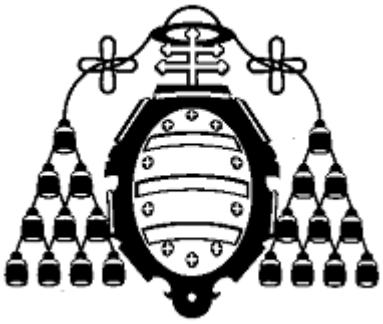


UNIVERSIDAD DE OVIEDO

ESCUELA POLITÉCNICA DE INGENIERÍA DE GIJÓN

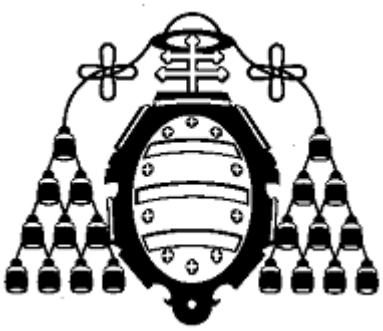
MÁSTER EN INGENIERÍA INFORMÁTICA

TRABAJO FIN DE MÁSTER

SISTEMA DE GESTIÓN DE LA CIBERSEGURIDAD INDUSTRIAL

Pablo Sánchez Fernández

Junio de 2013



UNIVERSIDAD DE OVIEDO

ESCUELA POLITÉCNICA DE INGENIERÍA DE GIJÓN

MÁSTER EN INGENIERÍA INFORMÁTICA

TRABAJO FIN DE MÁSTER

SISTEMA DE GESTIÓN DE LA CIBERSEGURIDAD INDUSTRIAL

DOCUMENTO Nº 1

Pablo Sánchez Fernández

Junio de 2013

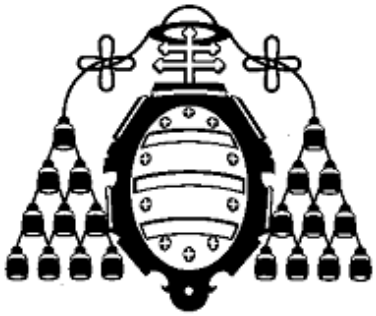
Dpto. de Informática – Área de Arquitectura y Tecnología de Computadores

TUTOR: Daniel F. García

ÍNDICE

LISTADO DE FIGURAS

LISTADO DE TABLAS



UNIVERSIDAD DE OVIEDO

ESCUELA POLITÉCNICA DE INGENIERÍA DE GIJÓN

MÁSTER EN INGENIERÍA INFORMÁTICA

TRABAJO FIN DE MÁSTER

SISTEMA DE GESTIÓN DE LA CIBERSEGURIDAD INDUSTRIAL

-MEMORIA-

Pablo Sánchez Fernández

Junio de 2013

1 INTRODUCCIÓN

Los sistemas de control industrial son sistemas y redes de mando y control diseñados para supervisar y actuar sobre los procesos industriales. Debido a sus características, y al nuevo panorama de interconexión de estos sistemas a las redes corporativas, los sistemas de control industrial se ven expuestos a amenazas no contempladas en el pasado, resultando muy vulnerables, y quedando expuestas a riesgos, que en muchas ocasiones no son analizados, y que pueden suponer serias consecuencias para las actividades y las finanzas de las organizaciones propietarias, y más allá, para el entorno y las personas.

En este nuevo contexto, se hacen necesarias por tanto, nuevas iniciativas de protección sobre los sistemas de control industrial, que consideren sus características y requisitos de actuación, y la integración con el mundo de las tecnologías de la información de las organizaciones.

La existencia de un sistema de gestión de la ciberseguridad industrial, que tenga en cuenta todo lo anterior, puede resultar de gran utilidad para una organización, de manera que pueda servir de guía de protección de sus sistemas de control industrial, durante todo el ciclo de vida. Para desarrollar dicho sistema de gestión, hemos de considerar las nuevas necesidades en materia de seguridad de los sistemas de control industrial, los estándares y guías existentes y las iniciativas en desarrollo, tanto de protección de infraestructuras críticas, como de protección sistemas de control industrial, y de seguridad TIC.

2 OBJETIVOS

El objetivo principal del presente trabajo será el de desarrollar una guía con un enfoque práctico que trate de manera integral, el establecimiento de un Sistema de Gestión de Ciberseguridad Industrial (SGCI, en adelante). Para alcanzar este objetivo principal, establecemos otra serie de objetivos que marcarán los hitos del trabajo a desarrollar y guiarán el enfoque del SGCI. Los objetivos secundarios son:

- Estudiar la problemática que presentan los sistemas de control industrial en el contexto actual de amenazas y vulnerabilidades, y la situación internacional de iniciativas relacionadas con la protección de sistemas de control industrial.
- Contribuir a la creación de documentación en castellano, sobre protección de sistemas de control industrial en general, y sobre un sistema de gestión de la ciberseguridad industrial en particular, ámbitos muy escasos en cuanto a lo que a documentación se refiere.
- Servir de ayuda práctica para organizaciones de cualquier tipo y tamaño, que cuenten con una parte de sistemas de control industrial.
- Guiar al sistema de gestión durante todo el ciclo de vida, dirigiendo a la organización desde la creación y establecimiento del SGSI, pasando por la implementación y operación del mismo, la supervisión y revisión, y el mantenimiento y mejora del SGSI, procurando siempre la mejora contínua del sistema por parte de la organización, mediante.
- Enfocar hacia procesos, considerando los elementos de entrada y salida de cada actividad del sistema de gestión, y el encadenamiento de procesos.

3 ALCANCE

El trabajo consistirá en el desarrollo de una norma para la creación de un sistema de ciberseguridad industrial:

- Siente los elementos básicos a implementar por una organización para la protección de los sistemas ICS, teniendo en cuenta los estándares, guías, etc. relativos a los ICS, IC y sistemas de información.
- Abarque todo el ciclo de vida, creación, etc, etc. (con breve explicación de qué conseguir en cada fase).
- Presente controles implementables por la organización para mitigar los riesgos.

4 RESUMEN DE DOCUMENTOS

El trabajo se estructura en nueve documentos:

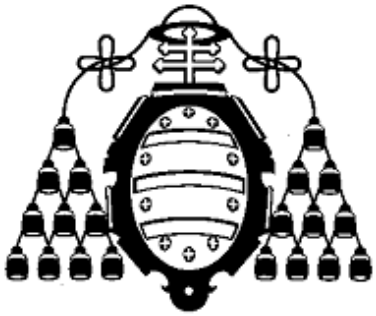
- Memoria. Este documento recoge los aspectos básicos del proyecto, como son los objetivos del mismo y su alcance.
- Términos y acrónimos. Contiene definiciones de términos utilizados en el trabajo y acrónimos.
- Método de trabajo. Expone las bases y los pasos que se emplearán para desarrollar el trabajo.
- Planificación y presupuesto. Este documento detalla la planificación del tiempo y los recursos a utilizar, durante la elaboración del trabajo, y el presupuesto del trabajo, teniendo en cuenta los costes de mano de obra, etc. etc.
- Introducción a la protección de ICS. Presenta el panorama de protección sobre los sistemas de control industrial e infraestructuras críticas, y sus problemáticas.
- Estado del Arte. Recoge las principales iniciativas relacionadas a los ICS así como a las infraestructuras críticas, infraestructuras de información críticas y sistemas de información.
- Sistema de Gestión de la Ciberseguridad Industrial. Este documento es el resultado del trabajo, consistiendo en un marco integral de gestión, dividido a su vez en cuatro partes:
    - Introducción, Términos y acrónimos, Estructura del documento y Sistema de Gestión de la Ciberseguridad Industrial.
    - Anexo A: Controles de seguridad.
    - Anexo B: Lista de documentos del SGCI.
    - Anexo C: Listas de amenazas y vulnerabilidades.
- Resultados y Conclusiones finales. Se presentan las verificaciones efectuadas y las conclusiones extraídas de todo el proceso llevado a cabo para la elaboración del trabajo, incluyendo las ideas y perspectivas de trabajo futuro.
- Bibliografía/Referencias

4.1 Consideraciones

Debido al futuro uso individual, fuera de este trabajo, del documento 'Sistema de Gestión de la Ciberseguridad Industrial', éste ha de tener una numeración de apartados y subapartados independiente. Presentar dicho documento dentro de este trabajo, con sus apartados numerados correlativamente a los demás documentos que componen el trabajo, podría prestarse a confusión cuando el documento fuera consultado de manera aislada fuera del contexto del presente trabajo. Teniendo en cuenta lo anterior, se opta por establecer el siguiente convenio de numeración:

- Cada documento que compone el trabajo, llevará un título numerado correlativamente
- Dentro de cada documento, los apartados, subapartados, tablas y figuras estarán numerados de manera independiente entre documentos, si bien en el caso de las tablas de figuras, en caso necesario se añadirá algún identificador a la numeración, en caso necesario, para clarificar sus índices.
- El número de página será correlativo para todo el trabajo

Además, el documento 'Sistema de Gestión de la Ciberseguridad Industrial', poseerá su propio apartado dedicado a la bibliografía y referencias.



UNIVERSIDAD DE OVIEDO

ESCUELA POLITÉCNICA DE INGENIERÍA DE GIJÓN

MÁSTER EN INGENIERÍA INFORMÁTICA

TRABAJO FIN DE MÁSTER

SISTEMA DE GESTIÓN DE LA CIBERSEGURIDAD INDUSTRIAL

-TÉRMINOS Y ACRÓNIMOS-

Pablo Sánchez Fernández

Junio de 2013

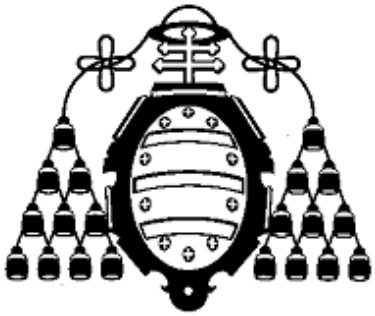
1 TÉRMINOS Y ACRÓNIMOS

Relación de los términos utilizados en el presente trabajo, adoptados de fuentes industriales, de documentación técnica y de guías y estándares.

1. **Acceso remoto**: comunicación o uso de activos o sistemas dentro de un determinado perímetro desde cualquier localización fuera de dicho perímetro.
2. **Activo**: objeto físico o lógico perteneciente o bajo custodia de una organización, que posee un cierto valor real o percibido para la organización.
3. **Ataque**: método por el que un individuo, mediante un sistema informático, intenta tomar el control, desestabilizar o dañar otro sistema informático.
4. **Autenticación**: medida de seguridad diseñada para establecer la validez de una transmisión, mensaje u origen, o los medios para verificar una autorización individual para acceder a categorías específicas de información.
5. **Autorización**: derecho o permiso que es otorgado a una entidad del sistema para acceder a un recurso del sistema.
6. **Backup**: copia de los datos originales que se realiza con el fin de disponer de un medio de recuperarlos en caso de su pérdida.
7. **Bot-net**: conjunto de robots informáticos que se ejecutan de manera autónoma y automática, normalmente de manera inadvertida para sus propietarios, y controlada de manera remota, con el propósito de utilizar los equipos infectados para envío de spam, descarga de ficheros de gran volumen, o realización de ataques de denegación de servicio.
8. **Brecha de seguridad**: acto desde el exterior de la organización que esquiva o contraviene las políticas de seguridad, las prácticas o los procedimientos.
9. **CCN**: acrónimo de Centro Criptológico Nacional.
10. **Ciberseguridad**: es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno.
11. **CIKR**: acrónimo de Critical Infrastructure Key Resources.
12. **CIP**: acrónimo de Critical Infrastructure Protection.
13. **CNPIC**: acrónimo de Centro Nacional para la Protección de Infraestructuras Críticas.
14. **Control**: procedimiento o mecanismo tecnológico que reduce el riesgo
15. **CPNI**: acrónimo de Centre for the Protection of National Infrastructure.
16. **CSMS**: acrónimo de Cyber Security Management System.
17. **Cuenta de acceso**: función de control de acceso que permite a un usuario acceder a un conjunto particular de datos, funciones o cierto equipamiento.
18. **DCS**: acrónimo de Distributed Control System. Sistema de control en el que los elementros que realizan el control no se encuentran en una ubicación centralizada sino distribuidos sobre todo el sistema, donde cada subsistema se encuentra controlado por uno o más controladores.
19. **DHCP**: acrónimo de Dynamic Host Configuration Protocol. Protocolo para la asignación parámetros de red a dispositivos dentro de una red de manera automática.
20. **DNS**: acrónimo de Domain Name System. sistema de nomenclatura jerárquica para computadoras, servicios o cualquier recurso conectado a Internet o a una red privada.
21. **ENISA**: acrónimo de European Network and Information Security Agency.

