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

SEGURIDAD EN SISTEMAS SCADA

MARZO 2010

Edita:

NIPO: 076-10-072-4

Tirada: 1000 ejemplares
Fecha de Edición: marzo de 2010

LIMITACIÓN DE RESPONSABILIDAD

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.

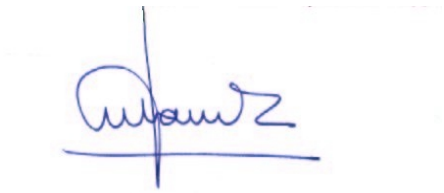
Una de las funciones más destacables del Centro Criptológico Nacional es la de elaborar y difundir normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los sistemas de las tecnologías de la información y las comunicaciones de la Administración, materializada en la existencia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

Marzo de 2010



Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

ÍNDICE

ANEXOS

FIGURAS

1. INTRODUCCIÓN

1. Los sistemas SCADA o sistemas de Supervisión, Control y Adquisición de Datos, comprenden todas aquellas soluciones de aplicación que recogen medidas y datos operativos de equipos de control locales y remotos. Los datos se procesan para determinar si los valores están dentro de los niveles de tolerancia y, de ser necesario, tomar medidas correctivas para mantener la estabilidad y el control. ([Ref.- 22])
2. La arquitectura básica comprende un servidor, o granja de servidores, centralizado; los RTU o PLC que manejan los dispositivos; consolas desde donde los operadores monitorizan y controlan los diferentes equipos y un servidor histórico de bases de datos que almacena en disco toda la información que recibe y maneja el servidor central. ([Ref.- 22])
3. Estas infraestructuras suelen estar localizadas en
   - sistemas de transportes: metro, trenes, puertos o aeropuertos,
   - sistemas industriales: químicas, refinerías, etc.,
   - distribución y control de electricidad, agua, gas
   - centrales generadoras de electricidad: térmicas, hidroeléctricas, nucleares, etc.
4. Los sistemas de control de procesos son críticos en muchas industrias. Toda la producción depende de unos pocos sistemas, y un fallo de estos puede ocasionar que no se detecten malos funcionamientos que produzcan graves pérdidas económicas, cuando no un peligro para la seguridad de los empleados o desastres medioambientales. Por lo tanto, y como punto único de fallo, la seguridad de estos sistemas debe ser una materia de máxima prioridad.
5. La seguridad de los sistemas SCADA es especialmente relevante en el ámbito de las Infraestructuras Críticas. Un fallo en una Infraestructura Crítica supone un perjuicio para toda la sociedad, en muchos casos para todo un país y su entorno. Su seguridad trasciende el ámbito de la empresa y requiere del asesoramiento y el control de organismos superiores. Así lo ve la Unión Europea en varias resoluciones ([Ref.- 19], [Ref.- 20]) adoptadas por la administración española ([Ref.- 21]).
6. En este documento se utiliza el término SCADA para referirse a todo sistema de control industrial, de control de procesos, de Control Distribuido (DCS), de Supervisión, Control y Adquisición de DAtos (SCADA), de automatización industrial y sistemas relacionados con la seguridad física o industrial.

2. OBJETO

7. Presentar la problemática planteada por los sistemas SCADA y sus vulnerabilidades, su impacto y la necesidad imperativa de controlar su seguridad.
8. Describir las técnicas necesarias para analizar los riegos derivados de dichos sistemas.
9. Enumerar todos los elementos, técnicos o no, que tienen un papel en la seguridad de los sistemas SCADA, estableciendo los ámbitos en los que intervienen y presentando los mecanismos adecuados para que su actuación sea efectiva.

10. Presentar algunas soluciones técnicas ante determinadas amenazas, referenciando los documentos donde se puede encontrar más información de cada una de ellas.

3. ALCANCE

11. Esta guía es de aplicación a todos los sistemas SCADA. Aunque cobra especial importancia en las Industrias que trabajen con Infraestructuras Críticas, está orientada a cualquier organismo, institución, industria o empresa que cuente con sistemas SCADA.

12. Debido a la evolución del mercado, la presente guía deberá ser actualizada convenientemente con los nuevos productos, tendencias y amenazas que aparezcan y los avances en seguridad que se produzcan.

13. 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.

4. INTRODUCCIÓN A LA SEGURIDAD EN SISTEMAS SCADA

14. Los sistemas SCADA fueron diseñados antes del surgimiento de Internet. Fueron pensados para ser sistemas aislados y no conectados en red. Tradicionalmente carecen de dispositivos de seguridad como cortafuegos, mecanismos de cifrado o software antivirus ([Ref.- 23]). Su diseño se centraba en la funcionalidad, la fiabilidad y la seguridad física, en limitar el acceso. Utilizaban tecnologías propietarias y poco probadas fuera de ambientes controlados. Esta filosofía producía sistemas no preparados para ataques externos.

15. Con el fin de abaratar costes y acelerar el desarrollo de nuevos sistemas y la implantación de mejoras, los sistemas SCADA hacen cada vez más uso de **tecnologías estándar**, como Microsoft Windows, TCP/IP, navegadores Web y las conexiones inalámbricas. De ese modo se consigue centrar los esfuerzos en la funcionalidad buscada, utilizando como base tecnologías ampliamente probadas y fiables.

16. En la misma línea evolutiva, y gracias al tremendo avance de las comunicaciones y la conectividad de los últimos años, los sistemas SCADA han aumentado su **conectividad** a interconectarse con otros sistemas. Gracias a ello, ahora es posible utilizar sistemas SCADA distribuidos, o centralizar el control de instalaciones diversas, integrar los resultados del control de procesos en los sistemas administrativos y mejorar el rendimiento no sólo de la producción de toda la empresa.

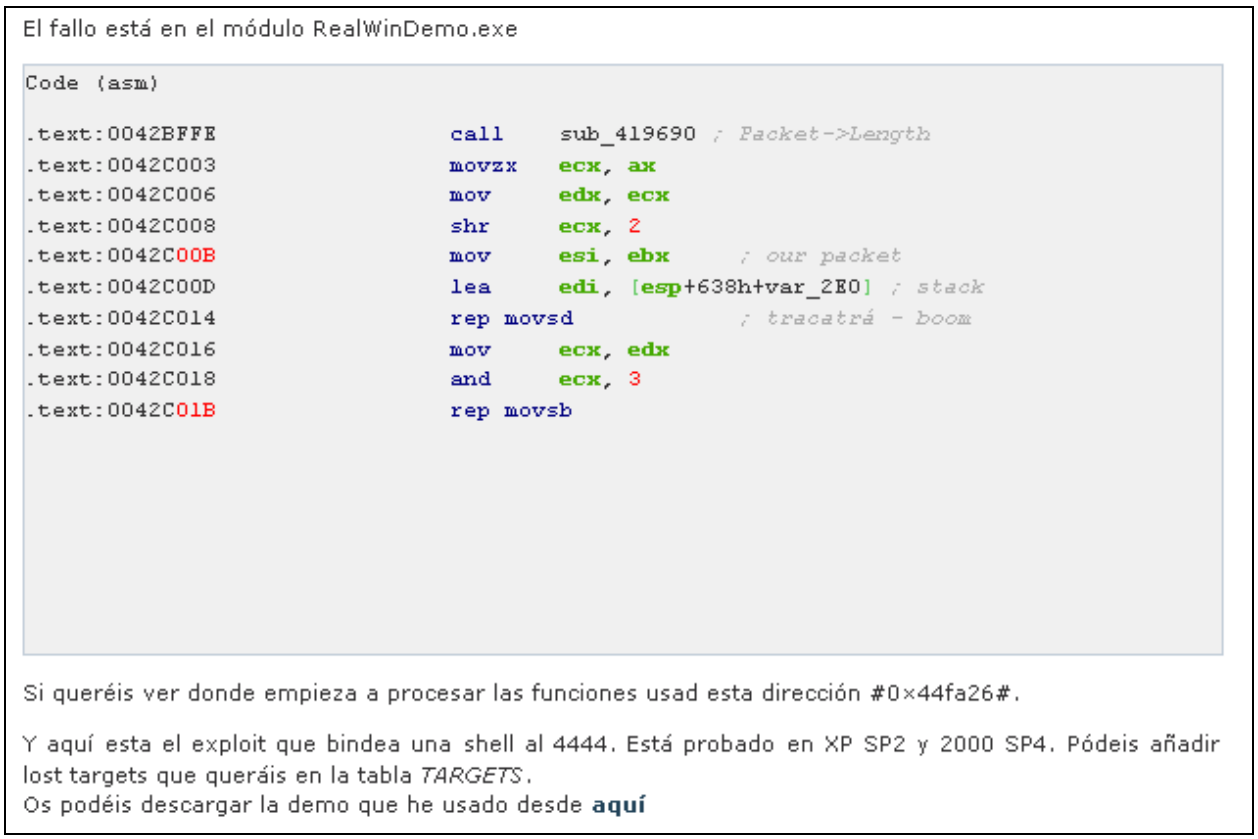
4.1. RIESGOS DE LOS SISTEMAS SCADA

17. A pesar de los beneficios derivados de este desarrollo, el **aumento de la conectividad** los ha expuesto a nuevas amenazas para las que no están preparados (ej., gusanos, virus y *hackers*). Al aumentar las redes de SCADA y su conectividad entre redes, los riesgos de amenazas electrónicas para los sistemas de SCADA continúan intensificándose.

18. Además, ahora los proveedores dan soporte remoto a través de enlaces telefónicos o de conexiones a Internet. Los módems rara vez están sujetos a los comprobaciones de

seguridad. Un ataque a un sistema no crítico, como es la red de un proveedor, puede suponer de puerta de entrada de virus o ser usado para realizar ataques indirectos.

19. El ***software* comercial** y el ***hardware* de propósito general** se está usando para sustituir el propietario de los sistemas SCADA. Este tipo de *software* y *hardware* a menudo no se adapta a la singularidad, complejidad, los requerimientos de tiempo real y seguridad del entorno SCADA. Los sistemas SCADA se vuelven vulnerables a ataques comunes y a *malware* ampliamente disponible desarrollado para otras plataformas. Aumenta su vulnerabilidad y el rango de posibles atacantes. En Internet es posible encontrar demostraciones de ataques sobre sistemas SCADA comerciales ([Ref.- 29]).


