NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

NERC-CIP: Estado Actual y Lecciones Aprendidas en Norteamérica

Hugo F. Pérez
Gerente de Relaciones para Norteamérica (NERC)

RELIABILITY | RESILIENCE | SECURITY




Vision/Mission

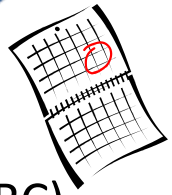
The vision for the ERO Enterprise, which is comprised of NERC and the six Regional Entities, is a highly reliable and secure North American BPS.

Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Para garantizar la confiabilidad del sistema eléctrico de potencia en Norteamérica, NERC trabaja en:

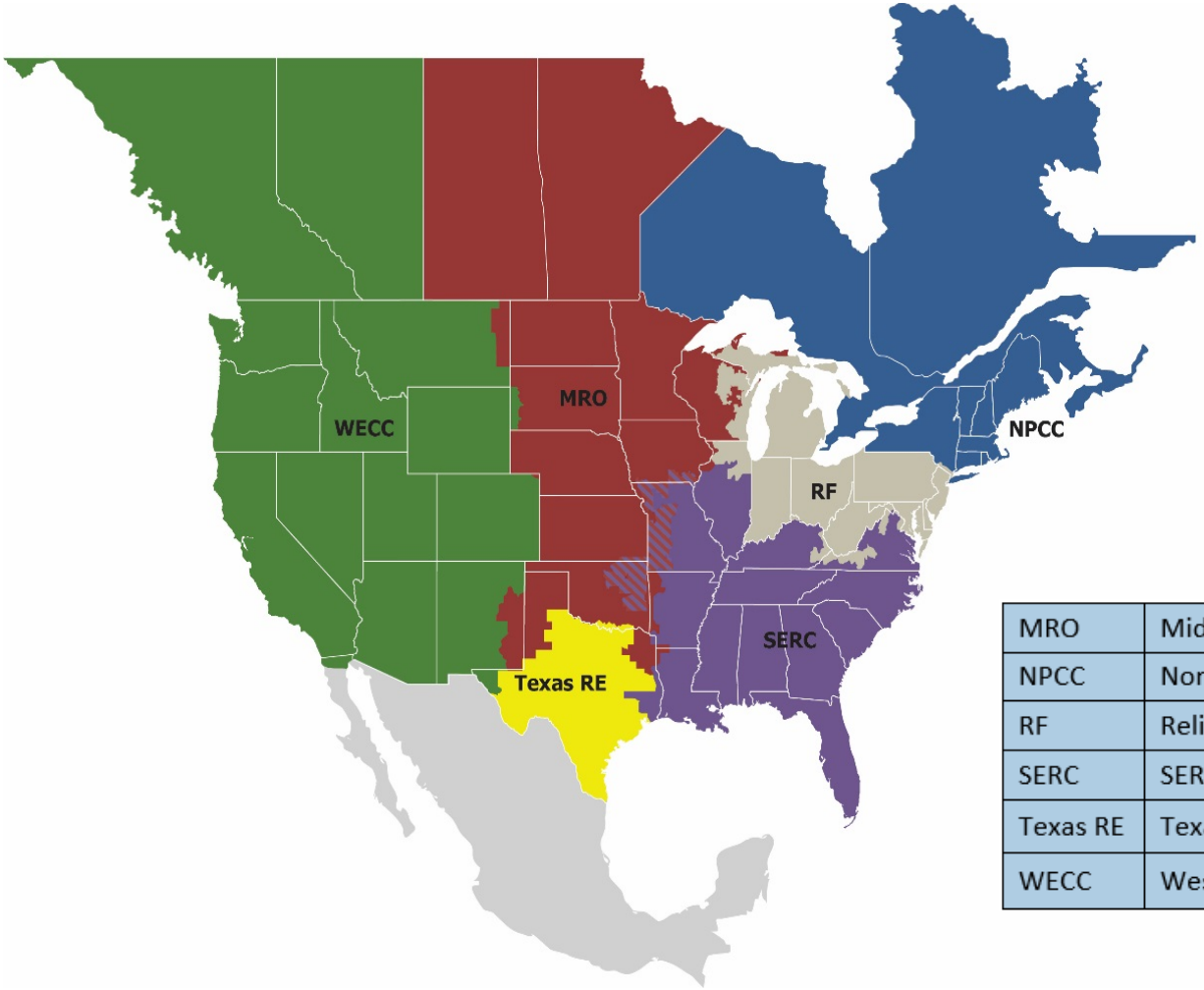
- Desarrollo y cumplimiento de los estándares de confiabilidad
- Evaluación de problemas de confiabilidad actuales y futuros
- Análisis de eventos del sistema, recomendación de mejores prácticas
- Protección de infraestructura crítica
- Educación, capacitación y conciencia situacional
- Es responsable como Electric Reliability Organization (ERO) ante organismos reguladores en los Estados Unidos (Federal Energy Regulatory Comission - FERC) y Canadá (entes gubernamentales)

