

DOCUMENTO DE GERENCIA

259 - - - - -

"Por medio del cual se establece la política de la seguridad de la información para todos los colaboradores de planta y en misión, contratistas, outsourcing y proveedores de ElectroHuila S.A. E.S.P"

EL GERENTE GENERAL DE LA ELECTRIFICADORA DEL HUILA S.A E.S.P.

En uso de las facultades consagradas en el artículo 52 de los estatutos sociales de la empresa y

CONSIDERANDO QUE:

1. *Teniendo en cuenta que la Organización cuenta con un gran desarrollo de las tecnologías de las telecomunicaciones, aplicaciones estratégicas para las diferentes Divisiones, la seguridad es vital para poder proteger el activo más importante que tenemos, nuestra información. La utilización maliciosa de los sistemas de información que cuenta Electrohuila y de los recursos internos puede acarrear desastrosas consecuencias como robo de la información, pérdidas económicas, fraude, software ilegal, códigos maliciosos, entre otras amenazas referente a la seguridad de la información. Es por ello por lo que la Oficina de Sistemas y Organización ha establecido Políticas de Seguridad de la Información bajo el estándar ISO-27001 que contienen medidas de seguridad para proteger la información, en concordancia con la Ley 1581 de 2012 de protección de datos personales y la Ley 1712 de 2014 de transparencia y acceso a la información pública.*
2. *tendría los siguientes beneficios.*
 - **Reducción de costos o gastos** relacionados con incidentes de seguridad
 - **Organización.** Con la implementación de esta norma, es necesario organizar los procesos, incluso los que no están directamente relacionados con la Seguridad en la Información.
 - Se hace una **revisión continua de los riesgos** a los que están expuestos los clientes. Adicionalmente, se hacen controles de manera periódica.
 - **Establece una metodología** gracias a la cual se puede gestionar la seguridad de la información de forma clara y concisa.
 - **Implanta medidas de seguridad** para que los propios clientes puedan acceder a la información.
 - **Protección del sistema de información.** Los usuarios podrán navegar en internet con mínimas amenazas, el hardware, software y equipos estarán protegidos.

- **Protección de la información confidencial de sus empleados y clientes.** Los cibercriminales están en la búsqueda de información personal; un buen sistema dará confianza a sus usuarios.
- **Se mejora la eficiencia en las operaciones.** Los virus pueden afectar la velocidad de las operaciones. Un buen sistema evitará la pérdida de tiempo.

DISPONE

PRIMERO: Autorizar la política de seguridad.

SEGUNDO: Declara en sistema de gestión de calidad.

TERCERO: Divulgarla.

CUARTO: Seguimiento por la Gerencia General

Neiva, **17 SET. 2021**


LUIS ERNESTO LUNA RAMIREZ
Gerente General



ElectroHuila

***POLÍTICAS DE SEGURIDAD DE LA
INFORMACIÓN***

VERSIÓN 1

VIGENCIA, MAYO DE 2021

Electrohuila-Transmitimos buena energía

TABLA DE CONTENIDO

1. OBJETIVO	4
1.1. Objetivos específicos:	4
2. ALCANCE	5
3. DEFINICIONES	6
4. RESPONSABILIDADES	9
5. DOCUMENTOS DE REFERENCIA	10
6. NORMAS PARA LA SEGURIDAD DE LA INFORMACIÓN DE LA ELECTRIFICADORA DEL HUILA S.A.E.S.P.	11
6.1 Política de seguridad de la información de Electrificadora del Huila	11
6.2 Propiedad de la Información	11
6.3 Privacidad de la Información	12
6.4 Procedimiento para la elaboración y clasificación de la Información	14
7. SEGURIDAD FÍSICA Y DEL ENTORNO	16
7.1 Áreas de Acceso Restringido	16
7.2 Normas de seguridad para el Acceso Físico a las áreas restringidas	16
7.2.1 Protección y Ubicación de Equipos y redes	17
7.2.2 Seguridad de Equipos Móviles	17
7.2.3 Suministros de Equipos de Soporte Energético	18
7.2.4 Configuración de Equipos	18
8 Gestión de Comunicaciones y Operaciones	18
8.1 Protección contra código malicioso	18
8.1.1 Software no autorizado	19
8.1.2 Gestión de copias de respaldo	19
8.2 Gestión de seguridad de redes	19
8.2.1 Intercambio de información confidencial	20
8.2.2 Monitoreo	21
8.3 Control de Acceso	22
8.3.1 Política de control de acceso de ELECTROHUILA	22

8.3.2	<i>Gestión de acceso de usuarios</i>	22
8.3.3	<i>Definición nombre de usuarios aplicativos</i>	23
8.3.4	<i>Definición nombre de usuarios acceso a la red corporativa (Dominio)</i>	24
8.3.5	<i>Definición nombre del equipo</i>	24
8.3.6	<i>Definición Identificación del equipo</i>	24
9.	GESTIÓN DE PRIVILEGIOS	25
9.1	<i>Manejo de contraseñas</i>	25
9.1.2	<i>Responsabilidades de los usuarios</i>	26
9.1.3	<i>Política de Escritorio y Pantalla Limpia de Información</i>	27
9.1.4	<i>Controles de seguridad en los servicios de red</i>	27
9.1.5	ENCUESTAS	33

1. OBJETIVO

Establecer directrices para proteger la información de la Electrificadora del Huila E.S.P. asegurando que en ella se cumplan las características de integridad, disponibilidad y confidencialidad mediante, las directrices y normas establecidos por la Gerencia de la Electrificadora del Huila E.S.P., para garantizar altos niveles de seguridad de la información así como los activos de la Organización, nuestros Clientes y grupos de interés.

1.1. Objetivos específicos:

- a) Comunicar a los colaboradores de la Organización, contratistas, outsourcing, proveedores y Clientes las políticas las directrices y normas establecidos por la Gerencia de la Electrificadora del Huila E.S.P.*
- b) Garantizar altos niveles de seguridad a la información de **ELECTROHUILA** y sus Clientes*
- c) Proteger la información en la forma en que se encuentre (física o digital) de las amenazas que afecten su confidencialidad, integridad y disponibilidad.*
- d) Optimizar los controles de seguridad en el manejo de recursos de la oficina de sistemas y organización.*
- e) Establecer mecanismo de apoyo contractual para garantizar la protección de la información que manejan los colaboradores (acuerdo de confidencialidad).*
- f) Proteger los activos de información de la organización y grupos de interés.*

2. ALCANCE

*Este documento establece la política de seguridad de la información y las normas relacionadas con la seguridad y es de obligatorio cumplimiento para todos los colaboradores de planta y en misión, contratistas, outsourcing y proveedores de **ELECTROHUILA**.*

*La consulta permanente de este documento está reservada a los colaboradores de planta y en misión y los contratistas que por sus funciones tienen acceso a los sistemas de información de **ElectrohUILA**.*

Este documento tiene la clasificación de confidencial

La estructura de este documento este enmarcado bajo la norma ISO/IEC 27001:2013 y documenta las normas de seguridad para los siguientes dominios:

- a. A.5 Política de Seguridad de la información*
- b. A.6 Organización de la seguridad de la información.*
- c. A.9 Control de Acceso*
- d. A.11 Seguridad física y del entorno*
- e. A.12 Seguridad de las operaciones.*
- f. A.13 Seguridad de las comunicaciones.*
- g. A.14 Adquisición, desarrollo y mantenimiento de sistemas.*
- h. A.15 Relaciones con los proveedores.*

