a resguardar la misma	**Información Organizacional:** - Estados Financieros. - Diseño de los Proyectos. - Informes de Instalación. **Información Personal (Colaborador/Cliente):** - Datos Médicos. - Fines Políticos, Religiosos, Sexuales, Biológicos. - Firma Electrónica. - Controles Biométricos.	**Información Organizacional:** - Pérdidas Financieras. - Daño Imagen o Reputación. - Pérdidas de Clientes. - Pérdidas de Oportunidades de Negocio. - Aspectos Legales. **Información Personal (Colaborador/Cliente):** - Aspectos Legales. - Discriminación.

Clasificación	Definición	Ejemplos	Posibles Impactos
Privada	Información pertenece al ámbito propio, particular y privado o semiprivado de una persona o de la Organización, por lo que, su acceso se considerará como la información que se dispone en cada uno de los departamentos y que es del conocimiento del personal que labora en estos o para personas específicas que pueden tener acceso.	**Información Organizacional:** - Correos electrónicos. - Propuestas de Servicios. - Facturas y Pagos. - Comunicados Internos. - Minutas. - Planes de Gestión de Proyecto. **Información Personal (Colaborador/Cliente):** - Créditos e Hipotecas. - Seguros. - Datos Bancarios. - Información Salarial - Teléfono Celular - Dirección Física de Vivienda.	**Información Organizacional:** - Daño Imagen o Reputación. - Aspectos Legales. **Información Personal (Colaborador/Cliente):** - Aspectos Legales. - Discriminación.

Clasificación	Definición	Ejemplos	Posibles Impactos
Pública	Información que puede ser accesible sin restricción, ya que la misma ha sido declarada de forma explícita como pública o provenga de fuentes de información pública que puedan tener acceso sin ningún tipo de restricción	**Información Organizacional:** - Comunicados Públicos Organizacionales. - Campañas de Mercadeo Públicas. - Puntos de Contacto Establecidos y Acordados. - Información del Sitio Web. **Información Personal (Colaborador/Cliente):** - Cédula de Identidad. - Nombre. - Estado Civil. - Fecha de Nacimiento. - Firma.	**Información Organizacional:** - Ninguno. **Información Personal (Colaborador/Cliente):** - Ninguno.

9.2.3 Medidas de Protección Acorde a la Clasificación de la Información

En este paso las medidas de protección son aplicados a los tipos de información, con el objetivo de asegurar que las medidas de protección son apropiadas según el nivel de criticidad.

Clasificación	Autenticación	Acceso Basado en Roles	Controles Administrativos	
Confidencial	Cualquier acceso a información confidencial debe estar precedido por una autorización por parte del Responsable de la Información, para lo cual por medio del usuario y contraseña de dominio se brindará acceso a los contenedores de la información (base de datos, carpetas compartidas, equipos de cómputo, correo electrónico).	El acceso a la información se brindará conforme al grado de acceso que deba tener para la ejecución de sus actividades, por lo que se deberá brindar acceso por roles y mínimo privilegio a la información confidencial, asegurando que tenga acceso (total o un extracto de esta) únicamente a la persona o área que corresponda.	- El Responsable de la Información será el encargado de implementar los controles administrativos necesarios para la protección. - Todo documento, carpeta, y otros medios de almacenamiento que contienen información sensitiva, restringida o confidencial debe ser ubicada en áreas protegidas. - Los medios de almacenamiento de información que contienen información sensitiva, restringida o confidencial debe ser guardada en un área segura a final de cada día laborable. - Todas las computadoras deben ser aseguradas cuando el área de trabajo está desocupada o desatendida. - Todos los colaboradores que tengan acceso a información confidencial deberán asegurar el envío y recepción de usuarios autorizados únicamente.	- La información Confidencial únicamente puede ser enviada o utilizada en equipos de cómputo de la organización y por el correo electrónico institucional, no permitiendo su uso por medio de dispositivos USB, discos duros externos, contenedores de datos públicos como Dropbox o OneDrive. - Se brindará un usuario y contraseña de dominio a cada colaborador para que tenga acceso autenticado a este tipo de información. - Como medida de seguridad, los documentos de ofimática deberán ser convertidos a PDF y asignar una contraseña a los mismos cuando la información sea confidencial.

Clasificación	Autenticación	Acceso Basado en Roles	Controles Administrativos	
Privada	Cualquier acceso a información privada debe estar precedido por una autorización por parte del Responsable de la Información, para lo cual por medio del usuario y contraseña de dominio se brindará acceso a los contenedores de la información (base de datos, carpetas compartidas, equipos de cómputo, correo electrónico)	El acceso a la información se brindará conforme al grado de acceso que deba tener para la ejecución de sus actividades, por lo que se deberá brindar acceso por roles y mínimo privilegio a la información confidencial, asegurando que tenga acceso (total o un extracto de esta) únicamente a la persona o área que corresponda.	- El Responsable de la Información será el encargado de implementar los controles administrativos necesarios para la protección de la información privada. - Todo documento, carpeta, y otros medios de almacenamiento que contienen información privada, debe ser ubicada en áreas restringidas. - Los medios de almacenamiento de información que contienen información privada restringida o confidencial debe ser guardada en un área segura a final de cada día laborable.	- La información Privada únicamente puede ser enviada o utilizada en equipos de cómputo de la organización y por el correo electrónico institucional, así como por medio de dispositivos USB, discos duros externos, no se permite el uso de contenedores de datos públicos como Dropbox o OneDrive.

