GUÍA DE SEGURIDAD DE LAS TIC (CCN-STIC-480E)

SEGURIDAD EN EL CONTROL DE PROCESOS Y SCADA

Guía 4
Mejorar la concienciación y las habilidades

ENERO 2010

Edita:

NIPO: 076-10-072-4

Tirada: 1000 ejemplares
Fecha de Edición: enero de 2010

LIMITACIÓN ORIGINAL DE RESPONSABILIDAD

Esta guía está diseñada para difundir y garantizar las buenas prácticas en la protección de sistemas de control industrial, tales como: control de procesos, automatización industrial, sistemas de control distribuido (SCD) y Control Supervisor y Adquisición de Datos (SCADA). Estos sistemas se utilizan ampliamente en todo el panorama nacional. El documento proporciona valiosos consejos sobre la protección de estos sistemas de ataques electrónicos y ha sido producido por PA Consulting Group para CPNI.

La referencia a cualquier producto comercial, proceso o servicio específico con nombre comercial, marca fabricante, o de otro modo, no constituye ni implica su respaldo, recomendación o favor por CPNI o PA Consulting Group. Los puntos de vista y las opiniones de los autores expresadas en este documento no se utilizarán para fines publicitarios ni de respaldo.

CPNI y PA Consulting Group no aceptarán la responsabilidad de cualquier error u omisión contenida en este documento. En particular, CPNI y PA Consulting Group no se hacen responsables de cualquier pérdida o daño alguno, derivados de la utilización de la información contenida en este documento.

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el **Centro Criptológico Nacional** puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

La referencia a cualquier producto comercial específico, proceso o servicio con nombre comercial, marca fabricante, o de otro modo, no constituye ni implica su respaldo comercial. Los puntos de vista y las opiniones de los autores expresadas en este documento no se utilizarán para fines publicitarios ni de respaldo.

AVISO LEGAL

PRÓLOGO

El uso masivo de las tecnologías de la información y las telecomunicaciones (TIC), en todos los ámbitos de la sociedad, ha creado un nuevo espacio, el ciberespacio, donde se producirán conflictos y agresiones, y donde existen ciberamenazas que atentarán contra la seguridad nacional, el estado de derecho, la prosperidad económica, el estado de bienestar y el normal funcionamiento de la sociedad y de las administraciones públicas.
La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información en su artículo 4.e), y de protección de la información clasificada en su artículo 4.f), a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional en su artículo 9.2.f).

Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través de su Centro Criptológico Nacional, regulado por el Real Decreto 421/2004, de 12 de marzo, diversas actividades directamente relacionadas con la seguridad de las TIC, orientadas a la formación de personal experto, a la aplicación de políticas y procedimientos de seguridad, y al empleo de tecnologías de seguridad adecuadas.

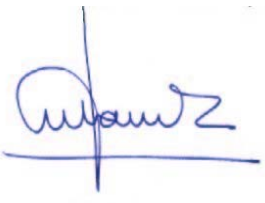
Una de las funciones más destacables del Centro Criptológico Nacional es la de elaborar y difundir normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los sistemas de las tecnologías de la información y las comunicaciones de la Administración, materializada en la existencia de la serie de documentos CCN-STIC.

Disponer de un marco de referencia que establezca las condiciones necesarias de confianza en el uso de los medios electrónicos es, además, uno de los principios que establece la ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos, en su artículo 42.2 sobre el Esquema Nacional de Seguridad (ENS).

Precisamente el Real Decreto 3/2010 de 8 de Enero de desarrollo del Esquema Nacional de Seguridad fija los principios básicos y requisitos mínimos así como las medidas de protección a implantar en los sistemas de la Administración, y promueve la elaboración y difusión de guías de seguridad de las tecnologías de la información y las comunicaciones por parte de CCN para facilitar un mejor cumplimiento de dichos requisitos mínimos.

En definitiva, la serie de documentos CCN-STIC se elabora para dar cumplimiento a los cometidos del Centro Criptológico Nacional y a lo reflejado en el Esquema Nacional de Seguridad, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo su difícil, y en ocasiones, ingrata tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Febrero de 2010



Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

ÍNDICE

ANEXOS

FIGURAS

0. INTRODUCCIÓN A LA TRADUCCIÓN

0.1. ALCANCE DE ESTA TRADUCCIÓN

1. Como parte del acuerdo de colaboración entre el Centro para la Protección de la Infraestructura Nacional de Reino Unido (CPNI en adelante) y el Centro Criptológico Nacional de España (CCN en adelante), se han traducido la colección de guías "Process Control and SCADA Security" publicadas por el CPNI. La presente traducción se corresponde con la versión 2 de las guías del CPNI, publicadas en Junio de 2008, y que consta de las siguientes guías:
   - 00752 - Process Control and SCADA Security
   - 00753 - Process Control and SCADA Security Guide 1. Understand the business risk
   - 00754 - Process Control and SCADA Security Guide 2. Implement secure architecture
   - 00755 - Process Control and SCADA Security Guide 3. Establish response capabilities
   - 00756 - Process Control and SCADA Security Guide 4. Improve awareness and skills
   - 00757 - Process Control and SCADA Security Guide 5. Manage third party risk
   - 00758 - Process Control and SCADA Security Guide 6. Engage projects
   - 00759 - Process Control and SCADA Security Guide 7. Establish ongoing governance
2. En el momento de publicación de esta traducción, las guías originales pueden encontrarse en http://www.cpni.gov.uk/WhatsNew/scada.aspx.
3. Este documento traduce la siguiente guía:
   - 00756 - Process Control and SCADA Security Guide 4. Improve awareness and skills
4. El CCN ha publicado la guía CCN-STIC-480 "Seguridad en sistemas SCADA" que, junto con el resto de guías publicadas y utilizando estas traducciones adapta la seguridad al contexto de España.
5. El CCN se adhiere a la cláusula de responsabilidad del CPNI sobre el contenido de la presente guía.

0.2. CAMBIOS EN EL CONTENIDO

6. Por coherencia con el resto de guías CCN-STIC, se han añadido la portada, la Limitación de Responsabilidad y el Prólogo el presente capítulo 0 de introducción.
7. Se ha traducido de todos los apartados desde el 1 hasta el final, incluyendo la Cláusula Original de Exención de Responsabilidad y los Agradecimientos. Se respeta el contenido original, con las siguientes salvedades:
   - Cuando una traducción requiere una explicación, (ej., cuando el conocimiento de los términos del documento original pueda suponer algún matiz), se incluyen notas a pie

de página, precedidas de "N.T.:", indicando matices de la traducción. Debido a este hecho, el orden de las notas al pie no se corresponde con el orden en la guía original

- Siempre que aparece una referencia a un recurso en inglés y exista un recurso equivalente en español o relativo a España, se habrá sustituido. Las referencias a recursos del CPNI han sido convertidas a referencias del CCN-CERT siempre que ha sido posible. La referencia original se indicará a pie de página como una N.T.
- Los nombres propios y las siglas se han traducido. Las equivalencias entre referencias en inglés y en español se lista en el apartado "B.3. Tabla de equivalencias de la traducción" del "ANEXO B. Glosario de Términos y Abreviaturas". No se han traducido las siglas CPNI, SCADA, PA Consulting Group.

