ElectroHuila

195 - - - - -

DOCUMENTO DE GERENCIA

"Por medio del cual se adopta la Versión 2 de la Política de Seguridad de la Información, aplicable a todos los colaboradores de planta y en misión, contratistas, outsourcing y proveedores de ElectroHuila S.A. E.S.P."

LA 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:

1. Que la Electrificadora del Huila S.A. E.S.P. ha alcanzado un importante desarrollo en tecnologías de la información y telecomunicaciones, siendo la **información uno de los activos más críticos** para el cumplimiento de sus objetivos estratégicos.

2. Que la **utilización indebida o maliciosa** de los sistemas de información y de los recursos tecnológicos internos puede generar consecuencias severas como robo de información, fraude, pérdidas económicas, instalación de software no autorizado, entre otras amenazas.

3. Que la **Oficina de Sistemas y Organización**, conforme a su rol institucional, ha elaborado y actualizado la **Política de Seguridad de la Información – Versión 2**, conforme a los lineamientos establecidos en la **norma internacional ISO/IEC 27001:2013**, y ha incorporado medidas técnicas y administrativas que garantizan la confidencialidad, integridad y disponibilidad de la información institucional.

4. Que esta política está debidamente alineada con el marco legal y normativo colombiano, incluyendo entre otras: la **Ley 1581 de 2012** (protección de datos personales), la **Ley 1712 de 2014** (transparencia y acceso a la información pública), la **Ley 1273 de 2009** (delitos informáticos), y los decretos reglamentarios respectivos.

5. Que la implementación de la presente versión traerá consigo beneficios organizacionales como:
   - Reducción de costos por incidentes de seguridad.
   - Organización y fortalecimiento de los procesos internos.
   - Gestión eficiente de riesgos tecnológicos.
   - Protección de la infraestructura informática.
   - Seguridad de la información confidencial de empleados, clientes y proveedores.
   - Fomento de una cultura institucional basada en la ciberseguridad.

- Cumplimiento de estándares internacionales en la materia.

RESUELVE:

ARTÍCULO PRIMERO: Adoptar la Versión 2 de la Política de Seguridad de la Información de la Electrificadora del Huila S.A. E.S.P., la cual será de **cumplimiento obligatorio** para todos los colaboradores de planta y en misión, contratistas, outsourcing y proveedores, en todos los procesos donde se maneje información institucional.

ARTÍCULO SEGUNDO: Incluir dicha política como componente esencial del **Sistema de Gestión de Calidad** y del **Sistema de Gestión de Seguridad de la Información (SGSI)** institucional.

ARTÍCULO TERCERO: Divulgar y socializar esta política a través de los canales de comunicación internos, asegurando su comprensión, apropiación y aplicación efectiva por parte de todos los actores involucrados.

ARTÍCULO CUARTO: Encomendar a la **Gerencia General** y a la **Oficina de Sistemas y Organización** la **supervisión, seguimiento y evaluación periódica** de la implementación de esta política, promoviendo su mejora continua.

ARTÍCULO QUINTO: La presente política entrará en vigencia a partir de la fecha de aprobación del presente Documento de Gerencia y se mantendrá vigente hasta que sea actualizada, modificada o derogada expresamente por la Empresa.

COMUNÍQUESE, PUBLÍQUESE Y CÚMPLASE.

Dado en Neiva, a los ___ días del mes de _____ de 2025.

09 OCT. 2025

NIKA DUNIEZHKA CUÉLLAR CUENCA
Gerente General

Elaboro: Diego Mauricio Palacios Castro
Revisó: Jorge Lorenzo Escandón Ospina
Aprobó: Luis Alfredo Carballo Gutiérrez

ElectroHuila

Transmitimos Buena Energía

POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

VERSIÓN 2

Tabla de Contenido

Índice de Ilustraciones

Índice de Tablas

1. Finalidad

El propósito de esta política es establecer la dirección, los principios y las reglas básicas para la seguridad de la información, acogiéndose y dando cumplimiento a lo dispuesto en la norma internacional ISO-27001. Así como también, establecer una cultura de seguridad y confianza para todo el personal que integra la **ELECTRIFICADORA DEL HUILA S.A. E.S.P. – ElectroHuila S.A. E.S.P.** El esfuerzo efectivo de todos los funcionarios o contratistas de la empresa puede ayudar a proteger la información sensible de los clientes, proceso, proyectos, objetivos estratégicos entre otros.

La política de Seguridad de la Información reduce el riesgo de accesos no autorizados, revelación, robo, pérdida y daño de información durante y fuera del horario de trabajo normal.

2. Ámbito y Usuarios

El objetivo de este documento es definir el propósito, la dirección, los principios y las reglas básicas para la seguridad de la información.

Este documento se aplica a todos los procesos, actividades, colaboradores y contratistas de la Electrificadora del Huila S.A. E.S.P., así como todos nuestros Clientes y grupos de interés.

3. Objetivo

Establecer directrices para proteger la información de la Electrificadora del Huila S.A. 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 S.A. 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.

3.1 Objetivos Específicos

- 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 S.A. E.S.P.
- Garantizar altos niveles de seguridad a la información de Electrohuila S.A. E.S.P. y sus Clientes
- Proteger la información en la forma en que se encuentre (física o digital) de las amenazas que afecten su confidencialidad, integridad y disponibilidad.
- Optimizar los controles de seguridad en el manejo de recursos de la Oficina de Sistemas y Organización.
- Establecer mecanismo de apoyo contractual para garantizar la protección de la información que manejan los colaboradores (acuerdo de confidencialidad).
- Proteger los activos de información de la organización y grupos de interés.

4. 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 Electrificadora del Huila S.A. E.S.P

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 S.A. E.S.P.

Este documento tiene la clasificación de confidencial, la estructura es bajo la norma ISO/JEC 27001:2013 como se muestra a continuación:

Ilustración 1: Cumplimiento del alcance de la Política de Seguridad de Información

Dentro del alcance se documenta las normas de seguridad para los siguientes dominios:

DOMINIO ISO 27001	OBJETIVOS DE CONTROL
Política de Seguridad de la información	A.5
Organización de la seguridad de la información	A.6
Seguridad del Recurso Humano	A.7
Gestión de Activos	A.8
Control de Acceso	A.9
Seguridad física y del entorno	A.11
Seguridad de las operaciones	A.12
Seguridad de las comunicaciones	A.13
Adquisición, desarrollo y mantenimiento de sistemas	A.14
Relaciones con los proveedores	A.15

Tabla 1 Alcance Dominios ISO 27001:2013

Para el alcance de esta política se incluyen los procesos que se muestran en la siguiente ilustración:

