TECNOLOGÍA Y MODELO DE SEGURIDAD DE NEGOCIO PARA EL CENACE: SIMEC UN CASO A CONSIDERAR

Gonzalo Uquillas
Germán Pancho
Dirección de Sistemas de Información

RESUMEN

El artículo formula en base a principios y prácticas aceptados por la industria, un *modelo de seguridad* para empresas del sector eléctrico, con conceptos y fundamentos de uso extenso que pueden ser personalizados, en el cual la *gestión del riesgo* es un componente central que interactúa con elementos asociados a estrategias y procesos de negocio, infraestructura física y sistemas IT[1].

Se describe el proyecto *Sistema de Medición Comercial (SIMEC)* que está siendo implantado por el CENACE, y que prevé tendrá un impacto significativo en la administración de riesgos operativos, financieros y de información, así como en la productividad y desempeño de los procesos de liquidación de las transacciones del *Mercado Eléctrico Mayorista (MEM)*.

PALABRAS CLAVE: Modelo de Seguridad, Administración de Riesgos, Sistemas de Medición Comercial.

1. MERCADOS, RIESGOS Y SEGURIDAD

La operación de un Sistema Eléctrico de Potencia (SEP) es altamente interdependiente, una falla en la generación, transmisión y/o distribución, puede comprometer la confiabilidad de todo el sistema. Así mismo, los mercados eléctricos, al ser una *red de transacciones económicas interdependientes*, basan su funcionamiento confiable y continuo, no solo en la disponibilidad de recursos de la infraestructura eléctrica, sino también en los sistemas de monitoreo, despacho y en las propias aplicaciones que permiten la administración comercial del negocio.

Es una realidad que el núcleo de las operaciones del sector depende de manera creciente de las tecnologías de información expuestas a amenazas particulares. En el segmento de gestión eléctrica los sistemas SCADA/EMS expanden su interconexión a otros centros de control en varios niveles de jerarquía, a aplicaciones y servicios corporativos, muchos de los cuales a su vez son accesibles desde el exterior[2]. Por su parte, los procesos y transacciones de mercado se han incrementado dramáticamente a consecuencia del surgimiento de los mercados regionales, la expansión de las transacciones digitales en Internet y las redes privadas virtuales; de hecho, funciones de gestión y casación de ofertas, subastas de servicios, gestión de la medición de energía se están ejecutando en estos entornos.

La propia interconexión de soluciones IT inter-empresas para compartir información, debe ser planificada, configurada, implantada, monitoreada, mantenida y desconectada (si fuera el caso), pues, en función de los métodos y niveles de conectividad, se caracterizan los riesgos asociados a la integración[3]. En definitiva, el negocio eléctrico se está convirtiendo en una expresión pura de comercio electrónico.

Debido a esta mutua vulnerabilidad, es preciso proteger los recursos críticos[4] de la red eléctrica y del mercado mediante un *modelo de seguridad*, basado en estándares mínimos aceptadas como prácticas probadas en el ámbito de la seguridad[5], que defina planes de mitigación y acciones, la asignación y reconocimiento de los roles de los entes participantes[6] y la identificación de los riesgos a ser controlados. Aunque se disponga de modelos de referencia, la estructuración de programas particulares, si bien puede tomar como base estos conceptos, deben ser personalizados para reflejar la evaluación individual de una organización en cuanto a necesidades, vulnerabilidades, consecuencias y su tolerancia al riesgo.

Con fines de ilustración, en la Tabla 1, se indican los ítems claves que la FERC[7] considera para una *evaluación rápida* acerca de la existencia de estándares de seguridad en una empresa del sector eléctrico.

