Factibilidad de Adaptación y Adopción de las Normas NERC – CIP en el CENACE

A. Narváez

Centro Nacional de Control de Energía - CENACE

***Resumen*— NERC CIP son un conjunto de regulaciones y normas, creadas por la Corporación de Confiabilidad Eléctrica de Norte América - NERC, que especifican los requerimientos mínimos, en el ámbito de seguridad electrónica, seguridad física y preparación de las personas, para mantener la confiabilidad del sistema eléctrico y por ende el abastecimiento de electricidad. El objeto de este trabajo es analizar estas normas para conocerlas y establecer la factibilidad de aplicarlas en el CENACE y las implicaciones para hacerlo.**

***Palabras clave*— Protección de Infraestructura Crítica, Seguridad Cibernética, Estándares de Seguridad, Ataques Cibernéticos, Sector Eléctrico.**

1. INTRODUCCIÓN

La Protección de la Infraestructura Crítica – CIP, por sus siglas en inglés, abarca varias industrias verticales, así como el gobierno y entidades públicas y privadas. La gestión del conocimiento y de la seguridad de la Tecnología de la Información - TI es crucial para la aplicación de las normas NERC CIP.

Las normas NERC – CIP surgieron luego del blackout de agosto de 2003 en Estados Unidos, que afectó a unos 50 millones de personas, dejando grandes centros de la población, entre ellos Nueva York, Toronto y Detroit, sin comunicaciones, sin transporte público y sin otras infraestructuras y servicios esenciales. Una de las enseñanzas fundamentales fue que las empresas deben planificar y estar preparadas para continuar su operación ante emergencias y desastres.

La protección de la infraestructura de TI de eventos, tales como: los delitos informáticos, terroristas cibernéticos, guerra, desastres naturales y otras amenazas maliciosas requiere mucha coordinación y colaboración. Un fondo de gestión del conocimiento es útil en estos casos. Considerando únicamente la seguridad de TI, la Protección de Infraestructura Crítica – CIP puede convertirse rápidamente en una batalla de: firewalls, detección de intrusos, autenticación, identificación, parches de seguridad y así sucesivamente. Todas esas técnicas están diseñadas para impedir el acceso a los intrusos. Por desgracia, también dificultan el acceso a los usuarios legítimos.

En cada empresa existe la necesidad de colaborar, acceder a sistemas y compartir información y datos. Consecuentemente, como si no fuera ya difícil para los profesionales de seguridad blindar los sistemas a los intrusos, los usuarios suelen buscar formas de evitar las protecciones o de abrir agujeros de seguridad.

Aunque el objetivo principal de CIP es la seguridad informática, la práctica ha demostrado que CIP no es sólo TI, sino que consiste sobre todo en la parte física de los sistemas fundamentales para la sociedad moderna, como es el caso del suministro de combustibles, de las redes de energía eléctrica, telecomunicaciones, transporte y banca. Todos estos sistemas son muy dependientes de TI. En la economía del tiempo actual, los sistemas físicos y electrónicos son cada vez más interdependientes. En este tiempo la Internet es la infraestructura más importante de todas, dado que sin información, el mundo actual se detiene.

2. DESCRIPCIÓN DE LAS NORMAS NERC CIP

NERC CIP establece estándares en nueve áreas clave, diseñadas para proteger no solamente las centrales y subestaciones, sino todos los otros aspectos que permiten la operación global de un sistema eléctrico. Las normas incluyen: el reporte de sabotajes (sección 001), la identificación de los actives cibernéticos críticos (sección 002), desarrollo de controles para la gestión de la seguridad (sección 003), entrenamiento (sección 004), identificar e implementar perímetros de seguridad (sección 005), implementar programas de seguridad física para proteger la infraestructura crítica (sección 006), protección de activos e información dentro del perímetro (sección 007), reportes de incidentes y planes de respuesta (sección 008) diseño e implementación de planes de restablecimiento (sección 009).

