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

SEGURIDAD EN EL CONTROL DE PROCESOS Y SCADA

Guía 3
Establecer capacidades de respuesta

MARZO 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.

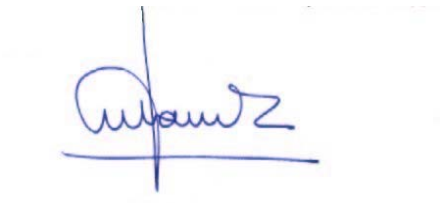
Una de las funciones más destacables del Centro Criptológico Nacional es la de elaborar y difundir normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los sistemas de las tecnologías de la información y las comunicaciones de la Administración, materializada en la existencia 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)
3. Este documento traduce la siguiente guía:
   - 00755 - Process Control and SCADA Security Guide 3. Establish response capabilities
4. El CCN ha publicado la guía CCN_STIC-480 "Seguridad en sistemas SCADA" que, junto con el resto de guías publicadas y utilizando estas traducciones adapta la seguridad al contexto de España.
5. El CCN se adhiere a la cláusula de responsabilidad del CPNI sobre el contenido de la presente guía.

0.2. CAMBIOS EN EL CONTENIDO

6. Por coherencia con el resto de guías CCN-STIC, se han añadido la portada, la Limitación de Responsabilidad y el Prólogo el presente capítulo 0 de introducción.
7. Se ha traducido de todos los apartados desde el 1 hasta el final, incluyendo la Cláusula Original de Exención de Responsabilidad y los Agradecimientos. Se respeta el contenido original, con las siguientes salvedades:

- Cuando una traducción requiere una explicación, (ej., cuando el conocimiento de los términos del documento original pueda suponer algún matiz), se incluyen notas a pie de página, precedidas de "N.T.:", indicando matices de la traducción. Debido a este hecho, el orden de las notas al pie no se corresponde con el orden en la guía original
- Siempre que aparece una referencia a un recurso en inglés y exista un recurso equivalente en español o relativo a España, se habrá sustituido. Las referencias a recursos del CPNI han sido convertidas a referencias del CCN-CERT siempre que ha sido posible. La referencia original se indicará a pie de página como una N.T.
- Los nombres propios y las siglas se han traducido. Las equivalencias entre referencias en inglés y en español se lista en el apartado "B.3. Tabla de equivalencias de la traducción" del "ANEXO B. Glosario de Términos y Abreviaturas". No se han traducido las siglas CPNI, SCADA, PA Consulting Group.

8. Se han añadido los Anexos comunes a las guías CCN-STIC, con el siguiente contenido:
9. ¡Error! No se encuentra el origen de la referencia.**.** ¡Error! No se encuentra el origen de la referencia.: Contiene todas las referencias que aparecen tanto en el documento original en inglés como en el documento actual. Los Anexos originales de referencias se han integrado en este Anexo. Las referencias se han numerado en base al resto de guías CCN-STIC.
    - A.1. Referencias Generales SCADA: Contiene el Anexo "*General SCADA References*" del documento original del CPNI.
    - A.2. Documentos y Páginas Web de Referencia: Contiene el Anexo "*Appendix A: Document and website references used in this guide* " del documento original del CPNI.
    - A.3. Referencias en esta traducción: Contiene las nuevas referencias añadidas en este documento de traducción.
10. **ANEXO B. Glosario de Términos y Abreviaturas**: Contiene las definiciones de los términos y abreviaturas que aparecen en el texto.
    - B.3. Tabla de equivalencias de la traducción: Contiene las equivalencias entre los términos técnicos en inglés, utilizados en el documento original, y los términos en español usados en la traducción.

0.3. CAMBIOS EN EL FORMATO

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

1. INTRODUCCIÓN

1.1. TERMINOLOGÍA

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

1.2. ANTECEDENTES

16. Los sistemas de control de procesos y SCADA hacen uso y se están volviendo progresivamente más dependientes de las tecnologías 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 TI estándar, sus entornos operacionales difieren significativamente de un entorno TI corporativo. Pueden aprovecharse muchas lecciones de la experiencia adquirida por los expertos de seguridad en TI y, tras la adaptación de algunas herramientas y técnicas de seguridad estándar, se pueden usar para proteger sistemas de control de procesos. Otras medidas de seguridad estándar pueden ser completamente inapropiadas o no estar disponibles para su uso en un entorno de control.

22. Este marco de seguridad en el control de procesos se basa en las buenas prácticas de la industria para seguridad en el control de procesos y en TI. Está centrado en siete temas clave para el uso de las tecnologías TI estándar en el entorno de control de procesos y SCADA. Este marco pretende ser un punto de referencia para que una organización comience a desarrollar y adaptar la seguridad en el control de procesos adecuado a sus necesidades. Los siete módulos del marco se muestran a continuación en la Figura 1.

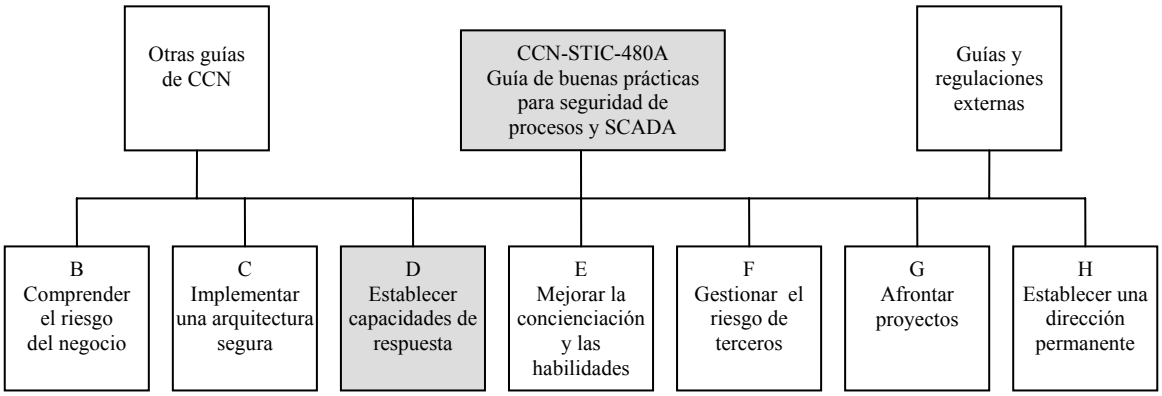


Figura 1: ***Dónde encaja esta guía dentro del marco de buenas prácticas***

23. Cada uno de estos módulos se describe con mayor detalle en su documento aparte, el presente documento proporciona una guía de buenas prácticas para comprender implementar una arquitectura segura. Todas las guías de este marco pueden encontrarse en la página Web de CCN en https://www.ccn-cert.cni.es ([Ref.- 56][2]).

