VII/CE-D2-05

Análisis de la Seguridad del Sistema SCADA/EMS en la Itaipu Binacional

Alfredo Humberto Fernández Insfrán

Itaipu Binacional

Paraguay / Brasil

RESUMEN

Diversas clases de computadoras son utilizadas en todos los niveles del sistema de potencia y en las operaciones de negocios dentro de la empresa eléctrica. Así son utilizadas en operaciones primarias tales como en los arreglos de los relés de protección, en la operación de plantas de potencia y de redes eléctricas vía SCADA/EMS, en operaciones de mercadeo y/o de negocios, y con propósitos administrativos tales como en editores de texto y planillas de cálculo en computadoras de escritorio.

A lo largo del tiempo estos sistemas han sido introducidos y construidos como islas computacionales separadas. Sin embargo actualmente, estas islas están cada vez más próximas, intercomunicandose o integrandose ya sea en forma parcial o total con otras islas. Este nuevo horizonte de intercomunicabilidad, independiente de los beneficios que genera a nivel económico, operacional y administrativo, presenta problemas serios, en lo relativo a la seguridad e integridad de los datos intercambiados, a la seguridad del sistema computacional que posibilita esta nueva facilidad y finalmente a la seguridad y operabilidad de la propia planta y de la red eléctrica.

En este contexto, el propósito de este articulo es el de presentar primeramente los problemas emergentes en los sistemas computacionales de empresas eléctricas, relacionados a la seguridad de la información. A continuación se presentarán las normas de seguridad aplicadas al caso, y finalmente las medidas adoptadas en la Itaipu Binacional para reducir o evitar los riesgos de seguridad introducidos con la implantación de los sistemas computacionales de apoyo a la operación.

PALABRAS-CLAVES

Seguridad Cibernética, Sistemas de Control, Sistemas Abiertos, Amenaza Digital, Auditoria de la Información, Vulnerabilidad Informática

1.0 – INTRODUCCIÓN

Debido a la falta de normas y procedimientos generalmente aceptados, los nuevos sistemas digitales, se han vuelto, por utilizar productos de mercado y *softwares* no propietarios, cada vez más vulnerables a ataques de amenazas digitales, tales como los *hackers/crackers*, virus y *malwares*. Así, es una cultura generalizada entre estos, de que si se consigue el IP de una máquina, entonces es posible atacarla.

En el inicio los Sistemas de Control eran "Islas Tecnológicas Seguras", con procesadores industriales específicos, sistemas operacionales propietarios en tiempo real, con Aplicaciones individuales de *hardware* y de *software*, en redes industriales deterministicas, generando informes especiales, *customizados* al cliente.

Posteriormente, en una evolución natural de los sistemas, se utilizaron tanto el *MS Windows* ® como el *Unix* en las *workstations* de los sistemas de operación, basados en *hardware* de mercado que ya no eran propietarios, y utilizando los padrones *Ethernet* y *TCP/IP* en redes compuestas de componentes de aplicación comercial, abriendo aquí los primeros puntos de vulnerabilidad.

Finalmente, las exigencias de integración con los aplicativos gerenciales de las redes corporativas y a su vez éstas abiertas al mundo a través de la conexión *Internet*, han convertido a los Sistemas de Control en sistemas abiertos perdiendo su característica de "Islas Seguras".

Esta situación obliga entonces a responder a la pregunta: ¿Puede existir un sistemas con dichas dos condiciones?, es decir ¿Puede ser el sistema abierto y al mismo tiempo seguro?.

2.0 - DESCRIPCIÓN DEL PROBLEMA

De acuerdo a publicaciones del *Briítos Columbia Institute of Technology*, de 1982 a 1999, el 70% de los incidentes de violación de los Sistemas de Automatización, han sido de origen interno. Luego del 2000 y más específicamente en las investigaciones concluidas en 2003 esta tendencia se ha invertido, dando como resultado que el 70% de los problemas (ataques) se han vuelto de origen externo. Los siguientes son hechos históricos:

- En el año 2001, en Queenisland (Australia), millones de litros de desagüe de cloaca han sido vertidos en parques y ríos debido a un ataque planificado por un proveedor descontento por haber perdido su empresa un concurso de precios.

- Durante los años de 2001 y 2002, un joven invadió el servidor del puerto de Houston (Texas) para tener acceso a la página de una funcionaria, congestionando varias veces a los servidores internos, desconectando el sistema de programación de carga y descarga de buques, que era fundamental para la operación.

