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

SEGURIDAD EN EL CONTROL DE PROCESOS Y SCADA

GUIA DE BUENAS PRÁCTICAS

FEBRERO 2010

Edita:

NIPO: 076-10-072-4

Tirada: 1000 ejemplares
Fecha de Edición: enero de 2010

LIMITACIÓN ORIGINAL DE RESPONSABILIDAD

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

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

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

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

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

AVISO LEGAL

PRÓLOGO

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

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

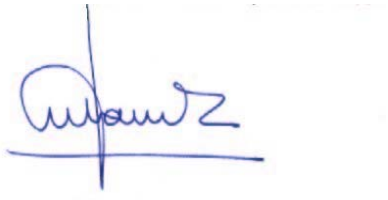
Una de las funciones más destacables del Centro Criptológico Nacional es la de elaborar y difundir normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los sistemas de las tecnologías de la información y las comunicaciones de la Administración, materializada en la existencia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

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

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

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

Febrero de 2010



Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

ÍNDICE

ANEXOS

FIGURAS

0. INTRODUCCIÓN A LA TRADUCCIÓN

0.1. ALCANCE DE ESTA TRADUCCIÓN

1. Como parte del acuerdo de colaboración entre el Centro para la Protección de la Infraestructura Nacional de Reino Unido (CPNI en adelante) y el Centro Criptológico Nacional de España (CCN en adelante), se han traducido la colección de guías "Process Control and SCADA Security" publicadas por el CPNI. La presente traducción se corresponde con la versión 2 de las guías del CPNI, publicadas en Junio de 2008, y que consta de las siguientes guías:
   - 00752 - Process Control and SCADA Security.
   - 00753 - Process Control and SCADA Security Guide 1. Understand the business risk
   - 00754 - Process Control and SCADA Security Guide 2. Implement secure architecture
   - 00755 - Process Control and SCADA Security Guide 3. Establish response capabilities
   - 00756 - Process Control and SCADA Security Guide 4. Improve awareness and skills
   - 00757 - Process Control and SCADA Security Guide 5. Manage third party risk
   - 00758 - Process Control and SCADA Security Guide 6. Engage projects
   - 00759 - Process Control and SCADA Security Guide 7. Establish ongoing governance
2. En el momento de publicación de esta traducción, las guías originales pueden encontrarse en http://www.cpni.gov.uk/WhatsNew/scada.aspx ([Ref.- 48])
3. Este documento traduce la siguiente guía:
   - 00752 - Process Control and SCADA Security
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.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

- Documentos y Páginas Web de Referencia: Contiene el Anexo "*Appendix A: Document and website references* " del documento original del CPNI.
- A.3. Referencias en esta traducción: Contiene las nuevas referencias añadidas en este documento de traducción.

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.
15. El último párrafo de los subapartados “Principios de buenas prácticas” de los capítulos 3 al 9 ha sido movido al principio de cada subapartado. Este párrafo dice:

La guía detallada de buenas prácticas se puede encontrar en: https://www.ccn-cert.cni.es ([Ref.- 95])

16. En los subapartados “Principios de buenas prácticas” de los capítulos 3 al 9, suelen incluir enumeraciones sin introducción. A pesar de no ser coherente con la numeración garrafal de las guías del CCN, se ha mantenido.

1. INTRODUCCIÓN

1.1. METAS Y OBJETIVOS

17. El objetivo de este documento es proporcionar los principios de buenas prácticas para la seguridad en el control de procesos y SCADA. Específicamente este documento:

    - Ofrece el panorama general necesario para la seguridad en el control de procesos y de los sistemas SCADA.
    - Pone de relieve las diferencias entre la seguridad en el control de procesos y de los sistemas SCADA, y la seguridad de las tecnologías de la información.
    - Describe los principios fundamentales para desarrollar este marco.
    - Identifica siete módulos a seguir para acometer la seguridad de los sistemas de control de procesos y, para cada uno, presenta los principios de buenas prácticas.

1.2. TERMINOLOGÍA

1.2.1. SISTEMAS DE CONTROL DE PROCESOS Y SCADA

18. 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.

1.2.2. BUENAS PRÁCTICAS

19. Buena práctica, en el contexto de este documento, se define como:

    Las mejores prácticas de la industria tales como estrategias, actividades o enfoques, que han demostrado ser eficaces a través de la investigación y la evaluación.

20. Las buenas prácticas resumidas en este documento sólo pretenden ser directrices. Para algunos entornos y control de sistemas de proceso, puede que no sea posible aplicar todos estos principios. Por ejemplo:

- **Principio de buenas prácticas**: Proteger los sistemas de control de proceso con software antivirus en estaciones de trabajo y servidores.
  Complicación: No siempre es posible aplicar el software antivirus en los sistemas de control de procesos de las estaciones de trabajo o servidores.

- **Principio de buenas prácticas**: Obtener acreditación de proveedores y una guía de configuración para sistemas de control de proceso de los proveedores antes del despliegue de ese tipo de software.
  Complicación: Algunos proveedores no acreditarán el software antivirus y otros sistemas de control de proceso son incompatibles con su software.

21. Si se da este caso, deberán ser investigadas otras medidas de protección.

2. PROTEGIENDO EL CONTROL DE PROCESOS Y LOS SISTEMAS SCADA

2.1. DESCRIPCIÓN GENERAL

22. 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[1].

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

24. En primer lugar, los sistemas de control de procesos eran tradicionalmente sistemas cerrados, diseñados para la funcionalidad, la seguridad y la fiabilidad donde la principal preocupación era la seguridad física. El aumento de la conectividad a través de tecnologías TI estándar los ha expuesto a nuevas amenazas para las que no están preparados (ej., gusanos, virus y *hackers*). Como estas redes de control de procesos siguen aumentando en número, ampliándose y conectándose, los riesgos de amenazas electrónicas para los sistemas de control de procesos continúan intensificándose.

25. Los procedimientos de soporte para los sistemas de control de procesos están complicando aún más la situación. Ahora los proveedores dan soporte remoto a través de enlaces telefónicos o de conexiones a Internet. Los módems rara vez están sujetos a las comprobaciones de seguridad y se sabe que estas conexiones con los sistemas de los proveedores han servido de puerta para virus o han sido usadas para ataques directos de *hackers*.

26. Un avance reciente en control de procesos es la interconexión de los sistemas en una red de suministro más amplia. Por ejemplo, los datos de sensores de nivel de los tanques pueden ser usados para activar la reordenación automática de productos de los proveedores. Este aumento en la conectividad puede exponer sistemas de control de procesos vulnerables a amenazas externas a los sistemas proveedores e introducir riesgos en otros sistemas de la red de suministro.