1.4. FINALIDAD DE ESTA GUÍA

24. La colección de guías "**Seguridad en el Control de Procesos y SCADA**" de CCN-CERT[3], proponen un marco que consta de siete módulos para abordar la seguridad en el control de procesos. Esta guía "**Establecer capacidades de respuesta**" se basa en los fundamentos explicados en la guía de buenas prácticas y proporciona orientación para establecer las capacidades de respuesta relacionadas con las amenazas a la seguridad digital del control de procesos y los sistemas SCADA.

25. En esta guía no incluye planes ni procedimientos detallados de respuesta, pues pueden variar de organización a organización y de sistema a sistema.

[2] N.T.: www.ccn-cert.cni.es
[3] N.T.: Traducción de las guías del CPNI y complementadas con la guía "Seguridad en Sistemas SCADA" ([Ref.-57])

1.5. DESTINATARIOS

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

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

2. RESUMEN DE "ESTABLECER CAPACIDADES DE RESPUESTA"

27. Las organizaciones que se dedican al control de procesos ya tendrán preparados planes de recuperación de desastres (PRC) y de continuidad de negocio (PCN). Sin embargo, debido a los cambios en entorno operativo del control de procesos que se ha discutido, estos planes a menudo son insuficientes para responder ante la amenaza de ataques electrónicos.

28. Las medidas de protección no pueden proporcionar el 100% de protección a los sistemas, porque las vulnerabilidades, tanto técnicas como no técnicas, seguirán existiendo independientemente del régimen de protección. Una parte esencial de cualquier estrategia de seguridad es, por tanto, reconocer que el riesgo residual seguirá existiendo y tendrá que ser gestionado junto con la capacidad de identificar y responder a cualquier otro cambio en las amenazas.

29. Los análisis indican que los incidentes de seguridad en el proceso de control causados por un ataque electrónico han ocurrido raramente y causado interrupciones mínimas. Estos incidentes se están volviendo más que frecuentes[4] y las organizaciones tienen que prepararse contra ellos, tanto revisando su régimen de seguridad como desarrollando y revisando las políticas y procedimientos de respuesta a incidentes.

30. Una de las cuestiones que debe considerarse es que los enfoques habituales para garantizar la información que se aplican en una oficina pueden no ser adecuados para los sistemas de control de procesos. Estos sistemas se enfrentan a menudo a diferentes desafíos y limitaciones. Aunque las diferencias pueden ser sutiles, es importante considerarlas en particular al desarrollar los requisitos de seguridad de la información y al preparar los planes de respuesta a incidentes.

[4] *El 70% de los incidentes de seguridad en el período 2001-2003 fueron generados externamente en comparación con el 31% entre 1982-2000. El 41% de los incidentes produjo pérdida de producción, más un 29% informó de una pérdida de la visión del proceso.*
"Los mitos y hecho para los sistemas de control industrial detrás de los riesgos de seguridad cibernética", Eric Byre & Justin Lowe

31. Un ejemplo es la aplicación de parches de seguridad o actualizaciones de software, donde los proveedores del sistema de control de procesos a menudo consideran necesario probar y acreditar los parches antes de aplicarlos a sistemas en producción. Durante este tiempo, los sistemas pueden ser vulnerables a los ataques (de allí la necesidad de considerar la amenaza potencial de no parchear y la necesidad de usar contramedidas adecuadas).

32. Otro ejemplo es que estos sistemas a menudo controlan directamente equipos críticos de seguridad, y si se detecta un intruso la reacción normal es aislar el sistema comprometido para que el resto de equipos puedan continuar funcionando sin interferencias. Con los sistemas TI tradicionales, la reacción puede ser permitir que el atacante permanezca en el sistema para supervisar sus actividades, reunir información para un posible enjuiciamiento o para comprender la vulnerabilidad o *exploit* usado para acceder al sistema.

33. A lo largo de este marco de buenas prácticas se han utilizado tres principios rectores. Estos principios son **proteger, detectar y responder**. La mayoría de las guías de este marco tratan sobre la protección de los sistemas de control de procesos mediante el despliegue de una variedad de medidas de seguridad. Esta guía se centra en la detección de posibles incidentes y en el despliegue de las respuestas adecuadas para minimizar el alcance y el impacto de cualquier incidente o evitarlo por completo.

3. ESTABLECER CAPACIDADES DE RESPUESTA

3.1. CONTEXTO DE ESTA SECCIÓN DENTRO DEL MARCO GENERAL

34. Establecer capacidades de respuesta eficaces a un incidente está estrechamente relacionado con todos los demás elementos de este marco de guías de buenas prácticas. La capacidad para responder eficazmente a los eventos de seguridad dependerá de la capacidad para vigilar y detectar eventos relacionados con la seguridad y la calidad de los planes de respuesta preparados. Esto a su vez depende de sistemas bien protegidos y monitorizados, una dirección clara, y las habilidades y la sensibilidad del personal.

