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

SEGURIDAD EN EL CONTROL DE PROCESOS Y SCADA

Guía 2
Implementar una arquitectura segura

MARZO 2010

Edita:

NIPO: NIPO: 076-10-072-4

Tirada: 1000 ejemplares
Fecha de Edición: diciembre de 2010
Jess García con la colaboración de Carlos Fragoso han participado en la elaboración y modificación del presente documento y sus anexos.

LIMITACIÓN 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.

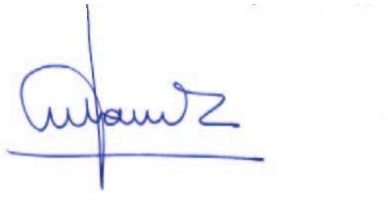
Una de las funciones más destacables del Centro Criptológico Nacional es la de elaborar y difundir normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los sistemas de las tecnologías de la información y las comunicaciones de la Administración, materializada en la existencia 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 Este documento traduce la siguiente guía:
   - 00754 - Process Control and SCADA Security Guide 2. Implement secure architecture
3. 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.
4. El CCN se adhiere a la cláusula de responsabilidad del CPNI sobre el contenido de la presente guía.

0.2. CAMBIOS EN EL CONTENIDO

5. 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.
6. 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.

7. Se han añadido los Anexos comunes a las guías CCN-STIC, con el siguiente contenido:
8. ¡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*" del documento original del CPNI.
   - A.3. Referencias en esta traducción: Contiene las nuevas referencias añadidas en este documento de traducción.
9. **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

10. 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:
11. Todos los párrafos han sido numerados.
12. El formato de algunos títulos, especialmente de cuarto nivel y sucesivos, ha sido adaptado.
13. 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

14. 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

15. Los sistemas de control de procesos y SCADA hacen uso y se están volviendo progresivamente más dependientes de las tecnologías de información (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.

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

17. 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.

18. 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.

19. 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

20. 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.

21. 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.

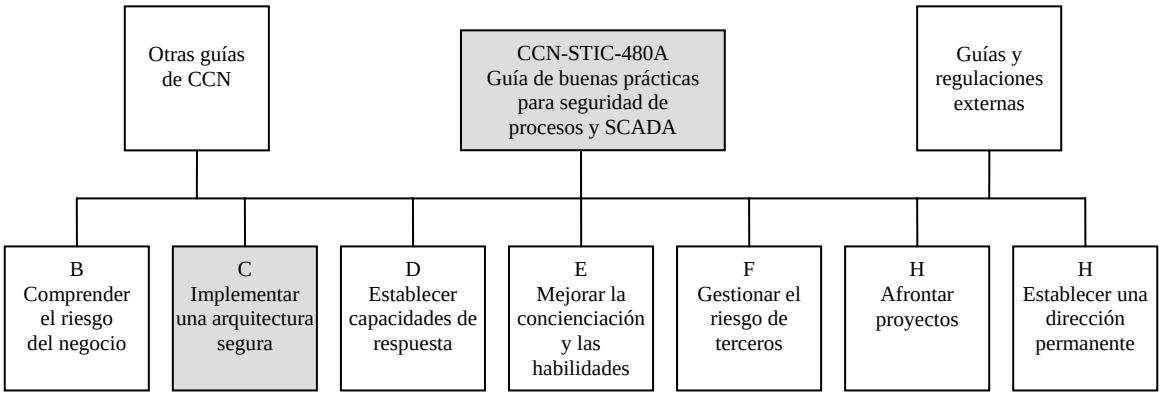


FIGURA 1: ***DÓNDE ENCAJA ESTA GUÍA DENTRO DEL MARCO DE BUENAS PRÁCTICAS***

22. 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.- 56][2]).

1.4. FINALIDAD DE ESTA GUÍA

23. 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 "**Implementar una arquitectura segura**" se basa en los fundamentos explicados en la guía de buenas prácticas y proporciona orientación para decidir una arquitectura de seguridad adecuada para los sistemas de control de procesos.

24. En esta guía no incluye soluciones, arquitecturas ni estándares técnicos detallados.

[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.- 57])

1.5. DESTINATARIOS

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

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

2. RESUMEN DE "IMPLEMENTAR UNA ARQUITECTURA SEGURA"

26. Dentro del marco de buenas prácticas, este módulo "Implementar una arquitectura segura" trata la definición e implementación de arquitecturas seguras para los sistemas de control.

