GESTIÓN DE SEGURIDAD DE LA INFORMACION EN SISTEMAS DE CONTROL INDUSTRIAL SCADA

Julián Duarte Suarez atosnanos2480@hotmail.com
Nelson Andres Arbeláez Jiménez nelsonarbelaez@hotmail.com
Universidad Piloto de Colombia

Resumen— *La implementación de un Sistema de Gestión de Seguridad de la información, permite establecer procedimientos fundamentados en principios sólidos como lo son la confidencialidad, la integridad y la disponibilidad pilares esenciales para los procesos propios de los sistemas de control industrial.*

Actualmente los sistemas de control industrial son susceptibles al robo de información critica e inclusive al daño de la infraestructura encargada de la gestión del sistema, lo cual puede llegar a impactar desde las finanzas hasta la imagen corporativa de la compañía, razón por la cual surge la necesidad de la implementación de mejores prácticas que permitan establecer procesos de aseguramiento que faciliten el cumplimiento de los objetivos de la organización.

La identificación de las necesidades, el diagnostico y la implementación y seguimiento de los procesos serán parte de la adopción y formación de un ambiente ideal y seguro que establecerá procedimientos y conductas que aseguren el adecuado tratamiento de la Gestión de la Información en los Sistemas de Control Industrial.

Palabras clave—Gestión de la Información, Sistemas de control, SCADA, mejores prácticas, caracterización, proceso, divulgación y concientización.

Índice de Términos

Sistemas de Control: Los sistemas de control están formados por un conjunto de dispositivos de diversa naturaleza (mecánicos, eléctricos, electrónicos, neumáticos, hidráulicos) cuya finalidad es controlar el funcionamiento de una máquina o de un proceso.

SCADA: Supervisory Control And Data Acquisition. Un sistema SCADA está basado en computadores que permiten supervisar y controlar a distancia una instalación, proceso o sistema de características variadas.

Divulgación: difundir, promover o publicar algo para ponerlo al alcance del público.

Concientización: todo aquello acto que signifique hacer que una persona tome conciencia sobre determinas circunstancias, fenómenos, elementos de su personalidad o actitud, para mejorar su calidad de vida y sus vínculos no sólo con el resto de los individuos si no también con el medio ambiente que lo rodea.

I. INTRODUCTION

La gestión de seguridad de la información en los sistemas de control industrial SCADA, ofrecen un alto índice de aseguramiento dirigido a la optimización de las operaciones de la compañía, garantizando un alto redimiendo.

Los sistemas de control industrial SCADA han sido vulnerados y expuestos a tipos de malware o virus que ponen en riesgo la información que se transmite y almacena a través de sus redes, este tipo de intrusión compromete el buen nombre de grandes organizaciones a nivel nacional.

Razón por la cual es importante que las industrias adquieran buenas prácticas de Gestión de la Información, que se creen campañas de concientización dirigidas a todos los integrantes de las compañías que permitan mitigar el riesgo de cualquier tipo de intrusión, manteniendo la información y la continuidad de los servicios tecnológicos que mal empleados podrían a carrear pérdidas económicas o del good will de la empresa.

II. METODOLOGIA

Actualmente a los sistemas de seguridad de la información no se le da el reconocimiento ni la importancia requerida tanto a nivel corporativo como gerencial, teniendo en cuenta que a través de esta se emana la mayoría de sus procesos necesarios para el buen desarrollo de sus compañías.

Así mismo nos encontramos frente a un gran vacío normativo, teniendo en cuenta que no existe norma alguna aplicable en seguridad de la información a los sistemas de control industrial SCADA; Razón por la cual surge la necesidad de implementar mejores prácticas, enfocadas a la gestión de seguridad de la información en los sistemas de control industrial.