3. DEFINICIONES

- **ACTIVOS DE INFORMACIÓN:** Recursos del sistema de información o relacionados con éste, necesarios para que Electrohuila funcione correctamente y alcance los objetivos propuestos por su dirección. Se pueden estructurar en cinco categorías: La gente (empleados, contratistas, en misión, practicantes, clientes y entidades), la información en cualquiera que sea su medio (oral, escrita, magnética, óptica, digital), los procesos de la **ELECTRIFICADORA DEL HUILA E.S.P.**, el hardware (equipos de cómputo centrales y locales, redes de comunicación y redes eléctricas) y el software (programas aplicativos en general, licenciamiento, Bases de Datos y sistemas operacionales).
- **CONFIDENCIALIDAD:** Criterio de seguridad de la información que hace referencia a la protección y acceso a la información por parte únicamente de quienes estén autorizados
- **DISPONIBILIDAD:** Criterio de seguridad de la información que hace referencia al acceso a la información y a los sistemas de tratamiento de la misma por parte de los usuarios autorizados cuando lo requieran. La información debe estar en el momento y en el formato que se requiera ahora y en el futuro, al igual que los recursos necesarios para su uso.
- **INCIDENTE:** Un incidente de seguridad de la información está indicado por un solo evento o una serie de eventos, inesperados o no deseados, de seguridad de la información que tienen una probabilidad significativa de poner en peligro las operaciones y procesos del negocio y amenazar la seguridad de la información.
- **INCONSISTENCIA:** La inconsistencia se trata de la falta o carencia de consistencia en la información. También es el término empleado para referirse a la falta de coherencia o estabilidad de la información.
- **INFORMACIÓN:** Es un conjunto organizado de datos, que constituyen un mensaje sobre un determinado ente o fenómeno. Indicación o evento llevado al conocimiento de una persona o de un grupo. Es posible crearla, mantenerla, conservarla y transmitirla.
- **INTEGRIDAD:** Criterio de seguridad de la información que hace referencia al mantenimiento de la exactitud y completitud de la información y sus métodos de proceso. La información debe ser precisa, coherente y completa desde su creación hasta su destrucción.
- **INTERNET:** es un sistema mundial de redes interconectadas entre sí, accesible desde cualquier parte del mundo mediante un dispositivo electrónico diseñado para navegar en la red, extrayendo y/o adicionando información que el usuario considere pertinente en su momento.

- **INTRANET:** el servicio que utiliza tecnología de internet aplicada a una red interna o de área local, con la diferencia que el contenido solo está disponible dentro de la misma red.
- **ISO 27001:** Código de práctica para la administración de la seguridad de la información de la Organización Internacional para la Estandarización (ISO)
- **RECURSOS INFORMATICOS:** Todos aquellos componentes de hardware y programas (software) que son necesarios para el buen funcionamiento y la optimización del trabajo con ordenadores y periféricos, tanto a nivel individual como colectivo u organizativo, sin dejar de lado el buen funcionamiento de los mismos.
- **RESPONSABLE DE LA INFORMACIÓN:** Es responsable de la información que le sea asignada, así como de la clasificación, control y monitoreo del uso y gestión de la misma. Los Responsables de la información son encargados de preservar los principios de seguridad de la información (integridad, disponibilidad y confidencialidad) y deben coordinar la implementación de políticas con otros dueños de información y con custodios de la información.
- **SEGURIDAD DE LA INFORMACIÓN:** Es la preservación de la confidencialidad, integridad y disponibilidad de la información; otras características también pueden estar involucradas, tales como la autenticidad, responsabilidad, aceptabilidad y confiabilidad.
- **SISTEMA DE INFORMACIÓN:** Un sistema de información es un conjunto de datos que interactúan entre sí con un fin común. En informática, los sistemas de información ayudan a administrar, recolectar, recuperar, procesar, almacenar y distribuir información relevante para los procesos fundamentales y las particularidades de cada organización.
- **CORREO ELECTRÓNICO:** Es el intercambio de mensajes escritos digitalmente entre usuarios con el mismo servicio en donde se pueden adjuntar archivos de cualquier tipo, y se realiza por medio de una conexión a Internet o Intranet.
- **EQUIPO MÓVIL:** Un dispositivo de computación móvil se describe como pequeño, ligero, portátil y con WI-fi por la Asociación de la biblioteca pública. Un equipo sin un navegador de Internet no es generalmente referido a como un dispositivo de computación móvil. Hay un número de aparatos clasificados como dispositivos informáticos móviles, como, ordenadores portátiles, PDAs, smartphones y terminales de datos portátiles.
- **BASES DE DATOS:** Es un conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso. Una base de datos es un "almacén" que nos permite guardar grandes cantidades de información de forma organizada para que luego podamos encontrar y utilizar fácilmente.

- **INFRAESTRUCTURA:** *Un elemento fundamental de una organización es su infraestructura tecnológica. Se podría definir como el conjunto de elementos para el almacenamiento de los datos de una empresa. En ella se incluye el hardware, el software y los diferentes servicios necesarios para optimizar la gestión interna y seguridad de información.*

4. RESPONSABILIDADES

Jefe de Oficina de Sistemas y Organización

Es responsable de:

- ✓ *Elaborar y actualizar el Manual de Políticas de Seguridad de la Información.*

Gerencia

Es responsable de:

- ✓ *Aprobar el Manual de Políticas de Seguridad de la Información.*
- ✓ *Velar por el cumplimiento de las Políticas de Seguridad de la Información.*

Talento Humano

Es responsable de:

- ✓ *Publicar, difundir, capacitar y concienciar a todos los colaboradores y externos de **ELECTROHUILA E.S.P** acerca de las políticas de seguridad de la información y su cumplimiento.*
- ✓ *Incluir en los contratos de los terceros la responsabilidad del manejo de la información, acuerdo de confidencialidad donde se comprometa al buen uso de la información que tengan acceso y a la no divulgación no autorizada de la información.*

Subgerencia Administrativa

Es responsable de:

- ✓ *Asegurar que todos los equipos de cómputo de Electrohuila cuentan con un sistema de alimentación continua (UPS).*
- ✓ *Revisar periódicamente el funcionamiento de las UPS y si tienen la capacidad adecuada para soportar la carga.*

5. DOCUMENTOS DE REFERENCIA

- Norma ISO/IEC 27001:2013
- Norma ISO/IEC 27002:2013

6. NORMAS PARA LA SEGURIDAD DE LA INFORMACIÓN DE LA ELECTRIFICADORA DEL HUILA S.A.E.S.P.

6.1 Política de seguridad de la información de Electrificadora del Huila

La Gerencia de la **ELECTRIFICADORA DEL HUILA S.A. E.S.P** teniendo en cuenta que la información y los sistemas implicados en su procesamiento, almacenamiento y comunicación son recursos críticos para el normal desarrollo de los procesos de la Organización y soporte primordial para la consecución de los objetivos estratégicos, establece el Manual de Políticas de Seguridad de la Información en el cual se definen las normas necesarias para preservar su confidencialidad, integridad y disponibilidad e invita a todos los funcionarios y contratistas de la Organización a acatarlas y velar por el uso adecuado y seguro de la información de **ELECTROHUILA** y sus Clientes.

- **Responsabilidad del personal:** Todos los colaboradores y terceros que presten servicios para Electrohuila, serán responsables del cumplimiento de las políticas, normas, procedimientos y estándares establecidos que buscan garantizar la seguridad de la plataforma tecnológica.
- **Responsabilidad en manejo de la información:** Es responsabilidad de todos los colaboradores de Electrohuila, velar por la veracidad, integridad, seguridad, confidencialidad y disponibilidad de los datos y porque la información sea elaborada, generada, operada, modificada, almacenada, conservada, transportada, accedida, divulgada o destruida, de acuerdo con las normas establecidas.

La información confidencial y la jerarquía de los colaboradores han de emplearse de manera acorde con su naturaleza y carácter, y ningún empleado podrá aprovecharse de ellas para obtener ventajas o beneficios para sí o para terceros, ni ejercer tráfico de influencias con ellas.

