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

SEGURIDAD EN EL CONTROL DE PROCESOS Y SCADA

Guía 5
Gestionar el riesgo de terceros

MARZO 2009

Edita:

NIPO: 076-10-072-4

Tirada: 1000 ejemplares
Fecha de Edición: marzo de 2010

LIMITACIÓN ORIGINAL DE RESPONSABILIDAD

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

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

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

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

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

AVISO LEGAL

PRÓLOGO

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

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

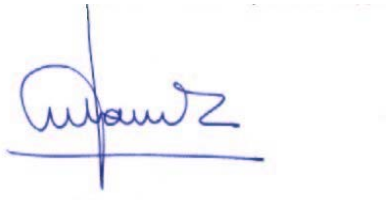
Una de las funciones más destacables del Centro Criptológico Nacional es la de elaborar y difundir normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los sistemas de las tecnologías de la información y las comunicaciones de la Administración, materializada en la existencia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

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

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

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

Febrero de 2010



Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

ÍNDICE

ANEXOS

FIGURAS

0. INTRODUCCIÓN A LA TRADUCCIÓN

0.1. ALCANCE DE ESTA TRADUCCIÓN

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

0.3. CAMBIOS EN EL FORMATO

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

1. INTRODUCCIÓN

1.1. TERMINOLOGÍA

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

1.2. ANTECEDENTES

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

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

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

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

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

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

1.3. MARCO DE SEGURIDAD EN EL CONTROL DE PROCESOS

21. Aunque los sistemas de control de procesos están a menudo basados en tecnologías de información (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 tecnologías TI estándar en el entorno de control de procesos y SCADA. Este marco pretende ser un punto de referencia para que una organización comience a desarrollar y adaptar la seguridad en el control de procesos adecuado a sus necesidades. Los siete módulos del marco se muestran a continuación en la Figura 1.

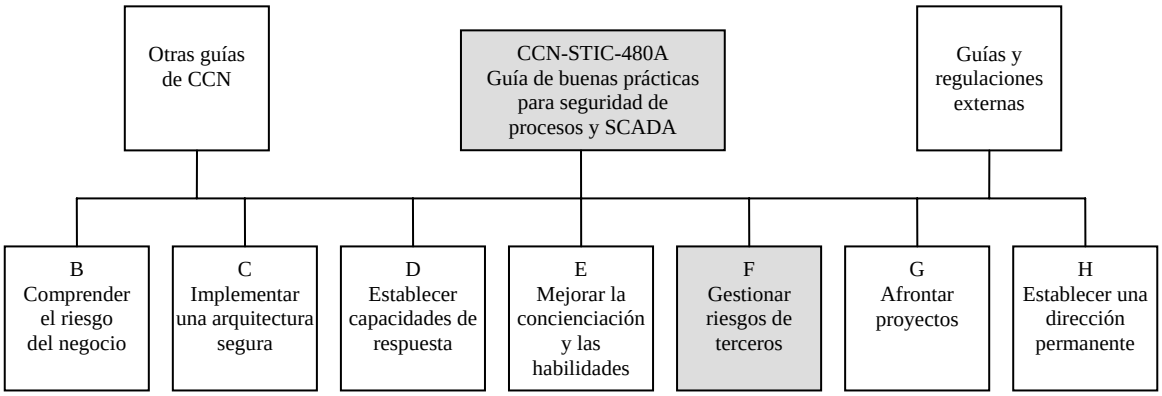


Figura 1: ***Dónde encaja esta guía dentro del marco de buenas prácticas***

23. Cada uno de estos módulos se describe con mayor detalle en su documento aparte, el presente documento proporciona una guía de buenas prácticas para comprender implementar una arquitectura segura. Todas las guías de este marco pueden encontrarse en la página web de CCN en https://www.ccn-cert.cni.es ([Ref.- 50][2]).

1.4. FINALIDAD DE ESTA GUÍA

24. La colección de guías "**Seguridad en el Control de Procesos y SCADA**" de CCN[3], proponen un marco que consta de siete módulos para abordar la seguridad en el control de procesos. La guía "Gestionar el riesgo de terceros" se basa en los fundamentos explicados en la guía de buenas prácticas, y proporciona orientación sobre las buenas prácticas de gestión de riesgos de terceros para la seguridad de los sistemas de control de procesos.

25. Esta guía no proporciona de políticas ni metodologías detalladas.

[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.- 51])

1.5. DESTINATARIOS

26. Esta guía está dirigida a cualquier persona involucrada en la seguridad de los sistemas de procesos, SCADA y automatización industrial, incluyendo:

- 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 de sistemas.

2. RESUMEN DE "GESTIONAR EL RIESGO DE TERCEROS"

27. La seguridad de los sistemas de control de procesos de una organización puede ser puesta en un importante riesgo por parte de terceras partes, por ejemplo proveedores, organizaciones de soporte y otros eslabones de la cadena de suministro, y, por tanto, este aspecto merece una atención considerable. Las tecnologías que permiten una mayor conectividad, como el acceso telefónico o Internet, traen nuevas amenazas desde el exterior de la organización. Terceras partes deben, por lo tanto, ser incluidos como parte del programa de seguridad en control de procesos y deben tomarse medidas para reducir el riesgo asociado.

28. En el pasado, los sistemas de control de procesos eran a menudo sistemas hechos en casa. Hoy en día la mayoría de los sistemas de control son desarrollados por terceros y proveedores especializados. En consecuencia, los productos y servicios de terceros están presentes en casi todos los sistemas de control de procesos, y con ellos una serie de factores de riesgo asociados.

29. La concienciación o la visibilidad del riesgo de terceros es clave para que una organización comience a gestionarlo. El reconocimiento de posibles lagunas en materia de seguridad permite a la organización buscar un compromiso adecuado con los proveedores y las organizaciones de soporte a fin de mitigar el riesgo identificado.