El fallo está en el módulo RealWinDemo.exe

Code (asm)

```
.text:0042BFFE                call    sub_419690 ; Packet->Length
.text:0042C003                movzx   ecx, ax
.text:0042C006                mov     edx, ecx
.text:0042C008                shr     ecx, 2
.text:0042C00B                mov     esi, ebx      ; our packet
.text:0042C00D                lea     edi, [esp+638h+var_2E0] ; stack
.text:0042C014                rep movsd             ; tracatrá - boom
.text:0042C016                mov     ecx, edx
.text:0042C018                and     ecx, 3
.text:0042C01B                rep movsb
```

Si queréis ver donde empieza a procesar las funciones usad esta dirección #0×44fa26#.

Y aquí esta el exploit que bindea una shell al 4444. Está probado en XP SP2 y 2000 SP4. Pódeis añadir lost targets que queráis en la tabla *TARGETS*.
Os podéis descargar la demo que he usado desde **aquí**

Figura 1: *Xploit en en software RealWin ([Ref.- 29])*

20. Muchas medidas estándar de protección de la seguridad en TI utilizadas normalmente en estas tecnologías no han sido adaptadas al entorno SCADA. Por tanto, las medidas de seguridad disponibles para proteger los sistemas de control y mantener el entorno seguro pueden ser insuficientes.

21. Hay consecuencias potencialmente serias en el caso en el que se explotaran estas vulnerabilidades. Los efectos de un ataque electrónico en los sistemas SCADA pueden incluir, por ejemplo:

    ⇒ denegación del servicio

    ⇒ pérdida de la integridad de los datos

    ⇒ pérdida de confidencialidad de los datos

    ⇒ pérdida de reputación

⇒ impacto en las condiciones de trabajo

22. Se puede considerar que la seguridad SCADA no es algo a tener en cuenta en España al no tratarse de un objetivo prioritario. En cambio, un reciente estudio de Team Cymru rastreando escaneos de puertos sobre servicios conocidos de SCADA ([Ref.- 27]) reveló que España era origen de una parte importante de estos escaneos, que probablemente fueron hechos desde ordenadores personales infectados.

Figura 2: ***Origen de ataques SCADA***

5. SEGURIDAD EN SISTEMAS SCADA

23. Como elemento único de fallo del que depende tan fuertemente la producción, la seguridad de los sistemas SCADA debe ser una prioridad y, como tal, implicar a todos los ámbitos, desde aquellos que abarcan toda la empresa hasta las decisiones técnicas.

5.1. EMPRESA

24. Toda gestión de la seguridad debe ser promovida desde las etapas superiores o directivas. De otro modo, probablemente fracasará. Esto es especialmente importante en el caso de los sistemas SCADA.

25. La importancia de los sistemas SCADA debe ser asumida por los cargos con más responsabilidad e incorporada en todas las decisiones que tomen.

5.1.1. GESTIÓN DEL RIESGO

26. Se puede encontrar más información útil sobre este tema en el documento “CCN-STIC-403 Gestión de incidentes de seguridad” ([Ref.- 2]).

5.1.1.1. ANÁLISIS DEL RIESGO

27. Todo ejercicio en torno a la seguridad debe comenzar por comprender el riesgo que se corre. Una definición útil consiste en expresar el riesgo en función de la probabilidad de que se produzca ese riesgo y el impacto que tendría lugar si ese riesgo se produjera.

Otra define el riesgo total como la suma de todos los riesgos individuales de las amenazas identificadas. ([Ref.- 12]).

28. Desde el CCN se recomienda utilizar la metodología Magerit ([Ref.- 25]), elaborado por el Consejo Superior de la Administración electrónica y de obligado cumplimiento para todos los órganos de la Administración Española y la herramienta PILAR que desarrolla bibliotecas específicas para infraestructuras críticas. El Instituto Nacional de Administración Pública suele convocar acciones formativas en el empleo de esa metodología y esta herramienta en sus distintas modalidades en colaboración con el Centro Criptológico Nacional.

29. La metodología Magerit se basa en los siguientes elementos: activos, amenazas, vulnerabilidades, impactos, riesgos y salvaguardas.

30. Es importante conocer las amenazas y sus motivaciones para poder responder ante ellas. Las posibles amenazas incluyen entre otras:

    - Denegación de servicio
    - Ataques dirigidos
    - Incidentes accidentales
    - Accesos y controles no autorizados
    - Código malicioso o no autorizado instalado en las máquinas (gusanos, virus, troyanos, *spam*, *phising*, *bots*, etc.).

31. Las fuentes de amenazas o atacantes potenciales (conscientes o inconscientes) incluyen (pero no se limitan a):

    - *Hackers* y delincuentes
    - *Malware* de propagación automática (gusanos, *bots*, etc.)
    - Atacantes internos
    - Personal descontento
    - Personal realizando acciones no autorizadas (ej., acceder a Internet)
    - Inteligencia corporativa
    - Contratistas
    - Servicios de inteligencia extranjeros
    - Crimen organizado
    - Terroristas
    - Manifestantes y activistas (ej, medioambientales, políticos, pro-derechos de los animales)

32. Para identificar las vulnerabilidades deben partirse del catálogo de activos (ver apartado 120).

33. En general, cualquier medida técnica de seguridad que se pueda aplicar en TI puede ser utilizada en SCADA y viceversa, siempre que se cumplan una serie de requisitos formales en SCADA que garanticen una coherencia y un endurecimiento de dichas medidas.

34. Gestión de activos.Para identificar los activos se deben estudiar y evaluar al menos los siguientes elementos (consultar la guía CCN-STIC-470 Herramienta PILAR [Ref.- 6] para más información):
    - Infraestructura
    - Sistemas operativos y *firmware*
    - Aplicaciones y *software* usado
    - Conexiones de red
    - Accesos remotos
    - Procesos y procedimientos
    - Gestión de empleados
    - Gestión de subcontratas y proveedores
35. Debe intentarse que el impacto posible de cualquier amenaza sea asumible:
    - Pérdida de una o varias máquinas o reducción de su funcionalidad
    - Pérdida de disponibilidad (denegación de servicio)
    - Pérdida de conectividad
    - Cambios de configuración
    - Funcionamiento incorrecto, falsos negativos o falsos positivos
    - Pérdida de integridad de los datos capturados o almacenados
    - Pérdida de confidencialidad
36. El atractivo o interés que un sistema puede suscitar en un atacante potencial es un factor importante que puede modificar el riesgo. El término atractivo, puede no ser aplicable a ciertos riesgos, como la infección de un gusano. La mayoría de los gusanos infectan de manera indiscriminada y, por tanto, cualquier sistema vulnerable está en peligro. En consecuencia, el término no es relevante en este caso, pero sí en muchos otros.
37. El atractivo de un blanco depende de la fuente de amenaza, pero ha de considerarse alto para toda aquella empresa que trabaje o forme parte de la Infraestructura Crítica Nacional (ICN). Para más información acerca de lo que puede considerarse ICN, consultar el **Catálogo de Infraestructuras Críticas** Nacionales en http://www.cnpic-es.es ([Ref.- 21]).
38. Se pueden encontrar consejos útiles sobre este tema en la guía "CCN-STIC-410 Análisis de riesgos en sistemas de la Administración" ([Ref.- 4]).

5.1.1.2. LA HERRAMIENTA PILAR

39. Existen múltiples herramientas y metodologías que permiten realizar un análisis de riesgos (ver por ejemplo [Ref.- 24]). Desde el CCN se recomienda utilizar la **Herramienta de Análisis de Riesgos PILAR**.
40. La Herramienta Pilar analiza los siguientes aspectos: confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad. A partir del análisis propone:

- salvaguardas (o contra medidas)
- normas de seguridad
- procedimientos de seguridad
- elementos de respaldo (back up)
- planes de recuperación de desastres

41. Existe una versión sencilla, llamada **PILAR Basic**, orientada a PYMES y a la Administración Local.
42. Puede encontrar más información sobre esta herramienta en su manual ([Ref.- 10]), en la pagina web del CCN-CERT ([Ref.- 1]) o poniéndose en contacto directamente con éste.

5.1.1.3. GRUPO DE CONTROL DE LA SEGURIDAD EN SCADA

43. El conocimiento y control del riesgo y de las variables de las que depende es una tarea continua porque están continuamente evolucionando. Para mantener el conocimiento actualizado una buena técnica es establecer **un grupo de control de la seguridad en SCADA** que revise periódicamente las políticas y normas, su ejecución, los resultados y el entorno existente.
44. En dicho grupo deben estar representados al menos los siguientes grupos:
    - Gestión: proporciona una perspectiva de lo que el negocio necesita, puede ser uno o varios altos directivos.
    - SCADA: proporciona representación y capacidades de los sistemas de control de procesos, identificación de activos críticos y el nivel de exposición existente.
    - Seguridad: proporciona una perspectiva de conocimiento, experiencia e integración en seguridad física y de la información.
    - Ingeniería: en caso de que sea un grupo distinto al de SCADA se puede necesitar orientación práctica sobre el funcionamiento de la empresa.
    - Tecnologías de la información: en caso de que se trate de un grupo distinto de ingeniería y de SCADA, proporcionará orientación sobre nuevas fuentes de amenazas.
    - Recursos humanos: orientación clave para garantizar la coherencia y el cumplimiento de las condiciones de trabajo necesarias.
45. Este grupo no buscará soluciones técnicas, pues su trabajo será a un nivel superior. Sus responsabilidades principales son (se pueden encontrar más en [Ref.- 18]):
    - Controlar el programa de seguridad en SCADA: activos, amenazas, vulnerabilidades, riesgos, impactos y contramedidas (salvaguardas).
    - Examinar los factores de riesgo identificados
    - Seleccionar las medidas apropiadas de reducción de riesgos.
    - Equilibrar la política y las estrategias de seguridad con otros factores: necesidades de la empresa, requisitos legales, recursos disponibles (materiales, técnicos y humanos).

- Desarrollar los procedimientos asociados que apoyen a las medidas de reducción de riesgos. Cabe señalar que no se trata sólo de escribir y publicar estos procedimientos; a menudo el esfuerzo se centra en incluirlos en las actividades del día a día.
- Mantener la política, normas y procesos actualizados con las amenazas actuales.
- Integrar los requisitos de condiciones de trabajo en la seguridad en SCADA.
- Gestionar el plan de concienciación y formación en SCADA.
    - Asegurar que todos los ingenieros, usuarios y administradores son conscientes de la seguridad e implementan los procesos y procedimientos de forma segura.
    - Garantizar una capacidad respuesta adecuada para reaccionar ante los cambios en las amenazas a la seguridad.
    - Asegurar que el riesgo derivado de colaboradores es gestionado.
- Monitorizar e informar del estado de la seguridad en el SCADA, manteniendo un control de proyectos y cambios.
    - Vigilar que se incluyen las pruebas de integración y despliegue y garantizar que las medidas se han aplicado correctamente.
    - Una vez finalizados los proyectos y los cambios, debe garantizarse que las medidas han sido desplegadas conforme al diseño de la arquitectura de seguridad.
- Definir y delegar en su caso las responsabilidades.