22. **EPCIP**: acrónimo de European Program for Critical Infrastructure Protection.
23. **Equipamiento ambiental**: infraestructuras y dispositivos destinados a mantener un entorno ambiental controlado.
24. **Firewall**: puerta de enlace entre redes que restringe el tráfico de datos desde y hacia una de las redes conectadas, considerada la interna al firewall, y de dicha forma es capaz de proteger los recursos conectados a la red contra amenazas de la otra red, la considerada externa al firewall.
25. **Framework**: conjunto estandarizado de conceptos, prácticas y criterios para afrontar una problemática particular.
26. **HSE**: acrónimo de Health, Safety, and Environment. Responsabilidad de proteger la salud de los trabajadores y de la comunidad circundante (surrounding), y mantener la gestión ambiental.
27. **IACS**: acrónimo de Industrial Automation and Control Systems.
28. **ICE**: acrónimo de Infraestructura Crítica Europea.
29. **ICN**: acrónimo de Infraestructura Crítica Nacional.
30. **ICS**: acrónimo de Industrial Control System.Sistemas de control industrrial, abarcando varios tipos de sistemas de control, incluyendo sistemas SCADA, sistemas DCS y otras configuraciones basadas en PLCs.
31. **IDS**: acrónimo de Intrusion Detection System. Servicio de seguridad que monitoriza y analiza los eventos de la red o el sistema con el propósito de encontrar y proporcionar avisos en tiempo real, o casi, sobre los intentos de acceso a recursos no autorizados.
32. **IED**: acrónimo de Intelligent Electronic Device. Dispositivo electrónico multifunción que presenta algún tipo de inteligencia local.
33. **Incidente**: evento que no es parte de la operación que se espera de un sistema o servicio, que causa o puede causar una interrupción o una reducción en la calidad del servicio proporcionada por el sistema.
34. **IPS**: acrónimo de Intrusion Protection System. Sistema que puede detectar actividades de intrusión y es capaz de detener la actividad, idealmente antes de que dicha actividad alcance su objetivo.
35. **ISA**: acrónimo de International Society of Automation.
36. **ISO**: acrónimo de International Organization for Standardization.
37. **IT**: acrónimo de Information Technologies.
38. **ITU**: acrónimo de International Telecommunications Union.
39. **Log**: registro oficial de eventos durante un rango de tiempo en particular.
40. **LPIC**: acrónimo de de Protección de Infraestructuras Críticas.
41. **Malware**: software que tiene como objetivo infiltrarse o dañar una computadora o Sistema de información sin el consentimiento de su propietario.
42. **Man-in-the-middle**: ataque en el que el adversario adquiere la capacidad de leer y modificar los mensajes entre dos comunicantes sin que estas se percaten de dicha violación de la seguridad.
43. **NAT**: acrónimo de Network Address Translation. Mecanismo utilizado por dispositivos de red para el intercambio de paquetes entre dos redes, convirtiendo en tiempo real, las direcciones utilizadas en los paquetes transportados.
44. **NERC**: acrónimo de North American Electric Reliability Corporation.
45. **NIPP**: acrónimo de National Infrastructure Protection Plan.

46. **NIST**: acrónimo de National Institute of Standards and Technology.
47. **Norma**: regla que se debe seguir o a que se deben ajustar las conductas, tareas, actividades, etc.
48. **Parche**: pieza de software diseñada para solventar problemas mediante el cambio o actualización de un programa o sus datos de soporte, incluyendo la solución de vulnerabilidades de seguridad y otros fallos, y la mejora de la usabilidad y el rendimiento.
49. **Phishing**: envío de mensajes electrónicos que, aparentando provenir de fuentes fiables , intentan obtener datos confidenciales del usuario,con el ánimo de ser usados posteriormente en algún tipo de fraude.
50. **PIC**: acrónimo de Protección de Infraestructuras Críticas.
51. **PIIC**: acrónimo de Protección de Infraestructuras de Información Críticas.
52. **PLC**: acrónimo de Programmable Logic Controller. Dispositivo programable basado en microprocesador usado en la industria para controlar líneas de ensamblaje, maquinaria y otros tipos de equipamiento mecánico, eléctrico y electrónico de planta.
53. **PSM**: acrónimo de Process Safety Management. Gestión de la seguridad de los procesos en relación a la liberación accidental de líquidos y gases en procesos en los que estén implicados productos químicos o biológicos peligrosos.
54. **Resiliencia**: capacidad humana de asumir con flexibilidad situaciones límite y sobreponerse a ellas.
55. **RTU**: acrónimo de Remote Terminal Unit. Dispositivo basado en microprocesador que sirve de interfaz entre objetos del mundo físico y un sistema de control mediante la transmisión de datos de telemetría.
56. **SCADA**: acrónimo de Supervisory Control And Data Acquisition. Tecnología que permite al usuario recolectar datos de una o más instalaciones y/o enviar un conjunto limitado de instrucciones hacia ellas.
57. **SGCI**: acrónimo de Sistema de Gestión de la Ciberseguridad Industrial
58. **SGSI**: acrónimo de Sistema de Gestión de la Seguridad de la Información.
59. **SI**: acrónimo de Seguridad de la Información.
60. **SO:** acrónimo de Sistema Operativo. Programa o conjunto de programas que en un sistema informático gestiona los recursos de hardware y provee servicios a los programas de aplicación, ejecutándose en modo privilegiado respecto de los restantes.
61. **Spamming**: abuso de cualquier tipo de sistema de mensajería electrónica
62. **Spyware**: software que recopila información de un ordenador y después transmite esta información a una entidad externa sin el conocimiento o el consentimiento del propietario del ordenador.
63. **TI**: acrónimo de Tecnologías de la Información.
64. **TISN**: acrónimo de Trusted Information Shared Network.
65. **VLAN**: Virtual Local Area Network. Grupo de dispositivos en una o más LANs que son configurados de tal manera que se pueden comunicar como si estuvieran conectados al mismo cable, cuando en realidad están localizados en un segmento diferente de LAN
66. **VPN**: Virtual Private Network. Una red privada virtual o VPN, es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada, como por ejemplo Internet.



UNIVERSIDAD DE OVIEDO

ESCUELA POLITÉCNICA DE INGENIERÍA DE GIJÓN

MÁSTER EN INGENIERÍA INFORMÁTICA

TRABAJO FIN DE MÁSTER

SISTEMA DE GESTIÓN DE LA CIBERSEGURIDAD INDUSTRIAL

-MÉTODO DE TRABAJO-

Pablo Sánchez Fernández

Junio de 2013

1 MÉTODO DE TRABAJO

La consecución de los objetivos del presente trabajo, se fundamentará en cuatro fases: la investigación, la adecuación y adaptación de información, la identificación de necesidades y la definición de nuevas soluciones.

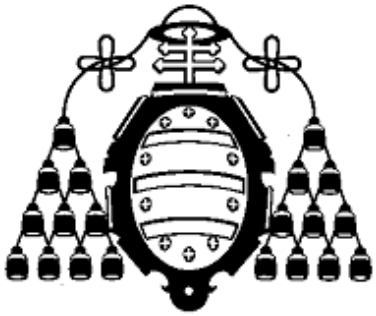
Mediante la investigación, se recopilará la información necesaria sobre sistemas de control industrial, infraestructuras críticas, iniciativas de seguridad y protección relacionadas, y el contexto actual en el que conviven las amenazas, vulnerabilidades y dichas iniciativas, extrayendo aquella información que será relevante o que será utilizada para la elaboración del trabajo.

La adecuación y adaptación de la información recopilada, tras la selección de la información que será utilizada para elaborar la norma, consistirá en la traducción, realización de cambios de redacción, la agregación o separación de apartados de otras documentaciones etc. necesarios para alinear la información existente con el objetivo del trabajo.

Mediante la identificación de necesidades, se tratará de reconocer aquellos aspectos mejorables o que no están definidos por las fuentes consultadas hasta el momento.

La definición de nuevas soluciones, consistirá en proponer nuevas medidas, actualizar las existentes al nuevo contexto, añadir nueva información etc. para tratar de mejorar o completar las carencias encontradas.

Todo este proceso se apoyará en la documentación publicada sobre el ámbito del trabajo, en diferentes medios y formatos, y en el conocimiento de expertos de la materia, mediante la presentación ante ellos de los resultados de cada fase para su revisión, y la realización de reuniones para indicar cambios, sugerencias y guiar en la dirección correcta del trabajo.



UNIVERSIDAD DE OVIEDO

ESCUELA POLITÉCNICA DE INGENIERÍA DE GIJÓN

MÁSTER EN INGENIERÍA INFORMÁTICA

TRABAJO FIN DE MÁSTER

SISTEMA DE GESTIÓN DE LA CIBERSEGURIDAD INDUSTRIAL

-PLANIFICACIÓN Y PRESUPUESTO-

Pablo Sánchez Fernández

Junio de 2013

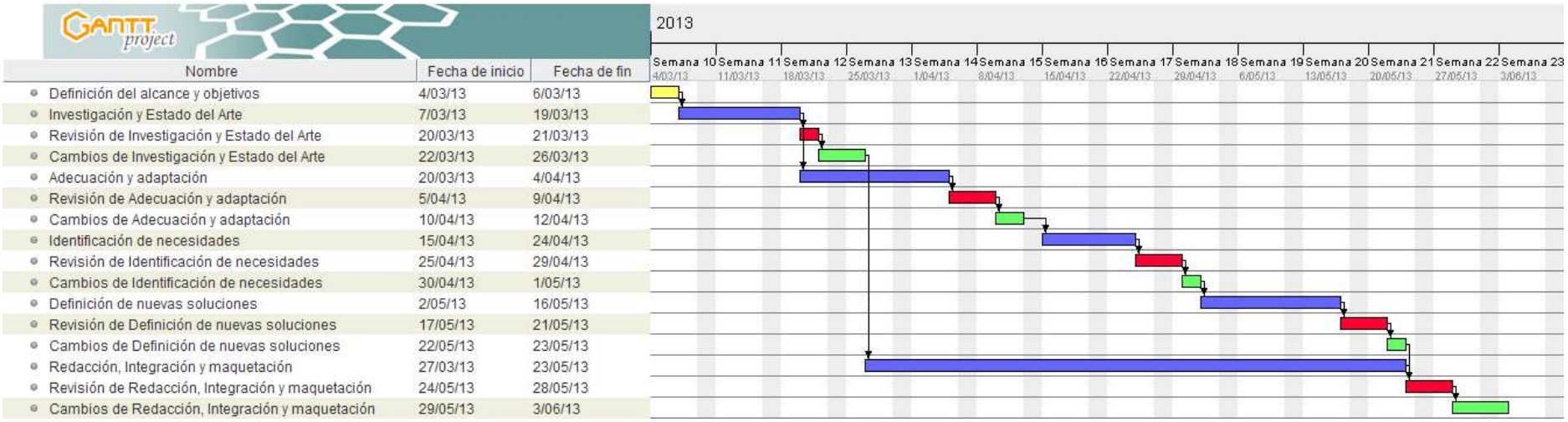
1 PLANIFICACIÓN

La planificación se basa en las cuatro fases planteadas en el método de trabajo (investigación, adecuación y adaptación de información, identificación de necesidades y definición de nuevas soluciones). Además, se incluyen otras dos etapas, como son la de Definición del alcance y objetivos, y la Redacción, Integración y maquetación.