30. La percepción común del riesgo de terceros respecto a los sistemas de control de procesos se centra en las conexiones de acceso remoto a los sistemas de control operacional. Sin embargo, el panorama es mucho más amplio que este detalle técnico y, por lo tanto, este marco necesita una guía de buenas prácticas dedicada a este tema. Existen distintas categorías de terceros, como proveedores de sistemas de control, proveedores de soporte y diferentes elementos de la cadena de suministro. Cada una tiene sus propios temas relacionados.

31. Al considerar la vulnerabilidad de los sistemas de control de procesos se puede omitir fácilmente la importancia de estudiar la cadena completa de suministro. Sistemas aparentemente inocuos que proporcionan soporte pueden tener un efecto directo o indirecto en los sistemas críticos.

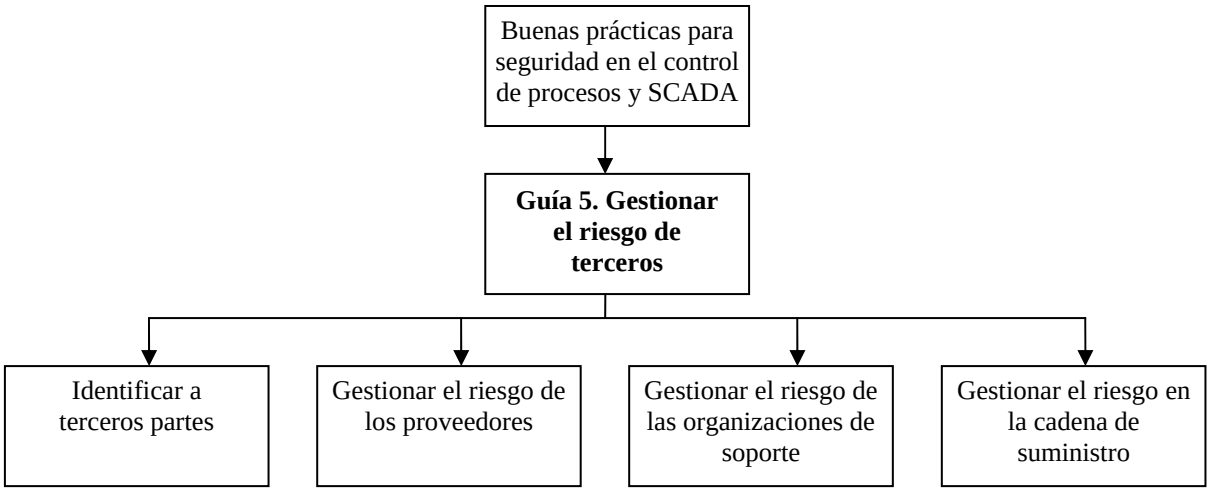


Figura 2: ***Estructura del documento "Gestionar el riesgo de terceros"***

3. IDENTIFICAR TERCERAS PARTES

3.1. CONTEXTO DE ESTA SECCIÓN DENTRO DEL MARCO GENERAL

32. Este elemento del marco se centra en la identificación todos los terceros relacionados con la seguridad de los sistemas de control de procesos. Se basa en el inventario de seguridad del control de procesos elaborado en el elemento de este marco "Comprender el Riesgo del Negocio". Esta sección hace referencia al inventario para identificar el riesgo relevante de terceros con el fin de garantizar que se gestionen adecuadamente.

33. Esta guía de identificación de terceros es la base para las otras tres secciones.

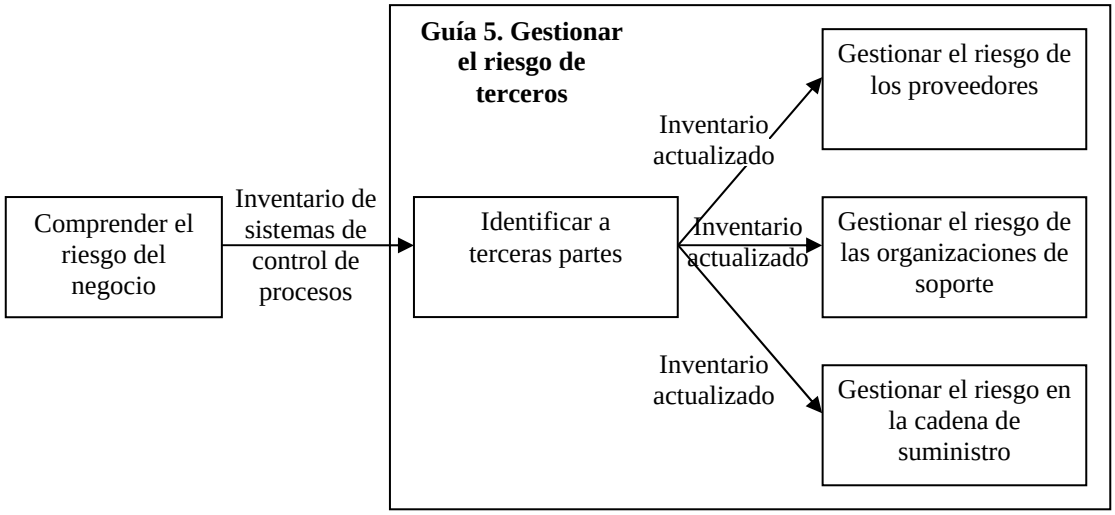


Figura 3: ***Cómo encaja "Identificar terceras partes" en este marco***

3.2. JUSTIFICACIÓN

34. La identificación de los terceros asociados con los bienes de control de procesos permite que la organización planifique y mitigue el riesgo que suponen.

3.3. PRINCIPIOS DE BUENAS PRÁCTICAS

35. Los principios generales de buenas prácticas del documento general "CCN-STIC-480A – Guía de buenas prácticas – Seguridad en el Control de Procesos y SCADA" ([Ref.- 52]), son los siguientes:

    - 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.

