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

SEGURIDAD EN EL CONTROL DE PROCESOS Y SCADA

Guía 6
Afrontar proyectos

MARZO 2009

Edita:

MINISTERIO DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

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.

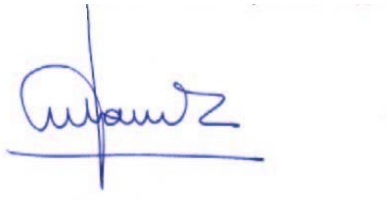
Una de las funciones más destacables del Centro Criptológico Nacional es la de elaborar y difundir normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los sistemas de las tecnologías de la información y las comunicaciones de la Administración, materializada en la existencia 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:
   - 00758 - Process Control and SCADA Security Guide 6. Engage projects
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 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.

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 imagen (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 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.

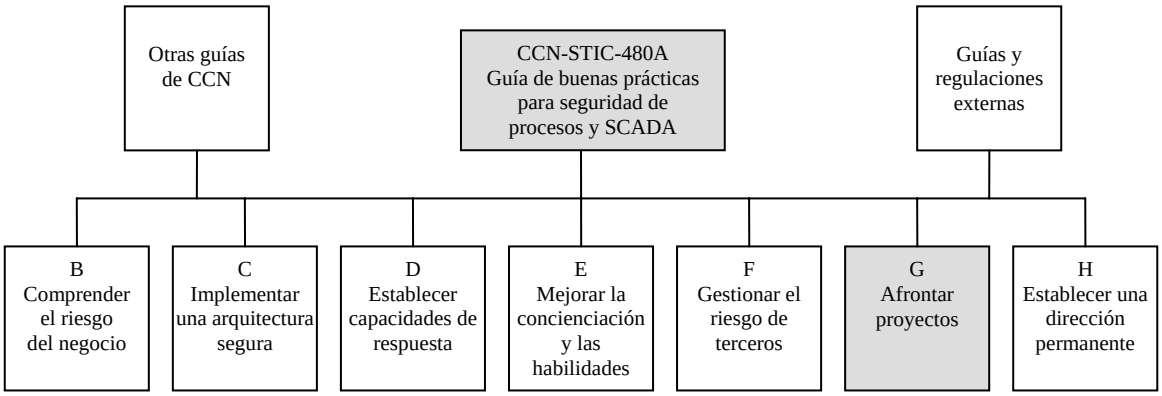


Figura 1: ***Dónde encaja esta guía dentro del marco de buenas prácticas***

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 "**Afrontar proyectos**" se basa en los fundamentos explicados en la guía de buenas prácticas y proporciona orientación de buenas prácticas sobre cómo incluir consideraciones de seguridad en los proyectos de seguridad en control de procesos.

25. Esta guía no proporciona requisitos detallados de seguridad de control de procesos pues éstos varían de un sistema a otro.

[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 del control de procesos, SCADA y sistemas de automatización industrial, incluyendo:

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

2. RESUMEN DE "AFRONTAR PROYECTOS"

27. Los sistemas de control de procesos suelen instalarse con la expectativa de una larga vida útil y unos cambios mínimos durante su vida. Sin embargo decir esto para todos los sistemas de control existentes es probablemente una generalización excesiva. En muchas organizaciones hay a menudo algunos procesos en marcha relacionados con los sistemas de control de procesos, cualquiera de los cuales puede tener implicaciones de seguridad.

28. Proyectos como nuevos sistemas de control, cambios en los sistemas de control o TI, actualizaciones, el desarrollo de información sobre la gestión de sistemas y la introducción de nuevas conexiones conllevan un riesgo de seguridad para el control de procesos y deben ser sometidos a una evaluación de riesgos.

29. Una vez que el sistema ha sido estudiado, cualquier proyecto que pueda afectarlo debe ser afrontado para que incorpore la seguridad desde sus primeras etapas. Cualquier nuevo sistema en un centro de nueva creación debería incluir requisitos de seguridad en los procesos de diseño y construcción desde la primera etapa. El cumplimiento de estos requisitos se debe asegurar en todo el ciclo vida del proyecto.