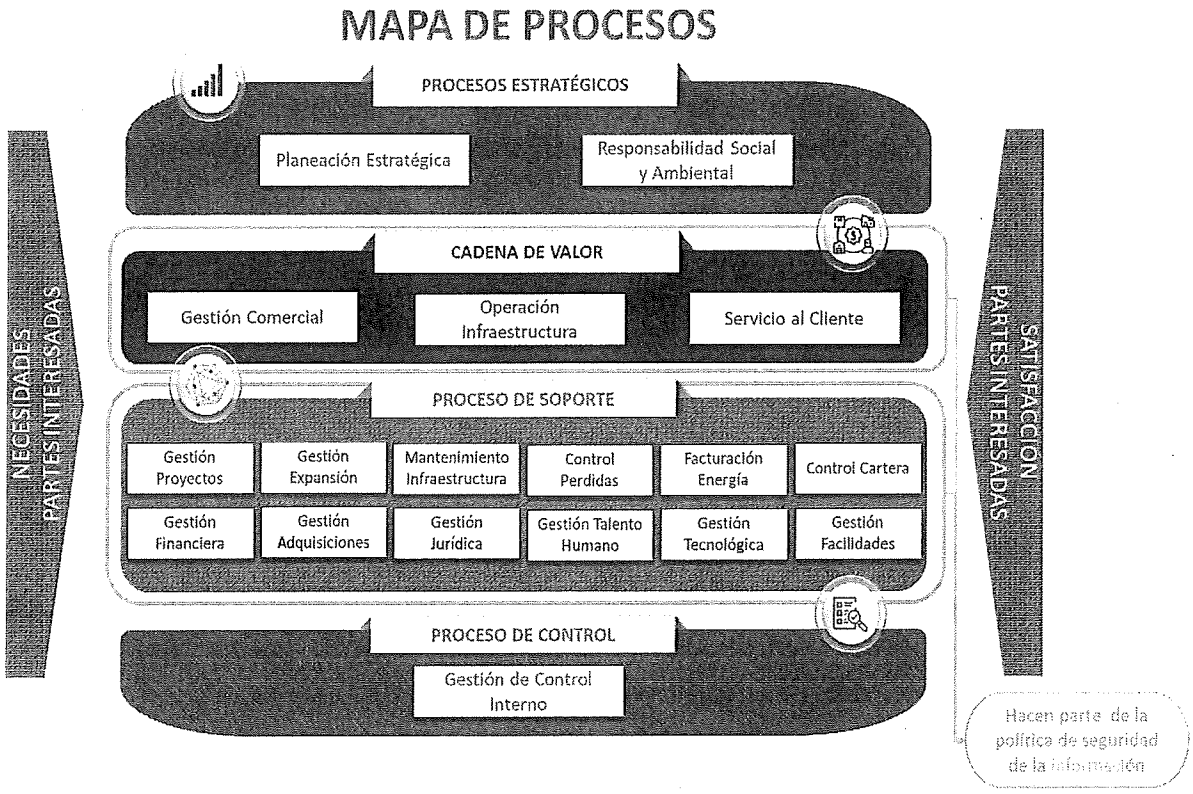

Ilustración 2: Procesos incluidos en el alcance de la Política de Seguridad de la Información

5. Marco legal y normativo aplicable:

Todas las políticas de seguridad de la información y ciberseguridad deben obedecer a las leyes aplicables, tal como leyes asociadas a la protección de los datos personales, protección de la información personal y documentos electrónicos, normas relativas a la de seguridad de datos, reglamentación de ciberseguridad y ciberdefensa, etc., las cuales se entienden incorporadas a esta política y prevalecen sobre éstas.

Las políticas de seguridad y el sistema de gestión de seguridad definidos velan por el cumplimiento a los requerimientos y a la regulación establecida en la normatividad vigente:

- **Constitución Política de Colombia (1991):**
  - **Artículo 15:** Derecho a la intimidad personal y familiar, al buen nombre, y el derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas (Hábeas Data). Este artículo es la base fundamental de la protección de datos.
  - **Artículo 20:** Libertad de expresar y difundir el pensamiento y opiniones, y el derecho a informar y recibir información veraz e imparcial. Implica la responsabilidad social de los

medios de comunicación y la libertad de prensa, pero también el límite a la difusión de información que afecte derechos fundamentales.

- **Artículo 74:** Derecho de acceso a los documentos públicos, salvo los casos que determine la ley. Pilar de la transparencia y el acceso a la información pública.

- **Ley 527 de 1999 (Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se dictan otras disposiciones):**
  - **Artículos 5, 6 y 7:** Validez jurídica y probatoria de los mensajes de datos y las firmas digitales. Fundamental para la confiabilidad de las transacciones y comunicaciones electrónicas de la empresa.
  - **Artículos 9 y 10:** Reconocimiento jurídico de los mensajes de datos como medio de prueba.
  - **Artículo 11:** Principio de equivalencia funcional.

- **Ley 594 de 2000 (Ley General de Archivos y se dictan otras disposiciones):**
  - **Artículos 1 y 2:** Objeto y ámbito de aplicación, estableciendo las reglas y principios generales que regulan la función archivística del Estado. Esencial para la gestión y conservación de la información de ELECTROHUILA, incluyendo la digital.
  - **Artículo 13:** Obligatoriedad de la gestión documental.

- **Ley 1266 de 2008 (Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones):**
  - **Artículos 4 al 8:** Principios de la administración de datos (veracidad, finalidad, circulación restringida, seguridad), derechos de los titulares y deberes de los operadores de los bancos de datos. Aunque se centra en datos crediticios, sus principios son aplicables a la gestión de datos personales en general.

- **Ley 1437 de 2011 (Código de Procedimiento Administrativo y de lo Contencioso Administrativo - CPACA):**
  - **Artículos 13 al 33:** Derecho de petición, acceso a la información y su reserva. Establece los procedimientos para la solicitud de información y los límites a su divulgación por razones de reserva legal o clasificación.

- **Ley 1581 de 2012 (Por la cual se dictan disposiciones generales para la protección de datos personales):**
  - **Artículos 4 al 9:** Principios rectores (legalidad, finalidad, libertad, veracidad o calidad, transparencia, acceso y circulación restringida, seguridad, confidencialidad), derechos de los

titulares (acceso, actualización, rectificación, supresión, revocatoria de la autorización) y deberes de los responsables y encargados del tratamiento de datos personales. Esta ley es el pilar fundamental de la protección de datos personales en Colombia.

- **Artículo 17:** Deberes de los responsables del Tratamiento.
- **Artículo 18:** Deberes de los Encargados del Tratamiento.
- **Artículo 25:** Creación y administración del Registro Nacional de Bases de Datos (RNBD) por la Superintendencia de Industria y Comercio (SIC).

- **Ley 1712 de 2014 (Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones):**
  - **Artículos 4, 6 y 18:** Concepto y principios del derecho de acceso a la información pública, excepciones a la regla general de divulgación (información reservada y clasificada). Fundamental para la gestión de la información en una entidad pública como ELECTROHUILA.
  - **Artículos 22 al 28:** Procedimientos de acceso a la información pública.

- **Ley 1757 de 2015 (Por la cual se dictan disposiciones en materia de promoción y protección del derecho a la participación democrática y se dictan otras disposiciones):**
  - Esta ley, como estatutaria, refuerza el acceso a la información como un mecanismo para la participación ciudadana. Sus disposiciones complementan la Ley 1712 en el fomento de la transparencia.

- **Ley 1273 de 2009 (Por medio de la cual se modifica el Código Penal y se crean nuevos tipos penales relacionados con delitos informáticos y otras infracciones):**
  - **Artículos 269A al 269H (Libro II, Título XII, Capítulo VI):** Delitos contra la protección de la información y de los datos (ej. acceso abusivo a un sistema informático, violación de datos personales, interceptación de datos informáticos, daño informático, hurto por medios informáticos). Es crucial que la política establezca que las conductas que encajen en estos tipos penales serán puestas en conocimiento de las autoridades competentes.

- **Decreto 1074 de 2015 (Decreto Único Reglamentario del Sector Comercio, Industria y Turismo, Parte 2, Título 2, Capítulo 25, Subcapítulo 2 - Protección de Datos Personales):**

  Reglamenta parcialmente la Ley 1581 de 2012. Es vital para entender la aplicación práctica de la ley, especialmente en lo referente a la autorización del titular, el deber de informar, y los derechos de los titulares.