Las Normas NERC CIP-001 a CIP-009 proporcionan un marco de seguridad cibernética

para la identificación y protección de los activos cibernéticos críticos, para apoyar la operación confiable del sistema eléctrico global.

Estas normas reconocen: los diferentes roles de cada entidad en la operación del sistema eléctrico global, la criticidad y vulnerabilidad de los activos necesarios para mantener la confiabilidad del sistema eléctrico y los riesgos a los que están expuestos.

Los requerimientos operativos y de negocio para la gestión y confiabilidad del sistema eléctrico dependen cada vez más de activos cibernéticos críticos que apoyan las funciones de confiabilidad y los procesos para comunicarse entre sí. Esto se traduce en un mayor riesgo de estos activos.

Los siguientes términos son importantes para entender de forma apropiada estas normas:

- Activos Críticos: facilidades, sistemas y equipamiento cuyo daño o destrucción tendría un impacto significativo en la confiabilidad del sistema eléctrico de potencia o pondría en riesgo el suministro de electricidad.
- Activos Cibernéticos: dispositivos electrónicos programables y redes de comunicación, incluyendo hardware, software y datos, que son utilizados en la operación del sistema eléctrico de potencia.
- Activos Cibernéticos Críticos: activos cibernéticos esenciales para la operación confiable del sistema eléctrico de potencia.
- En la figura 1 se presenta la clasificación de los activos de una empresa.

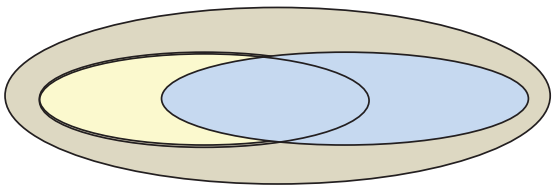

Figura 1: Clasificación de los Activos de una Empresa

2.1. CIP – 001: Reporte de Sabotajes

Las perturbaciones u ocurrencias inusuales, sospechosas o posiblemente causadas por un sabotaje, serán informadas oportunamente a los niveles apropiados, organismos gubernamentales y organismos reguladores.

2.2. CIP – 002: Identificación de Activos Cibernéticos Críticos

Esta norma requiere la identificación y documentación de los activos cibernéticos críticos asociados a los activos que soportan la operación confiable del sistema eléctrico. Estos activos críticos deben ser identificados mediante la aplicación de un análisis de riesgo.

Se debe crear un procedimiento que asegure que estos inventarios se actualicen de forma periódica.

2.3. CIP – 003: Controles de Gestión de Seguridad

Esta norma requiere que las entidades responsables tengan un mínimo de controles de gestión de seguridad, para proteger los activos críticos cibernéticos.

Se debe crear un procedimiento que asegure la atención y prioridad de la seguridad como un objetivo corporativo.

2.4. CIP – 004: Personal y Entrenamiento

Esta norma requiere que el personal que tenga acceso remoto o físico a los activos cibernéticos críticos, incluyendo a contratistas y proveedores de servicios, tenga un nivel adecuado de administración del riesgo personal, capacitación suficiente y concienciación sobre la seguridad.

Se requiere crear un procedimiento que evalúe de forma periódica la calificación del personal que tiene acceso a los activos cibernéticos críticos. Adicionalmente, se debe revisar y ajustar los permisos en función de los cambios de roles del personal.

2.5. CIP – 005: Perímetros de Seguridad Electrónica

Esta norma requiere la identificación y protección del perímetro de seguridad electrónica, dentro del cual todos los activos cibernéticos críticos residen; así como, todos los puntos de acceso en este perímetro.

Se requiere establecer un procedimiento que proteja la información y documentación de los procesos; asegurando también, que las vulnerabilidades sean evaluadas periódicamente y que se apliquen las medidas preventivas y correctivas necesarias.