8. Se han añadido los Anexos comunes a las guías CCN-STIC, con el siguiente contenido:
9. ¡Error! No se encuentra el origen de la referencia.**.** ¡Error! No se encuentra el origen de la referencia.: Contiene todas las referencias que aparecen tanto en el documento original en inglés como en el documento actual. Los Anexos originales de referencias se han integrado en este Anexo. Las referencias se han numerado en base al resto de guías CCN-STIC.
    - A.1. Referencias Generales SCADA: Contiene el Anexo "*General SCADA References*" del documento original del CPNI.
    - A.2. Documentos y Páginas Web de Referencia: Contiene el Anexo "*Appendix A: Document and website references used in this guide* " del documento original del CPNI.
    - A.3. Referencias en esta traducción: Contiene las nuevas referencias añadidas en este documento de traducción.
10. **ANEXO B. Glosario de Términos y Abreviaturas**: Contiene las definiciones de los términos y abreviaturas que aparecen en el texto.
    - B.3. Tabla de equivalencias de la traducción: Contiene las equivalencias entre los términos técnicos en inglés, utilizados en el documento original, y los términos en español usados en la traducción.

0.3. CAMBIOS EN EL FORMATO

11. El formato de la guía original se ha adaptado al formato utilizado en el resto de guías CCN-STIC editadas por el CCN. Esto implica algunas adaptaciones que se explican a continuación:
12. Todos los párrafos han sido numerados.
13. El formato de algunos títulos, especialmente de cuarto nivel y sucesivos, ha sido adaptado.
14. La numeración de las notas al pie ha variado al incluir nuevas notas de traducción. Todas las notas que no comiencen con N.T. estaban en el documento original.

1. INTRODUCCIÓN

1.1. TERMINOLOGÍA

15. A lo largo de este marco los términos "sistema de control de procesos" y "sistemas control de procesos y SCADA" se utilizan para referirse a todo control industrial, control de procesos, Sistemas de Control Distribuido (DCS), Supervisión, Control y Adquisición de Datos (SCADA), automatización industrial y sistemas relacionados con la seguridad.

1.2. ANTECEDENTES

16. Los sistemas de control de procesos y SCADA hacen uso y se están volviendo progresivamente más dependientes de las tecnologías TI estándar. Estas tecnologías, como Microsoft Windows, TCP/IP, navegadores Web y las tecnologías inalámbricas, en uso creciente, están reemplazando a las tecnologías propietarias convencionales y más a medida que los sistemas de control de procesos son sustituidos por software comercial.

17. A pesar de que existen beneficios empresariales positivos derivados de este desarrollo, esta transformación conlleva dos principales preocupaciones:

18. Primero, tradicionalmente los sistemas de control de procesos han sido diseñados sólo con el propósito de controlar y proteger. Debido a la necesidad de conectividad, por ejemplo para extraer de información bruta sobre la planta o para poder realizar descargas directas a la producción, estos sistemas, que estaban aislados, se están conectando a redes abiertas. De ese modo se exponen a nuevas amenazas no esperadas, como gusanos[1], virus y hackers). La seguridad a través del secreto ya no es un tipo de defensa válido.

19. En segundo lugar, el software comercial y el hardware de propósito general se está usando para sustituir sistemas de control de procesos propietarios. Muchas medidas estándar de protección de la seguridad en TI utilizadas normalmente en estas tecnologías no han sido adaptadas a un entorno de control de procesos. Por tanto, las medidas de seguridad disponibles para proteger los sistemas de control y mantener el entorno seguro pueden ser insuficientes.

20. En caso de que se explotaran estas vulnerabilidades habría consecuencias potencialmente serias. Los efectos de un ataque electrónico en los sistemas de control de procesos pueden incluir, por ejemplo: denegación del servicio, pérdida de la integridad, pérdida de confidencialidad, pérdida de reputación empresarial, y el impacto en las condiciones de trabajo y el medio ambiente.

[1] Referencia de la Wikipedia para Gusano Informático: es un Malware que tiene la propiedad de duplicarse a sí mismo. (…) A diferencia de un virus, un gusano no precisa alterar los archivos de programas, sino que reside en la memoria y se duplica a sí mismo. (…)Los gusanos se basan en una red de computadoras para enviar copias de sí mismos a otros nodos (…) y son capaces de llevar esto a cabo sin intervención del usuario propagándose, utilizando Internet.

1.3. MARCO DE SEGURIDAD EN EL CONTROL DE PROCESOS

21. Aunque los sistemas de control de procesos están a menudo basados en tecnologías TI estándar, sus entornos operacionales difieren significativamente de un entorno TI corporativo. Pueden aprovecharse muchas lecciones de la experiencia adquirida por los expertos de seguridad en TI y, tras la adaptación de algunas herramientas y técnicas de seguridad estándar, se pueden usar para proteger sistemas de control de procesos. Otras medidas de seguridad estándar pueden ser completamente inapropiadas o no estar disponibles para su uso en un entorno de control.

22. Este marco de seguridad en el control de procesos se basa en las buenas prácticas de la industria para seguridad en el control de procesos y en TI. Está centrado en siete temas clave para el uso de las tecnologías TI estándar en el entorno de control de procesos y SCADA. Este marco pretende ser un punto de referencia para que una organización comience a desarrollar y adaptar la seguridad en el control de procesos adecuado a sus necesidades. Los siete módulos del marco se muestran a continuación en la Figura 1.

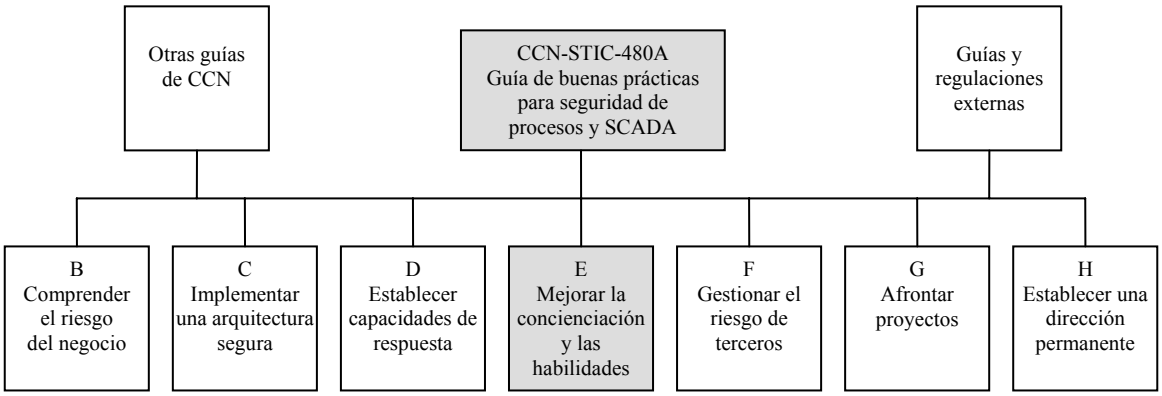


Figura 1: ***Dónde encaja esta guía dentro del marco de buenas prácticas***

23. Cada uno de estos módulos se describe con mayor detalle en su documento aparte, el presente documento proporciona una guía de buenas prácticas para comprender implementar una arquitectura segura. Todas las guías de este marco pueden encontrarse en la página web de CCN en https://www.ccn-cert.cni.es ([Ref.- 49][2]).

1.4. FINALIDAD DE ESTA GUÍA

24. La colección de guías "**Seguridad en el Control de Procesos y SCADA**" del CCN[3], proponen un marco que consta de siete módulos para abordar la seguridad en el control de procesos. Esta guía "**Mejorar la concienciación y las habilidades**" se basa en los fundamentos explicados en la guía de buenas prácticas, y lo desarrolla examinando en detalle cada una de las áreas clave y proporciona orientación general sobre la mejora de las habilidades de seguridad en el control de procesos dentro de las organizaciones.