Clasificación	Autenticación	Acceso Basado en Roles	Controles Administrativos	

Pública	Cualquier acceso a información confidencial debe estar precedido por una autorización por parte del Responsable de la Información, para lo cual por medio del usuario y contraseña de dominio se brindará acceso a los contenedores de la información (base de datos, carpetas compartidas, equipos de cómputo, correo electrónico)	El acceso a la información es público, por lo que cualquier persona o área puede visualizar la misma.	- El Responsable de la Información será el encargado de implementar los controles administrativos necesarios para brindar adecuadamente la información pública.	- Brindar disponibilidad de la información declarada como pública

9.3 Lineamiento de Protección de Información Sensible de Asociados JPS

ASEJUPS orientará sus esfuerzos a la preservación de la confidencialidad, integridad, disponibilidad de la información que se acceda, cree o gestione de sus clientes.

Por lo tanto, debido a la importancia y sensibilidad de la información de clientes que ASEJUPS puede tener acceso, crear o almacenar es que se establecen las siguientes directrices que regirán la manera en cómo se dará protección a esta información en particular:

1. ASEJUPS se compromete a establecer, gestionar, revisar y mejorar continuamente la seguridad de la información sensible que tenga acceso, almacene o cree de sus clientes.

2. ASEJUPS se compromete a salvaguardar la información que genera en la ejecución de sus funciones o la que le es entregada en custodia por usuarios dentro de la ejecución de los trámites de la Organización, identificando y mitigando los riesgos asociados mediante la definición de lineamientos y directrices a las dependencias, funcionarios, contratistas y terceros que tenga interacción con esta información.

3. Toda la información que es generada por los funcionarios, contratistas o terceros en beneficio, desarrollo o prestación de un servicio debe ser analizada, para aplicar los mecanismos de control necesarios para su protección.

4. Documentos o salidas de procesos internos que registren o detallen elementos de configuración o características de la arquitectura del cliente, que pueda ser utilizada por un tercero malicioso para afectar servicios, comprometer información o afectar disponibilidad de la solución o servicio prestado, deben ser resguardada y protegida, por lo que, elementos como los siguientes deben aplicarse los controles definidos en los presentes lineamientos:

a. Diseño de soluciones con información sensible como direcciones IP, puertos, entre otros.

b. Arquitectura de equipos y servicios que permitan identificar vulnerabilidades que no sean de carácter público, como sistema operativo, versión de software, entre otros.

c. Informes de configuración actual de elementos de infraestructura del cliente.

d. Informes de instalación y configuración.

e. Consultas legales o multas que no sean de carácter público.

f. Informes de afectación como impactos o consecuencias de un incidente de seguridad de la información que pueda dañar la imagen de los clientes.

g. Disputas contractuales que no sean de carácter público.

h. Cuentas de acceso (usuarios y contraseñas) para brindar soporte o servicio administrado.

i. Entre otras salidas de los procesos de negocio y operativo que brinde información que por su naturaleza pueda afectar la imagen del cliente, servicio brindado o compromiso de los elementos de la solución brindada por mal manejo de ASEJUPS

5. ASEJUPS protegerá la información sensible de los clientes creada, procesada, transmitida o resguardada por los procesos de su competencia y su infraestructura tecnológica.

6. Las responsabilidades frente a la seguridad de la información de ASEJUPS serán definidas, compartidas, publicadas y aceptadas por cada uno de los funcionarios, contratistas, proveedores o clientes.

7. Los colaboradores deben proteger la información sensible de los clientes creada, procesada, transmitida o resguardada por sus procesos de operación, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta.

8. Los Colaboradores deben controlar la operación de sus actividades, garantizando la seguridad de los recursos tecnológicos e información de los clientes que tengan acceso.

9. El acceso a la información se va a autorizar, restringir y delimitar de acuerdo con los roles y responsabilidades que los usuarios tengan dentro de la organización y los que el cliente solicite.

10. Los Colaboradores deben gestionar adecuadamente la Información de los clientes de ASEJUPS y rendir cuentas por su mal uso, mientras que este bajo su custodia, uso o gestión.

11. La información sensible catalogada en el punto 9.3 debe aplicar los siguientes controles:

    a. No se puede transmitir en texto claro, sin ningún control por vías comunes o riesgosas de acceso no autorizado, como por ejemplo correo electrónico, chats de WhatsApp, entre otros.

    b. Al almacenarse deben considerar estar accesibles únicamente a las personas que por su rol deba tener acceso. Además, este acceso debe tener configurado al menos con una contraseña para evitar un acceso sin autorización. Ejemplo, un documento o informe cifrado o que pida una contraseña para accederlo.

    c. Esta protección de cifrado o acceso por medio de una contraseña deberá considerarse durante todo el ciclo de vida de la información, es decir, desde que se está creando el documento, durante la presentación o envió de revisiones y control de cambios, así como, entrega oficial, respaldo de información y custodia de esta.

    d. No se puede compartir la contraseña de acceso por medios inseguros, como por ejemplo correos electrónicos, chats de aplicaciones públicas, equipos de cómputo o redes públicos como restaurantes, hoteles, entre otros.

12. Los colaboradores deben informar a sus superiores sobre la violación de las políticas de seguridad establecidas o si conocen de alguna falla en alguna de ellas, así como, reportar los incidentes de seguridad, eventos sospechosos y el mal uso de los recursos que identifique.