- **Decreto 1081 de 2015 (Decreto Único Reglamentario del Sector Presidencia de la República, Parte 1, Título 2, Capítulo 1, Sección 1 - Transparencia y Acceso a la Información Pública):**

Reglamenta parcialmente la Ley 1712 de 2014. Establece lineamientos para la implementación de la ley de transparencia en las entidades públicas.

- **Decreto 1377 de 2013** (Reglamenta parcialmente la Ley 1581 de 2012).
- **Decreto 1078 de 2015** (Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones).
- **NTC ISO/IEC 27001:2013** - Norma Técnica Colombiana Sistemas de Gestión de Seguridad de la Información.
- Acuerdos, ordenanzas, Resoluciones, circulares de las entidades públicas u organismos de control.

6. Definiciones

DEFINICIONES/ACRÓNIMOS	DESCRIPCIÓN
Activo de información	Recursos del sistema de información o relacionados con éste, necesarios para que ElectroHuila S.A. E.S.P. 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 S.A. 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).
Autorización	Consentimiento previo, expreso e informado del director o jefe del área donde pertenece el usuario que solicita un servicio.
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.
Brecha de seguridad	Es un evento en el que se viola la seguridad de un sistema, red o dispositivo, permitiendo el acceso no autorizado a información confidencial o sensible. Este acceso puede ser intencional, como un ataque de hackers, o accidental, como un error humano que expone datos.
Ciberseguridad	Capacidad empresarial para defender y anticipar las amenazas cibernéticas con el fin de proteger y asegurar los datos, sistemas y aplicaciones en el ciberespacio que son esenciales para la operación de la entidad.
Ciberespacio	Entorno resultante de la interacción de personas, software y servicios en Internet a través de dispositivos tecnológicos

	conectados a dicha red, el cual no existe en ninguna forma física.
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.
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,
Dato personal	Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables
Datos sensibles	Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos.
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.
Equipo de cómputo/computador	Dispositivo electrónico capaz de recibir un conjunto de instrucciones y ejecutarlas realizando cálculos sobre los datos numéricos, o bien compilando y correlacionando otros tipos de información.
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.
Funcionario – usuario / contratista	Se refiere a directores, gerentes, funcionarios o empleados permanentes o temporales y practicantes o pasantes que forman parte de ElectroHuila S.A. E.S.P.
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.
Incidente de seguridad	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 / red interna	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)
Propietario de Activo de Información	Responsable de la creación de la información, responsable del activo, es quien debe velar por el cumplimiento de los requerimientos establecidos frente a las propiedades de disponibilidad, confidencialidad e integridad.
Recursos informáticos	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 estos.
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 esta. 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.
Riesgos de seguridad de la información	Son la posibilidad de que amenazas aprovechen vulnerabilidades en sistemas y datos, causando pérdidas o daños. Estos riesgos incluyen desde amenazas internas como el uso indebido de datos por empleados, hasta externas como ataques de phishing o programa maligno.
Seguridad de la Información	Es el conjunto de políticas, estrategias, metodologías, recursos, soluciones informáticas, prácticas y competencias para proteger, asegurar y preservar la confidencialidad, integridad y disponibilidad de la información que se almacene, reproduzca o procese en los sistemas informáticos de la entidad. Es la preservación de la confidencialidad, integridad y disponibilidad

	de la información; otras características también pueden estar involucradas, fales 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.
Sistema de Gestión de Seguridad de la Información (SGSI)	Es un conjunto de políticas, procedimientos, y herramientas que una organización utiliza para proteger su información y recursos informáticos. Se basa en la identificación, evaluación y gestión de riesgos, y la implementación de controles para proteger la información contra amenazas internas y externas.
Tratamiento de datos personales	Se refiere a cualquier operación o conjunto de operaciones realizadas sobre datos personales, como la recolección, registro, organización, conservación, utilización, comunicación, supresión o destrucción.

Tabla 2 Definición de conceptos de seguridad de la información

7. Responsabilidades

La Política de Seguridad de la Información es de aplicación obligatoria para todo el personal de la Electrificadora del Huila S.A. E.S.P., cualquiera que sea su situación contractual, la dependencia a la cual se encuentre adscrito y el nivel de las tareas que desempeñe.

Todos los colaboradores contratistas, proveedores deben utilizar los activos de información de la empresa para el desarrollo de las actividades misionales, nunca para su uso personal o en detrimento de los objetivos de la empresa.

Así mismo, todos los colaboradores, contratistas y proveedores deben salvaguardar la confidencialidad de la información que por razones de su cargo o responsabilidades designada esté bajo su custodia.

7.1 Jefe de Oficina de Sistemas y Organización

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

7.2 Gerencia

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

7.3 Talento Humano

- Publicar, difundir, capacitar y concienciar a todos los colaboradores y externos de ElectroHuila S.A. 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.

7.4 Subgerencia Administrativa

- Asegurar que todos los equipos de cómputo de ElectroHuila S.A. E.S.P. 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.

7.5 Funcionarios/Usuarios /contratistas

- Conocer y cumplir las disposiciones de esta Política.
- Solicitar orientación cuando sea requerido.
- Conocer Reportar inquietudes y preocupaciones con respecto a esta Política.
- Responsables de cualquier acción que se realice utilizando el nombre y contraseña de usuario que le sean asignados.

8. Declaración De Política General De La Seguridad De La Información

La Electrificadora del Huila S.A. E.S.P. establece mecanismos para asegurar la implementación y gestión de los lineamientos establecidos para la seguridad de la información y ciberseguridad de acuerdo con el estándar internacional ISO 27001.

8.1 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 S.A. E.S.P. y sus Clientes.

- **Responsabilidad del personal:** Todos los colaboradores y terceros que presten servicios para ElectroHuila S.A. E.S.P., 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 S.A. E.S.P., 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 S.A. E.S.P. tendrán iguales responsabilidades y esta exigencia deberá hacerse constar en los contratos por ellos suscritos. (Acuerdo de Confidencialidad).

9. Seguridad del Recurso Humano

La Electrificadora del Huila S.A. E.S.P. debe tener en cuenta el ciclo de vida del recurso humano, es decir, establecer controles y mecanismos para asegurar la implementación de los lineamientos establecidos antes, durante y después de su contratación, teniendo en cuenta el estándar internacional ISO 27001.

9.1 Control de la Política de Personal

En este sentido se darán los lineamientos en las tres etapas establecidas en el ciclo de vida del recurso humano.