25. En esta guía no incluye requisitos detallados de sensibilidad de la seguridad en el control de procesos ni de cursos de formación.

[2] N.T.: **¡Error! No se encuentra el origen de la referencia.**
[3] N.T.: Traducción de las guías del CPNI(**¡Error! No se encuentra el origen de la referencia.**) y complementadas con la guía "Seguridad en Sistemas SCADA" ([Ref.- 50])

1.5. DESTINATARIOS

26. Esta guía está dirigida a todos los que participan en la seguridad de los sistemas de automatización industrial, control de procesos, y SCADA, incluyendo:

- Ingenieros en control de procesos, automatización, SCADA y telemetría.
- Especialistas en seguridad de la información.
- Especialistas en seguridad física.
- Líderes empresariales.
- Gestores de riesgos.
- Encargados de las condiciones de trabajo.
- Ingenieros de operación.

2. RESUMEN DE "MEJORAR LA CONCIENCIACIÓN Y LAS HABILIDADES"

27. El éxito de cualquier marco de seguridad depende en última instancia del elemento humano – las personas son el recurso más importante y la mayor amenaza potencial a la seguridad. En un entorno de control de procesos, a menudo el personal de control de procesos no está familiarizado con la seguridad en TI y el personal de seguridad en TI no está familiarizado con los sistemas de control de procesos.

28. Tradicionalmente se ha visto la seguridad como una materia del entorno corporativo de TI, y no del entorno del control de procesos, y ha sido responsabilidad del departamento de TI. Además, la creencia de que las herramientas y técnicas de seguridad disponibles no eran compatibles ha provocado que los sistemas de control no estén debidamente protegidos. La seguridad de los sistemas de control de procesos puede ser mejorada aumentando la concienciación, mejorando de las habilidades y desarrollando una estrecha relación con el personal de seguridad en TI.

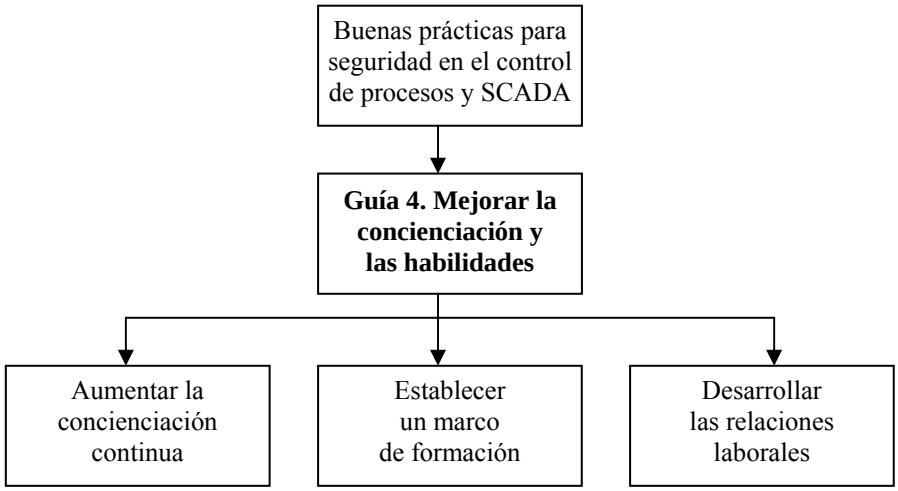


Figura 2: ***Estructura de "Mejorar la Concienciación y las Habilidades"***

29. El tema de la seguridad en el control de procesos abarca un público amplio dentro de una organización; aumentar la concienciación en este tema pone de relieve las vulnerabilidades, amenazas y riesgos de estos sistemas, los impactos potenciales de fallos en la seguridad del control de procesos en la empresa. Los programas de concienciación, deben dar una visión de las soluciones técnicas y de procedimientos que se pueden desplegar para prevenir que los ciberataques a la seguridad tengan éxito.
30. Hay que formar al personal para darles el conocimiento adecuado para proteger adecuadamente los sistemas de control de procesos. Esta formación debe abarcar un área técnica amplia, desde las habilidades en TI a las habilidades en control de procesos. Hay pocos cursos de formación diseñados para esta necesidad específica, por lo que es necesario que las organizaciones desarrollen sus propios marcos de formación para garantizar que el personal tenga las habilidades y conocimientos apropiados para desempeñar sus trabajos de forma segura.
31. La concienciación y la formación ayudan a desarrollar una estrecha relación de trabajo entre los departamentos de control de procesos y TI, proporcionando un lenguaje y procesos comunes que se pueden utilizar para desarrollar un programa efectivo de seguridad en el control de procesos. Implantar la seguridad en el control de procesos en la organización es esencial para el éxito continuo de cualquier programa de seguridad en el control de procesos.

3. AUMENTAR LA CONCIENCIACIÓN CONTINUA

3.1. CONTEXTO DE ESTA SECCIÓN DENTRO DEL MARCO GENERAL

32. Este elemento del marco se centra en incrementar en una amplia gama de público la concienciación sobre las materias de seguridad en el control de procesos, y se basa en las guías “Comprender el riesgo del negocio” ([Ref.- 51]) y “Establecer una dirección permanente” ([Ref.- 58]) del marco de guías de buenas prácticas.

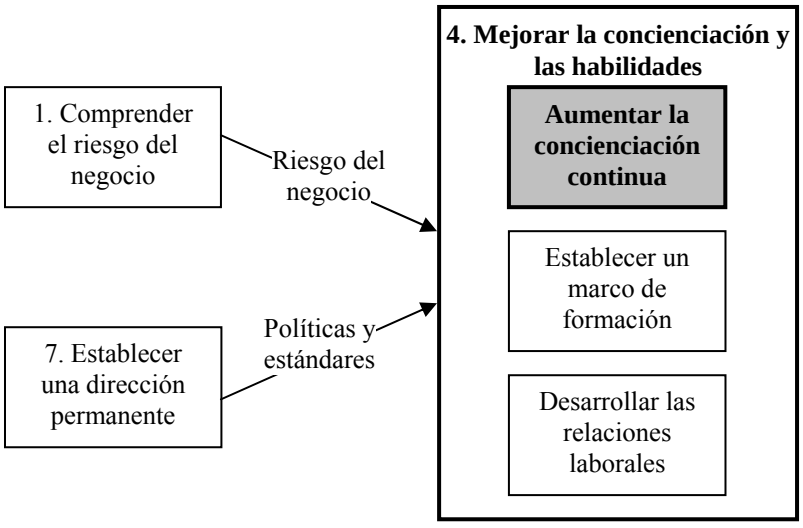


Figura 3: ***Cómo encaja “Aumentar La Concienciación Continua” en este marco***

3.2. JUSTIFICACIÓN

33. Aumentar la concienciación es potencialmente la acción única más valiosa en la tarea continua de la seguridad en el control de procesos. Aumentar la concienciación se compromete a garantizar que todo el personal pertinente tiene suficiente conocimiento de la seguridad en los sistemas de control de procesos y del impacto potencial en el negocio de los fallos de seguridad. El personal necesita saber qué hacer para prevenir los ataques y qué hacer en caso de un incidente.