Contribuyendo de este modo al aseguramiento de sus datos evitando el robo o pérdida de la misma, ofreciendo así un cumplimiento de manera oportuna en la preservación de los tres pilares de seguridad como lo son la confidencialidad, la integridad y la disponibilidad, obteniendo un sistema de control SCADA más seguro y así evitando ser víctima de ataques cibernéticos como:

- Slamer,
- Stuxnet
- Flame
- Duqu
- Shamoon

Que solo resultan ser un pequeño ejemplo entre los que actualmente se están propagando alrededor del mundo y los cuales se presentan como un riesgo latente pues en cualquier momento se puede ser infectado por cualquier tipo de virus o malware que generaría impacto en la disponibilidad de los sistemas de control SCADA, que al materializarse podría causar pérdidas económicas, del medio ambiente y humanas, dada la importancia y la criticidad de estos sistemas en los procesos industriales.

Ante estos aspectos la ejecución de un plan de Gestión de seguridad de la información debe apoyar los objetivos estratégicos de la organización, dándole un enfoque de inversión y no de gasto.

En el mercado actual existen estándares, metodologías y marcos de referencia que involucran la Gestión de Seguridad de la Información, y muestran la importancia de la misma sin embargo siempre surge un gran cuestionamiento:

¿Cómo garantizar el aprendizaje y el estudio de mejores prácticas en Gestión de Seguridad de la información en sistemas de control Industrial SCADA?

III. OBJETIVO

El objetivo general de acuerdo a la necesidad identificada en diversas organizaciones, es garantizar el aprendizaje y la implementación del uso de mejores prácticas para la gestión de la información en los sistemas de control industrial SCADA.

Para lograr esto es necesario realizar actividades adicionales como definir y establecer lineamientos en Seguridad de la Información que garanticen la protección de los Sistemas de Control industrial SCADA, asegurando de esta manera la disponibilidad, confidencialidad e integridad de los mismos.

Para lo anterior expuesto, se ha hecho necesario el planteamiento de algunos objetivos específicos los cuales permitirían alcanzar un alto porcentaje del desarrollo propuesto:

- Elaboración y ejecución de procedimientos.
- Delegación de responsables.
- Procesos de formación que permitan establecer lineamientos que establezcan responsabilidades y conductas para asegurar el adecuado tratamiento de la Gestión de la Información.

IV. ANTECEDENTES

En el mundo ya es normal encontrar que las empresas se están alineando a la tecnología de punta, implementando en ellas sistemas de control industrial SCADA el cual le da mayor beneficio en la simplificación de la gestión de procesos y mejora de su eficiencia.

Los sistemas de control industrial es una herramienta fundamental para controlar los procesos de producción y distribución, ya que a través de estos se hace seguimiento remoto y en tiempo real de sus operaciones, sin embargo estos sistemas no se encuentran exentos de ataques informáticos los cuales están encaminados principalmente al robo de información critica y al daño de la infraestructura que controla y gestiona estos sistemas, lo cual podría acarrear impactos sobre las finanzas, el medio ambiente, la imagen corporativa de la compañía e incluso la integridad de las personas.

Dada la complejidad e importancia de la información que se manejan a través de los sistemas de control industrial SCADA para la organización, nace la necesidad de la implementación de mejores prácticas y sus diferentes ítem con sus respectivos procedimientos, ajustado a las necesidades de un sistema seguro en el cual se establezcan políticas de seguridad de la información y sensibilización en cuanto a su activo más importante de información.

V. SISTEMAS DE CONTROL INDUSTRIAL

Son sistemas informáticos que poseen una infraestructura tecnológica robusta la cual permite recibir información y actuar remotamente sobre el mismo, estos procesos pueden ser industriales, por ejemplo la fabricación de algún producto, la atención de servicios de primera necesidad a los ciudadanos como el suministro de electricidad, agua y gas, también se utilizan en refinerías, industrias petroquímicas e industrias relacionadas con alta producción y transformación de recursos naturales, los cuales tienen que manejar un número elevado de variables de control para su operación.