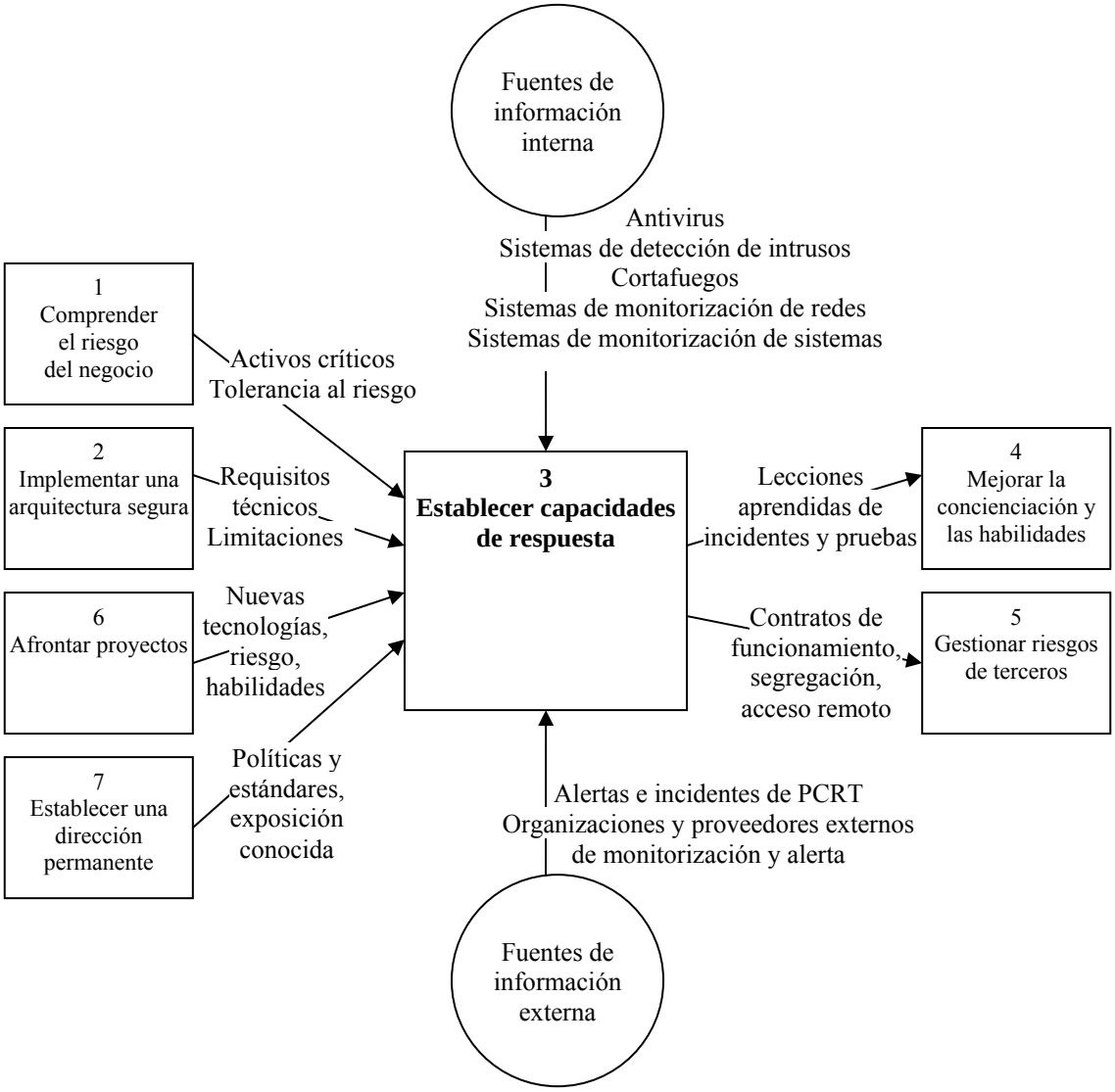


Figura 2: ***Cómo encaja "Establecer Capacidades de Respuesta" en este marco***

3.2. JUSTIFICACIÓN

35. La capacidad para responder a las alertas e incidentes es una parte importante del marco de seguridad del control de procesos. Obtener apoyo de la gerencia, determinar las responsabilidades, establecer canales de comunicación, elaborar políticas y procedimientos, identificar acciones predefinidas, proporcionar la formación adecuada y practicar todo el proceso antes de que ocurran los incidentes permite una respuesta rápida, eficaz y adecuada que puede minimizar el impacto en el negocio y su coste, y posiblemente evitar que este tipo de incidentes ocurran en el futuro. A pesar de estas ventajas, muchas organizaciones no tienen preparados planes de respuesta a ciberataques exhaustivos que cubran los sistemas de control de procesos.

3.3. PRINCIPIOS DE BUENAS PRÁCTICAS

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

    - Crear un Equipo de Respuesta de Seguridad en el Control de Procesos (ERSCP) para responder a los incidentes de seguridad.
    - Garantizar que están preparados los planes adecuados de respuesta a incidentes y de continuidad del negocio para todos los sistemas de control de procesos.
    - Garantizar que todos los planes de seguridad electrónica son regularmente mantenidos, ensayados y probados.
    - Establecer un sistema de alerta temprana que notifique al personal apropiado de los incidentes y alertas de seguridad.
    - Establecer procesos y procedimientos para monitorizar, evaluar y poner en marcha las respuestas a los incidentes y alertas de seguridad. Entre las posibles respuestas se pueden incluir: aumentar la vigilancia, aislar el sistema, aplicar los parches, o movilizar el ERSCP.
    - Garantizar que todos los incidentes de seguridad del control de procesos son reportados oficialmente y revisados.
    - Las lecciones aprendidas deben ser retroalimentadas para mejorar los planes y actualizar las políticas y estándares.

37. La localización de guía para respuesta a incidentes ([Ref.- 5]) puede encontrarse en el "ANEXO A. Referencias". Esa guía se centra en establecer de planes de respuesta para incidentes como infecciones de *malware* o sistemas comprometidos por *hackers*. Aunque fue elaborada principalmente para sistemas TI tradicionales, muchos de los principios incluidos son extrapolables a los sistemas de control de procesos y SCADA.

38. Esta guía "Establecer capacidades de respuesta" coincide con la guía general y cubre con más detalle algunas de las áreas preactivas, como la respuesta a las alertas de seguridad y el parcheado de sistemas, que son retos mayores en los entornos de control de sistemas que en los sistemas TI corporativos.

3.4. ORIENTACIÓN SOBRE LAS BUENAS PRÁCTICAS

3.4.1. CREAR UN EQUIPO DE RESPUESTA DE SEGURIDAD EN EL CONTROL DE PROCESOS (ERSCP)

39. Un Equipo de Respuesta de Seguridad en el Control de Procesos (ERSCP) es un elemento fundamental de la capacidad de respuesta de una organización y proporciona las bases para la monitorización, análisis y administración eficaz de la respuesta a alertas e incidentes. El ERSCP debe participar en cada una de las etapas del proceso de monitorización de una situación, analizando cualquier cambio en la ciberamenaza e iniciando las respuestas apropiadas.

40. Un requisito fundamental para el éxito del ERSCP es garantizar que las personas con las capacidades y conocimientos adecuados están involucradas. El equipo puede ser a tiempo

parcial o a tiempo completo, y puede ser un recurso central, un recurso de cada centro o una combinación de éstos. Sus miembros deben ser proceder de varias fuentes, con representantes de un número de áreas de negocio, ejemplos de los cuales incluyen:

- Equipos de Control de Procesos, SCADA y automatización.
- Seguridad TI.
- Infraestructura TI.
- Gestión de negocios.
- Operaciones.
- Reguladores internos.
- Departamento jurídico.
- Oficina de contacto con los medios.
- Equipo de seguridad empresarial.

3.4.1.1. CONSIDERACIONES DE ORGANIZACIÓN

41. Los ERSCP pueden estructurarse de varias maneras, ya sea de forma centralizada, por ejemplo como un Centro de Coordinación (CC), o como entidades de ámbito local o ejecutar una combinación de ambos.
42. En organizaciones grandes puede ser posible tener un Centro de Coordinación (CC) que monitorice y analice los acontecimientos, asesore a los centros locales en las medidas apropiadas y coordine sus actividades. Un CC puede proporcionar un enfoque mejor de la respuesta a incidentes, ya que está en una situación ideal para compartir y obtener información de otros grupos como los socios comerciales, proveedores, otros Equipos de Respuesta a Incidentes, y los equipos policiales y de protección de infraestructuras, como el CCN.
43. Un CC también puede proporcionar un funcionamiento efectivo 24x7 usando menos recursos que una colección de equipos locales. Sin embargo, un CC también tiene desventajas. Por ejemplo, es posible que no tenga suficiente conocimiento de los centros locales para comprender su entorno de funcionamiento o las personalidades involucradas.
44. La alternativa es que un equipo local del centro sea creado utilizando el personal que tenga un rol de respuesta a incidentes a tiempo parcial junto con sus actividades normales del día a día. Los equipos locales del centro tendrán un amplio conocimiento de los problemas locales y entornos operativos.
45. En la práctica, a menudo es preferible un enfoque híbrido, un CC intercambiando información con los equipos locales con sede en los centros operativos. Este modelo aprovecha la eficiencia de un CC en el desempeño de la vigilancia diaria, permitiendo que el centro local se concentre en sus actividades normales pero responda a incidentes o alertas cuando se avise desde la central.
46. Una de las principales dificultades en este ámbito, independientemente del modelo operativo preferido, es la disponibilidad de personal con las habilidades operativas, interpersonales, técnicas y de gestión de incidentes necesarias. La formación puede ser necesaria antes de que un equipo sea plenamente efectivo.