30. Las cuestiones de seguridad en el control de procesos, a menudo son relegadas a las fases posteriores de los proyectos, y es probable que en estos casos una decisión sobre las posibles opciones adoptadas en las primeras fases no considere las implicaciones de seguridad. Esto significa que el equipo del proyecto está omitiendo un componente vital que sin duda impactará en tiempo y recursos en una etapa posterior, y, más importante, puede reducir la eficacia global del marco de seguridad.

31. Implementar medidas de protección en los sistemas, es bastante más difícil y costoso de hacer una vez que los sistemas han sido desarrollados y desplegados. Es más importante aún el hecho de que implantar medidas de seguridad en un sistema vivo resulta a menudo menos eficaz. Es más efectivo combatir los riesgos de seguridad integrando medidas de protección en los procesos de desarrollo del proyecto en una etapa temprana, evita excesos y es normalmente menos costoso.

3. REALIZACIÓN DE PROYECTOS

3.1. CONTEXTO DE ESTA SECCIÓN DENTRO DEL MARCO GENERAL

32. Esta guía toma otros elementos del marco de buenas prácticas, relacionados con las políticas y las normas, la comprensión del riesgo y las observaciones sobre terceros, y los incorpora en proceso de realización de proyectos de seguridad en control de procesos.

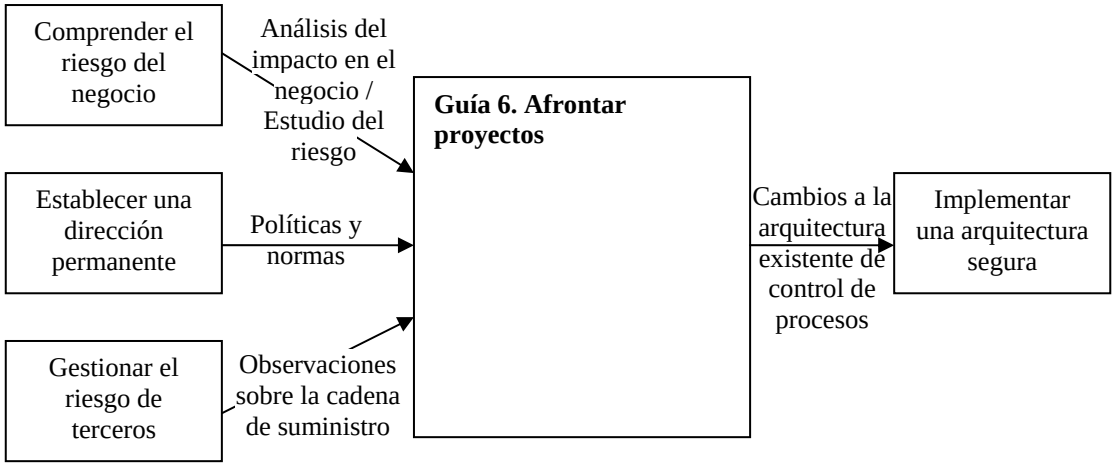


Figura 2: ***Cómo encaja "Afrontar Proyectos" en este marco***

3.2. JUSTIFICACIÓN

33. Incluir la seguridad en los sistemas de control de procesos desde las primeras etapas integrando requisitos de la calidad de la seguridad en los procesos de diseño y construcción de la organización. Implantar la seguridad en un sistema tras su construcción es mucho menos eficaz y por lo general más caro.

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.- 51]), son los siguientes:

- Identificar y afrontar todos los proyectos que tienen implicaciones en los sistemas de control de procesos en las primeras etapas de su desarrollo.
- Garantizar que se nombra un encargado (arquitecto) de seguridad como responsable único de la gestión de los riesgos de seguridad durante el ciclo de vida completo del proyecto.
- Asegurar las cláusulas y las especificaciones estándar de seguridad están incluidas en todos los contratos de adquisición.
- Incluir requisitos de seguridad en el diseño y la especificación de los proyectos y garantizar que se fijan todas las políticas y normas de seguridad adecuadas.