46. Pero el objetivo fundamental de este grupo es ayudar a elaborar una Arquitectura de Seguridad.

5.1.1.4. ARQUITECTURA DE SEGURIDAD

47. Se realizará teniendo en cuenta las recomendaciones del análisis de riesgos. Es importante comprender las prioridades y los activos de la empresa antes de elaborar un plan.

48. Para cada riesgo hay tres tipos de acciones disponibles:

- Aplicar medidas de reducción de riesgos (o medidas de mejora de la seguridad): el resto de esta sección trata la selección de estas medidas con más detalle.
- Aplicar un plan de continuidad: este tema se trata en el módulo “Establecer capacidades de respuesta” y se puede localizar en el Apéndice A.
- Tratar como riesgo residual (no tomar ninguna acción): en caso de que se decida tratar un riesgo como residual, se debe aceptar por la dirección y debe registrarse en un registro de riesgos.

49. Al adoptar medidas de reducción de riesgos, hay una serie de factores a tener en cuenta:

- El coste
- La eficacia de la medida. Suele relacionarse con el coste para tener una mejor capacidad de evaluación.

- El modelo de negocio: la necesidad de seguridad (muy alta en el caso de ICN), las necesidades legislativas, el Retorno de la Inversión en Seguridad (RIS).
- La dificultad de implementación de la medida. Algunas medidas de seguridad necesitan poco tiempo porque implican pequeños cambios en la configuración de los sistemas existentes o modificaciones menores en prácticas de trabajo existentes. Sin embargo, la implementación de otras medidas de seguridad mayores pueden implicar la implantación de un nuevo sistema o la creación de nuevas prácticas o procedimientos de trabajo.
- La soluciones existentes, teniendo en consideración estándares, tecnologías certificadas y recomendaciones de la industria.

50. Las medidas de seguridad pueden necesitar algún tiempo para ser implementadas (ej. rediseñar la red e implementar el cortafuegos). Considerar la posibilidad de medidas cautelares simples y de bajo coste que puedan proporcionar alguna protección a corto plazo.

5.1.1.5. CONTRAMEDIDAS

51. 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.
52. 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.
53. Las contramedidas mínimas que se deben garantizar son:
    - Un Equipo de Respuesta ante incidentes de Seguridad SCADA para responder a los incidentes de seguridad.
    - Los adecuados planes de respuesta a incidentes y de continuidad del negocio para todos los sistemas de control de procesos.
    - El mantenimiento, ensayo y pruebas de todos los planes de seguridad.
    - Un sistema de alerta temprana que notifique al personal encargado de los incidentes y alertas de seguridad.
    - 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.
    - Procedimientos de comunicación y revisión de todos los incidentes de seguridad.
    - Actualización de las políticas y estándares con las lecciones aprendidas.
54. Los planes de respuesta son a menudo bastante amplios y deben estar redactados de acuerdo al modelo operativo elegido. 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.

5.1.1.6. EQUIPO DE RESPUESTA DE SEGURIDAD SCADA

55. Un Equipo de Respuesta de Seguridad SCADA (ERS) es un elemento fundamental de la capacidad de respuesta de una organización y proporciona las bases para la monitorización, análisis y respuesta eficaz a alertas e incidentes. El ERS debe participar en cada una de las etapas del proceso de monitorización de una situación, analizando cualquier cambio en la amenaza e iniciando las respuestas apropiadas.
56. Es un requisito fundamental que las personas con las capacidades y conocimientos adecuados están involucradas en el ERS, ya sea a tiempo parcial o completo. Sus miembros deben de proceder de varias fuentes, con representantes de distintas áreas, incluyendo:

- Equipo de control de procesos, SCADA y automatización.
- Seguridad TI.
- Infraestructura TI.
- Gestión del negocio.
- Operaciones.
- Reguladores internos.
- Departamento jurídico.
- Oficina de contacto con los medios.
- Equipo de seguridad empresarial.

57. Según el tamaño y las necesidades de la empresa, puede haber un ERS centralizado, como un Centro de Coordinación (CC), o una red de ERS locales, o una combinación de ambos.

58. Entre sus responsabilidades, están:

- Garantizar que se cumple el plan de alerta temprana.
    - **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**: responder en base al tipo y categoría de la amenaza y el riesgo asociado para la organización.
- Ejecutar los planes de respuesta y continuidad existentes.
- Ensayar y probar periódicamente los planes existentes, al menos anualmente y con mayor frecuencia para sistemas críticos o de alto riesgo.
- Revisar y mantener actualizados los planes existentes a raíz de cualquier cambio en la amenaza, en los requisitos de protección, el sistema, la estructura organizativa, o las lecciones aprendidas durante un ejercicio o tras un incidente.
- Revisar regularmente los riesgos residuales.
- Proponer cambios al grupo de gestión de la seguridad en SCADA.

5.1.1.7. REVISIONES CONTINUAS

59. El estudio del riesgo suele ser un proceso muy largo y que necesita información de muchas fuentes. Por ello, es fácil que quede desactualizado, obsoleto e inservible. Para evitarlo, hay que definir “disparadores” que pongan en marcha el proceso de actualización cuando sea necesario. Tales factores desencadenantes pueden variar , pero suelen incluir:

- Cambios en:
    - Nivel de amenaza.
    - Tolerancia al riesgo.
- Criticidad y riesgo de sistema.
- Cumplimiento de las garantías necesarias.
- Nuevos proyectos.
- Cambios en un sistema.
- Fusiones y adquisiciones.
- Circunstancias políticas.
- Tiempo transcurrido (revisiones periódicas).

- Incidente/s importante/s

60. Una revisión del análisis de riesgo suele desencadenar una serie de cambios en los siguientes elementos de la empresa:
    - Programa de seguridad SCADA.
    - Estructura jerárquica y responsabilidades.
    - Planes de respuesta (que deben reflejar con exactitud los sistemas y procesos existentes.
    - Inventario, actualizándolo para hacer frente a los nuevos riesgos.

5.1.2. POLÍTICAS, NORMAS Y GUÍAS

5.1.2.1. ÁMBITO

61. Las **políticas** de seguridad en SCADA son el resultado directo de la gestión del riesgo. Definen los límites dentro de los que se pueden tomar medidas. Tienen aplicación amplia, entran en poco detalle y sufren pocas modificaciones a lo largo del tiempo.
62. Las **normas / instrucciones técnicas (IT)** son la aplicación práctica de las políticas. Definen la creación, el mantenimiento y la eliminación de componentes en los sistemas SCADA. Proporcionan una interpretación organizativa coherente para lograr la calidad deseada de la política definida. Están influenciadas por la legislación, la tecnología y las necesidades. Se adaptan a cambios de escenario y suelen revisarse con frecuencia media.
63. Las **guías** proporcionan los detalles adicionales para asegurar que las normas e instrucciones técnicas se plasman apropiadamente en soluciones prácticas para entornos específicos, sin el problema de complicar innecesariamente la normativa de nivrel superior. Se trata generalmente de los documentos más detallados y sólo se centran en una aplicación específica, como la forma de configurar un modelo de cortafuegos de acuerdo a la norma / IT de rango superior. Están en continua evolución y adaptación.
64. Las políticas y las normas son el mecanismo mediante el cual una organización puede comunicar a todos los niveles el objetivo buscado de protección de la seguridad en SCADA, y cómo se debe alcanzar.
65. Las políticas y normas de seguridad en SCADA pueden estar combinadas o ser independientes de las políticas de seguridad generales, las de seguridad en TI y las de seguridad en la producción. La decisión de combinarlas o separarlas dependerá del tamaño y la estructura de la empresa, de la dependencia entre ámbitos y de la disponibilidad de recursos.

5.1.2.2. DEFINICIÓN Y REVISIÓN

66. Las **políticas** las definen los grupos directivos y gestores, normalmente a través del Grupo de control de la seguridad en SCADA. El mínimo detalle que debería incluirse en un documento de política es:

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

67. Las **normas / instrucciones técnicas** pueden ser elaboradas con la ayuda de grupos internos de especialistas o con la ayuda de terceros, pero deben ser siempre aprobadas por los grupos directivos y gestores, normalmente a través del Grupo de control de la seguridad en SCADA. El detalle que debería incluirse en una norma es:

- La política a la que se aplica la norma; “que política o políticas"
- La audiencia o lectores: “el nivel de detalle”
- La definición y aplicación de la norma: “¿qué es esto, cómo se aplica a las personas, los procesos y la tecnología?"
- A qué o quiénes se aplica la norma: “el objetivo o los límites de las normas”
- quién es propietario de la norma: “quién la publicará y actualizará”
- qué significa la actualización de la norma: “cuando debería revisarse la norma”
- los criterios y procesos de excepción: “cuando no es aplicable la norma”.

68. Las **guías** las elabora cada grupo para aplicar las normas / IT recibidas y no deben ser aprobados, aunque es conveniente que se supervisen. Su contenido dependerá del ámbito.

5.1.2.3. APLICACIÓN

69. No sólo es necesaria la existencia de políticas y normas adecuadas, sino también la vigilancia de su cumplimiento. Esta vigilancia proporciona una información muy importante para poner de relieve las dificultades de la política y las normas, y puede ser un mecanismo para actualizar o corregir donde no se alcancen los objetivos deseados. El cumplimiento de las políticas y normas:

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

70. Para garantizar una buena aplicación de las políticas y normas, ha de vigilarse los siguientes aspectos:

- ¿Es la información suministrada suficiente (ni demasiada ni escasa) para el público objetivo en cada ámbito?
- ¿Quién es el responsable de la difusión y aplicación de las políticas y normas en cada nivel?

- ¿Quién es el responsable de recopilar los datos sobre los resultados de seguridad en SCADA? Esta pregunta debe tener en cuenta el siguiente apartado de auditoría.