- En enero de 2003, *hackers* crearon el *Slammer Worm*, introdujeron este virus en la red de la planta nuclear de Davis Besse y deshabilitaron el sistema de monitoreo de seguridad por cerca de 5 horas, mismo con el *firewall* instalado, utilizando una conexión no protegida entre la red de automatización y la red corporativa. En esa

misma época algunas plantas de los EUA perdieron sus interfaces hombre/máquina y sus historiadores a causa del mismo virus.

Estos ejemplos muestran la gravedad de los ataques informáticos a los activos empresariales, exigiendo por lo tanto un tratamiento especial.

3.0 – NORMAS DE SEGURIDAD DIGITAL

En la actualidad existen dos normas aplicables a la seguridad de los sistemas informáticos: la norma ISA 99 y la norma ISO 17799 [6]. Presentamos a seguir una breve descripción de estas normas.

3.1 – La Norma ISA 99

La norma ISA 99 publicada en 2003, es una norma que trata de la seguridad de la información en los sistemas de manufactura y control. El comité SP99, redactor de esta norma, fue constituido en Octubre de 2002 y cuenta actualmente con 260 miembros que actúan en mas de 220 empresas. La Figura 1 muestra la estructura de esta norma.

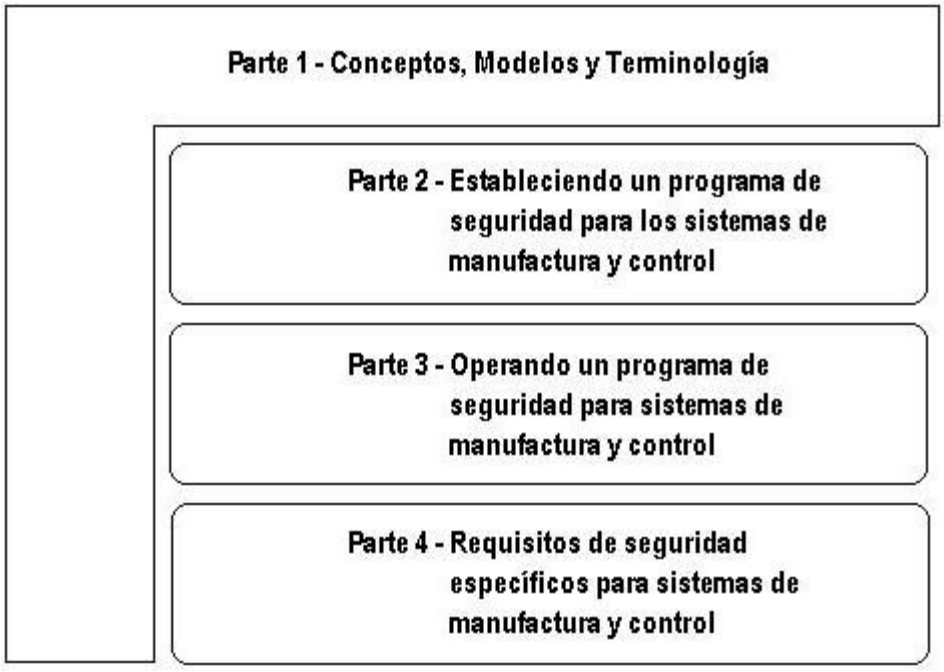

FIGURA 1 – ESTRUCTURA DE LA NORMA ISA 99

Dentro de esta norma se han publicado dos informes:

- ISA TR99.00.01 – *Tecnologías de Seguridad para los Sistemas de Manufactura y Control* [1].
- ISA TR99.00.02 – *Integrando la Seguridad Electrónica en ambientes de Sistemas de Manufactura y Control* [2].

Dos módulos ya han sido publicados:

- ISA S99.00.01 – *Modelos, Definiciones y Terminología* [3].
- ISA S99.00.02 – *Estableciendo un programa de Seguridad para los Sistemas de Manufactura y Control* [4].

Dos módulos se encuentran en estudio:

- ISA S99.00.03 – *Operando un programa de seguridad para Sistemas de Manufactura y Control*.
- ISA S99.00.04 – *Requisitos de seguridad específicos para Sistemas de Manufactura y Control*.