La circulación de “rumores o comunicaciones informales” es un comportamiento contrario a la cultura de la Organización y a la dignidad de las personas que afecta. El adecuado manejo de la información y de la comunicación obliga a brindar, un trato digno, respetuoso y cordial.

Los contratistas que tengan acceso a la información de Electrohuila tendrán iguales responsabilidades y ésta exigencia deberá hacerse constar en los contratos por ellos suscritos. (Acuerdo de Confidencialidad).

6.2 Propiedad de la Información

Toda la información generada, adquirida o administrada por las personas que laboran para la Organización es propiedad de Electrohuila, y como tal no debe ser empleada para usos diferentes al cumplimiento de sus funciones. Asimismo, toda la información generada, adquirida o administrada por terceros, en virtud de la ejecución de procesos

Electrohuila-Transmitimos buena energía

institucionales y de la prestación de servicios, también se considera propiedad de la Organización y en consecuencia no deberá ser empleada para usos diferentes a los que se acuerden contractualmente.

6.3 Privacidad de la Información

La información institucional será clasificada y requerida por cada Subgerencia según el grado de privacidad y confidencialidad. Los usuarios de la información tendrán restricciones para el acceso a la misma, de acuerdo con las clasificaciones establecidas, en el presente manual.

Las normas y procedimientos restrictivos para el acceso a la información no aplicarán cuando se trate de suministrarla a los entes de control y a las instancias que legalmente tengan derecho, siempre y cuando busquen acceder a ella a través de los conductos regulares.

La información oficial de la Organización, dirigida a públicos externos deberá siempre contar con la revisión y la aprobación de la Gerencia y/o Secretario(a) General y Asesoría Legal, quien la suscribirá.

De acuerdo a la privacidad de la información de Electrohuila cuenta con el siguiente esquema de clasificación:

CLASIFICACIÓN	EJEMPLOS	DESCRIPCIÓN
<i>Pública</i>	<i>Información de página Web</i>	<i>Información compartida con los usuarios externos a ELECTROHUILA. Normas, reglamentos, resultados, servicios ofrecidos, etc.</i>
<i>Interna o Semiprivada</i>	<i>Información de beneficios de los colaboradores, reglamento interno de trabajo.</i>	<i>Información que solo le compete a los colaboradores de ELECTROHUILA, que puede ser conocida por todos estos pero que no debe ser conocida por terceros o personal externo.</i>

<p><i>Privada o Confidencial</i></p>	<p><i>Facturación, Nómina, Presupuesto, Cartera, Jurídica, Calidad, Financiera, Perdidas, Comercial y Operación y mantenimiento. Usuario y Contraseña.</i></p>	<p><i>Información de ELECTROHUILA que soporta los procesos de negocio de información. Procedimientos, políticas, datos de identificación del cliente interno (Colaboradores) y externo (proveedores, usuarios),etc.</i></p>
------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

6.4 Procedimiento para la elaboración y clasificación de la Información

- ✓ *El dueño de la información es responsable por la definición de la clasificación de la misma.*
- ✓ *Toda actualización realizada en la información clasificada, debe estar soportada por un cambio previamente aprobado por el Jefe de oficina y/o división y/o procedimiento del proceso sobre los componentes que afectan la información.*
- ✓ *Debe ser posible, en todo momento, determinar el estado de la información con respecto a posibles cambios relacionados que lo afecte. (Incluir en las aplicaciones diseñadas que contenga la autorización para la elaboración, actualización y anulación de los registros).*
- ✓ *Toda inconsistencia entre la información de las bases de datos y la infraestructura real del sistema, deberá ser reportada a través del aplicativo de mesa de servicio al jefe de la oficina de sistemas y organización.*
- ✓ *Toda inconsistencia entre la información de las bases de datos y la infraestructura real del sistema deberá ser investigada y rastreada para determinar los responsables.*
- ✓ *La información debe seguir los estándares de clasificación definidos.*
- ✓ *La Matriz de información debe documentarse en un formato consolidado por proceso que contenga la clasificación establecida por ELECTROHUILA.*
- ✓ *La Matriz de información se debe actualizar anualmente, con el fin de mantenerla identificada.*

- ✓ *La información no puede desclasificarse o disminuir su nivel de clasificación sin llevar a cabo un análisis, el cual debe ser aprobado por el dueño de la información, quien determinará si su información puede moverse a una clasificación más baja basado en las definiciones de clasificación desarrolladas por ELECTROHUILA. Alternativamente, el dueño de la información determinará si se incrementa el nivel de clasificación de un activo de información basado en dichas definiciones. Es responsabilidad del dueño de la información supervisar sus activos de información y de validar continuamente su clasificación de la información.*

Normas de uso de la información física

- 6.4.1 Cada responsable adaptará el archivo de gestión con las condiciones de seguridad necesarias para archivar y salvaguardar la información confidencial.*
- 6.4.2 Los colaboradores de planta y en misión, contratistas, outsourcing y proveedores de Electrohuila no podrán emplear la información entregada para obtener un beneficio propio, ni podrán compartirla con terceros para que ellos obtengan algún beneficio.*
- 6.4.3 Los documentos o archivos que contienen información confidencial no deben exhibirse en lugares públicos, no pueden dejarse abandonados en salas de reuniones, escritorios o mesas de trabajo en donde puedan ser vistos por personas ajenas a Electrohuila o por personal no autorizado de ésta. De igual forma, los computadores personales o terminales que permitan acceso a información confidencial deben quedar apagados y bloqueados a personas ajenas a Electrohuila o de personal no autorizado.*

7. SEGURIDAD FÍSICA Y DEL ENTORNO

7.1 Áreas de Acceso Restringido

Se definen como aquellas áreas que por la naturaleza y nivel de confidencialidad de la información que se maneja el acceso físico se encuentra restringido y exclusivo para los funcionarios pertenecientes al área. Los invitados sean funcionarios de Electrohuila o no necesitan autorización previa para el ingreso. Las áreas de acceso restringido en **ELECTROHUILA** son:

- a) Datacenter tercer piso - Edificio Promisión.
- b) Cuarto de comunicaciones segundo piso - Edificio Promisión.
- c) Cuarto UPS primer piso - Edificio Promisión.
- d) Oficina pagaduría primer piso - Edificio Promisión.
- e) Gerencia general - Edificio Promisión.
- f) Cuarto de Operadores - Edificio Promisión.
- g) Pagaduría - Edificio Promisión.
- h) CAD - Edificio Promisión.
- i) Oficina de archivo en recursos humanos - Edificio Promisión.
- j) Datacenter primer piso - Edificio Centro de Control.
- k) Cuarto UPS primer piso - Edificio Centro de Control.
- l) Cuarto de Operadores - Edificio Centro de Control.
- m) Cuarto Sonido y Comunicaciones Auditorios - Edificio Auditorio.
- n) Cuarto de comunicaciones Primer Piso - Edificio Saire.
- o) Cuarto de comunicaciones y Datacenter Segundo Piso - Edificio Saire.
- p) Cuarto de comunicaciones Tercer Piso - Edificio Saire.
- q) Oficina Servicio al Cliente PQR - Edificio Saire.
- r) Cuarto de comunicaciones - Edificio Garzon.
- s) Cuarto de comunicaciones - Edificio Pitalito.
- t) Cuarto de comunicaciones - Edificio La Plata.

