POLITICA DE SEGURIDAD DE LA INFORMACIÓN

1. OBJETO

Garantizar y salvaguardar la confidencialidad, integridad, autenticidad, control, utilidad y disponibilidad de los recursos o datos de la organización, así como de la tecnología utilizada para su procesamiento, tratamiento y custodia, con el fin de proteger la información de los distintos riesgos en que pueda verse afectada, los cuales pueden producirse por circunstancias internas o externas a Empresa de Energía de Pereira S.A. E.S.P.

La información como los demás recursos y procesos es de gran valor para la Compañía, puesto que es esencial para mantener los niveles de confianza de los socios estratégicos, colaboradores y usuarios, así mismo para mantener los estándares de competitividad, confidencialidad comercial, propiedad intelectual e imagen corporativa. Por tanto, es necesario establecer una metodología de gestión de la seguridad que sea clara y estructura, la cual haga parte de la cultura organización de la Empresa, por ello asegurar el cumplimiento y la difusión de la política es un compromiso de todos los directivos de la EEP, del área de Tecnología Informática y de la subgerencia de gestión humana.

2. TABLA DE CONTENIDO

3. MARCO JURÍDICO

Norma técnica NTC-ISO/IEC Colombiana 27001 esta norma ha sido elaborada para brindar un modelo para el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora de un sistema de gestión de la seguridad de la información (SGSI).

4. ALCANCE

La política de seguridad de la información protege a LA EMPRESA DE ENERGIA DE PEREIRA S.A ESP de una amplia gama de amenazas con el fin de garantizar la continuidad de los sistemas de información, minimizar los riesgos de daño y asegurar el eficiente cumplimiento de los objetivos de la compañía.

El área de Gestión Tecnológica e Informática, la Gerencia Administrativa y Financiera y la Gerencia General, acuerdan y establecen la presente Política de Seguridad como mecanismo de protección, prevención y control a la Información, los Sistemas de Información, los Equipos de Cómputo y demás recursos de Tecnología e Informática de LA EMPRESA DE ENERGIA DE PEREIRA S.A ESP.

Esta política se aplica en todo el ámbito empresarial, a sus recursos, y a la totalidad de sus procesos, ya sean internos o externos vinculados a la entidad a través de contratos o acuerdos.

5. GLOSARIO

- Recursos o datos: es toda la información independientemente de la forma en que se guarde o trasmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración.

- Integridad: Hace referencia a la precisión y coherencia de los datos e información enviada y guardada en la infraestructura de EEP.

- Confidencialidad: Los reportes que genera el sistema no pueden ser entregados a terceros, solamente a los funcionarios de las empresas cliente autorizados.

- Disponibilidad: La información se debe mantener actualizada y disponible para el normal desarrollo de las actividades de la compañía con el fin de garantizar la continuidad el negocio y traumas a los usuarios y clientes.

- Confiabilidad: La información debe revisarse antes de ser divulgada o generar medios contables, de pagos o similares, de tal forma que se garantice que no tiene problemas. Dichos problemas se pueden generar porque se grabó mal la información, no se ejecutaron algunos procesos adecuadamente en el sistema o porque el software tiene errores. Para el último caso, se debe informar oportunamente al Área de Tecnología Informática.

- Información Crítica: Las bases de datos en general, especialmente los datos de: Notas de Cartera, Financiaciones, Otros Cobros, Pagos, Rutas, Claves de Acceso, Claves de Correo y bases de datos de Clientes o Usuarios, que constituyen parte fundamental para el negocio y sus actividades relacionadas.

6. RESPONSABILIDAD

Todos los gerentes, subgerentes y líderes son responsables de la implementación de la política de seguridad de la información dentro de sus áreas de responsabilidad, así como del cumplimiento de dicha política por parte de su equipo de trabajo.

La política de seguridad de la información es de aplicación obligatoria para todo el personal de la Compañía y contratistas, que en el desempeño de sus funciones y/o actividades tenga acceso a la información de la compañía, cualquiera que sea su vinculación laboral, el área a la cual pertenezca y el nivel de las tareas que desempeñe.

A través de la presente política se establece "El Comité de Seguridad de la Información", el cual estará conformado por personal de las siguientes áreas:

- Gerencia Direccionamiento y Control Estratégico
- Gerencia Jurídica
- Subgerencia de Desarrollo Humano y Organizacional
- Subgerencia Tecnología de la Información
- Subgerencia Logística

Estos serán designados por los Gerentes de cada una de las Áreas convocadas y será presidido por el Subgerente de TI.