El primer informe, TR99. 00.01 - *Tecnologías de Seguridad para los Sistemas de Manufactura y Control* describe las principales tecnologías de seguridad existentes hoy en día y sus respectivas debilidades. Para cada una de ellas presenta recomendaciones sobre su utilización en los sistemas de automatización [5]. Seis grupos de tecnología son analizados:

- Autorización y Autenticación: determina quien puede usar el sistema e identificar al usuario.
- Filtro, bloqueo y control de acceso: *firewall's*, *VLANS's*, etc.
- Criptografia y Validación: criptografia de llaves simétricas y públicas, *VPN's*, etc.
- Herramientas de Auditoria, Medición, Monitoreo y Detección: sistemas de detección de virus, detección de intrusión, log/auditoria de eventos, herramientas de investigación forense.
- Software en general: sistemas operativos, sistemas aplicativos, servidores Web, etc.
- Seguridad Física: identificación, monitoreo, y limitación de acceso a través de tarjetas de identificación, cámaras, puertas especiales, y seguridad del personal que van desde políticas de admisión hasta la elaboración de contratos especiales especificando las obligaciones y comportamientos esperados de los empleados.

El segundo informe, TR99.00.02 – *Integrando la Seguridad Electrónica en ambientes de Sistemas de Manufactura y Control*, contiene orientaciones relativas a las políticas generales, criterios, objetivos, padrones y requisitos necesarios para que los objetivos de seguridad sean alcanzados. Es una metodología para el análisis de riesgo, no enseñando a resolver los problemas mas sí a encuadrarlos, considerando que las amenazas y las vulnerabilidades cambian constantemente.

El módulo S99.00.01 – *Modelos, Definiciones y Terminología*, tiene por objetivo proporcionar definiciones comunes que serán utilizadas en otras partes de la norma. Este documento comienza con un diccionario de términos relacionados con la seguridad, el cual es seguido por un glosario de acrónimos que representa casi el 25% del contenido del documento.

El capitulo 5 de esta norma presenta los conceptos de seguridad para los Sistemas de Manufactura y Control. El modelo de contexto (Figura 2) ha sido prestado de la norma ISO/IEC 15408 y explica los activos que están sometidos a amenazas, que a su vez son producidos por los agentes de amenaza. Las amenazas alimentan el riesgo de los activos atacando sus vulnerabilidades. Cada activo posee un propietario que irá a minimizar su riesgo aplicando contra medidas.

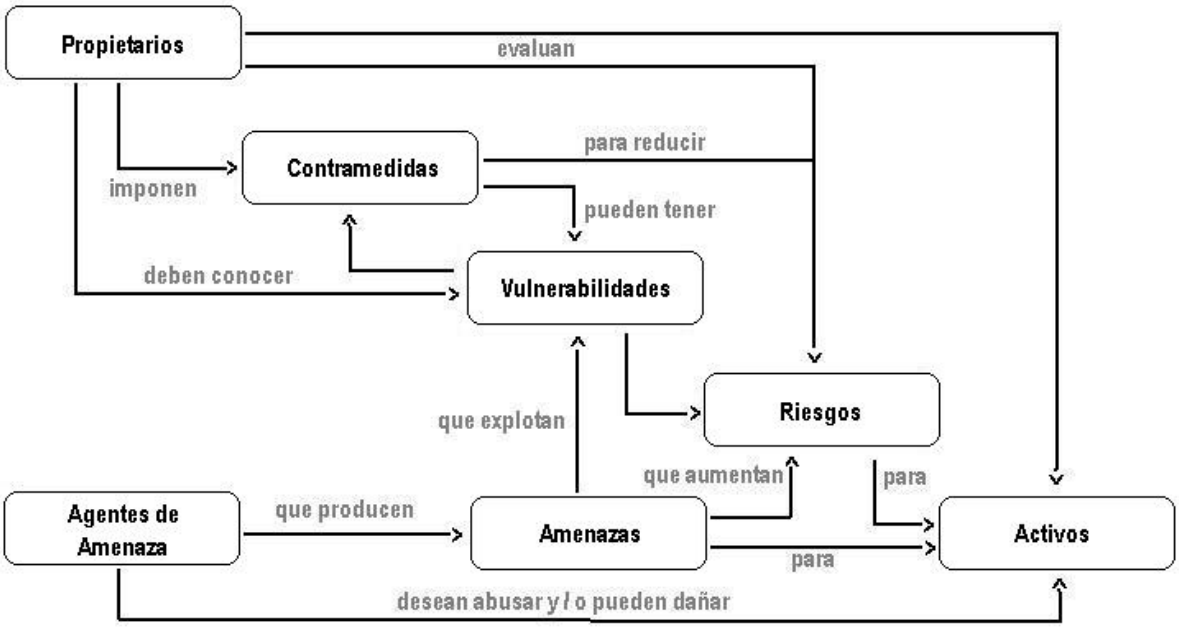

FIGURA 2 – MODELO DE CONTEXTO

Los activos a su vez han sido representados por diversos sub. modelos agrupados en cinco clases, de forma a evaluar los riesgos. Estos sub. modelos son: modelo de referencia, modelo físico, modelo lógico, modelo funcional y modelo conceptual.