7.2 Normas de seguridad para el Acceso Físico a las áreas restringidas

- a) La autorización de ingreso de visitantes a las áreas restringidas está en cabeza de los Jefes de las divisiones y se debe otorgar exclusivamente por razones del negocio.
- b) Una vez autorizado el ingreso del visitante, el colaborador visitado debe recogerlo y acompañarlo todo el tiempo durante el recorrido o su permanencia en el área restringida.
- c) Todos los visitantes deben registrar su ingreso en el medio diseñado para tal fin.
- d) Se deben conservar los registros de las bitácoras de acceso a las áreas restringidas de la Organización, con el objeto de contar con información acerca de las personas que entran y salen de las instalaciones con información sensible, la cual deberá ser proporcionada en caso de revisiones de auditoría.

- e) *El uso de cualquier dispositivo de grabación de audio, fotos y video a las áreas de acceso restringido está restringido.*

7.2.1 Protección y Ubicación de Equipos y redes

- a) *Todos los equipos principales que soportan los aplicativos, bases de datos, sistemas de comunicación y sistemas de seguridad se deben alojar en áreas restringidas protegidas por un perímetro de seguridad y con controles de acceso físico.*
- b) *Los Jefes de división y/o oficina de Electrohuila deben establecer controles de seguridad física contra la pérdida de computadores, impresoras, equipos de oficina o sus partes.*
- c) *Está totalmente prohibido retirar computadores o algunos de sus accesorios fuera de las instalaciones de las oficinas de Electrohuila sin la debida autorización y diligenciamiento del formato correspondiente.*
- d) *El retiro de las instalaciones de la Organización de cualquier equipo de cómputo, debe ser autorizado por el Jefe de oficina y/o división. La autorización en las zonas será firmada por el jefe de la zona.*
- e) *El jefe de la oficina de sistemas y organización debe establecer un plan de mantenimientos preventivos y correctivos para todos los computadores de Electrohuila.*
- f) *Está prohibido manipular las redes de cableado estructurado de voz, datos o eléctrico así como instalar cables, extensiones eléctricas, desprender marcaciones de tomas de cableado o dañar los tubos o canaletas de cableado.*
- g) *Está totalmente prohibido fumar, beber y comer cerca de los equipos de cómputo o en áreas de alojamiento de equipos críticos como los centros de cómputo o centros de distribución de cableado estructurado.*
- h) *Se debe dar cumplimiento al manual de Bioseguridad REPORTE INTEGRADO 2020 establecido por la ELECTRIFICADORA DEL HUILA S.A. E.S.P.*

7.2.2 Seguridad de Equipos Móviles

- a) *El suministro de equipos móviles de Electrohuila debe ser autorizado por el jefe de oficina y/o división y se entregará por razones estrictas del negocio.*
- b) *No se debe almacenar ningún tipo de información confidencial en los dispositivos móviles que permanezca parte o todo el tiempo fuera de las instalaciones de **ELECTRIFICADORA DEL HUILA .S.A. E.S.P.***

- c) *Si por razones estrictas del negocio se requiere almacenar información confidencial en equipos móviles, esta información debe estar, en lo posible, cifrada o en su defecto autorizada por el jefe de oficina y/o división respectivo.*
- d) *La seguridad física de los equipos móviles de propiedad de **ELECTROHUILA** está bajo responsabilidad del custodio, por lo tanto dichos equipos no deben ser desatendidos en sitios públicos. En caso de pérdida o daño del dispositivo, se deberá cumplir con el procedimiento de Manual de Activos Fijos diseñado para tal fin.*

7.2.3 Suministros de Equipos de Soporte Energético

- a) *La subgerencia Administrativa debe asegurarse que todos los equipos de cómputo de Electrohuila cuentan con un sistema de alimentación continua (UPS) y que dichos equipos son revisados periódicamente para asegurar su funcionamiento y que tienen la capacidad adecuada para soportar la carga.*

7.2.4 Configuración de Equipos

Todos los equipos de cómputo de la organización que requieran configuración de IP (Internet Protocol), deberán gestionar la aprobación a través del jefe de la división y/o zona y del jefe de la oficina de sistemas y organización.

8 Gestión de Comunicaciones y Operaciones

8.1 Protección contra código malicioso.

- a) *El jefe de la oficina de sistemas, en coordinación con el jefe de oficina y/o división deberán garantizar que los computadores conectados a la red de **ELECTROHUILA** tengan instalado el software antivirus si lo requieren.*
- b) *El software antivirus debe configurar para que realice un escaneo de todas las unidades de almacenamiento de manera automática.*
- c) *El software antivirus debe contar con los mecanismos de actualización automática.*
- d) *Los archivos adjuntos a los correos electrónicos deben ser escaneados por el antivirus y/o herramienta que garantice la seguridad antes de su entrega en el buzón.*
- e) *Todos los archivos enviados a terceros (Clientes, proveedores, entidades de regulación, etc.), sin importar el medio por el cual sean enviados (correo electrónico, CD, DVD, etc.), deben ser escaneados por el antivirus antes de su envío.*
- f) *Si los usuarios detectan un comportamiento anormal del computador y sospechen la presencia de virus o código malicioso, deben reportar de inmediato el incidente a la oficina de sistemas y organización para que se tomen las acciones correspondientes y prevenir la propagación del mismo.*

8.1.1 Software no autorizado

a) La descarga, instalación o uso de aplicativos o programas informáticos no autorizados será considerada como una violación a las Políticas de Seguridad de la Información de la Organización.

8.1.2 Gestión de copias de respaldo

- a) El jefe de la oficina de sistemas es responsable de disponer del sistema de almacenamiento centralizado para custodiar las copias de seguridad de la información, sin embargo es responsabilidad de los dueños de la información coordinar con la oficina de sistemas la información sensible y crítica a respaldar.
- b) El dueño de la información de cada área, debe garantizar que la información a su cargo almacenada en los equipos de cómputo está incluida en los procedimientos de backup.
- c) Los respaldos de información sensible y crítica deben almacenarse en un sitio protegido contra amenazas físicas y ambientales. Así mismo, debe existir un sitio de almacenamiento alterno para dichos respaldos.
- d) El jefe de la oficina de sistemas debe documentar e implementar un sistema de rotación y retención de medios de backup para la información sensible y crítica. La rotación y custodia de medios debe considerar las exigencias de los organismos de control y la legislación aplicable a Electrohuila.
- e) Los usuarios de **ELECTROHUILA** que requieran respaldo de la información sensible y crítica para el negocio almacenado en sus estaciones de trabajo, dentro de los sistemas de backup centralizado, deben hacer un requerimiento a la oficina de sistemas y organización mediante el aplicativo de mesa de servicio.
- f) El jefe de la oficina de sistemas y organización garantizará que se realice una prueba de restauración con el fin de verificar su funcionalidad y que la información almacenada corresponda a la que se debe hacer backup.
- g) El jefe de la oficina de sistemas y organización y los jefes de cada división deben garantizar que toda información de Electrohuila que ya no sea utilizada por la operación y no se requiera por requerimientos legales, será destruida de manera segura evitando su recuperación por un tercero.

8.2 Gestión de seguridad de redes

- a) El jefe de la oficina de sistemas y organización debe garantizar que se instalen sistemas de protección perimetral que filtren el tráfico de información desde las redes externas a la red interna de **ELECTROHUILA**.