2.6. CIP – 006: Seguridad Física de los Activos Cibernéticos Críticos

Esta norma tiene por objeto garantizar la aplicación de un programa de seguridad física para la protección de los activos cibernéticos críticos.

Se requiere un procedimiento que asegure que el acceso remoto y físico a los activos cibernéticos críticos se restrinja al personal autorizado. El control de accesos debe ser monitoreado y auditable a través

de logs. Los permisos de acceso deben ser revisados y ajustados de acuerdo a los cambios en el estado y roles del personal.

2.7. CIP – 007: Gestión de la Seguridad de los Sistemas

Esta norma requiere que los responsables de los activos críticos cibernéticos definan los métodos, procesos y procedimientos para modificar estos sistemas e incrementar nuevos.

Se requiere un procedimiento que permita garantizar que las políticas y buenas prácticas de seguridad se apliquen y se mantengan actualizadas.

2.8. CIP – 008: Reporte de Incidentes y Planes de Respuesta

Esta norma garantiza la identificación, clasificación, respuesta y notificación de incidentes de seguridad relacionados con los activos cibernéticos críticos.

Se requiere un procedimiento que guíe al personal a través de los procesos de reporte, documentación, respuesta y recuperación ante incidentes cibernéticos.

2.9. CIP – 009: Planes de Restablecimiento de los Activos Cibernéticos Críticos

Esta norma asegura la creación y verificación de planes de recuperación para activos cibernéticos críticos y sistemas. Adicionalmente, es necesario verificar que estos planes consideren la continuidad del negocio y técnicas prácticas de recuperación de desastres.

En la tabla 1 se presenta un resumen de las normas NERC - CIP y sus respectivos requerimientos, los cuales están numerados como: R1, R2, etc.

Tabla 1: Resumen de las Normas NERC CIP

Seguridad de Red		
CIP-001	Reporte de Sabotajes	• Disponer de un procedimiento para identificar los sabotajes (R1) • Disponer de procedimientos para el reporte de sabotajes (R2) • Disponer de guías de restablecimiento(R3) • La obligación de reportar los sabotajes a las autoridades (R4)
CIP-002	Identificación de Activos Cibernéticos Críticos	• Método de Identificación de Activos Críticos (R1) • Identificación de Activos Críticos (R2) • Identificación de Activos Cibernéticos Críticos (R3) • Revisión Anual para Aprobación (R4)
CIP-003	Controles de Gestión de Seguridad	• Política de Seguridad Cibernética en Sitio (R1) • Asignaciones de liderazgo (R2) • Política de Control de Excepciones (R3) • Protección de la Información (R4) • Control de Accesos (R5) • Gestión de Cambios y Configuración (R6)
CIP-005	Perímetros de Seguridad Electrónica	• Establecer Perímetro de Seguridad Electrónica (R1) • Controles Electrónicos de Acceso (R2) • Seguimiento de Acceso Electrónico (R3) • Evaluación de la Vulnerabilidad Cibernética(R4) • Revisión y Mantenimiento de la Documentación (R5)

Seguridad de Red		
CIP-007	Gestión de la Seguridad de los Sistemas	• Procedimientos de Prueba (R1) • Puertos y Servicios (R2) • Gestión de Parches de Seguridad (R3) • Prevención de Software Malintencionado (R4) • Gestión de Cuentas (R5) • Supervisión del Estado de la Seguridad (R6) • Eliminación o Redistribución (R7) • Evaluación de la Vulnerabilidad Cibernética (R8) • Revisión de la documentación y Mantenimiento (R9)
CIP-008	Reporte de Incidentes y Planes de Respuesta	• Plan de Respuesta a Incidentes de Seguridad Cibernética (R1) • Documentación de Incidentes (R2)
CIP-009	Planes de Restablecimiento de los Activos Cibernéticos Críticos	• Planes de Recuperación (R1) • Ejercicios y Pruebas(R2) • Control de Cambios (R3) • Respaldos y Recuperación (R4) • Pruebas de Copias de Seguridad (R5)
Seguridad Física		
CIP-006	Estándar de Seguridad Física	• Plan de Seguridad Física (R1) • Controles de Acceso Físico (R2) • Supervisión del Acceso Físico (R3) • Registro de Acceso Físico (R4) • Log de Accesos (R5) • Mantenimiento y Pruebas (R6)
Entrenamiento y Conciencia de las Personas		
CIP-004	Personal y Entrenamiento	• Conciencia (R1) • Formación (R2) • Evaluación de Riesgos del Personal (R3) • Accesos (R4)

