COORDINADOR
ELÉCTRICO NACIONAL

Estándar de Ciberseguridad Sector Eléctrico Nacional

Octubre 2020

AGENDA

1 CONTEXTO CIBERSEGURIDAD

2 PLAN DE CIBERSEGURIDAD PARA EL SEN

3 ESTÁNDAR NERC-CIP

4 IMPLEMENTACIÓN

5 PRÓXIMOS PASOS

CIBERSEGURIDAD

Conjunto de tecnologías, procesos y prácticas diseñadas para prevenir, mitigar, proteger y recuperar, activos de información, datos y/o servicios contra amenazas, ataques, o acceso no autorizado. Apunta a proteger la confidencialidad, integridad y disponibilidad de la información.

Lunes 07 septiembre de 2020 | 11:19

Secuestro de datos: ataque a la ciberseguridad de BancoEstado es sin precedentes y de carácter grave

Lunes 07 septiembre de 2020 | 20:21

Jorge Atton, exdelegado de ciberseguridad: "Vas a pensar dos veces en abrir cuenta en Banco Estado"

CIBERSEGURIDAD

ATAQUES A SISTEMAS DE CONTROL INDUSTRIALES ICS (SCADA)

Abril – Junio 2020

Saudi Insider Likely Key to Aramco Cyber-Attack

by Richard Sale (Washington) | Friday, October 19, 2012
Inter Press Service

WASHINGTON, Oct 19 (IPS) - Last weekend's disclosure that Iranian cyber warriors had disabled some 30,000 computer owned by the Saudi oil giant Aramco is attracting considerable attention here, particularly in light of a warning last we by Pentagon chief Leon Panetta that Washington could face a "cyber-Pearl Harbor".

EDP sufre un ciberataque y le piden 10 millones en bitcoin para no publicar la información robada

La compañía asegura que ni el suminitro eléctrico ni la continuidad de su actividad están en riesgo. Según los ciberdelincuentes, 10 tebabytes de información habrían sido robados

Hackers bloquean los sistemas de compañía eléctrica en Brasil y piden 7 millones de dólares en Monero como rescate

La Compañía de Energía Eléctrica Light, que suministra energía a 31 municipios de Río de Janeiro en Brasil, sufrió un ataque de hackers que bloqueó sus sistemas el pasado martes 16 de junio. La información la publicó el diario local de Veja Rio.

Según el informe, los hackers hackearon el sistema y cifraron todos los archivos, que funcionaban en Windows, con malware.

CIBERSEGURIDAD - CONTEXTO NACIONAL

2015 - Política Nacional de Ciberseguridad 2017/22:

- ✓ Lineamiento político en materia de Ciberseguridad cuyo objetivo es tener un Ciberespacio libre, abierto, seguro y resiliente.
- ✓ Ejes estratégicos: Infraestructura, Legislación, Difusión, Colaboración Internacional y Desarrollo de Industria.
- ✓ ***Infraestructura de información del sector Energía es definida como critica.***
- ✓ Establece al creación de un CSIRT Nacional – Ministerio del Interior, y promueve CSIRT sectoriales.
- ✓ ***Recomienda al sector privado establecer estándares, políticas, normativas y procedimientos de ciberseguridad.***

AGENDA LEGISLATIVA

Ley Marco de Ciber Seguridad

Ley de Infraestructura Crítica para SI

- Ley General de Bancos
- Proyecto de ley de registro de celulares prepago
- Nueva ley de delitos informáticos
- Proyecto de ley de datos personales

PLAN DE CIBERSEGURIDAD PARA EL SEN

SEC ➔

Of. Ord. 13436
Solicita información de Medidas implementadas, modelo de riesgo e información sobre incidentes y/o Intentos de Intervención.

Of. Ord. 3377
Instruye al CEN definir requisitos mínimos para el resguardo de la ciberseguridad del SEN.

Of. Ord. 11508
Solicita Cronograma y plan de actividades para implementar requerimientos mínimos.

Of. Ord. 16160
Recibe Plan e instruye acciones sobre coordinados.

Of. Ord. 21877
Solicita Fecha de instrucción medidas
Solicita reporte Bimensual.

Of. Ord. 5778
Aprueba propuesta de estándar, emite observaciones e instruye acciones

CEN ➔

DE 2927-18
Se indican Actividades de Ciberseguridad en el Coordinador.