3.4.2. ESTABLECER PLANES DE RESPUESTA DE SEGURIDAD Y CONTINUIDAD

47. En muchas organizaciones, coexisten a menudo varios de planes de respuesta y continuidad. Esos planes incluyen la continuidad del negocio, recuperación de desastres, y planes de emergencia específicos para incidentes de condiciones de trabajo, medio ambiente u otro tipo de emergencias empresariales o industriales.

48. Sin embargo, es raro que los planes existentes cubran adecuadamente la variedad de amenazas potenciales a las que se enfrentan los sistemas de control (sencillamente algunas amenazas, especialmente las amenazas cibernéticas, no eran reconocidas cuando los planes se concibieron originalmente). Por ejemplo, si un sistema de recuperación de desastres instalado para proteger de incidentes físicos un centro de control está conectado a la misma red que el centro de control principal, es probable que un incidente de *malware* en el sistema principal tenga repercusiones sobre el sistema de recuperación de desastres y puedan volverlo prácticamente inútil.

49. Puede incluirse la gestión de incidentes de ciberamenazas dentro de los planes existentes para ahorrar tiempo y esfuerzo, pero hay que tener cuidado y asegurarse de que todas las amenazas al control de procesos se cubre adecuadamente y que los diversos planes interactúan de manera satisfactoria.

50. Puede haber confusión sobre cómo encajan juntos los planes de respuesta a incidentes, recuperación de desastres y continuidad de negocio. La Figura 3 muestra cómo algunos de estos planes se interrelacionan.

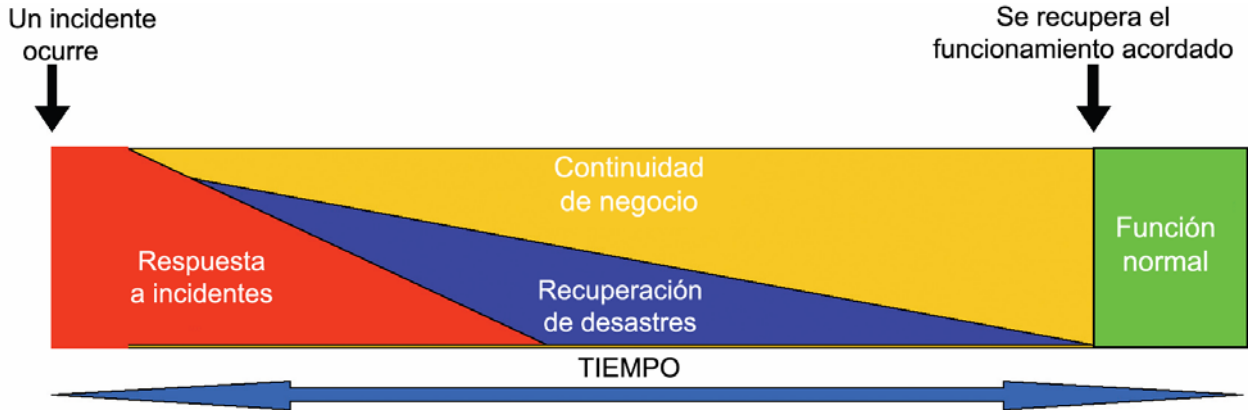


Figura 3: ***Diferentes tipos de planes de respuesta***

51. La figura muestra cómo los planes de respuesta a incidentes se centran en el corto período de tiempo directamente después de un incidente. Los planes de respuesta a incidentes se centran en proporcionar una respuesta inmediata a los incidentes mediante la aplicación de acciones inmediatas. Según el incidente continúa, el foco se traslada a iniciar la continuidad del negocio (garantizando que el servicio puede seguir funcionando durante el incidente) y la recuperación de desastres (la restauración de datos y sistemas perdidos o dañados).

52. Al establecer planes de respuesta eficaces para los sistemas de control de procesos, debe darse importancia a la respuesta a incidentes, puesto que los incidentes de seguridad informáticos a menudo se producen sin previo aviso y requieren una respuesta rápida y efectiva para evitarlos o minimizar su impacto si no pueden ser evitado.

3.4.3. PRINCIPALES CONTENIDOS DE UN PLAN DE RESPUESTA A INCIDENTES

53. Los planes de respuesta de seguridad en el control de procesos son a menudo bastante amplios y deben estar redactados de acuerdo al modelo operativo elegido, ya sea CC o centros locales. Sin embargo como mínimo deben incluir:

- Procedimientos de cómo informar sobre los incidentes
- Proceso para invocar el plan de respuesta
- Detalles del personal del equipo de respuesta, sus suplentes, funciones y responsabilidades, y los detalles de contacto 24x7.
- Centros, sistemas y activos críticos.
- Procedimientos predefinidos a los posibles escenarios previamente identificados (ver sección 3.4.6)
    - Una definición clara de cómo identificar cada escenario
    - Un plan de acción claro en el caso de identificar un escenario
- Un ruta clara de escalado y los requisitos de autorización necesarios para la escalada
- Listas de herramientas de apoyo disponibles
- Información de contacto (incluyendo organismos tanto internos como externos, empresas, cuerpos policiales, proveedores, etc).
- Un plan de comunicación claro
    - Cómo comunicar
    - Qué comunicar
    - A quién comunicar
    - Cuándo comunicar y con qué frecuencia
- Los criterios que deben cumplirse para cerrar los incidentes.

3.4.4. GARANTIZAR QUE LOS PLANES SON MANTENIDOS, ENSAYADOS Y PROBADOS PERIÓDICAMENTE

54. A pesar de una planificación cuidadosa, es frecuente descubrir que los planes y el personal se comportan de forma diferente en situaciones de la vida real. Todo el personal debe prepararse para la ejecución de planes que deben probarse periódicamente para garantizar que se llevan a cabo como fueron diseñados.

55. Este tema se trata con más detalle en la guía “Mejorar la concienciación y las habilidades” de este marco ([Ref.- 62]).

56. Los planes deben ser revisados al menos anualmente y con mayor frecuencia para sistemas críticos o de alto riesgo. Deben modificarse a raíz de cualquier cambio en la amenaza, en los requisitos de protección, el propio sistema o la estructura organizativa. Las lecciones aprendidas durante un ejercicio o después de que se produzca un incidente también deben incorporarse en los planes.