Este grupo revisará y propondrá ante las directivas para su aprobación la Política de Seguridad de la Información y las funciones generales en materia

de seguridad de la información, monitoreará cambios significativos en los riesgos que afectan a los recursos de información, tendrá conocimiento y supervisará la investigación y monitoreo de los incidentes relativos a la seguridad, aprobará las principales iniciativas para incrementar la seguridad de la información, de acuerdo a las competencias y responsabilidades asignadas a cada área, así como acordará y aprobará metodologías y procesos específicos relativos a seguridad de la información, garantizará que la seguridad sea parte del proceso de planificación de la información, evaluará y coordinará la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios, promoverá la difusión y apoyo a la seguridad de la información dentro de la compañía y coordinará el proceso de administración de la continuidad de sus actividades.

El Subgerente de tecnología e informática cumplirá funciones relativas a la seguridad de los sistemas de información de la EEP, lo cual incluye la supervisión de todos los aspectos inherentes a los temas tratados en la presente política.

Los propietarios de la información y/o lideres de cada proceso son responsables de clasificarla de acuerdo con el grado de sensibilidad y criticidad de la misma, de documentar y mantener actualizada la clasificación efectuada, y de definir qué usuarios deberán tener permisos de acceso a la información de acuerdo a sus funciones y competencia.

El Subgerente Desarrollo Humano y Organizacional, cumplirá la función de notificar a todo el personal que ingresa a la Compañía de sus obligaciones respecto del cumplimiento de la política de seguridad de la información y de todas las normas, procedimientos y prácticas que de ella surjan. Así mismo, tendrá a su cargo la notificación del presente manual a todo el personal, de los cambios que en ella se produzcan, la implementación de la suscripción de los compromisos de confidencialidad (entre otros) y las tareas de capacitación continúa en materia de ciberseguridad.

El Subgerente del área de tecnología informática cumplirá la función de cubrir los requerimientos de seguridad informática establecidos para la operación, administración y comunicación de los sistemas y recursos de tecnología de la compañía. Por otra parte, tendrá la función de efectuar las tareas de desarrollo y mantenimiento de los sistemas de información.

El Gerente Jurídico verificará el cumplimiento del presente manual en la gestión de todos los contratos, acuerdos u otra documentación de la

Empresa suscrita con los colaboradores y con terceros; De igual forma, asesorará en materia legal, en lo que se refiere a la seguridad de la información.

Los usuarios de la información y de los sistemas utilizados para su procesamiento son responsables de conocer, dar a conocer, cumplir y hacer cumplir la política de seguridad de la información que se encuentre vigente.

El área de auditoría interna, o en su defecto quien sea propuesto por el comité de seguridad de la información es responsable de practicar auditorías periódicas sobre los sistemas y actividades vinculadas con la tecnología de información, debiendo informar sobre el cumplimiento de las especificaciones y medidas de seguridad de la información establecidas por esta política y por las normas, procedimientos y prácticas que de ella surjan.

7. ASPECTOS GENERALES

LA EMPRESA DE ENERGIA DE PEREIRA S.A ESP ha establecido las siguientes condiciones generales de seguridad de la información, las cuales representan la visión de la compañía en cuanto a la protección de sus activos de información:

a. Los aspectos contemplados en esta política de seguridad hacen parte de la cultura organizacional de la empresa, por lo que demanda compromiso manifiesto de las Directivas tanto de su difusión como de su implementación.

b. Existirá un Comité de Seguridad de la Información, que será el responsable del mantenimiento, revisión y mejora del Sistema de Gestión de Seguridad de la Información.

c. Los activos de información de la compañía serán identificados y clasificados para establecer los mecanismos de protección necesarios.

d. Se definirán e implantarán controles para proteger la información contra violaciones de autenticidad, accesos no autorizados, la perdida de integridad y que garanticen la disponibilidad requerida por los clientes y usuarios de los servicios ofrecidos por la compañía.

e. Todos los colaboradores, contratistas y/o proveedores serán responsables de proteger la información a la cual accedan y procesen, para evitar su pérdida, alteración, destrucción o uso indebido.

f. El Comité de Seguridad de la Información revisará cada año la presente política, a efectos de mantenerla actualizada. También efectuará toda modificación que sea necesaria en función de posibles cambios que puedan afectar su definición, como son: cambios tecnológicos, variación de los costos de los controles, impacto de los incidentes de seguridad, etc.

g. Únicamente se permitirá el uso de software autorizado que haya sido adquirido legalmente por LA EMPRESA DE ENERGIA DE PEREIRA S.A ESP.

h. Es responsabilidad de todos los colaboradores y proveedores de la Empresa reportar los incidentes de seguridad, eventos sospechosos y el mal uso de los recursos que identifique.

i. Las violaciones a la policita y a los controles de seguridad de la información serán reportadas, registradas y monitoreadas.

j. La compañía contará con un plan de continuidad del negocio que asegure la continuidad de las operaciones, ante la ocurrencia de eventos no previstos o desastres naturales.

Adicionalmente la compañía cuenta con políticas específicas y un conjunto de estándares y procedimientos que soportan la política corporativa.