Historia



1965: Apagón en el noreste. Afectados Estados Unidos y Canadá
1968: La industria eléctrica forma el National Electric Reliability Council (NERC)
1996: 10 de Agosto - Apagón en la costa oeste. Afectados Estados Unidos, Canadá y México.
2002: Las políticas de operación y estándares de NERC se vuelven obligatorios en Ontario, Canadá.
2003: 14 de Agosto - Peor apagón en la historia de Norteamérica.
2005: La ley de política energética del gobierno federal en Estados Unidos crea la ERO.
2006: Federal Energy Regulatory Commission (FERC) certifica a NERC como ERO; Se firman memorandos de entendimiento con algunas provincias en Canadá.
2007: North American Electric Reliability Council se convierte en North American Electric Reliability Corporation; FERC emite la orden para que los estándares de NERC sean obligatorios.

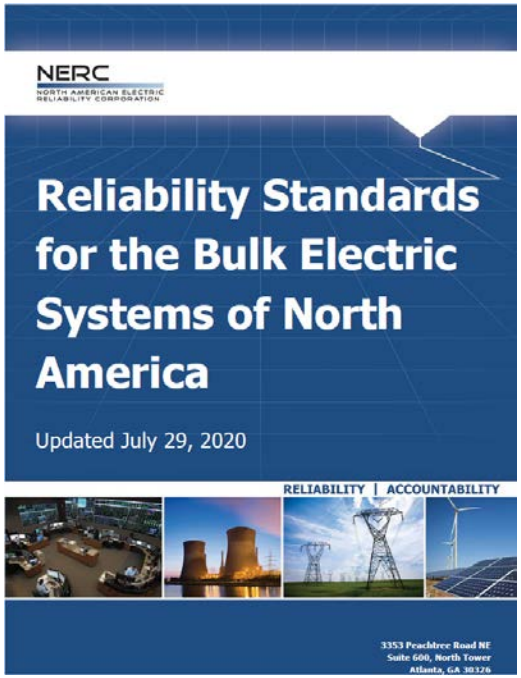
Entes Regionales



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	Western Electricity Coordinating Council