3.4.5. ESTABLECER UN SISTEMA DE ALERTA TEMPRANA

57. Tener un sistema de alerta temprana bien definido y ensayado permite a las organizaciones responder de forma rápida y eficaz a los incidentes y alertas de seguridad, minimizando su coste y los trastornos.

58. Muchas organizaciones tienen planes de respuesta y continuidad preparados, pero no son eficaces identificando los incidentes de seguridad, determinando las medidas adecuadas e iniciando los planes de respuesta.

59. Un problema común es no tener el acceso oportuno a la información pertinente, de fuentes internas y externas, en la que poder basar las decisiones. Otro problema puede ser estar desbordado por un gran volumen de información que no se puede procesar eficientemente. En consecuencia, no se está seguro del problema ni de cómo reaccionar.

60. Un ejemplo de un proceso de selección en un incidente de alto nivel se muestra en la Figura 4, que describe tres etapas clave parte de la respuesta a eventos.

    - **Monitorizar:** recoger información de seguridad de dentro y fuera de la organización, como alertas, infecciones de virus, amenazas, notificaciones de parches, y datos de la red y de los sistemas de monitorización del rendimiento.
    - **Analizar:** categorizar la información recibida de varias fuentes en diferentes niveles y tipos de amenaza potencial, filtrando los datos apropiados que necesitan una respuesta.
    - **Responder:** cómo responder en base al tipo y categoría de la amenaza y el riesgo asociado para la organización.

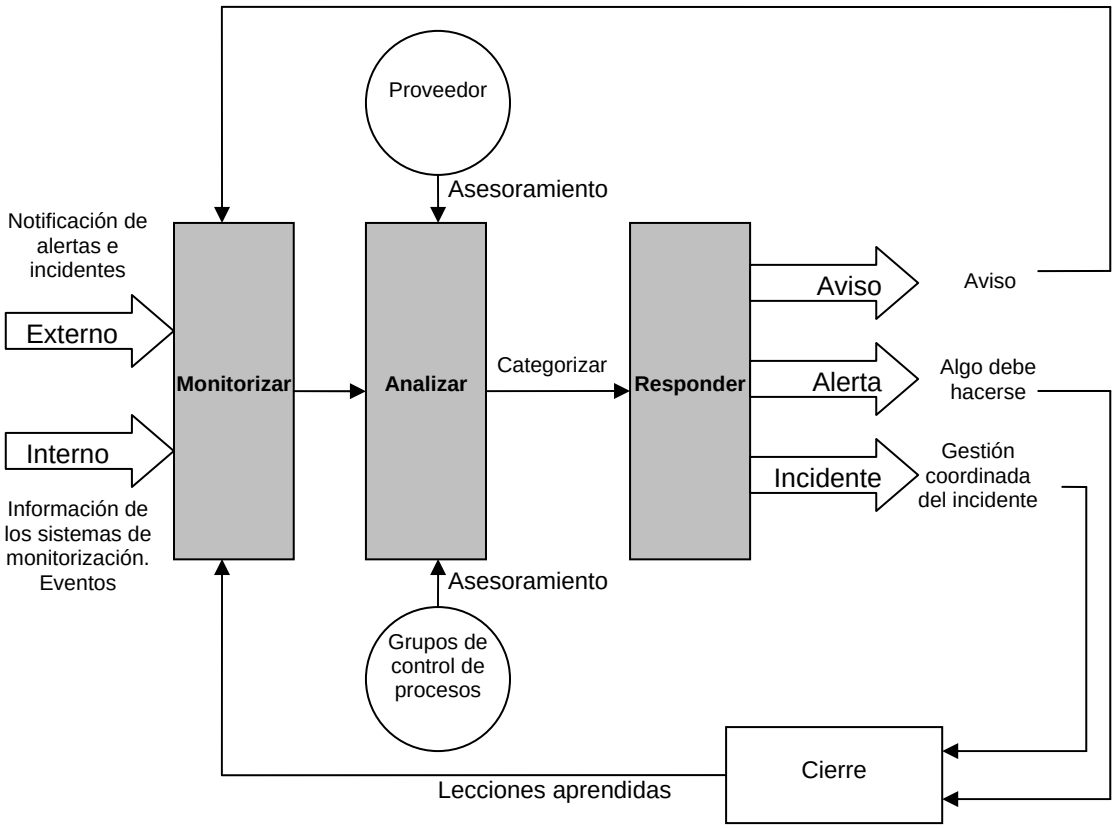


Figura 4: ***Esquema de respuesta de seguridad en el control de procesos***

3.4.5.1. ETAPA DE MONITORIZACIÓN

61. El estado normal de las operaciones se da cuando las fuentes internas y externas de información son monitorizadas para detectar cualquier evento relevante, como alertas de seguridad, *malware* y notificaciones de vulnerabilidades o un comportamiento anormal del sistema. Se necesita un equilibrio entre intentar procesar cada entrada de información disponible, lo que requerirá un gran esfuerzo de recursos, y recoger datos suficientes para que las alertas o incidentes importantes no sean ignorados.

62. La monitorización debe adaptarse a las amenazas aplicables a los sistemas relevantes. Esto se puede hacer cruzando las alertas de seguridad con el inventario de sistemas de control de procesos. Hay un número de fuentes típicas internas y externas que son por lo general importantes para la mayoría de organizaciones. Algunos ejemplos son:

3.4.5.2. FUENTES DE INFORMACIÓN INTERNAS COMUNES

63. Ejemplos de fuentes internas de información incluyen:

- Sistemas de monitorización de cortafuegos
- Sistemas de detección de intrusos
- Sistemas de monitorización y vigilancia de la red y sistemas

- Informes de virus y *malware*
- Informes de fallos de sistema
- Informes del servicio de atención al usuario

3.4.5.3. FUENTES EXTERNAS DE INFORMACIÓN COMUNES

64. Ejemplos de fuentes de información externa incluyen:
    - Equipos de protección de infraestructuras, por ejemplo CCN-CERT
    - Equipos de Seguridad y Atención a Incidentes (CSIRT) ([Ref.- 66])
    - US-CERT ([Ref.- 49])
    - Intercambios de información con el CCN-CERT
    - Fabricantes de hardware
    - Proveedores de software de control de sistemas y aplicaciones
    - Proveedores de sistemas operativos
    - Empresas de antivirus
    - Organizaciones externas de monitorización de seguridad (ej. monitorización subcontratada de cortafuegos e IDS)
    - Medios de comunicación técnicos
    - Grupos de noticias
    - Foros de seguridad
    - Agencias policiales
65. La información de diversas fuentes de monitorización puede ser recibida de diferentes formas, por ejemplo *logs* de sistema en bruto, correos electrónicos, sitios web, alimentadores RSS, o incluso mensajes SMS. La tarea de evaluar estos datos puede consumir bastante tiempo por lo que merece la pena poner en marcha procesos para filtrar los datos superfluos y presentar sólo la información importante, preferiblemente de la forma más clara posible.
66. Algunas organizaciones especializadas proporcionan servicios de alerta que se adapten a las necesidades de una organización, reduciendo la carga de los sistemas internos de monitorización. Lamentablemente, esta información se centra normalmente en seguridad TI general, sin cubrir los relacionados directamente con los sistemas de control de procesos. La información suele ser muy técnica y puede necesitar personal experimentado para analizarla eficazmente.
67. Existen una serie de servicios de intercambio de información que pueden ser utilizados tanto para proporcionar como para recibir información de:
    - WARPS ([Ref.- 50])
    - Intercambio de información CPNI ([Ref.- 51])
68. Las referencias se pueden encontrar en el Apéndice A.

