Versión: 1

Fecha de aprobación: 8/04/19

Proceso responsable: Tecnología

Aprobado por: Comité Directivo

Política de Ciberseguridad

- **Política de Ciberseguridad**

Política de Ciberseguridad

Establecer todas aquellas medidas organizativas, técnicas, físicas y legales destinadas a la identificación, protección, detección, respuesta y recuperación de los ciber activos críticos de tal forma que se logre el cumplimento de las leyes, reglamentos y regulación vigente que sean aplicables a la organización, contra el acceso no autorizado, divulgación, duplicación, interrupción de la operación, modificación, destrucción, pérdida, robo, o mal uso, que se pueda producir en forma intencional o accidental, buscando garantizar la confiabilidad, confidencialidad, integridad y disponibilidad de las tecnologías de operación, para asegurar la sostenibilidad y seguridad de los negocios.

A través de esta política se difunden los objetivos de ciberseguridad de CELSIA, que se consiguen con la aplicación de controles de ciberseguridad, para gestionar un nivel de ciber riesgo aceptable.

Tecnología es el responsable de realizar las acciones de sensibilización, comunicación, entrenamiento y socialización de la política de ciberseguridad y de los procesos de seguridad cibernética donde se incluyan como mínimo los siguientes objetivos:

- Identificación y documentación de la situación actual.
- Establecimiento de procedimientos de seguridad cibernética.
- Diseño de arquitecturas de seguridad aplicable a los ciber activos.
- Definición e implantación de controles legales, técnicos, organizativos y físicos.
- Implementación de un ciclo de mejora continua de la gestión de ciberseguridad.

Los principios de la política son parte de la cultura de CELSIA, por lo que se asegura un compromiso por parte del Comité Directivo de CELSIA para la difusión, consolidación y cumplimiento de la presente política.

Estándares de la Política de la Política de Ciberseguridad

Esta política es aplicable a todos los colaboradores, proveedores, contratistas, terceras partes, que ingresen física o remotamente a los perímetros de seguridad y accedan a ciber activos críticos propiedad de CELSIA y sus filiales.

Esta política debe ser revisada como mínimo una vez al año o cuando sea necesario.

Organización para la ciberseguridad

La presente política establece un modelo de gobierno de ciberseguridad que proporciona una guía y dirección para la gestión de la ciberseguridad, así como los recursos necesarios para la realización de las tareas relacionadas con la gestión, proyectos y operación de la ciberseguridad.

La ciberseguridad será soportada por un Centro de Operaciones de Seguridad, que poseerá las capacidades necesarias para la identificación, operación y respuesta a incidentes de ciberseguridad, tendrá asignadas las responsabilidades pertinentes en dicha materia y reportará directamente al Líder de Ciberseguridad.

Modelo de gobierno

CELSIA ha definido la siguiente estructura organizacional con instancias, roles y responsabilidades, con el fin de asegurar un adecuado cumplimiento de esta política:

Junta Directiva y Alta Dirección: Responsables por la adopción y adecuada implementación de la política de ciberseguridad, el establecimiento de una estructura organizacional que proporcione guía y dirección para la gestión de la ciberseguridad, otorgar los recursos necesarios para la implementación de medidas en pro de la ciberseguridad, y ejercer frente a sus colaboradores el liderazgo apropiado para disminuir los riesgos de ciberseguridad.

Comité de Ciberseguridad: Responsables por la definición, gestión y operación del programa de ciberseguridad, incluyendo las políticas y lineamientos de ciberseguridad establecidos aplicables para la organización.

El Comité de Ciberseguridad debe establecer los criterios de dirección y control, que permitan implantar los mecanismos más apropiados de protección de los ciber activos críticos de CELSIA, aplicando los principios de confidencialidad, integridad y disponibilidad, autenticidad, autorización, trazabilidad y no repudio.

Responsables de activos y ciber activos críticos: Celsia es el propietario de los activos y ciber activos críticos, su tenencia y manejo es delegada a Generación, Transmisión y Distribución, Gestión Humana Administrativa y Tecnología quienes son responsables de los activos y ciber activos críticos que le sean asignados, así como de la clasificación, control y monitoreo del uso y gestión de los mismos. Por ello deben ser conscientes de los riesgos a los que están expuestos los activos y ciber activos críticos a su cargo, de forma que ejerzan frente a sus colaboradores el liderazgo apropiado para disminuirlos.

Tecnología: Responsable de la gestión de las medidas necesarias para mitigar los riesgos asociados a la ciberseguridad y reportarán al comité de ciberseguridad cualquier evento asociado.

Auditoria: Responsables por evaluar el cumplimiento de la política de ciberseguridad, contribuyendo en la identificación de nuevos riesgos y controles asociados para el fortalecimiento de la ciberseguridad.

Usuarios: Cualquier colaborador, proveedor, contratista, u otra persona autorizada que utiliza activos y ciber activos críticos de la organización en la ejecución de las actividades de su trabajo diario.

Clasificación y control de ciber activos

Los ciber activos críticos deben estar identificados y priorizados de acuerdo con los ciber riesgos y exposiciones de ciberseguridad en un inventario actualizado; con el objetivo de evitar pérdidas financieras, operativas y/o de imagen para la organización.

Tratamiento y Gestión del ciber riesgo

Generación, Transmisión y Distribución, Gestión Humana Administrativa y Tecnología son responsables de analizar, priorizar y realizar el tratamiento de los ciber riesgos con base en los objetivos de negocio y alineados con la política de gestión de riesgos.

