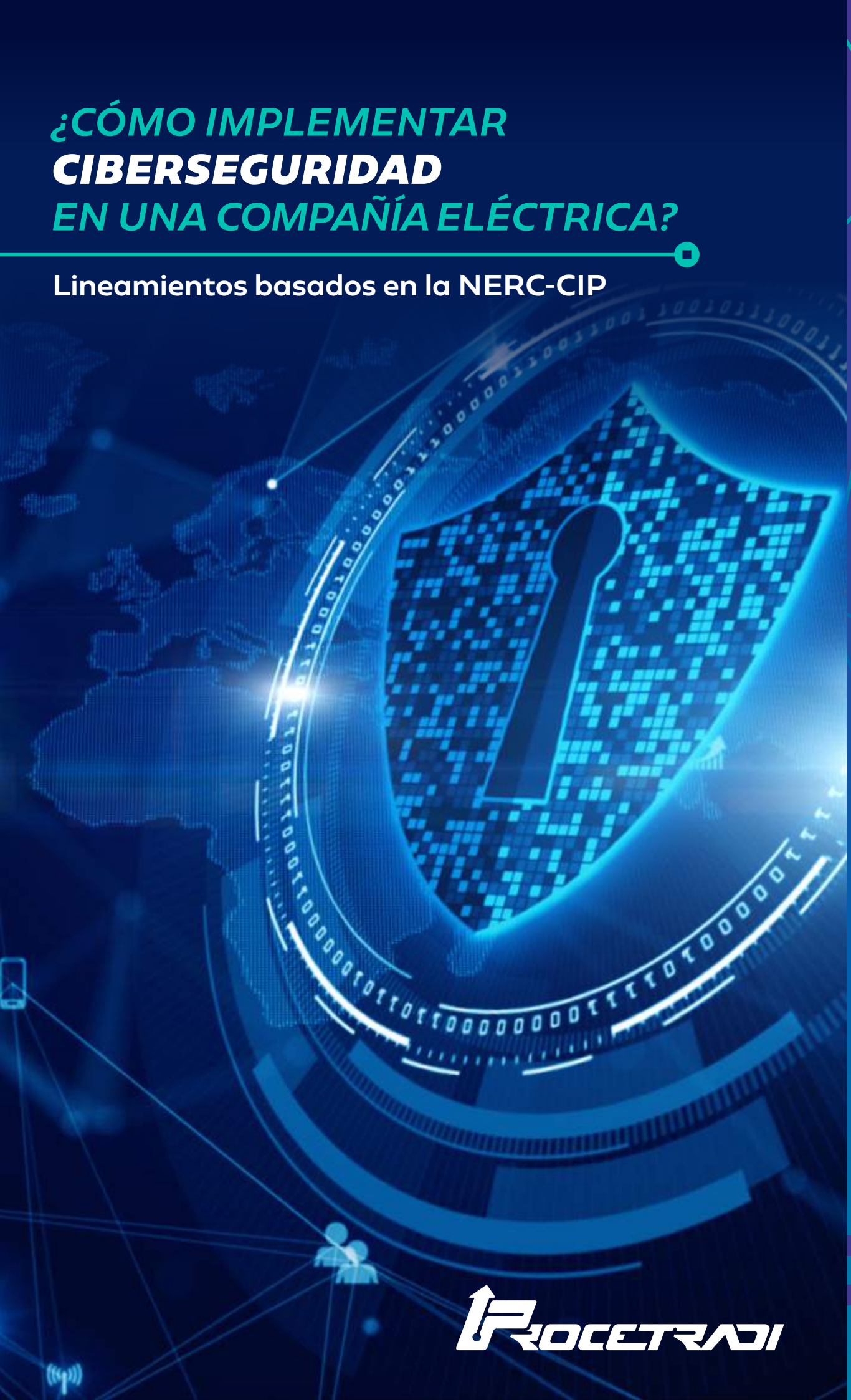
¿CÓMO IMPLEMENTAR **CIBERSEGURIDAD** EN UNA COMPAÑÍA ELÉCTRICA?

Lineamientos basados en la NERC-CIP



PROCETRADI

Ciberseguridad es la práctica de métodos, lineamientos y uso de tecnologías para resguardar y prevenir la extracción, modificación y/o eliminación no autorizada de la información digital de servidores y computadoras personales. Si lo llevamos a la **industria eléctrica**, se entiende como el conjunto de políticas y lineamientos que las empresas eléctricas toman para la protección de su data operativa y administrativa utilizada para el suministro del servicio eléctrico.

A pesar de que es más común escuchar referencias sobre **ciberseguridad** en la actualidad, es un concepto que se viene desarrollando desde el inicio de la transformación digital, desde finales de la década de los 60-70, y que ha venido tomando fuerza los últimos 20 años a nivel normativo, siendo parte de las exigencias que las empresas eléctricas deben de cumplir para garantizar la continuidad del suministro eléctrico.

¿Por qué es necesaria la CIBERSEGURIDAD?