Cualquiera sea la referencia a escoger y personalizar, la magnitud de la infraestructura a proteger y el tipo de empresa, existen principios intrínsecos de alto nivel con especial énfasis en el componente IT que guían la estructuración de un modelo de seguridad, así:

[1] IT- Information Technologies: hardware, software, datos, redes, comunicaciones y servicios de información.
[2] Referencia: Report of the President's Commission on Critical Infrastructure Protection.
[3] Referencia: Security Guide for interconnecting information technology systems. Recommendations of the National Institute of Standards and Technology.
[4] Recurso o combinación estos, que en caso de afectación o destrucción adversa, tendría un impacto en la capacidad de atender a grandes cantidades de clientes por un período de tiempo extenso, en la confiabilidad/operación de la red eléctrica o puede causar un riesgo significativo sobre la salud y/o seguridad pública.
[5] CTSEC, ITSEC, IPSEC, ISO 17799, NIST Guidelines, and the NERC Security Guidelines.
[6] Operadores de mercado (ISO, RTO), comercializadores, transmisores, generadores, distribuidores y otras entidades.
[7] FERC: Federal Energy Regulatory Commission.

a) La gestión de seguridad ayuda al cumplimiento de la misión de una organización, mediante la protección de sus recursos, reputación, posición legal, empleados y otros activos tangibles e intangibles, por tanto es un elemento integral de la administración moderna de empresas.

TABLA 1: Hints Evaluación de Estándares de Seguridad - FERC

ITEM	SI	NO
Seguridad perimetral definida y documentada?		
Programas y políticas de seguridad establecidos y documentados?		
Políticas, estándares y procedimientos revisados al menos anualmente?		
Sistema de clasificación de activos definidos e implementados?		
Cumplimiento de los requerimientos de capacitación de personal que tiene acceso a activos críticos?		
Todo el personal recibe un programa de concientización en temas de seguridad al menos una vez por año?		
Administradores y operadores en activos críticos tienen un background en temas relacionados de al menos 5 años?		
Procedimientos de control de acceso para personal autorizado implementado?		
Personal no autorizado dentro del perímetro de seguridad está acompañado todo el tiempo?		
Procedimientos informáticos para seguridad de sistemas han sido desarrollados y su cumplimiento es monitoreado todo el tiempo?		
Procedimientos físicos para seguridad de sistemas han sido desarrollados y su cumplimiento es monitoreado todo el tiempo?		
Requerimientos de seguridad para el desarrollo y pruebas de sistemas críticos están documentados		
Entornos de desarrollo de software no están conectados a sistemas operacionales?		
Planes de respuesta a incidentes están implementados?		
Planes de continuidad de negocio están establecidos y probados?		

Nota: Referencia tomada del documento **ADDENDUM.-** Annual Self-Certification of Compliance with FERC Security Standards (Due January 31, 200).

b) La gestión de seguridad debe ser evaluada para asegurar que el costo de los controles no excedan los beneficios esperados. La seguridad debe ser apropiada y proporcional al valor y el grado de dependencia de los sistemas, a la severidad, probabilidad y extensión del potencial daño.

c) La gestión de seguridad debe ser comunicada y difundida. A los clientes externos se debe compartir el conocimiento acerca de los mecanismos de seguridad implantados que otorguen confianza de los niveles de protección en procesos e infraestructura. La responsabilidad de los propietarios, proveedores y usuarios de los sistemas IT debe ser explícita.

d) La seguridad IT requiere de un enfoque integrado, que considere áreas internas y externas, el ciclo de vida de la información, con revisiones periódicas en virtud de la propia dinámica del entorno, la aplicación de nuevas tecnologías, la conexión con otras redes, al cambio en el valor o uso de la información o debido a la existencia de nuevas amenazas.

e) La seguridad IT está limitada por factores sociales, ya que generalmente se hacen implementaciones para realizar la identificación de usuarios y el seguimiento de sus acciones, sin embargo las expectativas de privacidad pueden ser violadas por algunas medidas de seguridad, a veces apoyadas por leyes y regulaciones.