3. BENEFICIOS DE LA APLICACIÓN DE LAS NORMAS NERC CIP

NERC - CIP no se trata sólo de cumplir con un conjunto de obligaciones, que a un costo razonable permiten minimizar el daño de los ataques maliciosos y los desastres naturales.

El cambio de los procesos y la aplicación de nuevas tecnologías para apoyar CIP pueden tener el efecto adicional de mejorar el rendimiento de las empresas. CIP involucra mejor recopilación de información, más rápidamente y usarla de la manera más eficaz. Dado que CIP se aplica al núcleo de los sistemas de la empresa, las mejoras traerán robustez y mayor confiabilidad.

La información requerida para apoyar CIP proporcionará mejor conocimiento de las áreas operativas, en el cual se basan las decisiones críticas de negocio.

Aquellas empresas que ponen atención en los beneficios empresariales de las nuevas inversiones en CIP van a obtener una ventaja competitiva sobre aquellas que no lo hacen.

4. CONSIDERACIONES E IMPLICACIONES DE LA IMPLEMENTACIÓN DE LAS NORMAS NERC – CIP

4.1. Implicaciones desde el Punto de Vista Legal y Regulatorio

Los gobiernos deben asignar nuevas responsabilidades de CIP a las empresas del sector privado; así se logrará un impacto más directo sobre la industria. Sin embargo, la incertidumbre es un elemento muy importante en este tema. Los gobiernos pueden imponer estas responsabilidades en tres formas:

a) Pagar por los programas de restablecimiento y medidas CIP.
b) Obligatoriedad de determinadas medidas de CIP.
c) Fomentar la adopción voluntaria de mejores prácticas.

Debido a las diferentes agencias gubernamentales que regulan diferentes industrias, las empresas del sector privado no pueden esperar un enfoque uniforme, situación que se añade un desafío adicional a las empresas relacionadas con dos o más industrias y áreas geográficas múltiples. Nuevas leyes y regulaciones también vendrán de los diferentes niveles de gobierno; sin embargo, el gobierno nacional tiene la responsabilidad global.

4.2. Consideraciones de las Empresas Respecto a la Protección de Infraestructura Crítica

En la realidad, las amenazas a CIP no se centran en las empresas individuales, sino en las regiones e industrias. Las amenazas a CIP van desde personas malintencionadas, como los terroristas, a los desastres naturales, como los terremotos. Los terroristas no atentarán en contra de cualquier empresa en particular; sino que, tratará de derribar partes de la infraestructura que sustenta la economía de una nación; por ejemplo: las redes públicas de telecomunicaciones. Para lograr este objetivo, los terroristas buscarán los puntos más débiles para atacar. Por lo tanto, CIP será más efectiva cuando las empresas actúan en coordinación con sus similares y aumentan el nivel general de seguridad para una industria.

Estos requerimientos se presentan en un ambiente en el que las empresas temen compartir información, porque podría implicar la exposición de su seguridad, divulgación de sus debilidades competitivas, divulgación de propiedad intelectual, etc. Para CIP las industrias necesitan nuevos foros en los que se sientan cómodas intercambiando información sobre las amenazas y mejores prácticas de seguridad. Los medios para lograr una mejor colaboración en CIP varían según la industria, dependiendo de la naturaleza de los esquemas de negocios y regulaciones que la rigen.