DE2590-19
Envío Cuestionario para generar Diagnóstico de seguridad y ciberseguridad

DE03631-19
Se envía plan de trabajo (Medidas Urgentes y NERC-CIP) e informe de análisis de respuestas

DE06034-19
Solicitud de Implementación 13 medidas de ciberseguridad.

DE00503-20
Monitoreo de Reportes Bimensuales.

DE3714-20
Emite Propuesta de Estándar basado en NERC-CIP

ESTÁNDAR NERC-CIP

Objetivo: Establecer requerimientos y medidas de control destinadas a proteger infraestructura crítica contra eventos y/o amenazas de ciberseguridad que pudiesen poner en riesgo la seguridad de la operación en el sistema eléctrico.

Aplicabilidad: Todos los agentes y operadores. Categorización de instalaciones según impacto en la seguridad del sistema:

- Alto: Centros de control (principales y de respaldo)
- Medio: Instalaciones (SSEE) de Gen., Sistema Troncal (>200kV), otras que defina el ente coordinador.
- Bajo: Todo el resto de las instalación de transmisión (excluye Distribución - MT/BT)

Cumplimiento: Basado en riesgo del incumplimiento (A, M, B) y niveles de severidad de los mismos (Bajo, Moderado, Alto, Severo).

Monitoreo: Auto-evaluación anual (evidencia 3 años), salvo que hayan auditorias. "Compliance Enforcement Authority (CEA)" es la entidad responsable por la confiabilidad en cada región "Regional Entity".

Reportabilidad de Incidentes: Incidentes de Ciberseguridad Reportables (ICR) deben reportarse al E-ISAC (Information Sharing & Analysis Center) dentro de una hora de ocurrido el evento.

Fiscalización: FERC, que es la entidad reguladora, es el que fiscaliza y sanciona.

ESTÁNDAR NERC-CIP

Capítulos del estándar actualmente en vigencia

- CIP-002: Ciber Seguridad - Categorización de Ciber Sistemas SEN
- CIP-003: Ciber Seguridad – Controles de Gestión de la Seguridad
- CIP-004: Ciber Seguridad – Personal y Capacitación
- CIP-005: Ciber Seguridad – Perímetro de Seguridad Electrónica (PSE)
- CIP-006: Ciber Seguridad – Seguridad Física de Ciber Sistemas SEN
- CIP-007: Ciber Seguridad – Gestión de la Seguridad de Sistemas
- CIP-008: Ciber Seguridad – Reporte de Incidentes y Planes de Respuesta
- CIP-009: Ciber Seguridad – Planes de Recuperación para Ciber Sistemas SEN
- CIP-010: Ciber Seguridad – Gestión de Cambio de Config. y Evaluación de Vulnerabilidades
- CIP-011: Ciber Seguridad – Protección de Información
- CIP-012: Ciber Seguridad – Comunicaciones entre Centros de Control
- CIP-013: Ciber Seguridad – Gestión de Riesgos en la Cadena de Suministros
- CIP-014: Ciber Seguridad – Seguridad Física