Entre los cuatro documentos emitidos por el comité SP99, el módulo S99.00.02 – *Estableciendo un programa de Seguridad para los Sistemas de Manufactura y Control*, es el de mayor impacto pues establece un programa de seguridad que puede servir de base para la implantación de programas reales.

El punto mas importante de este módulo es el de suministrar una metodología basada en PDCA(*Plan/Do/Check/act.* - Planifica/Ejecuta/Verifica/Actúa), buscando desarrollar un programa de seguridad para un Sistema d Manufactura y Control especifico. El objetivo final es el de construir un Sistema de Gerenciamiento de Seguridad de Información conocido como *CSMS – Cyber Security Management System*.

3.2 – La Norma ISO 17799

La norma ISO 17799 trata específicamente de la seguridad de la TI, sin ocuparse de la seguridad de los sistemas de control. Su alcance no se sobrepone con la norma ISA 99, siendo complementaria a esta (Figura 3). Esta norma ha sido originada a partir de la norma BS 99 abarcando los siguientes puntos:

- Política de seguridad: política de seguridad de la información.
- Organización de la seguridad: infraestructura de la seguridad de la información y seguridad de acceso.
- Control y clasificación del patrimonio: contabilización del patrimonio y clasificación de las informaciones.

- Seguridad relacionada a las personas: seguridad en la definición de los trabajos y los recursos, adiestramiento de usuarios, atención a incidentes de seguridad y funcionamiento inadecuado.
- Seguridad física y de infraestructura: áreas seguras, seguridad de equipos y controles en general.
- Comunicación y gerenciamento de operaciones: procedimientos y responsabilidades operacionales, planificación y aceptación de sistemas, protección contra softwares nocivos, gerenciamento de la red, seguridad y almacenamiento de datos y documentación en medios magnéticos, intercambio de informaciones y de softwares.
- Control de acceso: requisitos para el control de acceso, gerenciamento del acceso del usuario, control del acceso a la red, control de acceso al sistema operacional, control de acceso a los aplicativos, monitoreo del uso y del acceso al sistema.
- Mantenimiento y desarrollo de sistemas: requisitos de seguridad de los sistemas, seguridad en los sistemas aplicativos, controles criptograficos, seguridad de archivos del sistema, seguridad en el desarrollo y soporte de los procesos.
- Gerenciamento de la continuidad de producción: aspectos de la continuidad de producción.
- Atención a los requisitos legales: revisión de políticas de seguridad y de atención técnica, consideraciones sobre sistemas de auditoria.

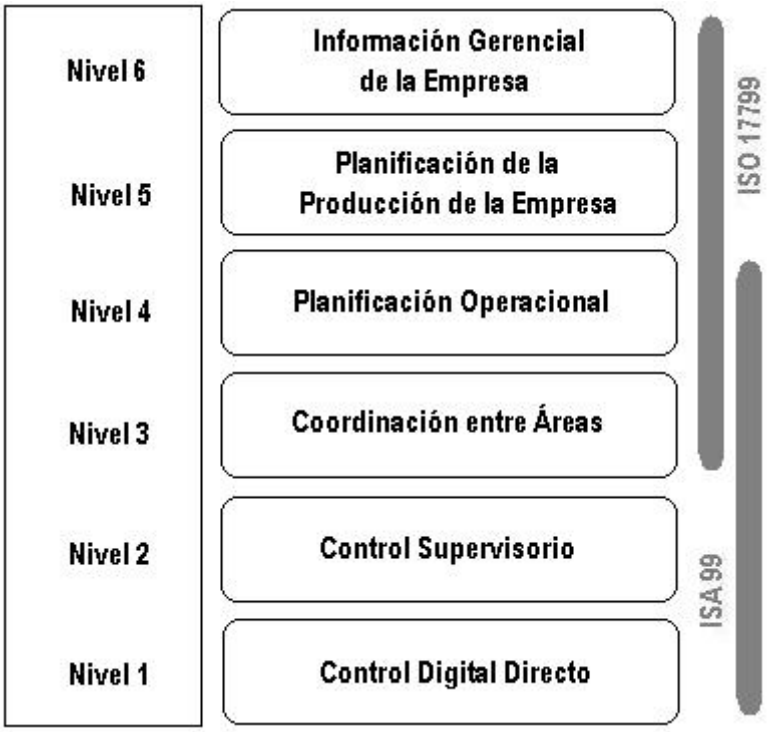

FIGURA 3 – ALCANCES DE LAS NORMAS ISA 99 E ISO 17799

Esta norma, a igualdad de la norma ISA 99, permite la implantación de un sistema de gestión de seguridad de la información basado en controles y prácticas definidos internacionalmente.