- Llevar a cabo revisiones de seguridad en todo el ciclo de vida de desarrollo del proyecto, por ejemplo, al mismo tiempo que los controles de las condiciones de trabajo.
- Planear pruebas de seguridad en puntos clave del ciclo de vida (ej., oferta, puesta en marcha, la fabricación, pruebas de aceptación, y durante las operaciones).

3.4. ORIENTACIÓN SOBRE LAS BUENAS PRÁCTICAS

3.4.1. IDENTIFICAR Y AFRONTAR TODOS LOS PROYECTOS DE CONTROL DE PROCESOS

35. Para gestionar eficazmente los riesgos de seguridad en el control de procesos relacionados con los proyectos es necesario tener una buena visibilidad de qué proyectos están planificados y en marcha. En muchas organizaciones puede ser difícil determinar qué proyectos se planifican y están en curso y a menudo se identifican tarde para incorporar los requisitos de seguridad.
36. Deberían establecerse procesos que permitan conocer en una etapa temprana cualquier proyecto que pueda tener implicaciones en la seguridad del control de procesos. Debe mantenerse un registro o inventario de proyectos que impliquen elementos del control de procesos. Así se garantiza que el desarrollo del proyecto pueda ser modificado para asegurar que todos los proyectos incorporan la seguridad en el proceso de desarrollo.
37. Ejemplo de tipos de proyectos que podrían tener implicaciones de seguridad en el control de procesos incluyen:
    - Actualizaciones de cortafuegos en la empresa
    - Actualización o cambios de la infraestructura
    - Conexión de la red de trabajo a Internet
    - **Conexión de la red de trabajo a la red de control de procesos**
    - Actualizaciones de sistemas de control
    - Nuevos sistemas de control
    - Cambios en los procedimientos operativos
    - Actualizaciones de los sistemas de información / control de versiones
    - Implementación de Sistemas de Información para la Administración (SIA[4]), Sistemas de Ejecución de Fabricación (MES[5]), Sistemas de Informes de Producción o históricos de procesos.
    - Conexión con terceros
    - Cambio del código embebido (*firmware*).

[4] Original: MIS: *Management Information System*
[5] Original: MES: *Manufacturing Execution System*

3.4.2. AFRONTAR UNA ARQUITECTURA DE SEGURIDAD

38. Los proyectos con implicaciones de seguridad en el control de procesos deberían nombrar un encargado (arquitecto) de seguridad que sea responsable de las cuestiones de seguridad en todo el ciclo de vida del proyecto. Este arquitecto de seguridad sólo trabajaría a tiempo parcial en el proyecto y asesoraría sobre la forma en que el proyecto debe incorporar los requisitos de seguridad, y proporcionaría garantías de que el sistema entregado está protegido adecuadamente.

39. Tener un experto que pueda traducir las necesidades de seguridad de las políticas y normas de forma que se puedan incorporar en el proyecto puede ser una decisión muy rentable. Integrar la calidad y la contabilidad desde el punto de vista de seguridad en el diseño y el ciclo de vida del proyecto garantiza que los requisitos de seguridad en control de procesos no se olvidan y que los proyectos son conscientes de las implicaciones de seguridad de las decisiones que se toman.

3.4.3. INTEGRAR LOS REQUISITOS DE SEGURIDAD EN LOS CONTRATOS DE ADQUISICIÓN

40. Las cláusulas de seguridad a menudo son dejadas fuera de los contratos porque están mal consideradas y a veces son inadecuadas; en la prisa por definir los requisitos de seguridad, algunas especificaciones realizadas en el entorno TI de la empresa son “trazadas” con poca reflexión. También es común que las cuestiones de seguridad no se consideren con suficiente antelación para ser incorporadas en los contratos de adquisición.