En los proyectos o nuevas adquisiciones se debe realizar la identificación de los activos críticos y ciber activos críticos, los riesgos, vulnerabilidades y el nivel de gestión de ciberseguridad en la operación para establecer un plan de ciberseguridad.

Seguridad Física y del Entorno

Protección de Recursos, debe documentar, implementar y mantener un programa de seguridad física para la protección de los ciber activos críticos.

Todos los ciber activos críticos definidos en un perímetro de seguridad electrónico deben residir dentro de un perímetro de seguridad física y estar en áreas protegidas físicamente contra el acceso no autorizado, daño o interferencia.

Control de acceso a los ciber activos

Generación, Transmisión y Distribución, Gestión Humana Administrativa y Tecnología conforme a la clasificación de los ciber activos críticos, deben implementar las medidas de ciberseguridad aplicables según el caso, con el fin de evitar la adulteración, pérdida en la continuidad de la operación, fuga, consulta, uso o acceso no autorizado o fraudulento.

El control de acceso a los ciber activos críticos se debe basar en el principio del menor privilegio, lo que implica que no se otorgará acceso a menos que sea explícitamente autorizado.

Los perímetros de seguridad electrónica dentro de los cuales residen los ciber activos críticos y sus puntos de acceso deben ser identificados, protegidos y contar con trazabilidad.

Gestión de incidentes de ciberseguridad

Todos los colaboradores, consultores, contratistas, terceras partes deben reportar cualquier vulnerabilidad que hayan observado o que sospechen que existe en los sistemas o servicios que soportan la operación a través de la Mesa de Ayuda de Servicios.

El Centro de Operaciones de Seguridad reportará los incidentes con impacto sobre los ciber activos críticos al Líder de Ciberseguridad para que sean evaluados y reportados al Líder del Centro de Operaciones de acuerdo con el procedimiento de incidentes de la organización.

Plan de recuperación de ciber activos críticos

Generación, Transmisión y Distribución, Gestión Humana Administrativa y Tecnología, deben implementar planes de recuperación para los ciber activos críticos y que dichos planes correspondan a las técnicas y prácticas establecidas para la continuidad de negocios.

Excepciones

Las excepciones a cualquier cumplimiento de la política deben ser aprobadas por el Líder de Tecnología y de Ciberseguridad, las cuales pueden requerir autorización del Líder de Gestión Humana Administrativa y Tecnología y el Líder de CELSIA. Todas las excepciones a la política deben ser formalmente documentadas, registradas y revisadas.

Incumplimiento a la política de ciberseguridad

Las violaciones a la política de ciberseguridad o sus lineamientos por parte de los colaboradores, desencadenarán en medidas de tratamiento a los incidentes de ciberseguridad generados y podrían ser objeto de acciones disciplinarias por parte de Gestión Humana.

DEFINICIONES

Para los propósitos de este documento, se definen los siguientes conceptos:

- **Activo crítico:** Instalaciones, sistemas o equipo eléctrico que, si es destruido, degradado o puesto indisponible, afecta la confiablidad u operatividad del sistema eléctrico. Acorde con las recomendaciones del Comité Tecnológico del CNO para la definición de activos críticos que comprometan la seguridad de operación del SIN.

- **Ciber activo.** Dispositivo electrónico programable y elementos de las redes de comunicaciones incluyendo hardware, software, datos e información. Así como aquellos elementos con protocolos de comunicación enrutables, que permitan el acceso al mismo de forma local o remota.

- **Ciber activo crítico**. Dispositivo para la operación confiable de activos críticos que cumple los siguientes atributos:
  - El ciber activo usa un protocolo enrutable para comunicarse afuera del perímetro de seguridad electrónica, o,
  - El ciber activo usa un protocolo enrutable con un centro de control, o,
  - El ciber activo es accesible por marcación.

- **Confidencialidad:** propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

- **Desastre o contingencia:** interrupción de la capacidad de acceso a información y procesamiento de la misma a través de computadoras u otros medios necesarios para la operación normal de un negocio.

- **Disponibilidad:** propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.

- **Evento de ciberseguridad:** presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de ciberseguridad o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad.

- **Lineamientos de ciberseguridad:** son productos, procedimientos y métricas aprobadas, que definen en detalle como las políticas de seguridad serán implementadas para un ambiente en particular, teniendo en cuenta las fortalezas y debilidades de las características de seguridad disponibles. Deben estar reflejadas en un documento que describe la implantación de una guía para un componente específico de *hardware, software* o infraestructura.

- **Integridad:** propiedad de salvaguardar la exactitud y el estado completo de los activos.

- **Vulnerabilidad:** debilidad de un activo o grupo de activos, que puede ser aprovechada por una o más amenazas.

ANEXOS Y REFERENCIAS

- *Normas ISO 27000.*
- *Normas NIST Cyber Security framework.*
- *Normas IEC 62443 Industrial Communication Networks – Network and System Security*
- *NERC CIP (North American Electric Reliability Corporation critical infrastructure protection)*
- *Acuerdo 788 Concejo Nacional de Operaciones.*
- *Lineamientos de Ciberseguridad y Anexos.*

CONTROL DE CAMBIOS

VERSION	FECHA	JUSTIFICACIÓN DE LA VERSIÓN
1	15/02/2019	Creación del documento