27. Cuando se acomete la protección de un sistema de control, es fácil comenzar implementando medidas de seguridad evidentes, tales como la instalación de un cortafuegos o el despliegue de software antivirus. Sin embargo, es posible que este tipo de acciones no sean la mejor inversión en recursos valiosos, como los financieros y el personal, si se utilizan indiscriminadamente. Por lo tanto, se considera una buena práctica comprender plenamente el riesgo al que se enfrenta el sistema de control antes de seleccionar e implementar medidas de protección, a fin de que los recursos disponibles puedan ser utilizados de la mejor manera.

28. Para comprender estos riesgos, debe llevarse a cabo un estudio del riesgo que estudie los sistemas de control en estudio y examine las amenazas, los impactos y las vulnerabilidades a que se enfrentan dichos sistemas. Este asunto se describe con más detalle en el módulo "Comprender el riesgo del negocio" de este marco. El estudio del riesgo determina cuáles son las áreas más críticas a tratar y proporciona los datos para un proceso de selección que garantice que los recursos disponibles se utilicen en las áreas en las que supongan una mayor reducción del riesgo.

29. Una vez que el riesgo empresarial se comprenda bien, se pueden elegir una serie de medidas de reducción del riesgo (mejoras de seguridad) para construir una estructura global de seguridad para el sistema de control. En este contexto, el término "arquitectura" se utiliza en el sentido más amplio para cubrir los elementos humanos del sistema, así como las tecnologías. Una arquitectura de seguridad constará de una variedad de procesos, procedimientos y medidas de protección de la gestión y no sólo de un conjunto de soluciones técnicas.

30. Elegir medidas de de seguridad de control de procesos no es una ciencia exacta en absoluto y una solución no es válida para todo. Debido a la naturaleza relativamente inmadura del campo de la seguridad en el control de procesos y a la amplia variedad de

sistemas heredados que existen, no se trata solo de una simple cuestión de cumplir con las normas internacionales. Hay una serie de estándares industriales actualmente en desarrollo, pero estamos lejos de ser capaces de implementar un conjunto estándar de medidas de protección de seguridad. Se puede encontrar una lista de muestra de estas normas el Apéndice A.

31. Una vez que se selecciona una arquitectura segura, todo lo que necesita es implementarla. Esto puede sonar sencillo; sin embargo, el proceso de implementación de estas soluciones conlleva riesgos y puede causar interrupciones en el sistema si no se maneja con cuidado.

3. IMPLEMENTAR UNA ARQUITECTURA SEGURA

3.1. CONTEXTO DE ESTA SECCIÓN DENTRO DEL MARCO GENERAL

32. Esta sección utiliza los resultados de "Comprender el riesgo del negocio" para seleccionar un conjunto de medidas de seguridad apropiadas y construir una arquitectura segura que pueda ser implementada para proteger los sistemas de control.

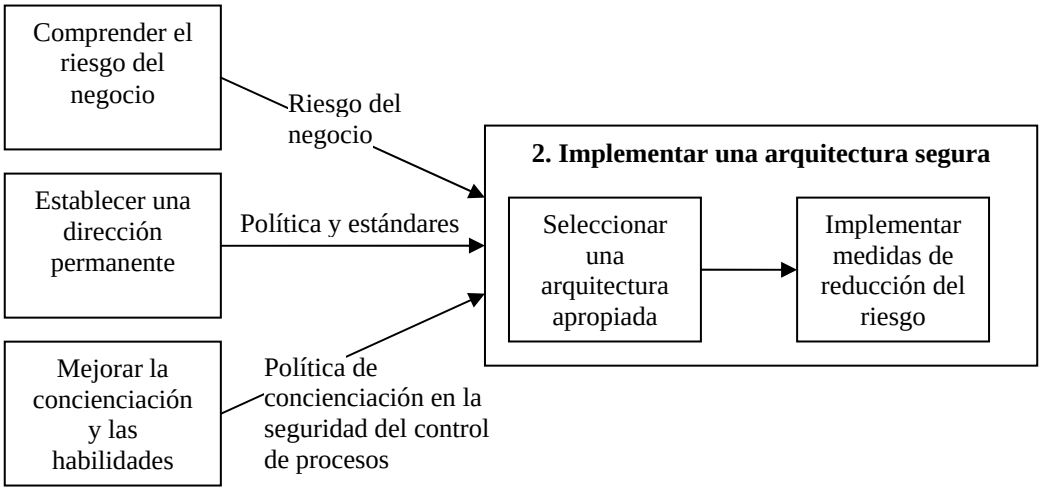


FIGURA 2: ***CÓMO ENCAJA "IMPLEMENTAR UNA ARQUITECTURA SEGURA" EN ESTE MARCO***

3.2. JUSTIFICACIÓN

33. Diseñar una arquitectura segura para un sistema de control puede ser un ejercicio difícil, ya que existen muchos tipos diferentes de sistemas y posibles soluciones, algunas de las cuales podrían no ser apropiadas para entorno del control de procesos. Dada la limitación de los recursos, es importante que el proceso de selección garantice que el nivel de protección esté en consonancia con los riesgos del negocio y no dependa para su defensa de una única medida de seguridad.