41. Hay que definir los requisitos de seguridad del control de procesos en una etapa temprana y garantizar que se incluyen cláusulas en los contratos. Así se garantiza que el proveedor considera la seguridad como uno de los requisitos fundamentales para el sistema y, por tanto, debe ser entregado como parte del sistema.

42. Los errores de código de *software* pueden crear vulnerabilidades, tanto en los sistemas de control como en las aplicaciones TI normales. Incluir que se programa pensando en la seguridad como una cláusula en un contrato de adquisición es necesario para garantizar que el código esté bien desarrollado y es probado.

43. Los contratos de adquisición deben referirse a las políticas o normas (internas o de la industria) que deben cumplirse en el diseño y la implementación del sistema.

44. Los contratos también deben contener suficiente detalle de los requisitos de seguridad que se esperan en el sistema entregado. Sin embargo, es importante establecer un nivel de detalle apropiado para que los requisitos no sean demasiado preceptivos. El contrato debe indicar claramente qué requisitos son obligatorios y cuales son opcionales. Para más orientación sobre qué cláusulas de seguridad deben considerarse en los contratos, consultar el elemento del marco “CCN-STIC-480F Gestionar el riesgo de terceros” ([Ref.- 56]).

45. Además de establecer los requisitos de seguridad, los contratos de adquisición deben indicar claramente las expectativas de garantía de seguridad en todo el ciclo de vida. Ejemplos de estas expectativas son las siguientes:

    - Revisiones de seguridad del diseño
    - Revisiones de la seguridad del código

- Pruebas de seguridad
- Sustitución segura de elementos defectuosos que contenga datos (ej., discos duros).

46. Muchos proveedores se quejan que sus usuarios los critican por no proveer sistemas seguros. Sin embargo, esos requisitos de seguridad rara vez se incluyen en las especificaciones del sistema y los contratos de adquisición. Al incluir medidas de seguridad significativas en las propuestas que no están en los requisitos de diseño, un proveedor puede poner su propuesta en desventaja desde el punto de vista del coste y ser perjudicial en el proceso de selección. Si se especifican claramente los requisitos de seguridad en los contratos de adquisición, los usuarios pueden informar de sus requisitos de seguridad y garantizar la igualdad de condiciones a los proveedores que compiten por el negocio. La seguridad en los sistemas de control de procesos debe ser considerada como un requisito básico para todos los sistemas, no como una opción extra.
47. Más información sobre los requisitos de seguridad puede encontrarse en el documento "Cyber Segurity Procurement Language for Control Systems" del Laboratorio Nacional de Idaho ([Ref.- 43]), así como en el documento "Catalog of Control System Security Requirements" elaborado por el DHS ([Ref.- 19]), referenciados en el apéndice A.

3.4.4. INCLUIR LOS REQUISITOS DE SEGURIDAD EN LAS ESPECIFICACIONES DE DISEÑO

48. Integrar la seguridad en el proceso de diseño y construcción durante la fase de proyecto parece obvio, pero es a menudo pasado por alto u omitido por muchas organizaciones. Una inversión (relativamente pequeña) en la fase de proyecto será mucho más barata que integrar la seguridad más tarde, o enfrentarse a repeticiones y cambios de diseño que afecten a todo el sistema.
49. Los requisitos de seguridad no deben ser considerados distintos a cualquier otro requisito funcional. Deben estar expresados claramente e incluidos en cualquier especificación de diseño funcional.
50. Es importante que los requisitos de seguridad para cualquier sistema se basen en el riesgo de negocio. Un sistema de bajo riesgo puede requerir menos protección que uno crítico o con riesgo mayor. Si no se considera el riesgo de negocio, existe el peligro de que un sistema pueda estar demasiado protegido (lo que sería un desperdicio de recursos que se habrían usado mejor en otros lugares) o que no lo esté suficientemente.
51. Para obtener una lista de cuestiones que deberían tenerse en cuenta al desarrollar los requisitos de seguridad del sistema, consultar las políticas y normas de la organización y el documento de este marco "CCN-STIC-480C Implementar Arquitectura Segura" ([Ref.- 53]).
52. Más información sobre los requisitos de seguridad pueden encontrarse en el documento "Cyber Segurity Procurement Language for Control Systems" del Laboratorio Nacional de Idaho ([Ref.- 43]), así como en el documento "Catalog of Control System Security Requirements" elaborado por el DHS ([Ref.- 19]), referenciados en el apéndice A.