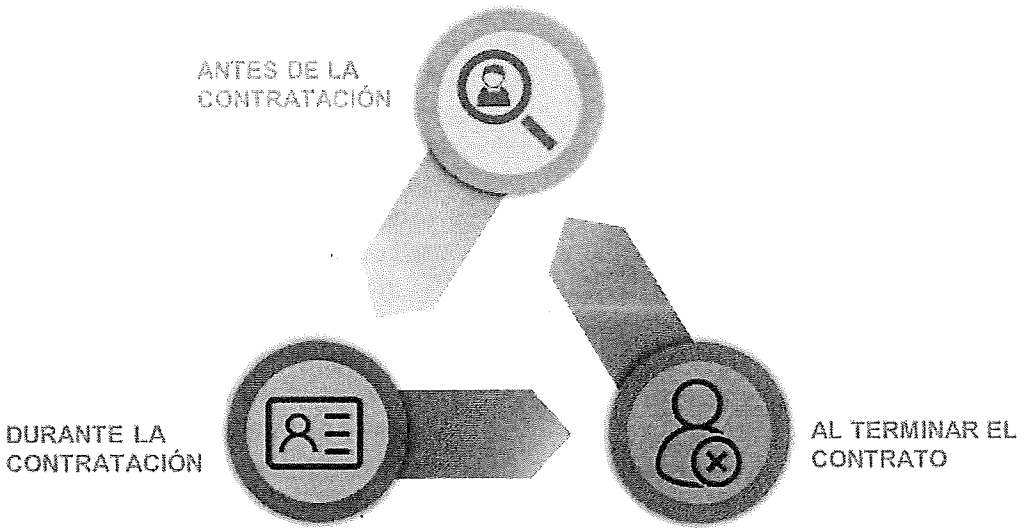

Ilustración 3: Ciclo de Vida del Recurso Humano

9.1.1 Antes de la contratación:

Dentro del procedimiento de selección de personal, el responsable del Área de Recursos Humanos, teniendo en cuenta las leyes y reglamentos, debe realizar los siguientes controles de verificación en el momento que se solicita el puesto:

- Verificación de referencias
- Verificación de la hoja de vida completa
- Verificación de la identidad del aspirante
- Verificación de competencia
- Pruebas psicotécnicas
- Verificar que sea una persona confiable por medio de consulta de antecedentes.

9.1.2 Durante el periodo de contratación:

Dentro de esta etapa se debe tener en cuenta a que tipo de información tiene acceso el colaborador contratado.

- Compromiso de Confidencialidad y no divulgación:

Responsable	DESCRIPCIÓN
Colaboradores	Los colaboradores y contratistas que tengan acceso a información reservada, confidencial o sensible al iniciar las actividades en ElectroHuila S.A. E.S.P., deberán firmar el Compromiso de Confidencialidad y no divulgación, **ANTES** de acceder a dicha información contenida en cualquier medio, teniendo en cuenta el tratamiento de la información de ElectroHuila S.A. E.S.P. El colaborador al firmar el compromiso de confidencialidad declara que conoce y acepta la existencia de actividades específicas que pueden ser objeto de control y monitoreo. Las actividades se detallan con el fin de no violar el derecho a la privacidad del colaborador.
Recursos Humanos	• El responsable de Área de Recursos Humanos establecerá el procedimiento para la suscripción del Compromiso de Confidencialidad donde se incluirán aspectos sobre: o Suscripción inicial del Compromiso por parte de la totalidad del personal. o En caso de modificación del texto del Compromiso se debe volver a firmar el documento por parte de los colaboradores. o El documento firmado del compromiso de confidencialidad será almacenado de forma segura por el responsable del Área de Recursos Humanos.
Área Legal	El responsable del Área Legal revisará anualmente el contenido del Compromiso.

Tabla 3 Compromiso de confiabilidad

- Todos los colaboradores y contratistas al iniciar las actividades en ElectroHuila S.A. E.S.P., deberán firmar la cesión de derechos de propiedad intelectual a favor de la Electrificadora del Huila S.A. E.S.P. sobre los desarrollos y modificaciones que se realicen fruto de su trabajo en la entidad.
- Todos los colaboradores y contratistas deben seguir las normas sobre el manejo y tratamiento de cada tipo de información de acuerdo con lo definido en el ítem de la clasificación de activos de información para la Electrificadora del Huila S.A. E.S.P.
- Sí se incumple cualquiera de las normas de seguridad establecidas, se debe abrir un proceso disciplinario, teniendo en cuenta la responsabilidad en incidentes de seguridad de la información en los que se determine y demuestre la participación de algún colaborador de la Electrificadora del Huila S.A. E.S.P.
- Establecer un canal anónimo mediante el cual los colaboradores puedan reportar posibles incidentes de seguridad de la información en la Electrificadora del Huila S.A. E.S.P.
- Realizar capacitaciones del modelo de seguridad de la información aprobado, también, capacitaciones periódicas en temas de seguridad, todo esto, con el fin de que los colaboradore tomen conciencia sobre la seguridad de la información pertinente a sus roles, y lograr crear una cultura de seguridad al interior y exterior de la Electrificadora del Huila S.A. E.S.P. El programa de capacitaciones continuas en seguridad que deben cubrir., como mínimo, los siguientes aspectos:
  - Concientización sobre riesgos de seguridad de la información.
  - Conocimiento del modelo, políticas, normas y procedimientos asociados a la seguridad de la información.
  - Matriz de Contacto para información de problemas o reportes de incidentes de seguridad de la información.
  - Tips prácticos de seguridad de la información orientado a las actividades que realiza cada colaborador según sus funciones.

9.1.3 Al terminar la contratación:

Dentro del procedimiento de terminación de contrato, el responsable del Área de Recursos Humanos debe solicitar a La Oficina de Sistemas y Organización la realización del backup de la información que el colaborador manejaba, así como también la eliminación de todos los usuarios, contraseñas y accesos remotos de teletrabajo a los que tenía acceso el colaborador.

La Oficina de Sistemas y Organización debe dar un visto bueno, o una paz y salvo. Esta paz y salvo debe ser requisito para completar el proceso de desvinculación.

El Almacén recibe los activos de información y queda disponible para su respectivo backup o reasignación.

9.2 Seguridad de Puestos de Trabajo y la Asignación de Recursos.

La Oficina de Sistemas y Organización de ElectroHuila S.A. E.S.P., deberá incorporar las funciones y responsabilidades de seguridad de la información, teniendo en cuenta la protección de los activos, la ejecución de procesos o actividades determinadas de acuerdo con el puesto de trabajo.

10. Gestión de Activos

Dentro de este dominio se pretende determinar la propiedad de la información de ElectroHuila S.A. E.S.P., y su clasificación con el fin de brindarles un tratamiento apropiado de acuerdo con su clasificación.

10.1 Inventario de Activos

La Oficina de Sistemas y Organización de ElectroHuila S.A. E.S.P., identificará los activos importantes y críticos asociados a cada sistema de información, teniendo en cuenta sus propietarios y su ubicación.

El responsable de cada dependencia involucrado deberá tener un inventario con la información relevante y deberá actualizarlo loa momento de ser modificada la información registrada y revisarlo cada seis meses.

10.2 Propiedad de la Información

Toda la información generada, adquirida o administrada por las personas que laboran para la Organización es propiedad de ElectroHuila S.A. E.S.P., 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 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.

10.3 Clasificación de la Información

La información de ElectroHuila S.A. E.S.P será clasificada por cada dependencia según el grado de privacidad, integridad, disponibilidad y confidencialidad.

Los usuarios de la información tendrán restricciones para el acceso a la misma, de acuerdo con las clasificaciones y niveles de permisos y privilegios establecidos, en la presente política.

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 con la privacidad de la información de ElectroHuila S.A. E.S.P. cuenta con el siguiente esquema de clasificación:

CLASIFICACIÓN	DESCRIPCIÓN	EJEMPLOS
Pública	Información compartida con los usuarios externos a ElectroHuila S.A. E.S.P., la cual puede ser conocida y utilizada sin autorización.	Información de página Web. Normas, reglamentos, resultados, servicios ofrecidos, etc.
Interna o semiprivada	Información que solo le compete a los Colaboradores de ElectroHuila S.A. E.S.P., que puede ser conocida por todos, pero no debe ser conocida por terceros o personal externo.	Información de beneficios de los colaboradores, reglamento interno de trabajo.
Privada o Confidencial	Información de ElectroHuila S.A. E.S.P. que soporta los procesos de negocio de información. Procedimientos, — políticas, datos de identificación del cliente interno (Colaboradores) y externo (proveedores, usuarios), etc.	Facturación, Nómina, Presupuesto, Cartera, Jurídica, Calidad, Financiera, Perdidas, Comercial y Operación y mantenimiento. Usuario y Contraseña.