Las prácticas de seguridad que forman parte de un modelo están derivadas y/o limitadas en relación de uno o más principios. Así por ejemplo, la gestión del riesgo es directamente derivada del principio de costo-beneficio, mientras que la auditoría de control de accesos y protección a información sensible puede estar limitada por el factor social de confidencialidad. Mapear esta correlación probablemente no es relevante, lo trascendente es proveer los fundamentos de un modelo sustenta la sección siguiente.

2. FORMULACIÓN DE UN MODELO DE SEGURIDAD

A continuación se propone un modelo de seguridad práctico que integra los principios enunciados, lineamientos enfocados al sector eléctrico y prácticas de seguridad IT, a fin de guiar al CENACE y cualquier organización en el tipo de controles, objetivos y procedimientos, en base a los siguientes elementos:

i) *Definición de políticas* que establezcan las directrices de alto nivel en cuanto al alcance y aplicabilidad del programa de seguridad, objetivos, responsabilidades, estrategias y decisiones organizacionales. Las políticas deben ser coherentes con la misión de la empresa, normas y cultura interna, impartida desde la alta dirección, difundida adecuadamente y soportada por estándares, instructivos y procedimientos.

ii) *La Administración del Riesgo*[8] como un proceso constante de evaluación y priorización sistemática de riesgos sobre los *objetivos de negocio*, ejecución de acciones para controlar el riesgo y análisis del costo/beneficio de las alternativas de mitigación (*esto es aceptar, transferir, eliminar, controlar, compartir y/o evitar el riesgo*).

Los objetivos del negocio son oportunidades que una organización escoge poseer, definen la filosofía de la compañía y su misión, orientan las estrategias corporativas, definen los productos y servicios y las relaciones fundamentales con empleados, proveedores, accionistas, gobierno y sociedad y los riesgos que sobre éstos pueden existir son de diversa naturaleza:

[8] Riesgo según COSO (Comitee of Sponsoring Organizations of the Treadway Commission, 2004): factor interno o externo, de posible ocurrencia, que podría afectar adversamente la consecución de un objetivo del negocio.

- *Estratégicos*: relacionados con hacer las cosas erradas.
- *Operativos:* relacionados con hacer las cosas correctas de una manera errada.
- *Financieros:* relacionados con pérdidas financieras o incurrir en responsabilidades inaceptables.
- *De información:* relacionados con información equivocada o no relevante, sistemas no confiables o reportes inexactos.

Una adecuada gestión de riesgos realiza en forma iterativa evaluaciones, definiciones de políticas, implementación de controles, auditorias y mediciones, a fin de mantener niveles aceptables de seguridad sobre sus activos, incrementar la probabilidad de alcanzar los objetivos estratégicos y lograr iniciativas de cambio, afianzar ventajas competitivas, desarrollar una cultura de responsabilidad, ajustar las políticas y procedimientos de la empresa y promover el mejoramiento a través de proyectos y planes de acción.

iii) *Planeación del Ciclo de Vida* que integre conceptos y criterios de seguridad en cada una de las fases del desarrollo/adquisición de infraestructura IT, desde la formulación de requerimientos funcionales y de diseño y la ejecución de pruebas durante la implantación, hasta la determinación de los niveles de servicio (*SLA-Service Level Agreement*) durante la operación y administración.

iv) *Gestión del Personal* que mitigue las amenazas al interior de la organización, mediante estándares y procedimientos cuidadosos de contratación del personal, especialmente aquel que estará a cargo de la operación/administración de activos críticos, incluyendo contratistas y proveedores.

v) *Preparación de contingencias y desastres,* para apoyar el cumplimiento de los procesos y estrategias de la organización, ante la ocurrencia de incidentes en diferentes grados de severidad.