71. Las actividades típicas de vigilancia del cumplimiento incluyen:

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

5.1.2.4. PLANES DE RESPUESTA

72. Los planes de respuesta de seguridad SCADA son a menudo bastante amplios y deben estar redactados de acuerdo al modelo operativo elegido. 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 procedimiento claro de escalado y los requisitos de autorización necesarios para la escalada del incidente
- 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.

5.1.3. AUDITORÍAS

73. En ocasiones se tiene la falsa impresión de que por que no se haya detectado ningún fallo de seguridad en los sistemas, estos no han sido comprometidos. El 8 de abril de 2009, el Wall Street Journal publicó la noticia de que la red eléctrica de EE.UU. había sido comprometida por organizaciones extranjeras ([Ref.- 28]). En cambio, no se había producido ninguna pérdida de servicio ni de información. Las intrusiones se habían limitado a preparar puertas traseras para accesos posteriores.

74. Las revisiones o auditorias son importantes para poder detectar y corregir a tiempo vulnerabilidades en la seguridad de los sistemas SCADA. Estas auditorias se pueden realizar de diferentes maneras:

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

75. Se puede encontrar más información sobre auditorias en los documentos referenciados en el ANEXO A. Referencias ([Ref.- 18])

5.1.4. GESTIÓN DE PROYECTOS EN SCADA

76. Los sistemas SCADA suelen instalarse con la expectativa de una larga vida útil y unos cambios mínimos durante su vida. Sin embargo, muchos proyectos cuyo ámbito no sea el control de procesos pueden tener impacto en los sistemas SCADA y en su seguridad. Algunos ejemplos son la implantación, actualización o cambio de sistemas SCADA o TI, cambios en los procedimientos, el desarrollo de información sobre la gestión de sistemas y la introducción de nuevas conexiones.

77. Estos proyectos deben ser controlados estrechamente.

5.1.4.1. FASES PREVIAS

78. Cualquier proyecto que pueda afecta a la seguridad en sistemas SCADA debe incorporar los requisitos de seguridad adecuados desde sus primeras etapas. Cualquier nuevo sistema en un centro de nueva creación debería incluir requisitos de seguridad en los procesos de diseño y construcción desde la primera etapa. El cumplimiento de estos requisitos se debe asegurar en todo el ciclo vida del proyecto.

79. Es recomendable nombrar un **ingeniero de seguridad** que se encargue de garantizar que la seguridad está convenientemente tratada en los requisitos, el análisis y la arquitectura del proyecto, con visibilidad de futuro de todas las etapas de implantación, explotación y baja del proyecto. Algunas sugerencias son:

- Revisiones de seguridad del diseño
- Revisiones de la seguridad del código
- Rutinas de mantenimiento
- Administración y monitorización de los elementos de seguridad (cortafuegos, antivirus)
- Pruebas de entrega
- Procedimientos de parcheado y control de cambios
- Planes de respuesta, continuidad y de pérdida de visión
- Aislamiento del sistema
- Garantía continuada
- Documentación actualizada del sistema
- Plan de sustitución y baja del sistema (destrucción de datos, etc.)

80. Los requisitos de seguridad no deben ser considerados distintos a cualquier otro requisito funcional. La no inclusión, por el motivo que sea, es fuente de problemas en fases posteriores y el coste de solucionarlos es mayor que el coste de invertir el tiempo suficiente en las primeras etapas para garantizar que el proyecto está bien definido.

5.1.4.2. REALIZACIÓN

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

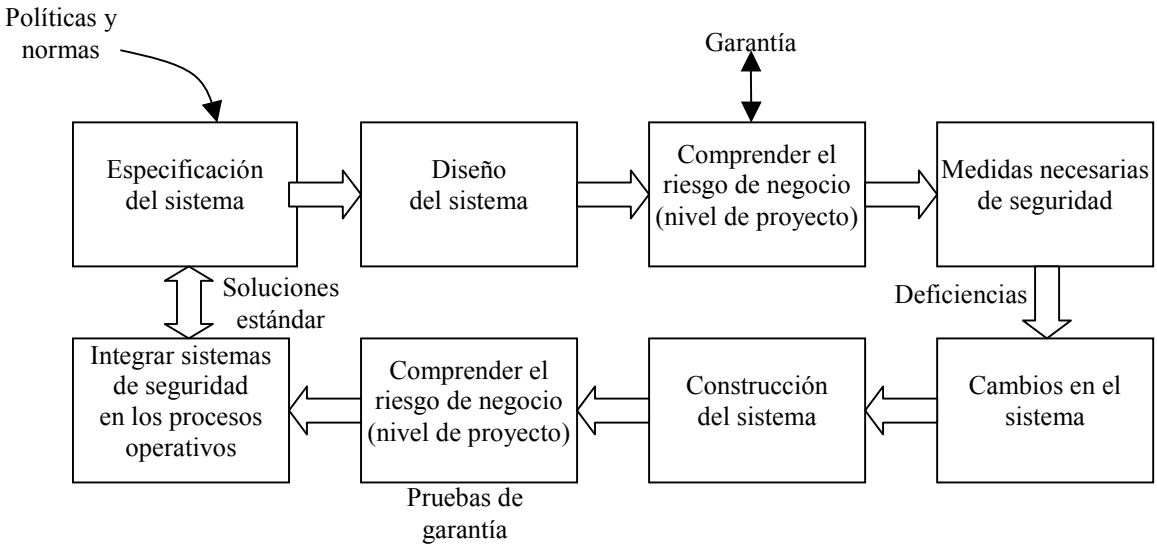


Figura 3: ***Seguridad en el ciclo de vida del desarrollo ([Ref.- 17])***

82. La vigilancia de la seguridad debe realizarse a través de una serie de **pruebas** para confirmar la seguridad del sistema resultante y para garantizar que se podrán gestionar las vulnerabilidades en el futuro, incluyendo ([Ref.- 17]):

- **Pruebas de unidad**: comprobación de que cada elemento independiente cumple los requisitos de seguridad acordados.
- **Pruebas de sistemas integrados**: los elementos integrados que se incorporen a un proyecto, sobre los que no se tenga control en su funcionalidad y vulnerabilidades, deben ser probados independientemente, garantizando que cualquier fallo en su funcionamiento va a tener un impacto mínimo en el resto del sistema.
- **Pruebas en desarrollo**: en el caso de proyectos externos o compra de sistemas completos, o antes de pasar el sistema a producción en el caso de proyectos internos, han de probarse al menos los siguientes elementos:
  - Configuración de seguridad
  - Escaneado de vulnerabilidades en todo el sistema
  - Pruebas de penetración
  - Pruebas de las reglas del cortafuegos
  - Pruebas de recuperación de fallos/desastres
  - Pruebas de copias de seguridad
  - Pruebas de parcheados (actualizaciones de seguridad)
  - Pruebas de actualización del antivirus
  - Pruebas de acceso remoto
  - Garantía de protección del sistema
- **Pruebas de puesta en servicio**: Finalmente, una vez llegado al entorno productivo, pero antes de comenzar a prestar servicio, es importante repetir todas las pruebas anteriores.

5.1.4.3. REQUISITOS DE FINALIZACIÓN

83. Los requisitos para aceptar la entrega de un proyecto externo o la finalización de uno interno deben estar estipulados desde la primera fase o, en caso contrario, serán difíciles de exigir. Los requisitos de seguridad, como el resto de requisitos, deben estar igualmente contemplados.
84. Es importante que junto con el sistema se documenten una serie de procedimientos operativos que garanticen que la seguridad podrá ser mantenida durante toda la vida del sistema:

- Vigilancia de los registros del sistema
- Rutinas de mantenimiento
- Administración y monitorización de los cortafuegos
- Despliegue y garantía de los antivirus
- Planes de respuesta y continuidad
- Procedimientos de control de cambios
- Pruebas de fallo

- Procesos de parcheado (actualizaciones de seguridad)
- Aislamiento del sistema
- Procedimientos de pérdida de visión
- Garantía continuada (véase la guía "CCN-STIC-480B Comprender el riesgo del negocio" [Ref.- 12])
- Confirmación de todo el software en los discos duros y el *firmware*
- Documentación actualizada del sistema
- Resultados de las pruebas de aceptación en fábrica y de puesta en servicio

5.1.4.4. OTROS ASPECTOS

85. Ha de considerarse muy detalladamente la gestión de los recursos humanos implicados en los proyectos realizados, especialmente cuando dichos recursos pertenezcan a empresas subcontratadas. Este aspecto se trata en el apartado siguiente.

5.1.5. EMPRESAS EXTERNAS

86. En el ciclo de vida de todo sistema de cierta complejidad es inevitable que intervengan empresas externas. Estas empresas pueden participar en la implementación, en la operación, en el soporte o en otros aspectos. Y su acción no debe comprometer la seguridad del sistema.
87. Entre las empresas externas con las que se colabora se pueden encontrar, entre otras:
    - Proveedores y fabricantes
    - Desarrolladores e implantadores
    - Empresas de soporte
    - Acuerdos de servicio
    - Subcontratistas
    - Consumidores / receptores de servicio
88. Se recomienda elaborar un **inventario de terceros** que contenga información sobre todas las empresas externas. Si se registra muy poca información, puede que no sea suficiente para un análisis profundo en etapas posteriores. Si se registra demasiada, será difícil de mantener. Cualquier nueva información debe ser añadida al inventario para mantenerlo actualizado.
89. El inventario de terceros debe contener, al menos:
    - Empresas externas que tienen relación con los sistemas SCADA.
    - Conexiones que dichas empresas realizan a los sistemas SCADA, sean en serie, por módem, VPN o a través de otras redes o Internet.
    - Empleados de la empresa externa acreditados para formar parte de la relación.
90. El inventario de terceros se elabora a partir del inventario de sistemas SCADA (descrito en 119), considerando 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?

91. A la hora de acordar una relación con una empresa externa, es importante incluir cláusulas que ayuden a mantener la seguridad y a gestionar el riesgo. Gran parte de esta tarea es llevada a cabo por los departamentos legales o de adquisiciones, pero es importante garantizar que los contratos incluyen los siguientes compromisos:

- **Acuerdo de no divulgación**: La empresa externa puede tener acceso a información sensible sobre la organización y sus sistemas, especialmente sobre los sistemas SCADA, y es esencial que ésta no se explote ni utilice sin el permiso de la organización propietaria de la información.
- **Controles de antecedentes/controles de seguridad interna**: La organización debe pedir garantías a los proveedores de que sus empleados que trabajan en áreas sensibles se han sometido a los pertinentes controles de seguridad (habilitaciones o garantías personales de seguridad) antes de ser empleados o contratados. Esto es especialmente importante en el caso de proveedores y subcontratistas.
- **Derecho a auditar:** Incluir cláusulas que garanticen el derecho a auditar o revisar los servicios sistemas y locales de terceros.
- **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.