Consideraciones de las Empresas Respecto a la Continuidad del Negocio

Las mejoras en los planes de continuidad de negocio incluyen asegurar espacios de trabajo alternativos. Muchas empresas han trasladado sus centros de datos fuera de las áreas metropolitanas; sin embargo, sus oficinas pueden ser afectadas, en cuyo caso, los empleados deben ser capaces de seguir trabajando en una ubicación alternativa, como en un proveedor de servicio de recuperación de desastres, a través de las opciones de teletrabajo o ambos.

Es necesario disponer de una fuente de energía de reserva para garantizar un apagado ordenado de los equipos de cómputo, para evitar la pérdida de datos o daños en el hardware; así como, la continuación de las operaciones en el sitio de producción. Tener un generador de energía de reserva puede significar la diferencia para evitar o retrasar un desastre.

Un componente clave de estos planes de continuidad del negocio es una comunicación clara y efectiva con los empleados para asegurarse de que conocen sus roles durante una emergencia.

Existe la necesidad de definir los roles y misiones relacionadas con la infraestructura crítica, es decir, determinar quién es responsable de qué, en la empresa, en la industria, en las organizaciones y dentro del gobierno.

4.3. Interacción de las Áreas de Tecnología y Áreas Operativas

La mejora continua en seguridad debe ser una parte del plan de manejo del riesgo en las empresas. Para alcanzar este objetivo se debe lograr un trabajo conjunto del personal del área de tecnología y del personal de las áreas operativas. Mediante esta sinergia se logrará un enfoque correcto de los problemas generales y aquellos relacionados con seguridad.

Un plan exitoso y efectivo para la seguridad de una empresa inicia con una estrategia que incorpore la seguridad a todos los niveles de la operación. Es muy importante mantener los sistemas de control y redes con sus actualizaciones, procedimientos de seguridad, mejores prácticas documentadas y verificaciones regulares.

El primer paso para el cumplimiento de las normas NERC - CIP es la evaluación del nivel de seguridad actual, lo cual involucra el conocimiento del ambiente interno y externo de la empresa. Esto incluye:

- Alerta sobre los riesgos electrónicos antes que éstos lleguen a la organización.
- Identificación del nivel de cumplimiento regulatorio en temas de seguridad.
- Determinación de la efectividad de las herramientas de administración y seguridad.

A continuación es necesario crear una política de seguridad, determinando qué personas tendrán acceso a qué información y qué funciones podrán ejecutar.

La puesta en marcha de NERC CIP incluye:

- El diseño y la implementación de medidas de seguridad, respondiendo de forma efectiva a las vulnerabilidades.
- Garantizar la seguridad de los dispositivos, redes y aplicaciones frente a los riesgos, antes de que los mismos ocurran.
- Tomar acciones para asegurar que la información está actualizada, completa y recuperable. Esto incluye procedimientos y herramientas de recuperación, en el caso que un ataque eluda las otras medidas de seguridad.
- Finalmente, se requiere un monitoreo de seguridad del tipo 24/7 y la administración

de los recursos de información de seguridad, a fin de prevenir disturbios y minimizar las indisponibilidades.

5. ANÁLISIS DE LA FACTIBILIDAD DE ADAPTAR Y ADOPTAR LAS NORMAS NERC CIP EN EL CENACE

5.1. Determinación de los Activos Cibernéticos Críticos

De acuerdo a los lineamientos de las normas NERC-CIP, los activos cibernéticos del Sector Eléctrico Ecuatoriano son:

- El Centro de Control del Operador del Sistema Eléctrico, que en el caso del Ecuador es el CENACE.
- El Centro de Control de la empresa encargada del Sistema de Transmisión, que en el caso del Ecuador es CELEC EP - TRANSELECTRIC.
- Los Centros de Control de las Empresas de Generación.
- Los Centros de Control de las Empresas de Distribución.
- Los sistemas de control de las Subestaciones y Centrales de Generación.