3.4.5. REVISAR LA SEGURIDAD EN TODO EL CICLO DE VIDA DEL DESARROLLO

53. La seguridad es una parte importante en todo el ciclo de vida del proyecto, pero tiene más importancia en las primeras etapas. El siguiente diagrama muestra cómo los asuntos de seguridad deben considerarse en todo el ciclo de vida del desarrollo.

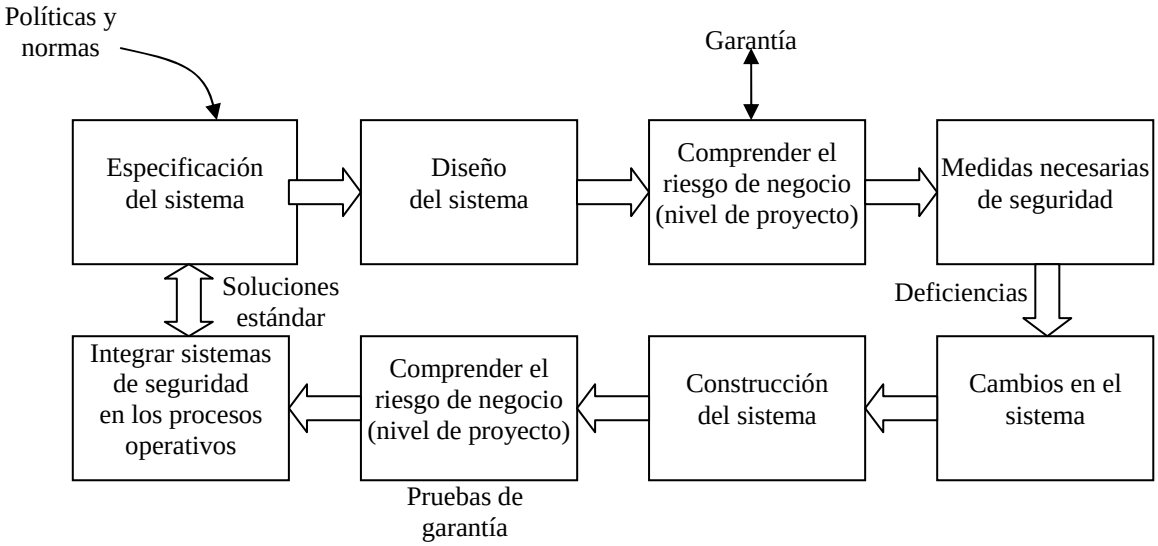


Figura 3: ***Seguridad en el ciclo de vida del desarrollo***

54. Las etapas clave en el ciclo de vida del desarrollo se describen en las secciones siguientes. Se pueden encontrar más recomendasciones sobre el ciclo de vida en el documento “Using Operational Security (OPSEC) to support a Cyber Security Culture in Control Systems Environments” (véase el apéndice A, [Ref.- 18]).

3.4.6. REVISIONES DE SEGURIDAD DEL DISEÑO DEL SISTEMA

55. Una vez que un proyecto ha alcanzado una etapa donde hay diseño de alto nivel y una arquitectura convenida, deberían revisarse las especificaciones y los requisitos de seguridad en el diseño. En esta etapa el sistema no existe, pero la revisión puede llevarse a cabo de forma similar a en los sistemas existentes, pero como un ejercicio sobre el papel. Se pueden encontrar más recomendaciones en el documento de este marco “CCN-STIC-480B Comprender el riesgo del negocio” ([Ref.- 52]). La revisión debe tratar de identificar las lagunas que existen entre el proyecto de diseño y los requisitos y especificaciones de seguridad, las políticas y las normas.