8. POLÍTICAS ESPECÍFICAS Y PROCEDIMIENTOS QUE SOPORTAN LA POLÍTICA CORPORATIVA

8.1 Acuerdos de confidencialidad

Todos los colaboradores, contratistas y/o proveedores de servicio deben aceptar los acuerdos de confidencialidad definidos por LA EMPRESA DE ENERGIA DE PEREIRA S.A ESP, los cuales reflejan los compromisos de protección y buen uso de la información de acuerdo con los criterios establecidos en ella.

Para el caso de contratistas, los respectivos contratos deben incluir una cláusula de confidencialidad, de igual manera cuando se permita el acceso a la información y/o a los recursos de LA EMPRESA DE ENERGIA DE PEREIRA S.A ESP a personas o entidades externas.

Estos acuerdos deben aceptarse por cada uno de ellos como parte del proceso de contratación, razón por la cual dicha cláusula y/o acuerdo de confidencialidad hace parte integral de cada uno de los contratos.

8.2 Uso adecuado de los activos

El acceso a los documentos físicos y digitales estará determinado por las normas relacionadas con el acceso y las restricciones a los documentos, a la competencia del área o dependencia específica y a los permisos y niveles de acceso de los funcionarios, contratistas y/o proveedores determinada por los responsables de los procesos.

Para la consulta de documentos cargados en el software de Gestión Documental se establecerán privilegios de acceso a los colaboradores y/o proveedores de acuerdo con el desarrollo de sus funciones y competencias. Dichos privilegios serán establecidos por el Gerente del Área o quien haga sus veces, quien comunicará al área de Tecnología e Informática (administrador del software) el listado con los colaboradores y sus privilegios.

Todos los colaboradores y terceros que manipulen información en el desarrollo de sus funciones deberán firmar un "acuerdo de confidencialidad de la información", donde individualmente se comprometan a no divulgar, usar o explotar la información confidencial a la que tengan acceso, respetando los niveles establecidos para la clasificación de la información; y que cualquier violación a lo establecido en este parágrafo será considerada como un "incidente de seguridad".

8.3 Acceso a Internet

El internet es una herramienta de trabajo que permite navegar en muchos otros sitios relacionados o no con las actividades propias del negocio de

EMPRESA DE ENERGIA DE PEREIRA S.A ESP, por lo cual el uso adecuado de este recurso se debe controlar, verificar y monitorear, considerando, para todos los casos, los siguientes lineamientos:

a. No está permitido:

- El acceso a páginas relacionadas con pornografía, drogas, alcohol, webproxys, hacking, streaming juegos y/o cualquier otra página que vaya en contra de la ética moral, las leyes vigentes o políticas aquí establecidas.

- El acceso y el uso de servicios interactivos redes sociales como Facebook, Instagram, Snapchat y otros similares, que tengan como objetivo crear comunidades para intercambiar información, o bien para fines diferentes a las actividades propias del negocio de LA EMPRESA DE ENERGIA DE PEREIRA S.A ESP.

- El intercambio no autorizado de información de propiedad de LA EMPRESA DE ENERGIA DE PEREIRA S.A ESP, de sus clientes y/o de sus colaboradores, con terceros.

- 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, 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 Jefe respectivo y el área de tecnología informática, o a quienes ellos deleguen de forma explícita para esta función, asociando los procedimientos y controles necesarios para el monitoreo y aseguramiento del buen uso del recurso.

b. LA EMPRESA DE ENERGIA DE PEREIRA S.A ESP debe realizar monitoreo permanente de tiempos de navegación y páginas visitadas por parte de los colaboradores y/o terceros. Así mismo, puede inspeccionar, registrar y evaluar las actividades realizadas durante la navegación, de acuerdo con la legislación nacional vigente por medio de su UTM o Firewall.

c. Cada uno de los colaboradores es responsable de dar un uso adecuado a este recurso y en ningún momento puede ser usado para realizar prácticas ilícitas o mal intencionadas que atenten contra terceros, la legislación vigente y los lineamientos de seguridad de la información, entre otros.

d. Los colaboradores y proveedores no pueden asumir en nombre de LA EMPRESA DE ENERGIA DE PEREIRA S.A ESP posiciones personales en redes sociales, encuestas de opinión, foros u otros medios similares.

e. El uso de Internet no considerado dentro de las restricciones anteriores es permitido siempre y cuando se realice de manera ética, razonable, responsable, no abusiva y sin afectar la productividad ni la protección de la información de LA EMPRESA DE ENERGIA DE PEREIRA S.A ESP.

