# Capacitación teórico práctica
# CIBERSEGURIDAD NERC-CIP

**Capítulo 1**

- Introducción a la Ciberseguridad
  - Historia de ataques
  - Ciberataques del día a día
  - Modelo CIA
  - Modelo AIC
  - Modelo Deep Defense
  - Diferencias Redes IT/OT
- Seguridad operacional
  - Cuantificación de riesgos
- Estándares para la Ciberseguridad
  - Estándares, Normas y Guías
- Estructura de los estándares NERC-CIP
  - Historia del Estándar NERC
  - Sistema de Numeración NERC
  - Estructura de los estándares NERC-CIP
  - ¿Qué es infraestructura crítica?
  - Definición del alcance de la infraestructura crítica
  - Clasificación de los componentes CIP
- Ingeniería Social
  - Seguridad y Usabilidad de Contraseñas
- Demostración
- NERC-CIP-002-5.1a
  - Aplicabilidad
  - Clasificación de Activos y CiberActivos
  - Lista de Activos y Ciberactivos
- Práctica

**Capítulo 2**

- NERC-CIP-003
  - Control de Acceso Electrónico
  - Cyber Security Incident Response
  - Sensibilización en Ciberseguridad
  - Implementación de Controles para Seguridad Física
  - Respuesta Incidentes
  - Gestión de Controles de Seguridad
- Concepto de Vulnerabilidades
- Demostración
- Gestión de Seguridad de Ciber Activos Críticos
  - Mecanismos para el cumplimiento de la gestión
- Práctica

**Capítulo 3**

- NERC-CIP-004
  - Personal & Entrenamiento
- Demostración
- NERC-CIP-005
  - Perímetro de Seguridad Electrónico
  - Acceso Remoto Interactivo
  - Sistema de Monitoreo
  - Servidor AAA
- Práctica

AXON Group

**Capítulo 4**

- NERC-CIP-006
  - Plan de Seguridad Física
  - Programa de Control de Visitantes
  - Mantenimiento y Pruebas al Sistema
- Demostración
- Modelo Defensa Exhaustiva
- Modelo de Referencia OSI Aplicabilidad a la Ciberseguridad
- Switching y Data Link Layer, Media Control Access y Logical Link Control
- Práctica

**Capítulo 5**

- NERC-CIP-007
  - Servicios y Puertos → Firewall
  - Prevención de Código Malicioso
  - Gestión de Parches y Actualización de Huellas
  - Monitoreo de Eventos de Seguridad SysLog
  - Control de Acceso, Contraseñas y Autenticación
- Demostración
- Mecanismos de ciberseguridad aplicables a capa 3
- Fundamento de cifrado
- Infraestructura de llave pública y privada
- Routing
- Práctica

**Capítulo 6**

- VRRP - Virtual Router Redundancy Protocol (RFC 3768)
- Static Route y OSPF Open
- Demostración
- NERC-CIP-008
  - Plan de Respuesta para Incidentes de Ciberseguridad
  - Implementación, Pruebas y Simulacros
  - Revisión, Actualización y Documentación
- Práctica

**Capítulo 7**

- Segmentación, Alta disponibilidad
- Protocolo de Redundancia de Red
- Tunneling - IPSec
- Firewall como elemento de ciberseguridad en Subestaciones
- Demostración
- NERC-CIP-009
  - Plan de Recuperación en Ciberseguridad
  - Implementación, Pruebas y Simulacros
  - Revisión, Mejoras, Actualización y Documentación
- Práctica

**Capítulo 8**

- Gestión de acceso
- Acceso remoto interactivo
- Gestión de configuración, cambios y evaluación de vulnerabilidades
- Demostración
- NERC-CIP-010
  - Administración de Cambios de Configuraciones
  - Supervisión de Configuración
  - Evaluación de Vulnerabilidades
  - Ciberactivos Transitorios - Medios Removibles
- Práctica