Cada una de las etapas estará compuesta por varias tareas, de desarrollo, de revisión (por parte de los tutores del trabajo y los expertos en la materia), y de cambio.

La planificación temporal está comprendida entre el 4/03/2013 y el 3/06/2013, y puede verse en la figura PP.1.

Figura PP.1. Planificación temporal de tareas



Nombre	Fecha de inicio	Fecha de fin
Definición del alcance y objetivos	4/03/13	6/03/13
Investigación y Estado del Arte	7/03/13	19/03/13
Revisión de Investigación y Estado del Arte	20/03/13	21/03/13
Cambios de Investigación y Estado del Arte	22/03/13	26/03/13
Adecuación y adaptación	20/03/13	4/04/13
Revisión de Adecuación y adaptación	5/04/13	9/04/13
Cambios de Adecuación y adaptación	10/04/13	12/04/13
Identificación de necesidades	15/04/13	24/04/13
Revisión de Identificación de necesidades	25/04/13	29/04/13
Cambios de Identificación de necesidades	30/04/13	1/05/13
Definición de nuevas soluciones	2/05/13	16/05/13
Revisión de Definición de nuevas soluciones	17/05/13	21/05/13
Cambios de Definición de nuevas soluciones	22/05/13	23/05/13
Redacción, Integración y maquetación	27/03/13	23/05/13
Revisión de Redacción, Integración y maquetación	24/05/13	28/05/13
Cambios de Redacción, Integración y maquetación	29/05/13	3/06/13

2 PRESUPUESTO

Para la elaboración del presupuesto únicamente consideraremos la mano de obra, puesto que se necesitarán materiales, ni licencias de documentación o software adicionales.

2.1 Mediciones

Tabla PP.1. Mediciones de mano de obra

Concepto	Unidades	Cantidad
Investigación y desarrollo	Horas	362
Revisión y dirección	Horas	36

En la tabla PP.1 se refleja la cantidad de horas a emplear, calculadas a partir de la planificación, haciendo una estimación de la cantidad de horas necesarias para el desarrollo de cada tarea. Los conceptos que presenta la tabla son:

- Investigación y desarrollo, que incluye los aspectos de recopilación y adaptación de información, y desarrollo del trabajo mediante la identificación de necesidades, la definición de nuevas soluciones, y la redacción, integración y maquetación del trabajo, por parte del investigador.
- Revisión y dirección, que incluye las tareas de verificación e identificación de deficiencias, mejoras y orientación sobre el trabajo, por parte del tutor/consultor.

2.2 Precios

Tabla PP.2. Precios de mano de obra

Concepto	Unidades	Precio/Unidad
Investigación y desarrollo	Horas	80€
Revisión y dirección	Horas	120€

2.3 Presupuesto de Mano de obra

Tabla PP.3. Presupuesto de mano de obra

Concepto	Mediciones	Precio/Unidad	Importe
Investigación y desarrollo	423	80€	33840€
Revisión y dirección	36	120€	4320€
TOTAL			38160€

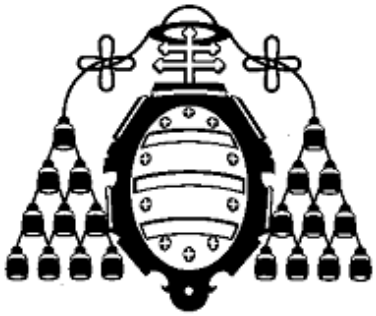
2.4 Presupuesto Total

Tabla PP.4. Presupuesto total

Concepto	Euros
Mano de obra	38160€

Presupuesto de Ejecución Material	**38160€**
Gastos generales (13%)	4960,80€
Beneficio industrial (6%)	2289,60€
Presupuesto de Contrata	**45410,40€**
IVA (21%)	9536,18€
Presupuesto de Ejecución por Contrata	**54946,58€**

Asciende el Presupuesto de Ejecución por Contrata a la cantidad de cincuenta y cuatro mil novecientos cuarenta y seis euros con cincuenta y ocho céntimos (#54946,58€#).



UNIVERSIDAD DE OVIEDO

ESCUELA POLITÉCNICA DE INGENIERÍA DE GIJÓN

MÁSTER EN INGENIERÍA INFORMÁTICA

TRABAJO FIN DE MÁSTER

SISTEMA DE GESTIÓN DE LA CIBERSEGURIDAD INDUSTRIAL

-INTRODUCCIÓN A LA PROTECCIÓN DE ICS-

Pablo Sánchez Fernández

Junio de 2013

1 INTRODUCCIÓN

Los sistemas de control industrial (*Industrial Control Systems*, ICS, en adelante) son sistemas y redes de mando y control diseñados para supervisar y actuar sobre los procesos industriales. Debido a sus características, y al nuevo panorama de interconexión de estos sistemas a las redes corporativas, los sistemas de control industrial se ven expuestos a amenazas no contempladas en el pasado, resultando muy vulnerables, y quedando expuestas a riesgos, que en muchas ocasiones no son analizados, y que pueden suponer serias consecuencias para las actividades y las finanzas de las organizaciones propietarias, y más allá, para el entorno y las personas.

En este nuevo contexto, se hacen necesarias por tanto, nuevas iniciativas de protección sobre los sistemas de control industrial, que consideren sus características y requisitos de actuación, y la integración con el mundo de las tecnologías de la información de las organizaciones.

Durante la última década aproximadamente, han aparecido iniciativas, sobre todo de carácter nacional, que ahora conscientes de los nuevos peligros, tratan de afrontar esta situación, ocupándose primeramente de aquellas infraestructuras de importancia vital para la economía, la salud y la seguridad en general, debido al alto grado de desprotección , que se puso de manifiesto con la ejecución de diferentes ataques sobre infraestructuras críticas, pero sobre todo, con los atentados terroristas de las Torres Gemelas.

Estas iniciativas de protección sobre infraestructuras críticas se diferencian de las iniciativas de protección de sistemas industriales en que el centro de sus esfuerzos son, no sólo los sistemas de control industrial, que suelen estar en la base de actividad de dichas infraestructuras, sino que además, incluyen la protección de los activos de distinta naturaleza, necesarios para el funcionamiento de las infraestructuras. Además, las iniciativas de protección o seguridad sobre sistemas de control industrial, no están restringidos solamente a aquellos sistemas críticos, sino a cualquier sistema industrial. Sin embargo, pese a sus diferencias, presentan un buen punto de partida, para que las organizaciones apliquen las nuevas normativas, estándares y recomendaciones surgidas en dicho ámbito a sus sistemas de control industrial.

Por otra parte, encontramos las estándares y guías de seguridad TIC, que debemos tener en cuenta al desarrollar una iniciativa de seguridad para sistemas de control industrial, ya que como apuntábamos, actualmente, la integración del mundo industrial y el TIC es cada vez más alta y gran parte de los nuevos problemas a los que se enfrentan ahora los sistemas de control industrial, ya han sido previamente estudiados por las iniciativas de seguridad TIC.

La existencia de un sistema de gestión de la ciberseguridad industrial, que tenga en cuenta todo lo anterior, puede resultar de gran utilidad para una organización, de manera que pueda servir de guía de protección de sus sistemas de control industrial, durante todo el ciclo de vida. Para desarrollar dicho sistema de gestión, hemos de considerar las nuevas necesidades en materia de seguridad de los sistemas de control industrial, los estándares y guías existentes y las iniciativas en desarrollo, tanto de protección de infraestructuras críticas, como de protección sistemas de control industrial, y de seguridad TIC.

2 INFRAESTRUCTURAS CRÍTICAS Y SU PROTECCIÓN

2.1 Infraestructuras Críticas

El término "infraestructura crítica" es usado normalmente por los gobiernos, para describir el conjunto de activos, sistemas, y redes, sean físicas o virtuales, que resultan vitales para un país, dado que su incapacitación o destrucción debilitarían la seguridad económica nacional, la salud pública, la seguridad en general, o una combinación de ellas. Las infraestructuras críticas se consideran por tanto, la columna vertebral de la economía, seguridad y salud de una nación.

Los sectores considerados que incluyen infraestructuras críticas varían según la iniciativa (ver Estado del Arte, apartados 1.2 y 1.4.4), pero a modo de ejemplo, suelen incluirse instalaciones de [27]:

- Suministro de agua, electricidad y combustible
- Sistemas de transporte y comunicación
- Gestión de residuos y suministro de alimentación
- Finanzas
- Redes de información y telecomunicaciones
- Sistemas de defensa y militares
- Servicios de emergencia, de salud y rescate
- Agencias publicas y administración
- Principales centros de investigación y medios de comunicación

En el apartado de España, la ley de 2011 por la que se establecen las medidas sobre las IC [37], hace un grado de distinción entre lo que denomina infraestructuras estratégicas, y las infraestructuras críticas. Las primeras las define como las instalaciones, redes, sistemas y equipos físicos y de tecnología de la información sobre las que descansa el funcionamiento de los servicios esenciales. Mediante la definición de las infraestructuras críticas, restringe aún más el ámbito, declarando que son aquellas infraestructuras estratégicas cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales.

2.1.1 Infraestructuras de Información Críticas

Se consideran "infraestructuras de información críticas" (IICs en adelante) a los servicios, redes, funciones y sistemas de información físicos o virtuales que controlan, procesan, transmiten, reciben o almacenan información electrónica en cualquier forma, y que son vitales para el funcionamiento de una infraestructura crítica.

Las IIC incluyen la red telefónica, Internet, y las redes terrestres y vía satélite, ya que la interrupción de sus servicios o su destrucción desembocaría en serio impacto para las funciones vitales de una IC.

Desde las diferentes iniciativas de protección de IICs, se hace referencia a las mismas de varias maneras, como recoge un informe desarrollado por OECD sobre el desarrollo de políticas para la protección de IICs [51]:

- *Information components supporting the critical infrastructure.* (Componentes de información que dan soporte a la infraestructura crítica).
- *Information infrastructures supporting essential components of government business.* (Estructuras de información que dan soporte a los componentes esenciales de los asuntos gubernamentales).

- *Information infrastructures essential to the national economy*. (Infraestructuras de información esenciales para la economía nacional).

Este concepto ha cobrado importancia en los últimos años, dado el carácter transversal de las infraestructuras de información en la actualidad para todos los sectores, siendo parte imprescindible hoy en día para el funcionamiento de las infraestructuras críticas.

2.2 Protección de Infraestructuras Críticas

El concepto de "protección de infraestructuras críticas" (PIC en adelante) se refiere a la preparación y capacidad de respuesta de una región o nación ante amenazas e incidentes que pongan en riesgo la seguridad de las infraestructuras críticas.

La preocupación por la seguridad de estas infraestructuras ha estado presente durante toda la historia de la humanidad, sin embargo no es hasta finales del siglo XX cuando comienza a tratarse el asunto de la protección de tales infraestructuras de manera explícita.