27. En segundo lugar, el *software* comercial y el *hardware* de propósito general se está usando para sustituir sistemas de control de procesos propietarios. Este tipo de *software* y *hardware* a menudo no se adapta a la singularidad, complejidad, los requerimientos de tiempo real y seguridad del entorno de control de procesos. 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.

[1] N.T.: El software *comercial off-the-self* o COTS, nombrado en el documento original, se refiere a los productos disponibles para el público en general, ya sean comerciales o gratuitos, propietarios o libres, en contraposición a los productos desarrollados y utilizados en un entorno controlado.

28. Hay consecuencias potencialmente serias en el caso en el que se explotaran estas vulnerabilidades. Los efectos de un ataque electrónico en los sistemas de control de procesos pueden incluir, por ejemplo: denegación del servicio, pérdida de la integridad, pérdida de confidencialidad, pérdida de reputación (imagen), impacto en las condiciones de trabajo e impacto ambiental.

2.2. MARCO DE SEGURIDAD EN EL CONTROL DE PROCESOS

29. Las normas y las soluciones ampliamente usadas para proteger los sistemas TI a menudo no son adecuadas en un entorno de control de procesos. Aunque los sistemas de control de procesos se basan frecuentemente en tecnologías TI estándar, sus entornos operacionales difieren significativamente de un entorno TI corporativo. Mientras que algunas herramientas y técnicas de seguridad estándar se pueden utilizar para proteger sistemas de control de procesos, pueden requerir una aplicación o adaptación cuidadosa. Otras medidas de seguridad pueden ser completamente inadecuadas o no estar disponibles para su uso en un entorno de control.

30. Por ejemplo, puede que no sea posible instalar protección antivirus en los sistemas de control de procesos, debido a la falta de potencia del procesador de sistemas heredados, la edad de los sistemas operativos o la falta de certificación del proveedor. Además, las pruebas de seguridad sobre los sistemas de control de procesos deben ser abordadas con suma cautela (los análisis de seguridad pueden afectar gravemente el funcionamiento de muchos dispositivos de control). Rara vez se dedican entornos de prueba y hay pocas oportunidades de apagar los sistemas para realizar pruebas, parcheos (actualizaciones de seguridad) o mantenimiento.

31. Este documento ha sido desarrollado para proporcionar un marco de protección para los sistemas de control de procesos de ataques electrónicos. Este marco está basado en las buenas prácticas de la industria para seguridad en control de procesos y en TI y se centra en siete temas clave:

    - Comprender el riesgo del negocio
    - Implementar una arquitectura segura
    - Establecer capacidades de respuesta
    - Mejorar la concienciación y las habilidades
    - Gestionar el riesgo de terceros
    - Afrontar proyectos
    - Establecer una dirección permanente

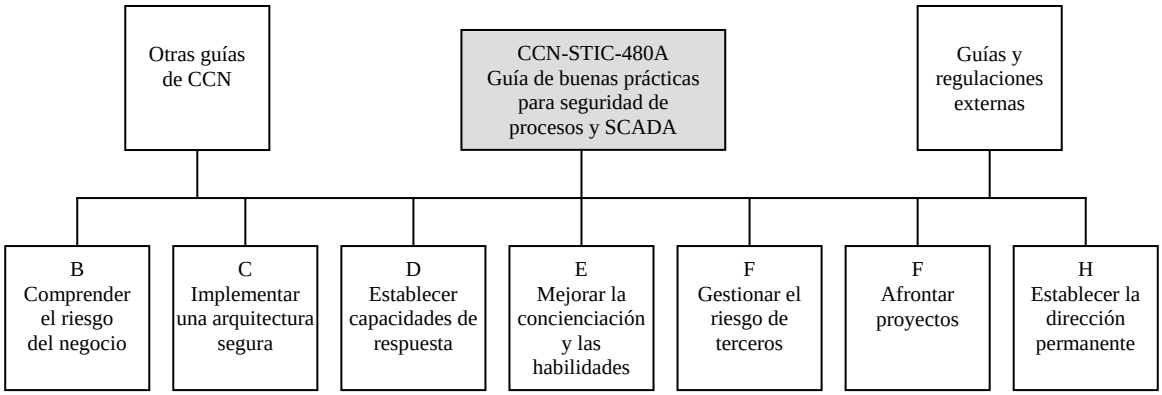


FIGURA 1: ***MARCO EN EL QUE SE INSCRIBE LA GUÍA DE BUENAS PRÁCTICAS***

32. Cada uno de estos módulos es descrito con mayor detalle en su documento aparte, este documento ofrece una visión general de todas las guías de este marco. Todas las guías de este marco pueden encontrarse en la página Web de CCN en https://www.ccn-cert.cni.es ([Ref.- 95][2]).

2.2.1. PRINCIPIOS RECTORES

33. A lo largo del desarrollo de este marco, se han utilizado tres principios rectores. Estos principios son los siguientes:

2.2.1.1. PROTEGER, DETECTAR Y RESPONDER

34. La construcción de un marco de seguridad para cualquier sistema no es sólo una cuestión de despliegue de medidas de protección. Es importante ser capaz de detectar posibles ataques y responder de forma adecuada con el fin de minimizar su impacto.

35. **Proteger**: Implementar medidas de protección específicas para prevenir y desalentar el ataque electrónico contra los sistemas de control de procesos.

36. **Detectar**: Establecer mecanismos para identificar rápidamente los ataques electrónicos reales o supuestos.

37. **Responder**: Adoptar medidas apropiadas en respuesta a incidentes de seguridad confirmados contra los sistemas de control de procesos.

2.2.1.2. DEFENSA EN PROFUNDIDAD

38. En caso de que solo se haya desplegado una única medida de protección para proteger un sistema, existe el riesgo de que si una debilidad en esa medida es identificada y explotada, no quede ninguna protección efectiva. Ninguna medida de seguridad es infalible ya que se pueden identificar vulnerabilidades y debilidades en cualquier momento. Con el fin de reducir estos riesgos, aplicar múltiples medidas de protección en serie evita puntos únicos de fallo.

[2] N.T.: [Ref.- 48]

39. Con el fin de salvaguardar los sistemas de control de procesos de ataques electrónicos (ej., *hackers*, gusanos y virus), puede ser insuficiente confiar en un único cortafuegos, diseñado para proteger entornos TI empresariales. Un modelo de seguridad mucho más eficaz sería utilizar los beneficios de un cortafuegos empresarial con un cortafuegos adicional dedicado para el control de procesos y desplegar otro tipo de medidas tales como software antivirus y detección de intrusos. Este tipo de modelo de seguridad multi-capa es denominado defensa en profundidad.