92. Pero además, algunos tipos de colaboradores tienen consideraciones específicas que se listan a continuación:

- **Proveedores**.
- **Empresas de soporte**
- **Cadena logística (suministro)**

5.1.5.1. PROVEEDORES

93. Deben incluirse al menos las siguientes cláusulas específicas de seguridad en SCADA:

- **Compartición de información sobre los sistemas**, incluyendo**:**
  - **Especificaciones técnicas de los sistemas provistos**: Las organizaciones deben incitar a los proveedores a detallar los puertos y protocolos utilizan.
  - **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.
- **Acreditación de proveedores**: Introducir los requisitos de seguridad en el control de proceso en la selección y acreditación del proveedor es una herramienta muy poderosa para garantizar que la cultura y el enfoque de seguridad deseados forman

parte de las decisiones tomadas. La lista resultante de proveedores 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 acreditados, ya que puede ser una buena fuente de negocio.

- **Pruebas de seguridad / certificación de seguridad:** Las organizaciones deben incitar a los proveedores para que lleven a cabo pruebas de seguridad – certificaciones de seguridad (contra el estandar Common Criteria) de sus productos para identificar y eliminar vulnerabilidades de seguridad. Las organizaciones deben obtener garantías de los proveedores y vendedores de que los 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 o certificaciones de seguridad sobre los sistemas de control y sus componentes (tales como PLC) para garantizar que están libres de vulnerabilidades de seguridad.
- **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.
- **Revisiones de seguridad**: Deben realizarse revisiones regulares de seguridad con el proveedor para tratar cuestiones de seguridad extraordinarias, los planes de mejora, y para discutir el cumplimiento de la política de seguridad.
- **Asistencia en la securización del sistema:** La mayoría de los sistemas y equipos de control de procesos vienen de fábrica bastante desprotegidos (configurados por defecto), 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 toda la información sobre la securización de los sistemas en un documento específico.

5.1.5.2. EMPRESAS DE SOPORTE

94. Algunas empresas de soporte prestan éste después de proveer un sistema, en cuyo caso son también proveedores y deben incluir las cláusulas específicas.

95. Deben incluirse al menos las siguientes cláusulas específicas de seguridad en SCADA:

- **Cláusula de aceptación de cambios**: cualquier nueva tecnología introducida en un sistema SCADA debe estar autorizada. 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 acreditarse el servicio por el procedimiento aprobado.
- **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.
- **Control del personal:** 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. Esta concienciación debe estar adaptada a la empresa para la que se hace el soporte. Además los empleados que trabajan en este soporte se han sometido a los pertinentes controles de seguridad (habilitaciones o garantías personales de seguridad) y esta debidamente formado.

- **Garantía de soporte remoto:** La conexión remota debe ser segura y existe un procedimiento que fija cuando se realiza. Los sistemas desde los que se conectan los proveedores también deben ser seguros, tanto física como electrónicamente. Cualquier información confidencial de los clientes que se guarde en dependencias remotas debe estar debidamente protegida. Las organizaciones se deben asegurar del cumplimiento de estos requisitos a través de las visitas o auditorias pertinentes.

5.1.5.3. CADENA DE SUMINISTRO

96. Deben incluirse al menos las siguientes cláusulas específicas de seguridad en SCADA:

    - **Cláusula de responsabilidad:** Allí donde los sistemas o conexiones superan los límites de la organización, se deben acordar convenios claros de responsabilidad en seguridad del proveedor.

5.2. RECURSOS HUMANOS

97. La mayor parte de los incidentes de seguridad se producen por causa del factor humano. De poco sirve tener un sistema seguro si los encargados de mantenerlo no están preparados o predispuestos para la tarea.

98. Cuando se habla de recursos humanos, se habla de toda persona, contratada o no por la empresa, que tenga relación con los sistemas SCADA. Deben cuidarse los siguientes aspectos:

    - Contratación
    - Formación
    - Relaciones interdepartamentales
    - Baja

5.2.1. CONTRATACIÓN

99. Antes de contratar a un empleado que por su trabajo vaya a tener acceso operativo o administrativo al entorno SCADA, es necesario asegurarse de que se trata de una persona en el que se puede confiar. Esto se puede lograr por medio de controles iniciales y periódicos de seguridad, y una investigación más o menos exhaustiva. Es recomendable una investigación de antecedentes en el caso de personal para entornos críticos. Estos procesos estan definidos en las habilitaciones / garantías personales de seguridad.

100. También es necesario implementar los procedimientos necesarios para garantizar que los nuevos usuarios de cualquier entorno reciben las cuentas correspondientes, los

niveles de autorización y capacitación necesarias en materia de seguridad cuando se unan a un equipo SCADA.

5.2.2. FORMACIÓN

101. La formación del personal implicado en la producción o en los sistemas SCADA es importante porque permite aumentar su capacidad de respuesta ante incidentes, pero no debe centrarse sólo en ese punto.

5.2.2.1. OBJETIVO DE LA FORMACIÓN

102. La formación debe perseguir los siguientes objetivos ([Ref.- 15]):

- Concienciación general en la seguridad SCADA
- Establecer un lenguaje compartido que permita una comunicación fluida
- Comprender los distintos entornos operativos
- Transferir entre áreas los conocimientos necesarios para que todo el personal aplique y cumpla con medidas adecuadas de seguridad.

103. La formación no debe centrarse en los puestos técnicos sino abarcar todos los puestos que tengan alguna relación con SCADA en todos los escalafones de la jerarquía. Algunos de los principales beneficios de la participación de los altos directivos son:

- Elevar el perfil de la seguridad en el control de procesos
- Facilitar la concienciación mediante mensajes utilizando la jerarquía de gestión y los canales de comunicación de ésta
- Garantizar un presupuesto adecuado para el programa de concienciación
- Entender que algún riesgo residual seguirá existiendo
- Eliminación las barreras internas entre recursos.

5.2.2.2. PLAN DE FORMACIÓN

104. Un paso evidente pero a menudo pasado por alto es evaluar lo que ya se sabe, tal vez mediante el uso de una breve encuesta o sondeo. Este conocimiento debe ser utilizado como base para los temas de concienciación.

105. La formación debe adaptarse a las necesidades de cada público objetivo. Los siguientes elementos deberían ser comprendidos a todos los niveles:

- Políticas, normas e instrucciones técnicas vigentes.
- Procedimientos establecidos.
- Actualizaciones de los documentos existentes
    - Políticas y normas
    - Orientación de proveedores

- Respuesta a incidentes: responsabilidades de cada actor. Qué debe vigilar cada uno y cómo debe responder.
- Ejemplos de fallos de seguridad SCADA y sus efectos.

106. Además, deben cubrirse al menos los siguientes aspectos específicos para cada uno de los grupos siguientes:

- Para órganos directivos:
  - Una visión general del perfil de riesgo de la empresa (incluyendo el impacto de las amenazas potenciales, de los incidentes y las vulnerabilidades).
  - Los beneficios de mejorar la seguridad del control de sistemas, incluyendo el perfil de riesgo mejorado tras los incidentes (ej., el beneficio empresarial)
  - Los requisitos para un programa de seguridad, las principales actividades, recursos y costes
  - El Retorno de la Inversión en Seguridad (RIS).
- Para profesionales de TI:
  - Explicación y comprensión del ámbito SCADA.
  - Conocimiento de la arquitectura y conexiones entre equipos.
- Para profesionales SCADA:
  - Explicación y comprensión de seguridad en TI.
  - Conocimiento de la arquitectura y conexiones entre equipos.
  - Formación de seguridad específica para los sistemas de un proveedor

5.2.2.3. MÉTODOS DE FORMACIÓN

107. De los cursos de seguridad TI disponibles, encontrar cuál proporcionará un nivel adecuado de comprensión puede ser proceso difícil y largo. El análisis de las necesidades de formación es de gran ayuda en este ámbito y seleccionar cursos organizados por organizaciones profesionales reconocidas garantizará que se cumplan las necesidades de formación. Sin embargo, es poco probable que se oferte todo lo que se necesita y es probable que sea necesaria una mezcla de métodos de entrega.

108. Los métodos de formación más comunes son:

- Cursos externos: realizados por proveedores o por profesionales de la seguridad. Pueden incluir certificaciones, lo que supone un valor añadido para la organización.
- Cursos internos: se ocupan de temas específicos de organización y puede poner en contexto los conocimientos adquiridos externamente
- Conferencias: presenciales o remotas.
- Talleres: específicos o multidisciplinares, permitiendo estos últimos que se apliquen una amplia gama de experiencias y conocimientos a un problema.
- Boletines de seguridad: en papel o por correo electrónico.
- Repositorio centralizado de conocimientos sobre la seguridad en SCADA.

- Sitios Web y emisiones por Internet (*webcast*): dependen de la motivación de los individuos, pero pueden ser útiles como parte de almacenes de conocimientos.
- Llamadas telefónicas.
- Campañas con carteles.
- Videos y DVD.
- Inclusión de temas de seguridad en las agendas de las reuniones.

5.2.2.4. PLANES DE RESPUESTA

109. 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.
110. 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, en el propio sistema o en la estructura organizativa. Las lecciones aprendidas durante un ejercicio o después de que se produzca un incidente también deben incorporarse en los planes.

5.2.3. RELACIONES INTERDEPARTAMENTALES

111. Los sistemas SCADA suelen ser punto de confluencia de diferentes áreas de conocimiento. La operatividad de los sistemas controlados (energéticos, industriales, etc.) suele ser muy diferente a la de los sistemas que se utilizan para el control (TI).
112. La colaboración entre los grupos de SCADA y de TI comienzan en el grupo de control de la seguridad SCADA, donde otros departamentos de la empresa están también representados y debe comenzar a forjarse el compromiso entre ambos. Dicha colaboración ha de forjarse desde el respeto y la comprensión de los intereses mutuos y potenciarse desde la escala administrativa.
113. Algunos mecanismos para potenciar dicha colaboración son ([Ref.- 15]):

- Representación TI en el Equipo de Respuesta de Seguridad SCADA (ERS) o empleo de un único equipo multidisciplinar.
- Reuniones periódicas para discutir los desarrollos y el progreso de la seguridad.
- Invitar a representantes de TI a las reuniones de control de cambios en SCADA.
- Ampliar las listas de distribución e incluir los correspondientes contactos de TI.
- Establecer un sistema de tutoría.
- Tener una representación de SCADA en el equipo de seguridad de TI de la organización.
- Trabajo compartido: Formación cruzada del personal de TI y de SCADA, cubriendo cada uno los trabajos de los otros.
- Equipos de proyecto combinados.