3.4. ORIENTACIÓN SOBRE LAS BUENAS PRÁCTICAS

36. Esta sección propone la existencia de un inventario de sistemas de control de procesos que sirva de punto de partida para identificar todos los terceros. La realización de un inventario de seguridad en el control de procesos se describe en la guía "Comprender el riesgo del negocio". Para cada elemento del inventario, hay que determinar (si los hay) qué terceros están asociados con cada elemento. Un elemento del inventario puede estar relacionado con un número de terceros distintos. Al realizar este análisis deben considerarse las siguientes cuestiones:

    - ¿Quién es el proveedor del sistema?
    - ¿Quién proporciona soporte?
    - ¿Cómo es el soporte proporcionado?
    - ¿Qué nivel de acuerdos de servicio existe?
    - ¿Qué subcontratistas están involucrados?

37. Definiciones[4].

38. La longitud de la revisión inicial del inventario de terceros depende completamente del tamaño del inventario creado. Se debe tener cuidado de lograr un equilibrio adecuado en la captura de los datos de terceros. Si se registra demasiado poco, puede que no sea suficiente para un análisis profundo en etapas posteriores. Si se captura demasiado, será difícil de mantener. Cuando la información de terceros no esté disponible con suficiente detalle durante el cotejo del inventario, esta información debe buscarse como parte de este elemento del marco. Cualquier nueva información debe ser añadida al inventario para mantenerlo actualizado.

[4] N.T.: Las traducciones aquí incluidas en el original se han movido al "**¡Error! No se encuentra el origen de la referencia.**. **¡Error! No se encuentra el origen de la referencia.**"

4. GESTIONAR EL RIESGO DE LOS PROVEEDORES

4.1. CONTEXTO DE ESTA SECCIÓN DENTRO DEL MARCO GENERAL

39. Gestionar el riesgo de los proveedores se basa en la sección anterior, en identificar a terceros, y se centra específicamente en el trabajo con los proveedores de los sistemas de control de procesos. El resultado de esta sección se utiliza en los elementos del marco "Implementar una Arquitectura Segura" y "Establecer Capacidades de Respuesta".

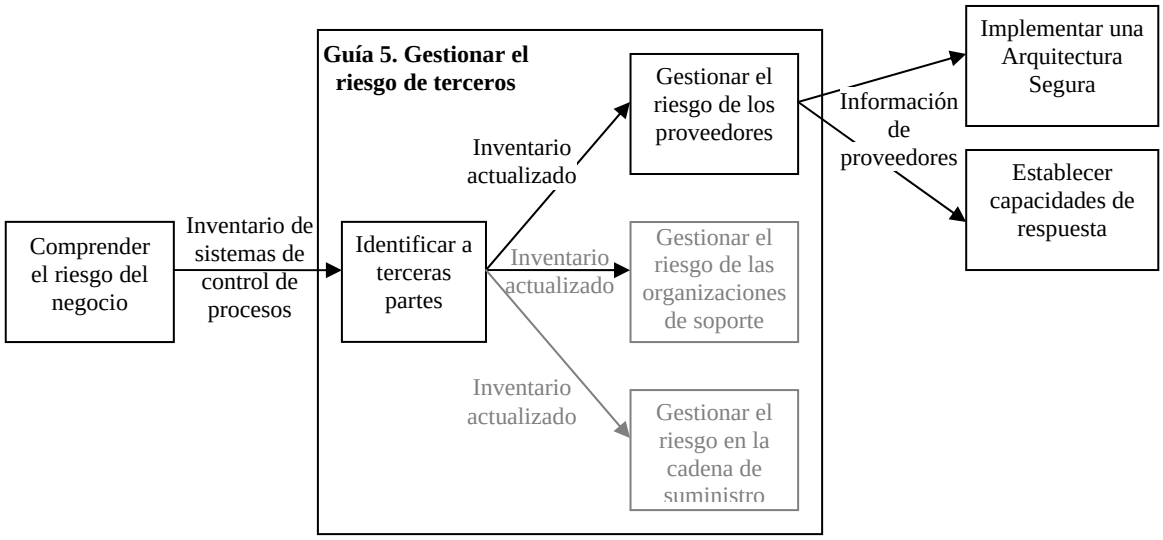


Figura 4: ***Cómo encaja "Gestionar el riesgo de los proveedores" en este marco***

4.2. JUSTIFICACIÓN

40. Desarrollando relaciones con los proveedores de sistemas de control, las organizaciones pueden influir en el diseño de los sistemas de procesos de control e influir en la seguridad de productos existentes y nuevos.

4.3. PRINCIPIOS DE BUENAS PRÁCTICAS

41. Los principios generales de buenas prácticas del documento general "CCN-STIC-480A – Guía de buenas prácticas – Seguridad en el Control de Procesos y SCADA" ([Ref.- 52]), son los siguientes:

- Asegurarse de que las cláusulas de seguridad se detallan en todos los contratos anteriores a los acuerdos.
- Involucrar a todos los proveedores de forma permanente para garantizar que cualquier descubrimiento de vulnerabilidades actual y futuro en los sistemas de suministro sea identificado y notificado rápidamente 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[5] del sistema 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.

4.4. ORIENTACIÓN SOBRE LAS BUENAS PRÁCTICAS

42. Al establecer un diálogo productivo con los proveedores de los sistemas de control de procesos, la organización tiene la oportunidad de construir una relación con ellos para comprender mejor las capacidades y limitaciones de los productos y servicios de los proveedores. Esta relación también permite a la organización comunicar mejor al proveedor sus necesidades específicas de aplicación y los requisitos asociados de seguridad.
43. Hay una serie de aspectos clave de seguridad que se beneficiarán de un diálogo bidireccional con los proveedores, y que se describen en las siguientes secciones.

