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

SEGURIDAD EN EL CONTROL DE PROCESOS Y SCADA

Guía 7
Establecer una dirección permanente

MARZO 2010

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.

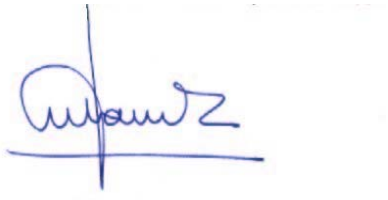
Una de las funciones más destacables del Centro Criptológico Nacional es la de elaborar y difundir normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los sistemas de las tecnologías de la información y las comunicaciones de la Administración, materializada en la existencia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

0. INTRODUCCIÓN A LA TRADUCCIÓN 5
0.1. ALCANCE DE ESTA TRADUCCIÓN 5
0.2. CAMBIOS EN EL CONTENIDO 5
0.3. CAMBIOS EN EL FORMATO 6
1. INTRODUCCIÓN 7
1.1. TERMINOLOGÍA 7
1.2. ANTECEDENTES 7
1.3. MARCO DE SEGURIDAD EN EL CONTROL DE PROCESOS 8
1.4. FINALIDAD DE ESTA GUÍA 8
1.5. DESTINATARIOS 9
2. RESUMEN DE "ESTABLECER UN DIRECCIÓN PERMANENTE" 9
3. ESTABLECER UN GRUPO DIRECTIVO 10
3.1. CONTEXTO DE ESTA SECCIÓN DENTRO DEL MARCO GENERAL 10
3.2. JUSTIFICACIÓN 10
3.3. PRINCIPIOS DE BUENAS PRÁCTICAS 11
3.4. ORIENTACIÓN SOBRE LAS BUENAS PRÁCTICAS 11
4. DESARROLLAR POLÍTICAS Y NORMAS 14
4.1. CONTEXTO DE ESTA SECCIÓN DENTRO DEL MARCO GENERAL 14
4.2. JUSTIFICACIÓN 15
4.3. PRINCIPIOS DE BUENAS PRÁCTICAS 15
4.4. ORIENTACIÓN SOBRE LAS BUENAS PRÁCTICAS 15
4.4.1. POLÍTICAS 17
4.4.2. NORMAS 18
4.4.3. ORIENTACIONES PARA LA IMPLEMENTACIÓN 19
4.4.4. NORMAS Y ORIENTACIONES DE REFERENCIA 19
5. GARANTIZAR EL CUMPLIMIENTO DE LAS POLÍTICAS Y NORMAS E INFORMAR A REGULADORES EXTERNOS 20
5.1. CONTEXTO DE ESTA SECCIÓN DENTRO DEL MARCO GENERAL 20
5.2. JUSTIFICACIÓN 21
5.3. PRINCIPIOS DE BUENAS PRÁCTICAS 21
5.4. ORIENTACIÓN SOBRE LAS BUENAS PRÁCTICAS 21
5.4.1. ¿QUÉ INFORMACIÓN SE REQUIERE, EN QUÉ DETALLE Y CUÁNDO? 22
5.4.2. ¿CÓMO Y QUIÉN DEBE RECOPILAR LA INFORMACIÓN? 22
5.4.3. ¿QUÉ IMPACTO TIENE EL INCUMPLIMIENTO EN LA EMPRESA? 23
6. ACTUALIZAR LAS POLÍTICAS Y LAS NORMAS 24
6.1. CONTEXTO DE ESTA SECCIÓN DENTRO DEL MARCO GENERAL 24
6.2. JUSTIFICACIÓN 25
6.3. PRINCIPIOS DE BUENAS PRÁCTICAS 25
6.4. ORIENTACIÓN SOBRE LAS BUENAS PRÁCTICAS 26
7. AGRADECIMIENTOS 27

ANEXOS

ANEXO A. REFERENCIAS 28
A.1. REFERENCIAS GENERALES SCADA 28
A.2. DOCUMENTOS Y PÁGINAS WEB DE REFERENCIA 30
A.3. REFERENCIAS EN ESTA TRADUCCIÓN 31
ANEXO B. GLOSARIO DE TÉRMINOS Y ABREVIATURAS 33
B.1. GLOSARIO DE TÉRMINOS 33
B.2. GLOSARIO DE SIGLAS 33
B.3. TABLA DE EQUIVALENCIAS DE LA TRADUCCIÓN 33

FIGURAS

FIGURA 1: DÓNDE ENCAJA ESTA GUÍA DENTRO DEL MARCO DE BUENAS PRÁCTICAS 8
FIGURA 2: ESTRUCTURA DEL DOCUMENTO "ESTABLECER UNA DIRECCIÓN PERMANENTE" 9
FIGURA 3: CÓMO ENCAJA "ESTABLECER UNA DIRECCIÓN PERMANENTE" EN ESTE MARCO 10
FIGURA 4: FUNCIÓN DEL GRUPO DE GOBIERNO 13
FIGURA 5: CÓMO ENCAJA "DESARROLLAR POLÍTICAS Y NORMAS" EN ESTE MARCO 14
FIGURA 6: RELACIÓN ENTRE LOS DOCUMENTOS DE POLÍTICAS, NORMAS Y ORIENTACIONES 16
FIGURA 7: CÓMO ENCAJA "ASEGURAR EL CUMPLIMIENTO DE LAS POLÍTICAS Y NORMAS" EN ESTE MARCO 21
FIGURA 8: CÓMO ENCAJA "ACTUALIZAR POLÍTICAS Y NORMAS" EN ESTE MARCO 25

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 (**¡Error! No se encuentra el origen de la referencia.**)
3. Este documento traduce la siguiente guía:
   - 00759 - Process Control and SCADA Security Guide 7. Establish ongoing governance
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 la salud, la seguridad y el medio ambiente.

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

1.3. MARCO DE SEGURIDAD EN EL CONTROL DE PROCESOS

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

22. Este marco de seguridad 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 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.

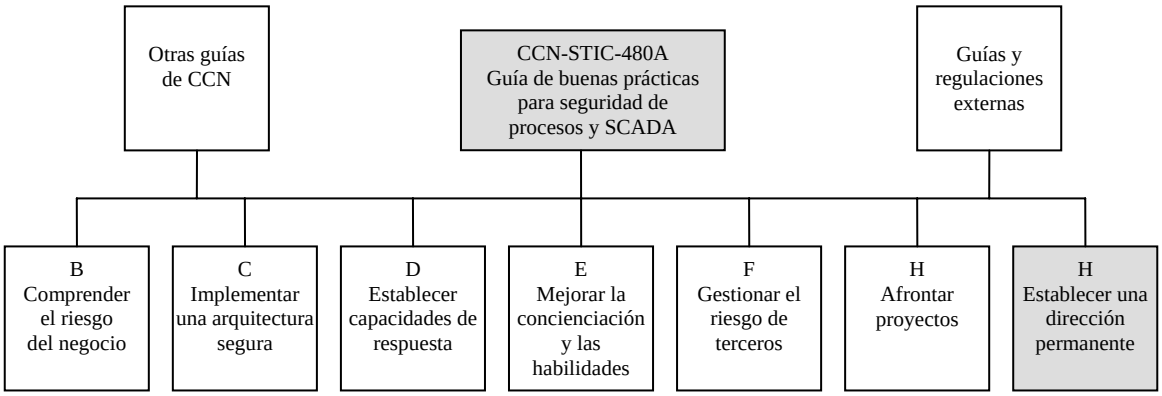


Figura 1: ***Dónde encaja esta guía dentro del marco de buenas prácticas***

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 establecer una dirección permanente. Todas las guías de este marco pueden encontrarse en la página Web de CCN en https://www.ccn-cert.cni.es ([Ref.- 69][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 "**Establecer una dirección permanente**" se basa en los fundamentos explicados en la guía de buenas prácticas y proporciona orientación para definir e implementar los marcos de gobierno adecuados para la seguridad en los sistemas de control de procesos.