3.3. PRINCIPIOS DE BUENAS PRÁCTICAS

34. Los principios generales de buenas prácticas relevantes del documento general "CCN-STIC-480A – Guía de buenas prácticas – Seguridad en el Control de Procesos y SCADA" ([Ref.- 51]), son los siguientes:

    - Comprometer a la alta dirección para asegurar que se entienden las consecuencias de los riesgos de seguridad en el control de procesos y por tanto, contribuir a las compras necesarias para la gestión de este riesgo.
    - Establecer programas de concienciación para aumentar el conocimiento general de la seguridad. Estos programas harán hincapié en las responsabilidades en seguridad, llamarán la atención sobre las amenazas actuales y aumentarán la vigilancia.
    - Crear un modelo de negocio que apoye el programa de seguridad en el control de procesos.

3.4. ORIENTACIÓN SOBRE LAS BUENAS PRÁCTICAS

35. Los mensajes de concienciación de seguridad en el control de procesos necesitan ser adaptados al público objetivo. Para asegurar que los mensajes son relevantes, que se han recibido y entendido, se debe tener en cuenta la organización y su entorno de trabajo.

36. Aumentar la concienciación no es un ejercicio único, es un proceso continuo que permita un cambio cultural que con el tiempo se irá integrando en la organización. Hay una serie de maneras de aumentar la concienciación; debería dedicarse un tiempo a planificar el enfoque más adecuado para transmitir estos mensajes al público deseado. El enfoque puede diferir de una organización a otra, pues la forma más eficaz de aumentar la concienciación en una organización dependerá de la cultura de la organización.

37. Para que un programa de seguridad en el control de procesos tenga éxito hay dos elementos clave relacionados con la concienciación que son necesarios: la participación de la dirección y el establecimiento de un programa de concienciación. Otro elemento clave es la existencia de un modelo de negocio comunicado con claridad que apoye el programa de seguridad en el control de procesos.

3.4.1. INVOLUCRAR AL PERSONAL DIRECTIVO

38. El simple proceso de examinar la seguridad en el control de procesos crea sensibilidad sobre esas cuestiones, sin embargo, tener el respaldo de la dirección indica que el tema es importante y la gente tiene que tomar nota.

39. Tener el apoyo y la participación de la dirección es un requisito esencial para ser capaces de poner en marcha un mensaje de seguridad en el control de procesos para un público más amplio. Un campeón para la seguridad en el control de procesos puede resolver muchos problemas internos asegurando que un mensaje se propaga en cascada a través de los niveles de gestión y evita retrasos consiguiendo la participación de los interesados.
40. Con el fin de que la dirección participe, puede ser necesario demostrar la importancia que tiene para el negocio la seguridad en el control de sistemas. Esto puede requerir el desarrollo de un modelo de negocio que muestre los riesgos asociados a no tener un programa de seguridad y los costes y beneficios asociados de tener uno.
41. Algunos de los principales beneficios de la participación de los altos directivos son:
    - Entender que el riesgo existe
    - Elevar el perfil de la seguridad en el control de procesos
    - Propagar los mensajes en cascada utilizando la jerarquía de gestión y los canales de comunicación
    - Garantizar un presupuesto adecuado para el programa de concienciación
    - Entender que algún riesgo residual seguirá existiendo
    - Facultar la eliminación de las barreras internas de recursos

3.4.2. ESTABLECER PROGRAMAS DE CONCIENCIACIÓN

42. La seguridad en el control de procesos puede ser complicada, abarca tecnologías oscuras y conceptos desconocidos, y en consecuencia los mensajes deben formar parte de un programa de concienciación. Al determinar el/los mensajes de concienciación, es importante darse cuenta de que aumentar la concienciación e integrarla en la empresa es un proceso a largo plazo, no un esfuerzo de una vez; es un maratón no una carrera rápida.
43. Es esencial que cualquier programa de concienciación de seguridad en control de procesos esté correctamente planificado, ya que una sucesión de intentos mal planificados y mal ejecutados pueden obstaculizar los programas de seguridad en control de procesos. Para garantizar que un programa de concienciación está bien dirigido y ejecutado hay una serie de áreas que deben considerarse:
    - ¿Cuál es el objetivo de concienciación de seguridad?
    - ¿Cuál es el público objetivo?
    - ¿Cómo funcionan las comunicaciones dentro de la organización?
    - ¿Qué conocimientos existen en la organización con anterioridad?
    - ¿Qué temas de concienciación necesitan tratarse?
    - ¿Qué métodos de concienciación pueden usarse para transmitir el mensaje?
    - ¿Cómo puede integrarse la concienciación de seguridad en la organización?
    - ¿Cómo de bien es comprendido el mensaje?
44. Estas áreas se describen en mayor detalle en los párrafos siguientes.

3.4.2.1. OBJETIVO DE CONCIENCIACIÓN DE SEGURIDAD

45. Tener un objetivo específico de concienciación centrará los esfuerzos de difusión del mensaje clave en el público apropiado y permitirá medir el éxito del programa. Integrar la seguridad en cualquier organización conlleva tiempo y el mejor enfoque es centrarse en los mensajes clave y construir lentamente y en profundidad la concienciación.

3.4.2.2. PÚBLICO OBJETIVO

46. Identificar los diferentes públicos y reconocer que el nivel de detalle del mensaje debe variar dependiendo del público es vital para el éxito de un programa de concienciación de seguridad en el control de procesos. Los públicos posibles incluyen:

- Ingenieros en control de procesos, automatización, SCADA y telemetría
- Líderes empresariales
- Equipo de respuesta de la seguridad en el control de procesos (ERSCP)
- Especialistas en la seguridad de la información
- Especialistas en seguridad física
- Usuarios de negocio
- Gestores de riesgo
- Gestores de proyectos y equipos
- Personal de operaciones
- Encargados de las condiciones de trabajo.
- Organizaciones de apoyo

3.4.2.3. COMUNICACIONES EXISTENTES

47. Antes de embarcarse en un programa de aumento de la concienciación es importante comprender qué marco y herramientas de comunicación hay disponibles. Entender cómo fluye la información en una organización, qué tipos de mensajes son enviados y recibidos, con quién se comunican los destinatarios del programa, cómo son planificadas y recibidas las comunicaciones y quién tiene la responsabilidad de las comunicaciones. Adoptar los mecanismos existentes puede facilitar la tarea de la concienciación de seguridad en el control de procesos.

3.4.2.4. CONOCIMIENTOS EXISTENTES

48. Un paso evidente pero a menudo pasado por alto es evaluar lo que ya se sabe, tal vez mediante el uso de una breve encuesta o sondeo. Este conocimiento debe ser utilizado como base para los temas de concienciación.

3.4.2.5. TEMAS DE CONCIENCIACIÓN

49. Hay temas comunes que pueden ser cubiertos en los programas de concienciación de seguridad en el control de procesos:

- Concienciación general en la seguridad en el control de procesos
- En qué fijarse y cómo reaccionar
- Ejemplos de fallos de seguridad en el control de procesos y sus efectos
- Políticas, normas y soluciones disponibles
- Actualizaciones de los documentos existentes
    - Políticas y normas
    - Orientación de proveedores
- Una explicación y comprensión del control de procesos para profesionales de TI.
- Una explicación y comprensión de seguridad en TI para profesionales en control de procesos.