La evaluación de la conveniencia de un plan de contingencia está determinado por el *punto óptimo de recuperación del sistema*, mediante un balance del costo de la inoperabilidad versus el costo de los recursos requeridos para restaurar el sistema.

vi) *Capacidad de respuesta ante amenazas* que asegure que la organización y su personal, entienda como reaccionar ante la ocurrencia de un espectro amplio de amenazas físicas o informáticas[9], caracterizados por varios niveles de alerta y que a su vez puede derivar en la activación de un plan de contingencia.

vii) *Seguridad física* que mitiguen las amenazas dentro y fuera de la organización con mecanismos dedicados a de protección de bienes y personal, control de accesos, extinción de incendios, suministro de servicios, colapso frente a terremotos, intercepción de datos en redes móviles, entre otros aspectos.

viii) *Concientización y entrenamiento* enfocado a temas de seguridad mediante actividades periódicas de planificación, implementación, preparación de documentación formación de instructores, ejecución de eventos, revisión de estrategias de motivación y evaluación.

ix) *Operaciones y soporte informático,* aspecto crítico si se considera la dependencia de las organizaciones en los sistemas IT. Elementos claves a considerar son: los inventarios de información sensible, bases de conocimientos para soporte técnico, gestión de la configuración, entornos de simulación y pruebas, respaldos, control de medios, etc.

En relación con la protección de *información sensible* contra daños, alteraciones y amenazas, se recomienda estructurar un esquema jerárquico de *clasificación de la confidencialidad* de la información, así como definir los requerimientos y condiciones de autorización para desclasificarla.

x) *Control de acceso lógico* que permita la identificación y autenticación de usuarios a servicios y aplicaciones para prevenir accesos no autorizados y auditar identidades. Especiales consideraciones se debe aplicar a sistemas IT delicados de tipo EMS, SCADA o de operaciones transaccionales de mercado, en la configuración de perfiles de acceso, instalación de firewall´s, ejecución de auditorías.

No obstante de las ventajas de la integración de sistemas IT para compartir información y servicios, éstos pueden exponer a las organizaciones participantes a riesgos, especialmente si la interconexión no está apropiadamente diseñada, es por eso que se recomienda que las partes suscriban los denominados *Interconnection Security Agreement (ISA)* y *Memorandum of Understanding-Agreement (MOU/A).* El ISA especifica los requerimientos de seguridad y técnicos de la interconexión, y el MOU/A define las responsabilidades de las empresas participantes.

3. NUEVO SISTEMA DE MEDICIÓN COMERCIAL DEL ECUADOR

La implementación de innovaciones tecnológicas alineadas con los objetivosrocesos de negocio es un pilar fundamental para empresas que tienen a su cargo la Administración y/o Operación de Mercados Eléctricos.

El CENACE, Administrador Técnico y Comercial del MEM, está en la fase final de implantación de un Sistema de Medición Comercial (SIMEC), que tendrá

[9] Referencia: NERC's "Threat Alert Levels and Response Guidelines".