13. Los Colaboradores y terceros deben proteger los datos almacenados, los equipos de cómputo y Sistemas de información a su disposición de la destrucción, alteración intencional o no justificada.

14. Aceptar y reconocer que en cualquier momento y sin previo aviso, la Gerencia de ASEJUPS puede solicitar una inspección de la información a su cargo sin importar su ubicación o medio de almacenamiento. Esto incluye todos los datos

y archivos en recursos de la empresa, sitios web, computadoras, servidores u otros medios de almacenamiento propios de la compañía. Esta revisión puede ser requerida para asegurar el cumplimiento de las políticas internamente definidas, por actividades de auditoría y control interno o en el caso de requerimientos de entes fiscalizadores y de vigilancia externos, legales o gubernamentales.

15. Todos los Colaboradores y terceros deben proteger y resguardar su información personal que no esté relacionada con sus funciones en ASEJUPS. La Organización no es responsable por la pérdida de información, fraude o daño que pueda tener un usuario al brindar información personal como identificación de usuarios, claves, números de cuentas o números de tarjetas débito/crédito, entre otros.

9.4 Lineamiento para la Gestión de Usuarios y Control de Acceso

Los siguientes lineamientos exponen las condiciones, normas y procedimientos necesarios para fijar los requisitos que se deben cumplir por cualquier funcionario, contratista o cliente de ASEJUPS, para obtener acceso a los sistemas de información, hardware y software propiedad de la Organización:

1. Todos los colaboradores deben utilizar solamente la información necesaria para llevar a cabo las funciones que le fueron asignadas, de acuerdo con los permisos establecidos o aprobados por el Responsable de la Información.

2. Todos los colaboradores deben proteger la información a la cual accedan y procesen, para evitar su pérdida, alteración, destrucción o uso indebido.

3. Todos los colaboradores deben proteger los datos almacenados en los equipos de cómputo y sistemas de información a su disposición de la destrucción o alteración intencional o no justificada y de la divulgación no autorizada.

4. Las redes de telecomunicaciones (cableadas e inalámbricas) deben contar con cuentas de acceso y contraseñas individualizadas, por lo que, para el acceso a estas deben de realizarse por medio de las credenciales de dominio de ASEJUPS

5. Los Responsables de la Información deben autorizar la creación, modificación o eliminación de las cuentas de acceso a las redes o recursos de red de su unidad de negocio u otro usuario que tenga acceso a la información que gestionan. Para la creación de cuentas se utilizará el siguiente formato:

    - Primera letra del nombre del colaborador, más su primer apellido. Quedando por ejemplo para Ana González el usuario interno sería “AGONZALEZ”.

- En el caso que ya exista una combinación con el mismo nombre de colaborador, se debe agregar la primera letra del segundo apellido para el usuario interno. Por ejemplo, para Andrea González Pérez su usuario interno sería "AGONZALEZP".

- Si de la combinación de letras según el formato indicado surgen palabras ofensivas o respectivas, estas deben ser modificadas para que los usuarios internos no presenten estas características.

6. Los Responsables de la Información deben verificar periódicamente los controles de acceso para los usuarios provistos (internos y externos), con el fin de revisar que dichos usuarios tengan acceso permitido únicamente a aquellos recursos de red y servicios de la plataforma tecnológica para los que fueron autorizados. Esta validación se deberá de realizar semestralmente.

7. Todos los colaboradores, proveedores y clientes antes de contar con acceso lógico por primera vez a la red corporativa de ASEJUPS, deben contar la autorización y el Acuerdo de Confidencialidad firmado previamente. En el caso que el acceso sea con perfil de visitas, se habilitará una conexión independiente a la red corporativa.

8. ASEJUPS 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 Organización. Así mismo, velará porque los colaboradores y el personal externo 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 y procedimientos establecidos para tal fin.

9. Los Responsables de la Información deben establecer un procedimiento formal para la administración de los usuarios en las redes de datos, los recursos tecnológicos y sistemas de información, que contemple la creación, modificación, bloqueo o eliminación de las cuentas de usuario.

10. Los Custodios de Información previa solicitud de los Responsables de la Información deben crear, modificar, bloquear o eliminar cuentas de usuarios sobre las redes de datos, los recursos tecnológicos y los sistemas de información administrados, acorde con el procedimiento establecido.

11. El formato de contraseñas que se define para la aplicación del acceso a cuentas y dominios de ASEJUPS contiene:

    - Tamaño de la contraseña con un mínimo 8 caracteres.

- Combinación de mayúsculas, minúsculas, números y caracteres especiales (¡”#$%&=.).
- Todas las contraseñas deben cambiarse cada 3 meses.
- No se pueden utilizar como contraseñas:
    - Nombres de personas o mascotas.
    - Números telefónicos.
    - Fechas de nacimiento o fechas importantes para el usuario.
    - Número de cédula.
    - Contraseñas conocidas o por defecto como por ejemplo Password1.
    - No utilizar histórico de contraseñas de al menos las 5 últimas utilizadas.

12. Ningún colaborador debe compartir su cuenta de usuario o contraseña a ningún otro colaborador o tercero, así mismo, tampoco debe utilizar credenciales de otras personas para el acceso a información o sistemas de ASEJUPS, cada colaborador es responsable de la utilización de sus credenciales.