Tabla 4 Clasificación de la información

10.4 Procedimiento para la Elaboración y Clasificación de la Información

a. El dueño de la información es responsable por la definición de la clasificación de esta.
b. 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.
c. 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).
d. 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.
e. 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.
f. La información debe seguir los estándares de clasificación definidos.
g. La Matriz de información debe documentarse en un formato consolidado por proceso que contenga la clasificación establecida por ElectroHuila S.A. E.S.P.

h. La Matriz de información se debe actualizar anualmente, con el fin de mantenerla identificada.
i. 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 S.A. E.S.P. 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.

10.5 Normas de uso de la información física

a. Cada responsable adaptará el archivo de gestión con las condiciones de seguridad necesarias para archivar y salvaguardar la información confidencial.
b. Los colaboradores de planta y en misión, contratistas, outsourcing y proveedores de ElectroHuila S.A. E.S.P. no podrán emplear la información entregada para obtener un beneficio propio, ni podrán compartirla con terceros para que ellos obtengan algún beneficio.
c. 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 S.A. E.S.P. 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 S.A. E.S.P. o de personal no autorizado.
d. La información en medio físico, clasificada confidencial, que no esté siendo utilizada por el personal autorizado, debe permanecer siempre en un sitio protegido.

10.6 Normas de uso medios removibles

- Se deben redactar normas para el uso de medios removibles, teniendo en cuenta el tipo de información de que manejan y realizando un tratamiento especial cuando la información sea confidencial/privada.
- Se debe llevar un control de los medios removibles usados en cada dependencia.
- Se debe tener registro de la información en medios removibles.
- Sí la información ya no se requiere tener en medios removibles o cuando el colaborador se retire de ElectroHuila S.A. E.S.P., debe realizarse un borrado seguro de la información contenida en el dispositivo.
- Sí la confidencialidad o integridad de la información contenida en un medio removible se considera importante, se debería utilizar los mecanismos criptográficos.
- La disposición final para los medios removibles debe realizarse de forma segura, por ejemplo, incineración o borrado seguro.

11. Control de Acceso

11.1 Política de control de acceso de ELECTROHUILA S.A. E.S.P

Todos los aplicativos de ElectroHuila S.A. E.S.P. deben usar controles de acceso lógico que mitiguen los riesgos relacionados con el acceso no autorizado a la información confidencial de la Organización y sus Clientes.

11.2 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 con los perfiles establecidos por la Oficina de Sistemas y Organización.

b) El control de acceso a los diferentes sistemas de información debe ser aprobados por los dueños de la información.

c) Los usuarios de los sistemas de información de ElectroHuila S.A. E.S.P. 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 S.A. E.S.P.

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 estos. 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 S.A. E.S.P., que adversamente afecte la capacidad de otros en el uso de los recursos informáticos o que sea nocivo u ofensivo.

11.3 Definición nombres de usuarios de Aplicativos

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

DEFINICIONES	EJEMPLO
Diego Armando Caballero Perez	diego.caballerop
Se repite con otra cuenta	armando.caballerop
Se repite con otra cuenta	diego.caballeroe

Tabla 5 Ejemplo de nombre de usuario aplicativos

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 S.A. E.S.P. en Línea y ElectroHuila S.A. E.S.P. App) será por correo electrónico, esto con el fin de asegurar a la autenticidad del usuario que está creando la cuenta.

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

Todos los computadores de escritorio o portátiles que tienen acceso a la red corporativa tendrán que identificarse en el dominio de ElectroHuila S.A. E.S.P. con un login compuesto así:
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; sí después de esto el login no fuese único se seguirán reemplazando las siguientes letras del segundo apellido hasta que se cumpla la política.

DEFINICIONES	EJEMPLO
Pepito Armando Perez Serrano	pepito. perezs
Se repite con otra cuenta	pepito. Pereze
Se repite con otra cuenta	pepito. perezr

Tabla 6 Ejemplo de nombre de usuario de acceso a la red

11.5 Definición nombre del equipo

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

DEFINICIONES	EJEMPLO
Oficina de Sistemas y Organización	O&SO-001
Oficina de Responsabilidad Social y Ambiental	ORSA-001

Tabla 7 Ejemplo de nombre de equipo

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.

DEFINICIONES	EJEMPLO
Contraloría	CONTRALORIA-001

Tabla 8 Ejemplo de nombre de equipo – casos especiales

11.6 Definición Identificación del equipo

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

a. XXXXX cuando sea placa.
b. SN_O000X cuando no tenga placa y se identifique con serial.
c. Para la identificación de los servidores dentro de la red de ElectroHuila S.A. E.S.P., 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.

12. Seguridad Física y del Entorno

ElectroHuila S.A. E.S.P., ha establecido estrategias para el control del acceso físico a sus instalaciones y el cuidado de los equipos y/o recursos de procesamiento de datos disponibles en la empresa.

El principal objetivo de estas estrategias es mitigar los riesgos potenciales relacionados con la pérdida, el robo o el daño accidental o intencional de los activos de información de la empresa, evitando la interrupción, total o parcial, de las actividades operativas, administrativas o comerciales. Así mismo, definir las directivas para la protección física de las instalaciones donde están situados este tipo de recursos.

12.1 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 S.A. E.S.P. o no necesitan autorización previa para el ingreso.

Las áreas de acceso restringido en ElectroHuila S.A. E.S.P. 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 Garzón.
s. Cuarto de comunicaciones - Edificio Pitalito.
t. Cuarto de comunicaciones - Edificio La Plata.
u. Archivo Central (Bote)
v. Ventanilla de Radicación Promisión
w. Ventanilla de Radicación Saire
x. Ventanilla de Radicación Zona Centro
y. Archivo de Gestión Centralizado Zona Centro
z. Ventanilla de Radicación Zona Occidente
aa. Archivo de Gestión Centralizado Zona Occidente
bb. Ventanilla de Radicación Zona Sur
cc. Archivo de Gestión Centralizado Zona Sur

12.2 Control de Acceso Físico a las áreas restringidas

Se debe tener acceso controlado a las Áreas de Acceso Restringido para lo cual se deben cumplir con las normas, controles y registros de acceso a dichas áreas como se indica a continuación:

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 requiere autorización por escrito del jefe del área.

12.2.1 Identificación de colaboradores

Todos los colaboradores de ElectroHuila S.A. E.S.P que ingresen a las instalaciones deberán portar carnet de identificación, asignado específicamente a la persona, de uso personal e intransferible y que debe ser visible, en todo momento, mientras se mantenga en las instalaciones de la compañía. Así mismo debe usar la dotación de la empresa con su respectivo logo.

12.2.2 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 S.A. E.S.P. 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 S.A. E.S.P. 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 S.A. E.S.P.
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. E.S.P.

12.2.3 Seguridad de Equipos Móviles

a) El suministro de equipos móviles de ElectroHuila S.A. E.S.P. 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. 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 respectiva.

d) La seguridad física de los equipos móviles de propiedad de ElectroHuila S.A. E.S.P. 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.

12.2.4 Suministros de Equipos de Soporte Energético

La subgerencia Administrativa debe asegurarse que todos los equipos de cómputo de ElectroHuila S.A. E.S.P. 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.