Electrohuila-Transmitimos buena energía

- b) *Todas las conexiones hacia redes externas con terceros deben ser autorizadas por el jefe de división a través del aplicativo mesa de servicio, previa verificación técnica de las condiciones del proveedor por el jefe de la Oficina de Sistemas y Organización de que se requiere por razones estrictas del negocio y que los riesgos de la información son conocidos y controlados.*
- c) *Sin excepción todas las conexiones a redes externas, mediante servicios de acceso Internet, que manejen protocolos de encriptación que aseguren la conexión que garanticen altos niveles de seguridad a la información en tránsito.*
- d) *La información relacionada con la configuración de la red y direccionamiento de la misma es considerada confidencial y su acceso físico y lógico debe estar restringido a personal autorizado por el jefe de la Oficina de Sistemas y Organización.*
- e) *La conexión de equipos personales o de terceros a la red interna de **ELECTROHUILA** debe ser previamente solicitada a la oficina de Sistemas y Organización mediante el aplicativo de mesa de servicio para su debida aprobación.*
- f) *El jefe de la oficina de sistemas en coordinación con los jefes de oficina y/o división verificarán que la conexión de equipos personales o de terceros a la red interna se hace por razones estrictas del negocio y que los equipos cuentan con las herramientas de seguridad y las licencias de software de los equipos están debidamente actualizadas y legalizadas.*
- g) *El acceso remoto de colaboradores, contratistas, proveedores o terceros en general a las redes de **ELECTROHUILA** debe ser autorizado por el jefe de la Oficina de Sistemas y Organización en coordinación con los jefes de oficina y/o división previa verificación de que se hace por razones estrictas del negocio y en todos los casos se realizará utilizando sistemas que aseguren la encriptación y seguridad de las conexiones.*
- h) *Programas o procesos que consumen excesivos recursos de Red, los usuarios no deben ejecutar programas o procesos automáticos que consuman demasiados recursos de máquina y que puedan afectar el normal desempeño de la red; en estos casos debe existir una tarea planeada con la oficina de Sistemas y Organización para ejecutarse en horas que no afecte el trabajo de los demás usuarios. En caso de no ser autorizados y estén generando consumos excesivos se desconectará de la red.*

8.2.1 Intercambio de información confidencial

- a) *El envío de archivos a terceros que contengan información confidencial de **ELECTROHUILA** y/o sus Clientes debe ser autorizado por el dueño de la información y debe hacerse por razones estrictas del negocio.*

- b) *Previo al envío de información confidencial a terceros, se debe firmar un acuerdo de confidencialidad entre las partes.*

8.2.2 Monitoreo

- a) *El jefe de la Oficina de Sistemas y Organización implementará los mecanismos necesarios para generar, almacenar y custodiar los registros de auditoría que permitan la trazabilidad de las transacciones realizadas en los aplicativos críticos (si su tecnología e infraestructura lo permita) para la operación de Electrohuila.*
- b) *El jefe de la Oficina de Sistemas y Organización velará para que los nuevos aplicativos adquiridos o desarrollados por Electrohuila, deben contar con la funcionalidad de auditoría y trazabilidad de las transacciones en las cuales se maneje información confidencial.*
- c) *El jefe de la Oficina de Sistemas y Organización debe implementar los mecanismos para generar, almacenar y custodiar los registros de auditoría que permita hacer seguimiento a la confidencialidad, integridad y disponibilidad de los sistemas operativos de servidores críticos, equipos de comunicaciones, equipos de protección perimetral, bases de datos, consolas de antivirus y en general todos los recursos de sistemas críticos para soportar la operación de Electrohuila.*
- d) *El jefe de la Oficina de Sistemas y Organización implementará un procedimiento automático que permita la visualización y análisis de los registros de auditoría de manera preventiva.*
- e) *Los registros de auditoría se deben conservar por un lapso de tiempo de 2 años y el acceso a los mismos debe estar restringido y exclusivo a personal autorizado por el jefe de la Oficina de Sistemas y Organización.*
- f) *Todas las actividades realizadas por los usuarios, con privilegios de administración sobre los sistemas de información (si su tecnología e infraestructura lo permita), deben ser registradas en un log que debe ser revisado periódicamente por el colaborador asignado por el jefe de la Oficina de Sistemas y Organización.*
- g) *Los registros de auditoría que reporten las fallas de aplicativos, servidores, sistemas operativos, bases de datos, sistemas de protección perimetral y sistemas de control ambiental (si su tecnología e infraestructura lo permita), deben ser revisadas periódicamente por los responsables asignados del personal de la Oficina de Sistemas y Organización y de manera preventiva y tomar las medidas adecuadas para detectar y prevenir posibles incidentes que afecten la continuidad de los procesos de Electrohuila.*
- h) *Los responsables de cada una de las aplicaciones debe garantizar que la fecha y hora de todos los recursos informáticos estén sincronizados, para asegurar que los registros reflejan el tiempo exacto de ocurrencia.*

8.3 Control de Acceso

8.3.1 Política de control de acceso de ELECTROHUILA

Todos los aplicativos de **ELECTROHUILA** deben usar controles de acceso lógico que mitíguen los riesgos relacionados con el acceso no autorizado a la información confidencial de la Organización y sus Clientes.

8.3.2 Gestión de acceso de usuarios

- a) La creación de usuarios se realizará mediante solicitud de la mesa de servicio previa aprobación del jefe de división y/o zona, en caso de terceros el supervisor del contrato, que garantice el acceso únicamente a los recursos e información que requiera para desempeñar sus funciones de acuerdo a los perfiles establecidos por la oficina de Sistemas y Organización.
- b) El control de acceso a los diferentes sistemas de información deben ser aprobados por los dueños de la información.
- c) Los usuarios de los sistemas de información de **ELECTROHUILA** son de carácter personal e intransferible. El funcionario y/o externo a cargo debe velar por la confidencialidad del usuario y será responsable de todas las actividades que se realicen con él.
- d) Cuando un funcionario o externo se retira o se traslada del área, el usuario se debe bloquear en todos los sistemas de información. Es responsabilidad de la división de Recursos Humanos reportar a la Oficina de Sistemas y Organización todos los retiros o traslados de personal para el bloqueo correspondiente. De igual forma, los jefes de división, supervisores de terceros y/o zonas de las diferentes áreas deben reportar a la Oficina el retiro de los externos y/o temporales para proceder con el bloqueo del usuario.
- e) El periodo de caducidad del usuario no debe ser superior a 12 meses, en el caso de prorrogar o ser indefinido el contrato, se deberá realizar nuevamente la solicitud de activación de usuarios a través de solicitud de mesa de servicio.
- f) Cuando un usuario es trasladado a otra dependencia y se crea un nuevo cargo, se requiere la solicitud formal del jefe de división, supervisor y/o zona de donde se retira el colaborador y/o de la división de recursos humanos para proceder a inactivar el usuario actual. El jefe de división y/o zona es quien recibe el traslado del colaborador debe solicitar la creación del nuevo usuario mediante una solicitud de la mesa de servicio.
- g) Está totalmente prohibido el uso de usuarios compartidos o genéricos en los sistemas de información de **ELECTROHUILA**.
- h) La división de Recursos Humanos reportará a la Oficina de Sistemas y Organización

los usuarios que no requieren el acceso a los sistemas de información por un periodo de tiempo determinado (ejemplo: colaboradores en vacaciones, licencias, etc) con el fin de que sistemas bloquee el acceso de los mismos. Está totalmente prohibido utilizar usuarios de colaboradores que se encuentren fuera de la Organización.

- i) En el contrato laboral de cada colaborador se establecerá el compromiso para cumplir con las políticas de seguridad y el uso adecuado y seguro del usuario asignado.
- j) Gestión inapropiada y revocación de privilegios de acceso, la administración de la entidad se reserva el derecho de revocar los privilegios de cualquier usuario en cualquier momento. No se permitirá la gestión, instalación, adición y/o modificación que interfiera con el funcionamiento normal y apropiado de los sistemas de información o la red corporativa de Electrohuila, que adversamente afecte la capacidad de otros en el uso de los recursos informáticos o que sea nocivo u ofensivo.