13. Los Responsables de la Información deben establecer un procedimiento que asegure la eliminación, reasignación o bloqueo de los privilegios de acceso otorgados sobre los recursos tecnológicos, los servicios de red y los sistemas de información de manera oportuna, cuando los funcionarios se desvinculan, toman licencias, vacaciones, son trasladados o cambian de cargo.

14. Los proveedores o clientes que posean acceso a la plataforma tecnológica, los servicios de red y los Sistemas de información de ASEJUPS deben acogerse a lineamientos para la configuración de contraseñas implantados por la Organización y todos los lineamientos de seguridad que se hayan establecido.

15. Los Responsables de la Información deben otorgar los privilegios para administración de recursos tecnológicos, servicios de red y sistemas de información sólo a aquellos funcionarios designados para dichas funciones.

16. Los Custodios de Información en conjunto con los Responsables de la Información, deben establecer cuentas personalizadas con altos privilegios para cada uno de los administradores de los recursos tecnológicos, servicios de red y Sistemas de información, por lo que, no se permiten cuentas genéricas que pueda ser utilizada por más de un usuario.

17. Los Responsables de la Información deben restringir las conexiones remotas a los recursos de la plataforma tecnológica; únicamente se deben permitir estos accesos a personal autorizado, de acuerdo con las labores desempeñadas.

18. Los Responsables de la Información deben asegurarse de que los usuarios o perfiles de usuario que traen por defecto los sistemas operativos, el firmware y las bases de datos sean suspendidos o renombrados en sus autorizaciones y que las contraseñas que traen por defecto dichos usuarios o perfiles sean modificadas.

19. Los Custodios de la Información deben certificar que se inhabilitan las cuentas luego de un número establecido de intentos fallidos de ingreso a los Sistemas. Máximo 3 intentos fallidos.

20. Los Custodios de la Información deben a nivel de los aplicativos, restringir acceso a archivos u otros recursos, a direcciones URL protegidas, a funciones protegidas, a servicios, a información de las aplicaciones, a atributos y políticas utilizadas por los controles de acceso y a la información relevante de la configuración, solamente a usuarios autorizados y acorde a la clasificación de la información que se haya realizado por los Responsables de la Información.

21. La conexión remota a la red de interna de ASEJUPS debe realizarse a través de una conexión VPN segura suministrada por la Organización, la cual debe ser aprobada, registrada y auditada, por el Responsable de la Información.

9.5 Lineamiento para el Uso Adecuado de la Infraestructura Tecnológica

Los siguientes lineamientos exponen las condiciones, normas y procedimientos necesarios para fijar los requisitos que se deben cumplir por cualquier funcionario, contratista o cliente de ASEJUPS, para el uso adecuado de la infraestructura y recursos informáticos propiedad de la Organización:

1. ASEJUPS es propietario de los equipos de cómputo, de los derechos de uso del software instalado en los mismos y de la información empresarial contenida en estos equipos.

2. Todo recurso informático e infraestructura de ASEJUPS, debe ser utilizada para fines legítimos que no pongan en riesgo la información o imagen de la Organización, por lo que, queda estrictamente prohibido el uso de estos recursos para fines distintos a los laborales.

3. Los usuarios deben proteger los equipos de cómputo con el fin de preservar la confidencialidad, la integridad y la disponibilidad de la información almacenada en estos dispositivos.

4. Todos los colaboradores y terceros a los que se les asigne equipo de cómputo serán los responsables de la utilización de estos, considerando los siguientes aspectos:

    - Cuidado físico de los equipos.
    - Información contenida.
    - Software instalado en el equipo.
    - Uso en actividades laborales y legitimas.

5. Los usuarios no tendrán permitido instalar o configurar nuevo software y/o hardware no autorizado, ni reconfigurar el ya instalado, a menos que este sea aprobado por el responsable de la unidad de negocio respectivo.

6. Los usuarios no podrán descargar software no autorizado de Internet para instalarlo en los equipos de cómputo.

7. Todo el software y hardware que sea necesario instalar en los equipos cómputo deberá contar con licencia de uso a nombre de ASEJUPS.

8. Las áreas o unidades de negocio que contengan equipo de cómputo crítico para la operación de la empresa deberán contar con accesos controlados que permitan la protección física de los equipos ante amenazas.

9. Las áreas destinadas a equipos de cómputo críticos deberán contar con sistemas contra incendios, redundancia de alimentación eléctrica o sistemas UPS, redundancia de conectividad, sistemas de climatización y salidas de emergencia entre otros.

10. La información clasificada confidencial almacenada en los equipos de cómputo deberá contar con los respaldos necesarios.

11. Los Sistemas, aplicaciones y archivos almacenados en los equipos de cómputo, podrán ser revisados por ASEJUPS en busca de cualquier aplicación no autorizada, programa o archivo sospechoso con el fin de tomar la acción que corresponda. Por lo que no se permite el uso de los dispositivos para fines personales, únicamente organizacionales que correspondan a actividades laborales relacionadas con ASEJUPS.

12. Los colaboradores de ASEJUPS. no tendrá permitido el préstamo o intercambio del equipo de cómputo portátil propiedad de la empresa a otros colaboradores o a personas externas a la institución.

13. Los usuarios no deben mantener almacenados en los discos duros de los equipos de cómputo o discos virtuales de red, archivos de vídeo, música, y fotos y cualquier tipo de archivo que no sean de carácter laboral de ASEJUPS.