12.2.5 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 del jefe de la Oficina de Sistemas y Organización.

13. Seguridad en las Operaciones

El objetivo en este aparte consiste en asegurar las operaciones en el procesamiento de información de ElectroHuila S.A. E.S.P.,

13.1 Protección contra código malicioso.

Se debe asegurar que los controles de detección, prevención y recuperación para proteger la información contra códigos maliciosos sean implementados en todas las áreas de ElectroHuila S.A. E.S.P., los colaboradores deben reconocer la importancia de la implementación de dichos controles y apoyar su implementación.

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 S.A. E.S.P. 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 de este.

13.1.1 Software No Autorizado

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

13.1.2 Gestión de copias de respaldo

La Oficina de Sistemas y Organización deberá realizar copias de seguridad de la información, del software y del sistema, según lo establecido en los procedimientos **"PR-AGT-02 Copias de Respaldo y Restauración Sistema de Informacion.xlsx"** y **"PR-AGT-04 Copias de Respaldo y Restauración Usuarios Finales.xlsx"** o de acuerdo con los requerimientos de los usuarios. Estas copias de respaldo se deberán verificar de forma periódica. Para ello, se deberán realizar copias de aplicaciones, ficheros y bases de datos con una periodicidad, al menos, semanal, salvo que en dicho período no se hubiese producido ninguna actualización. En algunos casos, se podrá establecer una prioridad alta para la realización de copias de respaldo, si la información a salvaguardar tiene impacto alto para los objetivos estratégicos de ElectroHuila S.A. E.S.P.

a) Las copias de seguridad deberán tener los mismos controles de seguridad que la información original, asegurando su correcta conservación.
b) Se debe establecer un período de retención de las copias de respaldo o seguridad hasta su destrucción o eliminación.
c) Como política general, siempre que sea posible, se deberá establecer que la información en las copias de respaldo o seguridad esté cifrada. Este requerimiento será obligatorio para información confidencial, privada o critica, que afecte los objetivos de negocio.
d) El jefe de la Oficina de Sistemas y Organización es responsable de disponer del sistema de almacenamiento centralizado para custodiar las copias de respaldo o seguridad, sin embargo, es responsabilidad de los dueños de la información coordinar con la oficina de sistemas la información sensible y crítica a respaldar.
e) 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.
f) 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.
g) Se debe garantizar que exista una copia de respaldo o seguridad adicional de la información sensible, la cual debe estar cifrada o protegida ante escritura, de forma que se avale su integridad ante la

necesidad de recuperación frente a posibles incidencias de seguridad o ciberseguridad, como, por ejemplo, Ransomware.

h) El jefe de la Oficina de Sistemas y Organización 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 S.A. E.S.P.

i) Los usuarios de ElectroHuila S.A. E.S.P. 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.

j) El jefe de la Oficina de Sistemas y Organización garantizará que se realice una prueba de restauración de las copias de respaldo disponibles, con el fin de verificar su funcionalidad y que la información almacenada corresponda a la que se debe hacer backup. Estas se realizarán de forma periódica y quedarán documentadas.

k) El jefe de la Oficina de Sistemas y Organización y los jefes de cada división deben garantizar que toda información de ElectroHuila S.A. E.S.P. 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.

l) El jefe de la Oficina de Sistemas y Organización debe garantizar que las copias de respaldo o seguridad, de archivos maestros de aplicaciones y archivos de información se almacenan en lugares seguros y su acceso debe ser restringido. Asimismo, las copias de respaldo deben estar almacenada preferiblemente en un lugar distinto al que la sede principal.

14. Seguridad en las Telecomunicaciones

En este aparte, se establecen los mecanismos para asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información, así como también, mantener la seguridad de la información transferida dentro de ElectroHuila S.A. E.S.P y con cualquier entidad externa.

14.1 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 S.A. E.S.P.

b. Todas las conexiones hacia redes externas con terceros deben ser autorizadas por el jefe de división a través del aplicativo de 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 esta 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 S.A. E.S.P. 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 S.A. E.S.P. 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.

14.1.1 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 S.A. E.S.P.
b) El jefe de la Oficina de Sistemas y Organización velará por que los nuevos aplicativos adquiridos o desarrollados por ElectroHuila S.A. E.S.P., 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 S.A. E.S.P.

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 auditoria se deben conservar por un lapso 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 (sí 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 S.A. E.S.P.
h) Los responsables de cada una de las aplicaciones deben garantizar que la fecha y hora de todos los recursos informáticos estén sincronizados, para asegurar que los registros reflejan el tiempo exacto de ocurrencia.

14.2 Intercambio de información confidencial

a) El envío de archivos a terceros que contengan información confidencial de ElectroHuila S.A. E.S.P. 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.

15. Adquisición, Desarrollo y Mantenimiento de Sistemas

Para ElectroHuila S.A. E.S.P., la adquisición, desarrollo y mantenimiento de los sistemas de información o aplicaciones deberá contar con los requisitos mínimos de seguridad para el desarrollo de software, los sistemas y los datos acorde con las buenas prácticas internacionales.

Además, deberá realizarse una gestión y control sobre las pruebas, el seguimiento de los cambios, y el inventario del software.

Cada división, oficina, zona y/o coordinación de ElectroHuila S.A. E.S.P., deberá prestar atención a la seguridad de la información en sus sistemas de información y datos, procedimientos de selección, desarrollo e implementación de aplicaciones, productos y servicios.

16. Gestión de Incidentes

Los colaborador o contratistas de la ElectroHuila S.A. E.S.P. que identifiquen un incidente de seguridad de la información o ciberseguridad que pueda comprometer los activos de información, están en la obligación y responsabilidad de reportar o notificar con rapidez y diligencia las supuestas violaciones de seguridad a través de su jefe de dependencia a la Oficina de Sistemas y Organización.

En casos especiales los reportes podrán realizarse directamente a la Oficina de Sistemas y Organización, la cual debe garantizar las herramientas informáticas para que formalmente se realicen tales denuncias.

La Oficina de Sistemas y Organización debe preparar, conservar y publicar las normas, procesos y guías para el reporte e investigación de incidentes de seguridad.

En conformidad con la ley, la Oficina de Sistemas y Organización podrá interceptar o realizar seguimiento a las comunicaciones por diferentes mecanismos previa autorización de la Oficina de Sistemas y Organización, y en todo caso notificando previamente a los afectados por esta decisión.

La Oficina de Sistemas y Organización conservará los procedimientos escritos para el desarrollo de la operación de sistemas cuya no disponibilidad suponga un alto impacto en el desarrollo normal de actividades de ElectroHuila S.A. E.S.P. A estos sistemas, se debe realizar seguimiento continuo del desempeño para asegurar la disponibilidad y confiabilidad del servicio que prestan.

17. Seguridad en los Proveedores

ElectroHuila S.A. E.S.P., deberá establecer mecanismos con el fin de valorar la criticidad de todos los servicios que pueden ser subcontratados con el din de identificar aquellos que sean relevantes en cuanto, a la seguridad de la información, ya sea por su naturaleza, la sensibilidad de los datos que maneja y deban tratarse o la dependencia sobre la continuidad de negocio.

En referencia a los proveedores de estos servicios se deberán prestar especial atención a los procesos de selección, requerimientos contractuales, la terminación contractual, la monitorización de los niveles de servicio, la devolución de datos y las medidas de seguridad implantadas por dicho proveedor, que deberán ser, semejantes o iguales a las que se establecen en la presente Política.

