DOCUMENTO DE GERENCIA 1947

"Por medio del cual se adopta la Política de Gestión de Incidentes de Seguridad de la Información – Versión 1, aplicable a todos los colaboradores, contratistas, outsourcing, proveedores y terceros 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. reconoce la información como uno de los activos más valiosos y críticos para el cumplimiento de sus objetivos estratégicos, la continuidad del negocio y la confianza de los grupos de interés.

2. Que la gestión adecuada de los incidentes de seguridad de la información es fundamental para minimizar riesgos asociados al uso indebido, malicioso o accidental de los sistemas, infraestructura tecnológica, servicios en la nube o datos institucionales.

3. Que la Oficina de Sistemas y Organización, en el marco de sus responsabilidades institucionales, ha elaborado la Política de Gestión de Incidentes de Seguridad de la Información – Versión 1, la cual establece los lineamientos para la detección, notificación, análisis, respuesta, resolución, documentación y mejora continua de los incidentes, en concordancia con la norma ISO/IEC 27035:2023.

4. Que esta política se encuentra alineada con la Política de Seguridad de la Información, la Política de Privacidad, Tratamiento y Protección de Datos Personales, y con el marco normativo colombiano aplicable, en especial las Leyes 1581 de 2012, 1266 de 2008, 1273 de 2009, 1712 de 2014, sus decretos reglamentarios, y la Circular Externa 001 de 2018 de la SIC.

5. Que la implementación de esta política permitirá a ELECTROHUILA S.A. E.S.P.:

    - Fortalecer el Sistema de Gestión de Seguridad de la Información (SGSI).
    - Prevenir la recurrencia de incidentes de seguridad.
    - Minimizar el impacto de los incidentes en la operación, los activos de información y la reputación institucional.
    - Asegurar el cumplimiento de las obligaciones legales frente a autoridades y titulares de datos personales.

- Promover una cultura organizacional de seguridad, responsabilidad y mejora continua.

RESUELVE:

ARTÍCULO PRIMERO Adoptar la Política de Gestión de Incidentes de Seguridad de la Información – Versión 1 de ELECTROHUILA S.A. E.S.P., la cual será de cumplimiento obligatorio para todos los colaboradores, contratistas, outsourcing, proveedores y terceros que accedan a los sistemas de información, infraestructura tecnológica o datos institucionales de la Empresa.

ARTÍCULO SEGUNDO Integrar dicha política al Sistema de Gestión de Seguridad de la Información (SGSI) y al Sistema de Gestión de Calidad, como componente esencial de la gestión institucional.

ARTÍCULO TERCERO Encomendar a la Oficina de Sistemas y Organización, en coordinación con la Asesoría Jurídica, la supervisión, seguimiento, gestión de notificaciones y mejora continua de esta política, garantizando su aplicación en todos los niveles de la organización.

ARTÍCULO CUARTO Divulgar y socializar la presente política a través de los canales de comunicación internos, asegurando su comprensión, apropiación y aplicación por parte de todos los colaboradores y terceros vinculados.

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

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

POLÍTICA DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

1. Objetivo

Establecer los lineamientos para la gestión integral del ciclo de vida de los incidentes de seguridad de la información (detección, notificación, análisis, respuesta, resolución, documentación y mejora continua), en concordancia con lo estipulado en la norma ISO/IEC 27035:2023. El propósito es minimizar el impacto de los incidentes, prevenir su recurrencia y fortalecer el Sistema de Gestión de Seguridad de la Información (SGSI) de la organización.

2.Alcance

Esta política es de obligatorio cumplimiento para todos los colaboradores, contratistas, proveedores y terceros que accedan a los sistemas de información, infraestructura tecnológica, servicios en la nube o datos institucionales de la organización, independientemente del nivel de acceso otorgado o de la modalidad de trabajo (presencial, remoto o híbrido).

La presente Política se alinea y complementa con las directrices establecidas en la Política de Seguridad de la Información de ELECTROHUILA S.A. E.S.P. y la Política de Privacidad, Tratamiento y Protección de Datos Personales, siendo un desarrollo específico de los procedimientos y responsabilidades en materia de gestión de incidentes.