8.3.3 Definición nombre de usuarios aplicativos

Política: Para la definición del nombre de usuario se establece de la siguiente manera:

1. El primer nombre (.) Seguido del primer apellido (.) Seguido de la primera letra del segundo apellido, si el nombre y/o apellidos se repite con los de otra persona, se tomará el segundo nombre y/o el segundo carácter del apellido hasta que se cumpla la política. En caso de no tener segundo apellido se tomará el primer nombre (.) Seguido del primer apellido.
2. Ejemplo: Diego Armando Caballero Perez
diego.caballerop
3. Si se repite con otra cuenta
armando.caballerop
4. Si se repite con otra cuenta
diego.caballeroe

Casos Especiales:

Para la aplicación SAMI WEB y SAMI APP será por código de funcionario, esto a su vez que es una plataforma para operadores.

Las aplicaciones que son para el Cliente (Electrohuila en Línea y Electrohuila App) será por correo electrónico, esto con el fin de asegurar la autenticidad del usuario que está creando la cuenta.

8.3.4 Definición nombre de usuarios acceso a la red corporativa (Dominio)

A: Todos los computadores, portátiles que tienen acceso a la red corporativa tendrán que identificarse en el dominio de Electrohuila con un login compuesto así:

- 1. El primer nombre (.) apellido seguido de la inicial del segundo apellido, si al confirmar el login este se repite con el de otro funcionario, se reemplaza la segunda letra del segundo apellido; si después de esto el login no fuese único se seguirán reemplazando las siguientes letras del segundo apellido hasta que se cumpla la política.*

*Ejemplo: Pepito Armando Perez Serrano
pepito.perezs*

8.3.5 Definición nombre del equipo

A: Todos los computadores, portátiles se denomina el nombre del equipo así:

- 1. Siglas del área al que pertenece el funcionario asignado seguido de un guion (-) y después de un consecutivo compuesto por tres dígitos que lo identifica como único. Esta estructura no debe superar los 15 dígitos.*

*Ejemplo: Oficina de Sistemas y Organización
O&SO-001*

*Ejemplo: Oficina de Responsabilidad Social y Ambiental
ORSA-001*

Casos Especiales

Para el caso de los equipos que se les asignan a los entes de control, estos quedarán denominados según el ente de control que corresponda seguido de un guion (-) y después de un consecutivo compuesto por tres dígitos que lo identifica como único. Esta estructura no debe superar los 15 dígitos.

*Ejemplo: Contraloría
CONTRALORIA-001*

8.3.6 Definición Identificación del equipo

A: Todos los computadores, portátiles se identificarán por la placa de inventario y/o serial que se le asigna al equipo de cómputo.

- 1. XXXXX cuando sea placa*
- 2. SN_XXXXXX cuando no tenga placa y se identifique con serial.*
- 3. Para la identificación de los servidores dentro de la red de Electrohuila, estos tendrán una denominación diferente a la de los equipos de cómputo, sin embargo sus especificaciones técnicas y su uso permiten diferenciarlos el uno del otro dentro del rango de servidores.*

9. GESTIÓN DE PRIVILEGIOS

- a) *Los perfiles de seguridad de los diferentes sistemas de información deben ser definidos y controlados por los dueños de la información y la Oficina de Sistemas y Organización.*
- b) *Los dueños de la información y la Oficina de Sistemas y Organización deben verificar periódicamente (cada dos años) que los usuarios con determinados perfiles son los que deben estar de acuerdo a sus cargos y responsabilidades.*
- c) *La asignación de los perfiles de seguridad para los sistemas de información debe ser aprobada por los dueños de la información mediante una solicitud de la mesa de servicio y asociado a la creación de usuarios.*
- d) *El jefe de la Oficina de Sistemas y Organización debe garantizar que los colaboradores que tienen permisos de administración sobre los aplicativos y sistemas de información, cuentan con un usuario personalizado para realizar sus tareas. Las contraseñas de los usuarios administradores que vienen por defecto en los diferentes sistemas de información deben permanecer en custodia y su uso es exclusivo para eventos de contingencia.*

9.1 Manejo de contraseñas.

- a) *El jefe de Oficina de Sistemas y Organización o a quién delegue, debe configurar los sistemas de autenticación de usuarios para que las contraseñas cumplan con las siguientes características:*
 - a. *Longitud mínima de 8 caracteres*
 - b. *Debe contener Números y letras*
 - c. *Debe contener mayúsculas y minúsculas*

Casos Especiales: *No aplica para usuarios donde el sistema de información no permite estos cambios.*

En el caso de aquellos aplicativos que no solicitan el cambio obligatorio de contraseña en el primer inicio de sesión, es responsabilidad del usuario realizar el cambio.

- b) *Todos los sistemas de información críticos deben solicitar el cambio obligatorio de contraseña en el primer inicio de sesión (si su tecnología e infraestructura lo permite).*

En el caso de aquellos aplicativos que no solicitan el cambio obligatorio de contraseña en el primer inicio de sesión, es responsabilidad del usuario realizar el cambio.

- c) *La contraseña debe expirar cada 90 días y el sistema de información crítico debe pedir cambio obligatorio.*

En el caso de aquellos aplicativos que no solicitan el cambio obligatorio de contraseña, es responsabilidad del usuario realizar el cambio.

El sistema de información crítico debe guardar un historial de la última contraseña y no se puede reutilizar. En el caso de aquellos aplicativos que no cuentan con este control de manera automática, responsabilidad del usuario cumplir la norma tratando de no utilizar la última contraseña.

d) Cuándo y cómo los password pueden ser cambiados por el administrador de Seguridad; El administrador de seguridad solamente puede eliminar un password si el usuario en cuestión ha olvidado su clave de acceso, la solicitud para eliminación de password se debe hacer por la mesa de servicio.

9.1.2 Responsabilidades de los usuarios

a) Los colaboradores y/o externos deben hacer uso adecuado de los usuarios asignados. Entre otros los cuidados que debe tener son:

- a. Bajo ninguna circunstancia se debe prestar el usuario y la contraseña.*
- b. Nunca suministrar el usuario y contraseña vía telefónica.*
- c. Si por razones de soporte, se requiere que los colaboradores de la oficina de sistemas conozcan o ingresen al sistema con la contraseña de un colaborador, el equipo no se debe dejar desatendido y se debe cambiar la contraseña una vez termine el soporte de la oficina de sistemas y organización.*
- d. La contraseña se debe memorizar, nunca la escriba en ninguna parte.*
- e. Se debe cambiar la contraseña cuando se tiene sospecha que ha sido descubierta por terceros.*

b) El jefe de la Oficina de Sistemas y Organización debe garantizar que el protector de pantalla de todos los equipos de Electrohuila sean configurados con los siguientes parámetros:

- a. Activar el protector de pantalla después de 5 minutos de inactividad del computador.*
- b. El desbloqueo requiere contraseña de red.*

c) El fondo de escritorio debe contener información comercial de Electrohuila y debe ser suministrada por la Oficina de Responsabilidad Social y Ambiental.

d) La información en medio físico, clasificada confidencial, que no esté siendo utilizada por el personal autorizado, debe permanecer siempre en un sitio protegido.