4.4.1. MEDIDAS CONTRACTUALES PARA GESTIONAR EL RIESGO DE LOS PROVEEDORES

44. La creación de un marco contractual correcto es una parte esencial en la gestión del riesgo de los proveedores. Gran parte de la ardua labor es probable que se haya llevado a cabo por los departamentos legales o de adquisiciones de las organizaciones, pero es importante garantizar que los contratos con los proveedores incluyen cláusulas específicas de seguridad en control de procesos. Las cláusulas de seguridad típicas incluyen:
45. **Acuerdo de no divulgación:** El proveedor puede tener acceso a información sensible sobre la organización y es esencial que ésta no se explote ni utilice sin el permiso de la organización. Esto incluye desde el conocimiento de las reglas del cortafuegos hasta información del sistema y otra propiedad intelectual.
46. **Divulgación de vulnerabilidades:** Es importante que los descubrimientos actuales y futuros de vulnerabilidades sean comunicados por el proveedor al dueño del sistema para que puedan adoptarse las medidas oportunas.
47. **Controles de antecedentes/controles de seguridad interna:** La organización debe pedir garantías a los proveedores de que sus empleados se han sometido a los pertinentes controles de seguridad de antecedentes antes de ser empleados o contratados. Se pueden encontrar más datos sobre la investigación previa al empleo en la guía “A Good Practice Guide on Pre-Employment Screening” ([Ref.- 43][6]), en la página web de medidas de

[5] N.T.: *hardening*
[6] N.T.: [Ref.- 43]

seguridad del personal del CPNI ([Ref.- 44][7]) y en BS7858 ([Ref.- 45][8]).. La ubicación de estos documentos puede encontrarse en el Apéndice A.

48. **Acreditación de proveedores:** Introducir los requisitos de seguridad en el control de proceso en la selección y acreditación del proveedor preferido es un proceso muy poderoso para garantizar que la cultura y el enfoque de seguridad deseados forman parte de las decisiones tomadas. La lista resultante de proveedores aprobados puede ahorrar tiempo y dinero a la organización reduciendo la duplicidad y previendo garantías de los posibles proveedores. Desde la perspectiva de los proveedores, es un incentivo para estar en la lista de proveedores aprobados, ya que puede ser una buena fuente de negocio.
49. **Requisitos de seguridad para nuevos proyectos:** Cuando se planean proyectos de nuevos procesos o nuevos sistemas es esencial que la seguridad se incluya desde el principio en las discusiones contractuales, especialmente si participan nuevos proveedores. Por favor, consulte la Guía 6 "Afrontar Proyectos" ([Ref.- 58]).
50. **Revisiones de seguridad:** Deben realizarse revisiones regulares de seguridad con el proveedor para tratar cuestiones de seguridad extraordinarias, el progreso frente a la mitigación y los planes de mejora, y para discutir la hoja de ruta de seguridad.
51. El documento de "Cyber Security Procurement Language for Control Systems" del Laboratorio Nacional de Idaho ([Ref.- 46][9]) proporciona más detalles sobre este tema (véase el apéndice A).

4.4.2. PRINCIPALES TEMAS A CONSIDERAR RESPECTO A LOS PROVEEDORES

52. Al trabajar con el proveedor, hay algunas formas de gestionar la mitigación del riesgo asociado a los proveedores, incluyendo:
53. **Antivirus:** Trabajar con los proveedores para garantizar la protección antivirus se incorpora en sus sistemas de control.
54. **Parcheado:** Acordar con el proveedor qué proceso se usará para probar y acreditar los parches de seguridad. Las cuestiones que deben considerarse son:
    - ¿Se acreditan los parches?
    - ¿Se notifica a los clientes y se despliegan los parches acreditados?
    - ¿Cuánto tiempo se tarda en acreditar?
    - ¿Hay notas de instalación o asistencia sobre los parches que se deban desplegar?
55. Algunos proveedores están dispuestos a probar todos los parches de seguridad antes de su aprobación para el despliegue. Esto puede implicar una estipulación de que sólo los parches y las actualizaciones recibidas directamente de los proveedores son válidas para actualizar el sistema. Puede haber un retraso como consecuencia de este enfoque, por lo que es importante trabajar en estrecha colaboración con el proveedor para garantizar que las necesidades de seguridad de la organización se cumplan, y que el proveedor tenga conocimiento de cualquier retraso que la organización imponga (ej., control de cambios).

[7] N.T.: [Ref.- 44]
[8] N.T.: [Ref.- 45]
[9] N.T.: [Ref.- 46]

56. **Asistencia en la securización del sistema[10]:** La mayoría de los sistemas y equipos de control de procesos vienen de fábrica bastante desprotegidos, lo que significa que pueden ser usadas todas sus funcionalidades. Dado que la organización tendrá requisitos relativamente específicos, es importante que las funcionalidades no usadas estén desactivadas para evitar riesgos innecesarios. Se debe pedir a los proveedores que proporcionen orientación sobre el bloqueo o la securización de los sistemas.

57. **Las tecnologías usadas:** Algunas aplicaciones de control de procesos usan tecnologías que suponen un riesgo potencial. Por ejemplo, algunos sistemas de control de procesos usan componentes de base de datos que no están demasiado visibles para el usuario, pero que pueden requerir parches y mantenimiento.

58. **Soporte remoto:** El principal riesgo que debe abordarse en el compromiso con los proveedores es el soporte remoto. Ese soporte debe proporcionarse a través de una conexión segura, pero la historia no termina ahí. Los sistemas desde los que se conectan los proveedores también deben ser seguros, tanto física como electrónicamente. El personal que los usa debe tener una comprobación de sus antecedentes y estar debidamente formado, y cualquier información confidencial de los clientes (como la documentación del sistema) debe estar debidamente protegida. Las organizaciones se deben asegurar de estos temas (posiblemente a través de las visitas o auditorías).