2.2.1 Protección de Infraestructuras de Información Críticas

La Protección de Infraestructuras de Información Críticas (PIIC en adelante) es un subconjunto de los esfuerzos de protección sobre ICs, centrándose en medidas para asegurar las infraestructuras de información que resultan vitales.

Además de los posibles impactos físicos, como los desastres naturales, las IICs pueden resultar vulnerables a otras eventualidades no físicas [25]; un aumento repentino de la demanda puede provocar una caída de sistemas, llevando a pérdidas o denegación de servicio. Otros escenarios similares pueden ocurrir a través de la acción humana, de manera accidental o deliberada.

Las IICs se han convertido en especialmente vulnerables a atacantes, con diferentes motivaciones. El método más común para atacar sistemas críticos es mediante malware, que modifica o destruye información o bloquea los sistemas informáticos. Otros métodos para espiar el intercambio de información en una red informática, así como modificación del funcionamiento normal de la red, o el bloqueo de acceso a sus propios servicios, también son comúnmente utilizados con propósitos maliciosos [28].

La siguiente lista presenta, ordenados por orden creciente de impacto (y decreciente en cuanto a probabilidad de ocurrencia), los tipos de ciberconflictos que puede sufrir una IIC [26]:

- **Hacktivismo**: combinación de hacking y activismo, incluye operaciones que usan técnicas de hacking contra el sitio de internet del objetivo con la intención de provocar una interrupción de las operaciones.
- **Cibercrimen**: actividades criminales usando ordenadores e internet.
- **Ciberespionaje**: el sondeo no autorizado para comprobar la configuración de un ordenador objetivo o evaluar las defensas del sistema o el acceso y copia de archivos de datos no autorizados.
- **Cibersabotaje**: la perturbación deliberada de un proceso económico o militar para conseguir un objetivo particular (normalmente político), con medios cibernéticos.
- **Ciberterrorismo**: ataques inmorales contra ordenadores, redes y la información almacenada en ellos, para intimidar o coaccionar a un gobierno o su población, en fomento de sus objetivos políticos o sociales. Tales ataques pueden resultar en violencia contra las personas o las propiedades, o al menos causar suficientes daños como para generar el nivel suficiente de temor para ser considerado 'ciberterrorismo'.
- **Ciberguerra**: El uso de ordenadores para afectar a las actividades de un país enemigo, especialmente, ataques deliberados sobre sistemas de comunicación.

En los citados ciberconflictos, para la consecución de sus objetivos, los atacantes pueden hacer uso de los siguientes tipos de malware y modos de ataque [26]:

- **Exploit**: hacer uso de la vulnerabilidad de ordenadores u otros dispositivos para causar un comportamiento del sistema no deseado o imprevisto. Esto incluye tomar el control del sistema de un ordenador.
- **Virus/gusanos**: programas de ordenador que se replican mediante copias funcionales de sí mismos y con variedad de efectos, desde simples molestias e inconvenientes hasta el compromiso de la confidencialidad o la integridad de la información. Mientras los virus necesitan de la existencia de algún programa adjunto, los gusanos no.
- **Spyware**: malware que recopila información sobre los usuarios sin su conocimiento.
- **Troyano**: programa malicioso que actúa de manera automática. Pueden hacer copias de sí mismos, robar información, dañar los sistemas huésped, o permitir a un hacer el acceso remoto hacia el sistema.
- **Ataque DDoS**: intento de hacer que un ordenador o un recurso de red resulten no disponibles para los usuarios a los que está destinado, normalmente mediante la saturación de la máquina objetivo con peticiones externas, de manera que no sea capaz de responder al tráfico legítimo, o responda de manera tan lenta que resulte prácticamente no disponible.
- **Amenazas Persistentes Avanzadas**: (Advanced Persistent Threats, APTs) es una categoría de ciberataques en sí misma, que conlleva un ataque con un alto grado de sofisticación y sigilo durante un largo período de tiempo. Sus objetivos típicamente se extienden más allá de la ganancia financiera inmediata.
- **Bot-net**: una colección de ordenadores comprometidos conectados a internet, ejecutando un programa de manera oculta y que pueden ser explotados para su uso posterior por la persona que los controla remotamente.

Las posibles consecuencias de un ciberataque hacia una IIC pueden resultar en bloqueos del transporte, del suministro de agua y electricidad, cortes de comunicaciones, fallos de transacciones financieras, pérdida o robo de dinero e información, pérdida de reputación o de propiedad intelectual, víctimas humanas, pérdidas materiales, etc. [28].

Actualmente, los estudios sobre la materia, y las iniciativas sobre PIC, tienden a tratar este apartado de una manera separada, debido a la gran presencia dentro de las IC, su importancia para el funcionamiento de estas últimas, y sus características comunes descritas anteriormente.

La Protección de Infraestructuras Críticas tiene unas características y unos objetivos a nivel estratégico concretos, que son, prevenir las IICs de ciberataques, reducir sus vulnerabilidades y minimizar el daño y el tiempo de respuesta frente a ciberataques [27].

Dentro de este campo, se proponen soluciones a diferentes niveles, incluyendo guías de buenas prácticas, estándares y listas de controles de carácter técnico, organizacional o de gestión. La PIIC, así como la PIC, con sus objetivos y requisitos específicos, están sin embargo relacionadas con la protección de sistemas de control industrial.

2.3 Antecedentes

La primera nación en abordar la protección de infraestructuras críticas fue EE.UU. que ya en 1995 hace mención, mediante una directiva [56], a la protección frente a ataques terroristas. Tres años más tarde, mediante otras directivas, se hablaría ya explícitamente de ciberprotección y CIP. En 2001 se produce el atentado contra las Torres Gemelas en N.Y., acontecimiento que marcará un antes y un después en el ámbito de la seguridad nacional; el ataque puso de manifiesto graves fisuras de seguridad, y la posibilidad de que sean aprovechadas para dañar de forma irreparable a un país.

En una revisión cronológica sobre los principales ciberataques, se observa que éstos van a la par que las iniciativas de protección. En los años 80, cabe destacar la introducción de un troyano para sabotear la red de tuberías de gas natural de la antigua URSS en 1982. Es a partir de los años 90 cuando comienza a considerarse la protección más seriamente; a finales de dicha década aparecen los primeros problemas de seguridad en sistemas SCADA, antes aislados, y ahora conectados a la red de redes. Ya en el año 2000, una planta de aguas residuales en Australia experimenta un ataque interno, por parte de un ex-empleado que realiza un ciberataque de forma inalámbrica, liberando gran cantidad de aguas residuales. En 2003, la central nuclear de Davi-Besse, en Ohio, EE.UU. [53] se ve afectada por el gusano *Slammer*, inhabilitando durante horas sus sistemas de monitorización de seguridad. Durante la segunda mitad de la década, se suceden diferentes vulnerabilidades en sistemas SCADA, que se comienzan a distribuir de manera libre a través de internet. En 2010 se detecta el gusano *Stuxnet*, con gran repercusión mediática; es el primer gusano capaz de reprogramar sistemas industriales, y cuya consecuencia más grave fueron los problemas surgidos en plantas nucleares iraníes. Posteriormente, el troyano *Duqu*, al que se relaciona con *Stuxnet*, de una complejidad nunca vista, y capaz de recopilar gran cantidad de información privada en entornos industriales. Estos ataques, cada vez más sofisticados, y afectando a infraestructuras críticas, ponen de manifiesto su capacidad para alterar la seguridad de una nación.

3 SISTEMAS DE CONTROL INDUSTRIAL Y SU PROTECCIÓN

3.1 Sistemas de Control Industrial

En el ámbito de los sistemas industriales, nos encontramos los Sistemas de Control Industrial (SCI en lo sucesivo), que son redes y sistemas de comando y control, diseñadas para dar soporte a los procesos industriales [24]. Dentro de los ICS, el mayor subgrupo lo forman los sistemas SCADA (*Supervisory Control And Data Acquisition*) pero también se engloban los Sistemas de Control Distribuido (DCS, por su acrónimo en inglés) y otras arquitecturas, como las basadas en PLCs. Los sistemas industriales son la base de las principales infraestructuras críticas, por tanto, la seguridad de éstas últimas recae sobre dichos sistemas.

En los últimos años, los ICS han sufrido una transformación; de sistemas propietarios aislados, a arquitecturas abiertas y tecnologías estándar altamente interconectadas con otras redes corporativas e internet.

Hoy en día, los productos que componen un ICS están basados principalmente en plataformas de sistemas estándar embebidos, aplicados en multitud de dispositivos, como routers o cable módems, y que usualmente emplean software comercial. Debido a la interconexión de los ICS, se ha visto altamente incrementada la vulnerabilidad de los sistemas industriales ante ataques informáticos de red.

Los ICS tienen una serie de características y requisitos que deberán tenerse en cuenta a la hora de diseñar cualquier política o guía de protección:

- **Sistemas heterogéneos**: son sistemas con multitud de tecnologías integradas, y de diferentes antigüedades, y donde confluyen el mundo industrial y el mundo TIC.
- **Robustez y fiabilidad**: son dos asuntos totalmente prioritarios, debido a los entornos en los que funcionan, por ello, estos sistemas están probados en condiciones como las de funcionamiento o peores, y certificados antes de su lanzamiento al mercado, por tanto, las actualizaciones o parches son materia delicada en estos sistemas.
- **Tiempo real**: los sistemas de control industrial, acometen acciones de control de manera continua en un rango de tiempo muy limitado. Para conseguir la ejecución dentro de un margen tan reducido de tiempo, se elimina todo aquello que no sea imprescindible, por tanto, añadir medidas de seguridad podría suponer el no cumplimiento de estas restricciones temporales.
- **Inexistencia de entornos de prueba**: no existen sistemas de respaldo o backup, y la imposibilidad de disponer de réplicas de los entornos para ejecutar pruebas, ralentiza en gran medida el desarrollo de la seguridad en el ámbito industrial.
- **Duración del ciclo de vida del equipamiento**: el ciclo de vida del equipamiento industrial, al contrario que en las TIC, es mucho más largo, incluso de décadas, por lo que en las instalaciones industriales suelen encontrarse sistemas heredados que no tienen en cuenta los requerimientos de seguridad actuales, y que además, deben seguir funcionando durante mucho tiempo.

Los ICS constituyen un activo estratégico contra el creciente potencial de catastróficos ataques terroristas que afectan a infraestructuras críticas [15].

3.2 Protección de Sistemas de Control Industrial

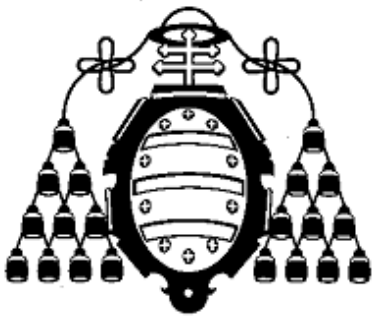
Parte fundamental de la PIC es la seguridad en Sistemas de Control Industrial (SCI en adelante), que se trata de un subconjunto dentro de la protección de infraestructuras de información críticas (PIIC), dado que los sistemas SCI, que incluyen sistemas SCADA, sistemas de control distribuido (DCS por su acrónimo en inglés) y otras configuraciones de sistema como las basadas en PLCs, constituyen la capa básica de la mayoría de infraestructuras críticas. Los SCI son usados típicamente en industrias

como las eléctricas, las relacionadas con distribución y tratamiento de aguas, industria petrolífera y de gas natural, transportes, industria química, farmacéutica, entre otras [50]. Por tanto, los ICS son vitales para la operación de las infraestructuras críticas, que habitualmente se encuentran altamente interconectadas y se trata de sistemas dependientes.