3.4.2.6. MÉTODOS DE CONCIENCIACIÓN

50. Hay muchos modos de crear concienciación. El mejor enfoque probablemente sea una mezcla de los indicados. Vale la pena considerar cuál sería la mejor manera de obtener el mensaje de concienciación a través del público objetivo. Los métodos incluyen;

- Conferencias
- Comunicaciones por correo electrónico
- Boletines de noticias
- Almacén centralizado para la información sobre la seguridad en el control de procesos
- Llamadas telefónicas
- Campañas con carteles
- Videos y DVD
- Sitios web y emisiones por Internet (webcast)
- Talleres
- Aparecer en agendas estándar de reuniones

3.4.2.7. INTEGRACIÓN

51. Integración la seguridad en el control de procesos en una organización no es algo que ocurra rápidamente. Se desarrolla con el tiempo hasta que la seguridad en el control de procesos se convierte en un aspecto cotidiano de una organización. Los programas de concienciación deben revisarse periódicamente para garantizar que los mensajes se han recibido, entendido y ejecutado en consecuencia para que el programa de seguridad en el control de procesos siga siendo de alta prioridad en una organización y está integrado en las operaciones habituales.

3.4.2.8. COMPRENSIÓN

52. No importa cómo de buena sea una presentación o un mensaje si no es entendido por los beneficiarios. La retroalimentación de los beneficiarios es necesaria para determinar si el mensaje se ha recibido correctamente. Los programas de concienciación deben revisarse periódicamente para garantizar que los mensajes se han recibido, entendido y ejecutado en consecuencia para que el programa de seguridad en el control de procesos siga siendo de alta prioridad en una organización y está integrado en las operaciones habituales.

3.4.3. CONSTRUIR EL MODELO DE EMPRESA

53. Es importante garantizar que hay suficiente comprensión a través de la empresa, en los diferentes niveles del modelo, para aumentar la seguridad en el control de sistemas. Los elementos clave del modelo de empresa incluyen:

    - Una visión general del perfil de riesgo de la empresa (incluyendo el impacto de las amenazas potenciales de los incidentes y las vulnerabilidades).
    - Los beneficios de mejorar la seguridad del control de sistemas, incluyendo el perfil de riesgo mejorado tras los incidentes (ej., el beneficio empresarial)
    - Los requisitos para un programa de seguridad , las principales actividades, recursos y costes
    - El Retorno de la Inversión en Seguridad (RIS).

54. Puede ser necesario llevar a cabo esta actividad a diferentes niveles dentro de una organización. Puede ser necesario construir un modelo de negocio a bajo nivel para las mejoras de un centro o un sistema de control específico. Sin embargo, en una gran organización puede ser necesario construir el modelo de negocio general para toda la organización. Una de las principales ventajas de este último es que el trabajo llevado a cabo centralmente para preparar para el cambio el modelo de negocio de una organización ayudará a los equipos de los centros en sus actividades y reducirá el esfuerzo total que una organización tiene que hacer para poner en marcha un programa de mejora de la seguridad.

55. Más orientaciones para el desarrollo de modelos de negocio para sistemas de control pueden encontrarse la guía “Guide to Industrial Control (ICS) Systems” ([Ref.- 43] en el apéndice A).

4. ESTABLECER UN MARCO DE FORMACIÓN

4.1. CONTEXTO DE ESTA SECCIÓN DENTRO DEL MARCO GENERAL

56. Este elemento del marco se centra en incrementar en una amplia gama de público la concienciación sobre las materias de seguridad en el control de procesos, y se basa en las guías “Comprender el riesgo del negocio” ([Ref.- 51]) y “Establecer una dirección permanente” ([Ref.- 58]) del marco de guías de buenas prácticas.

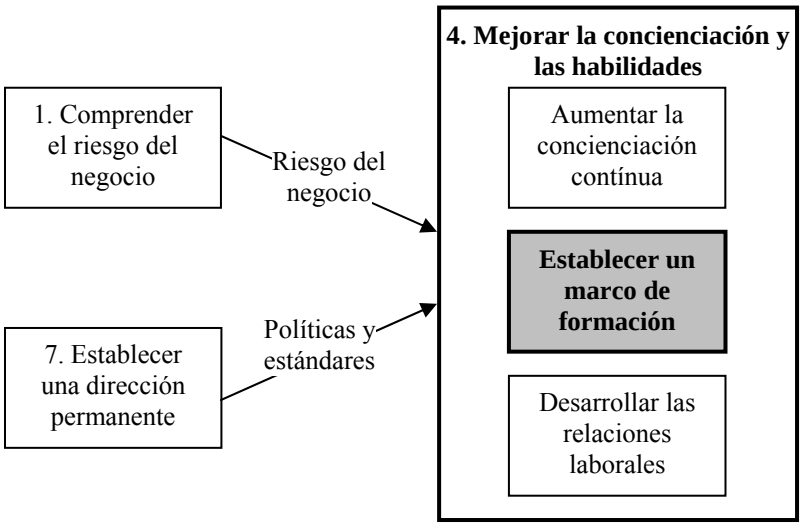


Figura 4: ***Cómo encaja "Establecer un marco de formación" en este marco***

4.2. JUSTIFICACIÓN

57. El concepto de la seguridad en el control de procesos es relativamente nuevo. En general existe un bajo nivel de comprensión técnica y poca conciencia del impacto potencial en el negocio. Hay pocas normas disponibles y el personal generalmente no tiene los conocimientos adecuados para llevar a cabo el trabajo requerido tanto de control de sistemas como de seguridad. Existe falta de cursos de formación específicos de seguridad en control de procesos.

4.3. PRINCIPIOS DE BUENAS PRÁCTICAS

58. Los principios generales de buenas prácticas relevantes del documento general "CCN-STIC-480A – Guía de buenas prácticas – Seguridad en el Control de Procesos y SCADA" ([Ref.- 51]), son los siguientes:

- Formar al personal de TI para desarrollar una apreciación y conocimiento de los sistemas de control de procesos y sus entornos operativos, poniendo de relieve las diferencias entre la seguridad en los sistemas de control de procesos y la seguridad en TI.
- Desarrollar las habilidades necesarias de seguridad en TI en los equipos de control de procesos y proporcionar los servicios adecuados de soporte a estos equipos en TI.

4.4. ORIENTACIÓN SOBRE LAS BUENAS PRÁCTICAS

59. La mayoría de las diferencias entre los entornos operativos de control de procesos y TI se reducen a la importancia que tiene la estabilidad de los sistemas de control de procesos. Esta necesidad impulsa una cultura de riesgos conservadora que da importancia a los procesos y sistemas estáticos, sólidos y repetibles.

60. Debe desarrollarse un marco de formación que cubra la formación para el personal clave detallando el nivel de comprensión de las vulnerabilidades de una organización, la información y los recursos que se pueden acceder para compartir las buenas prácticas y las medidas de mitigación aprobadas.

61. Desarrollar un plan de formación es parecido en muchos aspectos a desarrollar un programa de concienciación, y se puede utilizar en enfoque similar. Hay una serie de cuestiones que deben considerarse para garantizar que el marco de formación ofrece un programa valorado:

    - ¿Cuál es el objetivo marco de la formación?
    - ¿Cuál es el público objetivo?
    - ¿Cuáles son las necesidades de formación?
    - ¿Qué métodos se utilizarán?