59. **Pruebas de seguridad:** Las organizaciones deben incitar a los proveedores para que lleven a cabo pruebas de seguridad de sus productos para identificar y eliminar vulnerabilidades de seguridad. Puede hacerse una revisión del diseño del sistema, pruebas de laboratorio o pruebas de penetración. Las investigaciones recientes han puesto de relieve una serie de vulnerabilidades de seguridad en dispositivos de control de bajo nivel, tales como Unidades Terminales Remotas (UTR) y Controladores Lógicos Programables (PLC). Las organizaciones deben obtener garantías de los proveedores y vendedores de que estos dispositivos de control de bajo nivel han sido debidamente analizados para identificar qué puertos y servicios se usan y si existen vulnerabilidades conocidas. Las organizaciones deben exigir a los proveedores que lleven a cabo pruebas sobre los sistemas de control y sus componentes (tales como PLC) para garantizar que están libres de vulnerabilidades de seguridad. Más información sobre las pruebas y garantías de los dispositivos de control embebidos se incluyen en la guía 6 de este marco "Afrontar Proyectos" ([Ref.- 58]).

60. **Divulgación de los sistemas de comunicación:** Las organizaciones deben incitar a los proveedores a detallar los puertos y protocolos utilizan.

4.4.3. EMBEBER LA CULTURA DE SEGURIDAD EN LOS PROVEEDORES

61. La organización debe intentar influir la cultura de seguridad del proveedor para que cumpla o supere los requisitos de la organización. Las actividades típicas que crean una sólida cultura de seguridad y que deberían incitarse o incluso ordenarse a los proveedores incluyen:

- Revisiones regulares de seguridad
- Auditorías de seguridad
- Una cultura de seguridad y concienciación

[10] N.T.: *system hardening*

- Diálogo abierto acerca de vulnerabilidades
- Hoja de ruta de seguridad para mejorar esta en los proveedores
- Relaciones con proveedores de seguridad.

4.4.4. INFLUENCIAR EN LA HOJA DE RUTA DE SEGURIDAD DE LOS PROVEDORES

62. Una de las principales ventajas de construir una buena relación con los proveedores es la oportunidad de trabajar con ellos para influir en la dirección y el ritmo de su desarrollo de la seguridad, es decir, de la hoja de ruta de seguridad del proveedor. Es una potencial relación "ganador-ganador" pues el proveedor puede obtener una valiosa perspectiva de mercado y la organización puede mitigar las vulnerabilidades mejorando los productos y servicios del proveedor.

63. Los recientes avances en la acreditación de software antivirus y parches de sistema operativo por algunos de los principales proveedores se ha visto influida en cierta medida por el poder adquisitivo de un número de grandes organizaciones que buscan mejorar la seguridad de los sistemas de control de procesos. Estableciendo un diálogo permanente con las organizaciones de los proveedores pudieron transmitir sus prioridades y preocupaciones ante la incapacidad de protegerse contra los virus. La comunicación de estos requisitos de una serie de organizaciones permitió a los proveedores crear casos de negocio que permitieran la investigación y el desarrollo en este ámbito. Esto se ha traducido en mejores medidas de seguridad en los productos de sistemas de control.

5. GESTIONAR EL RIESGO DE LAS ORGANIZACIONES DE SOPORTE

5.1. CONTEXTO DE ESTA SECCIÓN DENTRO DEL MARCO GENERAL

64. Gestionar el riesgo de las organizaciones de soporte se basa en los terceros identificados y se centra específicamente en el trabajo con organizaciones de soporte. Los resultados de esta sección pueden ser utilizados en los elementos de este marco de buenas prácticas "Implementar una arquitectura segura", "Establecer capacidades de respuesta" y "Mejorar la concienciación y las habilidades".

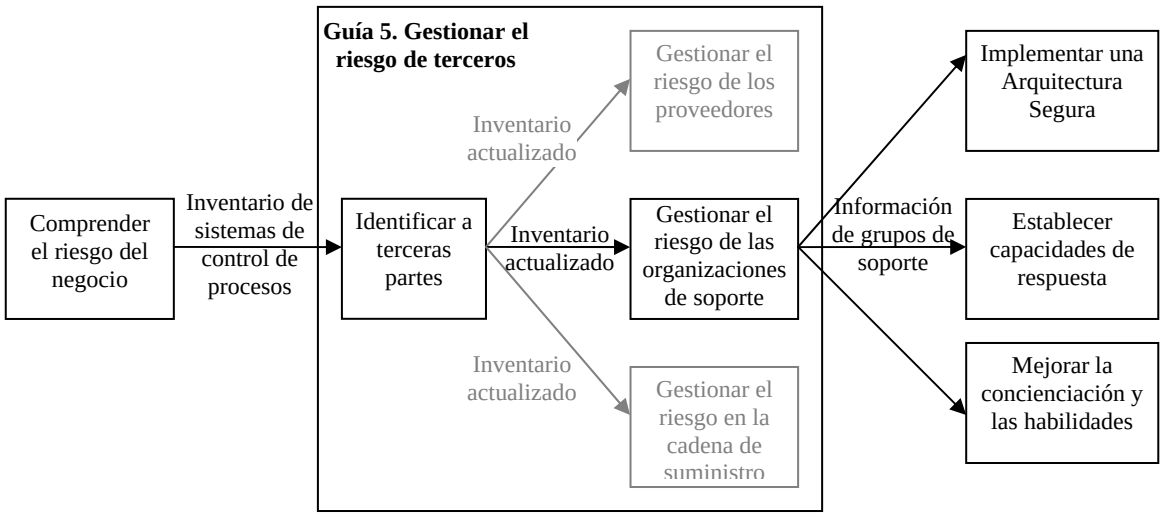


Figura 5: ***Cómo encaja "Gestionar el riesgo de las organizaciones de soporte" en este marco***

5.2. JUSTIFICACIÓN

65. Estableciendo una relación con las organizaciones de soporte, el potencial riesgo de seguridad relacionad puede ser tratado.