18. Continuidad de Negocio

Teniendo en cuenta, los requerimientos de calidad y buenas prácticas, ElectroHuila S.A. E.S.P., deberá disponer de un Plan de Continuidad de Negocio como parte de su estrategia para garantizar la continuidad del negocio en la prestación de los servicios esenciales o críticos y el apropiado manejo de los impactos sobre el negocio ante posibles eventos, incidentes o escenarios

de crisis, proporcionando un marco de referencia para que los colaborares, clientes y proveedores actúe en caso de requerirse.

El Plan de Continuidad de negocio se debe actualizar y probar periódicamente. También se debe contar con el Plan de Recuperación ante Desastres que estará alineado con la continuidad de negocio, este plan abarcará la continuidad en cuanto a funcionamiento de todas las tecnologías de información y comunicación de ElectroHuila S.A. E.S.P.

ElectroHuila S.A. E.S.P., deberá realizar concientización, formación y capacitación para todos sus colaboradores en materia de Continuidad del Negocio.

19. 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 con 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.

19.1 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:
    1. Longitud mínima de 8 caracteres
    2. Debe contener Números y letras
    3. 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 las contraseñas pueden ser cambiados por el administrador de Seguridad?; El administrador de seguridad solamente puede cambiar una contraseña si el usuario en cuestión ha olvidado su clave de acceso, la solicitud para cambiar de password se debe hacer por la mesa de servicio. La contraseña creada por el administrador es temporal, al siguiente inicio de sesión se debe cambiar por parte del usuario.

19.2 Responsabilidades de los usuarios.

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

1. En ninguna circunstancia se debe prestar el usuario y la contraseña.
2. Nunca suministrar el usuario y contraseña vía telefónica.
3. 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.
4. La contraseña se debe memorizar, nunca la escriba en ninguna parte.
5. Se debe cambiar la contraseña cuando se tiene sospecha que ha sido descubierta por terceros.

19.3 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. El jefe de la Oficina de Sistemas y Organización debe garantizar que el protector de pantalla de todos los equipos de ElectroHuila S.A. E.S.P. sean configurados con los siguientes parámetros:

1. Activar el protector de pantalla después de 5 minutos de inactividad del computador.
2. El desbloqueo requiere contraseña de red.

b. El fondo de escritorio debe contener información comercial de ElectroHuila S.A. E.S.P. y debe ser suministrada por la Oficina de Gestión Social y Ambiental
c. Cuando un colaborador se retire temporalmente de su puesto de trabajo, debe hacer un logout (cerrrar) de la sesión del aplicativo y activar el bloqueo (crtl + alt + sup) del escritorio de trabajo del computador.
d. 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 esta información.
e. Los puestos de trabajo deben permanecer limpios y ordenados.
f. Cuando se imprima o digitalice documentos con información pública clasificada o pública reservada, éstos deben retirarse inmediatamente de dichos dispositivos.
g. Los dispositivos de impresión y digitalización deben permanecer limpios de documentos
h. 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.

19.4 Controles de seguridad en los servicios de red

19.4.1 Uso de dispositivos de almacenamiento externo:

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 S.A. E.S.P. a diversos riesgos y peligros.

a. **Política:** ElectroHuila S.A. E.S.P. 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 S.A. E.S.P. 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, iPhone /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.

b. Uso indebido de dispositivos de almacenamiento externo:

1. Almacenar o transportar información clasificada o reservada de ElectroHuila S.A. E.S.P.
2. Ejecutar cualquier tipo de programa no autorizado por ElectroHuila S.A. E.S.P. 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 0 funcionarios, temporales, contratistas o practicantes de ElectroHuila S.A. E.S.P.

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 S.A. E.S.P. 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.

DEFINICIONES	EJEMPLO
Pepito Perez Paez de ElectroHuila S.A. E.S.P	pepitoperez. ElectroHuila S.A. E.S.P.
Se repite con otra cuenta	pepitopaez.ElectroHuila S.A. E.S.P
Se repite con otra cuenta	pepitoperezp.ElectroHuila S.A. E.S.P

Tabla 9 Ejemplo nombre de usuario VPN

c. **Solicitud de acceso para el almacenamiento por USB**
   - Para solicitar el acceso de almacenamiento a través de dispositivos USB, se deberá realizar una 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.

19.4.2 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 S.A. E.S.P.

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.
d. 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.

19.4.3 Normas de uso de correo electrónico.

a. **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 S.A. E.S.P.,
    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.

DEFINICIONES	EJEMPLO
Pepito Alejandro Perez Otalora	pepito.perezo@_
Se repite con otra cuenta	alejandro.perezo@_
Se repite con otra cuenta	pepito.perezta@_

Tabla 10 Ejemplo nombre de usuario correo interno y externo

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, vídeos 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.

19.4.4 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.

19.4.5 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 S.A. 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 de que el área requiera que las cuentas de correo tengan un nombre especifico 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"

20. Cumplimiento Regulatorio

ElectroHuila S.A. E.S.P., se compromete a dotar los recursos necesarios para dar cumplimiento a toda la legislación, normativa y regulación aplicable de acuerdo con su actividad en materia de seguridad de la información y a garantizar la responsabilidad de cumplimiento de todos los colaboradores.

ElectroHuila S.A. E.S.P., implementa estrategias para evitar el incumplimiento de cualquier ley y/o disposición reglamentaria o contractual que incluya obligaciones relacionadas con seguridad de la información y ciberseguridad.

La gestión de riesgos se realizará conforme a una metodología reconocida, como la basada en la serie de normas ISO 27000 (especialmente ISO 27005) o el Marco de Ciberseguridad del NIST, y que incluirá fases de identificación, análisis, valoración, tratamiento, monitoreo y revisión continua.

Los terceros que tengan acceso a activos con clasificación confidencial o privada de los cuales ElectroHuila S.A. E.S.P. es propietaria, posee o administra deben cumplir a cabalidad con las políticas, normas y procedimientos de seguridad.

21. Gestión de Excepciones

Cualquier cambio en cuanto a una excepción a la presente Política de Seguridad de la Información deberá ser informada al responsable de la Seguridad de la Información de ElectroHuila S.A. E.S.P.

Las excepciones identificadas serán analizadas para evaluar el riesgo que podrían introducir a ElectroHuila S.A. E.S.P. y, estableciendo la categorización de estos riesgos, deberán ser asumidos por quien realiza la petición de la excepción junto con los responsables del negocio.

22. Revisión de la Política

La aprobación de la política de seguridad de la información implica que su implantación contará con el apoyo de la Gerencia General para alcanzar todos los objetivos establecidos en la misma, así como también, cumplir con todos sus requisitos.

La presente Política de Seguridad de la Información, será revisada y aprobada anualmente o cuando ocurran cambios significativos para asegurar su continua idoneidad, eficiencia y efectividad.

23. Compromisos a La Seguridad

Toda actividad destinada a uso indebido o a obtener acceso no autorizado a sistemas sensibles y/o información clasificada como confidencial se encuentra expresamente prohibida en ElectroHuila S.A. E.S.P., incluyendo, pero no limitándose a:

- La posesión, el uso, o la descarga de herramientas que tratan de violar la protección de los derechos de autor de software, la captura de tráfico de red, descubrir contraseñas, identificar vulnerabilidades de seguridad, o descifrar archivos cifrados.
- El uso de la ingeniería social para comprometer la seguridad

Los colaboradores que utilicen este tipo de herramientas de diagnóstico deben recibir la aprobación previa por escrito de los responsables de la seguridad de la información.