https://www.nerc.com/pa/Stand/Pages/ReliabilityStandards.aspx

ADAPTACIÓN DE ESTÁNDAR A INDUSTRIA NACIONAL

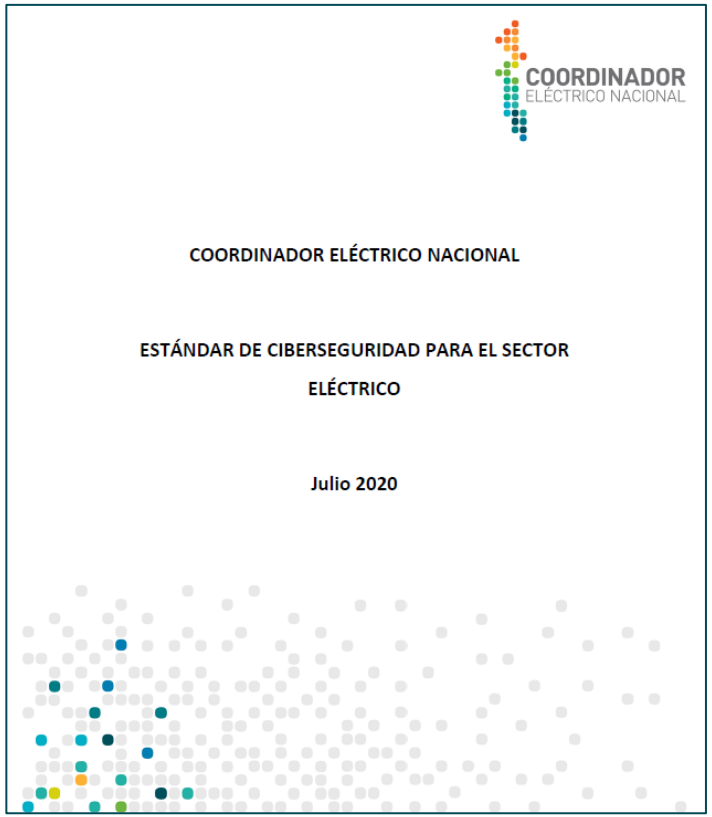
- **Capítulos**: CIP-002 al 014 (Pendiente CIP-012).
- **Aplicabilidad**: Empresas Coordinadas y Coordinador, según calificación impacto A-M-B.
- **Monitoreo y Auditorías**: Autoevaluación y entrega de reporte anual de cumplimiento al Coordinador, quien notificará de incumplimientos a la SEC y podrá instruir auditorías y/o certificaciones. Coordinador deberá monitorear implementación del estándar por parte de Coordinados.
- **Reporte de Incidentes**: ICR se notifican a la SEC y al Coordinador dentro de una hora de ocurrido el incidente. Eventualmente a otras autoridades y/o entidades responsables de la ciberseguridad nacional, en base a protocolo aprobado por SEC.
- **Confidencialidad/Reserva**: Reportes de carácter reservado a fin de proteger la información relacionada con la ciberseguridad en las instalaciones de Coordinados, así como la integridad del SEN.
- **Calificación de Instalaciones**:
  - ✓ **Impacto Alto**: CDC del Coordinador y CC de Coordinados (principales y de respaldo).
  - ✓ **Impacto Medio**: Generación >=300MW, Sistema Nacional (500/220kV), STZ 220kV FP>=300MW, PDCE, otras instalaciones que defina el Coordinador (Limites Tx en NTSyCS).
  - ✓ **Impacto Bajo**: Todas las instalaciones que no califiquen como impacto Alto o Medio. Se exceptúa la Distribución (MT/BT), asi como clientes y PMGD conectados a estos sistemas.

ESTÁNDAR NERC-CIP

FORMATO DE ESTÁNDAR

1. INTRODUCCIÓN
2. DEFINICIONES
3. APLICABILIDAD GENERAL
4. CUMPLIMIENTO Y MONITOREO
5. RESERVA Y CONFIDENCIALIDAD
6. CRITERIO CALIFICACION DE IMPACTO
7. ESTÁNDARES
   - ✓ Título
   - ✓ Propósito
   - ✓ Aplicabilidad Específica y Excepciones
   - ✓ Requerimientos y Medidas de Control

ANEXO I - Tabla Resumen de Requerimientos y su Implementación



PLAN DE IMPLEMENTACIÓN DEL ESTÁNDAR NERC-CIP

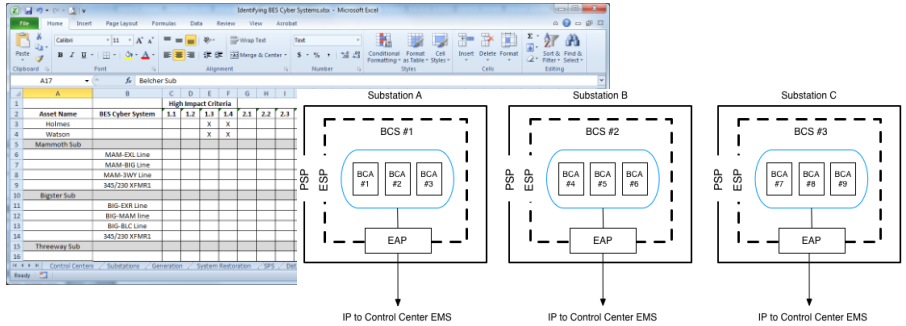
Estándar	Impacto	FRI	Marcha Blanca
CIP-002 Categorización de Ciber Sistemas SEN	A-M-B	Alto/Bajo	6 meses
CIP-003 Controles de Gestión de la Seguridad	A-M-B	Medio/Bajo	3-12 meses
CIP-004 Personal y Capacitación	A-M	Medio/Bajo	6-12 meses
CIP-005 Perímetro de Seguridad Electrónica	A-M	Medio	12 meses
CIP-006 Seguridad Física de Ciber Sistemas SEN	A-M	Medio	6-18 meses
CIP-007 Gestión de la Seguridad de Sistemas	A-M	Medio	12 meses
CIP-008 Reporte de Incidentes y Planes de Respuesta	A-M	Bajo	6-12 meses
CIP-009 Planes de Recuperación para Ciber Sistemas SEN	A-M	Medio/Bajo	8-12 meses
CIP-010 Gestión de Cambio de Configuración y Evaluación de Vulnerabilidades	A-M	Medio	10 meses
CIP-011 Protección de Información	A-M	Medio/Bajo	8 meses
CIP-014 Seguridad Física	A-M	Alto/Medio/ Bajo	6-24 meses