5.3. PRINCIPIOS DE BUENAS PRÁCTICAS

66. Los principios generales de buenas prácticas del documento general "CCN-STIC-480A – Guía de buenas prácticas – Seguridad en el Control de Procesos y SCADA" ([Ref.- 52]), son los siguientes:

- Realizar evaluaciones periódicas de riesgo de las organizaciones de soporte y garantizar que se aplican las contra-medidas 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. Acordar 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.

5.4. ORIENTACIÓN SOBRE LAS BUENAS PRÁCTICAS

67. Como sucede con muchas áreas dentro del entorno de TI, hay muchos sistemas de control de procesos que reciben soporte de alguna manera de terceros. En consecuencia, la

seguridad de los sistemas de control de procesos depende a menudo de manera crítica de la organización de soporte y los servicios que prestan tales como:

- Provisión y soporte de red y telecomunicaciones.
- Gestión de la infraestructura TI.
- Monitorización y soporte de aplicaciones y sistemas.

68. El soporte de terceros de sistemas de control de procesos permite a una organización recibir soporte especialista al mismo tiempo que reduce el coste asociado con la formación y contratación. Cuando se introducen nuevas tecnologías es el tercero el que debe asegurarse de que tiene los recursos adecuados para proporcionar un soporte eficaz.
69. Además de los servicios comunes que se han descrito, las organizaciones tal vez deseen considerar un aumento en el uso de terceros para proporcionar servicios adicionales de seguridad y administración como parte de una arquitectura global de seguridad. Ejemplos de estos servicios incluyen:
    - Monitorización del funcionamiento, la seguridad y la el rendimiento del sistema
    - Parcheados de seguridad
    - Administración y monitorización de cortafuegos
    - Monitorización de detección de intrusos
    - Protección antivirus
    - Rutinas habituales de monitorización de seguridad, por ejemplo, monitorización de registros, conexiones de acceso remoto, cambios de contraseñas, etc.
70. La elección de qué servicios pueden ser soportados por un tercero debe basarse en la criticidad del sistema, el soporte necesario, la disponibilidad de recursos internos adecuadamente cualificados y el alcance del mantenimiento.
71. Más detalles sobre contratación externa se pueden encontrar en la guía CPNI señalada en el apéndice A ([Ref.- 10][11]).
72. La implicación de terceras organizaciones en el soporte a sistemas de control de procesos puede introducir riesgo, así como ser parte de la solución de seguridad. Las áreas de riesgo principales que deben considerarse son:
    - Conexiones de soporte remotas
    - Seguridad de personal
    - Problemas contractuales
    - Concienciación y formación en seguridad
    - Seguridad física
    - Confidencialidad
73. Cada uno de estos temas se trata con más detalle en las secciones siguientes.
74. Las organizaciones de soporte a menudo desempeñan funciones y servicios similares que los proveedores de sistemas de control. En consecuencia, los principios de buenas

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

prácticas son muy similares a los trazados para gestionar el riesgo de los proveedores y se centrará en la necesidad de tener unos acuerdos contractuales claros, buena relación de trabajo y los canales de comunicación claros.

5.4.1. CONEXIONES DE SOPORTE REMOTO

75. El soporte de terceros debe garantizar que cualquier nueva tecnología introducida en un sistema de control de procesos seguro esté autorizado por la organización. La adición de dispositivos como módems o *routers* para permitir el soporte remoto o fuera de horario es un riesgo potencial, y solo deben utilizarse con la autorización previa de la organización y tras protegerse convenientemente. Probablemente haya una negociación entre la conveniencia y la seguridad, y muchos terceros pueden ofrecer importantes reducciones de precios ofreciendo soporte remoto. Para minimizar el riesgo asociado con el acceso/soporte remoto se debe considerar:

    - Negar el acceso hasta que las conexiones estén protegidas.
    - Garantizar que los permisos de acceso son revisados y auditados periódicamente.
    - Garantizar las instalaciones y los sistemas desde los que la organización de soporte se conecta también sean seguros, tanto física como electrónicamente.
    - Garantizar que la información confidencial del cliente (como la documentación del sistema) se almacenan de forma segura.
    - Las conexiones tienen un tiempo límite.

76. Las organizaciones pueden querer obtener garantías sobre estos temas a través de visitas, revisiones o auditorías.

5.4.2. SEGURIDAD DEL PERSONAL

77. Una parte esencial en cualquier marco de seguridad de sistemas es el elemento humano. Los aspectos de seguridad del personal deben ser considerados al garantizar la seguridad de terceros.

78. Todo el personal debe someterse a los controles apropiados de seguridad y a la entrega de sus antecedentes como parte rutinaria del proceso de contratación de los terceros.

79. Más datos sobre la investigación previa al empleo se puede encontrar en la guía del CPNI ”A Good Practice Guide on Pre-Employment Screening” ([Ref.- 47][12]) y en BS7858 ([Ref.- 49][13]).. La ubicación de estos documentos figura en el Apéndice A.

80. CCN-CERT presta asesoramiento sobre el control continuo del personal, así como los controles previos a la contratación (véase el apéndice A).

[12] N.T.: [Ref.- 47]
[13] N.T.: [Ref.- 49]

5.4.3. CUESTIONES CONTRACTUALES DEL PROVEEDOR

81. Hay una serie de elementos de seguridad que deben considerarse en cualquier contrato de soporte de terceros:

    - **Derecho a auditar:** Incluir cláusulas para garantizar el derecho a auditar o revisar los servicios sistemas y locales de terceros.
    - **Confidencialidad de la información:** Incluir cláusulas que garanticen la confidencialidad de la información confidencial del cliente (como la documentación del sistema). Asegurarse de que se incluye un acuerdo de no divulgación.
    - **Acuerdos de nivel de servicio adecuados:** Asegurarse de que los niveles de servicio están claramente definidos en el contrato y son adecuados a las necesidades de la organización.