25. Esta guía no incluye políticas ni normas detalladas o procedimientos.

[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.- 70])

1.5. DESTINATARIOS

26. Cualquiera involucrado en establecer la dirección o las normas de seguridad en el control de procesos:

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

2. RESUMEN DE "ESTABLECER UN DIRECCIÓN PERMANENTE"

27. Una dirección formal para la administración de la seguridad en los sistemas de control de procesos garantizará de que se siga en toda la organización una aproximación coherente y adecuada. Sin esa dirección, la protección de los sistemas de control de proceso puede ser improvisada[4] o insuficiente, y exponer a la organización a un riesgo adicional. Un marco directivo eficaz establece claramente los roles y responsabilidades, políticas y normas actualizadas para gestionar los riesgos de seguridad en el control de procesos, y la garantía de que esas políticas y normas se están siguiendo.

28. Gobierno[5]: Sistema por el que las organizaciones son dirigidas y controladas.

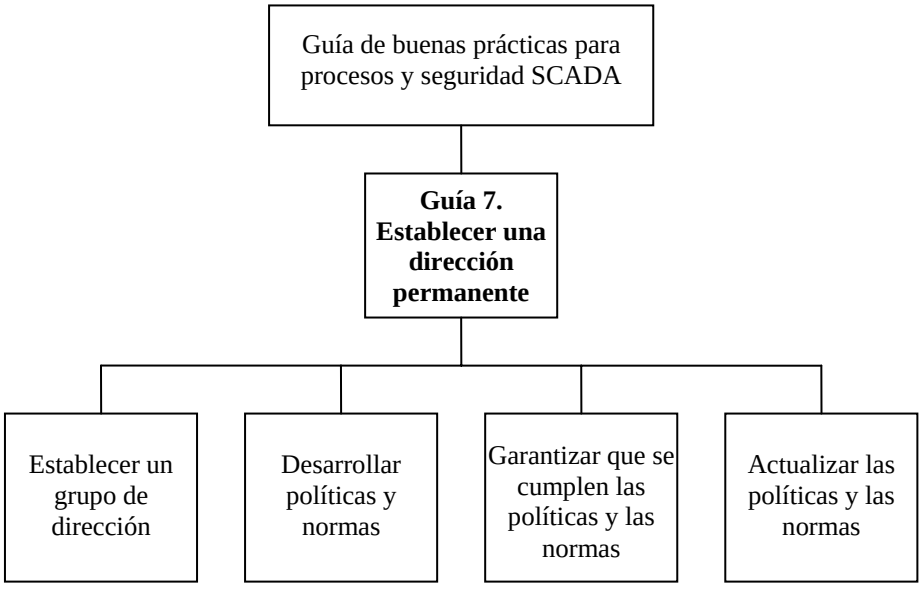


Figura 2: ***Estructura del documento "Establecer una Dirección Permanente"***

[4] N.T.: Original: *ad-hoc*
[5] N.T.: En el original, se habla de "*governance*", que literalmente se traduciría como gobierno, pero se ha preferido la traducción semántica de dirección.

3. ESTABLECER UN GRUPO DIRECTIVO

3.1. CONTEXTO DE ESTA SECCIÓN DENTRO DEL MARCO GENERAL

29. El grupo directivo (a veces conocido como un comité o consejo) proporciona un papel fundamental al dirigir cada uno de los siete elementos del marco. El grupo directivo tendrá responsabilidad sobre el riesgo y los impactos en la seguridad por lo que estará involucrado en todos los asuntos del marco de seguridad en el control de procesos. Los sujetos del negocio serán responsables de la seguridad en el control de procesos. El diagrama indica un flujo simple de información que ayuda a elegir a los miembros más adecuados para formar parte del grupo directivo, y las consideraciones clave en la selección de los miembros.

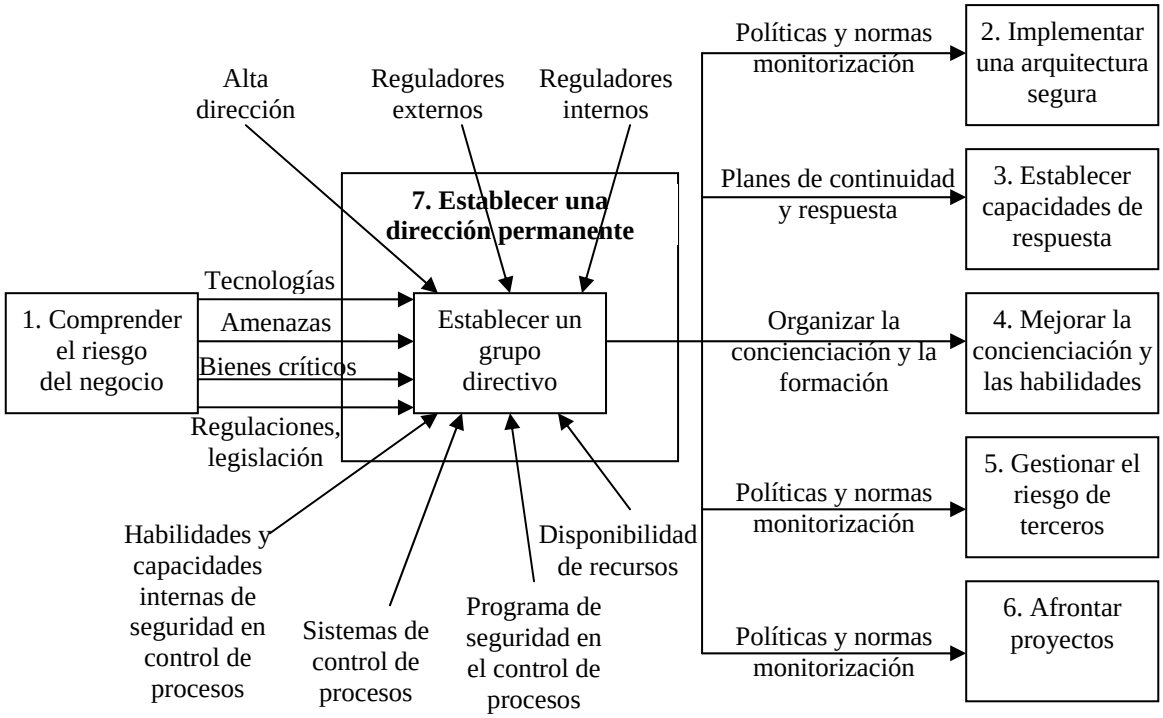


Figura 3: ***Cómo encaja "Establecer una dirección permanente" en este marco***

3.2. JUSTIFICACIÓN

30. Un grupo directivo bien definido con roles y responsabilidades bien articulados es esencial para garantizar que el riesgo de seguridad en el control de procesos se gestiona efectiva y exhaustivamente. Aunque sería imposible definir cómo este grupo directivo encaja en cada organización, los miembros deben ser una mezcla de encargados de adoptar decisiones y expertos técnicos procedentes de las disciplinas adecuadas. Este grupo tiene que encajar en la estructura de dirección e informativa existente en la empresa, y tener el cometido de habilitar dicha estructura para dirigir el control de procesos de la organización, tanto a nivel estratégico como operativo.

3.3. PRINCIPIOS DE BUENAS PRÁCTICAS

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

    - Obtener el apoyo de la alta dirección para la seguridad de los sistemas de control de procesos.
    - Identificar el impacto de los requisitos legales y reglamentarios en la seguridad en control de procesos.
    - Garantizar que la seguridad de los sistemas de control de procesos es acorde con las necesidades del negocio y operativas.
    - Definir los roles y las responsabilidades de todos los elementos de la seguridad en control de procesos.
    - Designar un responsable único del riesgo de seguridad en el control de procesos. Dependiendo del tamaño de la organización, puede ser una persona o una serie de responsable regionales que respondan ante un responsable único.

3.4. ORIENTACIÓN SOBRE LAS BUENAS PRÁCTICAS

32. Independientemente del tipo de dirección que una organización elija, se debe garantizar que, como mínimo, están representadas las siguientes funciones como mínimo:

    - Empresa: proporciona una perspectiva de lo que el negocio necesita, puede ser uno o varios altos directivos.
    - Control de procesos: proporciona representación y capacidades del control de procesos, identificación de activos críticos y de la exposición existente.
    - Seguridad: proporciona una perspectiva de conocimiento, experiencia e integración en seguridad física y de la información.
    - Ingeniería: en caso de que la ingeniería sea una función distinta al control de procesos se puede necesitar orientación práctica sobre el funcionamiento / la implementación.
    - Condiciones de trabajo: orientación clave para garantizar la coherencia y el cumplimiento de las condiciones de trabajo necesarias.