14. ASEJUPS permite el acceso al servicio de Internet, estableciendo lineamientos que garanticen la navegación segura y el uso adecuado de la red por parte de los usuarios finales, evitando errores, pérdidas, modificaciones no autorizadas o uso inadecuado de la información en las aplicaciones WEB o actividades que desencadenen un incidente de seguridad, por lo que se debe considerar lo siguiente:

    - Las páginas de streaming como YouTube serán limitadas y accesibles a usuarios aprobados por la Gerencia.

    - Las redes sociales como Facebook y WhatsApp serán limitadas y accesibles a usuarios aprobados por la Gerencia

    - Se filtrará el acceso a sitios web maliciosos y peligrosos relacionados a pornografía, armas, drogas, juegos en línea, apuestas, entre otros.

    - Queda estrictamente prohibido la transmisión o almacenamiento de datos confidenciales o privados de la Organización, de sus Clientes o de sus Colaboradores en aplicaciones no aprobadas por ASEJUPS, ¡como por ejemplo WhatsApp, Facebook, Gmail, Hotmail, Yahoo!!, Dropbox, entre otros.

15. Queda prohibido acceder a sitios de divulgación, descarga o distribución de películas, videos, música, real audio, webcams, emisoras online, etc.

16. Queda prohibido publicar o enviar opiniones, declaraciones políticas y asuntos no propios de ASEJUPS, dirigidos a funcionarios, contratistas o clientes y público en general, a través de servicio corporativos y cuentas de la Compañía.

17. Todos los medios y equipos donde se almacena procesan o comunica la información confidencial o privada, 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.

18. ASEJUPS suministra el servicio de correo electrónico organizacional, el cual debe ser utilizado únicamente para fines laborales, por lo que, se debe considerar los siguientes elementos:

    - El acceso al servicio de correo electrónico es un privilegio otorgado por ASEJUPS a sus Colaboradores, Proveedores o Clientes, por lo que, el mismo sobrelleva responsabilidades y compromisos para su uso.

    - El correo electrónico organizacional es para uso exclusivo de actividades laborales relacionadas a ASEJUPS, por lo que, queda prohibido su utilización para fines personales.

    - No se permite el uso del correo electrónico organizacional para ofrecer servicios personales, cadenas de correo electrónico, bromas, spam u otra actividad fuera de la laboral hacia cuentas de correo de compañeros.

    - No se permite utilizar la cuenta de correo electrónico para registrarse en redes sociales, blogs u otro elemento externo de la Organización como promociones comerciales, agencias de viajes, entre otros.

    - Cuando se transmita información confidencial o privada, esta debe de ir etiquetada y dirigida a las personas que puedan tener acceso a la misma, por lo que, los usuarios deben de verificar el destino de los correos electrónicos.

    - No se permite la utilización de cuentas de correo externas (como por ejemplo Gmail, Hotmail o Yahoo) para la transmisión de ningún tipo de información confidencial o privada de ASEJUPS, de sus Clientes o de sus Colaboradores.

    - No se permite descargar, enviar, imprimir o copiar documentos o contenidos en contra de las leyes de derechos de autor.

    - No se permite distribuir listas de direcciones de correo personales sin expresa autorización de sus dueños.

    - Los usuarios no deben de abrir, dar clic en enlaces o descargas archivos de fuentes desconocidas de correos electrónicos que les lleguen a sus cuentas, ya que puede tratarse de ataques de phishing o malware que ponga en riesgo la infraestructura de ASEJUPS

    - Todo mensaje de correo electrónico que salga de una cuenta organizacional debe llevar por regla general una estructura de firma, por lo que, es responsabilidad del usuario su configuración y/o inclusión.

- Todo correo electrónico que sea enviado fuera de ASEJUPS, contendrá la siguiente clausula al pie de página del mensaje de este:

- "Este correo electrónico y cualquier archivo(s) adjunto al mismo, contiene información de carácter confidencial exclusivamente dirigida a su destinatario(s). Si usted no es el destinatario indicado, queda notificado que la lectura, utilización, divulgación y/o copia sin autorización está prohibida. En el caso de haber recibido este correo electrónico por error, agradecemos informarnos inmediatamente de esta situación mediante el reenvío a la dirección electrónica del remitente."

- Todos los Colaboradores deben cuidar y revisar el contenido de los correos electrónicos que se envíen a través de su cuenta. El uso no autorizado de una cuenta de correo electrónico es ilegal y constituye una violación de la Política de la Institución.

- ASEJUPS tiene el derecho a acceder y revelar los contenidos electrónicos de los correos electrónicos institucionales de sus funcionarios, contratistas y clientes, con el consentimiento de los usuarios a la empresa en caso de que algún ente fiscalizador a nivel interno o externo requiera esta información. Priman las exigencias de carácter legal o disciplinario.

19. No se permite almacenar las credenciales de acceso en libretas, agendas, post-it, hojas sueltas, archivos digitales u otro que pueda ser accesado por otra persona.

20. No se permite intentar acceder de forma no autorizada con otro usuario y clave diferente a la personal en cualquier sistema de información o plataforma tecnológica.

21. Se debe utilizar el servicio de mensajería instantánea de ASEJUPS exclusivamente para fines laborales.

22. No se permite la captura de imágenes y/o grabación de video en las instalaciones ASEJUPS, así como, del personal por parte de la ciudadanía, colaboradores, contratistas y clientes de la Organización, sin previa autorización de la Gerencia General o Dirección de Talento Humano.