56. Un resultado clave de esta revisión debería ser la garantía de que el diseño está conforme a las políticas, normas, especificaciones y requisitos de seguridad. Otro resultado debería ser una lista de deficiencias y riesgos de seguridad, que deben revisarse para ser incorporados en el diseño mientras aún se esté a tiempo, o aceptando estas como riesgo residual.

57. Es posible que deban llevarse a cabo una serie de revisiones en las distintas etapas del ciclo de desarrollo. Dependerá de lo grande y complejo que sea el sistema y de si su aplicación se realiza por etapas. Cuando sea posible, estas revisiones deberían ser incorporadas o al menos compartir resultados con otras evaluaciones de sistemas que ya existan en el plan de ejecución, ej. la revisión de condiciones de trabajo, etc.

3.4.7. PRUEBAS DEL SISTEMA

58. Algunos aspectos de seguridad deben considerarse como parte del plan de pruebas global. En los proyectos de control de procesos, a menudo no se consideran las pruebas de seguridad hasta etapas muy tardías, o no se incluyen en absoluto. Las pruebas de seguridad encuentran a menudo vulnerabilidades inesperadas y es importante identificarlas en una etapa temprana del ciclo de vida.

59. Una vez que un sistema de control de procesos está en marcha, es muy difícil llevar a cabo pruebas de seguridad o de vulnerabilidad. Hay muchos incidentes documentados de pruebas de seguridad que han causado importantes incidentes de seguridad. En consecuencia se valora mucho realizar la mayor cantidad posible de pruebas antes de que un sistema entre en funcionamiento. Los resultados de estas pruebas pueden usarse en un proceso de gestión de vulnerabilidades para el sistema una vez que esté en marcha.

60. La planificación de las pruebas de seguridad debe comenzar al principio del proyecto y debe considerar una serie de áreas diferentes que se describen en las secciones siguientes.

61. Durante las diversas etapas de las pruebas, debe desarrollarse un documento base del sistema que ayudará a confirmar la seguridad del sistema según se aplica y a gestionar las vulnerabilidades en el futuro. Este documento debería incluir al menos:

    - Las direcciones IP
    - Los puertos, protocolos y servicios
    - Los proceso de ejecución en las máquinas
    - Los parámetros típicos de operación (ej, uso de CPU, ancho de banda de red, etc.)

3.4.7.1. PRUEBAS DE UNIDAD

62. Deben incluirse pruebas de seguridad en todo el ciclo de desarrollo del sistema. Cuando los sistemas se desarrollan por secciones o unidades, es probable que algunas pruebas de funcionamiento se lleven a cabo en esas unidades. Deberían planificarse pruebas de seguridad en esas pruebas de unidad para identificar cualquier problema en una etapa inicial, y para que puedan ser abordados lo bastante pronto en el ciclo de vida antes de que los problemas puedan causar un impacto significativo.

3.4.7.2. PRUEBAS DE SISTEMAS INTEGRADOS

63. Investigaciones recientes han puesto de relieve vulnerabilidades generalizadas en sistemas integrados, como controladores de bajo nivel, PLC y UTR[6]. Un ejemplo muy citado es el de una empresa de fabricación que sufrió una parada importante de sus operaciones cuando una exploración de seguridad autorizada rompió muchos de los PLC en su planta. Muchas vulnerabilidades conocidas podrían ser leves, pero algunas son graves y podrían tener como implicaciones de seguridad dependiendo de cómo sean usados los dispositivos.

64. Por lo tanto, se considera una buena práctica, obtener garantías de este tipo de dispositivos antes usarlos en producción. Hay algunas empresas que realizan pruebas de

[6] Original: RTU

seguridad de PLC (consulte al CCN-CERT para conocer algunas[7]), más detalles de las entidades que realizan este tipo de pruebas se pueden encontrar en el apéndice A.