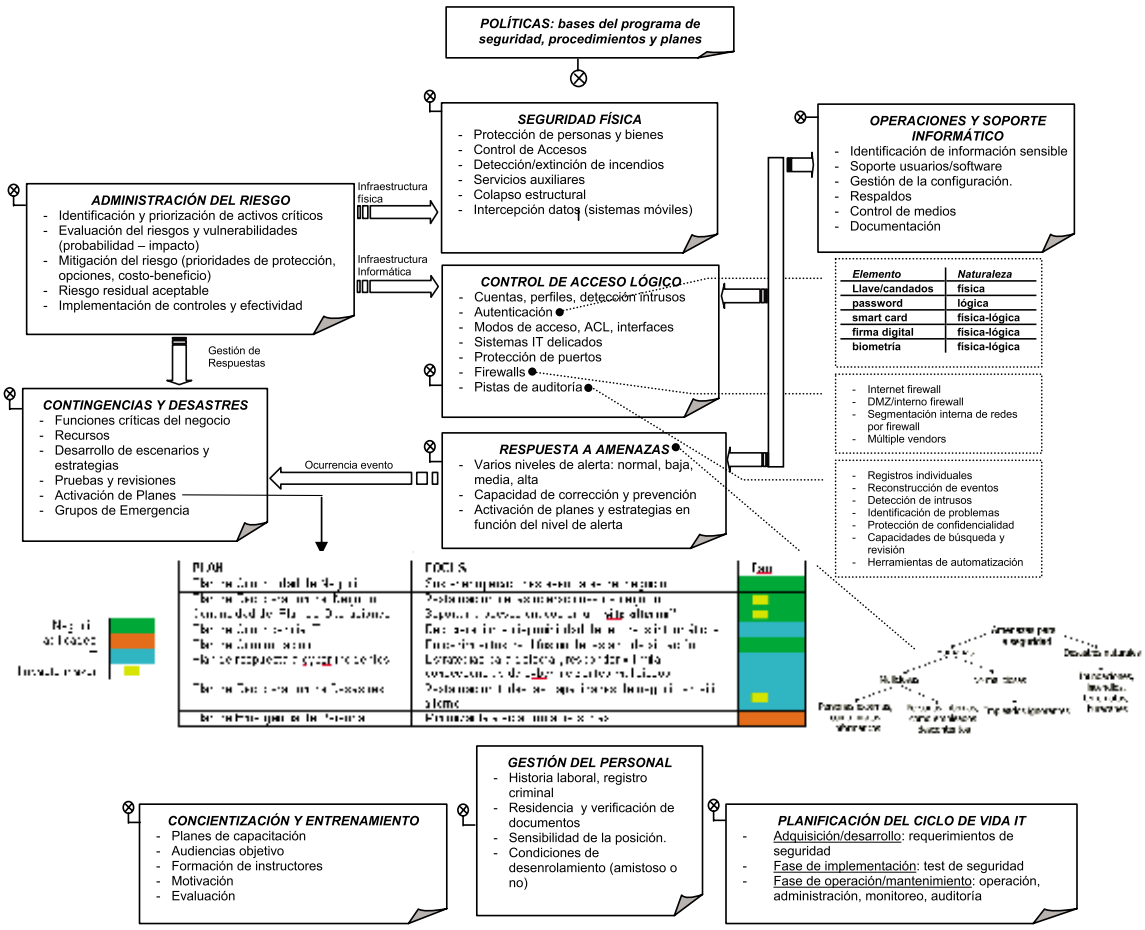


FIGURA 1: Modelo de Seguridad

un impacto importante en la administración de riesgos operativos, financieros y de información y en la productividad de los procesos de liquidación de las transacciones del MEM cuya facturación alcanza un monto aproximado de 900 millones de dólares anuales.

3.1. Arquitectura Funcional

SIMEC prevé formar parte de una arquitectura corporativa informática integrada al nuevo *Sistema de Gestión de Energía*, con el fin de importar datos registrados por éste y exportar curvas de carga para la ejecución de funciones de aplicación; y con el nuevo *Sistema de Transacciones Comerciales*, a fin de proporcionar una base de datos para el cálculo económico de las obligaciones financieras del MEM.

El SIMEC es un componente del denominado *Proyecto de Complementación del CENACE* que permitirá gestión de la medición de los registros horarios de energía, potencia y otros parámetros eléctricos, en alrededor de 500 puntos de generación/entrega del *Sistema Nacional Interconectado (SNI)*.

La arquitectura funcional del SIMEC incluye los

componentes de adquisición y gestión de datos, de procesamiento de información, y de almacenamiento y recuperación, integrados a través de la plataforma de sistemas operativos, base de datos y software de gestión de red.