8.4 Correo electrónico

Los funcionarios, contratistas y/o proveedores autorizados a quienes LA EMPRESA DE ENERGIA DE PEREIRA S.A ESP les asigne una cuenta de correo deberán seguir los siguientes lineamientos:

a. La cuenta de correo electrónico debe ser usada para el desempeño de las funciones asignadas dentro de EMPRESA DE ENERGIA DE PEREIRA S.A ESP.

b. Los mensajes y la información contenida en los buzones de correo electrónico son propiedad de LA EMPRESA DE ENERGIA DE PEREIRA S.A ESP y cada usuario.

c. El tamaño de los buzones de correo es determinado por el área de tecnología informática de acuerdo con los perfiles y roles que desempeñan los colaboradores de la compañía.

d. El tamaño de envío y recepción de mensajes, sus contenidos y demás características propias de éstos están definidos de acuerdo con los perfiles y roles que desempeñan los colaboradores de la compañía.

e. Cuando un colaborador requiere ausentarse de la empresa por un periodo superior a 8 días debe programar el correo electrónico para que

automáticamente responda a los remitentes indicando fecha de llegada, nombre y dirección de correo electrónico de la persona encargada durante su ausencia.

f. Antes de enviar un mensaje de correo electrónico se deberá verificar que este va dirigido solamente a los interesados y/o a quienes deban conocer dicho mensaje.

g. Todo mensaje tipo phishing, spam, smishing, vishing, o alguno similar, debe ser calificado como correo no deseado, eliminado, y nunca respondido.

h. No es permitido:

- Enviar cadenas de correo, mensajes con contenido religioso, político, racista, sexista, pornográfico, publicitario no corporativo o cualquier otro tipo de mensajes que atenten contra la dignidad y la productividad de las personas o el normal desempeño del servicio de correo electrónico en la compañía, mensajes mal intencionados que puedan afectar los sistemas internos o de terceros, mensajes que vayan en contra de las leyes, la moral y las buenas costumbres y mensajes que inciten a realizar prácticas ilícitas o promuevan actividades ilegales.

- Utilizar la dirección de correo electrónico de LA EMPRESA DE ENERGIA DE PEREIRA S.A ESP como punto de contacto en comunidades interactivas de contacto social, tales como *Facebook, Instagram* y/o *Twitter*, entre otras, o cualquier otro sitio que no tenga que ver con las actividades laborales.

- El envío de archivos que contengan extensiones ejecutables, en ninguna circunstancia.

- El envío de archivos de música y videos. En caso de requerir hacer un envío de este tipo de archivos deberá ser autorizado por la gerencia respectiva y el área de tecnología y comunicaciones.

i. El envío de información corporativa debe ser realizado exclusivamente desde la cuenta de correo que LA EMPRESA DE ENERGIA DE PEREIRA S.A ESP proporciona. De igual manera, las cuentas de correo corporativas no se deben emplear para uso personal.

j. El envío masivo de mensajes publicitarios corporativos solo podrá ser utilizado a través de los medios y/o dependencias autorizadas para tal fin. Además, en el caso que dichos mensajes tengan como usuario final terceros a la compañía se deberá incluir un mensaje que le indique al destinatario como ser eliminado de la lista de distribución. Si una dependencia debe, por alguna circunstancia realizar envío de correo masivo de manera frecuente, este debe ser enviado a través de una cuenta de correo electrónico a nombre de la dependencia respectiva y/o Servicio habilitado para tal fin y no a través de cuentas de correo electrónico asignadas a un usuario particular.

k. Toda información de LA EMPRESA DE ENERGIA DE PEREIRA S.A ESP generada con los diferentes programas computacionales que requiera ser enviada fuera de la compañía, y que por sus características de confidencialidad e integridad deba ser protegida, debe estar en formatos no editables, utilizando las características de seguridad que brindan las herramientas proporcionadas por el área de tecnología informática. La información puede ser enviada en el formato original bajo la responsabilidad del usuario y únicamente cuando el receptor requiera hacer modificaciones a dicha información.

l. Todos los mensajes enviados deben respetar el estándar de formato e imagen corporativa definido por LA EMPRESA DE ENERGIA DE PEREIRA S.A ESP y deben conservar en todos los casos el mensaje legal corporativo de confidencialidad.

8.5 Recursos tecnológicos

El uso adecuado de los recursos tecnológicos asignados por LA EMPRESA DE ENERGIA DE PEREIRA S.A ESP a sus colaboradores y/o proveedores se reglamenta bajo los siguientes lineamientos:

a. La instalación de cualquier tipo de software o hardware en los equipos de cómputo de LA EMPRESA DE ENERGIA DE PEREIRA S.A ESP es responsabilidad del área de tecnología informática y por tanto son los únicos autorizados para realizar esta labor. En este orden de ideas, los medios de instalación de software deben ser los proporcionados por la compañía a través de la mencionada área.

b. Los usuarios no deben realizar cambios en las estaciones de trabajo relacionados con la configuración del equipo, tales como conexiones de red, usuarios locales de la máquina, papel tapiz y protector de pantalla corporativo, entre otros. Estos cambios pueden ser realizados únicamente por el área de tecnología informática.

c. El área de tecnología informática debe definir y actualizar, de manera periódica, la lista de software y aplicaciones autorizadas que se encuentran permitidas para ser instaladas en las estaciones de trabajo de los colaboradores de acuerdo con sus procesos y labores. Así mismo, realizar el control y verificación de cumplimiento del licenciamiento del respectivo software y aplicaciones asociadas.