65. En el momento en que se elabora esta guía no hay ningún estándar industrial para obtener estas garantías (aunque ISA está trabajando en ello) y no hay organismos acreditados para realizar estas pruebas. Sin embargo, están surgiendo herramientas de prueba enfocadas en las pruebas a nivel de controladores. Se recomienda como buena práctica que dichos dispositivos sean probados usando una de las herramientas disponibles antes de ser desplegados.

3.4.7.3. PRUEBAS DE ACEPTACIÓN EN FÁBRICA

66. Es una gran oportunidad para probar todo el sistema antes de que entre en funcionamiento (cuando la realización de nuevas pruebas se hará más difícil). Esta etapa se realiza normalmente en las instalaciones del proveedor y por lo general incluye una variedad de pruebas de aceptación que llevan a cabo el cliente o terceros autorizados (en nombre del cliente). Estas pruebas se basan normalmente en los requisitos y especificaciones funcionales definidos en las primeras etapas del proyecto. Si se han incorporado los requisitos de seguridad a los requisitos funcionales, las pruebas de seguridad deben incorporarse a las pruebas de aceptación. Una vez que el sistema haya pasado las pruebas de aceptación, resulta muy difícil hacer cambios en el sistema para corregir cualquier problema de seguridad.

67. Temas clave que deben considerarse para incluirlos en las pruebas de aceptación son:

- Configuración de seguridad
- Escaneado de vulnerabilidades en todo el sistema
- Pruebas de penetración
- Pruebas de las reglas del cortafuegos
- Pruebas de recuperación de fallos/desastres
- Pruebas de copias de seguridad
- Pruebas de parcheados
- Pruebas de actualización del antivirus
- Pruebas de acceso remoto
- Garantía de protección del sistema

3.4.7.4. PRUEBAS DE ACEPTACIÓN EN CENTRO DE PUESTA EN SERVICIO

68. Tras las pruebas de aceptación, el sistema es implementado en el entorno de producción y normalmente se llevan a cabo una serie de las pruebas de puesta en servicio para verificar que el sistema ha sido instalado y configurado correctamente.

[7] Original: MU Security and Wurldtech

69. Las pruebas de seguridad deben incluirse dentro de estas pruebas de puesta en servicio para confirmar que los mecanismos de seguridad también se han configurado correctamente.

70. Orientación adicional sobre los requisitos de pruebas se pueden encontrar en el documento “Cyber Security Procurement Language for Control Systems” elaborado por el Laboratorio Nacional de Idaho (véase [Ref.- 43] en el apéndice A).

3.4.8. ENTREGA DEL SISTEMA

71. Normalmente, un gran proyecto de desarrollo de sistema está gestionado por un equipo de proyecto dedicado que esta a menudo separado del equipo de operaciones que gestiona y mantiene el sistema una vez está operativo. Como parte del proceso de entrega del sistema al equipo de operaciones, todos los procesos y procedimientos asociados que se necesitan para monitorizar la seguridad del sistema deben ser finalizados e incorporados en las actividades habituales de la empresa. Ejemplos de estos procedimientos incluyen:

    - Vigilancia de los registros del sistema
    - Rutinas de mantenimiento
    - Administración y monitorización de los cortafuegos
    - Despliegue y garantía de los antivirus
    - Planes de respuesta y continuidad
    - Procedimientos de control de cambios
    - Pruebas de fallo
    - Procesos de parcheado (actualización de seguridad)
    - Aislamiento del sistema
    - Procedimientos de pérdida de visión
    - Garantía continuada (véase la guía "CCN-STIC-480B Comprender el riesgo del negocio" [Ref.- 52])
    - Confirmación de todo el *software* en los discos duros y el *firmware*
    - Documentación actualizada del sistema
    - Resultados de las pruebas de aceptación en fábrica y de puesta en servicio

72. Más recomendaciones sobre este tema se pueden encontrar en el documento “Using Operational Security (OPSEC) to support a Cyber Security Culture in Control Systems Environments” (véase el apéndice A, [Ref.- 18]).