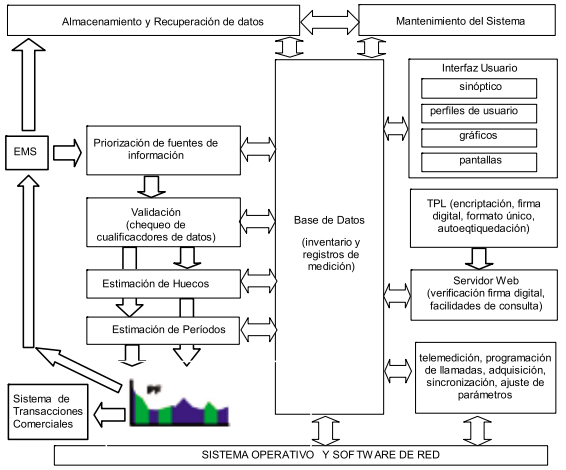


FIGURA 2: - Arquitectura Funcional del SIMEC

3.1.1. Adquisición y Gestión de la Información de Puntos de Medición: Con Capacidades de:

a) Recepción de la información remitida por parte de los Agentes, en un servidor Web, relativa a los registros cuarto-horarios de energía[10] (incluyendo códigos de validez), eventos y parámetros de calidad[11], los mismos que son obtenidos mediante una aplicación denominada *Terminal Portátil de Lectura* (TPL). TPL es un software multiprotocolo, que es "personalizado" para cada Agente, con capacidad de conexión y descarga local/remota a medidores/registradores y que genera archivos de salida de formato interno de datos predefinido, autoetiquetados en base a normas de codificación que identifican de manera unívoca al punto de medición y el rango de datos almacenados y que están acompañados de firma digital para asegurar la inviolabilidad e integridad de la información.

b) Telemedición de los datos almacenados en los medidores/registradores, mediante conexiones programadas (en función de horarios específicos, reintentos, número de sesiones, velocidad de transmisión, etc.) y a través de Internet para aquellos nodos IP.

c) Gestión remota de los medidores/re-gistradores, para propósitos de sincronización remota y ajuste de parámetros de los transformadores de potencial y corriente.

[10] Se dispone de mediciones de energía en 4 cuadrantes energía activa/reactiva/aparente – entrante/saliente

[11] Frecuencia y/o distorsión armónica.

3.1.2. Procesamiento de la Información

En el actual modelo de mercado es fundamental disponer en forma oportuna de la mejor información de puntos de medición, debido su impacto en los procesos de liquidación de las transacciones económicas de potencia, energía y servicios complementarios del MEM. La calidad de la información depende de la ubicación de la infraestructura de medición, de las capacidades técnicas de medidores/registradores (precisión, tolerancia a fallos, capacidades de registro) y de los mecanismos de procesamiento de información, que el caso del nuevo sistema de medición comercial contempla un proceso estructurado y secuencial de:

i) *Priorización* de las fuentes de información asociadas a cada punto de medición.

ii) *Chequeos de validez* sobre los registros individuales a fin de identificar que un dato no es válido cuando el registro es inexistente; o, cuando éste tiene asignado con una bandera de nulidad por parte del propio medidor/registrador, en cuyo caso se procede a reemplazarlos con datos de otras fuentes de menor prioridad. Si hasta esta instancia, no se dispone de manera completa los registros de medición, se aplica lo indicado en iii) o iv).

iii) *Estimación de "huecos"* en base a información histórica, siempre que el número de períodos de integración consecutivos sea menor o igual a tres. Los valores estimados estarán dados por la media aritmética para cada una de las magnitudes y período de integración de las medidas correspondientes a los períodos de integración anterior y posterior a la/s de la/s que se dispone de medida.

iv) *Estimación de períodos* (más de 3 registros consecutivos sin medida) en base a un cálculo de la media aritmética (x) y desviación típica(s) de la muestra[12] de energías, despreciando de ésta los valores máximo y mínimo. En el caso de que se repita el valor máximo en las muestras sólo se eliminará para el cálculo de la medida y desviación típica una de ellas. Análogamente, en caso de que se repita el valor mínimo en las muestras sólo se eliminará para el cálculo de la media y desviación típica una de ellas. A continuación se determinan los extremos de distribución de la muestra, suponiendo una distribución normal (muestra máxima = x + 2 * s; muestra mínima = x – 2 * s). El valor de medida estimado para cada uno de los periodos, magnitudes y días vendrá dado por la media aritmética de la muestra total sin despreciar valores máximos y mínimos, utilizando sólo los valores que entren dentro de la distribución normal.