23. Los colaboradores deben portar el carnet que los identifica como tales en un lugar visible mientras se encuentren en las instalaciones de la organización; en caso de pérdida del carné o tarjeta de acceso a las instalaciones, deben reportarlo a la mayor brevedad posible.

24. Cuando se presente una falla o problema de hardware o software en un equipo de cómputo u otro recurso tecnológico propiedad de ASEJUPS, el usuario responsable debe informar al Director/Gerente de su unidad de negocio y al área de soporte donde se atenderá o escalará al interior de la Organización, con el fin de realizar una asistencia adecuada.

25. En caso de pérdida o robo de un equipo de cómputo propiedad de ASEJUPS, se debe informar de forma inmediata al Director/Gerente de su unidad de negocio para que se inicie el trámite interno y se debe poner la denuncia ante la autoridad competente.

9.6 Lineamiento para el Borrado o Eliminación Seguro de Información

Existen métodos de borrado dispuestos por el propio sistema operativo de los equipos de cómputo como, por ejemplo, con la opción "eliminar" o la tecla "Supr" o "Delete", se realiza el borrado exclusivamente en la "lista de archivos" sin que se elimine realmente el contenido del dispositivo, el cual permanece en la zona de almacenamiento, por lo que, podría ser recuperado. Por lo tanto, ASEJUPS establece los siguientes lineamientos relacionados al borrado o eliminación de información:

1. Toda información confidencial que se encuentre en formato físico o impreso y que ya no sea de utilidad, debe ser triturada antes de ser desechada en los basureros de la Organización o en los basureros de reciclaje.

2. Cuando se requiere transferir, devolver o desechar un equipo de cómputo que almacenaba información confidencial, se debe realizar una sobreescritura segura a todo el disco duro antes de entregar el equipo, para asegurar un borrado seguro de la información que no puede recuperarse.

3. Las cintas, USB, CD, DVD o equipos de respaldo que sean desechados por tiempo de vida o que el ciclo de la información haya finalizado, cambio de tecnología, fallo u otra razón, deberán ser destruidos físicamente para asegurar un borrado seguro de la información que no puede recuperarse. Los métodos pueden ir desde desintegración, pulverización, fusión e incineración.

4. Los Responsables de la Información deberán realizar un seguimiento de los dispositivos que están en funcionamiento, las personas o departamentos responsables, la información contenida en ellos y su clasificación en función del grado de criticidad para el negocio.

5. Cuando se requiera realizar un borrado seguro en un equipo que almacena información sensible o crítica, se debe utilizar una herramienta de borrado de sobreescritura que permita la obtención de un documento que identifique

claramente que el proceso de borrado se ha realiza-do, detallando cuándo y cómo ha sido realizado.

9.7 Lineamiento para Uso de Escritorio Limpio

Los siguientes lineamientos dictan las pautas para mantener organizado y resguardado los documentos digitales, correos electrónicos en los computadores puestos a disposición de todos los usuarios de los Sistemas de información y estructura tecnológica, así como, la información física confidencial que se tenga impresa o archivada:

1. Estos lineamientos definen el uso adecuado y ordenado de las áreas de trabajo desde el punto de vista físico como tecnológico, por lo que, entiéndase para tal fin como escritorio el espacio físico o puesto de trabajo asignado a cada colaborador, proveedor o cliente de ASEJUPS, que contiene tanto sus carpetas electrónicas como los archivos y accesos a los diferentes aplicativos Organizaciones o documentos confidenciales impresos.

2. El uso y conservación de los puestos de trabajo (escritorios) y de los fondos de escritorio de sus computadores (pantallas) es una responsabilidad de cada uno de los colaboradores, proveedores o clientes de ASEJUPS que tengan acceso a la información de la Organización, sea de manera temporal o indefinida, en el normal desarrollo de sus actividades laborales.

3. Se deben dejar organizados los puestos y áreas de trabajo, entendiéndose por esto el resguardo de documentos con información confidencial o privada, evitando que queden a la vista o al alcance de la mano de personal sin autorización de acceso a la misma.

4. Los documentos con información confidencial o privada deben quedar bajo llave o custodia en horas no laborables, almuerzos, desatención de puestos de trabajo y vacaciones.

5. No se permite el retiro de documentos confidenciales o privados fuera de la Organización y en el caso de ser necesario, se debe autorización del Responsable de la Información, asegurar su protección y su pronta devolución al mismo.

6. Se deben controlar la recepción, flujo envío de documentos físicos categorizados como confidenciales, por medio de registro de sus destinatarios desde el punto de correspondencia.

7. No se permite el fotocopiado de documentos confidenciales fuera de las instalaciones de ASEJUPS

8. Al imprimir o fotocopiar documentos con información confidencial o privada, esta debe ser retirada inmediatamente de las impresoras o multifuncionales utilizadas para tal fin. Y no debe ser dejada desatendida sobre los escritorios.

9. No se debe reutilizar papel que contenga información confidencial o privada.

10. Las computadoras o estaciones de trabajo deben ser bloqueados por los usuarios al retirarse de los mismos y los mismos deben ser desbloqueados por medio del usuario y contraseña asignado para su acceso a los mismos. Es responsabilidad del usuario, asegurar que el equipo tenga la protección adecuada.

11. Las áreas de trabajo virtuales "escritorios" del equipo de cómputo deben tener el mínimo de iconos visibles, limitándose estos a los accesos necesarios para la ejecución de la ofimática, accesos a sistemas de información y a carpetas y unidades de red necesarios para la ejecución de las actividades.