3. Definiciones

- Activos de Información: Elementos que almacenan, procesan o transmiten información, incluyendo hardware, software, datos, documentos y servicios.
- Amenaza: Causa potencial de un incidente no deseado, que puede resultar en daño para un sistema o la organización.
- Brecha de Seguridad: Incidente de seguridad que implica la pérdida, alteración, acceso no autorizado, uso indebido, divulgación o destrucción accidental o ilícita de datos personales, requiriendo notificación a las autoridades competentes y/o a los titulares.
- Cadena de Custodia: Conjunto de procedimientos que garantizan la integridad, autenticidad, preservación e inalterabilidad de la evidencia digital desde el momento de su recolección hasta su presentación.
- Confidencialidad: Propiedad de que la información no sea puesta a disposición o revelada a individuos, entidades o procesos no autorizados.
- Dato Personal: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables (según

Ley 1581 de 2012).

- Disponibilidad: Propiedad de ser accesible y utilizable por una entidad autorizada cuando sea requerido.
- Evidencia Digital: Información o datos obtenidos de cualquier medio electrónico o dispositivo de almacenamiento digital que pueda ser utilizado como prueba en una investigación o proceso judicial.
- Evento de Seguridad: Ocurrencia identificada en un sistema, servicio o red que indica una posible violación de la política de seguridad o una falla en los controles.
- Incidente de Seguridad de la Información: Evento o serie de eventos que comprometen, o tienen el potencial de comprometer, la confidencialidad, integridad o disponibilidad de la información.
- Integridad: Propiedad de salvaguardar la exactitud y totalidad de la información y los métodos de su procesamiento.
- Vulnerabilidad: Debilidad de un activo o control que podría ser explotada por una o más amenazas.

4. Marco Legal y Normativo Relevante

La gestión de incidentes de seguridad de la información en ELECTROHUILA S.A. E.S.P. se rige, entre otras, por las siguientes disposiciones normativas, las cuales deben ser consideradas durante todo el proceso:

- Ley 1581 de 2012: Por la cual se dictan disposiciones generales para la protección de datos personales.
- Decreto 1074 de 2015: Decreto Único Reglamentario del Sector Comercio, Industria y Turismo, que reglamenta parcialmente la Ley 1581 de 2012.
- Decreto 1377 de 2013: Por el cual se reglamenta parcialmente la Ley 1581 de 2012, estableciendo aspectos específicos sobre la Autorización del Titular y los procedimientos internos para el tratamiento de datos personales.
- 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 los financieros, crediticios, comerciales y de servicios, y de los datos personales de sus titulares.
- Circular Externa 001 de 2018 de la Superintendencia de Industria y Comercio (SIC): Imparte instrucciones sobre el Principio de Seguridad

en el Tratamiento de Datos Personales y el deber de notificación de incidentes de seguridad que afecten bases de datos personales.

- Ley 1273 de 2009: Por medio de la cual se modifica el Código Penal, creando tipos penales relacionados con delitos informáticos.
- 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.
- La presente política se complementa con el "Marco Legal y Normativo Aplicable" detallado en la Política de Seguridad de la Información de ELECTROHUILA S.A. E.S.P.

5. Proceso de Gestión de Incidentes de Seguridad de la Información

El proceso de gestión de incidentes de seguridad de la información sigue un ciclo de vida estructurado para asegurar una respuesta eficaz y oportuna:

5.1. Detección

La detección de incidentes puede ocurrir a través de monitoreo de sistemas, alertas de seguridad, informes de usuarios o auditorías. Es fundamental que cualquier persona que detecte un evento o sospecha de incidente lo notifique de inmediato.

5.2. Notificación

Todo evento o incidente de seguridad de la información debe ser notificado de forma inmediata a la Mesa de Servicio de la Oficina de Sistemas y Organización o al canal de comunicación establecido para tal fin. La notificación debe contener la información relevante y disponible en el momento del descubrimiento.