114. Las ventajas de un aumento de las relaciones interdepartamentales son muchas en cualquier ámbito, pero especialmente importantes en la seguridad SCADA:

- Aumento de la transferencia de conocimientos.
- Acceso a una base más amplia de capacidades técnicas en seguridad.
- Acceso a una base más amplia de capaciddes técnicas en control de procesos.
- Mejor comprensión de las medidas de seguridad aplicadas.
- Una oportunidad para compartir las mejores prácticas de cada departamento.
- Soluciones de seguridad a menor coste por ser compartidas
- Prácticas de trabajo más eficaces
- Mayor velocidad en la ejecución de proyectos

115. Los grupos de TI pueden proporcionar y facilitar varios servicios a otros departamentos de la organización y, por supuesto, a SCADA. Desarrollando de una estrecha relación pueden identificarse soluciones de TI que se puedan utilizar en el entorno SCADA, ya sea directamente (con ajustes mínimos) o modificando la configuración del entorno de control de procesos. Ejemplos de servicios / mecanismos que pueden ser proporcionados por TI son:

- Herramientas antivirus
- Administración y monitorización de cortafuegos y otros dispositivos de defensa perimetral
- Monitorización de los sistemas y las redes
- Gestión de acceso remoto a los sistemas
- Respuesta a incidentes y alertas
- Formación y concienciación en seguridad
- Gestión continua del aseguramiento

5.2.4. BAJA

116. Implementar los procedimientos para garantizar que la información y la documentación confidencial son recuperadas, se desactivan las cuentas y se cambian las contraseñas cuando ya no sea necesario un acceso al entorno SCADA. Esto puede producirse por:

- Cambio de roles y responsabilidades
- Baja de personal
- Finalización de relaciones con externos (proveedores, contratistas, etc.)

117. Es necesario que existan los procedimientos necesarios que garanticen la comunicación fluida entre distintos departamentos para que se tenga conocimiento inmediato cada vez que se produce una baja y se puedan activar los mecanismos correspondientes.

5.3. SISTEMAS

118. La mayoría de los análisis de seguridad en entornos tecnológicos empiezan por recomendar acciones relacionadas con los sistemas, su configuración y sus tecnologías. En este documento, los sistemas se tratan en último lugar porque la experiencia ha demostrado que enfocar los esfuerzos en ellos obtiene un **pico de seguridad** puntual en el momento del esfuerzo, pero esa seguridad desaparece rápidamente al no haber medidas que permitan mantenerla. Como la seguridad debe ser una preocupación constante, debe dedicarse la atención necesaria a los aspectos relacionados con la gestión de la empresa y los recursos humanos que se han tratado en los apartados anteriores.

119. Es importante garantizar una serie de aspectos básicos relacionados con los sistemas SCADA, lo que se puede hacer respondiendo a las siguientes preguntas:

- **Segregación:** ¿Están adecuadamente separadas las redes SCADA de las redes de administración y de otras redes externas (Internet), por los medios apropiados?
- **Monitorización y detección:** ¿Está el cortafuegos y los dispositivos de protección de perímetro de SCADA registrados y revisados? ¿Se monitoriza la actividad de los usuarios/sistemas? ¿Se monitorizan los *logs* de los antivirus y de otros dispositivos del sistema, etc.?
- **Parcheado – actualizaciones de seguridad:** ¿Con qué velocidad se aplican los parches? ¿De dónde se reciben? ¿Están parchadas todas las máquinas?
- **Protección antivirus:** ¿Con qué velocidad se realizan las actualizaciones? ¿Cuáles son el método y la frecuencia de escaneado?
- **Planes de respuesta:** ¿Se revisan y actualizan los manuales regularmente? (ej, anualmente)
- **Copias de seguridad:** procedimientos de copia de seguridad y restauración.

120. En general, cualquier medida técnica de seguridad que se pueda aplicar en TI puede ser utilizada en SCADA y viceversa, siempre que se cumplan una serie de requisitos formales en SCADA que garanticen una coherencia y un endurecimiento de dichas medidas.

5.3.1. GESTIÓN DE ACTIVOS

121. Toda gestión de activos debe comenzar con un inventario detallado y actualizado de éstos. El inventario es un bloque fundamental para construir el marco de seguridad En el caso de SCADA es importante capturar, documentar y tener bajo control de cambios todos los aspectos de los sistemas para garantizar su seguridad, identificar el alcance de los sistemas y la identidad de todas las interfaces, *hardware* y *software*.

122. El **inventario de sistemas SCADA** debe incluir localizaciones, centros, sistemas y activos que existen, especificando de cada uno:

- situación geográfica
- papel
- importancia en la cadena de producción

- puntos críticos de seguridad
- pertenencia o no al Catálogo de Infraestructuras Críticas Nacionales
- responsable único designado
- gestor
- proveedor/es de soporte (interno o externo). En sistemas sensibles es obligatorio que todo producto y sistema tenga soporte.
- organizaciones de apoyo (TI, SCADA, colaboradores remotos o locales, etc.)
- interacciones y dependencias, haciendo especial hincapié en los accesos remotos
- proyectos en curso
- problemas conocidos
- condiciones de trabajo especiales o implicaciones legales.

123. Los inventarios son muy difíciles de generar y mantener actualizados. Es importante realizar una auditoria y una evaluación formal del inventario de los sistemas SCADA. Además debe mantenerse actualizado, ya sea por medios automáticos o modificando los procedimientos adecuados para garantizar que queden registrados todos los cambios que se realicen en los activos.

124. Los inventarios son una fuente de información sensible, que puede ser muy útil para un atacante. En consecuencia, estos inventarios deben protegerse. El acceso a estos inventarios debe limitarse al mínimo número de personas que necesiten acceder a esta información.

5.3.2. SEGURIDAD FÍSICA

125. El acceso a los sistemas SCADA y a la información que genera debe estar reducido al mínimo. Si el acceso electrónico no autorizado es un riesgo, el acceso físico no autorizado debe ser algo totalmente impensable. Sólo deben tener acceso aquellas personas con la autorización de seguridad adecuada.

126. El control del acceso físico (salas, edificios, dependencias) y lógico (inicio de sesión informática) debe cumplir al menos los siguientes requisitos:

- Acceso personalizado. Existen muchas guías acerca del control físico. Se puede consultar al CCN acerca de unas directrices básicas.
- Registro automático de de accesos autorizados, que no esté disponible para las personas con acceso autorizado.
- Acceso autorizado y supervisado de personal de terceros que deban acceder por requerimientos técnicos.
- Vigilancia/monitorización (cámaras de video, registro, etc.) de las actividades realizadas en las dependencias más sensibles.

127. Deben estar protegidas física y lógicamente los siguientes elementos:

- Equipos de control y SCADA
- Instalaciones de suministro a dichos equipos (eléctrico o de otro tipo)

- Almacenamiento de datos obtenidos por SCADA
- Documentación relacionada con SCADA: Informes, guías, análisis, resultados de auditorías, etc.

128. A la hora de seleccionar al personal con acceso autorizado, es necesario recordar los aspectos desarrollados en el apartado "5.2.1. Contratación", como la verificación de los antecedentes en el caso de acceso a entornos sensibles.

5.3.3. SEGURIDAD PERIMETRAL

129. El escenario ideal en un entorno SCADA es aquel en el que no existe ninguna conexión con ningún otro sistema, es decir, el sistema esta aislado. Este escenario no es siempre posible por, entre otros motivos, el uso de tecnologías TI, la monitorización centralizada de dependencias separadas geográficamente, el uso generalizado de Internet y la necesidad de soporte remoto de terceros.

130. Al estar conectados a otros sistemas, corren el riesgo de ser comprometidos o infectados. Aplicar a estos sistemas medidas de protección como cortafuegos u otros dispositivos de protección de perímetro es un elemento importante de defensa.

131. La selección de las medidas de seguridad debería basarse en el análisis de riesgo correspondiente. No tiene sentido invertir en una medida de seguridad fuerte y costosa para un riesgo o impacto mínimo cuando la inversión podría ser mejor aprovechada en otros lugares. En la herramienta PILAR existe un conjunto completo de salvaguardas, no obstante se recomienda hacer uso de los siguientes elementos:

- Cortafuegos y otros dispositivos de protección de perímetro
- Servidores de autenticación con comunicaciones cifradas
- Zona desmilitarizada o el sistema de protección de perímetro que se determine del análisis de riesgos de la interconexión de diferentes redes donde estén situados aquellos servicios que sirvan de enlace, evitando el acceso directo a los servidores SCADA.
- Sistemas de detección de intrusiones (IDS).

132. Algunos servicios no deberían estar disponibles nunca desde los sistemas SCADA, como correo electrónico, navegación Web y redes inalámbricas. En caso de que se necesiten para el normal funcionamiento de la empresa, es recomendable la coexistencia de dos redes separadas, una SCADA y otra de trabajo.

133. El control de las conexiones con otros sistemas ha de estar controlado y monitorizado, usando cortafuegos y herramientas de monitorización de tráfico. ([Ref.- 9]). Siempre que sea posible, hay intentar utilizar servicios y soluciones ya disponibles, como las proporcionadas por el departamento TI. Las soluciones pueden necesitar ser adaptadas al entorno operativo de los sistemas de control. Algunos de estos servicios pueden ser proporcionados por el grupo de TI:

- Administración y monitorización de cortafuegos y de otros dispositivos de protección de perímetro
- Monitorización de los sistemas y las redes
- Supervisión del acceso remoto

- Respuesta a incidentes y alertas
- Eliminación de conexiones no utilizadas

134. Cuando los servicios antes mencionados no estén disponibles en la empresa, considerar la subcontrata a terceros. Ejemplos de los posibles servicios externos son:
    - Administración y monitorización de los cortafuegos y de otros dispositivos.
    - Administración y monitorización de las redes y las comunicaciones.
    - Administración y monitorización de las infraestructuras.
    - Administración y monitorización de los servidores y de los equipos de administración.
135. Controlar el acceso de la subcontrata, que puedan realizar las tareas requeridas teniendo el mínimo acceso a la información y los procesos SCADA.
136. Siempre que sea posible, utilizar protocolos de comunicación *firewall-friendly*. Usar protocolos que no sean *firewall-friendly* (por ejemplo OPC[1]) implica que las regla de los cortafuegos no pueden ser configuradas en detalle.
137. 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", es decir disponer de varios mecanismos de seguridad.
138. Se puede encontrar más ayuda en las guías "CCN-STIC-408 Seguridad perimetral-cortafuegos" ([Ref.- 3]) y "CCN-STIC-432 Seguridad perimetral-IDS" ([Ref.- 8]).