33. Es fundamental contar con todas estas funciones en el grupo directivo de la seguridad en el control de procesos, pues representan los principales puntos de vista que garantizarán un enfoque equilibrado para cumplir las necesidades en seguridad en el control de procesos del negocio. Otras funciones que deben considerarse para ser incluidas son los gestores de riesgo empresarial/operativo, el planeamiento de continuidad y emergencia del negocio, y la seguridad física, de la infraestructura TI y las telecomunicaciones. Estas pueden ser incluidas en los roles principales o, si resulta más apropiado, pueden tener un rol representado independientemente.

34. Cómo se reparten las responsabilidades entre estas funciones es algo específico a la cultura de cada organización, los recursos que tiene disponibles, y la estructura directiva elegida, alcance geográfico, etc. Las responsabilidades típicas que serían parte de la dirección de la seguridad en control de procesos son:

- Equilibrar las necesidades de la empresa con el coste de las medidas de mitigación.
- Integrar los requisitos de condiciones de trabajo en la seguridad en el control de procesos.
- Considerar los requisitos legales.
- Considerar las implicaciones de recursos humanos en la seguridad en el control de procesos.
- Gestionar el plan de concienciación y formación en el control de procesos.
- Monitorizar e informar del estado de la seguridad en el control de procesos a la junta.
- Comprometer a los responsables del diseño.
- Definir el alcance y los límites operativos.
- Definir las responsabilidades.
- Mantener un registro de los proyectos de control de procesos (garantizando la seguridad adecuada para prevenir el acceso no autorizado a la información del proyecto).
- Mantener la propiedad del registro de riesgo corporativo relacionado con el registro de riesgo relacionado con seguridad en el control de procesos.
- Controlar y mantener la estrategia de seguridad en el control de procesos (planes a corto y a largo plazo).
- Controlar el programa de seguridad en el control de procesos.

35. La responsabilidad de la seguridad en el control de procesos puede ser delegada por el grupo directivo, ya sea directamente o a través de una serie de niveles intermedios en función de la organización, su tamaño, cultura, estructura existente, etc. Las organizaciones que dependen en gran medida del control de procesos o que sufrirían un impacto significativo si se perdieran los sistemas de control de procesos son más propensas a tener un grupo directivo que esté más íntimamente relacionado con la junta directiva. A cambio de una responsabilidad delegada específicamente, el grupo directivo tendrá la tarea de ofrecer una indicación clara del nivel de exposición de la organización y de cómo planea afrontarlo. Un canal directo de información es esencial para asegurar que la escala de cualquier impacto potencial de un incidente en el control de procesos es comunicado con claridad para que cualquier impacto significativo en la empresa sea entendido y discutido en el nivel adecuado. También es muy importante que el grupo de directivo comprenda claramente los límites de la responsabilidad que se le ha delegado. El siguiente diagrama ofrece una visión general de las consideraciones del grupo directivo.

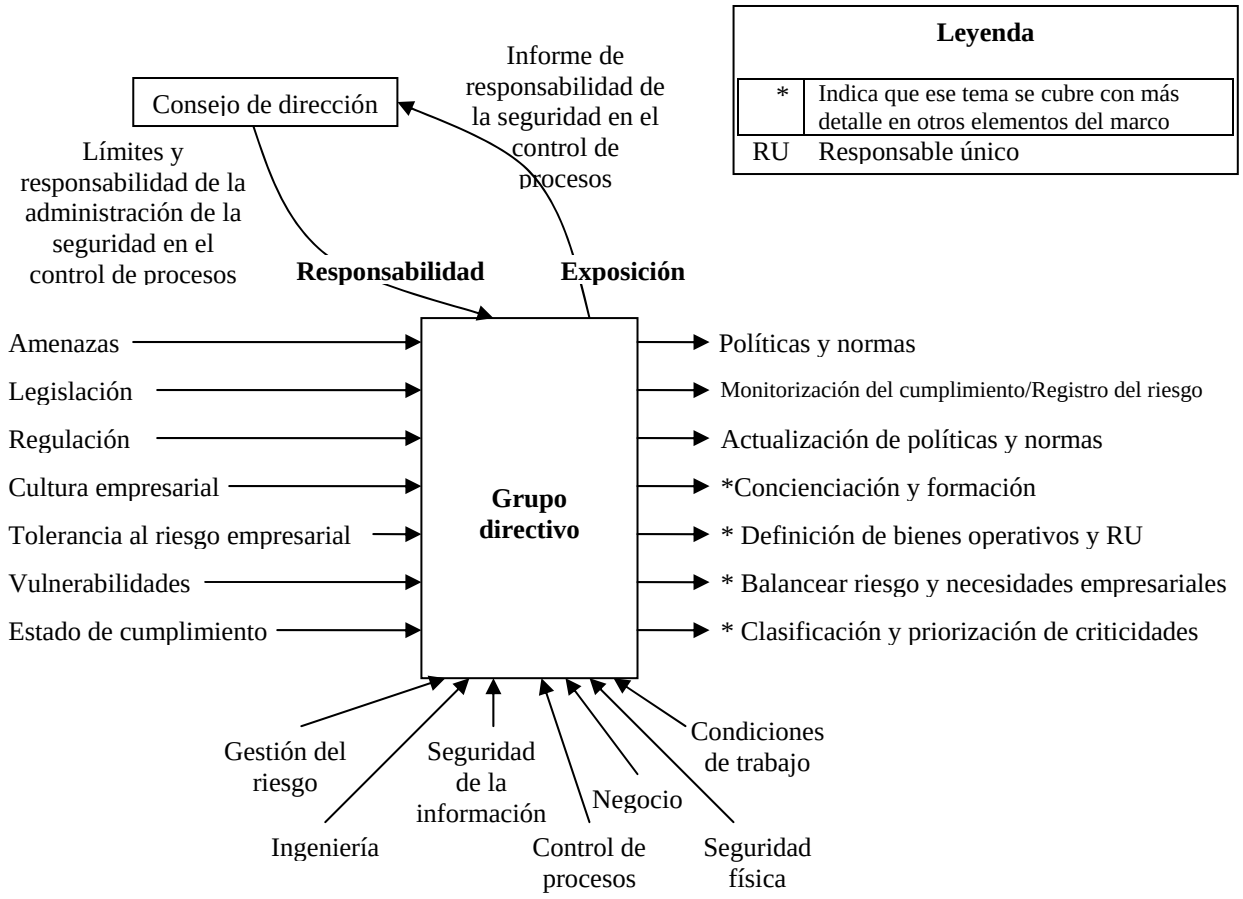


Figura 4: ***Funciones del grupo directivo***

36. Formar parte del grupo directivo de control de procesos es por lo general una función a tiempo parcial; cuánto tiempo se dedica a los deberes del grupo directivo de gobierno depende de la magnitud del riesgo existente y de las estructuras que ya existen. Los deberes del grupo directivo incluyen:

37. **Estratégico:** establecer la política de seguridad e iniciar el programa de seguridad del control de procesos.

38. **Táctico:** poner en práctica el programa de seguridad del control de procesos, proporcionar orientación para la concienciación y la formación en seguridad en control de procesos, y vigilar el cumplimiento de la política y las normas. Establecer y aprobar los presupuestos.

39. **Operativo:** crear y servir de enlace con el Equipo de Respuesta de Seguridad en el Control de Procesos, que monitoriza, analiza y responde a las alertas y los incidentes. Vigilar la exposición al riesgo.