62. Estas áreas se describen en mayor detalle en los párrafos siguientes.

4.4.1.1. OBJETIVOS DEL MARCO DE FORMACIÓN

63. El objetivo de esta formación no consiste en convertir a todo el mundo en expertos en seguridad en control de procesos, sino garantizar que el personal tiene las habilidades correctas para desempeñar sus funciones. Así como el personal de control de procesos aprenda sobre seguridad TI, los equipos de TI necesitan desarrollar una buena comprensión de los sistemas de control de procesos. El objetivo de la creación de un marco es proporcionar la comprensión básica para que puedan:

    - Comunicarse eficazmente con un lenguaje compartido
    - Entender los distintos entornos operativos
    - Transferir los conocimientos necesarios para que el personal de control de procesos aplique y cumpla con medidas correctas de seguridad TI aplicables en el entorno de control de procesos.
    - Transferir los conocimientos necesarios para que el personal de TI apoye eficazmente los requisitos de seguridad en el control de procesos.

4.4.1.2. IDENTIFICAR EL PÚBLICO OBJETIVO

64. A partir del objetivo del marco de formación y el análisis de los diversos públicos se pueden determinar las necesidades de formación para cada público. Identificar las distintas audiencias ayuda a descomponer las necesidades de formación en un plan manejable, y proporciona una herramienta para priorizar en qué orden se deben capacitar las partes interesadas. Ejemplos de los diversos públicos son los siguientes:

    - Encargado de la seguridad en el control de procesos
    - Responsable Único (RU)
    - Ingenieros de control de proceso, automatización, SCADA y telemetría
    - Personal de TI

- El equipo de respuesta
- El equipo de operaciones

4.4.1.3. NECESIDADES DE FORMACIÓN

65. El nivel de formación necesario varía en función de los individuos (ej., un RU tendrá que ser consciente de las normas y la regulación, mientras que una persona a cargo de las normas del cortafuegos tendrá que ser técnicamente competente en la gestión de cortafuegos).

66. Hay una serie de temas que pueden ser considerados para distintos públicos:

- Políticas y normas: se centra en las normas y la legislación.
- Procedimientos: detalla los procedimientos y cómo se relacionan con las políticas y las normas.
- Respuesta a incidentes: cubre lo que se debe hacer en caso de incidente.
- Arquitectura: cubre cómo los distintos sistemas están conectados entre sí y configurados, y será un tema técnico.
- Formación específica de proveedores: implica formación de seguridad específica para los sistemas de un proveedor.
- Formación técnica detallada: cubre normalmente la seguridad TI general y puede ser parte de acreditación formal reconocida por la industria.

4.4.1.4. MÉTODOS DE ENTREGA

67. Comparativamente hay pocos recursos diseñados específicamente para la seguridad en el control de procesos. De los cursos de seguridad TI disponibles, encontrar cuál proporcionará un nivel adecuado de comprensión puede ser proceso difícil y largo. El análisis de las necesidades de formación es de gran ayuda en este ámbito y seleccionar cursos organizados por organizaciones profesionales reconocidas garantizará que se cumplan las necesidades de formación. Sin embargo, es poco probable que se oferte todo lo que se necesita y es probable que sea necesaria una mezcla de métodos de entrega. Los métodos típicos que se pueden utilizar son:

- **Formación interna:** las sesiones organizadas internamente a menudo proporcionan la formación más relevante, ya que se ocupan de temas específicos de organización y puede poner en contexto los conocimientos adquiridos externamente. Sin embargo, pueden consumir una gran cantidad de tiempo y valiosos recursos en su planificación y ejecución.
- **Cursos de formación externos y formación aprobada de colaboradores:** ya sea proporcionada por proveedores o por profesionales de la seguridad, son de carácter técnico y a veces difíciles de relacionar con cuestiones específicas del centro. Hay una variedad de organismos profesionales que prestan acreditación de seguridad tales como los enumerados a continuación (se pueden encontrar enlaces en el apéndice A).
    - Certificado CISA de Auditor de Sistemas de Información (CISA) ([Ref.- 31])
    - Certificación CISM de Director de Seguridad de la Información ([Ref.- 31])

- Certificado CISSP de Profesional de Seguridad de los Sistemas de Información (CISSP) ([Ref.- 32])
- Certificado GIAC de Garantía Global de la Información ([Ref.- 33])

- **Formación informática, online y seminarios web:** se puede utilizar para formación de individuos y equipos con un coste relativamente bajo.
- **Conferencias y talleres:** asistir a conferencias es una buena manera de aprender acerca de la seguridad en el control de procesos y muchos organismos industriales que organizan conferencias suelen tener talleres de formación como parte del evento.
- **Cursos de actualización:** la formación no es algo puntual, se deben buscar cursos para garantizar que el personal se mantiene actualizado en los cambios en las amenazas y la tecnología y para mantener su nivel de destreza.
- **Sesiones personales:** se trata de una valiosa herramienta para los principales interesados, permitiendo que esas personas aprendan rápidamente y permitiendo que el mensaje se entiende.
- **Cursos de formación estructurados:** pueden ser tanto externos como internos, y se centran en un tema u objetivo específico (ej., instalación y configuración de cortafuegos).
- **Auto-evaluación:** la auto-evaluación es una valiosa herramienta que permite a una organización conservar la propiedad de la seguridad en el control de procesos y medir el éxito de los planes de mitigación.
- **Talleres multidisciplinares:** reuniendo a los interesados en la seguridad en el control de procesos para debatir las mejoras de la seguridad permite que se apliquen una amplia gama de experiencias y conocimientos a un problema, y puede poner de relieve las deficiencias que requieran ayuda externa.

68. El Departamento de Seguridad interior de Estados Unidos ofrece algunos recursos de formación basados en la web ([Ref.- 48] en el Apéndice A).

5. DESARROLLAR LAS RELACIONES LABORALES

5.1. CONTEXTO DE ESTA SECCIÓN DENTRO DEL MARCO GENERAL

69. Este elemento del marco se centra en mejorar las habilidades de seguridad en el control de procesos dentro de una organización desarrollando relaciones laborales e integrando en la organización la seguridad en el control procesos. Este apartado se basa en las guías “Comprender el riesgo del negocio” ([Ref.- 51]) y “Establecer una dirección permanente” ([Ref.- 58]) del marco de guías de buenas prácticas, y en los elementos de esta guía “Aumentar la Concienciación Continua” y “Establecer un Marco de Formación”.

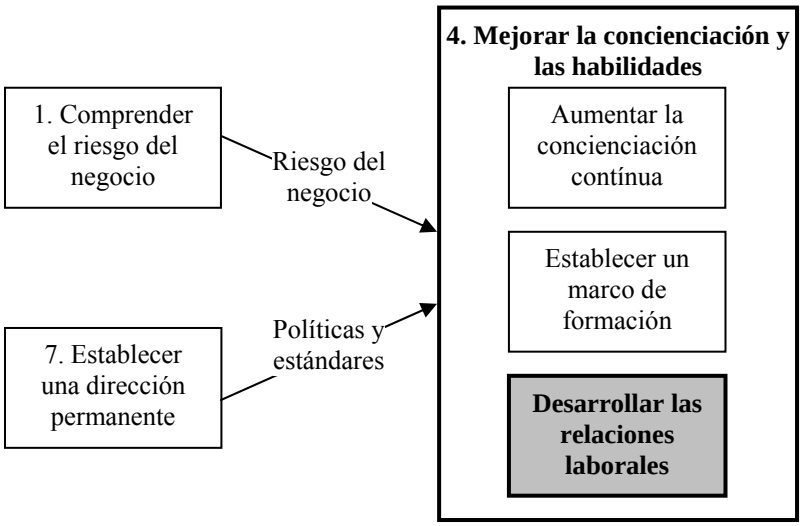


Figura 5: ***Cómo encaja "Desarrollar las relaciones laborales" en este marco***

5.2. JUSTIFICACIÓN

70. Conforme confluyen los mundos de control de procesos y TI, las dos comunidades necesitan trabajar juntas para proteger ambos entornos de manera eficaz proporcionando soluciones mejor integradas, mejorando el uso del personal y reduciendo los costes.