2.2.1.3. MEDIDAS DE PROTECCIÓN TÉCNICAS, DE PROCEDIMIENTO Y DE DIRECCIÓN.

40. Cuando se aplica la seguridad hay una tendencia natural a concentrar la mayoría de los esfuerzos en los elementos tecnológicos. Aunque es importante, la tecnología es insuficiente por sí sola para proporcionar una robusta protección.
41. Por ejemplo, instalar un cortafuegos no es sólo una cuestión de la instalación y configuración. También deben tenerse en cuenta los requisitos asociados de procedimiento y dirección:
    - Los requisitos del procedimiento deberían incluir el control de cambios y la vigilancia de las actividades realizadas por el cortafuegos.
    - Los requisitos de dirección deberían incluir garantizar el cortafuegos, normas, precauciones y entrenamiento.

3. COMPRENDER EL RIESGO DEL NEGOCIO

3.1. DESCRIPCIÓN

42. Antes de embarcarse en un programa para mejorar la seguridad, primero una organización debe comprender el riesgo para el negocio derivado de la posible exposición de los sistemas de control de procesos. El riesgo de negocio es una función de las amenazas, impactos y vulnerabilidades. Sólo con un buen conocimiento del riesgo de la empresa, una organización puede tomar decisiones informadas en los niveles apropiados de seguridad y las mejoras necesarias en las prácticas de trabajo. Los procesos deben establecerse para re-estudiar continuamente los riesgos de negocio a la luz de la evolución de las amenazas.

3.2. OBJETIVO

43. Obtener una profunda comprensión de los riesgos a los que se enfrenta el negocio de las amenazas de los sistemas de control de procesos con el fin de identificarlos y conducirlos al nivel adecuado de protección de seguridad que se requiere.

3.3. PRINCIPIOS DE BUENAS PRÁCTICAS

44. La guía detallada de buenas prácticas se puede encontrar en la guía "CCN-STIC-480B Seguridad en el control de procesos y SCADA – Guía 1: Comprender el riesgo del negocio" ([Ref.- 98][3]).

3.3.1. ESTUDIAR EL RIESGO DEL NEGOCIO

45. Llevar a cabo un estudio formal del riesgo de los sistemas de control de procesos para:

- **Comprender los sistemas:** realizar una auditoría y una evaluación formal del inventario de los sistemas de control de procesos. Es importante dar de alta, documentar y tener bajo control de cambios: qué sistemas existen, cuál es el papel de cada sistema, sus tareas y sus puntos críticos de seguridad, dónde se encuentran, quién es el propietario designado de cada sistema, quién gestiona cada sistema, quién da soporte a cada sistema y cómo los sistemas interactúan.
- **Comprender las amenazas:** Identificar y evaluar las amenazas a las que se enfrentan los sistemas de control de procesos. Las posibles amenazas incluyen: denegación del servicio, ataques dirigidos, incidentes accidentales, controles no autorizados, o infecciones de virus, gusanos o troyanos.
- **Comprender el impacto:** Identificar los posibles impactos y sus consecuencias para los sistemas de control de procesos. Ejemplos de tales consecuencias incluyen: pérdida de reputación (imagen), violación de requisitos reglamentarios o normativa vigente (ej., de condiciones de trabajo, medioambientales), incapacidad para cumplir los compromisos empresariales, o pérdidas financieras.

  Nota: Cuando los sistemas de control de procesos sean elementos críticos en el suministro de otros servicios clave, el impacto no debe limitarse a la empresa, pues puede tener graves consecuencias que pongan vidas en peligro.
- **Comprender las vulnerabilidades:** Llevar a cabo un estudio de vulnerabilidad de los sistemas de control de procesos. Dicha revisión debería incluir: evaluación de la infraestructura, sistemas operativos, aplicaciones, *software* usado, conexiones de red, conectividad de acceso remoto, y procesos y procedimientos.

3.3.2. REALIZAR ESTUDIOS CONTINUOS DEL RIESGO DEL NEGOCIO

- El riesgo del negocio es una función de las amenazas, los impactos y vulnerabilidades. Cualquier cambio de parámetros (ej., la modificación de un sistema) puede cambiar el riesgo del negocio. En consecuencia, es necesario un proceso continuo de gestión de riesgos para identificar cualquiera de estos cambios, reevaluar el riesgo del negocio y poner en marcha las mejoras de seguridad apropiadas.

[3] N.T.: [Ref.- 48]

4. IMPLEMENTAR UNA ARQUITECTURA SEGURA

4.1. DESCRIPCIÓN

46. En base al estudio del riesgo del negocio, las organizaciones deben seleccionar y aplicar medidas de protección técnicas, de procedimientos y de gestión para aumentar la seguridad de los sistemas de control de procesos.

4.2. OBJETIVO

47. Aplicar las medidas de protección de seguridad técnicas y los procedimientos asociados, en consonancia con los riesgos de negocio, que ofrecerán un entorno operativo seguro para los sistemas de control de procesos.

4.3. PRINCIPIOS DE BUENAS PRÁCTICAS

48. La guía detallada de buenas prácticas se puede encontrar en la guía "CCN-STIC-480C Seguridad en el control de procesos y SCADA – Guía 2: Implementar una arquitectura segura" ([Ref.- 99][4]).

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

49. Una guía detallada sobre cómo seleccionar las medidas de seguridad adecuadas y ponerlas en práctica para construir una arquitectura segura se suministra en la guía "Implementar una Arquitectura Segura" ([Ref.- 99]).

50. Las siguientes secciones ofrecen principios clave de diseño de buenas prácticas para medidas de seguridad útiles para construir una estructura de seguridad global.

4.3.1. ARQUITECTURA DE LA RED

- Identificar todas las conexiones a los sistemas de control de procesos.
- Minimizar el número de conexiones a los sistemas de control de procesos y garantizar que existen necesidades de negocio para las que se permitan.
- Separar o aislar los sistemas de control de procesos de otras redes siempre que sea posible.
- Construir infraestructuras dedicadas para los sistemas de control de procesos de seguridad crítica o específicos a un propósito.
- Eliminar, cuando sea posible, las conexiones TCP/IP entre los sistemas de seguridad (ej., sistemas de apagado de emergencia) y los sistemas de control de procesos u otras redes. En caso de que esto no sea posible, debe llevarse a cabo un análisis de riesgo.

[4] N.T.: [Ref.- 48]

4.3.2. CORTAFUEGOS

- Proteger adecuadamente las conexiones entre los sistemas de control de procesos y otros sistemas (ej., con un cortafuegos y una zona neutral[5]).
- Implementar cortafuegos con reglas ajustadas.
- La configuración del cortafuegos debe revisarse periódicamente.
- Los cambios en el cortafuegos deben gestionarse bajo un estricto control de cambios.
- Establecer unos procesos adecuados de gestión y supervisión del cortafuegos.
- Los cortafuegos deben ser gestionados por administradores con la adecuada formación.
- Debe establecerse una gestión y supervisión de los cortafuegos en régimen 24/7.