9.13. Política de Escritorio y Pantalla Limpia de Información

Prevenir el acceso no autorizado, pérdida y/o daño de la información que se encuentra en los puestos de trabajo, equipos de cómputo, medios extraíbles, dispositivos de impresión y digitalización de documentos, durante y fuera del horario laboral, mediante lineamientos establecidos para que sean aplicados por los funcionarios y contratistas:

- a) Cuando un colaborador se retire temporalmente de su puesto de trabajo, debe hacer un logout de la sesión del aplicativo y activar el bloqueo del escritorio de trabajo del computador mediante la opción de protector de pantalla.*
- b) Al levantarse del puesto de trabajo y al finalizar la jornada laboral, los escritorios deben permanecer despejados y libres de documentos físicos y/o medios extraíbles que contengan información pública clasificada o pública reservada, éstos deben guardarse en un lugar seguro y bajo llave. Los documentos y/o medios extraíbles con información pública también deben guardarse para evitar la pérdida de ésta información.*
- c) Los puestos de trabajo deben permanecer limpios y ordenados.*
- d) Cuando se imprima o digitalice documentos con información pública clasificada o pública reservada, éstos deben retirarse inmediatamente de dichos dispositivos.*
- e) Los dispositivos de impresión y digitalización deben permanecer limpios de documentos*
- f) Los gabinetes, cajones y archivadores de contengan documentos y/o medios extraíbles con información pública, pública clasificada o pública reservada deben quedar cerrados durante cuando el funcionario no está en el escritorio.*

9.14. Controles de seguridad en los servicios de red

a) Uso de dispositivos de almacenamiento externo

1. DEFINICIONES

El uso de medios de almacenamiento externo a los disponibles en los diferentes equipos de cómputo, unidades de red compartidas y servidores de la organización, constituyen una herramienta que sirve para la transferencia rápida y directa de información entre los funcionarios, temporales, contratistas o practicantes de la Organización que a la vez puede exponer información confidencial y sensible de Electrohuila a diversos riesgos y peligros.

2. POLÍTICA

Electrohuila limita el uso de medios de almacenamiento en las diferentes áreas que manejan información clasificada como sensible, privada y semiprivada y de menores de edad.

Electrohuila define los compromisos frente al uso de Dispositivos de Almacenamiento Externo para mitigar el riesgo que la información propietaria, adquirida o puesta en custodia en la organización no esté supeditada a fuga, uso no autorizado, modificación, divulgación o pérdida y que esta debe ser protegida adecuadamente según su valor, confidencialidad e importancia.

Los dispositivos de almacenamiento de uso externo comprenden las unidades que se pueden conectar como una memoria usb, por medio de un cable de datos, mediante una conexión inalámbrica directa a cualquier equipo de cómputo, entre otros se encuentran: memorias flash usb, reproductores portátil mp3/mp4, cámaras con conexión usb, iphones / smartphones, sd cards/mini sd cards/ micro sd cards, pdas / tablets, dispositivos con tecnología bluetooth, tarjetas compact flash, discos duros de uso externo, etc.

Nota: El acceso y empleo de servicios de almacenamiento de archivos On Line, es decir, aquellas unidades virtuales de almacenamiento personal por medio de internet, en las cuales se incluye pero no se limitan los servicios de Onedrive, Dropbox, Rapidshare, GigaSize, MediaFire, 4shared, etc.; están prohibidos a excepción de las solicitudes formales por los jefes de oficina, supervisores y/o jefes de zona.

Uso indebido de dispositivos de almacenamiento externo:

- 1. Almacenar o transportar información clasificada o reservada de Electrohuila.*
- 2. Ejecutar cualquier tipo de programa no autorizado por Electrohuila desde cualquiera de las unidades de almacenamiento en mención.*
- 3. Descargar cualquier archivo sin tomar las medidas de precaución para evitar el acceso de virus en las redes y equipos informáticos.*
- 4. Utilizar mecanismos y sistemas que intenten ocultar o suplantar la identidad del usuario de alguno de estos medios de almacenamiento.*
- 5. Emplear dispositivos de almacenamiento externo con el fin de almacenar o exponer información sensible o reservada de los usuarios o funcionarios, temporales, contratistas o practicantes de Electrohuila.*

En concordancia con lo anterior, queda RESTRINGIDO el uso de Dispositivos de Almacenamiento Externo, en las áreas que tengan acceso a información sensible, privada y semiprivada y de menores de edad.

Los colaboradores de la Oficina de Sistemas y Organización pueden en todo momento y en cualquier área o dependencia de Electrohuila operar, almacenar, adquirir o retirar dispositivos de almacenamiento externo que les permita garantizar la seguridad de la información.

Todos los equipos de cómputo de la organización que requieran una conexión

VPN (virtual private network), se debe solicitar por medio de la mesa de servicio y será autorizada por el jefe de división y/o Zona y/o Interventor.

Para la creación de los usuarios de las VPN se realizará de la siguiente forma: El primer nombre seguido del primer apellido (.) nombre de la entidad a la que pertenece, si al confirmar el login este se repite con el de otro funcionario, se reemplaza el primer apellido por el de segundo apellido; si después de esto el login no fuese único se dejará como la estructura inicial, el primer nombre seguido del primer apellido y seguido por la primera letra del segundo apellido (.) Nombre de la entidad, si no es único se seguirá reemplazando la letra del segundo apellido hasta que deje de ser único.

1. Ejemplo: Pepito Perez Paez de Electrohuila
pepitoperez.electrohuila
2. Se repite con otra cuenta
pepitopaez.electrohuila
3. Se repite con otra cuenta
pepitoperezp.electrohuila

3. SOLICITUD DE ACCESO PARA EL ALMACENAMIENTO POR USB

- Para solicitar el acceso de almacenamiento a través de dispositivos USB, se deberá realizar un solicitud a través de la mesa de servicio.
- Esta solicitud deberá ser aprobada por el jefe de la oficina.

Responsabilidades de los usuarios de dispositivos de almacenamiento externo:

- ✓ Usar de manera responsable la información a su cargo y de los dispositivos de almacenamiento externo que emplee para el transporte de dicha información.
- ✓ Velar porque los medios de almacenamiento externo estén libres de software malicioso, espía o virus para lo cual deberá realizar una verificación de dichos dispositivos cada vez que sea conectado a un equipo de cómputo de la Organización por medio del software de protección dispuesto para tal fin.
- ✓ Todos los eventos realizados sobre los dispositivos de almacenamiento externo, conectados a cualquier equipo de cómputo de la organización, podrán ser auditados con el ánimo de registrar y controlar las actividades realizadas sobre cada uno de estos, la ubicación y el usuario que los empleó. Los intentos de habilitar el uso de estos dispositivos donde su uso ha sido denegado o no autorizado igualmente podrán ser registrados.

b) Normas de uso de equipos de cómputo

- a. Los recursos de Sistemas se deben usar única y exclusivamente para cumplir con las responsabilidades asignadas por Electrohuila.
- b. Solo el personal de la oficina de sistemas y organización o a quien designe el jefe de la oficina en mención está autorizado para llevar a cabo tareas de mantenimiento de software, hardware y del acceso a la red.

- c. *Está prohibido descargar y almacenar archivos o documentos personales, tales como música, videos, fotos, fondos de pantalla, programas, juegos etc. los cuales representan un alto riesgo de virus y daños al computador y de legalidad en su uso por derechos de autor, en caso de evidenciar alguna de las situaciones anteriormente expuestas se notificará al usuario y de ser reincidente será acreedor de sanciones administrativas.*
 - cl. *Prohibición para explorar vulnerabilidades de los sistemas de seguridad, Los usuarios no deben explorar vulnerabilidades o deficiencias en la seguridad de los Sistemas de Información para dañar sistemas o datos, para obtener privilegios mayores a los que han sido autorizados, para tomar recursos de otros usuarios, o para tener acceso a otros sistemas a los cuales no se les ha otorgado autorización apropiada, a no ser que se haga con la intención de ayudar a mejorar la seguridad, en este caso las vulnerabilidades y deficiencias deben ser reportadas inmediatamente a la oficina de sistemas y organización.*
- c) *Normas de uso de correo electrónico.*

Gerente, Subgerentes, jefes de oficina, jefes de división y demás Colaboradores:

1. *Los espacios en disco para el buzón de correo electrónico externo para el gerente, usuarios miembros de la junta directiva, subgerentes, jefes de oficina y/o división y colaboradores que lo soliciten a través de requerimiento de mesa de servicio, será dependiendo del tipo de licencia asignado.*
2. *Servicio de correo electrónico durante 7 días a la semana, 24 horas del día, a excepción de los casos de mantenimiento y procesos externos del proveedor de Internet o por daños que interfieran el normal funcionamiento del centro de cómputo.*
3. *El usuario es el encargado de administrar el espacio de su correo electrónico y en caso de exceder el límite asignado en disco con mensajes recibidos, enviados y/o borrados, recibirá un mensaje informándole el espacio en disco disponible, con el fin de que libere espacio en el buzón y pueda recibir nuevamente mensajes.*
4. *Soporte técnico para la solución de problemas relacionados con el correo electrónico.*
5. *Acceso a Internet en los computadores de las áreas que así lo soliciten mediante requerimiento solicitado a través de la mesa de servicio.*
6. *Acceso a la Intranet o red corporativa de ELECTROHUILA.*
7. *Para la creación de usuarios con respecto a los correos internos y externos, el usuario será creado así:*

El primer nombre (.) Seguido del primer apellido Seguido de la primera letra del segundo apellido, si el nombre y/o apellidos se repite con los de otra persona, se tomará el segundo nombre y/o el segundo carácter del apellido hasta que se cumpla la política. En caso de no tener segundo apellido se tomará el primer nombre (.) Seguido del primer apellido.