3.3. PRINCIPIOS DE BUENAS PRÁCTICAS

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

    - Seleccionar las medidas de seguridad adecuadas (basadas en los riesgos de negocio) para construir una arquitectura segura.
    - Implementar las medidas de reducción de riesgos seleccionadas.

3.4. ORIENTACIÓN SOBRE LAS BUENAS PRÁCTICAS

35. Este módulo cubre la definición e implementación de una arquitectura segura para los sistemas de control de procesos en estudio. Para ello hay que seleccionar un conjunto de medidas de protección adecuadas, que aborden eficazmente los riesgos de negocio identificados. A continuación se presenta una sinopsis a alto nivel del proceso que podría ser adoptarse para la selección e implementación de la arquitectura.

    - Comprender el riesgo del negocio.
    - Priorizar las vulnerabilidades de negocio en base al riesgo del negocio.
    - Mantener un equipo de trabajo de arquitectura.
    - Acordar la arquitectura objetivo
    - Definir un plan de implementación
    - Implementar las medidas de mejora de la seguridad

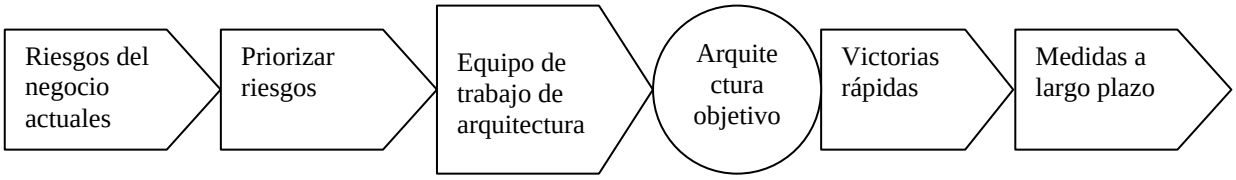


FIGURA 3: ***PROCESOS DE ALTO NIVEL PARA IMPLEMENTAR UNA ARQUITECTURA SEGURA***

36. Los elementos clave que deben considerarse en todo este proceso se describen en las secciones siguientes.

3.4.1. PRIORIZAR LAS VULNERABILIDADES SEGÚN EL RIESGO DEL NEGOCIO

37. Antes de decidir cualquier medida de seguridad es importante tener una buena comprensión del riesgo del negocio al que se enfrentan los sistemas de control. Al abordar la tarea de proteger un sistema de control es fácil comenzar implementando medidas de seguridad evidentes, como cortafuegos o software antivirus, sin tener en cuenta el contexto completo de riesgos. Este enfoque puede producir sistemas mal protegidos, al no considerar todas las medidas de protección como una arquitectura global. Se necesita una buena comprensión del riesgo del negocio para garantizar que las medidas de seguridad adecuadas son elegidas de manera que el sistema esté protegido

proporcionalmente al riesgo del negocio; es decir, sin demasiada protección (uso ineficiente de los recursos) ni demasiado poca (sistemas inseguros).

38. La comprensión del riesgo del negocio se centra en cuatro elementos clave que se enumeran a continuación y se describen con más detalle en el módulo "Comprender el riesgo del negocio".

    - Sistemas
    - Amenazas
    - Impactos
    - Vulnerabilidades

39. El resultado de este proceso es una comprensión de los sistemas clave, las amenazas que suponen y las vulnerabilidades que pueden ser explotadas. Éste es un requisito esencial previo para la definición de una arquitectura segura.

3.4.2. MANTENER UN EQUIPO DE TRABAJO PARA REDUCCIÓN DE RIESGOS

40. Una vez que hay una buena comprensión del riesgo del negocio, se puede proceder con la tarea principal de seleccionar posibles medidas de protección para hacer frente a cada una de las vulnerabilidades. A menudo la mejor manera de hacerlo es a través de un equipo de trabajo donde una serie de participantes, cada uno con distintos puntos de vista de los problemas, pueda contribuir a la selección de las medidas de protección adecuadas. La selección de una arquitectura no debe ser llevada a cabo por una persona aislada, ya que es probable que esa persona no tenga visibilidad de todo el sistema y el conocimiento de los problemas desde diferentes perspectivas.