d. Únicamente los colaboradores y proveedores autorizados por el área de tecnología informática, previa solicitud vía correo electrónico por parte de la dependencia que lo requiera, pueden conectarse a la red inalámbrica privada de LA EMPRESA DE ENERGIA DE PEREIRA S.A ESP.

e. La conexión a redes inalámbricas externas para usuarios con equipos portátiles que estén fuera de la oficina y que requieran establecer una conexión a la infraestructura tecnológica de LA EMPRESA DE ENERGIA DE PEREIRA S.A ESP, deben utilizar una conexión bajo los esquemas y herramientas de seguridad autorizados y establecidos por el área de tecnología y comunicaciones.

f. Sólo personal autorizado puede realizar actividades de administración remota de dispositivos, equipos o servidores de la infraestructura de procesamiento de información de la EMPRESA DE ENERGIA DE PEREIRA S.A ESP; las conexiones establecidas para este fin, deben utilizar los esquemas y herramientas de seguridad y administración definidas por el área de tecnología informática.

g. La sincronización de dispositivos móviles, tales como: smartphones, Tablet, portátiles personales u otros dispositivos electrónicos sobre los que se puedan realizar intercambios de información con cualquier recurso de la Compañía, debe estar autorizado de forma explícita por la dependencia respectiva, en conjunto con el área de tecnología informática.

h. Los equipos de cómputo, software y elementos tecnológicos que requieran ser ingresados y conectados a la red corporativa de la

EMPRESA DE ENERGIA DE PEREIRA S.A ESP debe contar con los soportes de licenciamiento conforme a lo establecido por la ley (licenciamiento y legalidad de software), al igual que antivirus debidamente actualizado.

8.6 Control de acceso físico

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 consideran áreas de acceso restringido. En consecuencia, deben contar con medidas de control de acceso físico en el perímetro tales que puedan ser auditadas, así como con procedimientos de seguridad operacionales que permitan proteger la información, el software y el hardware de daños intencionales o accidentales.

De igual forma, los centros de cómputo, cableado y cuartos técnicos de las oficinas deben contar con mecanismos que permitan garantizar que se cumplen los requerimientos ambientales (temperatura, humedad, etc.), especificados por los fabricantes de los equipos que albergan y que pueden responder de manera adecuada ante incidentes como incendios e inundaciones.

Toda información alojada en la infraestructura de EMPRESA DE ENERGIA DE PEREIRA S.A ESP o en la Nube debe estar aprobada y avalada por el área de Tecnologías de la Información, esto con el fin de garantizar la debida custodia de esta.

Se contará con un formato de ingreso y salida a los centro de datos el cual deberá diligenciarse cada que se realice alguna labor en sitio.

8.7 Protección y ubicación de los equipos

Los equipos que hacen parte de la infraestructura tecnológica de la EMPRESA DE ENERGIA DE PEREIRA S.A ESP tales como servidores, equipos de comunicaciones y seguridad electrónica, centros de cableado, UPS, subestaciones eléctricas, aires acondicionados, plantas telefónicas, así como

estaciones de trabajo y dispositivos de almacenamiento y/o comunicación móvil que contengan y/o brinden servicios de soporte a la información crítica de las dependencias, deben ser ubicados y protegidos adecuadamente para prevenir la pérdida, daño, robo o acceso no autorizado de los mismos. De igual manera, se debe adoptar los controles necesarios para mantener los equipos alejados de sitios que puedan tener riesgo de amenazas potenciales como fuego, explosivos, agua, polvo, vibración, interferencia electromagnética y vandalismo, entre otros.

Los colaboradores y proveedores, incluyendo sus empleados o subcontratistas, que tengan acceso a los equipos que componen la infraestructura tecnológica de la EMPRESA DE ENERGIA DE PEREIRA S.A ESP no pueden fumar, beber o consumir algún tipo de alimento cerca de los equipos.

LA EMPRESA DE ENERGIA DE PEREIRA S.A ESP garantizara ambientes seguros en sus Centros de Datos de producción y respaldo para un constante monitoreo de humedad y temperatura.

8.8 Segregación de funciones

Toda tarea en la cual los colaboradores tengan acceso a la infraestructura tecnológica y a los sistemas de información debe contar con una definición clara de los roles y responsabilidades, así como del nivel de acceso y los privilegios correspondientes, con el fin de reducir y evitar el uso no autorizado o modificación sobre los activos de información de la compañía.

En concordancia:

Todos los sistemas de disponibilidad crítica o media de la Compañía deben implementar las reglas de acceso de tal forma que haya segregación de funciones entre quien administre, opere, mantenga, audite y, en general, tenga la posibilidad de acceder a los sistemas de información, así como entre quien otorga el privilegio y quien lo utiliza.