3.4.5.4. ETAPA DE ANÁLISIS

69. El análisis de grandes volúmenes de datos de sistema y fuentes de información internas/externas debe ser realizado rápida y eficazmente. Por ejemplo, es de poco valor usar diez días en determinar si un nuevo gusano representa un problema para la organización ya que puede haber infectado los sistemas mucho antes.

70. Es importante contar con personal con experiencia correcta que contribuya al análisis de las alertas de seguridad, informes de incidentes y fuentes de información. Aunque los sistemas de control se basan a menudo en tecnologías TI estándar, existen diferencias entre ambos entornos. Por ejemplo, el personal con conocimientos de redes y de *software* de aplicación será capaz de comprender las cuestiones TI generales, pero en el entorno del control de procesos deberá participar el personal que tenga los conocimientos necesarios de esos sistemas.

71. Cada alerta debe analizarse para comprender su impacto potencial en los sistemas de control de procesos en uso y cualquier acción apropiada. La valoración puede ser compleja y cualquier análisis resultante debe expresarse de un modo claro y conciso antes de ser comunicado a los equipos ERSCP. Una norma útil es clasificar la información según la amenaza (Figura 5), por ejemplo:

    - **Grave:** un incidente en curso o una amenaza muy alta, ej. un gusano propagándose por Internet o en la red empresarial o de control de procesos.
    - **Alta:** vulnerabilidad de amenaza alta, ej. importante actividad exterior.
    - **Aviso:** vulnerabilidad de amenaza baja en ese momento que requiere más vigilancia, ej. actividad en Internet.
    - **Baja:** amenaza no dirigida al sistema de control, ej, virus de correo electrónico cuando éste no se usa en el sistema de control de procesos.

72. Para simplificar el proceso de toma de decisiones puede ser útil acordar criterios predefinidos para cada categoría. Cabe señalar que no todas las amenazas se encajan fácilmente en unos criterios predefinidos. Esas amenazas necesitan especialistas TI y de control de procesos que interpreten la información disponible y tomen las decisiones adecuadas.

73. Un examen detallado de los diversos niveles de amenaza se puede encontrar en el documento del US-Cert ([Ref.- 49]), cuya referencia puede encontrarse en el Apéndice A.

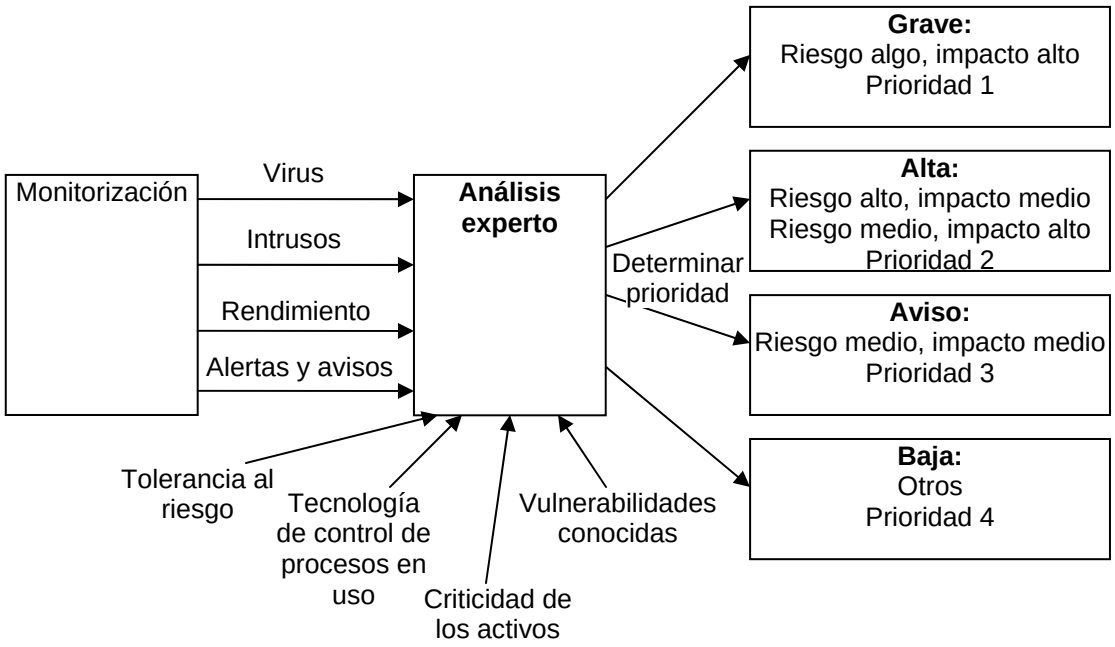


Figura 5: ***Categorización de los datos de amenazas de seguridad en el control de procesos***

74. Al responder a un incidente debería incluirse a los proveedores de sistemas de control de procesos en el proceso de análisis. Por ejemplo, puede ser necesario solicitar orientación a un proveedor sobre si un parche determinado debe aplicarse o discutir si un sistema utiliza algún componente software vulnerable.

75. Muchos proveedores de sistemas de control de procesos requieren que los parches sean probados y acreditados antes de aplicarlos en sistemas productivos. Algunos proveedores evalúan automáticamente los parches de sistema operativo en cuanto son distribuidos y prestan asesoramiento sobre la idoneidad de su aplicación. Cuando los proveedores no proporcionan automáticamente esta acción, puede ser necesaria una petición específica. Se puede encontrar más orientación sobre los parches en los sistemas de control en la sección 3.4.6.

3.4.5.5. ETAPA DE RESPUESTA

76. Esta etapa abarca el inicio de la respuesta adecuada a un incidente de la manera oportuna. El desencadenante es normalmente el resultado de la anterior fase de análisis. Situaciones típicas son:

- Alerta de seguridad (ej., aviso avanzado de un posible incidente, aumento de la actividad de *hackers* o un problema posible con *malware*)
- Notificación de vulnerabilidad (ej., una vulnerabilidad ha sido identificada o un parche de *software* ha sido distribuido para un sistema de control)
- Infección de *malware* (ej., un gusano o un virus es detectado en un sistema de control)
- Infiltración de *hacker* (ej., un *hacker* ha logrado comprometer un sistema de control)

3.4.6. ESTABLECER PROCESOS Y PROCEDIMIENTOS

77. Pueden encontrarse algunos ejemplos de lo que debe considerarse al preparar un plan de respuesta en la guía "CPNI First Responders' Guide: Policy and Principles" ([Ref.- 55]), cuya localización figura en el Apéndice A de esta guía.