51. Una guía detallada puede encontrarse en la guía "CCN-STIC-408 Seguridad perimetral - cortafuegos" ([Ref.- 105][6]).

4.3.3. ACCESO REMOTO

- Mantener un inventario de todas las conexiones de acceso remoto y sus tipos (ej., VPN o módem).
- Garantizar de que existe una necesidad de negocio válida para todas las conexiones de acceso remoto y mantener las mínimas conexiones remotas.
- Implementar mecanismos de autenticación adecuados (ej., la autenticación fuerte), para las conexiones de acceso remoto.
- Llevar a cabo auditorias periódicas para garantizar que no hay conexiones de acceso remoto no autorizadas.
- Implementar los procesos y mecanismos de garantía para habilitar y deshabilitar las conexiones de acceso remoto.
- Restringir el acceso remoto a máquinas específicas y para determinados usuarios y, si es posible, en determinados momentos.
- Llevar a cabo revisiones de seguridad de todos los terceros que tienen acceso remoto a los sistemas de control.
- Garantizar que los equipos usados para acceso remoto están debidamente protegidos (ej., antivirus, antispam y cortafuegos personales).

4.3.4. ANTI-VIRUS

- Proteger los sistemas de control de procesos con *software* antivirus en las estaciones de trabajo y los servidores. Donde el *software* no pueda desplegarse, deben ser aplicadas otras medidas de protección (ej., uso de pasarelas o gateways con antivirus o control manual).

[5] N.T. Original: DMZ o zona desmitiliarizada
[6] N.T.: [Ref.- 86]

- Obtener la acreditación y las guías de configuración de los proveedores de los sistemas de control de procesos antes del despliegue de este tipo de software.

4.3.5. CORREO ELECTRÓNICO Y ACCESO A INTERNET

- Desactivar todo el correo electrónico y acceso a Internet de los sistemas de control de procesos.

4.3.6. SECURIZACIÓN DEL SISTEMA

- Llevar a cabo procesos de securización de los sistemas de control para prevenir ataques en red. Eliminar o desactivar los servicios y los puertos sin utilizar en los sistemas operativos y las aplicaciones para prevenir el uso no autorizado.
- Entender qué puertos están abiertos y qué servicios y protocolos son usados por los dispositivos (especialmente dispositivos tales como PLC,s y UTR). Se puede averiguar realizando un escaneo de puertos en un entorno de prueba. Todos los puertos y los servicios innecesarios deben ser deshabilitados (ej., servidores Web embebidos).
- Garantizar que todos los sistemas de seguridad incorporados están habilitados.
- Siempre que sea posible, restringir el uso de los dispositivos extraíbles (ej., CD, disquetes, memorias USB, etc.) y si es posible no utilizarlos. Cuando sea necesario utilizar dispositivos extraíbles, deben aplicarse antes de su uso procedimientos que garanticen que no contienen *malware*.

4.3.7. COPIAS DE SEGURIDAD Y RECUPERACIÓN

- Garantizar que los procedimientos de copia de seguridad y restauración están preparados, y son apropiados para las amenazas electrónica y físicas identificadas. Deben ser revisados y probados periódicamente.
- Probar regularmente la integridad de las copias de seguridad a través de una restauración completa.
- Guardar las copias de seguridad tanto localmente como en centros remotos.
- Las copias deben ser transportadas con seguridad y almacenadas adecuadamente en lugares seguros.

4.3.8. SEGURIDAD FÍSICA

- Desplegar las medidas de protección de la seguridad física para proteger los sistemas de control de procesos y los equipos de redes asociados de ataques físicos y del acceso local no autorizado. Una combinación de medidas de protección que puede ser necesaria, incluyendo bloqueo de unidades, cubiertas a prueba de manipulaciones, salas seguras para servidores, sistemas de control de acceso y circuito cerrado de televisión.

4.3.9. MONITORIZACIÓN DE LOS SISTEMAS

- Vigilar en tiempo real los sistemas de control de procesos para determinar un comportamiento inusual que podría ser el resultado de un incidente electrónico (ej., un aumento de la actividad de la red podría ser el resultado de la infección de un gusano). Una variedad de parámetros debe estar definida y supervisada en tiempo real y compararse con unos valores base para un funcionamiento normal para proporcionar una indicación de comportamiento no usual.
- Siempre que sea posible, usar sistemas de detección y prevención de intrusiones para proporcionar una visión más detallada de la actividad de la red. Estos sistemas deben adaptarse al entorno del control de procesos.
- Revisar y analizar periódicamente un conjunto de archivos de registro del sistema. Realizar copias de seguridad de los archivos de registro y proteger el acceso no autorizado o su modificación.
- Dar la debida consideración tanto a la instalación de sistemas de vigilancia física como los circuitos cerrados de cámaras de televisión o las alarmas de manipulación. Esto es especialmente importante para los centros remotos.
- Asegurarse de que se registra el acceso a zonas seguras usando tarjetas de acceso.

4.3.10. REDES INALÁMBRICAS

- La creación de redes inalámbricas es un tema candente en el ámbito de los sistemas de control industrial, debido a los importantes beneficios que proporcionan. Sin embargo, los sistemas inalámbricos pueden introducir riesgos significativos y en consecuencia sólo deben utilizarse cuando se ha realizado un estudio del riesgo que considera tanto los riesgos operacionales como los de seguridad.
- El campo de la seguridad inalámbrica está cambiando constantemente y las soluciones que se creían seguras hace un par de años, son ahora reconocidas como vulnerables. Los sistemas inalámbricos deben estar protegidos por las mejores prácticas industriales. Deben hacerse verificaciones regulares para determinar si las mejores prácticas industriales han cambiado.
- Cuando se diseñen y despliegen soluciones inalámbricas, garantizar que los mecanismos de seguridad de la solución son comprendidos y configurados correctamente.
- Para saber más sobre la protección de los sistemas inalámbricos, acudir a las guías que figuran en el apéndice A.

4.3.11. ACTUALIZACIONES (PARCHES) DE SEGURIDAD

- Implementar los procesos para el despliegue de parches de seguridad a los sistemas de control de procesos.
- Estos procesos deben apoyarse en herramientas de despliegue y auditoria.

- Los procesos deben tener en cuenta la certificación de los proveedores de parches, las pruebas de las actualizaciones antes de su aplicación y un proceso de despliegue que minimice el riesgo de interrupción durante el cambio.
- Cuando los parches de seguridad que no sean posibles o prácticos, deben considerarse medidas alternativas apropiadas de protección.