VI. GESTIÓN DE SEGURIDAD Y MEJORES PRÁCTICAS

- ACTIVOS DE INFORMACION PARA SISTEMAS DE CONTROL INDUSTRIAL

Actualmente las organizaciones operan en entornos dinámicos y están en la necesidad de conocer y adaptarse a las necesidades de sus clientes, es por esta razón que cada área de negocio que utilice Sistemas de Control Industrial será responsable de efectuar las siguientes actividades para garantizar la protección sobre sus activos de información, teniendo en cuenta una identificación, un inventario y la asignación de un responsable.

- ROLES Y RESPONSABILIDADES EN SISTEMAS DE CONTROL INDUSTRIAL

Las mejores prácticas son actividades o procesos que más de una organización ha usado con éxito, son acciones que han dado buen rendimiento y excelentes respuestas como tener en cuenta qué cada área que administre Sistemas de Control Industrial será la encargada de establecer los roles y responsabilidades con respecto a la seguridad de la información de los funcionarios y contratistas que realicen tareas de índole administrativa y operativa en estos sistemas, garantizando que ninguno de los roles tenga bajo su responsabilidad actividades de autorización y ejecución dentro de un mismo proceso (Segregación de funciones).

- PLAN DE CONTINUIDAD DEL NEGOCIO

Las áreas de negocio que cuenten con Sistemas de Control Industrial deben desarrollar planes de continuidad que les permitan mantener la disponibilidad de sus operaciones o procesos en caso de contingencia. Estas actividades deben ser lideradas por el grupo de continuidad designado por la Compañía y deben tener en cuenta las siguientes actividades:

Análisis de Impacto al Negocio:

- Evaluar los impactos que podrían ocurrir si la actividad se ve interrumpida.

- Establecer el máximo tiempo tolerable de interrupción de cada actividad.
- Identificar actividades interdependientes, activos, infraestructura o recursos que tienen que ser mantenidos continuamente o recuperados a tiempo.
- Identificar las actividades críticas.
- Determinar los requerimientos de continuidad (personas, instalaciones, tecnología, información, etc.)
- Evaluar las amenazas para actividades críticas (evaluación de riesgos).
- Definir las estrategias de continuidad.
- Desarrollar e implementar el plan.
- Probar, mantener y revisar el plan.

- CONTROL DE ACCESO EN LOS SISTEMAS DE CONTROL INDUSTRIAL

Con el objeto de asegurar que únicamente los usuarios autorizados tengan acceso a los Sistemas de Control Industrial, cada área de negocio debe contemplar como mínimo la implementación de los siguientes controles:

- Gestión de Usuarios
- Elaborar un instructivo formal para la creación, modificación, bloqueo y eliminación de Usuarios en los Sistemas de Control Industrial.
- Establecer un único identificador por usuario (id) en los Sistemas de Control Industrial, en casos puntuales donde el negocio requiera identificadores de grupo (usuarios genéricos), deben estar aprobados por el funcionario autorizado.
- Administración de Privilegios
- Elaborar un instructivo formal para la asignación de privilegios a los Usuarios del Sistema de Control Industrial.
- Asignar y revisar periódicamente los permisos al Usuario teniendo en cuenta el "principio de menores privilegios".
- Administración de Contraseñas
- Control de Acceso
- Seguridad en sistemas y/o Software

- IMPLEMENTACION Y MANTENIMIENTO DE LOS SISTEMAS DE CONTROL INDUSTRIAL

Para cada área de negocio que utilice Sistemas de Control Industrial, se debe elaborar un instructivo de administración de cambios para la implementación y/o mantenimiento de los activos de información, teniendo como base las buenas prácticas del estándar Cobit del proceso AI6 (Administrar Cambios), con las siguientes actividades generales:

- Definir proceso para analizar y registrar el cambio.
- Evaluar el impacto y priorizar el cambio.
- Autorizar o rechazar el cambio.
- Ejecutar el cambio.
- Cerrar el cambio.