Inicialmente, los ICS constituían sistemas aislados, que se ejecutaban sobre protocolos propietarios, usando hardware y software especializado [50]. En la actualidad, los dispositivos basados en el Protocolo de Internet (IP), de bajo coste, y ampliamente disponibles en el mercado, están reemplazando las antiguas soluciones propietarias, lo cual incrementa la posibilidad de vulnerabilidades e incidentes de ciberseguridad. Los ICS están adoptando por tanto, arquitecturas, protocolos, sistemas operativos, y hardware propios de sistemas IT. Esta integración provee a la industria de nuevas capacidades, pero también conlleva una disminución del aislamiento de los sistemas y el entorno exterior, creando nuevas necesidades en cuanto a soluciones de seguridad para estos sistemas.

Aunque algunas características son similares, ya que los ICS están incorporando soluciones IT, como sistemas operativos o protocolos de red, existen muchas diferencias entre los ICS y los sistemas de procesamiento de información tradicionales, incluyendo diferentes riesgos y prioridades; la principal diferencia reside en que los ICS tienen un efecto directo en el mundo físico, lo que incluye riesgos significativos para la salud y la seguridad de las personas, daños al entorno, así como posibles problemas financieros, en forma de pérdidas de producción, impactos negativos en la economía nacional y el compromiso de información propietaria [50].

Los objetivos de los ICS, rendimiento y confiabilidad, a menudo entran en conflicto con los requisitos de seguridad, tanto en la etapa de diseño como de operación. Originalmente, las implementaciones de ICS estaban expuestas a amenazas locales, dado el aislamiento de sus componentes, que residían en áreas físicamente seguras, y no conectados a sistemas o redes de TI. Sin embargo, la tendencia hacia la integración de los sistemas ICS con las redes TI, expone a estos sistemas a amenazas externas. Además, el creciente uso de redes inalámbricas para comunicar ICS los exponen a un mayor riesgo, de adversarios que puedan encontrarse relativamente cerca, pero sin acceso físico directo al equipamiento. Las amenazas sobre los sistemas de control pueden provenir de numerosas fuentes, incluyendo gobiernos hostiles, grupos terroristas, empleados descontentos, intrusos con intenciones maliciosas, accidentes, desastres naturales o acciones accidentales por parte de personal de la organización. Los objetivos de seguridad de los ICS típicamente persiguen la disponibilidad, integridad y confidencialidad, por ese orden.



UNIVERSIDAD DE OVIEDO

ESCUELA POLITÉCNICA DE INGENIERÍA DE GIJÓN

MÁSTER EN INGENIERÍA INFORMÁTICA

TRABAJO FIN DE MÁSTER

SISTEMA DE GESTIÓN DE LA CIBERSEGURIDAD INDUSTRIAL

-ESTADO DEL ARTE-

Pablo Sánchez Fernández

Junio de 2013

1 PRINCIPALES INICIATIVAS DE PROTECCIÓN DE INFRAESTRUCTURAS CRÍTICAS

1.1 Introducción

Este apartado recoge varias iniciativas desarrolladas o en desarrollo, sobre la protección de infraestructuras críticas, lideradas en su mayoría por los gobiernos nacionales, pero también por organizaciones e instituciones de distintos ámbitos.

Se presentan las principales iniciativas al respecto, así como otras iniciativas, menos relevantes o desarrolladas, y también se incluye un subapartado sobre la protección de infraestructuras de información críticas.

1.2 EE.UU.

EE.UU. encabeza las iniciativas sobre PIC a nivel mundial. Actualmente y desde 2006, ha puesto en marcha un plan general sobre protección, y otros 16 planes sectoriales específicos, a partir de las directivas promulgadas en 2003 sobre PIC, promovidas por los atentados del 11S.

El NIPP (*National Infrastructure Protection Plan*) [22] provee un marco que integra un amplio rango de esfuerzos dirigidos a promover y mejorar la seguridad de las infraestructuras críticas de los EE.UU.

El plan fue desarrollado por varios agentes relacionados con las infraestructuras críticas, incluyendo departamentos y agencias federales, agencias gubernamentales de ámbito estatal y local, y entidades del sector privado.

La primera edición del plan se publicó en 2006 y actualmente se encuentra en vigor la segunda, de 2009 y trata de proteger y asegurar la continuidad de lo que llama CIKR (*Critical Infrastructure Key Resources*), que incluye activos físicos o virtuales, sistemas, y redes, y provee una aproximación coordinada que es empleada para establecer prioridades, objetivos y requisitos para la protección de los CIKR, de manera que los recursos sean aplicados de la manera más eficiente y efectiva para reducir la vulnerabilidad, disuadir las amenazas, y minimizar las consecuencias de ataques y otros incidentes.

Los sectores que considera el plan general en los que se incluyen las infraestructuras críticas, y para los que se desarrollaron planes asociados específicos son:

- Sector químico
- Sector de instalaciones comerciales
- Sector de comunicaciones
- Sector de fabricación
- Sector de presas
- Sector de base industrial de defensa
- Sector de servicios de emergencia
- Sector de energía
- Sector de servicios financieros
- Sector de alimentación y agricultura
- Sector de instalaciones gubernamentales
- Sector de asistencia sanitaria y salud pública
- Sector de tecnologías de información

- Sector de reactores, materiales y desechos nucleares
- Sector de sistemas de transportes
- Sector de sistemas de agua y aguas residuales

El plan general está estructurado en siete apartados, tratando los siguientes puntos:

1. **Introducción**. Se da una visión global de los objetivos, los CIKR a proteger, y las líneas a seguir para llevar a cabo el plan
2. **Autoridades, Roles y Responsabilidades**. Se determinan las entidades que estarán involucradas en el plan, su función y su responsabilidad. Estas entidades tienen diferente carácter (privado-público, local-estatal-nacional).
3. **Estrategia del Programa de Protección de los CIKR**: Gestión del Riesgo. Se trata de la piedra angular del NIPP, un framework que establece los procesos para combinar información de consecuencias, vulnerabilidades y amenazas para producir una evaluación del riesgo nacional o sectorial, estructurado de manera que se promueva una mejora contínua de la protección de los CIKR. Cada iteración del ciclo, siempre teniendo en cuenta los aspectos físico, cibernético y humano, se compone de las siguientes etapas: Definición de objetivos, Identificación de activos, sistemas y redes, Evaluación de riesgos, Priorización, Implementación de programas, y Medida de la efectividad.
4. **Organización y Asociación para la protección de los CIKR**. Debido a la complejidad y extensión de los recursos clave, el plan debe implementarse haciendo uso de estructuras organizacionales y asociaciones para compartir y proteger la información necesaria. Se deben definir consejos sectoriales de coordinación, formados generalmente por entidades privadas, así como otros consejos intersectoriales, que ayuden a la coordinación y la difusión de buenas prácticas entre sectores, y otros consejos gubernamentales.
5. **Protección de los CIKR**: una parte integral de la misión nacional de seguridad. El NIPP complementa y ha de ser complementado con otros planes y guías, como son el NPG (*National Preparedness Guidelines*) y NRF (*National Response Framework*).
6. **Asegurar un Programa Efectivo y Eficiente a Largo Plazo**. El NIPP asegura la eficiencia y efectividad siguiendo mecanismos como: construir una conciencia nacional, habilitar programas educacionales y de entrenamiento, conducir investigación y desarrollo para mejorar la protección, desarrollar, salvaguardar y mantener sistemas y simulaciones para refinar continuamente los análisis de riesgos, y mejorar continuamente los planes mediante revisiones.
7. **Proveer Recursos para Sostener el Plan**. En este último capítulo, se establecen mecanismos para priorizar, en base a estudios e informes, los CIKR a proteger, y asignar los recursos público-privados disponibles para mitigar el riesgo de la mejor forma posible.

1.3 Unión Europea

De manera semejante a EE.UU. tras los atentados del 11S, la Comisión Europea a raíz de los atentados del 11M presentó un programa para mejorar la seguridad de diferentes tipos de infraestructuras críticas, principalmente frente a posibles ataques terroristas. En esta línea, se han ido sucediendo publicaciones en los últimos años, y ya en el campo específico de PIC, se publicó en 2004 la directiva “Protección de las infraestructuras críticas en la lucha contra el terrorismo” [15], documento mediante el cual se define qué supone una amenaza para las infraestructuras críticas de los miembros de la Unión.

En su segundo capítulo, la citada directiva trata de establecer qué se considera por infraestructura crítica, y describe una relación de centros, instalaciones, redes, etc. que considerar como tal y, se establecen los criterios principales para la consideración de una infraestructura como crítica. Dentro del mismo capítulo se sientan las bases para tratar la gestión del riesgo, con los objetivos de colaboración y compartición de información para lograr un nivel de riesgo aceptable.

El siguiente punto trata sobre los avances en el ámbito de la PIC, las legislaciones a nivel nacional y europeo relacionadas con la PIC y la creación de ENISA (Agencia Europea de Seguridad de las Redes y de la Información), lo que pone de manifiesto la preocupación de la Unión por la seguridad en las redes de comunicaciones y sistemas informáticos esenciales. Finalmente, en la directiva se propone la creación del EPCIP (*European Program for Critical Infrastructure Protection*), con el objetivo de coordinar esfuerzos público-privados entre estados en el campo de la CIP. De nuevo en relación con el intercambio de información se anuncia la creación de la Red de Información sobre Alertas en Infraestructuras Críticas (CIWIN).

En 2005 la Unión publica la directiva "Libro Verde Sobre un programa europeo para la protección de infraestructuras críticas" [19], que trata de proponer opciones para desarrollar el EPCIP y asegurar unos niveles adecuados y equivalentes de seguridad en infraestructuras críticas para los estados de la Unión. Propone para ello unos principios básicos (subsidiariedad, complementariedad, confidencialidad, cooperación, y proporcionalidad). También se establece como necesario, la identificación de las infraestructuras críticas europeas (ICE, en adelante) y nacionales (ICN, en adelante), y la necesidad de crear un organismo de supervisión del EPCIP, y se enumeran responsabilidades de los agentes de los ICN e ICE. Finalmente se describen medidas de apoyo al EPCIP como son la creación del CIWIN, la definición de metodologías comunes de niveles de alerta entre los Estados miembro y otros asuntos, como la financiación y el control.

En 2006 se publica el documento "Comunicación de la Comisión sobre un Programa Europeo para la Protección de Infraestructuras Críticas" [16]; a raíz del Libro Verde, la Comisión elabora una propuesta de EPCIP, en la que define su objetivo como la mejora de la protección de las ICE mediante la creación de un marco. Este marco consta de un procedimiento para identificar las ICE, medidas para facilitar la aplicación del EPCIP, apoyo a los Estados miembro en sus ICN y medidas financieras. Se define también un grupo comunitario de PIC para coordinar los puntos de contacto nacionales. Para la aplicación del EPCIP, se establece un plan de acción, también la creación del CIWIN, y la creación de grupos de expertos para compartir información y protegerse de amenazas y vulnerabilidades. El documento promueve la creación de programas nacionales de PIC, proponiendo unos contenidos mínimos para que los Estados miembro sigan líneas similares y reducir costes y esfuerzos.