52. Se puede encontrar más información sobre la gestión de parches en sistemas Windows en la guía CCN-STIC 512 " Gestión de actualizaciones de seguridad en sistemas Windows" ([7]). Esta guía es un documento general y no es específico de los procesos de control y sistemas SCADA.

4.3.12. VERIFICACIÓN DE LOS ANTECEDENTES DEL PERSONAL

- Asegurarse de todo el personal con acceso operativo o administrativo está adecuadamente investigado.

4.3.13. CONTRASEÑAS Y CUENTAS

- Aplicar y hacer cumplir una política de contraseñas para todos los sistemas de control de procesos que incluya contraseñas fuertes y tiempos de caducidad. Se recomienda que las contraseñas sean cambiadas con frecuencia, pero cuando no sea posible o práctico, se deberían considerar alternativas apropiadas.
- Revisar periódicamente todos los derechos de acceso y borrar cuentas viejas.
- Siempre que sea posible, cambiar las contraseñas por defecto.
- Las contraseñas pueden no ser necesarias para algunas funciones (ej., el modo de sólo visualización).
- Considerar la posibilidad de implantar métodos de autenticación más fuertes para funciones críticas.

4.3.14. DOCUMENTOS DEL ENTORNO DE SEGURIDAD

- Documentar un inventario completo de los sistemas de control de proceso y sus componentes.
- Documentar el marco que proporciona la seguridad para los sistemas de control de procesos y revisarlo y actualizarlo periódicamente para reflejar las amenazas actuales. Este documento debe incluir detalles de los estudios del riesgo, asunciones hechas, vulnerabilidades conocidas y medidas de protección aplicadas.
- Garantizar que toda la documentación de los sistemas de control de procesos está segura y su acceso limitado al personal autorizado.

[7] N.T.: [Ref.- 89]

4.3.15. RESISTENCIA DE LA INFRAESTRUCTURA E INSTALACIONES

- Los sistemas deben instalarse utilizando una infraestructura adecuada, como redes redundantes.
- El equipamiento deben estar en zonas de ambiente controlado para garantizar el mantenimiento del mismo y las condiciones ambientales adecuadas.
- Cuando sea necesario, deben instalarse sistemas de extinción de incendios para proteger los sistemas de control.

4.3.16. GESTIÓN DE VULNERABILIDADES

- Implementar un sistema de gestión de vulnerabilidades para garantizar que las vulnerabilidades sean mínimas en el entorno del control de procesos. Un método común de gestión de vulnerabilidades es el análisis de seguridad. Hay riesgos potencialmente graves al escanear los sistemas de control de procesos y debe realizarse en momentos escogidos cuidadosamente, por ejemplo cuando una planta se apaga o en un entorno de prueba. Llevar a cabo un estudio completo del riesgo antes de cualquier actividad de exploración.

4.3.17. ALTAS Y BAJAS DE USUARIOS

- Implementar los procedimientos necesarios para garantizar que los nuevos usuarios reciben las cuentas correspondientes, los niveles de autorización y capacitación en materia de seguridad cuando se unan a un equipo de control de procesos.
- Implementar los procedimientos para garantizar que la información y la documentación confidencial son recuperadas, se desactivan las cuentas y se cambian las contraseñas cuando el personal deje un equipo de control de procesos o cuando los miembros del equipo cambien de roles y responsabilidades.

4.3.18. GESTIÓN DEL CAMBIO

- Certificar que todos los sistemas están sujetos a estrictos procesos de control de cambios. Deberían incluirse en estos procesos los estudios de seguridad. Puede ser necesario que los cambios sean estudiados y aprobados por múltiples procesos de control de cambios (ej., una modificación en un cortafuegos podría depender de los procesos TI y gestión de cambios en la planta).

4.3.19. PRUEBAS DE SEGURIDAD

- Siempre que sea posible deben llevarse a cabo pruebas de seguridad. Rara vez es posible hacer pruebas de seguridad en el entorno de producción, por lo que las pruebas deberían hacerse en entornos dedicados de prueba, en sistemas de respaldo, cuando estén disponibles, o durante la parada de las plantas.
- Todos los dispositivos con acceso IP deben someterse a pruebas de seguridad para comprender qué servicios y clasificaciones están disponibles y para poder garantizar que no poseen vulnerabilidades conocidas.

53. Más detalles sobre la implantación de las pruebas, se pueden encontrar en la guía CCN-STIC 303 "Inspección STIC" y ([8]). Esta guía es un documento general y no es específico para el control de proceso y sistemas SCADA.

4.3.20. PROCEDIMIENTOS DE CONEXIÓN DE DISPOSITIVOS

- Establecer un procedimiento para verificar que los productos estén libres de virus y gusanos antes de conectarlos a las redes de control de procesos.

5. ESTABLECER CAPACIDADES DE RESPUESTA

5.1. DESCRIPCIÓN

54. Establecer mecanismos de seguridad a través de los sistemas de control de procesos no es un ejercicio único. Las amenazas a la seguridad y al funcionamiento de los sistemas de control de procesos se desarrollan y evolucionan con el tiempo, y las organizaciones deben realizar el estudio continuo de la seguridad de los sistemas control de procesos. Esto incluye identificar, evaluar y reaccionar ante nuevas vulnerabilidades, cambios en las amenazas a la seguridad e incidentes de seguridad electrónica (ej., gusanos o ataques de *hackers*). Establecer procedimientos formales de gestión de las respuestas asegura que cualquier cambio en los riesgos sea identificado tan pronto como sea posible y cualquier acción correctiva necesaria se inicie rápidamente.

5.2. OBJETIVO

55. Establecer los procedimientos necesarios para supervisar, evaluar y tomar las medidas apropiadas como respuesta a los distintos eventos de seguridad electrónica.

5.3. PRINCIPIOS DE BUENAS PRÁCTICAS

56. La guía detallada de buenas prácticas se puede encontrar en la guía "CCN-STIC-480D Seguridad en el control de procesos y SCADA – Guía 3: Establecer capacidades de respuesta" ([Ref.- 100][9]).

- Formar un Equipo de Respuesta de Seguridad en Control de Procesos (ERSCP) para responder a los posibles incidentes de seguridad. Una empresa con Infraestructuras Críticas Nacionales (ICN) que desee establecer un ERSCP puede consultar al CCN para el asesoramiento y apoyo.
- Garantizar que están en funcionamiento las respuestas adecuadas para la seguridad electrónica, la continuidad del negocio y los planes de recuperación que para todos los sistemas de control de procesos.
- Garantizar que todos los planes de seguridad electrónica son regularmente mantenidos, ensayados y probados.