Los módulos ejecutables nunca deberán ser trasladados directamente de las librerías de pruebas a las librerías de producción sin que previamente sean compilados por el área asignada para tal efecto.

El nivel de súper usuario de los sistemas debe tener un control dual, de tal forma que exista una supervisión a las actividades realizadas por el administrador del sistema.

Todas las actividades que realice un usuario en la infraestructura tecnológica de la información de la EEP deben ser registrados y susceptibles de revisión por el responsable de la seguridad de la empresa o por el designado por el Comité de Seguridad Informática.

8.9 Protección contra software malicioso

LA EMPRESA DE ENERGIA DE PEREIRA S.A ESP establece que todos los recursos informáticos deben estar protegidos mediante herramientas y software de seguridad como antivirus, antispam, antispyware, antipishing y otras aplicaciones que brindan protección contra código malicioso y prevención del ingreso de este a la red corporativa, en donde se cuente con los controles adecuados para detectar, prevenir y recuperar posibles fallos causados por código malicioso. Será responsabilidad del área de tecnología informática autorizar el uso de las herramientas y asegurar que estas y el software de seguridad no sean deshabilitados en ninguna circunstancia, así como de su actualización permanente.

En este sentido, la EMPRESA DE ENERGIA DE PEREIRA S.A ESP define los siguientes lineamientos:

- No está permitido:

- La desinstalación y/o desactivación de software y herramientas de seguridad avaladas previamente por EMPRESA DE ENERGIA DE PEREIRA S.A ESP.

- Escribir, generar, compilar, copiar, propagar, ejecutar o intentar introducir cualquier código de programación diseñado para auto replicarse, dañar o afectar el desempeño de cualquier dispositivo o infraestructura tecnológica.

- Utilizar medios de almacenamiento físico o virtual que no sean de carácter corporativo o autorizados por el área de Tecnologías de la Información.

8.10 Copias de respaldo

LA EMPRESA DE ENERGIA DE PEREIRA S.A ESP debe asegurar que la información con cierto nivel de clasificación, definida en conjunto por el área de tecnología informática y las dependencias responsables de la misma, contenida en la plataforma tecnológica de la Compañía, como servidores, dispositivos de red para almacenamiento de información, estaciones de trabajo, archivos de configuración de dispositivos de red y seguridad, entre otros, sea periódicamente resguardada mediante mecanismos y controles adecuados que garanticen su identificación, protección, integridad y disponibilidad. Adicionalmente, se deberá establecer un plan de restauración de copias de seguridad que serán probados a intervalos regulares con el fin de asegurar que son confiables en caso de emergencia y retenidas por un periodo de tiempo determinado.

El área de tecnología informática establecerá procedimientos explícitos de resguardo y recuperación de la información que incluyan especificaciones acerca del traslado, frecuencia, identificación y definirá conjuntamente con las dependencias los períodos de retención de la misma. Adicionalmente, debe disponer de los recursos necesarios para permitir la identificación relacionada de los medios de almacenamiento, la información contenida en ellos y la ubicación física de los mismos para permitir un rápido y eficiente acceso a los medios que contienen la información resguardada.

Los medios magnéticos que contienen la información crítica deben ser almacenados en otra ubicación diferente a las instalaciones donde se encuentra dispuesta. El sitio externo donde se resguardan dichas copias debe tener los controles de seguridad adecuados, cumplir con máximas medidas de protección y seguridad física apropiados.

Es responsabilidad del usuario de la información almacenar la información en el espacio lógico asignado para la realización de las copias de seguridad que se hacen diarias de la compañía.

8.11 Gestión de medios removibles

El uso de medios de almacenamiento removibles (ejemplo: CDs, DVDs, USBs,discos duros externos, celulares) y acceso a almacenamiento en la nube que pueda ser usados sobre la infraestructura para el procesamiento de la información de EMPRESA DE ENERGIA DE PEREIRA S.A ESP, estará autorizado para todos los colaboradores cuyo perfil del cargo y funciones lo requiere.

Los usuarios de la información deben verificar que la información de los medios de almacenamiento extraíble, estén libres de cualquier código malicioso, y debe ejecutar el software antivirus autorizado por el área de tecnología informática.

8.12 Intercambio de información

LA EMPRESA DE ENERGIA DE PEREIRA S.A ESP firmará acuerdos de confidencialidad con los funcionarios, contratistas y/o proveedores, clientes y terceros que por diferentes razones requieran conocer o intercambiar información restringida o confidencial de la Compañía, ya sea dentro de los contratos u órdenes de servicio. En estos acuerdos quedarán especificadas las responsabilidades para el intercambio de la información para cada una de las partes y se deberán firmar antes de permitir el acceso o uso de dicha información.

Todo colaborador de la EMPRESA DE ENERGIA DE PEREIRA S.A ESP es responsable de proteger la confidencialidad e integridad de la información y debe tener especial cuidado en el uso de los diferentes medios para el intercambio de información que puedan generar una divulgación o modificación no autorizada.