41. Al formar un equipo para llevar a cabo este trabajo, se debe incluir (sin limitarse a):

    - Responsable Único (RU) de la seguridad del control de procesos.
    - Miembros del equipo de control de procesos.
    - Representantes empresariales.
    - Representantes del equipo de operaciones.
    - Representantes de seguridad TI.
    - Representantes de infraestructuras TI.
    - Representantes de aplicaciones TI.
    - Proveedores del control de procesos.

42. Una vez constituido, el equipo puede progresar con el examen de los factores de riesgo identificados y la selección de medidas apropiadas de reducción de riesgos.

3.4.3. ACORDAR LA ARQUITECTURA OBJETIVO

43. El objetivo fundamental del equipo de reducción de riesgos es considerar los factores de riesgo y las vulnerabilidades identificadas en el estudio del riesgo. Cada uno de los riesgos debe tenerse en cuenta y ser analizado.

44. Para cada riesgo hay tres tipos de acciones disponibles:

    - Aplicar medidas de reducción de riesgos (o medidas de mejora de la seguridad): el resto de esta sección trata la selección de estas medidas con más detalle.
    - Aplicar un plan de continuidad: este tema se trata en el módulo "Establecer capacidades de respuesta" y se puede localizar en el Apéndice A.
    - Tratar como riesgo residual (no tomar ninguna acción): en caso de que se decida tratar un riesgo como residual, se debe aceptar por la dirección y debe registrarse en un registro de riesgos. Los riesgos residuales deben revisarse regularmente.

3.4.4. FACTORES A CONSIDERAR AL ELEGIR MEDIDAS DE SEGURIDAD

45. Aunque la tarea de selección de medidas de reducción de riesgos parece simple, es a menudo más difícil de lo esperado debido a que la amplia gama de factores que influyen en la elección de cada medida introduce sus propias limitaciones. Los factores que deben considerarse pueden dividirse en seis áreas: coste, fuerza de protección, modelo de negocio, implementación, entrega y soluciones.

3.4.4.1. COSTE

46. El coste de implementar algunas de las medidas de seguridad puede ser relativamente barato con pequeños cambios en la configuración de los sistemas existentes o modificaciones menores a las actuales prácticas de trabajo. Sin embargo, la implementación de otras medidas de seguridad puede incluir un nuevo sistema o la creación de nuevas prácticas o procedimientos de trabajo que impliquen el gasto adicional de capital o ingresos.
47. La relación coste-eficacia de la solución debe ser considerada en función a la fuerza de la medida de protección.
48. Debe considerarse el coste de operación continuo de las medidas de protección adoptadas.

3.4.4.2. FUERZA DE PROTECCIÓN

49. Puede ser difícil determinar la fortaleza de una medida de protección; sin embargo, definir una escala simple que indique la fuerza y el coste de las medidas, puede simplificar el proceso de toma de decisiones.
50. La seguridad es tan fuerte como el eslabón más débil, y es importante que los elementos más débiles en la arquitectura de seguridad sean identificados y controlados.
51. Un principio básico para la elección de medidas de seguridad es elegir una arquitectura basada en una defensa en profundidad. Varias capas de medidas de seguridad son más efectivas que una sola medida que, si es comprometida, provocará que la arquitectura de seguridad sea ineficaz.

3.4.4.3. MODELO DE NEGOCIO

52. Puede ser necesario construir un modelo de negocio con el fin de obtener financiación para las mejoras de seguridad del sistema de control. Este modelo de negocio debería articular claramente los riesgos existentes y la necesidad de mejoras de seguridad. El resultado del módulo "Comprender el riesgo del negocio" puede ser útil para definir este modelo (véase el Apéndice A). Este modelo también debe mostrar claramente cómo las inversiones propuestas cambiarán el perfil de riesgo del negocio para los sistemas de control y debe contemplar el riesgo residual.

53. Los elementos clave del modelo de negocio son los siguientes:

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

54. Al construir un modelo de negocio suele ser útil articular el Retorno de la Inversión en Seguridad (RIS). Sin embargo, esto puede ser difícil de determinar en cifras debido a la falta de los datos disponibles de incidentes de seguridad en el control de procesos y SCADA.

55. Más información sobre cómo desarrollar un modelo detallado de negocio para seguridad puede encontrarse en la guía de NIST "*Guide to Industrial Control Systems (ICS)*" ([Ref.-16]).

3.4.4.4. IMPLEMENTACIÓN

56. Algunas medidas de seguridad son más fáciles de implementar que otras y por ello puede ser favorecidas por centros a corto plazo. Por ejemplo, desconectar un módem de una línea telefónica cuando no está en uso proporciona una protección limitada, y es fácil de implementar.