5.3. PRINCIPIOS DE BUENAS PRÁCTICAS

71. Los principios generales de buenas prácticas relevantes del documento general "CCN-STIC-480A – Guía de buenas prácticas – Seguridad en el Control de Procesos y SCADA" ([Ref.- 51]), son los siguientes:

    - Establecer vínculos entre los equipos de seguridad en TI y de control de procesos a fin de crear buenas relaciones laborales, compartir habilidades y facilitar la transferencia de conocimientos.

5.4. ORIENTACIÓN SOBRE LAS BUENAS PRÁCTICAS

72. El control de procesos y las TI han sido tradicionalmente dos ámbitos diferentes. La tendencia reciente de convergencia tecnológica y la necesidad de conectar los dos entornos ha puesto de relieve la necesidad de mejorar las relaciones entre los departamentos de TI y de control de procesos. Es importante para ambos equipos ser conscientes de cada entorno para que las relaciones y el entendimiento compartido puedan ser desarrollados con éxito.

73. El personal de control de procesos puede desarrollar habilidades en torno a las aplicaciones, la infraestructura y la seguridad TI. Asimismo, el personal TI puede desarrollar habilidades básicas de control de procesos, incluyendo control de cambios críticos de negocio y prácticas en la realización de pruebas.

74. Mediante el desarrollo de una relación en ambos sentidos, se pueden obtener una serie de beneficios mutuos:

- Aumento de la transferencia de conocimientos.
- Acceso a una base más amplia de habilidades de seguridad.
- Acceso a una base más amplia de habilidades de control de procesos.
- Mejor comprensión de la protección de la seguridad.
- Una oportunidad para compartir las prácticas mejores.
- Soluciones de seguridad a menor coste
- Prácticas de trabajo más eficaces
- Mayor velocidad en la ejecución de proyectos

75. Algunas medidas sencillas que se pueden tomar para ayudar a reforzar las buenas relaciones de trabajo son las siguientes:

- Representación TI en el Equipo de Respuesta de Seguridad en el Control de Procesos (ERSCP).
- Reuniones periódicas para discutir los desarrollos y el progreso de la seguridad.
- Invitar a representantes de TI a los comités de cambio en el control de procesos.
- Ampliar las listas de distribución e incluir los correspondientes contactos de TI.
- Establecer un sistema de tutoría.
- Tener una representación del control de procesos en el equipo de seguridad de la organización.
- Trabajo compartido: Formación cruzada del personal de TI y de control de procesos, cubriendo cada uno los trabajos de los otros.
- Equipos de proyecto combinados.

76. En muchas organizaciones las funciones de TI pueden proporcionar una gama de servicios a la organización. Desarrollando de una estrecha relación pueden identificarse soluciones de TI que se puedan utilizar en el entorno de control de procesos, ya sea directamente (con ajustes mínimos) o modificando la configuración del entorno de control de procesos. Ejemplos de servicios que pueden ser buenos candidatos a ser proporcionados por TI incluyen:

- Antivirus
- Administración y monitorización de cortafuegos
- Monitorización de los sistemas de red
- Gestión de acceso remoto
- Respuesta a incidentes y alertas
- Formación y concienciación en seguridad
- Gestión continua del aseguramiento

6. AGRADECIMIENTOS

PA and CPNI agradencen los comentarios y sugerencias recibidos del Grupo de Intercambio de Información de SCADA y Sistemas de Control, y de otros grupos relacionados con la protección de CNI de todo el mundo durante el desarrollo de este marco de guías de buenas prácticas. Las contribuciones han sido recibidas con gratitud y son demasiado numerosas para mencionarlas aquí individualmente.

Sobre los autores

Este documento[4] ha sido producido conjuntamente por PA Consulting Group y CPNI.

Centre for the Protection of National Infrastructure
Central Support
PO Box 60628
London
SW1P 9HA
Fax: 0207 233 8182
Email: enquiries@cpni.gov.uk
Web: www.cpni.gov.uk

Para más información del CPNI sobre la Seguridad en el Control de Procesos y SCADA:
Internet: www.cpni.gov.uk/ProtectingYourAssets/scada.aspx

PA Consulting Group
123 Buckingham Palace Road
London
SW1W 9SR
Tel: +44 20 7730 9000
Fax: +44 20 7333 5050
Email: info@paconsulting.com
Web: www.paconsulting.com

Para más información de PA Consulting Group sobre Seguridad en el Control de Procesos y SCADA:
Email: process_control_security@paconsulting.com
Web: www.paconsulting.com/process_control_security

[4] N.T.: La versión original de este documento. La traducción ha sido realizada por CCN-CERT (**¡Error! No se encuentra el origen de la referencia.**).

ANEXO A. REFERENCIAS

A.1. REFERENCIAS GENERALES SCADA

N.T.: Las siguientes referencias se reproducen tal cual aparecen en el documento original en el apartado "*General SCADA Referentes*".

[Ref.- 1] BS 7858:2006: Security screening of individuals employed in a security environment. Code of practice
www.bsi-global.com/en/Standards-and-Publications/Industry-Sectors/Security/Security-Products/

[Ref.- 2] BS-78582006/BS 8470:2006 Secure destruction of confidential material. Code of practice
www.bsi-global.com/en/Shop/Publication-Detail/?pid=000000000030127562

[Ref.- 3] CPNI: Best Practice Guide Commercially Available Penetration Testing
www.cpni.gov.uk/Docs/re-20060508-00338.pdf

[Ref.- 4] CPNI: Best Practice Guide on Firewall Deployment for SCADA and Process Control Networks
www.cpni.gov.uk/Docs/re-20050223-00157.pdf

[Ref.- 5] CPNI First Responders' Guide: Policy and Principles
www.cpni.gov.uk/docs/re-20051004-00868.pdf

[Ref.- 6] CPNI SCADA Good Practice Guides
www.cpni.gov.uk/ProtectingYourAssets/scada.aspx

[Ref.- 7] CPNI Information Sharing
www.cpni.gov.uk/ProtectingYourAssets/InformationSharing.aspx

[Ref.- 8] CPNI Personnel Security measures
www.cpni.gov.uk/ProtectingYourAssets/personnelSecurity.aspx

[Ref.- 9] CPNI: Good Practice Guide Patch Management
www.cpni.gov.uk/Docs/re-20061024-00719.pdf

[Ref.- 10] CPNI: Good Practice Guide Outsourcing: Security Governance Framework for IT Managed Service Provision
www.cpni.gov.uk/Docs/re-20060802-00524.pdf

[Ref.- 11] CPNI: Good Practice Guide on Pre-Employment Screening
www.cpni.gov.uk/Products/bestpractice/3351.aspx

[Ref.- 12] CPNI: An Introduction to Forensic Readiness Planning
www.cpni.gov.uk/docs/re-20050621-00503.pdf

[Ref.- 13] CPNI: Personnel Security Measures
www.cpni.gov.uk/ProtectingYourAssets/personnelSecurity.aspx

[Ref.- 14] DHS Control Systems Security Program
http://csrp.inl.gov/

[Ref.- 15] DHS Control Systems Security Program Recommended Practice
http://csrp.inl.gov/Recommended_Practices.html

[Ref.- 16] Guide to Industrial Control Systems (ICS)
http://csrc.nist.gov/publications/PubsDrafts.html