5.4.4. CONCIENCIACIÓN Y FORMACIÓN EN SEGURIDAD

82. El personal de soporte de terceros debe tener un nivel apropiado de concienciación en seguridad. No todo el mundo necesita ser un experto en seguridad, pero todos deben tener la concienciación técnica, de procedimiento y operacional en seguridad adecuada para llevar a cabo su función con seguridad. Se debe incluir:

    - **Políticas y normas:** garantizar que todo el personal es consciente de qué políticas y normas están vigentes para los sistemas soportados.
    - **Procedimientos de seguridad específicos de las empresas:** la organización puede tener procesos de seguridad específicos que deben ser comunicados a terceros.
    - **Plan de respuesta y continuidad:** garantizar que una organización de soporte tiene preparados los planes de respuesta y continuidad adecuados.
    - **Habilidades:** garantizar que el personal tiene las habilidades prácticas y la formación necesarias para realizar su tarea de soporte. Hay una serie de acreditaciones industriales estándares asociadas con seguridad y soporte, pero es importante obtener garantías de que el personal tiene tanto el conocimiento práctico como las calificaciones formales.

83. Puede encontrarse más información en la guía de buenas prácticas "Mejorar el conocimiento y habilidades" ([Ref.- 56]).

6. GESTIONAR EL RIESGO EN LA CADENA DE SUMINISTRO

6.1. CONTEXTO DE ESTA SECCIÓN DENTRO DEL MARCO GENERAL

84. Este elemento del marco se centra en la identificación de las conexiones y las dependencias dentro de la cadena de suministro que fueron identificadas en “Comprender el riesgo de negocio” y en la gestión del riesgo asociado. Los dos principales resultados de este elemento son "Implementar una arquitectura segura "y" Establecer capacidades de respuesta”.

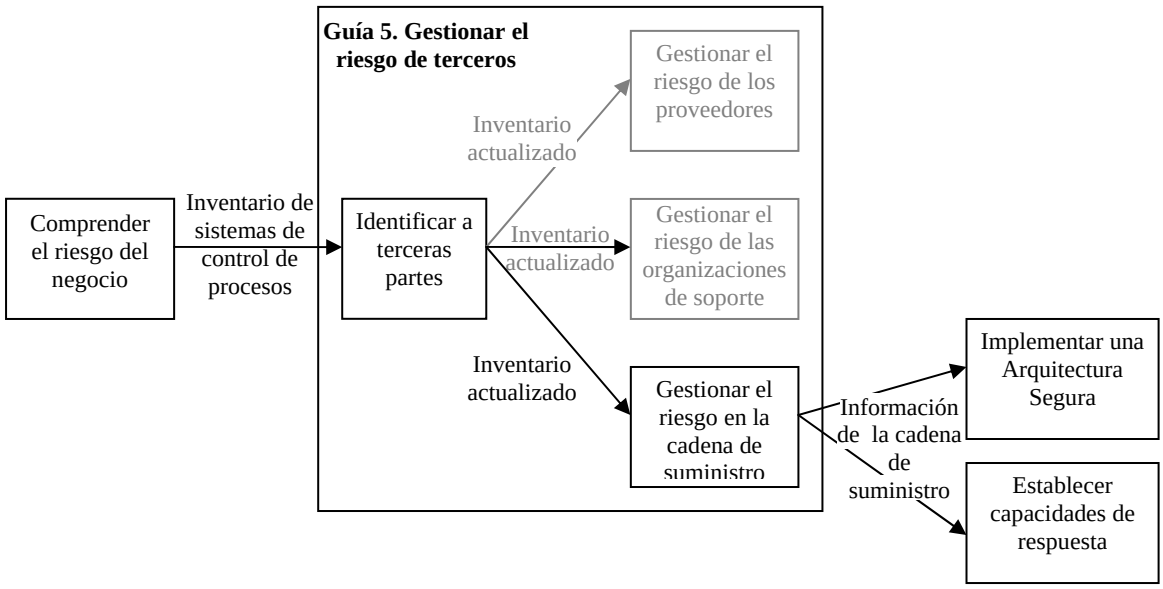


Figura 6: ***Cómo encaja "Gestionar el riesgo en la cadena de suministro" en este marco***

6.2. JUSTIFICACIÓN

85. Conectar los sistemas de control de procesos a otros elementos de la cadena de suministro puede proporcionar importantes beneficios empresariales en términos de menores costes y mayor eficiencia. Sin embargo estas conexiones pueden introducir un riesgo de seguridad al conectar redes o sistemas a sistemas externos. Forzar la integración en la cadena de suministro puede introducir más dependencias y volver toda la cadena menos resistente a las alteraciones de los sistemas individuales de la cadena de suministro. En consecuencia, un evento de seguridad en un sistema en la cadena de suministro podría repercutir en toda la cadena e interrumpir muchos otros sistemas (posiblemente en una serie de organizaciones distintas). Cuando los sistemas forman parte de una cadena de suministro es importante evaluar las dependencias y garantizar que todos los sistemas están protegidos convenientemente con medidas de seguridad y capacidades de respuesta.

6.3. PRINCIPIOS DE BUENAS PRÁCTICAS

86. Los principios generales de buenas prácticas del documento general "CCN-STIC-480A – Guía de buenas prácticas – Seguridad en el Control de Procesos y SCADA" ([Ref.- 52]), son los siguientes:

- 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 o clientes o *joint ventures*.

6.4. ORIENTACIÓN SOBRE LAS BUENAS PRÁCTICAS

87. Los requisitos fundamentales para gestionar el riesgo en la cadena de suministro son comprender la propia cadena de suministro y las dependencias que existen en ella. La organización debería identificar también los caminos críticos en la cadena de suministro. Allí donde los sistemas o conexiones superan los límites de la organización, se deben acordar convenios claros de responsabilidad en seguridad con las partes pertinentes.

88. Existe el peligro de que muchas de las funciones o procesos específicos en una cadena de suministro operen en una mentalidad de "silo", y sólo se preocupen de lo que tienen que hacer y no se centren en el riesgo desde el punto de vista de toda la cadena de suministro.