57. La implementación de algunas medidas de seguridad llevan relativamente poco tiempo porque implican pequeños cambios en la configuración de los sistemas existentes o modificaciones menores en prácticas de trabajo existentes. Sin embargo, la implementación de otras medidas de seguridad mayores pueden implicar la implantación de un nuevo sistema o la creación de nuevas prácticas o procedimientos de trabajo.

58. Debe buscarse el asesoramiento de los proveedores para determinar el plan de implementación, pues algunas apoyarán determinadas configuraciones pero lo que funciona para uno, puede no funcionar para otro.

59. Hay que considerar qué pruebas de una solución de seguridad deben necesario antes de desplegarla en los sistemas de control de producción. Los ensayos adicionales aumentan los costes y los plazos de despliegue.

3.4.4.5. ENTREGA

60. La implementación de algunas medidas de seguridad pueden estar limitadas por los recursos disponibles en los campos financieros o de personal de cada centro.

61. Hay que considerar quién será el responsable de la implementación de las medidas de seguridad. En particular, se debe identificar qué medidas requerirán la participación de los miembros del personal de control de procesos y si el personal necesario tendrá disponible el tiempo necesario.

62. Una organización debe tener en cuenta tanto las medidas de impacto rápido como las de largo plazo al seleccionar la arquitectura adecuada y el plan de implementación.

63. Al considerar las medidas de seguridad no hay que olvidar las necesidades de formación del personal y el soporte continuo y el mantenimiento. Puede suponer un coste financiero, y a menudo puede introducir el requisito de acceso remoto o la necesidad de actualización de hardware o software.

3.4.4.6. SOLUCIONES

64. Las medidas de reducción del riesgo en la arquitectura deben considerarse como un todo (ej., un conjunto de medidas y no solo soluciones puntuales).

65. Siempre que sea posible, hay que utilizar soluciones estándar que ya estén disponibles con el objetivo común de reducir al máximo el coste y la complejidad y lograr otros beneficios tales como:

    - **Reutilización de soluciones:** las soluciones probadas deber reutilizarse cuando sea posible.
    - **Estándar de calidad conocido:** la reutilización de una solución garantiza que se obtiene el mismo nivel de calidad en distintas partes del sistema de control de procesos o en distintos centros.
    - **Mayor facilidad de gestión:** si los problemas y riesgos se manejan de la misma manera, las respuestas a incidentes será más fácil de gestionar, pues la misma solución se puede aplicar a todos los sistemas de control de procesos que han utilizado el mismo enfoque.
    - **Economías de escala:** el uso de un determinado producto o proveedor en toda la organización puede dar como resultado un mayor poder de adquisición e influenciar sobre algunas mejoras en el diseño de la seguridad.
    - **Habilidades y experiencia:** la reutilización de aproximaciones de seguridad probadas en sistemas de control permite a las organizaciones limitar el desarrollo y la formación necesarios para apoyar las medidas de seguridad. El soporte subcontratado también puede reducir los gastos de mantenimiento.

66. Hay que considerar la posibilidad de adoptar soluciones aprobadas por el proveedor del sistema de control. Estas soluciones suelen haber sufrido una integración detallada y una acreditación por el mismo proveedor. Hay que buscar la garantía del vendedor para estas pruebas y su acreditación.

67. La selección de las medidas de seguridad debería basarse en el riesgo. No tiene sentido invertir en una medida de seguridad fuerte y costosa para una amenaza de bajo riesgo o impacto mínimo cuando la inversión podría ser mejor aprovechada en otros lugares.

68. Siempre que sea posible, utilizar protocolos de comunicación *firewall-friendly*. Usar protocolos que no sean *firewall-friendly* (por ejemplo OPC[4]) implica que las regla del cortafuegos no pueden ser configuradas en detalle.

69. La selección de una arquitectura de seguridad no se basa sólo en medidas técnicas; los procesos asociados y los requisitos de procedimiento y gestión también debe ser considerados.

70. Siempre que sea posible, hay intentar utilizar servicios y soluciones ya disponibles, como las proporcionadas por el departamento TI. Las soluciones pueden necesitar ser adaptadas al entorno operativo de los sistemas de control, por ejemplo el despliegue gradual de las actualizaciones de antivirus.

71. Al elaborar las posibles medidas de seguridad, desarrollar una serie de opciones distintas, con fuerzas distintas o posiblemente costes distintos. Esto ayudará al proceso de toma de decisión financiera.

72. Cuando los servicios no estén disponibles en la empresa, considerar la subcontrata a terceros. Ejemplos de los posibles servicios externos son:

    - Administración y monitorización del cortafuegos.
    - Administración y monitorización de las redes y las telecomunicaciones (tráfico).
    - Administración y monitorización de las infraestructuras (equipos de comunicaciones).
    - Administración y monitorización de los servidores.