4. DESARROLLAR POLÍTICAS Y NORMAS

4.1. CONTEXTO DE ESTA SECCIÓN DENTRO DEL MARCO GENERAL

40. Desarrollar políticas y normas de seguridad en control de procesos está estrechamente relacionado con el elemento del marco "Comprender el riesgo del negocio" ([Ref.- 72]). Gran parte de los resultados de comprender el riesgo del negocio se usa directamente para establecer las políticas adecuadas para la seguridad en el control del proceso en una organización. El proceso de elección de políticas debe estar dirigido por el riesgo del negocio, y habitualmente ocurrirá a nivel de la alta dirección. Tras considerar el riesgo del negocio y la tolerancia al riesgo de la empresa, la alta dirección buscará información de los equipos de control, la seguridad en TI, las condiciones de trabajo y la empresa para determinar qué política es eficaz. También es importante considerar qué reglamentaciones y legislación externas se deben cumplir, y qué medidas o tecnología de mitigación hay disponibles actualmente.

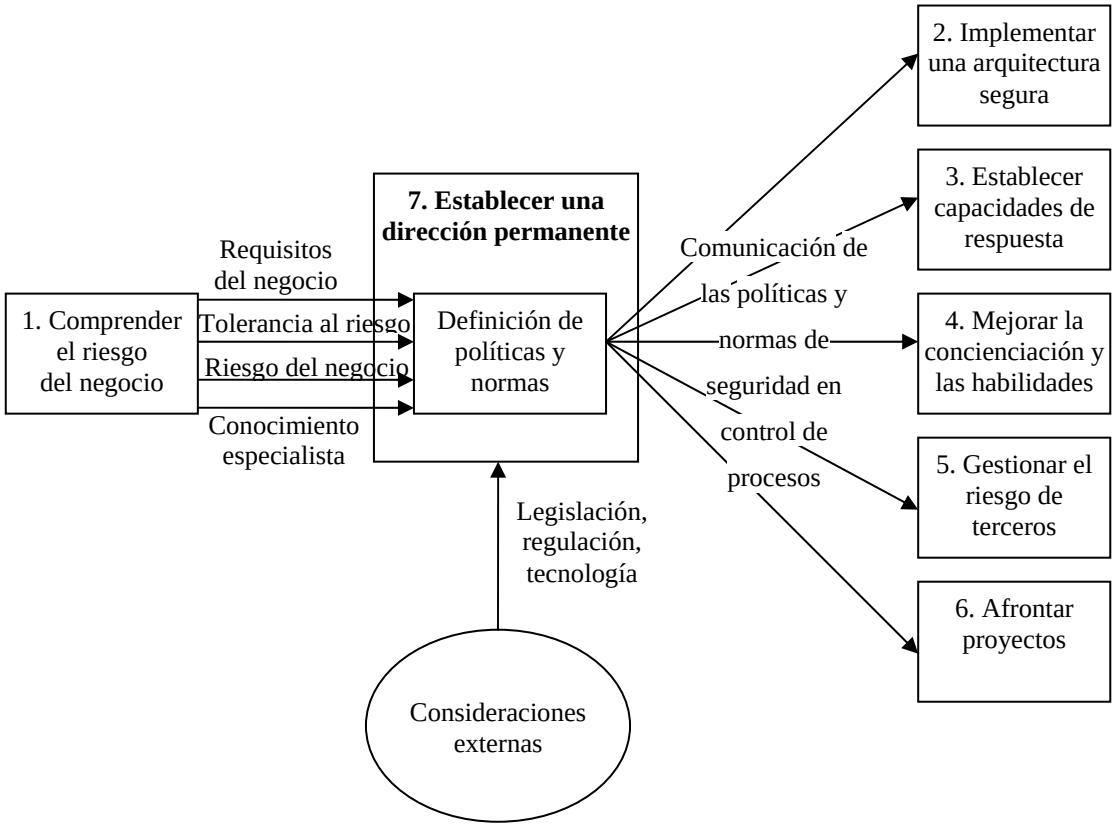


Figura 5: ***Cómo encaja "Desarrollar Políticas y Normas" en este marco***

41. Cada uno de los cinco restantes elementos del marco de seguridad en control de procesos se apoyará y hará uso de las políticas y normas de seguridad en control de procesos de la organización; a continuación se proporciona una visión general.

4.2. JUSTIFICACIÓN

42. Las políticas de seguridad en control de procesos son la traducción de la tolerancia al riesgo de la organización en los límites dentro de los que se pueden tomar medidas, y las normas son un conjunto de bloques de construcción repetibles que definen la creación, el mantenimiento y la eliminación de componentes en los sistemas de control de procesos. La política definirá los límites de la organización, y las normas proporcionarán una interpretación organizativa coherente para lograr la claridad deseada de la política definida.

43. Ejemplo: Una política podría describir qué tráfico se permite, aunque a alto nivel, por ejemplo, “ningún tráfico originado en los sistemas de oficina puede acceder el sistema de control de procesos”.

44. Las políticas y las normas son el mecanismo mediante el cual una organización puede comunicar el nivel deseado de protección de la seguridad en control de procesos y cómo se debe alcanzar.

4.3. PRINCIPIOS DE BUENAS PRÁCTICAS

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

- Definir, documentar, difundir y gestionar bajo el control de los cambios la formación, la política y las normas formales para la seguridad en el sistema de control de procesos.
- Garantizar que la política y las normas reflejan fielmente los requisitos de la organización, y apoyan los requisitos del negocio.
- Garantizar que la política y las normas son aceptadas por todas las partes pertinentes.

4.4. ORIENTACIÓN SOBRE LAS BUENAS PRÁCTICAS

46. La creación de la política y las normas de seguridad en el control de procesos puedes ser asumida enteramente como una entidad única o combinarse con las normas de seguridad TI existentes o las normas de ingeniería. Hay bastantes razones para cualquiera de los dos enfoques y funcionan igual de bien siempre que puedan representar con exactitud la calidad y el detalle necesario para proteger los sistemas de control de procesos según los requerimientos de negocio definidos.

47. Una organización puede optar por crear un conjunto separado de políticas y normas en caso de que:

- Los sistemas de control de procesos de negocios sean críticos o tengan un impacto severo sobre la seguridad.
- Haya una fuerte capacidad de recursos de control de procesos.
- Las actuales políticas y normas de seguridad no sean suficientes para cubrir los sistemas de control de procesos.
- Otras razones culturales o históricas.

48. Asimismo, puede ser conveniente combinar las políticas y normas de seguridad en control de procesos y las políticas y normas de seguridad actuales, o añadir una sección sobre seguridad en control de procesos a éstos documentos de normas si:
    - Los sistemas de control de procesos son críticos y están muy integrados en los procesos clave del negocio.
    - Hay una buena colaboración entre seguridad, control de procesos y soporte en TI.
    - Hay una buena adaptación entre los controles de seguridad de la empresa y los controles necesarios para proteger los sistemas de control de procesos.
    - Hay capacidades y recursos limitados para el control de procesos.
49. Se debe tener cuidado al combinar políticas y normas claras, pues se deben definir sin ambigüedad la responsabilidad, la calidad acordada, los principios de seguridad y muchos otros aspectos, para garantizar que se cumplen de modo eficiente tanto los objetivos de seguridad en control de procesos como de TI. Raramente es un proceso sencillo, pues los requisitos operativos de la seguridad TI y de la seguridad en control de procesos pueden diferir en algunos aspectos fundamentales como las actualizaciones de versiones.
50. Puede constituirse un grupo de trabajo de arquitectura y normas que informe al grupo directivo, garantizando que los grupos de TI y de control de procesos se involucran en la definición de políticas, normas y orientaciones para la implementación.
51. La figura 6 muestra cómo el detalle y el número de los documentos varía entre las políticas, normas y las orientaciones. Al subir en el triángulo hay menos detalle, menos documentos y menos cambios, y lo contrario se aplica al bajar en el triángulo con documentos de orientación para la implementación más detallados que necesitan actualizaciones periódicas.