5.3.3.1. ACCESOS REMOTOS

139. Los accesos remotos desde sistemas ajenos a la organización, aunque poco deseables, pueden ser necesarios por motivos de soporte, monitorización o centralización. En estos casos han de garantizarse una serie de medidas mínimas de seguridad, entre las que se encuentran:
    - Acceso controlado y seguro a través de VPN. Se puede encontrar más información sobre este tema en el documento "CCN-STIC-416 Seguridad en VPN" ([Ref.- 5]).
    - Securización y control de los sistemas remotos desde los que se accede. Se puede encontrar más información en el apartado "5.1.5. Empresas Externas". Además existen requisitos para estos accesos en el documento "CCN-STIC-302 Interconexión entre sistemas" ([Ref.- 5]).

5.3.4. SECURIZACIÓN

140. Además de controlar los accesos físicos y electrónicos a los sistemas, ha de garantizarse que éstos han sido desplegados de un modo seguro y tienen el menor número de vulnerabilidades posible.

[1] La definición de Wikipedia de OPC-OLE (*Object-Linking and Embedding*) para el control de procesos. La norma específica la comunicación de datos en tiempo real entre dispositivos de diferentes fabricantes.

141. Una vez se ha identificado una arquitectura de seguridad objetivo, hay que considerar al menos la siguiente lista de comprobación para verificar su completitud.

- Eliminación de todo software y servicio que no sea necesario.
- Mejora de la configuración de los sistemas existentes
- Antivirus y otras herramientas de detección de código dañino
- Controles de acceso: cuentas y contraseñas, altas y bajas. Empleo de mecanismos de autenticación fuerte.
- Monitorización del acceso remoto
- Respuesta a incidentes y alertas
- Gestión continua de la seguridad
- Copias de seguridad y restauración
- Parches o actualizaciones de seguridad

142. Siempre que sea posible, hay intentar utilizar servicios y soluciones de seguridad ya disponibles, como las proporcionadas por el departamento TI. Esto facilitará su despliegue y su mantenimiento, aumentando la seguridad. Las soluciones pueden necesitar ser adaptadas al entorno operativo de los sistemas de control.

143. Las pautas a seguir deben reflejarse en documentos de seguridad que formarán parte de los procedimientos utilizados por el personal implicado en SCADA.

144. En todo momento debe actualizarse el Inventario de los Sistemas SCADA para reflejar el estado de los sistemas.

5.3.4.1. PARCHEADOS

145. La mayoría de los sistemas de control actuales se basan en las tecnologías TI estándar, por lo que corren el riesgo de ser comprometidos o infectados. Suele ser frecuente que los proveedores desarrollen parches para resolver vulnerabilidades conocidas.

146. Por otro lado, al tratarse de entornos sensibles, pueden aparecer reticencias a realizar el parcheado por temor a lo que pueda ocurrir ([Ref.- 26]). La aplicación de parches no está libre de riesgos; existe el riesgo de que el parche pueda causar un funcionamiento incorrecto de un sistema. Un sistema que no está totalmente actualizado, que no mantiene sus antivirus al día y sus aplicaciones no están exentas de fallos conocidos, es un sistema vulnerable. Estas reticencias se pueden solucionar con una serie de sencillas precauciones:

- **Política de parcheado**. Si una organización no se plantea de manera consciente que debe actualizar sus sistemas, es muy posible que no se actualicen, o se actualicen sólo las cosas que sean automáticas. E incluso en este último caso, las actualizaciones automáticas si no se controlan pueden dar lugar a problemas de funcionamiento, compatibilidad y reinicios no programados. Una política de parcheado y actualización de los sistemas aprobada por la dirección debe contemplar:
    - Horarios: En SCADA puede haber sistemas 24x7 sin soporte, y también para ellos debe existir una política de parches.

- Personal.autorizado a la instalación
- Herramientas a utilizar.
- Pruebas previas
- Procedimiento habitual.
- Procedimiento de emergencia.
- Orden de parcheado.
- Procedimiento de regresión en el caso de un fallo derivado de un parcheo.
- Ventana de prueba: tiempo durante el que se mantienen los mecanismos necesarios para ejecutar la regresión.

- **Alerta por parches**. Los actualizadores automáticos, como los de Microsoft, cada vez están mas implantados, pero no cubren todo el software. En estos casos, ¿quién esta al tanto de que no aparezca una nueva vulnerabilidad en la BBDD Oracle o PostreSQL? ¿O en el *plugin* de foros instalado en el portal? Es importante concertar alertas automáticas de los proveedores, y que estas alertas no sea sólo recibidas y almacenadas, sino incorporadas en la monitorización. También se puede suscribir a boletines de vulnerabilidades como los del CCN-CERT.
- **Inventario de sistemas actualizado.** De nuevo, es necesario mantener el inventario de los sistemas y su estado actualizado. Siempre que sea posible, esta actualización debe realizarse automáticamente y a partir de los datos de monitorización.
- **Entornos de alta disponibilidad y de preproducción.** Cuando sea posible, los sistemas deben estar diseñados para facilitar el parcheo, por ejemplo servidores en cluster para garantizar la alta disponibilidad, o existencia de entornos de preproducción. En caso de no existir (lo que debería ser obligatorio en entornos sensibles como SCADA), deben intentar definirse sistemas son menos críticos en un entorno similar.
- **Soporte de proveedores**. Y no sólo de los proveedores de los sistemas a parchear sino de los de todos los sistemas que puedan sufrir efectos colaterales: sistemas que comparten información, aplicaciones instaladas en la misma máquina, etc.

147. En el caso de sistemas que no puedan ser parcheados, es necesario intentar que cualquier vulnerabilidad que contengan tenga el menor impacto posible. Algunas posibles soluciones son:
    - Reemplazarlos o actualizarlos
    - Aislarlos físicamente
    - Reducir sus vulnerabilidades mediante protecciones adicionales (ej., detrás un cortafuegos configurado adecuadamente)
    - Protegerlos con sistemas de prevención de intrusos

5.3.5. MONITORIZACIÓN

148. La monitorización no debe limitarse al estado de los sistemas y las comunicaciones, sino que debe recoger información de cualquier fuente interna y externa donde se pueda

dar cualquier evento relevante como alertas de seguridad, *malware* y notificaciones de vulnerabilidades.

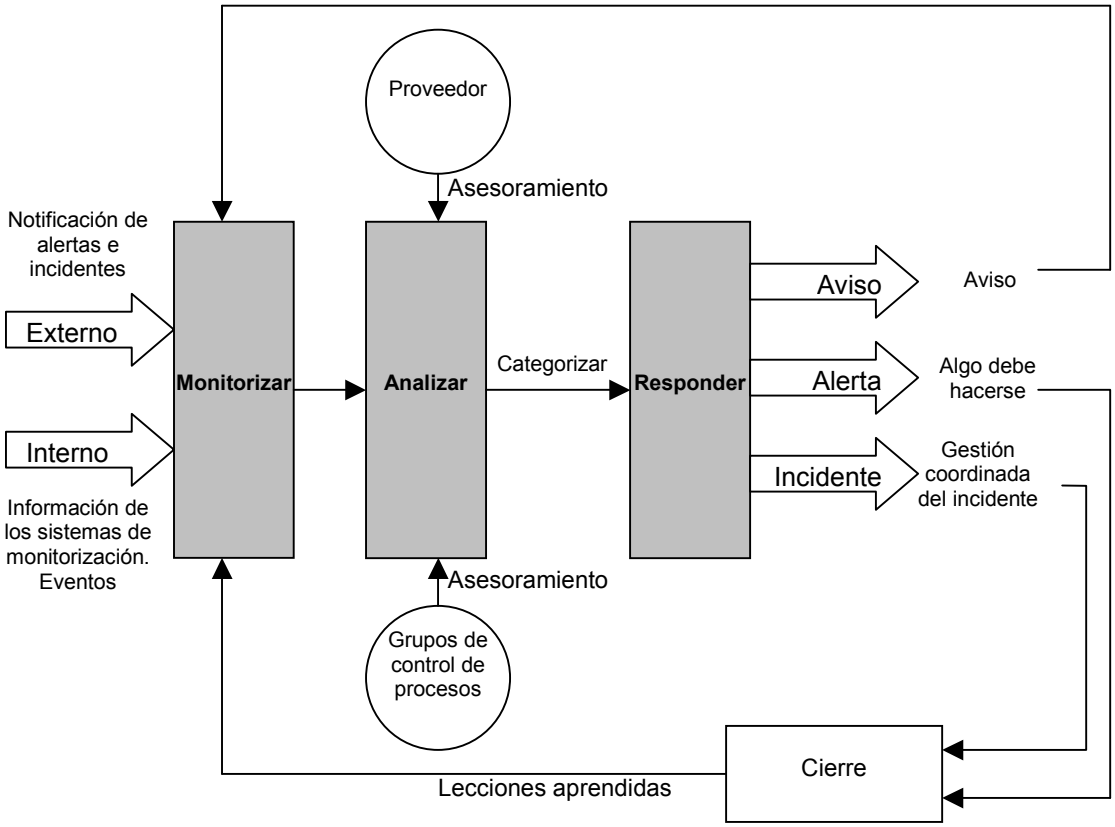


Figura 4: ***Esquema de respuesta de seguridad en el control de procesos***

149. Se necesita un equilibrio entre intentar procesar toda la información disponible, lo que requerirá un gran esfuerzo de recursos, y recoger los datos suficientes para que las alertas o incidentes importantes no sean ignorados.