- GESTION DE INCIDENTES DE SEGURIDAD DE LOS SISTEMAS DE CONTROL INDUSTRIAL

Dada la importancia en que un incidente se puede convertir en un accidente se debe establecer que cada área de negocio que utilice Sistemas de Control Industrial, debe elaborar un instructivo para la gestión de los incidentes de seguridad que ocurran en sus activos de información, para que sean notificados a un nivel apropiado, sean reportados adecuadamente e investigados y analizados por personal competente para:

- Salvaguardar el negocio.
- Prevenir la recurrencia y eliminar defectos
- Identificar y eliminar las causas potenciales de los incidentes.
- Mantener un registro que facilite el proceso de mejoramiento.

- CARACTERIZACIÓN DE UN PROCESO

La caracterización de un proceso es donde se identifican todos los factores que de una u otra manera que interviene en un proceso y que se deben controlar. Durante la caracterización todas las partes interesadas participan de las actividades y así se obtiene una visión integral o general del proceso, se despejan dudas, se aclaran conceptos y se entiende cual es la función de cada uno, favoreciendo la calidad de los productos y los servicios.

El enfoque a procesos en la Gestión de seguridad de la Información tiene como objetivo fundamental el desarrollar, implementar y mejorar la eficacia para aumentar la satisfacción de la organización, permitiendo el control de forma continúa de los puntos de interrelación entre los procesos individuales relacionados dentro del Sistema. Se incluyen las combinaciones e interacciones necesarias en sus operaciones, así como involucra a todos en la Organización, constituyendo una necesidad real en para una mejora continua.

VII. CONCLUSIONES

- Como resultado de las etapas anteriores es necesario desarrollar e implementar un modelo de Gestión de Seguridad de la Información, en el que se describan los elementos fundamentales que debe contener el proceso y se detalle de forma analítica las razones que justifican la definición del mismo.

- La implementación de un modelo de seguridad de la información y las buenas prácticas reduce el riesgo de posibles pérdidas económicas y el buen nombre de la compañía.

- A pesar que las compañías actualmente invierten en mejoras su infraestructura tecnológica y en sistemas de gestión de la información falta una cultura organizacional se debe crear una conciencia de la importancia de los activos de la organización.

REFERENCIAS

[1] COBIT 4.1 - Control Objectives for Information and related Technology, IT Governance Institute. Estados Unidos: ISACA, 2007. 196 p.
[2] ISO/IEC 27001:2005, Information Security Management System.
[3] ISO/IEC 27002:2005, Information Security Management – Code of Practice.
[4] http://isa99.isa.org/ISA99%20Wiki/Home.aspx
[5] http://www.inteco.es/blogs/post/Seguridad/Blog Seguridad/Articulo_y_comentarios/SCADA
[6] http://www.seinhe.com/noticias/62-flame-nuevo-virus-identificado-contra-sistemas-scada
[7]
[8] http://gobernabilidadseguridadinformacion.blogspot.com/
[9] http://www.iso27000.es/iso27000.html
[10] https://www.us-cert.gov/

VIII. PERFIL DE LOS AUTORES

- Carlos Julian Duarte Suarez, recibió el título de Ingeniero de Sistemas de la Universidad Autónoma de Colombia 2007. Actualmente cursa una Especialización en Seguridad Informática en la Universidad Piloto de Colombia. Trabaja en la Empresa Consultoría de Seguridad Informática, Su área de interés es Sistemas de Gestión de Seguridad de la Información. e-mail: atosnanos2480@gmail.com.

Nelson Andres Arbeláez Jimenez ingeniero electrónico y de telecomunicaciones experto en soluciones de seguridad informática enfocadas en seguridad web y correo electrónico.

Trabaja en ETB para la vicepresidencia Empresarial y Gobierno. Gerente de Cuenta Grandes Cliente Gobierno. Áreas de interés sector gobierno y sistemas de gestión de seguridad de la información.