3.4.9. BAJA

73. Al sustituir un equipo es esencial que su baja del servicio sea abordado adecuadamente. Muchos de estos sistemas contienen información sensible que podría ser de utilidad para una o varios grupos de amenazas como empresas competidoras, ladrones de identidad, delincuentes y terroristas. Los tipos de información incluyen nombres y direcciones del personal, contraseñas, cuentas de usuario, números de teléfono, información sobre el

producto, detalles de clientes, información protegida por la Ley de Protección de Datos[8], especificaciones técnicas, y datos químicos y biológicos. Se sabe que grupos terroristas han mostrado interés en los dos últimos ámbitos.

74. Los datos digitales deben ser sobrescritos varias veces con datos aleatorios para hacer que los datos originales sean irrecuperables en el soporte; esto debe hacerse en todos los datos y no sólo en la tabla de asignación de archivos. Cuando no se puedan sobrescribir, los datos deben ser borrados mediante desmagnetización con un campo magnético o destruido físicamente.

[8] Original: Data Protection Act

4. 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[9] 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

[9] 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 3.4.3

[Ref.- 43] Cyber Security Procurement Language for Control Systems
www.msisac.org/scada/documents/12July07_SCADA_procurement.pdf

Section 3.4.5

[Ref.- 44] Using Operational Security (OPSEC) to Support a Cyber Security Culture in Control Environments
http://csrp.inl.gov/Documents/Opsec%20Rec%20Practice.pdf

Section 3.4.7

[Ref.- 45] The Achilles Certification Program
www.wurldtech.com/index.php

[Ref.- 46] MU Security Industrial Control (MUSIC) Certification
www.musecurity.com/support/music.htm

Section 3.4.8

[Ref.- 47] Using Operational Security (OPSEC) to Support a Cyber Security Culture in Control Environments
http://csrp.inl.gov/Documents/Opsec%20Rec%20Practice.pdf

Section 3.4.9

[Ref.- 48] BS 8470:2006 Secure destruction of confidential material. Code of practice
www.bsi-global.com/en/Shop/Publication-Detail/?pid=000000000030127562

A.3. REFERENCIAS EN ESTA TRADUCCIÓN

[Ref.- 49] Portal de CCN-CERT
https://www.ccn-cert.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] CCN-STIC-403 Gestión de incidentes de seguridad

[Ref.- 60] CCN-STIC-406 Seguridad en redes inalámbricas

[Ref.- 61] CCN-STIC-418 Seguridad en Bluetooth

[Ref.- 62] CCN-STIC-303 Inspección STIC

[Ref.- 63] CCN-STIC-411 Modelo plan de Verificación STIC

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[10]	Nivel de riesgo, utilizado para determinar lo aceptable que puede ser un riesgo.
Probabilidad[11]	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
SIA	Sistemas de Información para la Administración
MES	*Manufacturing Execution System* Sistemas de Ejecución de Fabricación
PLC	Programmable Logic Controllers Controladores lógicos programables
UTR	Unidades de Terminal Remota

B.3. TABLA DE EQUIVALENCIAS DE LA TRADUCCIÓN

Traducción al español	Original en inglés
TI: Tecnologías de la Información	IT: Information Tecnologies

[10] Original: *Risk Appetite*
[11] Original: *Likelihood*

RU: Responsable Único	SPA: Single Point of Accountability
SCI: Sistema de Control Industrial	ICS: Industrial Coltrol Systems
RIS: Retorno de la Inversión en Seguridad	ROSI: Return On Security Investment
SIA: Sistemas de Información para la Administración	MIS: Management Information System
MES: Sistemas de Ejecución de Fabricación	MES: Manufacturing Execution System