5.3. Análisis y Clasificación

Una vez notificado, el incidente será analizado para determinar su naturaleza, alcance, criticidad e impacto potencial en la confidencialidad, integridad y disponibilidad de la información y los servicios. Se clasificará el incidente según su severidad y se le asignará una prioridad de respuesta.

5.4. Contención

Se implementarán acciones inmediatas para contener el incidente, con el objetivo de limitar su impacto, prevenir su propagación y minimizar el daño. Esto puede incluir el aislamiento de sistemas, desconexión de redes o el bloqueo de usuarios.

5.5. Erradicación

Una vez contenido, se procederá a erradicar la causa raíz del incidente. Esto implica la eliminación de malware, la corrección de vulnerabilidades, la restauración de configuraciones seguras y la implementación de medidas preventivas para evitar la recurrencia.

5.6. Recuperación

Se ejecutarán los planes de recuperación y continuidad del negocio, si son necesarios, para restaurar los sistemas y servicios afectados a su estado normal de operación. Se verificará la integridad y disponibilidad de la información antes de restablecer los servicios completamente.

5.7. Post-incidente y Lecciones Aprendidas

Después de la resolución del incidente, se realizará un análisis post-incidente para identificar lecciones aprendidas, mejorar los procesos, actualizar las políticas y fortalecer los controles de seguridad. Este análisis debe documentarse para referencia futura.

5.8. Evidencia Digital y Cadena de Custodia

En caso de que un incidente requiera una investigación forense o pueda dar lugar a acciones disciplinarias, contractuales o legales (civiles o penales), se asegurará la correcta recolección, preservación y análisis de la evidencia digital, siguiendo estrictos procedimientos de cadena de custodia para garantizar su integridad, autenticidad y validez. La Asesoría Jurídica podrá ser involucrada en esta fase para garantizar el cumplimiento de los requisitos legales.

5.9. Notificación de Brechas de Seguridad de Datos Personales

Cuando un incidente de seguridad implique una brecha que comprometa la confidencialidad, integridad o disponibilidad de datos personales (sensibles o no sensibles), ELECTROHUILA S.A. E.S.P. actuará conforme a lo establecido en la Ley 1581 de 2012, el Decreto 1074 de 2015, el Decreto 1377 de 2013 y la Circular Externa 001 de 2018 de la Superintendencia de Industria y Comercio (SIC), lo cual incluye:

- Evaluación de Riesgo: Se evaluará de manera inmediata la severidad de la brecha y el riesgo potencial para los derechos y libertades de los titulares de los datos.

- Notificación a la SIC: La Superintendencia de Industria y Comercio (SIC) será notificada de la ocurrencia de la brecha, a más tardar dentro de los quince (15) días hábiles siguientes al momento en que la entidad tuvo la posibilidad real de detectar el incidente o tener conocimiento de su ocurrencia, utilizando los formatos y canales establecidos por la SIC.

- Notificación a los Titulares: Se informará a los titulares de los datos personales afectados cuando exista un riesgo significativo que afecte sus derechos o en los términos y condiciones que la SIC determine. La comunicación incluirá, como mínimo, la naturaleza de los datos comprometidos, las medidas de mitigación adoptadas y las recomendaciones para que los titulares protejan sus derechos.

- La Oficina de Sistemas y Organización, en coordinación con la Asesoría Jurídica, serán los responsables de ejecutar y gestionar estas notificaciones.

6. Responsabilidades

La gestión de incidentes de seguridad de la información es una responsabilidad compartida, con roles y funciones específicas asignadas:

- Todos los Colaboradores, Contratistas y Terceros:
- Conocer y cumplir con esta política y los procedimientos asociados.
- Reportar de forma inmediata cualquier evento o incidente de seguridad detectado.
- Colaborar con el equipo de respuesta a incidentes durante la investigación y resolución.