- Implementación gradual
- Otorgar periodo de marcha blanca
- 3 a 24 meses de implementación

ESTÁNDAR NERC-CIP: REQUERIMIENTOS

CIP-002: Inventario y Categorización de Ciber Sistemas SEN

- Procedimiento de clasificación de Ciber sistemas SEN
- Nominación de Encargado CIP

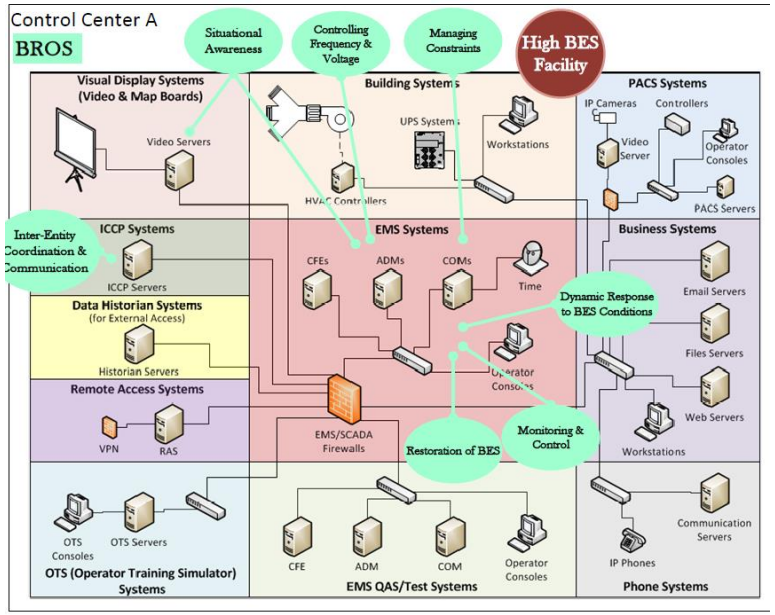


CIP-003: Controles de Gestión de la Seguridad

- Políticas de Ciberseguridad
- Requerimientos para instalaciones de impacto Bajo

CIP-004: Personal y Capacitación

- Capacitación en Ciberseguridad
- Concientización de Ciberseguridad



ESTÁNDAR NERC-CIP: REQUERIMIENTOS

CIP-005: Perímetro de Seguridad Electrónica (PSE)

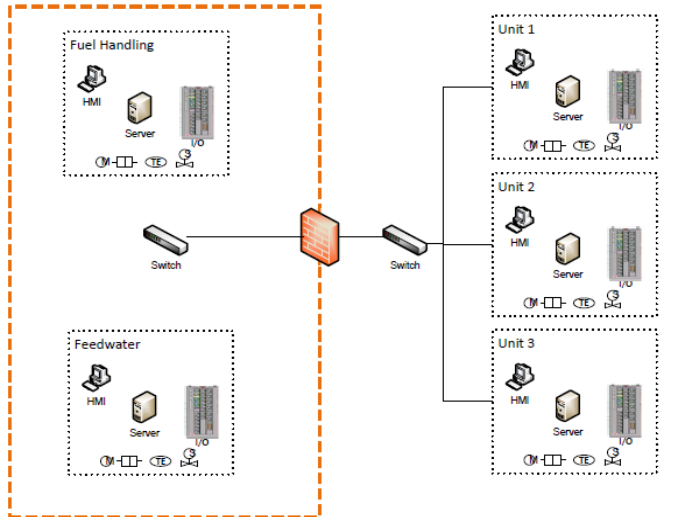
- Definición de PSEs e identificación de PAEs
- Reglas y controles de acceso