Es importante indicar que los activos cibernéticos críticos incluyen también el equipamiento utilizado para telemetría, monitoreo y control.

Adicionalmente, en todas las empresas del Sector Eléctrico existen otros sistemas, que complementan la función de los Centros de Control y por lo tanto, son esenciales para mantener el suministro de electricidad. En el CENACE, los principales sistemas de este tipo, son los siguientes:

- Plataforma para el planeamiento operativo de corto, mediano y largo plazos, (ePSR).
- Sistema de Administración del Mercado Eléctrico Mayorista – SIMEM.
- Sistema de Medición Comercial – SIMEC.
- Sistema de Gestión de Combustibles – SICOMB.
- Sistemas utilizados para el Análisis Post-Operativo.

5.2. Análisis de la Factibilidad de Adaptar las Normas NERC – CIP al CENACE

En Estados Unidos las normas NERC – CIP surgieron ante la necesidad de minimizar la indisponibilidad del servicio de electricidad, en condiciones de emergencia dadas por un blackout o por ataques terroristas o ataques cibernéticos. En este contexto, se estableció que todas las compañías del Sector Eléctrico debían cumplir completamente con las normas NERC – CIP y estar preparadas para una auditoría hasta diciembre de 2010 y se establecieron penalidades de hasta un millón de dólares por día para aquellas compañías que no cumplieran.

Consecuentemente, muchos de los requerimientos establecidos por las normas NERC – CIP, son demasiado exigentes y demandan una cuantiosa inversión, lo cual no se compadece de la realidad socio – económica del Ecuador. Sin embargo, en base a la revisión realizada se puede concluir que las normas NERC – CIP están basadas en las mejores prácticas de la seguridad física y cibernética y pueden adaptarse a cualquier sistema tecnológico.

Por lo tanto, el primer paso para la implementación de las normas NERC – CIP en el CENACE constituye un análisis que determine aquellos requerimientos aplicables y aquellos que requieren ser modificados para adaptarse a la realidad del Sector Eléctrico Ecuatoriano y a los sistemas tecnológicos del CENACE.

5.3. Análisis de la Factibilidad de Adoptar las Normas NERC - CIP en el CENACE

El CENACE desde hace varios años ha venido aplicando buenas prácticas en el tema de seguridad, por lo tanto, cumple con algunos de los requerimientos de las Normas NERC – CIP. En la tabla 2 se presenta un resumen de las actividades que se deberían desarrollar para cumplir los requerimientos de NERC – CIP y cuáles de aquellos requerimientos el CENACE ya cumple.

Tabla 2: Actividades para el Cumplimiento de las Normas NERC - CIP por parte del CENACE