Figura 6: ***Relación entre los documentos de políticas, normas y orientaciones***

4.4.1. POLÍTICAS

52. Una política necesita estar acompañada de declaraciones específicas de los directores o de acciones rectoras que muestren un claro compromiso de la organización; declaración de valores o intenciones que proporcionen una base consistente para la toma de decisiones y la asignación de recursos, y definir el método o los cursos de acción que orienten y determinen las decisiones presentes y futuras. Las características típicas de las políticas son:

    - tienen una amplia aplicación
    - cambian con poca frecuencia
    - son expresadas en términos generales
    - no son documentos técnicos
    - son declaraciones de "qué" y/o "por qué"
    - abordan las principales cuestiones operacionales.

53. Las políticas de seguridad en control de procesos suelen ser documentos de alto nivel que proporcionan en "marco" básico respetando las necesidades técnicas o del negocio. En la mayoría de los casos, una política sola sin las correspondientes normas será de un nivel demasiado alto para comunicar lo que hay que hacer. Son las normas (y las orientaciones para la implementación) las que proporcionan la información necesaria para aplicar los objetivos de las políticas al nivel requerido de calidad.

54. El mínimo detalle que debería incluirse en un documento de política es:

    - la declaración política de intenciones: "los controles deben estar en su lugar, con esta calidad"
    - a qué o a quién se aplica la política: "el objetivo o los límites de la política"
    - quién es propietario de la política: "quién la publicará y actualizará"
    - qué significa la actualización de la política: "cuando debería revisarse la política"
    - los criterios y procesos de excepción: "cuando no es aplicable la política".

55. Al escribir una política es importante reconocer que hay varios factores, incluyendo las políticas y normas de negocio existentes, que pueden influir en la política de seguridad en control de procesos. Es muy fácil escribir una política de seguridad en control de procesos de forma aislada, sin tener en cuenta el impacto en el negocio, el impacto operativo o el financiero de las declaraciones que se hacen. Los documentos escritos de esta manera tienen muy pocas probabilidades de ser aprobados y aceptados por la empresa y suponen una pérdida de esfuerzo.

56. Al escribir una política de seguridad en el control de procesos es importante verificar continuamente que cumple los siguientes criterios:

    - alineación con la estrategia empresarial
    - alineación con la estrategia y las políticas de TI
    - alineación con la política de condiciones de trabajo
    - alineación con las políticas de seguridad física de la organización

- uso coherente de la terminología existente/establecida
- coherencia con el nivel y la audiencia de otras políticas.

57. El Grupo Directivo es responsable de establecer una política de seguridad en control de procesos y garantizar que se aprueba al nivel que la organización requiera.

4.4.2. NORMAS

58. Las características de las normas respecto a las políticas son:
    - son de aplicación reducida
    - son propensas a cambiar
    - están descritas en detalle
    - pueden incluir información técnica
    - incluyen declaraciones de “cómo”, “cuando” y, a veces, “quién”
    - describen los procesos relacionados.
59. Los documentos de normas de seguridad en control de procesos proporcionan un enfoque común que se ha de seguir en toda la organización. Permiten una entrega más rápida con una calidad conocida que, en general, reduce la complejidad de la tarea. Las normas que proporcionan un enfoque coherente y repetible y que reducen la duplicación al compartir conocimientos especializados que son adaptados para una determinada organización. El desarrollo de buenas normas de calidad rompe las tareas en trozos manejables que proporcionan una mejor comprensión de la tarea y los riesgos que se reducen.
60. Las normas pueden ser elaboradas con la ayuda de grupos internos de especialistas o con la ayuda de terceros. Las normas definen las líneas de límite necesarias para alcanzar la calidad y la capacidad descritas en el documento de política de seguridad. Las normas están muy influenciadas por la legislación y las regulaciones vigentes (laborales, etc.), las normas industriales existentes, la tecnología disponible y las necesidades futuras del negocio o industria.
61. Al considerar lo que hay que incluir en una norma, el mínimo detalle esperable en un documento de normas es:
    - La política a la que se aplica la norma; “que política o políticas"
    - La audiencia o lectores: “el nivel de detalle”
    - La definición y aplicación de la norma: “¿qué es esto, cómo se aplica a las personas, los procesos y la tecnología?"
    - A qué o quiénes se aplica la norma: “el objetivo o los límites de las normas”
    - quién es propietario de la norma: “quién la publicará y actualizará”
    - qué significa la actualización de la norma: “cuando debería revisarse la norma”
    - los criterios y procesos de excepción: “cuando no es aplicable la norma”.

62. Debido al detalle contemplado en las normas y la frecuencia de los cambios, es común que sólo deba ser aceptada a nivel del grupo directivo. Esto no significa que el proceso sea menos estricto, pero sí refleja que el detalle sólo será comprendido por un grupo limitado de revisores.

4.4.3. ORIENTARCIONES PARA LA IMPLEMENTACIÓN

63. Existe un tercer grupo de documentos que suelen utilizarse para ayudar a las normas, y que son generalmente conocidos como documentos de "Orientación para la Implementación". Cuando una norma tiene varias aplicaciones posibles, estas guías proporcionan los detalles adicionales para asegurar que de la norma se plasma apropiadamente en soluciones prácticas para entornos específicos, sin el problema de complicar innecesariamente la propia norma. Se trata generalmente de los documentos más detallados y sólo se centran en una aplicación específica de la norma, como la forma de configurar un cortafuegos específico de acuerdo a la norma.

4.4.4. NORMAS Y ORIENTACIONES DE REFERENCIA

64. Hay una serie de fuentes de orientación para desarrollar las normas de seguridad en control de procesos, como los proveedores, instituciones gubernamentales y reguladores industriales. La mayor parte de la orientación ayudará a definir las expectativas requeridas de calidad. Algunas de las principales fuentes de normas y orientación se enumeran a continuación:

- Guías CCN-STIC descargables en el portal Web del CCN-CERT (www.ccn-cert.cni.es) ([Ref.- 69])
- CPNI Best Practice Guide on Firewall Deployment for SCADA and Process Control Networks ([Ref.- 79][6])
- CPNI Good Practice Guide Outsourcing: Security Governance Framework for IT Managed Service Provision ([Ref.- 44])
- CPNI Good Practice Guide Patch Management ([Ref.- 45])
- CPNI Best Practice Guide Commercially Available Penetration Testing ([Ref.- 46])
- CPNI guide on Personnel Security Measures ([Ref.- 47])
- ISO 27002 (antes 17799): Código de buenas prácticas para la Gestión de la Seguridad de la Información ([Ref.- 48])
- UNE-ISO/IEC 27001 (Traducción de la ISO 27001) ([Ref.- 80][7])
- PCSRF – Process Control Security Requirements Forum ([Ref.- 50])
- IEEE – Institution of Electrical and Electronics Engineers ([Ref.- 51])
- IEC – International Electrotechnical Comisión ([Ref.- 52])
- Orientación específica de organizaciones como American Petroleum Institute ([Ref.- 54]), North American Electric Reliability Corportation ([Ref.- 55]), American Gas

[6] N.T.: [Ref.- 43]
[7] N.T.: [Ref.- 49]

Association ([Ref.- 56]), Norwegian Oil Industry Commision ([Ref.- 53]), International Council on Farge Electric Systems ([Ref.- 57]), National Institute of Standards and Technology ([Ref.- 58]), etc.

- Orientación específica del proveedor
- Guía de practicas recomendadas para securizar redes inalámbricas ZigBee en Entornos de Sistemas de Control de Procesos ([Ref.- 59])
- Securizar redes WLAN usando 802,11i ([Ref.- 60])
- Using Operational Security (OPSEC) to support a Cyber Security Culture in Control Systems Environments ([Ref.- 61])
- Cyber Security Procurement Language for Control Systems ([Ref.- 62])
- NERC Critical Infrastructure Protection (CIP) ([Ref.- 63])
- DHS Catalog of Control System Security Requirements ([Ref.- 64] y [Ref.- 65])
- NIST Guide to Industrial Control (ICS) Systems ([Ref.- 67])
- ISA SP99, Manufacturing and Control Systems Security ([Ref.- 66])

65. Al escribir políticas, normas y orientaciones, los referentes indicados pueden usarse como un punto de partida a partir del cual adaptar un conjunto específico de documentos basado en los requisitos, las características y la cultura de la empresa.
66. El principal objetivo es fijar los requisitos importantes. Hay que evitar caer en la trampa de escribir una lista de deseos basada en un determinado proveedor, *hardware* o *software*.
67. Copiar las mejores prácticas del sector sin adaptarlas no mejorará la seguridad en el control de procesos, e incluso puede dificultar las operaciones y malgastar tiempo y recursos valiosos. Sin embargo, aplicar principios de buenas prácticas sobre una amenaza identificada en la organización ayuda a mitigar el problema de acuerdo al nivel de tolerancia al riesgo de la organización.
68. Los documentos de calidad escritos para hacer frente a una tolerancia al riesgo y unas amenazas específicas serán más fácil de aplicar, monitorizar, actualizar y cumplir, y serán muy superiores a la copia de unas buenas prácticas genéricas.