Ejemplo: Pepito Alejandro Perez

Otalora pepito.perezo@_

Si se repite con

otra cuenta

alejandro.perezo_____

Si se repite con

otra cuenta

pepito.perez@_____

Caso Especial:

Si el jefe de una división, oficina y/o zona requiere que la estructura del nombre sea por área y/o cargo y no por nombre de funcionario, deberá realizar dicha solicitud en la mesa de servicio. La estructura con el nombre de la división y/o cargo debe ser claro y entendible, en caso de no, el responsable del área de la Oficina de Sistemas y Organización devolverá la solicitud.

Nota: 1. Los contratistas o terceros que mediante contrato por prestación de servicios necesiten de acceso a la Intranet y/o Internet deberán solicitarlo por medio de la mesa de servicio, realizado y autorizado por el supervisor del contrato especificando las restricciones del permiso, la conexión a Internet será cargada al área al cual el contratista realiza el trabajo, el equipo de cómputo del contratista autorizada para disfrutar de estos servicios debe estar debidamente configurada para que cumpla con las políticas de seguridad en sistemas.

- a. Para el caso de las cuentas de correo que ya existen esas no serán objeto de modificación, solo en caso de que sean eliminadas y que requieren la creación nuevamente de la cuenta de correo.*
- b. El servicio de correo electrónico es para uso exclusivo de las actividades relacionadas con el trabajo de cada colaborador.*
- c. Está prohibido utilizar el correo electrónico para atentar contra la integridad de **ELECTRIFICADORA DEL HUILA S.A. E.S.P.** o cualquiera de sus colaboradores.*
- d. Todos los correos recibidos deben ser escaneados por el antivirus.*
- e. Se prohíbe difundir información que incite a la discriminación, la violencia o con contenido ilícito o que atente contra la dignidad humana: aquellas que hacen apología del terrorismo, racismo, pornografía, juegos, música, videos o cualquier tipo de contenido que no esté relacionado con el desempeño laboral.*
- f. Se prohíbe enviar mensajes con fines publicitarios y comerciales de bienes y servicios en beneficio propio, de familiares o terceros.*
- g. Se prohíbe enviar correo Spam es decir correo basura relacionado con falsos virus, publicidad de empresas, cadenas de mensajes, etc.*
- h. Se prohíbe falsificar mensajes de correo electrónico.*
- i. Se prohíbe leer, borrar, copiar o modificar mensajes de correo electrónico de otras personas sin su autorización.*
- j. Se prohíbe enviar mensajes de correo electrónico alterando la dirección electrónica del remitente para suplantar a terceros.*
- k. Está prohibido suscribir el correo electrónico corporativo a servicios de noticias no relacionadas con la actividad profesional.*

- l. No se puede usar para la transmisión, distribución, almacenamiento de cualquier material protegido por las leyes vigentes. Esto incluye todo material protegido por derechos de autor (copyright), Marcas registradas, secretos comerciales u otros de propiedad intelectual.*
- m. La firma predeterminada solo puede contener nombre y apellidos, cargo, extensión y nombre de la organización. No se pueden adjuntar firmas escaneadas.*

d) Normas de uso de internet

- a. El acceso a internet debe ser autorizado por el jefe de oficina y/o división.*
- b. No está permitido acceder a internet con fines diferentes a los propios de las actividades de **ELECTRIFICADORA DEL HUILA S.A. E.S.P.***
- c. No está permitido acceder a páginas web con contenido ilícito que atenten contra la dignidad humana como aquellas que hagan apología del terrorismo, páginas con contenido xenófobo, racista, antisemita, violento, pornográfico, juegos, descargas de música, videos, o cualquier tipo de contenido que no esté relacionado con la actividad laboral.*
- d. Está prohibido el Ingreso a páginas de pornografía infantil.*
- e. Está prohibido descargar música, videos, fotos, fondos de pantalla, programas, juegos etc. los cuales representan un alto riesgo de virus y daños al computador y de legalidad en su uso por derechos de autor.*
- f. Está prohibido utilizar los servicios de internet para la transmisión, distribución o almacenamiento de cualquier archivo protegido por las leyes vigentes. Esto incluye todos los archivos protegidos por derechos de autor, marcas registradas, secretos comerciales u otros de propiedad intelectual.*

e) Normas de uso de la Intranet

- a) Respetar la privacidad de otros usuarios. No está permitido obtener copias intencionales de archivos, códigos, contraseñas o información ajena; ni suplantar a otra persona en una conexión que no le pertenece o enviar información a nombre de otra persona sin consentimiento del titular de la cuenta.*
- b) Respetar la protección legal otorgada a programas, textos, artículos y bases de datos según legislación internacional sobre propiedad intelectual y las normas pertinentes de nuestro país.*
- c) Respetar la integridad de los sistemas de computación. Esto significa que ningún usuario podrá adelantar acciones orientadas a infiltrarse, dañar o atacar la seguridad informática de la **ELECTRIFICADORA DEL HUILA E.S.P.**, a través de medio físico o electrónico alguno.*
- d) No obtener ni suministrar información sin la debida autorización, no dar a conocer códigos de seguridad tales como contraseñas a otras personas, o entorpecer por ningún medio el funcionamiento de los sistemas de información y telecomunicaciones.*

- e) La creación de nuevas redes o reconfiguración de las existentes, solo podrá ser adelantada por personal autorizado por la Oficina de Sistemas y Organización.
- f) El uso indebido de los recursos de la Intranet recaerá directamente sobre el usuario que se registra en el sistema y sobre el recaerá toda la responsabilidad de los actos realizados.

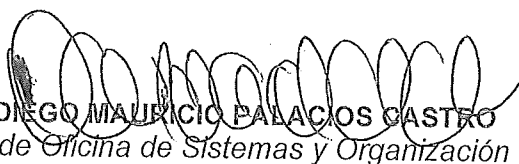
"Excepción: en caso que el área requiera que las cuentas de correo tengan un nombre específico y no aplique el nombre del usuario, esta observación se deberá realizar a través del requerimiento documentado en la mesa de servicio y se deberá crear la cuenta como lo solicite el área"

9.1.5. ENCUESTAS

Todos los usuarios que hacen uso de la mesa de servicio para el registro, control y seguimiento de los requerimientos, deberán diligenciar las encuestas, elaboradas por el proceso del área de Sistemas y Organización, a fin de recibir por parte de estos la retroalimentación de los casos registrados para poder conocer el grado de satisfacción.



↑ LUIS ERNESTO RAMIREZ LUNA
Gerente General



DIEGO MAURICIO PALACIOS CASTRO
Jefe de Oficina de Sistemas y Organización