12. Los documentos digitales deben ser organizados en carpetas y evitar dejarlos a la vista en las pantallas de los equipos de cómputo.

13. Los colaboradores y proveedores al retirarse de ASEJUPS deben apagar los computadores asignados. Queda fuera de esta indicación los servidores y estaciones de trabajo utilizados para acceso remoto. Las sesiones activas se deben terminar cuando el usuario finalice las actividades programadas.

14. No se permite mantener contraseñas en documentos físicos, post-it o notas, pegadas en la pantalla del computador, debajo del teclado o en algún lugar físico sin protección, así mismo, tener en archivos digitales de fácil acceso esta información.

9.8 Lineamiento para la Gestión de Respaldos de Información

ASEJUPS certificará la generación de copias de respaldo y almacenamiento de su información confidencial, proporcionando los recursos necesarios y estableciendo los lineamientos y mecanismos para la realización de estas actividades. Los Responsables de la información, definirán la estrategia a seguir y los periodos de retención para el respaldo y almacenamiento de la información.

Así mismo, ASEJUPS velará porque los medios magnéticos que contienen la información confidencial sean almacenados en una ubicación diferente a las instalaciones donde se

encuentra dispuesta. El sitio externo donde se resguarden las copias de respaldo debe contar con los controles de seguridad física y medioambiental apropiados. A continuación, se listan los lineamientos que corresponden a los respaldos de la información:

1. Los Custodios de Información deben generar y adoptar los procedimientos en conjunto con los Responsables de la Información para la generación, restauración, almacenamiento y tratamiento de las copias de respaldo de la información, velando por su integridad y disponibilidad.

2. Los Custodios de Información deben llevar a cabo los procedimientos para realizar pruebas de recuperación a las copias de respaldo, para así comprobar su integridad y posibilidad de uso en caso de ser necesario.

3. Los Responsables de la Información y los Usuarios de la Información deben identificar la información crítica que debe ser respaldada y almacenarla de acuerdo con su nivel de clasificación en los medios establecidos por la Organización.

4. Los medios de respaldo de la información estarán limitados por un control de acceso para que únicamente el personal autorizado tenga acceso a la información que le corresponda.

5. Los archivos de respaldos almacenados deben estar en un segmento de red separado del ambiente de operación y únicamente tener acceso por personal específico que requiera tener acceso a los respaldos para una restauración o prueba de funcionamiento.

9.9 Lineamiento para Seguridad Física y Ambiental para el Centro de Datos y Áreas Críticas

ASEJUPS brindará la protección necesaria a nivel físico y ambiental del centro de datos y áreas críticas del negocio, considerando los siguientes lineamientos como de atamiento obligatorio para el responsable de este y de las personas que por motivos laborales deben ingresar a los mismos:

1. ASEJUPS implementará las condiciones requeridas para el resguardo, acceso físico seguro y conservación de los activos de información y los activos de soporte de su centro de datos, así como, las condiciones ambientales adecuadas para garantizar su funcionamiento.

2. ASEJUPS debe implementar controles de seguridad física contra robo, acceso sin autorización, daño, manipulación no autorizada, incendios, inundaciones y

cualquier actividad que ponga en riesgo la seguridad de la información de la empresa.

3. ASEJUPS debe implementar controles de seguridad física de los puestos de trabajo, para prevenir el acceso y disposición no autorizada de la información.

4. ASEJUPS debe implementar controles para proteger la información contenida en los equipos o dispositivos que se retiren de su sitio original para mantenimiento o manipulación por terceros.

5. ASEJUPS debe proveer las condiciones físicas y medioambientales necesarias para certificar la protección y correcta operación de los recursos de la plataforma tecnológica ubicados en el centro de cómputo; deben existir Sistemas de control ambiental de temperatura y humedad, Sistemas de detección y extinción de incendios, Sistemas de descarga eléctrica, Sistemas de vigilancia y monitoreo y alarmas en caso de detectarse condiciones ambientales inapropiadas. Estos Sistemas se deben monitorear de manera permanente.

6. Las solicitudes de acceso al centro de cómputo o a los centros de cableado deben ser aprobadas; no obstante, los visitantes siempre deberán estar acompañados de un funcionario durante su visita al centro de cómputo o los centros de cableado.

7. Se debe registrar el ingreso de los visitantes al centro de cómputo y a los centros de cableado que están bajo su custodia, en una bitácora ubicada en la entrada de estos lugares de forma visible.

8. Se debe certificar que el centro de cómputo y los centros de cableado que están bajo su custodia, se encuentren separados de áreas que tengan líquidos inflamables o que corran riesgo de inundaciones e incendios.

9. Se 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; así mismo, se debe llevar control de la programación de los mantenimientos preventivos.

10. Se debe almacenar y custodiar los registros del sistema de control de acceso a las instalaciones y al centro de datos.

11. Se debe certificar la efectividad de los mecanismos de seguridad física y control de acceso al centro de cómputo, centros de cableado y demás áreas de procesamiento de información.

12. Se debe controlar el ingreso de los visitantes a los centros de cableado que están bajo su custodia.

13. Dentro de las instalaciones del centro de datos o críticas queda estrictamente prohibido:
    - Fumar dentro del centro de datos.
    - Introducir alimentos o bebidas.
    - Mover, desconectar o conectar equipo de cómputo sin autorización del encargado.
    - Modificar configuraciones de los equipos sin autorización del encargado.
    - Alterar o dañar las etiquetas de identificación de los Sistemas de información o sus conexiones físicas.
    - Extraer información de los equipos en dispositivos externos.
    - Toda persona debe hacer uso únicamente de los equipos y accesorios que les sean asignados y para los fines que se les autorice.