- **Responsable del Sistema de Gestión de Seguridad de la Información (SGSI) [Rol General]:**

  - Asegurar la implementación y mantenimiento de esta política.
  - Asegurar que los incidentes sean reportados y gestionados correctamente dentro del SGSI.
  - Coordinar el equipo de respuesta a incidentes, mantener los registros actualizados y garantizar la mejora continua del SGSI.

- **Jefe de la Oficina de Sistemas y Organización:**

  - Supervisar el cumplimiento de esta política y liderar la respuesta ante incidentes de alta criticidad.
  - Proponer y gestionar los recursos técnicos y humanos necesarios para la eficaz gestión de incidentes.
  - Coordinar la elaboración y actualización de los lineamientos de respuesta a incidentes.
  - Reportar de forma inmediata cualquier evento o incidente de seguridad detectado.

- **Oficial de Seguridad de la Información (OSI) / CISO (Si el rol existe o es designado):**

  - Supervisar la implementación estratégica y operativa de la gestión de incidentes, garantizando su alineación con los objetivos de seguridad de la información de la empresa.
  - Asesorar a la Alta Dirección en la toma de decisiones críticas durante la gestión de incidentes mayores o de alto impacto.

- Asegurar la coordinación entre las áreas involucradas en la respuesta a incidentes.

- **Área de Talento Humano:**

  - Apoyar en los procesos disciplinarios relacionados con incidentes atribuibles a conductas del personal, conforme a las políticas internas.

  - Participar en la definición de planes de capacitación en materia de concientización sobre seguridad y consecuencias del incumplimiento.

- **Asesoría Jurídica:**

  - Asesorar en la interpretación y aplicación del marco legal vigente en caso de incidentes que puedan tener implicaciones jurídicas (ej. protección de datos personales, delitos informáticos, responsabilidad civil o contractual).

  - Revisar y validar las comunicaciones externas, especialmente las notificaciones obligatorias a autoridades (SIC) y a titulares de datos.

  - Colaborar en la recolección y preservación de evidencia digital conforme a los requisitos legales.

- **Alta Dirección:**

  - Respaldar la implementación de esta política, asignando los recursos necesarios y promoviendo su cumplimiento en todos los niveles organizacionales.

  - Tomar decisiones estratégicas y autorizar acciones de alto nivel en la respuesta a incidentes críticos que puedan afectar la reputación o la continuidad del negocio.

7. Cumplimiento

El incumplimiento de esta política será objeto de investigación formal y podrá acarrear sanciones disciplinarias, contractuales y/o legales, de conformidad con las políticas internas de ELECTROHUILA S.A. E.S.P., incluyendo lo dispuesto en el Reglamento Interno de Trabajo, los contratos vigentes y la normatividad aplicable, respetando en todo momento el debido proceso. Adicionalmente, se advierte que ciertas conductas relacionadas con incidentes de seguridad de la información (como el acceso abusivo a un sistema, la violación de datos personales, o el daño informático) pueden constituir delitos tipificados en el Código Penal Colombiano, de conformidad con lo establecido en la Ley 1273 de 2009, lo que podría dar lugar a investigaciones por parte de las autoridades competentes.

Los reportes de incidentes, así como las denuncias sobre incumplimientos, se podrán realizar también por medio del canal confidencial de reportes "Línea de Transparencia".

Línea Telefónica: 018000117766
Correo Electrónico: electrohuila@lineatransparencia.com
Formulario Web: reporte.lineatransparencia.co/electrohuila

8. Revisión

La presente política será objeto de revisión de manera anual, o de forma anticipada cuando se produzcan cambios significativos en la infraestructura tecnológica, el marco normativo aplicable, los hallazgos de auditoría o la estructura organizacional. La revisión será responsabilidad del responsable del SGSI, en coordinación con la Asesoría Jurídica, y deberá quedar documentada conforme a los lineamientos establecidos por la organización para el control de documentos.

9. Aprobación

Versión: 1

Fecha de aprobación: 09 OCT. 2025

NIKA DUNIEZHKA CUÉLLAR CUENCA
Gerente General

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