En 2008 se publica la directiva "Identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección" [20], cuyo objetivo es establecer un procedimiento de identificación de las ICE y un planteamiento común para evaluar la necesidad de mejorar la protección de dichas infraestructuras. Mediante esta directiva, se insta a los Estados miembro a adoptar las medidas necesarias para dar cumplimiento a la misma. Analizando la directiva, se observan los siguientes aspectos a destacar:

1. **Identificación de ICE**. Todos los Estados han de identificar las ICE en su territorio conforme al procedimiento establecido.
2. **Designación de ICE**. Todos los Estados han de informar al resto de estados afectados por la designación de una ICE, así como a la Comisión y al propietario u operador, de manera anual.
3. **Planes de seguridad del operador**. Cada Estado ha de asegurar que las ICE dispongan de un Plan de Seguridad del Operador (PSO) o equivalente, garantizando su aplicación en el plazo de un año tras la designación del ICE.
4. **Responsables de enlace para la seguridad**. Cada Estado ha de asegurar que las ICE dispongan de un responsable de enlace para la seguridad, y de los mecanismos de comunicación adecuados entre la autoridad competente y el responsable de enlace para la seguridad.
5. **Informes**. Cada Estado ha de realizar una evaluación de las amenazas relativas a los subsectores de las ICE antes de un año desde su designación como ICE, y presentar cada dos años los datos generales sobre los riesgos en cada sector a la Comisión.

1.4 Otras iniciativas

Muchas naciones y algunos organismos han abordado la PIC con menor profundidad o con un ámbito más específico, creando políticas u objetivos generales, marcos estratégicos, organizaciones para la gestión o la respuesta ante incidentes.

1.4.1 Reino Unido

Dentro de la UE, Reino Unido es uno de los estados que más importancia otorga a la PIC, fruto de ello es el marco estratégico de 2010 [2] que aborda la protección frente amenazas naturales, estableciendo en dicho documento definiciones, objetivos, principios, calendario de actuación, una serie de políticas, roles y responsabilidades, así como un anexo para la categorización de infraestructuras críticas.

El gobierno escocés, ha elaborado por su parte, un framework específico para PIC [55], que trata de ser un enfoque más global que el marco desarrollado por el el gobierno de Reino Unido, incluyendo amenazas naturales y ataques terroristas, y dando importancia a la colaboración y compartición de información, y que aspira a poder ser asimilado en el futuro, tras los posibles refinamientos, por el gobierno británico, para toda la nación.

1.4.2 Australia

El gobierno australiano creó en 2003 un foro, llamado TISN (*Trusted Information Shared Network*) para que gobierno, propietarios y gestores de las infraestructuras críticas nacionales colaboren conjuntamente compartiendo información acerca de la seguridad de dichas infraestructuras, y está compuesto por grupos de diferentes sectores, coordinados por un consejo central llamado CIAC (*Critical Infrastructure Advisory Council*).

En 2010, el gobierno publica su estrategia sobre PIC, *Critical Infrastructure Resilience Strategy* [1], mediante la cual define las infraestructuras críticas nacionales, promueve acuerdos sectoriales e intersectoriales, define el rol del gobierno en materia de PIC, establece los objetivos de la política, establece unos imperativos estratégicos, y también una serie de criterios para revisar la estrategia y revisar su efectividad.

Los imperativos estratégicos constituyen en sí las políticas y procedimientos a alto nivel asociados sobre PIC, y aborda los siguientes puntos:

- Compartición de información entre actores implicados en PIC
- Integración de PIC en i+D
- Creación de cuerpo de conocimientos sobre PIC
- Asistencia a operadores para identificar, analizar y gestionar dependencias inter-sectoriales
- Prestación de consejo en materia de PIC
- Implementación de una estrategia de ciberseguridad, incluyendo los aspectos necesarios de PIC en ella
- Prestación de soporte a los programas de PIC, principalmente mediante un centro de coordinación nacional (NCIRC, *National Coordination Infrastructure Resilience Committee*)

Conjuntamente con la estrategia, se publicó un suplemento, con una serie de actividades, a modo de pautas, que ayuden a implementar los imperativos estratégicos.

1.4.3 NERC CIP

La corporación NERC (*North American Electric Reliability Corporation*), es una organización que tiene como uno de sus mayores objetivos, el desarrollo de estándares, conjuntamente con los stakeholders de la infraestructura de red eléctrica norteamericana, para la operación y monitorización del sistema, así como velar porque dichos estándares se cumplan. Además, desarrolla estándares para la protección de la infraestructura eléctrica, que se engloban bajo el nombre NERC CIP, de obligado

cumplimiento para compañías del sector. Este es un ejemplo de plan sectorial de PIC, desarrollado específicamente para la infraestructura eléctrica.

Actualmente (Mayo de 2013), NERC CIP está constituido por nueve estándares de obligado cumplimiento, y otros documentos en vías de desarrollo. Los documentos con validez son:

- CIP-001-2a Informes sobre sabotaje [40]
- CIP-002-3 Identificación de activos cibernéticos [41]
- CIP-003-3 Controles en la gestión de la seguridad [42]
- CIP-004-3a Personal y formación/capacitación [43]
- CIP-005-3a Perímetros de seguridad electrónica [44]
- CIP-006-3c Seguridad física [45]
- CIP-007-3a Gestión de la seguridad de sistemas [46]
- CIP-008-3 Notificación de incidentes y respuesta [47]
- CIP-009-3 Plan para la recuperación de activos cibernéticos de carácter crítico [48]

1.4.4 España

De manera similar a EE.UU., a raíz de los atentados del 11M, nace en España el CNCA (Centro Nacional de Coordinación Antiterrorista), que no tendrá focalización específica en la PIC hasta que en 2007 se desarrolla el PNPIC (Plan Nacional de PIC) y se crea el CNPIC (Centro Nacional para la Protección de Infraestructuras Críticas), que se apoya en el CCN (Centro Criptológico Nacional) para el tratamiento de los ciberataques sobre infraestructuras críticas y en la actualización de información sobre vulnerabilidades SCADA e incidentes de seguridad informáticos relacionados con infraestructuras críticas..

El PNPIC divide las ICs en doce sectores estratégicos:

- Centrales y redes de energía
- Tecnologías de la información y las comunicaciones
- Sistema Financiero y Tributario (por ejemplo, banca, valores e inversiones)
- Sector sanitario
- Espacio
- Instalaciones de Investigación
- Alimentación
- Agua (embalses, almacenamiento, tratamiento y redes)
- Transportes (aeropuertos, puertos, instalaciones intermodales, ferrocarriles y redes de transporte público, sistemas de control del tráfico)
- Industria Nuclear
- Industria Química
- Administración (servicios básicos, instalaciones, redes de información, activos, y principales lugares y monumentos nacionales)

En 2011 se publicó la LPIC (Ley de Protección de Infraestructuras Críticas [37]), así como el reglamento que la desarrolla y la Estrategia Española de Seguridad [38], tras la directiva europea de 2008 que obligaba a los estados miembro a desarrollar una política nacional sobre PIC.

La LPIC recoge una serie de medidas necesarias para cumplir con la citada directiva europea de 2008. Los objetivos de esta ley son, por un lado, la regulación de la protección de las infraestructuras críticas contra ataques deliberados de todo tipo (físicos o lógicos) [52] y, por otro lado, la definición de un sistema organizativo de protección de infraestructuras críticas, que sirva como nexo para Administraciones Públicas, y entidades privadas afectadas.

El "Reglamento de Protección de las Infraestructuras Críticas" [38] desarrolla los aspectos recogidos en la LPIC. Para ello, se establece la necesidad de elaborar diferentes planes a desarrollar por las Administraciones Públicas y por los operadores críticos (Planes de Seguridad del Operador, y Planes de Protección Específicos). Este reglamento consta de 36 artículos agrupados bajo cuatro títulos que tratan los siguientes aspectos:

1. Asuntos generales relativos a objetivo y ámbito de aplicación
2. Sistema de Protección de Infraestructuras Críticas, composición, competencias y funcionamiento de los órganos creados por la ley.
3. Regulación de los instrumentos de planificación
4. Seguridad de las comunicaciones y roles de una infraestructura crítica: Responsable de Seguridad y Enlace, y Delegado de Seguridad

La "Estrategia Española de Seguridad, una responsabilidad de todos", expone la necesidad de tratar los nuevos aspectos de seguridad, incluidas las amenazas tecnológicas, dentro de un amplio espectro de ámbitos contemplados [36] El documento destaca la necesidad de una coordinación entre el sector privado y las Administraciones Públicas, ya que buena parte de las infraestructuras críticas está en manos del sector privado.

1.4.5 Iniciativas de Protección de Infraestructuras de Información Críticas

A pesar de la presencia de servicios y sistemas de información prácticamente a todos los niveles de las IC, la mayoría de las iniciativas sobre PIC no separa aún de manera explícita ambos asuntos. La forma de abordar el problema y en nivel de profundidad tomado, varía entre las iniciativas gubernamentales. En algunos países como Corea, se ha iniciado el camino, promulgando una serie de políticas sobre PIIC [25], en otros, se han creado organismos para la resiliencia o el desarrollo de programas, como en Reino Unido, y en algunos existen marcos o planes en desarrollo, como EE.UU.

Este apartado presenta, dentro de la protección de infraestructuras críticas, las iniciativas específicas sobre PIIC

1.4.5.1 EEUU

Dentro de la orden ejecutiva de 2013 del gobierno de EE.UU. sobre la mejora de la ciberseguridad en infraestructuras críticas, se instaba al desarrollo de un marco de ciberseguridad, tarea que se encomendó al NIST (*National Institute of Standards and Technology*). Este nuevo marco trata de reducir los riesgos cibernéticos asociados a infraestructuras críticas.

En febrero de 2013 el NIST anunció el primer paso en el desarrollo del marco, llamado *Cybersecurity Framework*, que será un conjunto de estándares de cumplimiento voluntario y buenas prácticas para guiar a la industria con el fin de reducir los riesgos de redes y ordenadores que son vitales para la nación, y para ello actualmente (abril de 2013) está reuniendo información a través de diferentes medios sobre las prácticas de las organizaciones, tales como el uso de frameworks, estándares, buenas prácticas, etc.

El framework consistirá en una hoja de ruta y una estructura para futuros esfuerzos, incluyendo procesos recomendados, incluyendo los procesos de revisión de los estándares dentro de cada comunidad de stakeholders. El NIST revisará y actualizará continuamente el framework para adaptarse a los cambios en los negocios y las necesidades de seguridad de cada momento.

Este framework incluirá métricas, métodos y procedimientos que podrán ser usados para efectuar una evaluación y monitorización continuadas de la efectividad de los controles de seguridad desplegados así como la efectividad de los estándares del framework, sus directrices y buenas prácticas. Además,

presentará un menú de controles de seguridad de gestión, de operación y técnicos, incluyendo políticas y procedimientos.

1.4.5.2 Japón

En materia de PIIC, Japón formuló en 2005 el Plan de Acción en Medidas de Seguridad de la Información para Infraestructuras Críticas (actualmente vigente el segundo plan, *The Second Action Plan on Information Security Measures for Critical Infrastructures*, desde 2009 [54]), que aborda la creciente dependencia de TI en los sectores críticos así como la interdependencia entre ellos. Se trata de un plan sectorial, dentro de la estrategia nacional, que identifica diez infraestructuras críticas objetivo para asegurar su nivel de seguridad de la información. El plan también identifica las causas de mal funcionamiento de sistemas TI que pueden interrumpir los servicios o reducir el rendimiento de infraestructuras críticas, causas que incluyen tanto ciberataques intencionados como factores no intencionados y desastres naturales.