150. 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:

- Fuentes internas:
    - Sistemas de monitorización de cortafuegos y otros dispositivos de protección de perímetro
    - Sistemas de detección de intrusos
    - Sistemas de monitorización de la red y los sistemas
    - Informes de código dañino activo (virus y *malware)*
    - Informes de fallos de sistema
    - Informes del servicio de atención al usuario
    - Informes de vulnerabilidades para las tecnologías en uso

- Fuentes externas:
  - Informes de equipos de respuesta ante incidentes, por ejemplo CCN-CERT. Actualmente proporciona:
    i. Informes de código dañino activo (virus y *malware)*
    ii. Informes de vulnerabilidades específicas para SCADA
  - Equipos de Seguridad y Atención a Incidentes (CSIRT) ([Ref.- 30])
  - US-CERT ([Ref.- 31])
  - Intercambios de información con el CCN-CERT ([Ref.- 1])
  - 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

151. Es necesario que todas estas fuentes sean procesadas e incorporadas en el plan de alerta temprana que desencadene los correspondientes procedimientos de recuperación.

5.3.6. PROCEDIMIENTOS DE RECUPERACIÓN

152. Los planes de respuesta de seguridad en el control de procesos son a menudo bastante amplios. Deben cubrir todos los casos conocidos, estableciendo la prioridad de cada tipo de riesgo.

153. 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.
- Disponibilidad de copias de seguridad y procedimientos de restauración.
- 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 procedimiento de escalado y los requisitos de autorización necesarios para éste.
- Listas de herramientas de apoyo disponibles
- Prioridades de análisis forense.
- 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.

154. Se puede encontrar más información útil sobre este tema en el documento "CCN-STIC-403 Gestión de incidentes de seguridad" ([Ref.- 2]).

5.3.6.1. ANÁLISIS FORENSE

155. 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.

156. Si teniendo los medios se decide no realizar ningún análisis por seguridad, el riesgo conocido aumenta pues, aun resolviendo la vulnerabilidad, existe una amenaza conocida que no ha sido neutralizada. Compartir la información de incidentes 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.

157. Cualquier organización que ha experimentado incidentes de seguridad en el control de proceso debería compartir esa información (de manera adecuada, por ejemplo anónima) con en CNPIC y el CCN. Toda información será tratada como clasificada, y en caso necesario, convenientemente sanitizada 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 su página web ([Ref.- 1]). La información sensible no debe enviarse sin cifrar, para lo que se puede utilizar la clave pública del certificado disponible en dicha página Web en la sección "Contacto".

6. SOFTWARE SCADA

158. En el mercado existen numerosas empresas y herramientas centradas en el entorno SCADA, entre las que cabe destacar las siguientes:

- Digital Bond ([Ref.- 33])
- ABB Group ([Ref.- 34])
- Lauer ([Ref.- 35])
- Indusoft Web Studio ([Ref.- 36])
- eXpert Manager, de Satec ([Ref.- 37])
- Wonderware HMI/SCADA ([Ref.- 38])
- CitectHMI y CitectSCADA ([Ref.- 39])
- MiSCADA ([Ref.- 40])
- WinMachLite, de Automata ([Ref.- 41])
- PcVue Software SCADA ([Ref.- 42])
- Jako Scada ([Ref.- 43])
- Control Maestro y Wizcon Supervisor, de Elutions ([Ref.- 44])

159. Algunos proveedores de hardware tienen productos específicos de SCADA (como WinMSG de Piciorgros [Ref.- 46]). Estos productos suelen tener funcionalidades específicas pero son más difíciles de integrar en una monitorización centralizada.

160. Ninguna elección es garantía absoluta de seguridad. A la hora de seleccionar un software es recomendable comprobar las certificaciones existentes y garantizar el nivel de soporte adecuado. El CCN, como organismo de certificación, puede asesorar en la decisión:

6.1.1. OTRAS HERRAMIENTAS

161. Consulte las guías de la serie 400 del CCN-STIC y especialmente “CCN-STIC-430 Herramientas de seguridad” ([Ref.- 6]).

162. Para cualquier duda o asesoramiento, póngase en contacto directo con el CCN-CERT.

ANEXO A. REFERENCIAS

[Ref.- 1] Portal de CCN-CERT
https://www.ccn-cert.cni.es

[Ref.- 2] CCN-STIC-403 Gestión de incidentes de seguridad

[Ref.- 3] CCN-STIC-408 Seguridad perimetral – cortafuegos

[Ref.- 4] CCN-STIC-410 Análisis de riesgos en sistemas de la Administración

[Ref.- 5] CCN-STIC-416 Seguridad en VPN

[Ref.- 6] CCN-STIC-430 Herramientas de Seguridad

[Ref.- 7] CCN-STIC-431 Herramientas de Análisis de Vulnerabilidades

[Ref.- 8] CCN-STIC-432 Seguridad perimetral-IDS

[Ref.- 9] CCN-STIC-435 Herramientas de monitorización de tráfico

[Ref.- 10] CCN-STIC-470 Manual Herramienta de Análisis de Riesgos Pilar 4.4

[Ref.- 11] CCN-STIC-480A Seguridad en el control de procesos y SCADA
Guía de buenas prácticas

[Ref.- 12] CCN-STIC-480B Seguridad en el control de procesos y SCADA
Guía 1: Comprender el riesgo del negocio

[Ref.- 13] CCN-STIC-480C Seguridad en el control de procesos y SCADA
Guía 2: Implementar una arquitectura segura

[Ref.- 14] CCN-STIC-480D Seguridad en el control de procesos y SCADA
Guía 3: Establecer capacidades de respuesta

[Ref.- 15] CCN-STIC-480E Seguridad en el control de procesos y SCADA
Guía 4: Mejorar la concienciación y las habilidades

[Ref.- 16] CCN-STIC-480F Seguridad en el control de procesos y SCADA
Guía 5: Gestionar el riesgo de terceros

[Ref.- 17] CCN-STIC-480G Seguridad en el control de procesos y SCADA
Guía 6: Afrontar proyectos

[Ref.- 18] CCN-STIC-480H Seguridad en el control de procesos y SCADA
Guía 7: Establecer una dirección permanente

[Ref.- 19] COM/2004/0702 - Protección de las infraestructuras críticas en la lucha contra el terrorismo
Comisión de la Unisón Europea, junio 2004, adoptada el 20/10/2004
http://europa.eu/scadplus/leg/es/lvb/l33259.htm

[Ref.- 20] COM/2006/786 - Programa europeo para la protección de infraestructuras críticas
Comisión de la Unisón Europea, 12/12/2006
http://europa.eu/scadplus/leg/es/lvb/l33260.htm

[Ref.- 21] Catálogo Nacional de Infraestructuras Críticas

[Ref.- 22] Sugerencias para Mejorar la Seguridad en SCADA
S21Sec, 10/01/2007
www.s21sec.com/descargas/scada.pdf

[Ref.- 23] Steven S. Smith, The SCADA Security Challenge: The Race Is On:
http://www.infosecwriters.com/texts.php?op=display&id=521

[Ref.- 24] Entorno de Análisis de Riesgos
http://www.ar-tools.com

[Ref.- 25] MAGERIT v. 2. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información
Consejo Superior de Administración Electrónica, Ministerio de la Presidencia
http://www.csi.map.es/csi/pg5m20.htm

[Ref.- 26] Los enemigos de los parches
http://www.securityartwork.es/2009/05/29/los-enemigos-de-los-parches/

[Ref.- 27] Una de espías y un trabajo interesante
S21Sec
http://blog.s21sec.com/2009/05/una-de-espias-y-un-trabajo-interesante.html

[Ref.- 28] Electric Gris in U.S. penetrated by spies
Wall Street Journal
http://online.wsj.com/article/SB123914805204099085.html

[Ref.- 29] "Ska! Ska!... Da" Demostración de un exploit sobre un sistema SCADA
Blog 48 bits
http://blog.48bits.com/?p=281

[Ref.- 30] Equipos de Seguridad y Atencion a Incidentes (CSIRTs) españoles
http://www.csirt.es/

[Ref.- 31] US Cert
www.us-cert.gov/control systems/

[Ref.- 32] CCN-STIC-302 Interconexión de sistemas clasificados

A.1. EMPRESAS DESARROLLADORAS DE SOFTWARE SCADA

[Ref.- 33] Digital Bond
www.digitalbond.com

[Ref.- 34] The ABB Group
www.abb.com

[Ref.- 35] Lauer
www.lauer-hmi.de

[Ref.- 36] Indusoft – Tools for automation
www.indusoft.com

[Ref.- 37] Satec Powerful Solutions
www.satec-global.com

[Ref.- 38] Invensis Wolderware
www.wonderware.com

[Ref.- 39] Citect Real Time Intelligence by Schneider Electric
www.citect.com

[Ref.- 40] Iskra Mis
www.iskra-mis.si

[Ref.- 41] Automata
www.automataweb.com

[Ref.- 42] ARC Informatique
www.arcinfo.com

[Ref.- 43] Janus Software
www.ejanus.com.ar

[Ref.- 44] Elutions
www.elutions.com

[Ref.- 45] Dotvision
www.dotvision.com

[Ref.- 46] Piciorgros
www.piciorgros.com

[Ref.- 47] CNPIC
http://www.cnpic-es.es

ANEXO B. GLOSARIO DE TÉRMINOS Y ABREVIATURAS

B.1. GLOSARIO DE TÉRMINOS

Amenaza	Evento que puede desencadenar un incidente en la Organización, produciendo daños materiales o pérdidas inmateriales en sus activos.
Malware	Software o firmware que intenta llevar a cabo procesos no autorizados que pueden tener un impacto en la integridad, confidencialidad o disponibilidad de un sistema informático.

B.2. GLOSARIO DE SIGLAS

CCN	Centro Criptológico Nacional
CPNI	Centro para la Protección de la Infraestructura Nacional de Reino Unido
CSIRTUK	Combined Security Incident Response Team – United Kingdom
ERSCP	Equipo de Respuesta de Seguridad en Control de Procesos
INC	Infraestructura Nacional Crítica
SCADA	Sistema de Control Supervisor y Adquisición de Datos
SCD	Sistemas de Control Distribuido
TI	Tecnología de la Información
CSIRTUK	Combined Security Incident Response Team – United Kingdom Departamento dentro del CPNI que engloba el CERN gubernamental. Para un equivalente español, contactar con el CCN.
PLC	Programmable Logic Controller Controlador Lógico Programable.
UTR	Unidad de Terminal Remota
CD	Compact Disk
USB	Universal Serial Bus
VPN	Virtual Private Network.