Con los avances vienen nuevos retos

Protección de la infraestructura e Iniciativas de Ciberseguridad

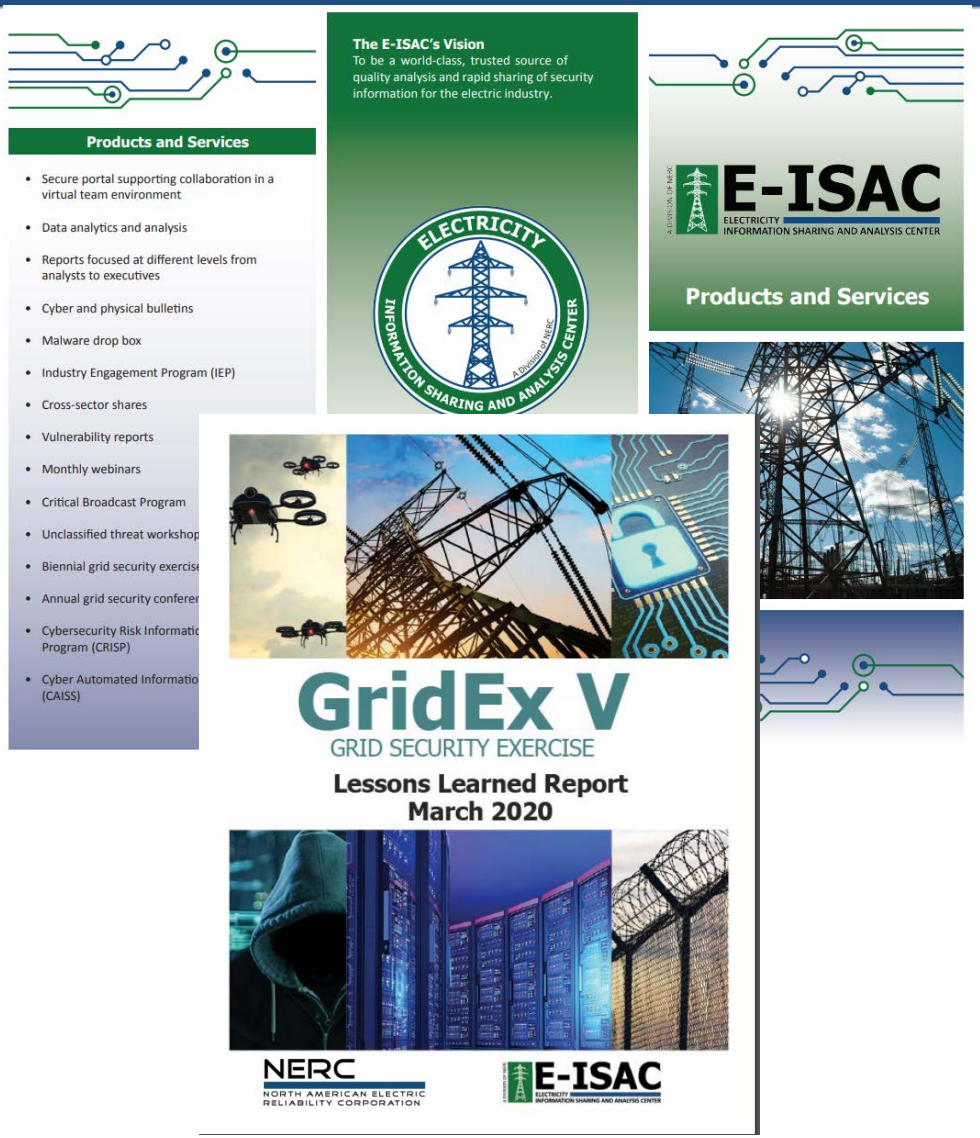


(CIP) Critical Infrastructure Protection (11)	
CIP-002-5.1a	Cyber Security — BES Cyber System Categorization
CIP-003-8	Cyber Security — Security Management Controls
CIP-004-6	Cyber Security - Personnel & Training
CIP-005-5	Cyber Security - Electronic Security Perimeter(s)
CIP-006-6	Cyber Security - Physical Security of BES Cyber Systems
CIP-007-6	Cyber Security - System Security Management
CIP-008-5	Cyber Security - Incident Reporting and Response Planning
CIP-009-6	Cyber Security - Recovery Plans for BES Cyber Systems
CIP-010-2	Cyber Security - Configuration Change Management and Vulnerability Assessments
CIP-011-2	Cyber Security - Information Protection
CIP-014-2	Physical Security

Electricity Information Sharing And Analysis Center (E-ISAC)

E-ISAC:

- E-ISAC es operado por NERC en forma independiente del área de cumplimiento de normas de confiabilidad.
- Recopila, analiza y comparte alertas de seguridad cibernéticas y físicas, advertencias y evaluaciones de vulnerabilidad basados en información de seguridad proporcionada por los miembros.
- Proporciona un medio seguro para que sus miembros intercambien información con el objetivo de defender la infraestructura crítica .
- Coordina la gestión de incidentes.
- Comunica estrategias de mitigación con las partes interesadas en todos los sectores.
- Sirve como un punto central de coordinación y comunicación para los miembros.



¿Que hemos aprendido con referencia a los estándares de ciberseguridad?

- Los estándares se deben desarrollar, implementar y monitorear con base en el riesgo e impactos al sistema.
- La claridad y la consistencia en su contenido son de vital importancia.
- El manejo adecuado de la información obtenida durante su desarrollo, implementación y monitoreo es importante para identificar riesgos a la confiabilidad y tendencias.
- El valor de los controles internos en cada una de las entidades participantes.

¿Que hemos aprendido con referencia a los estándares de ciberseguridad?

- Este es un proceso gradual.
- La colaboración entre el regulador y los participantes en la industria es primordial.
- Muchas organizaciones ya tenían los conceptos de ciberseguridad presentes en su operación.
- La ciberseguridad es responsabilidad de todos los involucrados en la industria.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Muchas gracias por su atención