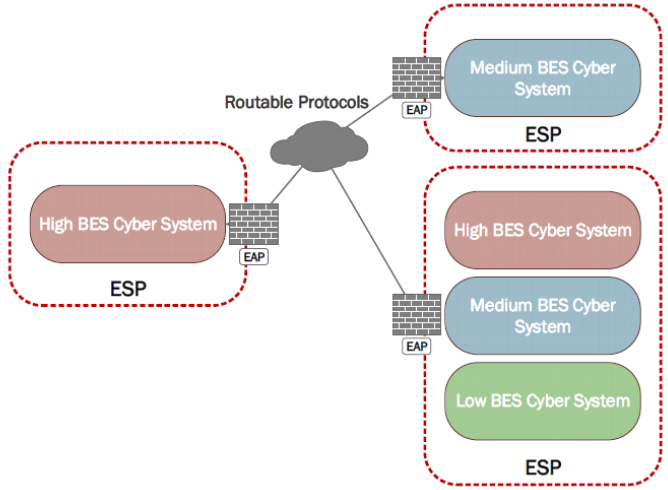
CIP-006: Seguridad Física de Ciber Sistemas SEN

- Procedimiento de control de acceso físico
- Monitoreo de acceso no autorizado y control de visitas

CIP-007: Gestión de la Seguridad de Sistemas

- Gestión de parches y protección contra código malicioso
- Protección de puertos físicos y control de acceso





ESTÁNDAR NERC-CIP: REQUERIMIENTOS

CIP-008: Reporte de Incidentes y Planes de Respuesta

- Plan y pruebas de respuesta a incidente de ciberseguridad

CIP-009: Planes de Recuperación para Ciber Sistemas

- Plan de recuperación de Ciber sistemas SEN
- Respaldo y almacenamiento de información

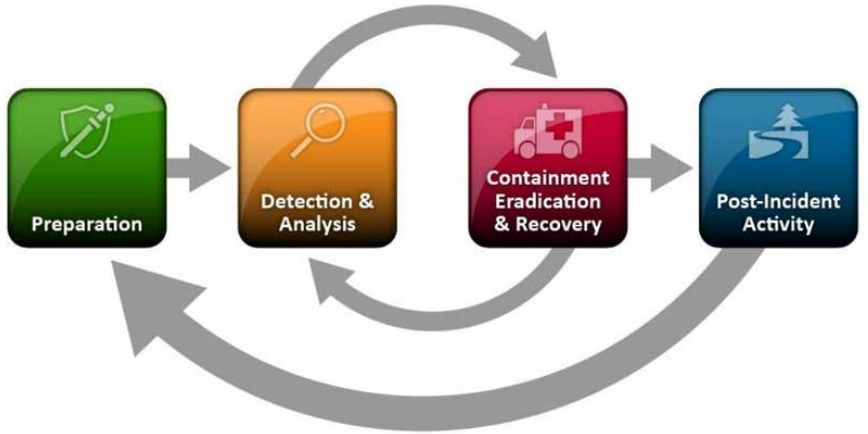
CIP-010: Gestión de Cambio de Config. y Evaluación de Vulnerabilidades

- Línea base de configuración para cada ciber activo
- Sistema de evaluación de vulnerabilidades

CIP-014: Seguridad Física

- Análisis de riesgos y evaluación de vulnerabilidades
- Plan de seguridad física de instalaciones

A DIVISION OF NERC
E-ISAC
ELECTRICITY INFORMATION SHARING AND ANALYSIS CENTER



PRÓXIMOS PASOS

- Inicio de Implementación de Estándar ➔ Octubre
- Plan de concientización y capacitación (webinars) ➔ Inicio en noviembre
- Desarrollo de guías, formatos y protocolos ➔ Continuo

NERC-CIP ONLINE TRAINING – WWW.SANS.ORG

https://meetsans.org/view/mail?iID=zghSCSqGBtHG6g6VwVL8

COORDINADOR
ELÉCTRICO NACIONAL

Estándar de Ciberseguridad Sector Eléctrico Nacional

Octubre 2020