73. Más detalles sobre la contratación externa se pueden encontrar en la guía CPNI, "*Good Practice Guide Outsourcing: Security Governance Framework for IT Managed Service Provision*" ([Ref.- 10]). Esta guía es un documento general y no es específico de sistemas de control de procesos y SCADA.

74. Las medidas de seguridad pueden necesitar algún tiempo para ser implementadas (ej. rediseñar la red e implementar el cortafuegos). Considerar la posibilidad de medidas urgentes simples y de bajo coste que puedan proporcionar alguna protección a corto plazo.

75. Es probable que haya un número de medidas de seguridad relativamente simples que puedan aplicarse rápidamente y entre los ejemplos se incluyen:

    - Mejora de la configuración de los sistemas existentes
    - Protección antivirus
    - Reforzar los controles de acceso
    - Capacidad de copia de seguridad y restauración
    - Seguridad física
    - Eliminación de conexiones no utilizadas

[4] La definición de Wikipedia de OPC-OLE (*Object-Linking and Embedding*) para el control de procesos. La norma específica la comunicación de datos en tiempo real entre dispositivos de diferentes fabricantes.

3.4.5. LISTA DE MEDIDAS DE REDUCCIÓN DE RIESGOS

76. Una vez se ha identificado una arquitectura de seguridad objetivo, hay que considerar la siguiente lista de comprobación para verificar su completitud. Esta lista sólo cubre las secciones de alto nivel que figuran en el documento "CCN-STIC-480A Seguridad en el Control de Procesos y SCADA - Guía de Buenas Prácticas" ([Ref.- 58][5]).

- Arquitectura de la red
- Cortafuegos
- Acceso remoto
- Antivirus
- Correo electrónico y acceso a Internet
- Configuración de seguridad del sistema
- Copias de seguridad y recuperación
- Seguridad física
- Monitorización de los sistemas
- Redes inalámbricas
- Actualizaciones (parches de seguridad)
- Verificación de los antecedentes del personal
- Contraseñas y cuentas
- Documentos del entorno de seguridad
- Resistencia de la infraestructura e instalaciones
- Gestión de vulnerabilidades
- Altas y bajas de usuarios
- Gestión del cambio
- Pruebas de seguridad
- Procedimientos de conexión de dispositivos

77. Hay una variedad de guías disponibles que exploran algunos de estos temas con más detalle, como:

- Best Practice Guide on Firewall Deployment for SCADA and Process Control Networks ([Ref.- 44])
- Good Practice Guide Outsourcing: Security Governance Framework for IT Managed Service Provision ([Ref.- 45])
- Good Practice Guide Patch Management ([Ref.- 46])
- Best Practice Guide Commercially Available Penetration Testing ([Ref.- 47])
- A Good Practice Guide on Pre-Employment Screening ([Ref.- 48])

[5] [Ref.- 6]

- CPNI guide on Personnel Security Measures ([Ref.- 49])
- Recommended Practices Guide for Securing ZigBee Wireless Networks in Process Control System Environments ([Ref.- 50])
- Securing WLANs using 802,11i ([Ref.- 51])
- Using Operational Security (OPSEC) to support a Cyber Security Culture in Control Systems Environments ([Ref.- 52])
- Cyber Security Procurement Language for Control Systems ([Ref.- 53])
- NERC Critical Infrastructure Protection (CIP) ([Ref.- 54])
- DHS Catalog of Control System Security Requirements ([Ref.- 55])
- NIST Guide to Industrial Control (ICS) Systems ([Ref.- 43])
- ISA SP99, Manufacturing and Control Systems Security ([Ref.- 19])

3.4.6. ACORDAR EL PLAN DE IMPLEMENTACIÓN

78. Una vez se ha acordado, presupuestado y financiado una arquitectura de seguridad, la siguiente tarea es definir el plan de implementación. Puede sonar simple, pero la aplicación de las mejoras de seguridad puede ser compleja en un entorno de sistemas de control y puede existir un riesgo significativo de interrupción del sistema provocada por la implementación de las medidas de reducción de riesgos. Es necesaria una planificación cuidadosa para reducir al mínimo el riesgo de interrupción del funcionamiento de los sistemas, y deben realizarse pruebas de despliegue antes de aplicar las medidas en el entorno productivo. También deben incluirse planes de marcha atrás en los planes de implementación, por si se encuentran problemas.