[12] La muestra esta formada por 6 medidas del mismo día tipo (más próximos del mismo mes de la estimación). Son días tipo los días calendario laborable, sábado, domingo o feriados nacionales bajo los lineamientos establecidos en la Codificación del Reglamento de Tarifas Eléctricas.

Al final de este proceso se habrá obtenido una curva de carga de cada punto de medición, con su correspondiente indicador de validez.

3.1.3. Almacenamiento y Recuperación de Información

En una base de datos ORACLE que permite mantener un inventario de toda la infraestructura de medición de MEM (en base a una codificación estándar) y el expediente histórico de todos los registros de puntos de medición.

3.2. SIMEC- Riesgo de Negocio y Productividad

SIMEC se constituye en una iniciativa estratégica del CENACE para el mejoramiento de la productividad, basado en el manejo y control de los riesgos que puede ser evaluado desde 2 puntos de vista:

3.2.1. Comparación entre las Funciones que Pueden Manejar los 2 Sistemas

Parámetros	Sistema Actual	Nuevo SIMEC
Puntos de medida accesibles actualmente	175	175
Puntos de medida a ser administrados	175	315
Crecimiento anual esperado**	28,3%	28,3%
Capacidad de crecimiento		
Tiempo de ejecución de proceso		
- Adquisición de datos*	10	4
- Gestión para adquisición alternativa de información*	2	1
- Validación	--------	1
- Reportes	2	0,5

** Referencia: junio 2004/julio 2005
* El tiempo de ejecución crecerá en la misma proporción que el incremento de puntos de medida (28.3%)

- **Índices de Proceso**

- Tiempo requerido por Sistema Actual: 14 Horas.
- Tiempo requerido por nuevo SIMEC: 6,5 Horas.
- Incremento en confiabilidad y optimización de tiempos en: 39,28%.

3.2.2. Considerando la Nueva Funcionalidad

Parámetros	Sistema Actual	Nuevo SIMEC
Tiempo para auditorias de sistemas de medición	-----	2,5 horas mes
Tiempo para generación de informes mensuales/anuales	-----	0,1 horas c/u
Balances energéticos	-----	Inmediatamente luego del cierre de medidas
Tiempo para publicación de información para Agentes	-----	Inmediatamente luego del cierre de medidas
Tiempo para notificación a Agentes	-----	
Tiempo para envío y recepción de observaciones	-----	Interacción vía web con el Agente
Disponibilidad de información para análisis	-----	100%
Mantenimiento y actualización del sistema	-----	15 horas-mes

4. CONCLUSIONES

a. La globalización y desregulación del negocio eléctrico están empujando a una evolución de la operación y funcionamiento de redes y mercados eléctricos a un entorno de comercio electrónico. Debido a la interoperación y vulnerabilidad mutua de estos segmentos de negocio y la naturaleza social que tienen estos servicios, hace indispensable formular y aplicar modelos de seguridad que le otorguen sostenibilidad y confiabilidad.

b. Proyectos IT alineados con los objetivos de negocio, son iniciativas que permiten a una organización no solo cumplir su misión, sino que también son elementos de control de riesgos que permiten el mejoramiento de la productividad y desempeño de procesos.

c. La administración del riesgo, es parte integral de la gestión moderna de empresas y un componente importante de un programa de seguridad, con un rol crítico para proteger los activos de información de la empresa y por consiguiente apoyar al cumplimiento de su misión, que no está asociado exclusivamente con una responsabilidad a cargo de especialistas, sino con una función administrativa esencial de toda la organización.

d. El SIMEC es una iniciativa de innovación tecnológica única en la región, que tendrá impacto directo en el control de riesgos claves de la organización, en la generación y publicación de mejores productos de información, en la disminución del número de reclamos por parte de los Agentes, en el incremento en la productividad de procesos internos, una óptima supervisión de la infraestructura de medición para la aplicación de auditorias técnicas; así como otros beneficios intangibles relacionados con satisfacción de cliente externo, imagen corporativa y transparencia en la gestión.