78. Los procedimientos a incluir en un plan de respuesta de control de procesos deben considerar el entorno operativo, las posibles amenazas, vulnerabilidades y experiencias de incidentes anteriores. Los siguientes son algunos procedimientos que podrían incluirse en un plan de respuestas:

- Infección *malware* y su eliminación
- Sospecha de infiltración de *hacker*
- Ataque de denegación del servicio (DoS)
- Desconexión del sistema de control de otras redes (si es posible)
- Reconexión del sistema de control a otras redes
- Incapacidad para ver la situación de la planta (pérdida de visión)
- Incapacidad para controlar la planta (pérdida de control)
- Actualizaciones de emergencia de la firma del sistema antivirus y de detección de intrusos
- Procesos de continuidad de negocio y parcheado de seguridad de emergencia
- Copia de seguridad del sistema y restauración
- Confirmación de la operación correcta del sistema (ej., un procedimiento para verificar que es un sistema está funcionando normalmente).

79. Las secciones siguientes examinan algunas consideraciones para un subconjunto de estos procedimientos.

3.4.6.1. PARCHES DE SEGURIDAD

80. En el pasado, la aplicación de parches de seguridad a los sistemas de control de procesos nunca fue un tema importante. Esto se debe a que estos sistemas se basaban en tecnologías propietarias o aisladas de otros sistemas. Los parches sólo eran realmente necesarios para actualizaciones del sistema o para la solución de errores. En consecuencia, la aplicación de estos parches podía planificarse dentro de un proceso de instalación ordenado.

81. Ahora la mayoría de los sistemas de control se basan en las tecnologías TI estándar y están conectados a otros sistemas, por lo que corren el riesgo de ser comprometidos o infectados. Aplicar a estos sistemas medidas de protección como cortafuegos es un elemento importante de defensa. Sin embargo, depender sólo de una capa de defensa fuerte no se considera una buena práctica para la protección de los sistemas de control de procesos y se recomienda un modelo multi-capa de "defensa en profundidad". Un elemento clave en este modelo es garantizar que los dispositivos situados dentro del perímetro de protección estén securizados con distintas medidas (siendo una fundamental la aplicación de parches de seguridad).

82. Parchear o no parchear – ¡esa es la cuestión!

83. Al enfrentarse con una alerta de seguridad o un incidente, una consideración clave es si se despliegan parches de seguridad o no. Debe impulsarse desde la evaluación del riesgo en la etapa de análisis. Sin embargo, la aplicación de parches no está libre de riesgos – existe el riesgo de que el parche pueda causar un funcionamiento incorrecto de un sistema. Asimismo, deben compararse el esfuerzo y la interrupción de sacar los sistemas de producción para aplicar los parches con el riesgo de no aplicar los parches. Cuando sea posible, los sistemas deben estar diseñados para facilitar el parcheo, por ejemplo servidores duales, pudiendo parchear uno mientras el otro mantiene las operaciones, o la disponibilidad de servidores pruebas o de *backup* donde los parches puedan ser probados antes de aplicarlos en los sistemas de producción.

84. Con el fin de proporcionar un enfoque coherente del parcheado del sistema y un despliegue ordenado de los parches, el plan de respuesta debe contener un proceso de parcheado. En el desarrollo de este proceso hay una serie de criterios que se deben considerar:

- ¿Cuáles son los sistemas que pueden necesitar ser parcheados? (se pueden obtener en el inventario de sistemas de control de procesos)
- ¿Cuál es la "parcheabilidad" de los sistemas?
    - Requisitos y consejos de los proveedores
    - Puede que no sea posible el despliegue de parches a la tecnología obsoleta.
- ¿Qué puede hacerse con los sistemas que no pueden ser parcheados?
    - Reemplazarlos o actualizarlos
    - Aislarlos físicamente
    - Separarlos (ej., detrás un cortafuegos configurado adecuadamente)
    - Protegerlos con sistemas de prevención de intrusos
- ¿Cuáles son las prioridades de parches?
- ¿En qué orden deben parchearse los sistemas?
- ¿Cómo serán aplicados los parches?
    - Bajo situaciones normales del negocio
    - Procesos de parcheado de emergencia
- ¿Qué herramientas de aplicación de parches y auditoria están disponibles y son adecuadas?
- ¿Qué pruebas se necesitan antes del despliegue?
    - ¿Es necesaria la acreditación de proveedores antes de que los sistemas se parcheen?
    - ¿Es posible hacer pruebas de garantía del centro en equipos de prueba o un sistema de formación?
    - ¿Es posible parchear algunos sistemas antes de la aprobación del proveedor?

- ¿Existen herramientas de garantía y despliegue que puedan utilizarse como ayuda al proceso de despliegue? (estas herramientas puede requerir la acreditación de proveedores antes de su uso)

85. Más detalles sobre la gestión de parches en general se pueden encontrar en la guía "Good Practice Guide Patch Management" ([Ref.- 53]). Esta guía es un documento general y no es específico de los sistemas de control de procesos y SCADA.

3.4.6.2. RESTAURACIÓN DEL SISTEMA Y FORENSE

86. Cuando un sistema se ha visto comprometido (ej., *malware* o un *hacker*), a menudo se presenta la difícil decisión de restaurar el sistema o mantenerlo en cuarentena para realizar una investigación más a fondo. Normalmente hay una necesidad urgente de restaurar el sistema a un estado operativo tan pronto como sea posible, lo que generalmente implica reconstruirlo o restaurarlo desde copias de seguridad. Por desgracia, esto generalmente implica que cualquier pista o rastro auditable dejado por el atacante será destruido y, por tanto, habrá pocas posibilidades de que el criminal pueda ser perseguido y llevado ante la justicia. En esta situación, la decisión clave es si mantener cualquier pista (y posiblemente retrasar la restauración de las operaciones) o restablecer las operaciones al coste de no poder perseguir a los criminales. Si hay sistemas repartidos o redundantes, se pueden restablecer las operaciones mientras las máquinas afectadas son puestas en cuarentena para su posterior análisis.

87. Si una organización es partidaria de perseguir a los criminales autores a raíz de un incidente, deberá incluirlo en los planes de respuesta para garantizar que los sistemas adecuados son puestos en cuarentena. Este tema es un campo de especialización en sí mismo; para mayor información consultar la guía "An Introduction to Forensic Readiness Planning" ([Ref.- 54]).

3.4.7. ESTABLECER LA NOTIFICACIÓN DE INCIDENTES

88. Hay una fuerte tendencia de mantener los incidentes de seguridad del control de procesos se mantengan confidenciales, y que las organizaciones no divulguen información de incidentes a agencias externas con el fin de proteger su reputación y no alentar al control externo.