[8] N.T.: [Ref.- 93]
[9] N.T.: [Ref.- 48]

- Establecer un sistema de alerta temprana que notifique al personal apropiado las alertas de seguridad y los incidentes.
- Establecer procesos y procedimientos para supervisar, estudiar y poner en marcha las respuestas a los incidentes y alertas de seguridad. Las posibles respuestas pueden incluir: aumentar la vigilancia, aislar el sistema, aplicar parches o movilizar el ERSCP.
- Garantizar que todos los incidentes de seguridad en control de procesos se informan oficialmente y son revisados y las lecciones aprendidas son asumidas.

6. MEJORAR LA CONCIENCIACIÓN Y LAS HABILIDADES

6.1. DESCRIPCIÓN

57. Un enfoque global de la seguridad incluye reconocimiento técnico, de procedimiento y social – el éxito de cualquier medida técnica o de procedimiento de protección de la seguridad depende en última instancia del componente humano. Los empleados son a la vez el recurso más importante y la amenaza más grande para la seguridad. El personal de los sistemas de control de procesos a menudo no están familiarizados con la seguridad en TI y el personal de seguridad en TI a menudo no están familiarizados con los sistemas de control de procesos y su entorno operativo. Esta situación puede mejorarse aumentando el conocimiento a través de programas de concienciación general, educación y el aumento de capacidades a través de la formación.

6.2. OBJETIVO

58. Aumentar la concienciación en la seguridad del control de procesos en toda la organización y garantizar que todo el personal tenga los conocimientos y habilidades adecuados para desempeñar su función.

6.3. PRINCIPIOS DE BUENAS PRÁCTICAS

59. La guía detallada de buenas prácticas se puede encontrar en la guía “CCN-STIC-480E Seguridad en el control de procesos y SCADA – Guía 4: Mejorar la concienciación y las habilidades” ([Ref.- 101][10]).

6.3.1. AUMENTAR LA CONCIENCIACIÓN

- Comprometer a la alta dirección para asegurar que se comprenden las consecuencias en el negocio de los riesgos de seguridad en el control de procesos, y, por tanto, se realiza aprovisionamiento para la gestión de estos riesgos.
- Establecer programas de concienciación para aumentar el conocimiento general de la seguridad. Estos programas harán hincapié en las responsabilidades en seguridad, llamarán la atención sobre las amenazas actuales y aumentarán la vigilancia.

[10] N.T.: [Ref.- 48]

- Crear un modelo de negocio que apoye el programa de seguridad en el control de procesos.

6.3.2. ESTABLECER UN MARCO DE FORMACIÓN

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

6.3.3. DESARROLLAR LAS RELACIONES LABORALES

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

7. GESTIONAR EL RIESGO DE TERCEROS

7.1. DESCRIPCIÓN

60. La seguridad de los sistemas de control de procesos de una organización pueden sufrir un riesgo significativo por terceras partes, por ejemplo, proveedores, organizaciones de soporte y otros eslabones de la cadena de suministro y, por lo tanto, este aspecto merece una atención considerable. Las tecnologías que permiten una mayor interconectividad, como el acceso telefónico o Internet, traen nuevas amenazas desde el exterior de la organización. Por lo tanto, los colaboradores deben estar controlados y deben adoptarse las medidas para reducir estos riesgos potenciales.

7.2. OBJETIVO

61. Garantizar que todos los riesgos para la seguridad de proveedores, organizaciones de soporte y otros colaboradores son gestionados.

7.3. PRINCIPIOS DE BUENAS PRÁCTICAS

62. La guía detallada de buenas prácticas se puede encontrar en la guía “CCN-STIC-480F Seguridad en el control de procesos y SCADA – Guía 5: Gestionar el riesgo de terceros” ([Ref.- 102][11]).

[11] N.T.: [Ref.- 48]

7.3.1. IDENTIFICAR A LOS TERCEROS

- Identificar a todos los terceros, incluyendo proveedores y prestadores de servicios, y todos los demás eslabones de la cadena de suministro que están relacionados con los sistemas de control de procesos.

7.3.2. GESTIONAR LOS RIESGOS DE LOS PROVEEDORES

- Garantizar que las cláusulas de seguridad se detallan en todos los contratos antes de los acuerdos.
- Involucrar a todos los proveedores de forma permanente para garantizar que cualquier descubrimiento de vulnerabilidades actual o futuro en los sistemas de suministro sea identificado y notificado con rapidez a la organización usuaria.
- Solicitar a los proveedores orientación en seguridad para sus actuales sistemas de control y una hoja de ruta de seguridad para futuros desarrollos del sistema.
- Garantizar que todos los proveedores incorporan protección antivirus dentro de su sistema de control de procesos.
- Establecer con los proveedores un proceso efectivo de parcheado del *software*.
- Acordar con los proveedores procedimientos de securización para los sistemas de control de procesos que están operativos.
- Identificar todas las tecnologías utilizadas (ej., bases de datos) en los sistemas de control de procesos para garantizar que se gestionan todas las vulnerabilidades.
- Llevar a cabo inspecciones y auditorias periódicas de seguridad de todos los proveedores.

7.3.3. GESTIONAR LOS RIESGOS DE LAS ORGANIZACIONES DE SOPORTE

- Realizar evaluaciones periódicas de riesgo de las organizaciones de soporte y garantizar que se aplican las contramedidas necesarias.
- Impedir a las organizaciones de soporte el acceso a los sistemas de control de procesos hasta que se hayan aplicado las medidas necesarias para prevenir o reducir las posibles brechas de seguridad. Formalizar un contrato que defina los términos de los accesos.
- Comprometer a todas las organizaciones de soporte de forma permanente para garantizar que cualquier descubrimiento actual y futuro sobre vulnerabilidades en sus sistemas que interactúan con los sistemas de control de procesos de la empresa sea identificado y notificado a la organización usuaria.
- Aumentar la concienciación de todas las organizaciones de soporte para que comprendan plenamente los sistemas de control de procesos a los que dan soporte y acordar que dicho soporte se hará de acuerdo con los procedimientos de seguridad acordados.

7.3.4. GESTIONAR LOS RIESGOS EN LA CADENA DE SUMINISTRO

- Comprometer a cualquier organización vinculada a los sistemas de control de procesos a través de la cadena de suministro para que ofrezcan garantías de que tratan los riesgos de seguridad de su control de procesos. Como ejemplos de tales organizaciones se podrían incluir: proveedores, distribuidores, fabricantes, clientes o *joint ventures*.

8. AFRONTAR PROYECTOS

8.1. DESCRIPCIÓN

63. La aplicación de medidas de protección de seguridad en los sistemas es notablemente más difícil y costosa de hacer una vez que los sistemas se han construido y desplegado. Es de gran importancia el hecho de que aplicar medidas de seguridad en un sistema existente, ya en producción, es normalmente menos eficaz. Lidiar con los riesgos de seguridad integrando medidas de protección en los procesos de desarrollo del proyecto en una etapa temprana es más eficaz, evita excesos y por lo general es menos costoso.