79. Los factores a considerar al planear la implementación son:

- **Priorización de los sistemas:** Los sistemas más críticos deben abordarse antes de los sistemas menos críticos.
- **Costes:** Puede que no sea posible desplegar todas las medidas de reducción de riesgos al mismo tiempo debido a restricciones de presupuesto. En este caso, deben considerarse medidas de seguridad cautelares.
- **Disponibilidad de recursos:** El personal necesario para aplicar las medidas de reducción de riesgos es a menudo muy escaso. Normalmente, hay poco personal con el perfil adecuado y con frecuencia son necesarios para realizar otras tareas. En consecuencia, el plan de implementación a menudo se ve afectado por la disponibilidad de los recursos adecuados.
- **Límite de la tasa de cambio:** Hay un límite a la cantidad de cambios que las empresas pueden asumir a la vez. A fin de mantener un bajo riesgo y un despliegue ordenado es importante que el plan de ejecución no sea demasiado agresivo.
- **Enfoque por etapas:** La implementación de las medidas de reducción de riesgos puede ser llevada a cabo durante un largo período de tiempo. Para planes grandes o complejos, debe considerarse un enfoque por etapas para minimizar el riesgo de los problemas de implementación.

- **Dependencias:** El plan de implementación debería considerar todas las dependencias identificadas. Algunas ya se han mencionado (ej., los recursos), pero puede que algunas medidas de reducción de riesgos deban ser aplicadas antes que otras. Un ejemplo podría ser la eliminación de los módems, que puede depender de que se establezca primero un medio alternativo de acceso remoto.
- **Plan de formación:** El plan de implementación debería abarcar todos los requisitos para la formación. No se debe incluir sólo a los técnicos implicados, sino también al personal de apoyo y mantenimiento y todos los usuarios y operadores de los sistemas.
- **Plan de comunicación y concienciación:** El plan de implementación debe incluir el plan de comunicación y los elementos de concienciación necesarios para informar a las partes pertinentes de los cambios que estén teniendo lugar.
- **Desarrollo y pruebas del procedimiento:** El plan de implementación debe incluir también el desarrollo de todos los procedimientos asociados que apoyen a las medidas de reducción de riesgos. Cabe señalar que no se trata sólo de escribir y publicar estos procedimientos; a menudo una cantidad significativa de esfuerzo es necesaria para incluirlos en las actividades del día a día.
- **Pruebas:** El plan de implementación debe incluir todos los elementos relevantes de las pruebas. Esto incluye pruebas de integración, de despliegue y garantizar que las medidas se han aplicado correctamente. Puede realizarse a través de una auditoría formal de seguridad o de una revisión tras la implementación.

3.4.7. IMPLEMENTAR LAS MEDIDAS DE MEJORA DE LA SEGURIDAD

80. Una vez se ha completado, revisado y aceptado el plan de implementación se puede proceder a la implementación de las medidas de reducción de riesgos. A lo largo del proceso de implementación hay una serie de áreas a tener en cuenta:

    - **Control de cambios**: Todos los cambios en los sistemas de control deben llevarse a cabo bajo los sistemas de control de cambios apropiados. Los cambios pueden afectar tanto a los sistemas de control como a los sistemas TI. Al bajar en la cadena de valores, los cambios pueden necesitar ser gestionados bajo diferentes sistemas de cambios, como los sistemas de planta y los sistemas TI.

      Conforme se realizan los cambios, los sistemas de control de cambios deben garantizar que los diagramas del sistema, el inventario y el estudio del riesgo se actualizan. Si los procesos de cambio no garantizan que se realizan estas actualizaciones, se deberían llevar a cabo controles para garantizar que toda la información esté actualizada. También debería considerarse modificar estos procesos para garantizar que la información del sistema esté siempre actualizada.
    - **Revisiones posteriores a la implementación**: Una vez que las medidas de reducción del riesgo se implementen, debe garantizarse que las medidas han sido desplegadas conforme al diseño de la arquitectura de seguridad. Puede realizarse de una variedad de maneras, desde una lista de comprobación a una revisión completa de seguridad o una auditoría. Sólo deberían hacerse pruebas de penetración bajo estrictas condiciones (ej, apagados de plantas), pues no es raro que este tipo de pruebas produzcan apagados de los sistemas de control y corrompan controladores de proceso de plantas.

- **Plan de comunicación y concienciación** En todo el proceso de implementación es importante realizar las correspondientes comunicaciones. Así se garantiza que todas las partes interesadas son conscientes de la situación y la evolución más recientes de la implementación del proyecto.