89. Sin embargo, existen ventajas del intercambio de información acerca de los incidentes. Compartir esa información puede permitir que otros organismos complementen la investigación, que se eviten incidentes similares en otras organizaciones y que se desarrolle un conocimiento mejor de los riesgos a los que enfrentan los sistemas de control.

90. Cualquier organización que ha experimentado incidentes de seguridad en el control de proceso debería compartir esa información (de manera adecuada, por ejemplo anónima). Al CCN, a través del CCN-CERT, le gustaría oír hablar de vulnerabilidades potenciales, incidentes o eventos de seguridad en las esferas de seguridad electrónica, física o de personal de las organizaciones de infraestructura crítica. Esta información será tratada como confidencial, y en caso necesario, convenientemente limpiada para borrar los datos que pudieran identificar a individuos u organizaciones, para incorporarla en su asesoramiento genérico de seguridad. Se puede contactar con el Servicio de Atención al Usuario del CCN-CERT a través de la siguiente dirección de correo electrónico,

csirtwk@cpni.gsi.gov.uk. La información sensible no debe enviarse sin cifrar a través de correo electrónico. Póngase en contacto con el Servicio de Atención al Usuario para el asesoramiento acerca de cómo puede ser enviada la información.

91. CCN-CERT es miembro del Foro de Respuesta a Incidentes y Equipos de Seguridad (FIRST) y tiene contactos interrelacionados con otros equipos de respuesta a incidentes (IRTs) con el fin de fomentar la cooperación y la coordinación en la prevención de incidentes, a la reacción rápida a los incidentes y para promover el intercambio de información entre sus miembros y la comunidad en general.

3.4.8. GARANTIZAR QUE SE APRENDE LA LECCIÓN TRAS LOS INCIDENTES

92. Es importante asegurarse de que, a raíz de las situaciones en que se dé una respuesta a una alerta o incidente de seguridad digital, cualquier lección o posible mejora del proceso será identificada y usada para garantizar la mejora continua de los procesos de respuesta.

93. Las revisiones de los incidentes deben llevarse a cabo tanto a nivel central como local y podrían desencadenar actualizaciones de los planes de respuesta, las políticas y los estándares y al perfil de riesgo empresarial.

4. AGRADECIMIENTOS

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

Sobre los autores

Este documento[5] 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

[5] 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*".

[Ref.- 43] CPNI
www.cpni.gov.uk/

[Ref.- 44] CPNI Good Practice Guides
www.cpni.gov.uk/ProtectingYourAssets/scada.aspx

[Ref.- 45] DHS Control Systems Security Program
http://csrp.inl.gov/

[Ref.- 46] DHS Control Systems Security Program Recommended Practices
http://csrp.inl.gov/Recommended_Practices.html

[Ref.- 47] NERC Critical Infrastructure Protection (CIP)
www.nerc.com/~filez/standards/Cyber-Security-Permanent.html

[Ref.- 48] ISA SP99, Manufacturing and Control Systems Security
www.isa.org/mstemplate.cfm?section=home&template=/TaggedPage/getStandards.cfm&MicrositeID=988&CommitteeID=6821

Section 3.4.5

[Ref.- 49] US Cert ([Ref.- 41])
www.us-cert.gov/control systems/

[Ref.- 50] WARPS ([Ref.- 42])
www.warp.gov.uk/

[Ref.- 51] CPNI Information Sharing ([Ref.- 7])
www.cpni.gov.uk/ProtectingYourAssets/InformationSharing.aspx

[Ref.- 52] Control System Cyber Security Self-Assessment Tool (CS2SAT)
www.us-cert.gov/control_systems/pdf/CS2SAT.pdf

Section 3.4.6

[Ref.- 53] Good Practice Guide Patch Management
www.cpni.gov.uk/Docs/re-20061024-00719.pdf

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

[Ref.- 55] CPNI First Responders' Guide: Policy and Principles
www.cpni.gov.uk/docs/re-20051004-00868.pdf

A.3. REFERENCIAS EN ESTA TRADUCCIÓN

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

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

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

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

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

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

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

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

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

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

[Ref.- 66] Equipos de Seguridad y Atencion a Incidentes (CSIRTs) españoles
http://www.csirt.es/

ANEXO B. GLOSARIO DE TÉRMINOS Y ABREVIATURAS

B.1. GLOSARIO DE TÉRMINOS

Amenaza*	Cualquier circunstancia o hecho que pueda dañar un sistema de control de procesos y SCADA a través de accesos no autorizados, destrucción, divulgación, modificación de datos y/o denegación del servicio.
Riesgo*	Posibilidad de que se produzca un hecho que tendrá un impacto negativo en el sistema de control. El hecho puede ser el resultado de una amenaza o una combinación de amenazas.
Tolerancia al riesgo*[6]	Nivel de riesgo, utilizado para determinar lo aceptable que puede ser un riesgo.
Probabilidad*[7]	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.
Plan de Continuidad de Negocio (PCN)	Plan empresarial que cubre la recuperación y la restauración parcial o total de las funciones críticas interrumpidas en un tiempo determinado tras un desastre o una interrupción continua.
Plan de Recuperación de Desastres (PRC)	Proceso de recuperación que cubre los datos, el hardware y el software crítico, para que un negocio pueda comenzar de nuevo sus operaciones en caso de un desastre natural o causado por humanos.

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

* Los términos así señalados se definían en el original al final del apartado “Especialistas en la seguridad de la información.

- Especialistas en seguridad física.
- Líderes empresariales.
- Gestores de riesgos.
- Encargados de las condiciones de trabajo.
- Ingenieros de operación.
- Equipos de respuesta de seguridad

Resumen de “Establecer capacidades de respuesta””.

[6] Original: *Risk Appetite*

[7] Original: *Likelihood*

INC	Infraestructura Nacional Crítica
SCADA	Sistema de Control Supervisor y Adquisición de Datos
SCD	Sistemas de Control Distribuido
TI	Tecnología de la Información
PCN	Plan de Continuidad de Negocio
RD	Recuperación de Desastres
ERSCP	Equipo de Respuesta de Seguridad en el Control de Procesos
IDS	*Intrusion Detection Systems* Sistemas de Detección de Intrusos
RSS	*Rich Site Summary (RSS 0.91)* *RDF Site Summary (RSS 0.9 y 1.0)* *Really Simple Syndication (RSS 2.0)* Suministro de contenidos web a través de formatos XML

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
RIS: Retorno de la Inversión en Seguridad	ROSI: Return On Security Investment
PCN: Plan de Continuidad de Negocio	*BCP:* Business Continuity Plan
RD: Recuperación de Desastres	DR: Disaster Recovery
ERSCP : Equipo de Respuesta de Seguridad en el Control de Procesos	PCSRT: Process Control Security Response Team
CC: Centro de Coordinación	CC: Coordination Centre
CSIRT: Equipos de Seguridad y Atención a Incidentes	CSIRT: Computer Security Incident Response Team