8.2. OBJETIVO

64. Garantizar que todos los proyectos e iniciativas que pueden afectar al sistema de control de procesos sean identificados en las etapas iniciales de su ciclo de vida e incluyan las medidas de seguridad adecuadas en su diseño y especificación.

8.3. PRINCIPIOS DE BUENAS PRÁCTICAS

65. La guía detallada de buenas prácticas se puede encontrar en la guía “CCN-STIC-480G Seguridad en el control de procesos y SCADA – Guía 6: Afrontar proyectos” ([Ref.-103][12]).

- 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 responsable de seguridad como responsable único de la gestión de los riesgos de seguridad durante el ciclo de vida completo del proyecto.
- Asegurar que 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).

66. El documento “Cyber Security Procurement Language for Control Systems” del Laboratorio Nacional de Idaho incluye más detalles sobre este tema (ver Apéndice A).

[12] N.T.: [Ref.- 48]

9. ESTABLECER UNA DIRECCIÓN PERMANENTE

9.1. DESCRIPCIÓN

67. Una dirección formal de la gestión de la seguridad de los sistemas de control de procesos garantizará que una aproximación adecuada y coherente es seguida en toda la organización. Sin esa dirección, la protección de los sistemas de control de procesos puede ser ad-hoc o insuficiente, y puede exponer a la organización a riesgos adicionales. Un marco de dirección efectivo provee funciones y responsabilidades claras, una política y unos estándares actualizados para la gestión de los riesgos de seguridad en el control de procesos, y garantiza de que esa política y esos estándares se cumplen.

9.2. OBJETIVO

68. Proporcionar una orientación clave para la gestión de los riesgos de seguridad de los sistemas de control de procesos y garantizar el cumplimiento y revisión de la política y los estándares.

9.3. PRINCIPIOS DE BUENAS PRÁCTICAS

69. La guía detallada de buenas prácticas se puede encontrar en la guía "CCN-STIC-480H Seguridad en el control de procesos y SCADA – Guía 7: Establecer una dirección permanente" ([Ref.- 104][13]).

9.3.1. DEFINIR ROLES Y RESPONSABILIDADES

- Nombrar un responsable único de los riesgos de seguridad en el control de procesos.
- Definir las funciones y responsabilidades de todos los elementos de seguridad en el control de procesos.
- Obtener apoyo de la dirección en la gestión para la seguridad de los sistemas de control de procesos.

9.3.2. DESARROLLAR LA POLÍTICA Y LOS ESTÁNDARES

- Definir, documentar, difundir y gestionar el control de los cambios, la política oficial y los estándares para la seguridad del sistema de control de procesos. Garantizar que la política y los estándares reflejan con precisión las necesidades de la organización, apoyan las necesidades del negocio y son aceptadas por todas las partes pertinentes.
- Identificar el impacto de los ordenamientos jurídicos y los requisitos reglamentarios en la seguridad en el control de procesos. Garantizar que son contemplados en la política y los estándares estblecidos.
- Garantizar que las prácticas de seguridad del sistema de control de procesos van en línea con las necesidades del negocio y operacionales.

[13] N.T.: [Ref.- 48]

9.3.3. VELAR POR EL CUMPLIMIENTO DE LA POLÍTICA Y LOS ESTÁNDARES

- Implementar un programa de garantía para asegurar que la política y los estándares de seguridad en el control de procesos se cumplen de manera continua.

9.3.4. ACTUALIZAR LA POLÍTICA Y LOS ESTÁNDARES

- Establecer un programa continuo para asegurar que la política y los estándares de seguridad en el control de procesos se revisan periódicamente, se actualizan de acuerdo con las amenazas actuales, los cambios en los requisitos legales y reglamentarios, los cambios en el negocio y las necesidades operacionales.

10. AGRADECIMIENTOS

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

Sobre los autores

Este documento[14] 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 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 Control de Procesos y SCADA:
Email: process_control_security@paconsulting.com
Web: www.paconsulting.com/process_control_security

[14] N.T.: La versión original de este documento. La traducción ha sido realizada por CCN-CERT ([Ref.- 95]).

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.- 43] 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.- 44] BS-78582006/BS 8470:2006 Secure destruction of confidential material. Code of practice
www.bsi-global.com/en/Shop/Publication-Detail/?pid=000000000030127562

[Ref.- 45] CPNI: Best Practice Guide Commercially Available Penetration Testing
www.cpni.gov.uk/Docs/re-20060508-00338.pdf

[Ref.- 46] CPNI: Best Practice Guide on Firewall Deployment for SCADA and Process Control Networks
www.cpni.gov.uk/Docs/re-20050223-00157.pdf

[Ref.- 47] CPNI First Responders' Guide: Policy and Principles
www.cpni.gov.uk/docs/re-20051004-00868.pdf

[Ref.- 48] CPNI SCADA Good Practice Guides
www.cpni.gov.uk/ProtectingYourAssets/scada.aspx

[Ref.- 49] CPNI Information Sharing
www.cpni.gov.uk/ProtectingYourAssets/InformationSharing.aspx

[Ref.- 50] CPNI Personnel Security measures
www.cpni.gov.uk/ProtectingYourAssets/personnelSecurity.aspx

[Ref.- 51] CPNI: Good Practice Guide Patch Management
www.cpni.gov.uk/Docs/re-20061024-00719.pdf

[Ref.- 52] CPNI: Good Practice Guide Outsourcing: Security Governance Framework for IT Managed Service Provision
www.cpni.gov.uk/Docs/re-20060802-00524.pdf

[Ref.- 53] CPNI: Good Practice Guide on Pre-Employment Screening
www.cpni.gov.uk/Products/bestpractice/3351.aspx

[Ref.- 54] CPNI: An Introduction to Forensic Readiness Planning
www.cpni.gov.uk/docs/re-20050621-00503.pdf

[Ref.- 55] CPNI: Personnel Security Measures
www.cpni.gov.uk/ProtectingYourAssets/personnelSecurity.aspx

[Ref.- 56] DHS Control Systems Security Program
http://csrp.inl.gov/

[Ref.- 57] DHS Control Systems Security Program Recommended Practice
http://csrp.inl.gov/Recommended_Practices.html

[Ref.- 58] Guide to Industrial Control Systems (ICS)
http://csrc.nist.gov/publications/PubsDrafts.html

[Ref.- 59] Securing WLANs using 802,11i
http://csrp.inl.gov/Documents/Wireless%20802.11i%20Rec%20Practice.pdf

[Ref.- 60] Using Operational Security (OPSEC) to support a Cyber Security Culture in Control Systems Environments
http://csrp.inl.gov/Documents/OpSec%20Rec%20Practice.pdf