La estrategia nacional está marcada actualmente por *The Second National Strategy on Information Security*, publicado en 2009 [39], que define tres políticas básicas:

1. Reforzar las políticas teniendo en cuenta posibles brotes de ciberataques y establecer una organización para contrarrestarlos
2. Establecer políticas adaptadas a los cambios en el entorno de seguridad de la información
3. Convertir a la nación como el país con la seguridad de la información más avanzada

1.4.5.3 Reino Unido

La Estrategia de Ciberseguridad Nacional de 2011 (*The UK Cyber Security Strategy. Protecting and promoting the UK in a digital world* [5]), tiene en cuenta la PIC dentro de sus objetivos, en la identificación de amenazas y en la implementación de la estrategia. Este documento de estrategia de ciberseguridad, muestra la situación presente y futura de los sistemas informáticos, su importancia y funciones, y el panorama de amenazas, y presenta cuatro objetivos de ciberseguridad y un anexo para guiar en su implementación.

Para unir esta estrategia y la relativa a PIC (ver capítulo 1.4.1) en torno a infraestructuras críticas, el gobierno creó el CPNI (*Centre for the Protection of National Infrastructure*), organismo que trata de proteger la seguridad nacional, mediante la provisión de consejos y advertencias de seguridad, que cubren, seguridad física, personal, y ciberseguridad.

1.4.5.4 ITU

La ITU (*International Telecommunications Union*) es el organismo especializado de las Naciones Unidas para las tecnologías de la información y la comunicación. Entre otras funciones, tiene la responsabilidad de atribuir el espectro radioeléctrico y las órbitas de satélite a escala mundial, o la elaboración de normas técnicas para asegurar la interconexión de redes y tecnologías.

Una de las iniciativas de la ITU, consiste en la elaboración de un framework genérico sobre PIIC [35], destinado a las naciones que están empezando a desarrollar su propia política PIIC, y que tienen dificultades para identificar buenas prácticas y ejemplos.

Este framework sugiere un modelo funcional para una construir unidad de CIIP, más que una solución exhaustiva para CIIP, con el objetivo de promover la colaboración entre los stakeholders para proteger las infraestructuras, tomando como referencia el modelo suizo, en el que el organismo MELANI se encarga de estos asuntos de manera eficiente.

El framework, se basa en cuatro pilares, que son, la prevención temprana, la detección, la reacción y la gestión de crisis.

2 PRINCIPALES INICIATIVAS DE PROTECCIÓN DE SISTEMAS DE CONTROL INDUSTRIAL

2.1 ENISA - Protecting Industrial Control Systems

En el ámbito europeo, en paralelo con las directivas relacionadas con el EPCIP, los asuntos de seguridad de la información para infraestructuras críticas son afrontadas por la Agenda Digital para Europa (DAE por su acrónimo en inglés) [17], y el plan de acción sobre PIIC, a raíz de la directiva de la Comisión Europea, *Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience*, [18]. Para el desarrollo de estos planes, la agencia europea ENISA, fue la encargada de explorar la problemática, realizando un estudio, principalmente centrado en Europa, pero también observando el contexto internacional, teniendo en cuenta las amenazas, riesgos y retos en el área de ICS, así como las iniciativas ya existentes.

ENISA, plasmó el trabajo realizado en un documento, que lleva por nombre *Protecting Industrial Control Systems - Recommendations for Europe and Member States* [24], y presentado en 2011, que consta de siete recomendaciones básicas en su documento principal, y una serie de anexos relacionados, todo ello dirigido tanto al sector público como privado. Estas recomendaciones tratan de dar un consejo práctico dirigido a mejorar las iniciativas actuales, promover la cooperación, desarrollar nuevas medidas y buenas prácticas, y reducir las barreras en materia de compartición de información.

Las recomendaciones que recoge ENISA son las siguientes:

- **Recomendación 1**: Creación de estrategias de seguridad ICS pan-europeas y nacionales.
- **Recomendación 2**: Creación de una guía de buenas prácticas para seguridad ICS.
- **Recomendación 3**: Creación de plantillas de seguridad ICS.
- **Recomendación 4**: Promover la concienciación y la formación
- **Recomendación 5**: Creación de un banco de pruebas común, o alternativamente, un marco de certificación de seguridad ICS.
- **Recomendación 6**: Creación de capacidades de respuesta de emergencia nacionales sobre ICS-informática.
- **Recomendación 7**: Promover la investigación en seguridad ICS haciendo uso de los programas de investigación existentes.

Los anexos desarrollados en conjunto con el documento son los siguientes:

- **Anexo 1**: presenta los principales resultados de la fase de investigación. Provee una exhaustiva visión general del panorama de la seguridad en ICS.
- **Anexo 2**: se trata de un análisis detallado de los datos reunidos a través de las entrevistas y las encuestas en las que participaron los expertos en seguridad de ICS.
- **Anexo 3**: es una recopilación de las guías y estándares actuales sobre ICS.
- **Anexo 4**: incluye una completa lista de iniciativas relacionadas con seguridad de ICS.
- **Anexo 5**: provee descripciones detalladas de los hallazgos clave que forman el conocimiento base sobre el que las recomendaciones están construidas.
- **Anexo 6**: incluye las actas del workshop.

2.2 ISA99 - ISA/IEC-62443

Es una de las iniciativas relacionadas con ICS dentro de ISA (*International Society of Automation*). ISA constituyó en 2002 el comité ISA99, un grupo de expertos con el propósito de establecer estándares, recomendaciones prácticas, informes técnicos e información relacionada que defina procedimientos para implementar sistemas de control electrónicamente seguros, prácticas de seguridad y evaluaciones de seguridad.

Con dichos objetivos, el comité ISA99 desarrolló una serie de documentos, anteriormente identificados con el mismo nombre, y actualmente renombrados a ANSI/ISA-62443. Los estándares e informes técnicos que conforman ISA-62443 están organizados en cuatro categorías generales:

General: incluye información de conceptos, modelos y terminología. También incluye documentación que describa métricas de seguridad y ciclos de vida de seguridad para IACS (*Industrial Automation and Control Systems*).

Políticas y procedimientos: documentación que aborde aspectos de creación y mantenimiento de un programa de seguridad efectivo de IACS. Esta categoría está principalmente dirigida a los propietarios de los activos.

Sistema: engloba los documentos que describan requisitos y guías de diseño del sistema para la integración segura de sistemas de control. El núcleo de esta categoría es el modelo de diseño de zonas y conductos.

Componentes: esta categoría incluye los trabajos sobre descripciones de desarrollo de producto y requisitos técnicos, para productos de control de sistemas. Está dirigido principalmente para fabricantes, pero también puede ser útil en labores de integradores y propietarios de los activos.

Puede verse gráficamente la organización en categorías de los documentos en la figura EA.1.

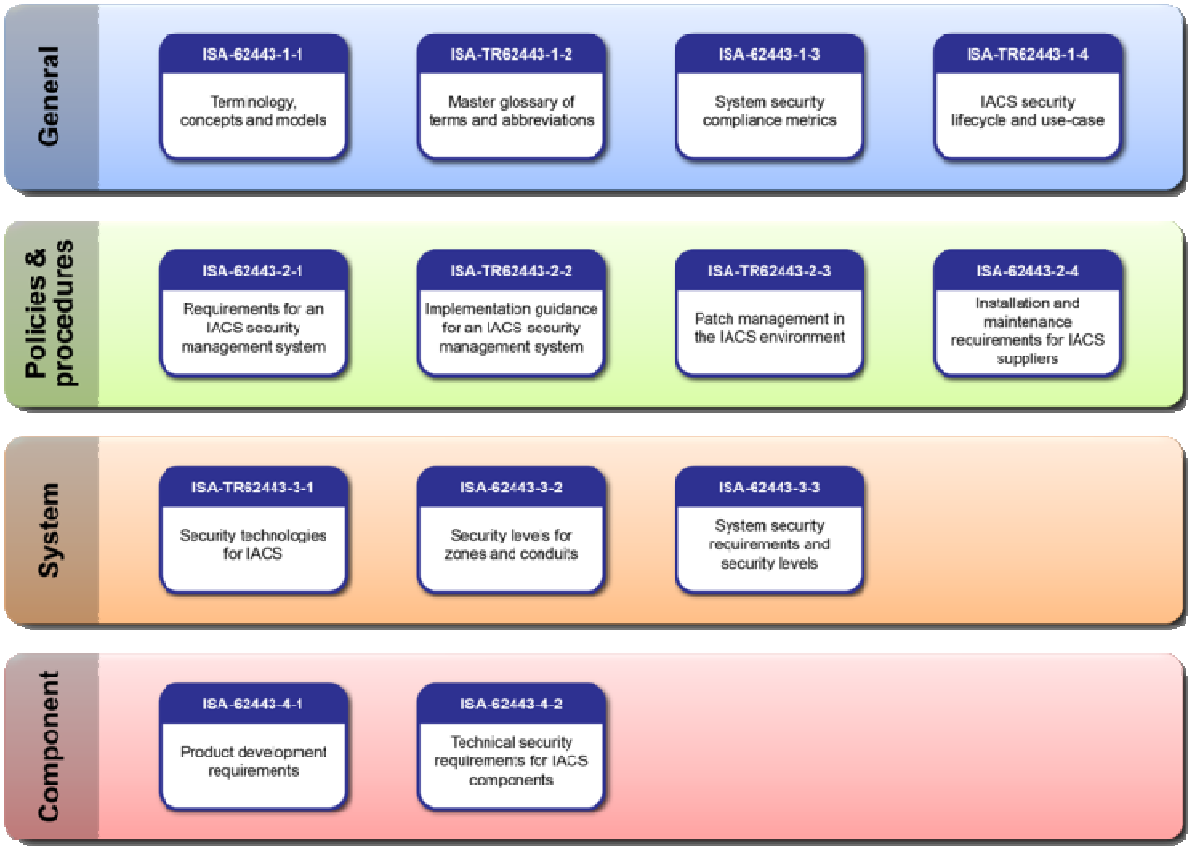


Figura EA.1. Documentos y categorías de ISA-62443

Los documentos publicados y planeados hasta el momento, dentro de las cuatro categorías son los siguientes:

- **Grupo 1**: General
  - ISA-62443-1-1 (IEC/TS 62443-1-1) (anteriormente "ISA-99 Part 1") Publicado como estándar ISA/ANSI y IEC. El Comité ISA99 está revisando el documento para alinearlo con otros documentos de la serie, y clarificar la parte de contenido normativo. Originalmente el documento contenía la terminología, conceptos y modelos.
  - ISA-TR62443-1-2 (IEC 62443-1-2) Es un glosario de términos usados por el Comité ISA99. Actualmente está en fase de borrador, pero su contenido ya es accesible.
  - ISA-62443-1-3 (IEC 62443-1-3) Identifica un conjunto de métricas de cumplimiento de seguridad de IACS. Actualmente en fase de desarrollo.
  - ISA-62443-1-4 (IEC/TS 62443-1-4) Define el ciclo de vida de seguridad de IACS y casos de uso. Documento planeado pero aún por desarrollar.
- **Grupo 2**: Políticas y procedimientos
  - ISA-62443-2-1 (IEC 62443-2-1) (anteriormente "ANSI/ISA 99.02.01-2009 o ISA-99 Part 2") aborda la manera de establecer un programa de seguridad IACS. Actualmente bajo revisión para un alineamiento con la serie de estándares ISO 27000.
  - ISA-62443-2-2 (IEC 62443-2-2) Afronta cómo operar un sistema de seguridad de IACS. Actualmente bajo desarrollo.
  - ISA-TR62443-2-3 (IEC/TR 62443-2-3) Un informe técnico en materia de gestión de actualizaciones de seguridad en entornos IACS. Actualmente bajo desarrollo.
  - ISA-62443-2-4 (IEC 62443-2-4) Se centra en la certificación de suministradores de IACS en cuanto a políticas de seguridad y prácticas. Es una adaptación de un documento de WIB (*International Instrument Users' Association*).
- **Grupo 3**: Sistema
  - ISA-TR62443-3-1 (IEC/TR 62443-3-1) Un informe técnico sobre las tecnologías apropiadas para seguridad de IACS.
  - ISA-62443-3-2 (IEC 62433-3-2) Documento que trata de definir cómo definir niveles de seguridad mediante el uso de zonas y conductos. En desarrollo actualmente.
  - ISA-62443-3-3 (IEC 62433-3-3) Define detalladamente requisitos técnicos sobre seguridad de IACS. En desarrollo actualmente.
- **Grupo 4**: Componentes
  - ISA-62443-4-1 (IEC 62443-4-1) Define los requisitos para el desarrollo de productos y soluciones de IACS seguras. En desarrollo actualmente.
  - ISA-62443-4-2 (IEC 62443-4-2) Define los requisitos técnicos para los componentes de IACS. En desarrollo actualmente.