[Ref.- 17] Securing WLANs using 802,11i
http://csrp.inl.gov/Documents/Wireless%20802.11i%20Rec%20Practice.pdf

[Ref.- 18] Using Operational Security (OPSEC) to support a Cyber Security Culture in Control Systems Environments
http://csrp.inl.gov/Documents/OpSec%20Rec%20Practice.pdf

[Ref.- 19] ISA SP99 –DHS Catalog of Control System Security Requirements
www.dhs.gov

[Ref.- 20] Manufacturing and Control Systems Security
www.isa.org/MSTemplate.cfm?MicrositeID=988&CommitteeID=6821

[Ref.- 21] ISO 17799 International Code of Practice for Information Security Management
www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=39612

[Ref.- 22] ISO 27001 International Specification for Information Security Management
www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42103

[Ref.- 23] Cyber Security Procurement Language for Control Systems
www.msisac.org/scada/documents/12July07_SCADA_procurement.pdf

[Ref.- 24] MU Security Industrial Control (MUSIC) Certification
www.musecurity.com/support/music.html

[Ref.- 25] Control System Cyber Security Self-Assessment Tool (CS2SAT)
www.us-cert.gov/control_systems/pdf/CS2SAT.pdf

[Ref.- 26] Department of Homeland Security Control Systems Security Training
www.us-cert.gov/control_systems/cstraining.html#cyber

[Ref.- 27] Recommended Practices Guide for Securing ZigBee Wireless Networks in Process Control System Environments
www.us-cert.gov/control_systems/pdf/Zigbee%20Rec%20Pract%20-%20draft-posted%207-10-07.pdf.

[Ref.- 28] Achilles Certification Program
www.wurldtech.com/index.php

[Ref.- 29] American Gas Association (AGA)
www.aga.org

[Ref.- 30] American Petroleum Institute (API)
www.api.org

[Ref.- 31] Certified Information Systems Auditor (CISA)
www.isaca.org/

[Ref.- 32] Certified Information Systems Security Professional (CISSP)
www.isc2.org/

[Ref.- 33] Global Information Assurance Certification (GIAC)
www.giac.org/

[Ref.- 34] International Council on Large Electric Systems (CIGRE)
www.cigre.org

[Ref.- 35] International Electrotechnical Commission (IEC)
www.iec.ch

[Ref.- 36] Institution of Electrical and Electronics Engineers (IEEE)
www.ieee.org/portal/site

[Ref.- 37] National Institute of Standards and Technology (NIST)
www.nist.gov

[Ref.- 38] NERC Critical Infrastructure Protection (CIP)
www.nerc.com/~filez/standards/Cyber-Security-Permanent.html

[Ref.- 39] Norwegian Oil Industry Association (OLF)
www.olf.no/english

[Ref.- 40] Process Control Security Requirements Forum
www.isd.mel.nist.gov/projects/processcontrol/

[Ref.- 41] US Cert
www.us-cert.gov/control_systems/

[Ref.- 42] WARPS
www.warp.gov.uk

A.2. DOCUMENTOS Y PÁGINAS WEB DE REFERENCIA

N.T.: Las siguientes referencias se reproducen tal cual aparecen en el documento original en el apartado "*Appendix A: Document and website references used in this guide*".

Section 3.4.1

[Ref.- 43] Guide to Industrial Control (ICS) Systems
http://csrc.nist.gov/publications/PubsDrafts.html

Section 3.4.3

[Ref.- 44] Guide to Industrial Control (ICS) Systems
http://csrc.nist.gov/publications/PubsDrafts.html

Section 4.4

[Ref.- 45] Certified Information Systems Auditor (CISA)
www.isaca.org/

[Ref.- 46] Certified Information Systems Security Professional (CISSP)
www.isc2.org/

[Ref.- 47] Global Information Assurance Certification (GIAC)
www.giac.org/

[Ref.- 48] Department of Homeland Security Control Systems Security Training
www.us-cert.gov/control_systems/cstraining.html#cyber

A.3. REFERENCIAS EN ESTA TRADUCCIÓN

[Ref.- 49] Portal de CCN-CERT
https://www.ccn-cern.cni.es

[Ref.- 50] CCN-STIC-480 Seguridad en sistemas SCADA

[Ref.- 51] CCN-STIC-480A Seguridad en el control de procesos y SCADA
Guía de buenas prácticas

[Ref.- 52] CCN-STIC-480B Seguridad en el control de procesos y SCADA
Guía 1: Comprender el riesgo del negocio

[Ref.- 53] CCN-STIC-480C Seguridad en el control de procesos y SCADA
Guía 2: Implementar una arquitectura segura

[Ref.- 54] CCN-STIC-480D Seguridad en el control de procesos y SCADA
Guía 3: Establecer capacidades de respuesta

[Ref.- 55] CCN-STIC-480E Seguridad en el control de procesos y SCADA
Guía 4: Mejorar la concienciación y las habilidades

[Ref.- 56] CCN-STIC-480F Seguridad en el control de procesos y SCADA
Guía 5: Gestionar el riesgo de terceros

[Ref.- 57] CCN-STIC-480G Seguridad en el control de procesos y SCADA
Guía 6: Afrontar proyectos

[Ref.- 58] CCN-STIC-480H Seguridad en el control de procesos y SCADA
Guía 7: Establecer una dirección permanente

[Ref.- 59]

ANEXO B. GLOSARIO DE TÉRMINOS Y ABREVIATURAS

B.1. GLOSARIO DE TÉRMINOS

Amenaza*	Cualquier circunstancia o hecho que pueda dañar un sistema de control de procesos y SCADA a través de accesos no autorizados, destrucción, divulgación, modificación de datos y/o denegación del servicio.
Riesgo*	Posibilidad de que se produzca un hecho que tendrá un impacto negativo en el sistema de control. El hecho puede ser el resultado de una amenaza o una combinación de amenazas.
Tolerancia al riesgo*[5]	Nivel de riesgo, utilizado para determinar lo aceptable que puede ser un riesgo.
Probabilidad*[6]	Probabilidad de un determinado resultado.
Impacto*	Consecuencias de que una amenaza ocurra.
Vulnerabilidad*	Grado en que un sistema de *software* o un componente está abierto a accesos no autorizados, cambio o divulgación de su información y es susceptible a las interferencias o a la interrupción de los servicios del sistema.

B.2. GLOSARIO DE SIGLAS

CCN	Centro Criptológico Nacional
CPNI	Centro para la Protección de la Infraestructura Nacional de Reino Unido
CSIRTUK	Combined Security Incident Response Team – United Kingdom
ERSCP	Equipo de Respuesta de Seguridad en el Control de Procesos
INC	Infraestructura Nacional Crítica
SCADA	Sistema de Control Supervisor y Adquisición de Datos
SCD	Sistemas de Control Distribuido
TI	Tecnología de la Información

B.3. TABLA DE EQUIVALENCIAS DE LA TRADUCCIÓN

Traducción al español	Original en inglés
TI: Tecnologías de la Información	IT: Information Tecnologies
RU: Responsable Único	SPA: Single Point of Accountability
SCI: Sistema de Control Industrial	ICS: Industrial Coltrol Systems
ROSI: Return On Security Investment	RIS: Retorno de la Inversión en Seguridad

* Los términos así señalados se definían en el original al final del apartado 2 "Resumen de "Mejorar la Concienciación y las Habilidades"".
[5] Original: *Risk Appetite*
[6] Original: *Likelihood*