5. GARANTIZAR EL CUMPLIMIENTO DE LAS POLÍTICAS Y NORMAS E INFORMAR A REGULADORES EXTERNOS

5.1. CONTEXTO DE ESTA SECCIÓN DENTRO DEL MARCO GENERAL

69. Una dirección eficaz necesita no sólo la existencia de políticas y normas adecuadas, sino también la vigilancia de su cumplimiento.
70. El proceso de cumplimiento proporciona una retroalimentación muy importante para poner de relieve las dificultades de la política y las normas, y puede ser un mecanismo para actualizar o corregir donde la orientación existente no alcance los objetivos deseados.

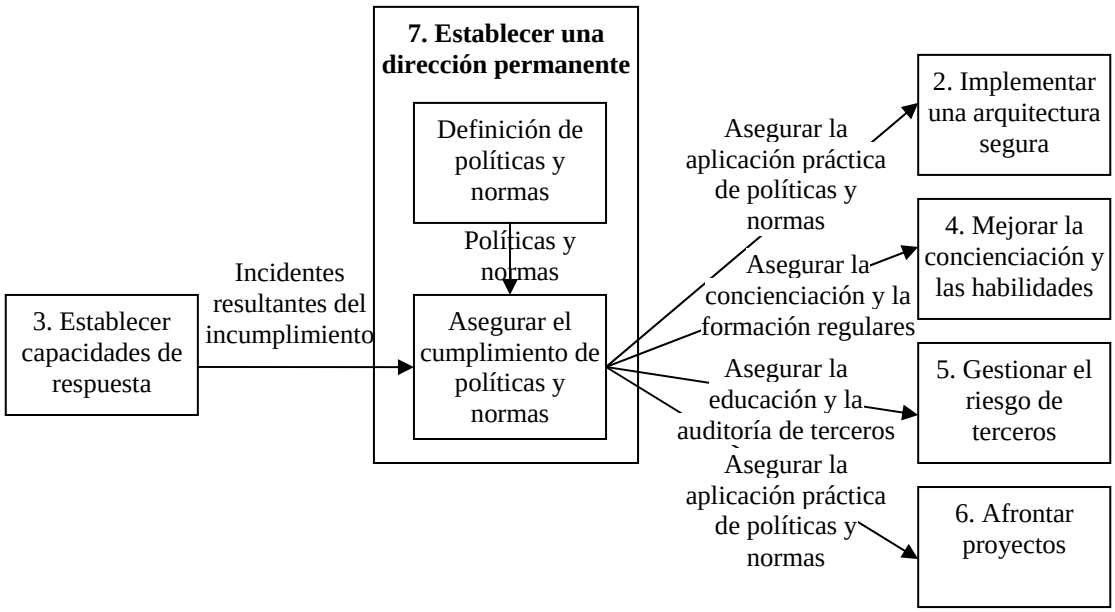


Figura 7: ***Cómo encaja "Asegurar el Cumplimiento de las Políticas y Normas" en este marco***

5.2. JUSTIFICACIÓN

71. Es fundamental asegurar el cumplimiento de la política y las normas para garantizar que se están realizando las acciones adecuadas para el cumplimiento de los requisitos correctos de calidad, y que es una función clave a establecer por la dirección. El cumplimiento de las políticas y normas:

    - Garantizará que los sistemas de control de procesos están protegidos al nivel acordado de riesgo del negocio
    - Asegurará que se evita la duplicidad innecesaria de esfuerzos, y que las soluciones coherentes se están aplicando en toda la organización.

5.3. PRINCIPIOS DE BUENAS PRÁCTICAS

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

    - Implementar un programa de garantía para asegurar que la política y las normas de los sistemas de control de procesos se cumplen de manera continua.

5.4. ORIENTACIÓN SOBRE LAS BUENAS PRÁCTICAS

73. Existen varios enfoques para garantizar el cumplimiento de la política y las normas que deben adaptarse a la cultura, las capacidades y las iniciativas existentes en la organización. Algunas organizaciones se sienten mejor con información detallada de las áreas que cumplen y las que no. Otras prefieren recibir informes de excepción donde sólo

se registren los incumplimientos. La labor de valorar el cumplimiento puede dividirse en tres decisiones clave:

- ¿Qué información se requiere, en qué detalle y cuándo?
- ¿Cómo y quién debe recopilar la información, es decir, qué proceso de cumplimiento se utiliza?
- ¿Qué impacto tiene el incumplimiento en la empresa?

5.4.1. ¿QUÉ INFORMACIÓN SE REQUIERE, EN QUÉ DETALLE Y CUÁNDO?

74. La pregunta que debe ser respondida para la primera decisión es "¿Qué nivel de información es manejable al mismo tiempo que proporciona suficiente detalle como para ser de valor en la toma de decisiones?"

75. Esto variará entre organizaciones, pero vale la pena recordar que el exceso de información puede ser tan malo como la insuficiencia. Si la gente siente que no se lee la información que genera, la calidad pronto disminuirá; si alguien intenta señalar un problema con una política o estándar pero no tiene el alcance para hacerlo, es posible que escriba sus propias guías informales y defienda los documentos de la empresa sólo de cara al exterior.

76. La información clave que debe tenerse para elaborar los informes sobre el cumplimiento:

- La gestión que identifica al responsable de aplicar los resultados de los informes
- El responsable único del cumplimiento
- Las desviaciones relevantes respecto a la política o las normas
- Las consecuencias del impacto en la empresa
- La fecha prevista de resolución
- Circunstancias atenuantes (ej., razones del incumplimiento).

5.4.2. ¿CÓMO Y QUIÉN DEBE RECOPILAR LA INFORMACIÓN?

77. Esta cuestión se refiere a las capacidades y los recursos disponibles para garantizar el cumplimiento y se puede abordar de varias maneras. Dependiendo de la cantidad, calidad y frecuencia del control de cumplimiento, una organización puede optar por realizar la actividad internamente a través de auto-evaluación, revisión paritaria o un departamento de auditoría interna. Este enfoque tiene muchas ventajas incluyendo un mayor sentido de propiedad de cualquier problema o excelencia, pero puede ocupar muchos recursos de especialistas internos.

78. Otro enfoque es la subcontratación de la tarea a un tercero especializado en la seguridad en control de procesos. Esta opción proporciona resultados más objetivos y hay menos posibilidades de que se oculten problemas, pero probablemente cueste más. También está el problema de que la información de seguridad se pase a un tercero y presente una posible vulnerabilidad, por lo que el uso de recursos externos debe ser considerado cuidadosamente. Si hay organismos externos que incurren en el incumplimiento, puede tener un impacto en la regulación y debe ser identificado.

79. La vigilancia externa del cumplimiento no tienen que ser una auditoría formal y se puede emplear un enfoque iterativo más informal.

80. Resumen de las opciones:

- Auto-evaluación: una evaluación llevada a cabo por el departamento responsable
- Auto-evaluación asistida: una evaluación llevada a cabo por el departamento, con la asistencia de un especialista en seguridad en control de procesos
- Revisión interna: un examen interno por un departamento asociado que no es responsable
- Auditoría interna: una auditoría llevada a cabo por el departamento interno de auditoría de la organización
- Auditoría externa: una auditoría llevada a cabo por una organización externa
- Control externo: una revisión de las principales vulnerabilidades específicas de la industria llevada a cabo por una organización externa.