89. Las conexiones en la cadena de suministro puede variar significativamente de un sector a otro. Ejemplos de algunas conexiones con terceros en la cadena de suministro son:

- Entre la generación de energía y los sistemas de distribución, transmisión o comercio de energía
- Entre los sistemas de producción de petróleo y gas y los sistemas de intercambio
- En los sistemas de pedidos automatizado
- En las tuberías (hacia el origen y hacia el destino)
- En las instalaciones de carga de cisternas
- En los proveedores de servicios (ej., gas, agua, electricidad, aire comprimido, vapor, etc.)
- En los socios, por los informes de producción.

90. Hay dos principales zonas de riesgo que deben considerarse para cada relación en la cadena de suministro:

- Seguridad de la relación
- Dependencias en la cadena de suministro.

6.4.1. SEGURIDAD EN LA RELACIÓN

91. Algunas relaciones entre sistemas de control de procesos pueden ser puertas traseras potenciales de entrada en los sistemas de control y pueden suponer una ruta de infección para virus y gusanos o de acceso no autorizado. Dichas conexiones pueden tener distintas formas, conexiones en serie, por módem, VPN o a través de otras redes o Internet.

92. Todas estas conexiones deben ser claramente identificadas, incluidas en el inventario de sistemas de control de procesos, documentadas en los diagramas de sistema y de red, y apropiadamente protegidas y monitorizadas. Se deben establecer planes de desconexión como parte de los planes de respuesta y continuidad.

93. Además de considerar estas conexiones para la seguridad en la relación, las conexiones debe ser consideradas para las dependencias que se describen a continuación.

6.4.2. DEPENDENCIAS EN LA CADENA DE SUMINISTRO

94. Cada elemento de la cadena de suministro debe ser evaluado en función a las amenazas de seguridad para el control de procesos. Donde haya dependencias críticas, es decir, donde los sistemas de la organización dependan de otros sistemas (como consumidores o proveedores), las terceras partes deben asegurar cómo están protegidos esos sistemas desde el punto de vista de la seguridad en control de procesos. Para obtener esta garantía, las organizaciones pueden considerar revisiones de seguridad, controles de estado o auditorías. Si se considera necesario, deben prepararse los planes adecuados de respuesta y continuidad para cada dependencia.

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[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 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

[14] 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 4.4.1

[Ref.- 43] A Good Practice Guide on Pre-Employment Screening
www.cpni.gov.uk/Products/bestpractice/3351.aspx

[Ref.- 44] Personnel Security Measures
www.cpni.gov.uk/ProtectingYourAssets/personnelSecurity.aspx

[Ref.- 45] 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.- 46] Cyber Security Procurement Language for Control Systems
www.msisac.org/scada/documents/12July07_SCADA_procurement.pdf

Section 5.4.2

[Ref.- 47] A Good Practice Guide on Pre-Employment Screening
www.cpni.gov.uk/Products/bestpractice/3351.aspx

[Ref.- 48] Personnel Security Measures
www.cpni.gov.uk/ProtectingYourAssets/personnelSecurity.aspx

[Ref.- 49] 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/

A.3. REFERENCIAS EN ESTA TRADUCCIÓN

[Ref.- 50] Portal de CCN-CERT
https://www.ccn-cern.cni.es

[Ref.- 51] CCN-STIC-480 Seguridad en sistemas SCADA

[Ref.- 52] CCN-STIC-480A Seguridad en el control de procesos y SCADA
Guía de buenas prácticas

[Ref.- 53] CCN-STIC-480B Seguridad en el control de procesos y SCADA
Guía 1: Comprender el riesgo del negocio

[Ref.- 54] CCN-STIC-480C Seguridad en el control de procesos y SCADA
Guía 2: Implementar una arquitectura segura

[Ref.- 55] CCN-STIC-480D Seguridad en el control de procesos y SCADA
Guía 3: Establecer capacidades de respuesta

[Ref.- 56] CCN-STIC-480E Seguridad en el control de procesos y SCADA
Guía 4: Mejorar la concienciación y las habilidades

[Ref.- 57] CCN-STIC-480F Seguridad en el control de procesos y SCADA
Guía 5: Gestionar el riesgo de terceros

[Ref.- 58] CCN-STIC-480G Seguridad en el control de procesos y SCADA
Guía 6: Afrontar proyectos

[Ref.- 59] CCN-STIC-480H Seguridad en el control de procesos y SCADA
Guía 7: Establecer una dirección permanente

[Ref.- 60]

ANEXO B. GLOSARIO DE TÉRMINOS Y ABREVIATURAS

B.1. GLOSARIO DE TÉRMINOS

Las definiciones indicadas con un asterisco aparecían en el apartado "3. Identificar terceras partes"del documento original.

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	Nivel de riesgo, utilizado para determinar lo aceptable que puede ser un riesgo.
Probabilidad*	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.
Proveedor*	Persona, organización o integrador que provee *software*, *hardware*, *firmware* y/o documentación a la organización por un precio o en un intercambio de servicios.
Soporte*	La "provisión de la capacidad para" o la capacidad "de interactuar con" los sistemas de control de procesos, por ejemplo, monitorizar sistemas, reiniciar contraseñas, problemas, soluciones para *bugs*, etc.
Subcontrata*	Persona o entidad que entra en un acuerdo contractual con uno de los principales contratistas para realizar un servicio o tarea.

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
PLC	Programmable Logic Controllers Controladores lógicos programables
UTR	Unidades de Terminal Remota

B.3. TABLA DE EQUIVALENCIAS DE LA TRADUCCIÓN

Traducción al español	Original en inglés
TI: Tecnologías de la Información	IT: Information Tecnologies
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
PLC: controladores lógicos programables	*PLC: programmable logic controllers*
UTR: Unidad de Terminal Remota	*RTU: Remote Terminal Unit*