[Ref.- 61] ISA SP99 –DHS Catalog of Control System Security Requirements
www.dhs.gov

[Ref.- 62] Manufacturing and Control Systems Security
www.isa.org/MSTemplate.cfm?MicrositeID=988&CommitteeID=6821

[Ref.- 63] ISO 17799 International Code of Practice for Information Security Management
www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=39612

[Ref.- 64] ISO 27001 International Specification for Information Security Management
www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42103

[Ref.- 65] Cyber Security Procurement Language for Control Systems
www.msisac.org/scada/documents/12July07_SCADA_procurement.pdf

[Ref.- 66] MU Security Industrial Control (MUSIC) Certification
www.musecurity.com/support/music.html

[Ref.- 67] Control System Cyber Security Self-Assessment Tool (CS2SAT)
www.us-cert.gov/control_systems/pdf/CS2SAT.pdf

[Ref.- 68] Department of Homeland Security Control Systems Security Training
www.us-cert.gov/control_systems/cstraining.html#cyber

[Ref.- 69] 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.- 70] Achilles Certification Program
www.wurldtech.com/index.php

[Ref.- 71] American Gas Association (AGA)
www.aga.org

[Ref.- 72] American Petroleum Institute (API)
www.api.org

[Ref.- 73] Certified Information Systems Auditor (CISA)
www.isaca.org/

[Ref.- 74] Certified Information Systems Security Professional (CISSP)
www.isc2.org/

[Ref.- 75] Global Information Assurance Certification (GIAC)
www.giac.org/

[Ref.- 76] International Council on Large Electric Systems (CIGRE)
www.cigre.org

[Ref.- 77] International Electrotechnical Commission (IEC)
www.iec.ch

[Ref.- 78] Institution of Electrical and Electronics Engineers (IEEE)
www.ieee.org/portal/site

[Ref.- 79] National Institute of Standards and Technology (NIST)
www.nist.gov

[Ref.- 80] NERC Critical Infrastructure Protection (CIP)
www.nerc.com/~filez/standards/Cyber-Security-Permanent.html

[Ref.- 81] Norwegian Oil Industry Association (OLF)
www.olf.no/english

[Ref.- 82] Process Control Security Requirements Forum
www.isd.mel.nist.gov/projects/processcontrol/

[Ref.- 83] US Cert
www.us-cert.gov/control_systems/

[Ref.- 84] 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*".

	Sección	Documento utilizado
[Ref.- 85]	**2.2.1**	Using Operational Security (OPSEC) to Support a Cyber Security Culture in Control Environments http://csrp.inl.gov/Documents/Opsec%20Rec%20Practice.pdf
[Ref.- 86]	**4.3.2**	Best Practice Guide on Firewall Deployment for SCADA and Process Control Networks www.cpni.gov.uk/Docs/re-20050223-00157.pdf
[Ref.- 87]	**4.3.10**	Recommended Practices Guide for Securing ZigBee Wireless Networks in Process Control System Environments http://www.us-cert.gov/control_systems/pdf/Zigbee%20Rec%20Pract%20-%20draftposted%207-10-07.pdf
[Ref.- 88]	**4.3.10**	Securing WLANs using 802,11i http://csrp.inl.gov/Documents/Wireless%20802.11i%20Rec%20Practice.pdf
[Ref.- 89]	**4.3.11**	Good Practice Guide Patch Management www.cpni.gov.uk/Docs/re-20061024-00719.pdf
[Ref.- 90]	**4.3.12**	A Good Practice Guide on Pre-Employment Screening www.cpni.gov.uk/Products/bestpractice/3351.aspx
[Ref.- 91]	**4.3.12**	Personnel Security Measures www.cpni.gov.uk/ProtectingYourAssets/personnelSecurity.aspx
[Ref.- 92]	**4.3.12**	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/BS-78582006/
[Ref.- 93]	**4.3.19**	Best Practice Guide Commercially Available Penetration Testing www.cpni.gov.uk/Docs/re-20060508-00338.pdf
[Ref.- 94]	**8.3**	Cyber Security Procurement Language for Control Systems www.msisac.org/scada/documents/12July07_SCADA_procurement.pdf

A.3. REFERENCIAS EN ESTA TRADUCCIÓN

[Ref.- 95] Portal de CCN-CERT
https://www.ccn-cert.cni.es

[Ref.- 96] CCN-STIC-480 Seguridad en sistemas SCADA

[Ref.- 97] CCN-STIC-480A Seguridad en el control de procesos y SCADA
Guía de buenas prácticas

[Ref.- 98] CCN-STIC-480B Seguridad en el control de procesos y SCADA
Guía 1: Comprender el riesgo del negocio

[Ref.- 99] CCN-STIC-480C Seguridad en el control de procesos y SCADA
Guía 2: Implementar una arquitectura segura

[Ref.- 100] CCN-STIC-480D Seguridad en el control de procesos y SCADA
Guía 3: Establecer capacidades de respuesta

[Ref.- 101] CCN-STIC-480E Seguridad en el control de procesos y SCADA
Guía 4: Mejorar la concienciación y las habilidades

[Ref.- 102] CCN-STIC-480F Seguridad en el control de procesos y SCADA
Guía 5: Gestionar el riesgo de terceros

[Ref.- 103] CCN-STIC-480G Seguridad en el control de procesos y SCADA
Guía 6: Afrontar proyectos

[Ref.- 104] CCN-STIC-480H Seguridad en el control de procesos y SCADA
Guía 7: Establecer una dirección permanente

[Ref.- 105] CCN-STIC-408 Seguridad perimetral – cortafuegos

ANEXO B. GLOSARIO DE TÉRMINOS Y ABREVIATURAS

B.1. GLOSARIO DE TÉRMINOS

Amenaza	Evento que puede desencadenar un incidente en la Organización, produciendo daños materiales o pérdidas inmateriales en sus activos.
Malware	

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 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
CSIRTUK	Combined Security Incident Response Team – United Kingdom Departamento dentro del CPNI que engloba el CERN gubernamental. Para un equivalente español, contactar con el CCN.
PLC	
UTR	
CD	
USB	
VPN	

B.3. TABLA DE EQUIVALENCIAS DE LA TRADUCCIÓN

Traducción al español	Original en inglés
TI: Tecnologías de la Información	IT: Information Tecnologies
ERSCP: Equipo de Respuesta de Seguridad en Control de Procesos	PCSRT, *Process Control Security Response Team*
ICN: Infraestructuras Críticas Nacionales	CNI, *Critical Nacional Infrastructure*
CSIRTUK	CSIRTUK , *Combined Security Incident Response Team – United Kingdom*
Zona neutral	DMZ: DeMilitarized Zone