81. La tarea de proteger el control de procesos no se acaba cuando todas las medidas de reducción de riesgos se han implementado para formar la arquitectura de seguridad completa. Esto es solo un hito en el ciclo de vida de la seguridad de los sistemas de control. Hay una tarea permanente para garantizar que los sistemas de control están adecuadamente protegidos en el futuro. Esto implica:

    - Mantener la política, normas y procesos actualizados con las amenazas actuales.
    - Garantizar permanentemente que los sistemas de control cumplen la política y los estándares de seguridad.
    - Asegurar que todos los ingenieros, usuarios y administradores son conscientes de la seguridad e implementan los procesos y procedimientos de forma segura.
    - Garantizar una capacidad respuesta adecuada para reaccionar ante los cambios en las amenazas a la seguridad.
    - Asegurar que el riesgo derivado de colaboradores es gestionado.

82. Deberían llevarse a cabo auditorias periódicas para garantizar que el riesgo se gestiona activamente y que se siguen los procesos y procedimientos que se han establecido. Más consejos sobre la gestión de riesgo pueden encontrarse en el módulo “Comprender el riesgo del negocio” de este marco.

83. Estas tareas se detallan en el resto de este marco de buenas prácticas.

4. AGRADECIMIENTOS

PA and CPNI agradecen 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[6] 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

[6] 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*".

Section 3.4.2

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

Section 3.4.5

[Ref.- 44] Best Practice Guide on Firewall Deployment for SCADA and Process Control Networks,
www.cpni.gov.uk/Docs/re-20050223-00157.pdf

[Ref.- 45] Good Practice Guide Outsourcing: Security Governance Framework for IT Managed Service Provision,
www.cpni.gov.uk/Docs/re-20060802-00524.pdf

[Ref.- 46] Good Practice Guide Patch Management,
www.cpni.gov.uk/Docs/re-20061024-00719.pdf

[Ref.- 47] Best Practice Guide Commercially Available Penetration Testing,
www.cpni.gov.uk/Docs/re-20060508-00338.pdf

[Ref.- 48] A Good Practice Guide on Pre-Employment Screening,
www.cpni.gov.uk/Products/bestpractice/3351.aspx

[Ref.- 49] CPNI Personnel Security measures,
www.cpni.gov.uk/ProtectingYourAssets/personnelSecurity.aspx

[Ref.- 50] 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.- 51] Securing WLANs using 802,11i –
http://csrp.inl.gov/

[Ref.- 52] Using Operational Security (OPSEC) to support a Cyber Security Culture in Control Systems Environments
http://csrp.inl.gov/Documents/OpSec%20Rec%20Practice.pdf

[Ref.- 53] Cyber Security Procurement Language for Control Systems
www.msisac.org/scada/documents/12July07_SCADA_procurement.pdf

[Ref.- 54] NERC Critical Infrastructure Protection (CIP)
www.nerc.com/~filez/standards/Cyber-Security-Permanent.html

[Ref.- 55] DHS Catalog of Control System Security Requirements
www.us-cert.gov/control_systems/pdf/Catalog_of_Control_Systems_Security_Recommendations.pdf

A.3. REFERENCIAS EN ESTA TRADUCCIÓN

[Ref.- 56] Portal de CCN-CERT
https://www.ccn-cern.cni.es

[Ref.- 57] CCN-STIC-480 Seguridad en sistemas SCADA

[Ref.- 58] CCN-STIC-480A Seguridad en el control de procesos y SCADA
Guía de buenas prácticas

[Ref.- 59] CCN-STIC-480B Seguridad en el control de procesos y SCADA
Guía 1: Comprender el riesgo del negocio

[Ref.- 60] CCN-STIC-480C Seguridad en el control de procesos y SCADA
Guía 2: Implementar una arquitectura segura

[Ref.- 61] CCN-STIC-480D Seguridad en el control de procesos y SCADA
Guía 3: Establecer capacidades de respuesta

[Ref.- 62] CCN-STIC-480E Seguridad en el control de procesos y SCADA
Guía 4: Mejorar la concienciación y las habilidades

[Ref.- 63] CCN-STIC-480F Seguridad en el control de procesos y SCADA
Guía 5: Gestionar el riesgo de terceros

[Ref.- 64] CCN-STIC-480G Seguridad en el control de procesos y SCADA
Guía 6: Afrontar proyectos

[Ref.- 65] CCN-STIC-480H Seguridad en el control de procesos y SCADA
Guía 7: Establecer una dirección permanente

[Ref.- 66]

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*[7]	Nivel de riesgo, utilizado para determinar lo aceptable que puede ser un riesgo.
Probabilidad*[8]	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 “Implementar una arquitectura segura””.
[7] Original: *Risk Appetite*
[8] Original: *Likelihood*