81. Se puede encontrar más orientación sobre la auditoría en el documento del NIST "Guide to Industrial Control Systems (ICS)" ([Ref.- 16][8]) y en las CCN-STIC 303 y 411.

5.4.3. ¿QUÉ IMPACTO TIENE EL INCUMPLIMIENTO EN LA EMPRESA?

82. La última decisión clave es qué riesgo adicional para la empresa hay, si lo hay, cuando se informa de una desviación significativa de la política o las normas de la organización. Es importante recopilar suficiente información sobre el incumplimiento para tomar una decisión informada sobre las potenciales amenazas, que se usará en el elemento de este marco "Comprender el Riesgo del Negocio" ([Ref.- 72]).

- ¿Cuál es la probabilidad de que el riesgo se materialice?
- ¿Con qué rapidez impactará en la empresa?
- ¿Qué medidas se están llevando a cabo o se han planeado?

83. **Requisitos mínimos del cumplimiento de la seguridad en el control de procesos:** Hay muchas áreas que pueden ser evaluadas con respecto al cumplimiento pero, como en la mayoría de los aspectos, debe alcanzarse un equilibrio entre los hechos y el contexto de la situación. Tres áreas que deben vigilarse siempre cuidadosamente son la segregación, la monitorización y detección de sistemas, y los parcheados (actualizaciones de seguridad). Para la mayoría de las organizaciones, estas tres áreas son la mayor amenaza para el negocio. Por tanto, debe haber políticas y normas en vigor y se debe prestar especial atención a la supervisión del cumplimiento en la organización, tales como:

- **Segregación**: ¿Están adecuadamente separadas las redes de control de procesos de las redes de oficina y del mundo exterior, por los medios apropiados?
- **Monitorización y detección:** ¿Está el cortafuegos del control de procesos registrado y revisado? ¿Se monitoriza la actividad de los usuarios/sistemas? ¿Se monitorizan los *logs* de los antivirus, etc?

[8] Original: [Ref.- 16]

- **Parcheado:** ¿Con qué velocidad se aplican los parches? ¿De dónde se reciben? ¿Están parchadas todas las máquinas?
- **Protección antivirus:** ¿Con qué velocidad se realizan las actualizaciones? ¿Cuáles son el método y la frecuencia de escaneado?
- **Planes de respuesta:** ¿Se revisan y actualizan los planes regularmente? (ej, anualmente)
- **Copias de seguridad:** procedimientos de copia de seguridad y restauración.

84. Las actividades típicas de vigilancia del cumplimiento incluyen:

- Usar herramientas automáticas o listas de verificación basadas en las normas (técnicas) aplicables.
- Entrevistar a los propietarios, usuarios y administradores de los sistemas, por ejemplo para evaluar la concienciación de los mismos
- Examinar la documentación como prueba del proceso que lleva a cabo (ej., control de cambios, procesos de excepción)
- Usar pruebas de penetración o escaneados de vulnerabilidad (con precaución).

85. Determinar con qué frecuencia deben llevarse a cabo las pruebas de cumplimiento puede variar entre organizaciones. No es raro ejecutar controles diarios si hay sistemas automatizados que lo permiten; para verificar controles como los privilegios de acceso es más conveniente que sean mensuales o trimestrales en función de la rotación del personal, el uso de subcontratas, etc. Las revisiones completas del sistema se suelen realizar anualmente o con menos frecuencia si los sistemas son de bajo riesgo. El punto clave es coordinar la periodicidad de los controles con el riesgo percibido del sistema.

6. ACTUALIZAR LAS POLÍTICAS Y LAS NORMAS

6.1. CONTEXTO DE ESTA SECCIÓN DENTRO DEL MARCO GENERAL

86. Las revisiones de las políticas o las normas pueden ser requeridas por cualquier elemento del marco de seguridad en el control de procesos. La decisión de la empresa de cambiar su actual postura sobre el riesgo, los avances en seguridad de la arquitectura facilitan una actualización, o la decisión de externalizar la gestión de un cortafuegos, pueden desencadenar un cambio de política o normas para adaptar el cambio al riesgo. Una fuente común de cambios es que la aplicación práctica de una norma resulte excesiva, por lo que la norma es relajada o modificada para facilitar el cumplimiento. También hay varios factores externos que pueden hacer que los elementos del marco de seguridad completen un ciclo a través de los procedimientos de seguridad y que, eventualmente, producirán una actualización de una política o norma. Independientemente del origen del cambio, es imprescindible que la organización cuente con un proceso efectivo para responder a la solicitud de cambio y tome las medidas apropiadas.

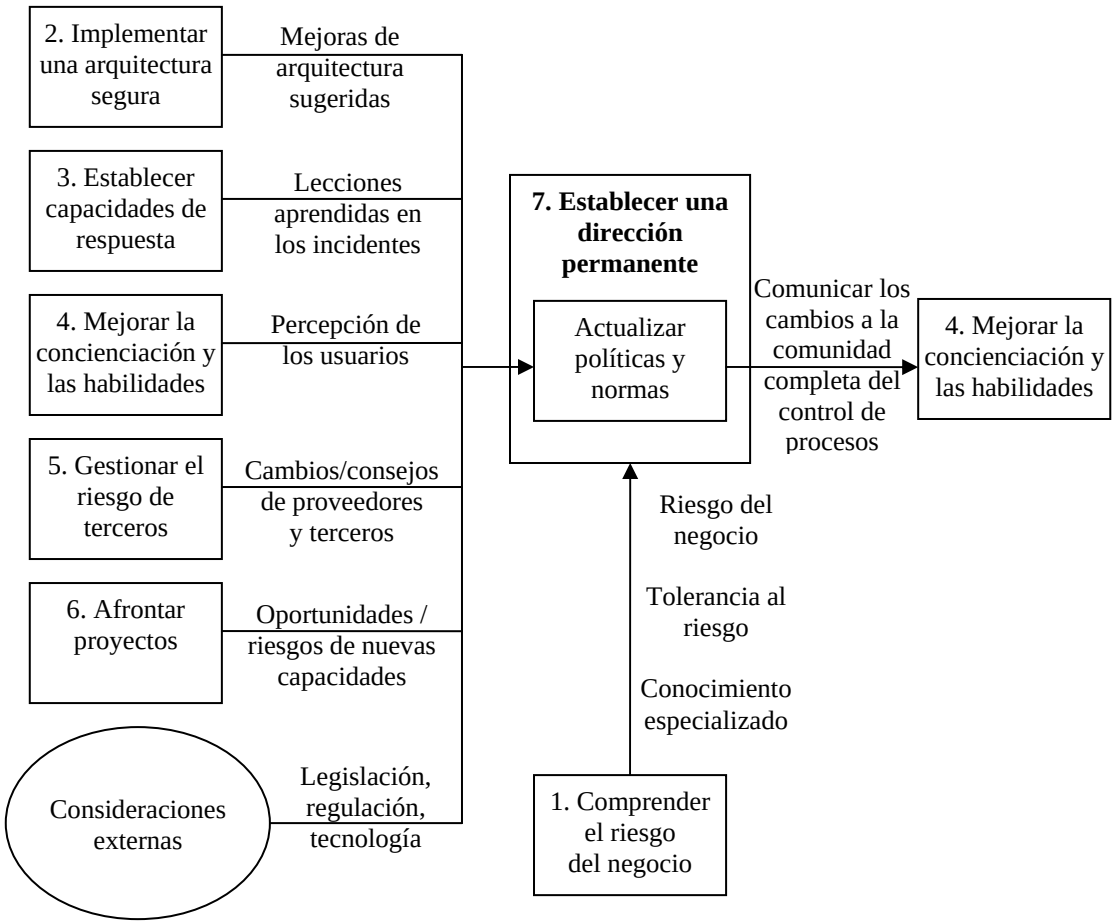


Figura 8: ***Cómo encaja "Actualizar Políticas y Normas" en este marco***

87. Tras la actualización de la política y las normas, es muy importante comunicar los cambios para aumentar la sensibilización o desarrollar nuevas habilidades en el entorno completo del control de procesos.