Los propietarios de la información que se requiere intercambiar son responsables de definir los niveles y perfiles de autorización para acceso, modificación y eliminación de la misma y los custodios de esta información son responsables de implementar los controles que garanticen el cumplimiento de los criterios de confidencialidad, integridad, disponibilidad y requeridos.

8.13 Control de acceso lógico

El acceso a plataformas, aplicaciones, servicios y en general cualquier recurso de información de LA EMPRESA DE ENERGIA DE PEREIRA S.A ESP debe ser asignado de acuerdo a la identificación previa de requerimientos de seguridad y del negocio que se definan por las diferentes dependencias de la compañía, así como normas legales o leyes aplicables a la protección de acceso a la información presente en los sistemas de información.

Los responsables de la administración de la infraestructura tecnológica de LA EMPRESA DE ENERGIA DE PEREIRA S.A ESP asignan los accesos a plataformas, usuarios y segmentos de red de acuerdo a procesos formales de autorización los cuales deben ser revisados de manera periódica por el área de auditoría interna.

La autorización para el acceso a los sistemas de información debe ser definida y aprobada por la dependencia propietaria de la información, o quien ésta defina, y se debe otorgar de acuerdo con el nivel de clasificación de la información identificada, según la cual se deben determinar los controles y privilegios de acceso que se pueden otorgar a los colaboradores y proveedores e implementada por el área de tecnología y comunicaciones.

Cualquier usuario interno o externo que requiera acceso remoto a la red y a la infraestructura de procesamiento de información de EMPRESA DE ENERGIA DE PEREIRA S.A ESP, sea por Internet, acceso telefónico o por otro medio, siempre debe estar autenticado y sus conexiones deberán utilizar cifrado de datos.

LA EMPRESA DE ENERGIA DE PEREIRA S.A ESP brinda tecnologías de acceso por VPN para que colaboradores, proveedores y/o puntos de pago móviles puedan ingresar a las plataformas y aplicativos remotamente.

Para conceder el acceso a la VPN el colaborador o contratista debe diligenciar el formato de solicitud para la creación de usuarios y marcar la opción de VPN. Una vez el formato es aprobado por el área de Tecnologías de la Información, se configura el acceso y se envían las credenciales para realizar las pruebas respectivas.

El acceso a la VPN se deberá realizar con el aplicativo cliente de la página del cliente web del fabricante del dispositivo Firewall de seguridad perimetral en su ultima versión y con el formato para la configuración enviado por el área de Tecnologías de la Información.

Todos los colaboradores deberán contar con perfiles y credenciales de acceso a las diferentes plataformas, portales y aplicativos ejecutados sobre la infraestructura de LA EMPRESA DE ENERGIA DE PEREIRA S.A ESP.

Los perfiles, credenciales y/o contraseñas de los colaboradores deberán estar almacenadas cumpliendo con la triada CID (Confidencialidad, Integridad y Disponibilidad), debidamente encriptadas.

8.14 Gestión de contraseñas de usuario

Todos los recursos de información críticos de LA EMPRESA DE ENERGIA DE PEREIRA S.A ESP tienen asignados los privilegios de acceso de usuarios con base en los roles y perfiles que cada colaborador requiera para el desarrollo de sus funciones, definidos y aprobados por las áreas de negocio y administrados por el área de tecnología y comunicaciones.

Todo colaborador o proveedor que requiera tener acceso a los sistemas de información de LA EMPRESA DE ENERGIA DE PEREIRA S.A ESP debe estar debidamente autorizado y debe acceder a dichos sistemas haciendo uso como mínimo de un usuario (ID) y contraseña (password) asignado por la organización. El colaborador debe ser responsable por el buen uso de las credenciales de acceso asignadas. Dichas credenciales son personales e intransferibles.

Las contraseñas de acceso a cada plataforma o aplicativo deberá contar con las siguientes características:

- Contener caracteres alfabéticos como letras mayúsculas (A-Z) y minúsculas (a-z)
- Contener caracteres numéricos dígitos del 0 al 9.
- Cuando el sistema lo permita, se deben incluir caracteres especiales como por ejemplo @ ! # $ % ^ & * ( ) _ + | ~ - = \ ` { } [ ] : " ; ' < > ? , . /

- Se recomienda utilizar en una misma contraseña caracteres alfabéticos, caracteres numéricos y caracteres especiales.
- Es recomendable que las letras alternen aleatoriamente entre mayúsculas y minúsculas.
- Se debe elegir una contraseña que sea de fácil recordación.

Cuando se entrega el nombre de usuario al colaborador, se debe proveer una contraseña inicial segura temporal, la cual deberá ser modificada (cuando sea factible por solicitud automática) ante su primer ingreso.

Las contraseñas se deberán cambiar cada 35 días calendario.