En todos los casos las actividades de mantenimiento que requieren el uso de herramientas de diagnóstico deben seguir los procedimientos de gestión de cambio.

24. Protección A Información Personal Y Privada

ElectroHuila S.A. E.S.P. cumple con la legislación aplicable en temas de protección a la privacidad y garantiza que los riesgos se reducen al mínimo en aquellos casos en que se requieran datos que están sujetos a protección.

25. Ciberseguridad

Para ElectroHuila S.A. E.S.P. la ciberseguridad, importante por lo cual se han creado un conjunto de políticas, directrices, controles y mecanismos de seguridad; métodos de gestión del riesgo, acciones, y buenas prácticas para prevenir y proteger los datos, sistemas y aplicaciones; salvaguardando a los usuarios y activos de la Entidad en el ciberespacio, siempre, teniendo en

cuenta los principios de la Seguridad de la Información (confidencialidad, integridad y disponibilidad).

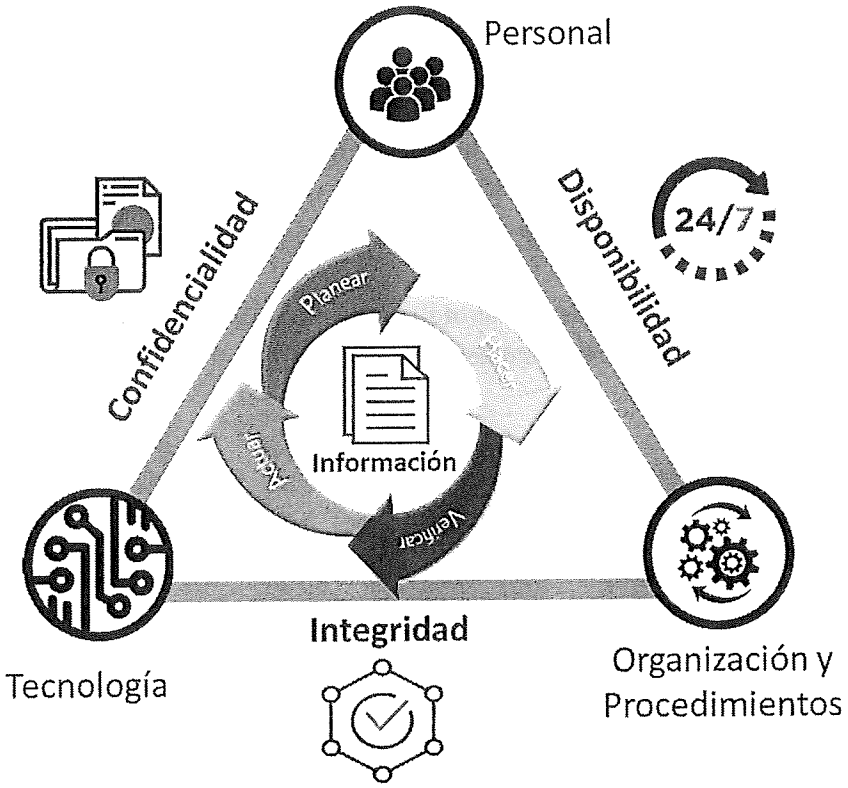

Ilustración 4: Principios de Seguridad de la Información

Otras de las características para tener en cuenta en ciberseguridad para ElectroHuila S.A. E.S.P., son:

- **Control de acceso:** controles que permite o no el acceso de un usuario a las aplicaciones, servidores, equipos tecnológicos entre otros, según los perfiles y manejo de información asignados.
- **No repudio o Irrenunciabilidad:** es un principio de seguridad de la información por medio del cual se da garantía de la participación en una actividad sobre una plataforma tecnológica, fue realizada por el usuario. De acuerdo con los registros de auditoría o log's se puede demostrar las actividades realizadas.

25.1 Principios De La Ciberseguridad

Con el fin de dar cumplimiento al marco normativo, regulatorio y a los objetivos de negocio, ElectroHuila S.A. E.S.P. considera los siguientes principios de la Ciberseguridad para preservar la información y correcto funcionamiento de los sistemas informáticos y plataformas tecnológicas para que no se afecten los procesos de la Entidad:

- **Mínimo privilegio:** Son los permisos necesarios y suficientes que tienen los usuarios de los sistemas y aplicaciones para desempeñar las actividades dentro de ElectroHuila S.A. E.S.P. Estos permisos son por tiempo limitado y con los mínimos derechos necesarios para ejecutar las tareas.

- **Mínima superficie de exposición:** consiste en la estrategia para minimizar los riesgos de ser víctima de algún tipo de incidente o ataque informático al reducir la visibilidad de ElectroHuila S.A. E.S.P. únicamente a lo imprescindible en distintos ámbitos, pasando desde lo tecnológico hasta la práctica de uso de los usuarios. Por ejemplo: bloqueo de accesos remotos sin VPN. Activar los servicios necesarios.
- **Defensa en profundidad:** Se trata de un modelo que pretende aplicar controles en seguridad para proteger los datos en diferentes capas por medio de controles y mecanismos necesarios con el fin de minimizar el riesgo de algún ataque informático o incidente de seguridad. En la gráfica a continuación se muestra un ejemplo del modelo.

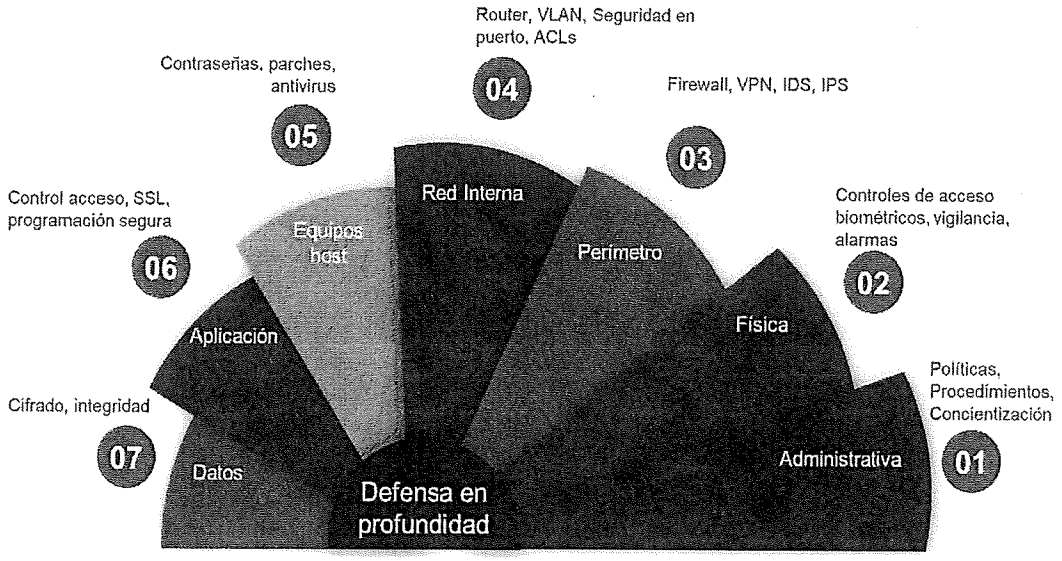

Ilustración 5: Principios de Seguridad de la Información

26. Encuestas

Todos los usuarios de ElectroHuila S.A. E.S.P. 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 de la Oficina 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.

NIKA DUNIEZHKA CUELLAR CUENCA
Gerente General

DIEGO MAURICIO PALACIOS CASTRO
Jefe de Oficina de Sistemas y Organización

09 OCT. 2025