6.2. JUSTIFICACIÓN

88. La tecnología, la legislación, la reglamentación y las amenazas al control de procesos están progresando y evolucionando continuamente. Es esencial que la política y las normas se actualicen regularmente para responder con precisión a estos cambios.

6.3. PRINCIPIOS DE BUENAS PRÁCTICAS

89. El principio de buenas prácticas del documento general "CCN-STIC-480A – Guía de buenas prácticas – Seguridad en el Control de Procesos y SCADA" ([Ref.- 71]), es:

90. Establecer un programa permanente que garantice que la política y las normas de seguridad en el control de procesos se revisan y actualizan periódicamente. Puede hacerse a través de revisiones anuales o de una revisión impulsada por cambios:

    - en las amenazas actuales

- en los requisitos legales y reglamentarios
- en los requisitos del negocio
- en las necesidades operacionales
- en el equipamiento operativo
- en la estrategia o el plan de largo plazo.

6.4. ORIENTACIÓN SOBRE LAS BUENAS PRÁCTICAS

91. Tiene que haber un equilibrio entre actualizar constantemente los documentos y garantizar que los documentos sean relevantes; el motivo es que la estructura y el detalle cubiertos en las políticas y las normas deben estar cuidadosamente escritos. Al invertir tiempo en construir políticas y normas de una buena calidad, flexibles, pero inequívocas, la organización será capaz de modificar sólo determinadas secciones, en lugar de tener que llevar a cabo una reescritura completa.
92. Un principio fundamental al redactar políticas y normas es considerar lo que se espera de la vida útil antes de tener que actualizarla; este enfoque no recogerá cambios inesperados pero podrá considerar la evolución de la tecnología.
93. Al igual que con la creación inicial de una política o norma, la actualización puede ser un proceso que consuma mucho tiempo. Las modificaciones pueden necesitar que las revisen y comenten varias partes interesadas, y debe considerarse cuidadosamente el impacto en los sistemas de control de procesos y el resto de la empresa. Algunos cambios pueden ser más sencillos que otros y es una buena práctica categorizar el cambio de manera que sólo se movilice a los revisores adecuados. Las categorías que una organización elige necesitan ser consideradas en la estructura de la organización y los procesos de revisión/control de cambios, pero algunas organizaciones utilizan las siguientes categorías:
    - actualización local
    - actualización nacional
    - actualización regional
    - actualización de toda la empresa.
94. Cabe señalar que el grupo directivo debe dar continuidad al asegurar que la información relevante esté disponible y se difunde adecuadamente, incluso si las actualizaciones de la política o las normas tienen una aceptación limitada de los revisores.
95. La posición óptima de una organización sería si la actualización de la política y las normas se integra en los procedimientos habituales del negocio, como las auditorías de condiciones de trabajo, a fin de que se conviertan en parte de las actividades cotidianas.
96. Cuando no sea posible cumplir una política y una norma, debería existir una política de excepción para garantizar que el incumplimiento está autorizado, se ha realizado un estudio del riesgo y se comprende el riesgo residual.

7. 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 3.4.5

[Ref.- 43] Best Practice Guide on Firewall Deployment for SCADA and Process Control Networks
www.cpni.gov.uk/Docs/re-20050223-00157.pdf

[Ref.- 44] Good Practice Guide Outsourcing: Security Governance Framework for IT Managed Service Provision
www.cpni.gov.uk/Docs/re-20060802-00524.pdf

[Ref.- 45] Good Practice Guide Patch Management
www.cpni.gov.uk/Docs/re-20061024-00719.pdf

[Ref.- 46] Best Practice Guide Commercially Available Penetration Testing
www.cpni.gov.uk/Docs/re-20060508-00338.pdf

[Ref.- 47] CPNI Personnel Security measures
www.cpni.gov.uk/ProtectingYourAssets/personnelSecurity.aspx

[Ref.- 48] ISO 17799 International Code of Practice for Information Security Management
www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=39612

[Ref.- 49] ISO 27001 International Specification for Information Security Management
www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42103

[Ref.- 50] Process Control Security Requirements Forum
www.isd.mel.nist.gov/projects/processcontrol/

[Ref.- 51] Institution of Electrical and Electronics Engineers (IEEE)
www.ieee.org/portal/site

[Ref.- 52] International Electrotechnical Commission (IEC)
www.iec.ch

[Ref.- 53] Norwegian Oil Industry Association (OLF)
www.olf.no/english

[Ref.- 54] American Petroleum Institute (API)
www.api.org

[Ref.- 55] North American Electric Reliability Corporation (NERC)
www.nerc.com

[Ref.- 56] American Gas Association (AGA)
www.aga.org

[Ref.- 57] International Council on Large Electric Systems (CIGRE)
www.cigre.org

[Ref.- 58] National Institute of Standards and Technology (NIST)
www.nist.gov

[Ref.- 59] 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.- 60] Securing WLANs using 802,11i
http://csrp.inl.gov/

[Ref.- 61] Using Operational Security (OPSEC) to support a Cyber Security Culture in Control Systems Environments
http://csrp.inl.gov/Documents/OpSec%20Rec%20Practice.pdf

[Ref.- 62] Cyber Security Procurement Language for Control Systems
www.msisac.org/scada/documents/12July07_SCADA_procurement.pdf

[Ref.- 63] NERC Critical Infrastructure Protection (CIP)
www.nerc.com/~filez/standards/Cyber-Security-Permanent.html

[Ref.- 64] DHS Catalog of Control System Security Requirements
www.dhs.gov

[Ref.- 65] DHS Control Systems Security Program Recommended Practices
http://csrp.inl.gov/Recommended_Practices.html

[Ref.- 66] ISA SP99, Manufacturing and Control Systems Security
www.isa.org/mstemplate.cfm?section=home&template=/TaggedPage/getStandards.cfm&MicrositeID=988&CommitteeID=6821

[Ref.- 67] Guide to Industrial Control (ICS) Systems
http://csrc.nist.gov/publications/PubsDrafts.html

Section 5.4.2

[Ref.- 68] NIST Guide to Industrial Control Systems (ICS) Security
http://csrc.nist.gov/publications/drafts/800-82/2nd-Draft-SP800-82-clean.pdf

A.3. REFERENCIAS EN ESTA TRADUCCIÓN

[Ref.- 69] Portal de CCN-CERT
https://www.ccn-cern.cni.es

[Ref.- 70] CCN-STIC-480 Seguridad en sistemas SCADA

[Ref.- 71] CCN-STIC-480A Seguridad en el control de procesos y SCADA
Guía de buenas prácticas

[Ref.- 72] CCN-STIC-480B Seguridad en el control de procesos y SCADA
Guía 1: Comprender el riesgo del negocio

[Ref.- 73] CCN-STIC-480C Seguridad en el control de procesos y SCADA
Guía 2: Implementar una arquitectura segura

[Ref.- 74] CCN-STIC-480D Seguridad en el control de procesos y SCADA
Guía 3: Establecer capacidades de respuesta

[Ref.- 75] CCN-STIC-480E Seguridad en el control de procesos y SCADA
Guía 4: Mejorar la concienciación y las habilidades

[Ref.- 76] CCN-STIC-480F Seguridad en el control de procesos y SCADA
Guía 5: Gestionar el riesgo de terceros

[Ref.- 77] CCN-STIC-480G Seguridad en el control de procesos y SCADA
Guía 6: Afrontar proyectos

[Ref.- 78] CCN-STIC-480H Seguridad en el control de procesos y SCADA
Guía 7: Establecer una dirección permanente

[Ref.- 79] CCN-STIC-408 Seguridad Perimetral – Cortafuegos

[Ref.- 80] UNE-ISO/IEC 27001

[Ref.- 81] CCN-STIC-403 Gestión de incidentes de seguridad

[Ref.- 82] CCN-STIC-406 Seguridad en redes inalámbricas

[Ref.- 83] CCN-STIC-418 Seguridad en Bluetooth

[Ref.- 84] CCN-STIC-303 Inspección STIC

[Ref.- 85] 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

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 “Establecer un Dirección Permanente””.
[10] Original: *Risk Appetite*
[11] Original: *Likelihood*