Actualmente, con la masificación del servicio, conexión a internet y la digitalización de procesos, es común encontrar servicios que están operando en servidores remotos, permitiendo conectar las distintas áreas de una empresa desde cualquier punto, sin la necesidad de encontrarse físicamente en la misma ubicación y sin la necesidad de invertir en la creación de una red privada para la comunicación. Sin embargo, es justamente esta conexión a un medio masivo como el internet lo que expone la información transmitida a todos los usuarios de la red.

De igual forma, **ciberseguridad** también involucra la protección de la información en medios privados e internos a una organización, teniendo especial énfasis en proteger la información de su extracción por usuarios no autorizados como es el caso de la información operativa en una empresa eléctrica, la cual no debe estar disponible a toda la organización al estar directamente relacionada con la continuidad del suministro eléctrico.

¿Por qué las empresas eléctricas necesitan **PROTEGER SU INFORMACIÓN OPERATIVA?**

Imaginemos el escenario en el que se utilice una red pública de internet para comunicar equipamiento que se encuentre dentro de la zona urbana de una ciudad como reconectadores o indicadores de falla para la distribución eléctrica. Al ser una red pública, el tráfico de información puede ser observado por un usuario con acceso a la red. Esto significa que el agente externo, puede obtener valores de operación como mediciones o estados, e inclusive simular los parámetros de comunicación para generar mandos remotos. Es este último el cual tiene el mayor impacto operativo, al representar una interrupción del servicio eléctrico.

¿Qué pasos necesito seguir para **IMPLEMENTAR CIBERSEGURIDAD?**

La implementación de ciberseguridad no solo involucra la instalación y puesta en servicio de equipamiento dedicado al control y análisis del tráfico en la red, sino también la implementación de políticas y lineamientos corporativos que pueden ir desde una cultura organizacional hasta políticas de transferencia de información.

Por lo cual, la mejor forma de implementar ciberseguridad es seguir con los lineamientos y buenas prácticas en la industria eléctrica, siendo la más usada, la normativa de ciberseguridad **NERC-CIP** emitida por la NERC de los Estados Unidos.

¿Qué es NERC-CIP?

NERC viene de las siglas en inglés de la Corporación Norteamérica para la Confiabilidad Eléctrica, mientras **CIP** hace referencia a Protección de la Infraestructura Crítica. Por lo que la **NERC-CIP** es el conjunto de lineamientos emitidos por la NERC para la protección de la infraestructura crítica como subestaciones o centros de control. La importancia de esta normativa para la implementación de ciberseguridad radica en que no solo cubre los aspectos no-físicos (o virtuales) de la protección de los datos, sino también incluye lineamientos para proteger de forma física cualquier acceso a la infraestructura crítica.

Esta normativa se divide en **14 capítulos** que describen los siguientes lineamientos:

CIP-002 Categorización de ciber-activos en una empresa eléctrica

Definición de qué activos eléctricos como equipos de patio (interruptores, transformadores) y equipos de control y protección son considerados críticos para la operación de la empresa eléctrica (generación, trasmisión y distribución).

CIP-003 Controles de gestión de seguridad

Definición y creación de políticas organizacionales referentes a ciberseguridad.

CIP-004 Planes de capacitación y entrenamiento para personal administrativo y operativo

Definición del calendario de capacitaciones y entrenamiento en las políticas de ciberseguridad de la empresa.

CIP-005 Definición del perímetro electrónico de seguridad

Por perímetro electrónico se define a la limitación de los accesos remotos o virtuales a los activos críticos definidos en el punto 2.

CIP-006 Definición del perímetro físico de acceso

Por perímetro físico se define a la limitación de accesos físicos a los activos críticos definidos en el punto 2.

CIP-007 Medidas para la gestión del estado de ciberseguridad

Todo aquello relacionado a la gestión de la ciberseguridad como gestión de parches, actualizaciones y evaluación de vulnerabilidades.

CIP-008 Planeamiento para el reporte de un incidente

Pasos a seguir para la ejecución de un plan de respuesta ante un incidente.

CIP-009 Planeamiento para la recuperación después de un incidente

Pasos a seguir para la ejecución de un plan de recuperación luego de un incidente.

CIP-010 Medidas para administrar los cambios y/o configuraciones de los ciber-activos críticos

Todo lo relacionado para la gestión de cambios de configuración de los ciber-activos y la identificación de vulnerabilidades.

CIP-011 Medidas para proteger la información

Lineamientos para proteger la información recopilada como documentación, backups, e historial de cambios.

CIP-012 Comunicación entre centros de control

Lineamientos relacionados a la comunicación e intercambio de información entre centros de control.

CIP-013 Gestión de riesgos de la cadena de suministro

Cómo gestionar y mitigar los riesgos en toda la cadena de suministro como subcontratas de mantenimiento y operación, así como ingeniería y nuevos proyectos.

CIP-014 Seguridad Física

Lineamientos para proteger los centros de control y subestaciones como establecimiento.

Si deseas tener más información de cómo implementar **ciberseguridad** en tu subestación eléctrica, no dudes en contactarnos: **admin@procetradi.com**

www.procetradi.com