En caso de perdida o bloqueo del perfil el líder de proceso o jefe inmediato deberán enviar un correo electrónico al área de Tecnologías de la Información para realizar el cambio de contraseña o el desbloqueo de la cuenta

En el caso de préstamo de contraseñas el usuario que facilite sus credenciales se responsabiliza de todas las acciones que realizaron con el mismo.

8.15 Escritorio y pantalla limpia

Con el fin de evitar pérdidas, daños o accesos no autorizados a la información, todos los colaboradores de LA EMPRESA DE ENERGIA DE PEREIRA S.A ESP deben mantener la información restringida o confidencial bajo llave cuando sus puestos de trabajo se encuentren desatendidos o en horas no laborales. Esto incluye: documentos impresos, CDs, dispositivos de almacenamiento USB y medios removibles en general. Adicionalmente, se requiere que la información sensible que se envía a las impresoras sea recogida de manera inmediata.

Todos los usuarios son responsables de bloquear la sesión de su estación de trabajo en el momento en que se retiren del puesto, la cual se podrá desbloquear sólo con la contraseña del usuario. Cuando finalicen sus actividades, se deben cerrar todas las aplicaciones y dejar los equipos apagados.

Todas las estaciones de trabajo deberán usar el papel tapiz y el protector de pantalla corporativo, el cual se activará automáticamente después de diez (10) minutos de inactividad y se podrá desbloquear únicamente con la contraseña del usuario.

8.16 Segregación de redes

La plataforma tecnológica de LA EMPRESA DE ENERGIA DE PEREIRA S.A ESP que soporta los sistemas de información debe estar separada en segmentos de red físicos y lógicos e independientes de los segmentos de red de usuarios, de conexiones con redes con terceros y del servicio de acceso a Internet.

La división de estos segmentos debe ser realizada por medio de dispositivos perimetrales e internos de enrutamiento y de seguridad si así se requiere. El área de tecnología informática es el área encargada de establecer el perímetro de seguridad necesario para proteger dichos segmentos, de acuerdo con el nivel de criticidad del flujo de la información transmitida.

LA EMPRESA DE ENERGIA DE PEREIRA S.A ESP establece mecanismos de identificación automática de equipos en la red, como medio de autenticación de conexiones, desde segmentos de red específicos hacia las plataformas donde operan los sistemas de información de la compañía.

Es responsabilidad de los administradores de recursos tecnológicos garantizar que los puertos físicos y lógicos de diagnóstico y configuración de plataformas que soporten sistemas de información deban estar siempre restringidos y monitoreados con el fin de prevenir accesos no autorizados.

Se deberá verificar por parte del personal de redes y telecomunicaciones el cambio de claves por defecto de todos los dispositivos de red de LA EMPRESA DE ENERGIA DE PEREIRA S.A ESP.

El encargado de redes y telecomunicaciones de la compañía deberá garantizar que los canales de comunicación entre proveedores, bancos usuarios externos solo tengan acceso a determinados puertos y/o servicios utilizados.

Se actualizarán continuamente el firmware de los dispositivos de red y UTM de la compañía, garantizando altos estándares de seguridad e intrusión desde internet.

8.17 Identificación de requerimientos de seguridad

La inclusión de un nuevo producto de hardware, software, aplicativo, desarrollo interno o externo, los cambios y/o actualizaciones a los sistemas existentes en LA EMPRESA DE ENERGIA DE PEREIRA S.A ESP, deben estar acompañados de la identificación, análisis, documentación y aprobación de los requerimientos de seguridad de la información, labor que debe ser responsabilidad del área de tecnología informática y las dependencias propietarias del sistema en cuestión.

Los requerimientos de seguridad de la información identificados, obligaciones derivadas de las leyes de propiedad intelectual y derechos de autor deben ser establecidos en los acuerdos contractuales que se realicen entre LA EMPRESA DE ENERGIA DE PEREIRA S.A ESP y cualquier proveedor de productos y/o servicios asociados a la infraestructura de procesamiento de información.

Es responsabilidad del área de tecnología informática garantizar la definición y cumplimiento de los requerimientos de seguridad de la Información y en conjunto con el área Jurídica establecer estos aspectos con las obligaciones contractuales específicas.

9. ACUERDO DE ACEPTACION Y CONFORMIDAD

Al hacer uso personal de los equipos de cómputo, sistemas de información y dispositivos los funcionarios indican su conformidad en acatar las condiciones impuestas para su utilización, y manifiesta su consentimiento a las actividades de monitoreo y control por parte LA EMPRESA DE ENERGIA DE PEREIRA S.A ESP a los activos informáticos de la misma, de conformidad con esta política.

No cumplir esta política puede provocar que se tome acción disciplinaria contra el Usuario de acuerdo con el procedimiento LA EMPRESA DE ENERGIA

DE PEREIRA S.A ESP, que podrían, dependiendo de las circunstancias, prohibir el retiro del equipo de la Empresa para propósitos personales.