CIP-001	
Cumple	Dispone procedimientos de restablecimiento
Por Cumplir	Elaborar un procedimiento para identificar los sabotajes
	Elaborar un procedimiento para reportar los sabotajes
CIP-002	
Por Cumplir	Elaborar un procedimiento para identificar los activos críticos
	Identificar los activos críticos
	Identificar los activos críticos cibernéticos
	Elaborar un procedimiento para la verificación anual de la metodología de identificación y aprobación de la lista de activos críticos
CIP-003	
Cumple	Se dispone de políticas de seguridad informática
	Se dispone de un sistema de control de accesos electrónicos
Por Cumplir	Complementar las políticas de seguridad cibernética
	Definir un Administrador que garantice el cumplimiento permanente de NERC - CIP
	Definir los requerimientos de NERC - CIP que no podrán cumplirse
	Elaborar un procedimiento para la identificación, clasificación y protección de la información relacionada con activos críticos cibernéticos
	Elaborar un procedimiento para el control de cambios y la administración de configuraciones.
CIP-004	
Por Cumplir	Elaborar un programa para asegurar que el personal que tiene acceso a los activos críticos cibernéticos reciba periódicamente refuerzos en las mejores prácticas de seguridad
	Elaborar un programa de entrenamiento en seguridad cibernética para el personal que tiene acceso a los activos críticos cibernéticos
	Elaborar un programa para la valoración de riesgos causados por el personal
	Elaborar una lista del personal con permiso de acceso a los activos críticos cibernéticos
CIP-005	
Cumple	Se han definido perímetros de seguridad electrónica
Por Cumplir	Elaborar un procedimiento sobre el control de acceso al perímetro de seguridad electrónica; así como, su monitoreo.
	Realizar una evaluación anual de la vulnerabilidad cibernética
	Mantener actualizada la documentación relacionada con los puntos anteriores
CIP-006	
Cumple	Se dispone de un sistema de control de accesos físicos
	Se dispone de procedimientos para la supervisión, registro y logs de los accesos físicos
Por Cumplir	Elaborar un plan global de seguridad física incluyendo auditorías periódicas al sistema de control de accesos
CIP-007	
Cumple	Existen políticas para asegurar que sólo los puertos indispensables están abiertos.
	Se dispone de mecanismos de prevención de software malicioso
Por Cumplir	Elaborar un procedimiento para la inclusión de nuevos activos críticos sin afectar la seguridad global.
	Elaborar un procedimiento para aplicar los parches disponibles y aplicables a cada activo cibernéctico crítico cibernético
	Elaborar un procedimiento para la administración de cuentas de acceso, incluyendo su revisión periódica.
	Elaborar un procedimiento para evaluar periódicamente el estado actual en materia de seguridad.
CIP-008	
Por cumplir	Elaborar un plan de respuesta ante incidentes de seguridad cibernética
CIP-009	
Cumple	Existen procedimientos para el respaldo, verificación de respaldos y recuperación de la información relacionada con los activos críticos cibernéticos
Por cumplir	Elaborar un procedimiento para la recuperación de los activos críticos cibernéticos
	Auditar y probar de forma anual el procedimiento de recuperación
	Actualizar periódicamente el plan de recuperación para complementarlo con las lecciones aprendidas

De este análisis se puede concluir que es factible adoptar las normas NERC – CIP en el CENACE.

5.4. Formulación de un Proyecto para Implementar las Normas NERC - CIP en el CENACE

5.4.1. Descripción del Problema

El CENACE administra gran parte de la información sensible del Sector Eléctrico Ecuatoriano; por lo tanto, es fundamental garantizar la seguridad de los

activos críticos cibernéticos que hacen factible el abastecimiento de energía eléctrica al país.

5.4.2. Definición de la Visión del Proyecto

Adaptar las normas NERC – CIP, que están basadas en las mejores prácticas de seguridad, a la realidad del CENACE y del Sector Eléctrico Ecuatoriano, implementarlas y monitorear de forma periódica su cumplimiento.

5.4.3. Requerimientos de Alto Nivel

Se necesita un grupo de trabajo multidisciplinario que elabore y ponga en práctica los procedimientos exigidos por las normas NERC – CIP. Se requiere la emisión de políticas claras en la materia de seguridad por parte de las autoridades del CENACE y las entidades responsables del Sector Eléctrico. Se requieren los recursos tecnológicos para la ejecución de los procedimientos y políticas antes mencionados.

5.4.4. Interesados

Los beneficiaros y actores de este proyecto serán el Personal Directivo y Operativo del CENACE; así como, el Personal Directivo de las entidades del Sector Eléctrico y los usuarios finales de la electricidad.

