Versión: 2	DOCUMENTO DE POLÍTICA
Fecha de aprobación: 04/05/2020	
Proceso: Gerencia	
Aprobado por: Gerencia	

Política de Ciberseguridad

Política de Ciberseguridad

Establecer todas las medidas organizativas, técnicas, físicas y legales destinadas a la identificación, protección, detección, respuesta y recuperación de los ciberactivos 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 del negocio de generación de energía.

Gestión Técnica 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 requisitos:

- Identificación y documentación de la situación actual.
- Establecimiento de procedimientos de seguridad cibernética.
- Diseño de arquitecturas de seguridad aplicable a los ciberactivos críticos.
- 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 PRIME TERMOFLORES, por lo que se asegura un compromiso por parte de la Gerencia de PRIME TERMOFLORES para su difusión, consolidación y cumplimiento.

Estándares de la Política de Ciberseguridad

Esta política es aplicable a todos los colaboradores, proveedores, contratistas, personal externo, que ingresen física o remotamente a los perímetros de seguridad e interactúen con los ciberactivos críticos propiedad de PRIME TERMOFLORES.

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 estará soportada por el área de Gestión Técnica en conjunto con Operaciones. La primera encargada de gestionar los proyectos aprobados y las actividades rutinarias de ciberseguridad; y la segunda monitoreando y notificando posibles situaciones de riesgo cibernético. Todas estas situaciones se reportarán directamente al Líder de Gestión Técnica, quien es a su vez el Líder de Ciberseguridad.

Modelo de gobierno

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

Gerencia: Responsable 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.

Responsables de ciberactivos críticos: PRIME TERMOFLORES es el propietario de los activos y ciberactivos críticos, su tenencia y manejo es delegada al área de Gestión Técnica quienes son responsables de los ciberactivos 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 ciberactivos críticos a su cargo, de forma que ejerzan frente a sus colaboradores el liderazgo apropiado para mitigarlos.

Usuarios: Cualquier colaborador, proveedor, contratista, u otra persona autorizada que interactúa con los ciberactivos críticos de la organización en la ejecución de sus actividades.

Clasificación y control de ciberactivos

Los ciberactivos críticos deben estar identificados y priorizados de acuerdo con la guía de ciberserguridad vigente en el país. Puede tomarse como referencia las buenas prácticas de organismos internacionales como NERC (del acrónimo en inglés "North American Electric Reliability Corporation").

Tratamiento y Gestión del ciber riesgo

Gestión Técnica es responsable 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 ciberactivos críticos, los riesgos, vulnerabilidades y el nivel de gestión de ciberseguridad en la operación para asegurar su cobertura dentro del plan de ciberseguridad.

Seguridad Física

Gestión Administrativa y de Recursos, debe documentar, implementar y mantener un programa de seguridad física para la protección de los ciberactivos críticos.

Todos los ciberactivos 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 ciberactivos críticos

Gestión Técnica conforme a la clasificación de los ciberactivos críticos, debe 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 ciberactivos 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 ciberactivos 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 del líder del equipo o administrador de contrato.

El Centro de Control reportará los incidentes con impacto sobre los ciberactivos críticos al Líder de Ciberseguridad para que sean evaluados y reportados a la Gerencia de acuerdo con el procedimiento de incidentes de la organización.

Plan de recuperación de ciber activos críticos

Gestión Técnica debe implementar planes de recuperación para los ciberactivos críticos y que dichos planes correspondan a las técnicas y prácticas establecidas para la continuidad del negocio.

Excepciones

Las excepciones a cualquier cumplimiento de la política deben ser aprobadas por el Líder de Ciberseguridad, las cuales pueden requerir autorización de la Gerencia de la empresa. 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.

Ciberactivo. 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.

Ciberactivo 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.

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 1241 Concejo Nacional de Operaciones (CNO).*
- *Lineamientos de Ciberseguridad y Anexos.*

CONTROL DE CAMBIOS

VERSION	*FECHA*	*JUSTIFICACIÓN DE LA VERSIÓN*
1	04/05/2020	Creación del documento