5. BIBLIOGRAFÍA

[1] NERC; Security Guidelines for the Electricity Sector, Versión 1.0, June 2002.

[2] NERC; An Approach to Action for the Electricity Sector, Working Group Forum on Critical Infrastructure Protection, Versión 1.0, June 2001.

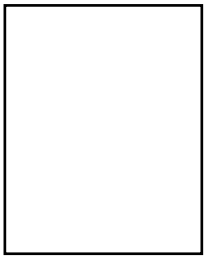
[3] NERC; Security Standards for Electric Market Participants.

[4] MARIANNE Swanson; AMY Wohl; LUCINDA Pope; TIM Grance, JOAN Hash, RAY Thomas; Contingency Planning Guide for Information Technology Systems, Recommendations of the National Institute of Standards and Technology, NIST Special Publication 800-34, June 2002.

[5] NIST, An Introduction to Computer Security: The NIST Handbook, Special Publication 800-12.

[6] SWANSON M.; Security Self-Assessment Guide for Information Technology Systems, NIST Special Publication 800-26, November 2001.

[7] GRANCE T.; HASH J.; PECK S.; SMITH J.; KOROW-Diks; Security Guide for Interconnecting Information Technology Systems, NIST Special Publication 800-47, August 2002.
[8] STONEBURNER G.; HAYDEN C.; FERINGA A.; Engineering Principles for Information Technology Security *(A Baseline for Achieving Security), Revision A.,* NIST Special Publication 800-27 Rev A, June 2004.
[9] STONEBURNER G.; Underlying Technical Models for Information Technology Security, NIST Special Publication 800-33, December 2001.
[10] SWANSON M.; Guide for Developing Security Plans for Information Technology Systems, NIST Special Publication 800-18, December 1988.
[11] SWANSON M.; GUTTMAN B.; Generally Accepted Principles and Practices for Securing Information Technology Systems, NIST, September 1996.
[12] NERC; Securing Remote Access to Electronic Control and Protection Systems, June 2003.
[13] SWANSON M.; BARTOL N.; SABATO J.; HASH J.; GRAFFO L.; Security Metrics Guide for Information Technology Systems, NIST Special Publication 800-55, July 2003.
[14] MARK E.; Information Integrity: La integridad de la Información de su Empresa; SYMANTEC, Enero 2005.
[15] BARKER W.; Guideline for Identifying an Information System as a National Security System, NIST Special Publication 800-59, August 2003.
[16] BARKER W.; Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories, NIST Special Publication 800-60, June 2004.
[17] BURR W.; DODSON D.; Polo T.; Electronic Authentication Guideline, NIST Special Publication 800-63, September 2004.
[18] NERC; Threat Alert System and Cyber Response Quidelines for the Electricity Sector, *October 2002.*
[19] VIZCAINO K.; Índices de Desempeño de Procesos en el Escenario Actual y Futuro del SIMEC, CENACE, Junio 2005.
[20] NINA G.; Perspectivas sobre Riesgo, Taller CENACE, Julio 2005.
[21] La Seguridad en Microsoft, Noviembre 2003.



Germán Pancho Carrera.

Ingeniero en Electrónica y Control otorgado por la Escuela Politécnica Nacional (EPN-1996). Master en Gerencia de Sistemas obtenido en la Escuela Politécnica del Ejército (ESPE-2003). Su actividad profesional se ha enfocado a la docencia universitaria y al desarrollo de proyectos de tecnologías de información. Actualmente ejerce las funciones de Coordinador de Informática y del Proyecto de Complementación del CENACE