4.0 - EL CASO ITAIPU

La seguridad del Sistema Digital de Itaipu ha sido desde el inicio de su implantación un motivo de preocupación. Este hecho se ha visto reflejado en los documentos generados para especificar el alcance del suministro con el proveedor, requisitos que han sido verificados cuidadosamente durante la etapa de ensayos en fábrica.

Posteriormente, ya durante la etapa de implantación en obra, se ha realizado un análisis exhaustivo de vulnerabilidad, de acuerdo a los procedimientos indicados en las normas ISA 99 e ISO 17799. La Tabla 1 a seguir muestra el análisis realizado.

TABLA I – ANÁLISIS DE VULNERABILIDAD

	ITEM	**Analizado**	**Nuevas Recomendaciones/ Acciones**
1	Ambiente e Infraestructura		
	Protección Física de edificios, puertas, etc.	SI	NO
2	Hardware		
	Almacenamiento de Copias de Seguridad	SI	NO
3	Software		
	Gerenciamento de Señas	SI	SI
	Procedimientos de Login y de Logout	SI	SI
	Ejecución de Copias de Seguridad	SI	NO
4	Comunicaciones		
	Interfaces con otros Sistemas	SI	SI
	Seguridad de la Red	SI	SI
5	Documentación	-	No Aplicable en el Momento
6	Asociada a Personas	-	No Aplicable en el Momento
7	Otras Vulnerabilidades		
	Aspectos de Proyecto	SI	NO

Las recomendaciones generadas en este análisis han sido implementadas en el año 2004, en forma coincidente con el inicio de la operación comercial del sistema SCADA/EMS de Itaipu.

5.0 – CONCLUSIONES

Actualmente nos encontramos frente a una automatización que se ha aproximado mucho a los sistemas gerenciales y de información. Esto exige de los técnicos del área no solamente los conocimientos relativos al control y al proceso, mas también de técnicas y procedimientos que pertenecen a otros grupos. Así, el ataque digital es un hecho concreto y además de no ignorarlo, es función de la empresa proteger sus activos de tales ataques.

El CSMS o Sistema de Gerenciamiento de la Seguridad de la Información es una nueva palabra que puede volverse cada día mas común en el vocabulario de los ingenieros de automatización. Así todos los fabricantes de equipos y sistemas de automatización deben investigar, analizar y discutir las vulnerabilidades de los sistemas que fabrican, de forma a mitigar los riesgos del usuario.

Este es un proceso permanente en donde el aprendizado y el ecuacionamiento de los problemas debe ser continuo, a través de una metodología que evalúe el riesgo existente y sus consecuencias para la organización y determine la mejor estrategia para mantenerla bajo control.

En este contexto en la Itaipu Binacional:

- la seguridad del sistema SCADA/EMS ha sido evaluada desde la fase de proyecto e implantación.
- han sido aplicados procedimientos de seguridad de datos, red y acceso a los usuarios.
- han sido utilizadas las facilidades padrones existentes en el sistema para garantizar la seguridad.
- los procedimientos y facilidades están siendo re evaluados continuamente en las acciones propuestas.
- nuevas normas internacionales a ser divulgadas en el futuro, serán introducidas para minimizar el impacto de un eventual ataque.

6.0 - BIBLIOGRAFÍA:

[1] – ISA TR99.00.01 – Technical Report – Security Technologies for Manufacturing and Control Systems

[2] – ISA TR99.00.02 – Integrating Electronic Security into the Manufacturing and Control Systems Environment

[3] – ISA S99.00.01 – Manufacturing and Control Systems Security – Part 1: Concepts, Models and Terminology

[4] – ISA S99.00.02 - Manufacturing and Control Systems Security – Part 2: Establishing a Manufacturing and Control System Security Program

[5] – SEIXAS F., Constantino, Tutorial ISA S99 – InTech Nº. 71, Abril 2005, pág. 14-18

[6] – ISO IEC 17799 – Information Security Standards