5.4.5. Estrategia de Implementación

- Definición del Equipo de Trabajo, con integrantes de todas las áreas del CENACE
- Determinación de los requerimientos de las normas NERC – CIP que aplican al CENACE
- Clasificación los requerimientos en etapas graduales de implementación y elaboración de cronogramas
- Emisión de las políticas de seguridad por parte del Directorio y Comité Ejecutivo del CENACE
- Conceptualización de los procedimientos exigidos por las normas NERC – CIP
- Concientización del personal del CENACE en la materia de seguridad
- Aplicación de las políticas y procedimientos establecidos
- Implementación del perímetro de seguridad electrónica mediante los recursos tecnológicos necesarios
- Evaluación periódica del nivel de cumplimiento de los requerimientos de las normas NERC – CIP

6. CONCLUSIONES Y RECOMENDACIONES

El CENACE dispone actualmente un alto nivel de seguridad física y cibernética; sin embargo, la tendencia actual de los sistemas de control, para pasar a una arquitectura abierta implica conexiones e interoperabilidad con los sistema corporativos, lo cual introduce impredecibles vulnerabilidades cibernéticas. En este contexto las normas NERC – CIP constituyen un régimen efectivo para la seguridad física y cibernética.

Se concluye que es factible adoptar las normas NERC – CIP en el CENACE. Para lograr este objetivo es necesario integrar un grupo interdisciplinario, definir políticas claras de seguridad, desarrollar un gran número de procedimientos, adicionales a los ya existentes, implementar un componente importante de infraestructura tecnológica y crear una cultura de seguridad en su personal.

Se recomienda que antes de iniciar la implementación de las normas NERC – CIP, se definan cuáles requerimientos son aplicables al CENACE sin ninguna modificación, cuáles requieren ser modificados para que se adapten a la realidad del Sector Eléctrico Ecuatoriano y aquellos requerimientos que no son aplicables al CENACE.

Los principales beneficios de la implementación de las normas NERC – CIP en el CENACE son: garantizar la disponibilidad de los activos críticos cibernéticos que hacen factible el abastecimiento de la demanda de energía eléctrica; y, asegurar una respuesta oportuna y efectiva en condiciones de emergencia, ante desastres y ataques cibernéticos.

REFERENCIAS BIBLIOGRÁFICAS

[1] Caldwell F. (2003). “What’s Critical in Critical Infrastructure Protection”, GARTNER Inc, Estados Unidos.

[2] Staggs K. (2008). “Meeting NERC - CIP Requirements”. Power Engineering Magazine, Estados Unidos.

[3] Critical Infrastructure Protection Standards. (2011). North American Electric Reliability Corporation - NERC. Estados Unidos.

[4] Witty R. (2003). “Blackout Lessons on How to Prepare for Emergencies”, GARTNER Inc, Estados Unidos.

[5] Mogull R, Moore C, Fraley D, Goodwin R and Earley A. (2004). “Predicts 2004 and Critical Infrastructure Protection”, GARTNER Inc, Estados Unidos.

[6] Mogull R. (2003). “Critical Infrastructure Protection Comes of Age”, GARTNER Inc, Estados Unidos.

[7] Bace J, Huntley H, Hunter R. (2010). “U.S. Cybersecurity Bills Show Regulatory Impulse Is Gaining Traction”, GARTNER Inc, Estados Unidos.

[8] Caldwell F. (2002). “U.S. Cyber Security Strategy Follows Best Practices”, GARTNER Inc, Estados Unidos.

[9] Pescatore J, Hunter R, Caldwell H, and Stiennon R. (2003). “What’s Critical in Critical Infrastructure Protection”, GARTNER Inc, Estados Unidos.

[10] Steenstrup K. (2011). “IT and Operational Technology Alignment Innovation Key Initiative Overview”, GARTNER Inc, Estados Unidos.

Andrés Narváez - Nació en Montufar en 1977. Recibió su título de Ingeniero Eléctrico de la Escuela Politécnica Nacional en el 2000; de Máster en Ingeniería Eléctrica de la Escuela Politécnica Nacional en el 2009. Sus campos de investigación están relacionados con el Control Automático de Generación, Redes Inteligentes, Sistemas de Monitoreo de Área Extendida, Aplicaciones de Análisis de Red y SCADA/EMS.