9.10 Lineamiento para Dispositivos Móviles

ASEJUPS establece los siguientes lineamientos que aplican para el uso de dispositivos móviles que sean propiedad de la empresa o que sean utilizados por colaboradores para acceder y transmitir información de la Organización:

9.10.1 Lineamientos de Seguridad para Uso Dispositivos Móviles que Accedan a Información de ASEJUPS

Los colaboradores, proveedores y clientes que hagan uso del dispositivo móvil para almacenar o acceder a la información de ASEJUPS, deberán:

1. Solicitar a los Responsables de la Información la autorización para el uso de aplicaciones o equipos móviles, aceptando el cumplimiento de la política de dispositivos móviles por medio de un correo electrónico.
2. Aceptar las configuraciones de seguridad del dispositivo por medio de correo electrónico, y estas no podrán modificarse mientras se acceda o almacene información de ASEJUPS
3. El dispositivo debe tener instalado y configurado un software de antivirus.

4. Establecer un mecanismo de control de acceso como contraseña superior a 8 caracteres, un patrón de seguridad de al menos 7 puntos de contacto, o huella digital.

5. Configurar el bloqueo de pantalla para un mínimo de 2 minutos de inactividad.

6. Configurar la opción de borrado remoto de información en los dispositivos móviles, con el fin de eliminar los datos de dichos dispositivos de forma remota, en caso de ser requerido.

7. Es necesario realizar el cifrado del dispositivo móvil.

8. Seguir los lineamientos definidos para la información crítica o sensible, la cual puede restringir el acceso o almacenamiento de este tipo de información en los dispositivos móviles.

9.10.2 Lineamientos de Seguridad para Uso Dispositivos Móviles propiedad de ASEJUPS

Los Colaboradores que se les haya entregado un dispositivo móvil por parte de ASEJUPS, deberán cumplir con los siguientes lineamientos:

1. Solicitar a los Responsables de la Información la autorización para el uso de aplicaciones o equipos móviles, aceptando el cumplimiento de la política de dispositivos móviles por medio de un correo electrónico.

2. Aceptar las configuraciones de seguridad del dispositivo por medio de correo electrónico, y estas no podrán modificarse mientras se acceda o almacene información de ASEJUPS

3. El dispositivo debe tener instalado y configurado un software de antivirus, el cual será brindado por ASEJUPS.

4. Establecer un mecanismo de control de acceso como contraseña superior a 8 caracteres, un patrón de seguridad de al menos 7 puntos de contacto, o huella digital.

5. Configurar el bloqueo de pantalla para un mínimo de 2 minutos de inactividad.

6. Configurar la opción de borrado remoto de información en los dispositivos móviles, con el fin de eliminar los datos de dichos dispositivos de forma remota, en caso de ser requerido.

7. Es necesario realizar el cifrado del dispositivo móvil.

8. Seguir los lineamientos definidos para la información crítica o sensible, la cual puede restringir el acceso o almacenamiento de este tipo de información en los dispositivos móviles.

9. Cumplir con las medidas de los lineamientos de uso adecuado de la infraestructura, uso del correo electrónico, navegación y utilización de los dispositivos, establecidos en el punto 9.5.

10. ASEJUPS es propietario de los equipos de cómputo, de los derechos de uso del software instalado en los mismos y de la información empresarial contenida en estos equipos.

11. Todos los colaboradores y terceros a los que se les asigne equipo de cómputo serán los responsables de la utilización de estos, considerando los siguientes aspectos:

    a. Cuidado físico de los equipos.

    b. Información contenida.

    c. Software instalado en el equipo.

    d. Uso en actividades laborales y legitimas.

12. Los sistemas, aplicaciones y archivos almacenados en los dispositivos móviles, podrán ser revisados en busca de cualquier aplicación no autorizada, programa o archivo sospechoso con el fin de tomar la acción que corresponda. Por lo que no se permite el uso de los dispositivos para fines personales, únicamente organizacionales que correspondan a actividades laborales relacionadas con ASEJUPS

13. Los colaboradores de ASEJUPS no tendrá permitido el préstamo o intercambio de los dispositivos móviles propiedad de la empresa a otros colaboradores o a personas externas a la Corporación.

14. Los usuarios no deben mantener almacenados en los dispositivos móviles archivos de vídeo, música, y fotos y cualquier tipo de archivo que no sean de carácter laboral de ASEJUPS

9. Sanciones e Incumplimientos

La política de seguridad de la información y los lineamientos que surjan de esta pretenden instruir y afianzar una cultura de seguridad de la información entre los colaboradores, personal externo, clientes y proveedores.

Por lo que, es necesario que las violaciones a estas normas sean clasificadas, con el objetivo de aplicar medidas correctivas conforme a las afectaciones contra la seguridad de la información que ocasionaron.

Las medidas correctivas pueden considerar desde acciones administrativas, hasta acciones de orden disciplinario o penal, de acuerdo con las circunstancias, si así lo ameritan.

Por tal razón, el incumplimiento de la política y lineamientos de seguridad que dé está emanen, dará derecho a la empresa a ejercer las acciones civiles, penales y administrativas que correspondan y, de ser ello procedente, a la terminación de los contratos respectivos.