2.2.1 ISA99.02.01-2009 - ISA-62443-2-1

Dentro de los documentos desarrollados, ISA-62443-2-1 [30] propone:

1. Una lista definida de los elementos de un sistema de gestión de ciberseguridad para IACS (CSMS, por su acrónimo en inglés). Estos elementos representan lo que debería y lo que podría ser incluido en un CSMS para proteger el sistema de ciberataques. Los elementos se presentan en tres categorías:

   a. Análisis de riesgos

b. Afrontar el riesgo mediante el CSMS
c. Monitorización y mejora del CSMS

Cada una de estas subcategorías se descompone en elementos, y para cada uno se define su objetivo, su descripción y sus razones, para posteriormente presentar una lista de los requisitos del elemento, que serán las actividades que la organización podría y/o debería implementar para cumplir dicho objetivo.

Análisis de riesgos: la primera categoría, se dividen en las siguientes subcategorías:

a. Descripción de la categoría
b. Fundamentos de negocio
c. Identificación de riesgos, clasificación y evaluación

Afrontar el riesgo mediante el CSMS: la segunda categoría, se divide en las siguientes subcategorías:

a. Descripción de la categoría
b. Política de seguridad, organización y concienciación. Esta categoría trata el desarrollo de políticas básicas de ciberseguridad, las entidades responsables de la ciberseguridad y la concienciación dentro de la organización sobre asuntos de seguridad. Contiene los siguientes elementos, cada uno de ellos con sus requisitos:
    i. Definición del alcance.
    ii. Organización para la seguridad.
    iii. Formación del personal y concienciación sobre seguridad
    iv. Plan de continuidad del negocio
    v. Políticas de seguridad y procedimientos
c. Contramedidas de seguridad seleccionadas. Contiene los principales tipos de controles de seguridad que deberían ser parte de un CSMS, mediante los siguientes elementos, cada uno con sus requisitos:
    i. Seguridad de personal
    ii. Seguridad física y del entorno
    iii. Segmentación de redes
    iv. Control de acceso: administración de cuentas
    v. Control de acceso: autenticación
    vi. Control de acceso: autorización
d. Implementación. Esta categoría trata asuntos relativos a la implementación del CSMS. Incluye los siguientes elementos de interés, cada uno con sus requisitos:
    i. Gestión de riesgos e implementación
    ii. Desarrollo y mantenimiento del sistema
    iii. Gestión de la información y la documentación
    iv. Planificación y respuesta a incidentes

Monitorización y mejora del CSMS: la tercera categoría, se divide en las siguientes subcategorías:

a. Descripción

b. Cumplimiento. Esta categoría trata de asegurar que el CSMS se cumple, mediante varios requisitos.

c. Revisión, mejora y mantenimiento del CSMS. Esta categoría trata de asegurar que el CSMS continúa cumpliendo objetivos a lo largo del tiempo, mediante varios requisitos.

2. Un anexo para guiar en el desarrollo de elementos del sistema de gestión de ciberseguridad para IACS.
3. Un anexo que describe un ejemplo del proceso que una organización podría usar para desarrollar los elementos de un sistema de gestión de ciberseguridad para IACS.

2.3 NIST SP800-82

El NIST (*National Institute of Standards and Technology*), es la agencia enmarcada dentro del Departamento de Comercio de los EE.UU. para la administración de la tecnología, cuya misión es promover la innovación y la competencia industrial del país mediante avances en medición, normativas y tecnología. Dentro de sus diversas áreas de publicaciones orientadas a diferentes sectores, se encuentran las *Special Publications 800 Series*, que desde 1990, engloba decenas de documentos de interés sobre seguridad TI, incluyendo publicaciones sobre investigación, guías, directrices, y recomendaciones, para diversos apartados dentro de la seguridad TI.

Dentro de la serie SP-800, se publicó en 2011 la versión final del documento *SP800-82 Guide to Industrial Control Systems (ICS) Security - Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC)* – [50].

Este documento trata de servir de guía para el establecimiento de ICS seguros, mediante una estrategia de defensa en profundidad, para seleccionar los controles de seguridad adecuados. Esta guía se complementa con la guía *SP 800-53, Recommended Security Controls for Federal Informations Systems and Organizations* [49], que aporta directrices en forma de establecimiento de controles de seguridad para las agencias gubernamentales de EE.UU., aplicando a todos los componentes de un sistema de información, que procese, almacene o transmita información federal.

El SP-800 82 aborda a través de secciones, los siguientes asuntos en materia de seguridad:

- **Sección 3**: Describe las diferencias entre sistemas ICS y TI, así como las amenazas, vulnerabilidades e incidencias.
- **Sección 4**: Visión general del desarrollo y despliegue de un programa de seguridad de ICS para mitigar el riesgo de las vulnerabilidades identificadas en la Sección 3. Esta sección trata los siguientes asuntos en varias subsecciones:
    - Caso de Negocio para seguridad: desarrollo de un caso de negocio que refleje el impacto en el negocio y justificación financiera para crear un sistema de ciberseguridad integrado.
    - Desarrollando un programa de seguridad exhaustivo: describe el proceso básico para desarrollar un programa de seguridad, incluyendo:
        - Obtención de apoyo de la gerencia
        - Formación de un equipo de personas multifuncional
        - Definición de políticas y procedimientos
        - Definición de un inventario de activos ICS
        - Realización de una evaluación de riesgos y vulnerabilidades
        - Definición de controles de mitigación

        - Formación y concienciación del personal de ICS

- **Sección 5**: Recomendaciones para la integración de la seguridad en arquitecturas de red típicamente encontradas en ICS, con énfasis en prácticas de segregación de redes. Esta sección trata los siguientes asuntos en varias subsecciones:
    - Firewalls
    - Red de control separada lógicamente
    - Segregación de redes
    - Arquitectura recomendada de defensa en profundidad
    - Políticas generales de firewall para ICS
    - Reglas de firewall recomendadas para servicios específicos
    - Traducción de direcciones de red (NAT)
    - Asuntos específicos de firewalls
    - Puntos de fallo
    - Redundancia y tolerancia a fallos
    - Prevención de ataques man-in-the-middle
- **Sección 6**: Resumen de controles identificados en el documento SP 800-53, y aporta orientación inicial sobre cómo aplicar estos controles de seguridad a ICS. Esta sección trata, mediante secciones, tres tipos de controles:
    - Controles de Gestión: Contramedidas para un ICS que se centran en la gestión del riesgo y la gestión de la seguridad de la información, agrupados en cinco familias:
        - Evaluación de Seguridad y Autorización
        - Planificación
        - Análisis de Riesgos
        - Adquisición de Sistemas y Servicios
        - Gestión de Programa (controles organizacionales)
    - Controles Operacionales: Contramedidas de seguridad para ICS implementadas y ejecutadas principalmente por personas, agrupadas en nueve familias:
        - Seguridad de Personal
        - Protección Física y del Entorno
        - Planificación de Contingencia
        - Gestión de la Configuración
        - Mantenimiento
        - Integridad de Sistemas e Información
        - Protección de Medios
        - Respuesta a Incidentes
        - Formación y Concienciación
    - Controles Técnicos: Contramedidas de seguridad principalmente implementadas y ejecutadas por el sistema, a través de mecanismos hardware, software o firmware, agrupadas en cuatro familias:
        - Identificación y Autenticación

- Control de Acceso
- Auditoría y Responsabilidad
- Protección de Sistemas y Comunicaciones

La guía contiene además tres apéndices, con listas de acrónimos, glosario, lista de referencias usadas en el desarrollo de la guía, y otros tres que se detallan a continuación:

- Apéndice C: Lista y descripción de algunas de las actividades de seguridad de ICS.
- Apéndice D: Lista de algunas capacidades emergentes en materia de seguridad desarrolladas para ICS.
- Apéndice E: Visión general de la implementación FISMA (Federal Information Security Management Act of 2002) y su relevancia para ICS.

2.4 CCN-STIC-480 (CPNI Process Control and SCADA Security)

El Centro Criptológico Nacional (CCN en adelante) tiene como una de sus funciones más destacables, 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, lo que se materializa en la serie de documentos CCN-STIC, cumpliendo con lo reflejado en el Esquema Nacional de Seguridad.

Dentro de dicha serie, la guía CCN-STIC-480 [6] en materia de sistemas SCADA es de aplicación a todos los sistemas SCADA, y está destinada cualquier organismo de cualquier índole que cuente con sistemas SCADA.

Los objetivos de esta serie de documentos son:

- Presentar la problemática planteada por los sistemas SCADA y sus vulnerabilidades, su impacto y la necesidad imperativa de controlar su seguridad.
- Describir las técnicas necesarias para analizar los riesgos derivados de dichos sistemas.
- 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.
- Presentar algunas soluciones técnicas ante determinadas amenazas, referenciando los documentos donde se puede encontrar más información de cada una de ellas.

Los documentos de esta serie son principalmente orientativos, de carácter práctico, y no tienen índole normativa. Esta serie es una traducción de las guías publicadas por el CPNI del Reino Unido, *Process Control and SCADA Security* [21], como parte del acuerdo de colaboración entre dicho organismo y el Centro Criptológico Nacional.

La serie CCN-STIC-480 está compuesta por nueve documentos diferentes:

- **480: Seguridad en sistemas SCADA** [6]. Documento principal que trata sin profundidad, a modo de listado de puntos a tener en cuenta:
  - Empresa: Gestión del riesgo, Políticas sobre SCADA, Auditorías, Gestión de proyectos SCADA, Gestión con empresas externas.
  - Recursos Humanos: Contratación, formación, Relaciones interdepartamentales, y Bajas
  - Sistemas: Gestión de activos, Seguridad Física, Seguridad perimetral, Securización, Monitorización, Procedimientos de recuperación

- **480A: Guía de buenas prácticas** [7]. Trata principalmente buenas prácticas, en forma de controles de todo tipo, en una lista no exhaustiva, complementada con otras listas de los demás documentos de la serie.
- **480B: Comprender el riesgo del negocio** [8]. Una guía, en varios pasos, para estudiar el riesgo del negocio, observando amenazas, vulnerabilidades e impactos, con el objetivo de poder elegir las medidas de seguridad necesarias.
- **480C: Implementar una arquitectura segura** [9]. Orientación de los pasos a seguir para seleccionar una arquitectura apropiada e implementar las medidas asociadas de reducción de riesgo para un sistema de control.
- **480D: Establecer capacidades de respuesta** [10]. Guía para establecer las capacidades de protección, detección y respuesta ante incidentes de seguridad en sistemas SCADA, mediante creación de equipos de respuesta, planes de respuesta y continuidad, sistemas de alerta temprana, establecimiento de procesos y procedimientos, la notificación de incidentes y el aprendizaje tras ellos.
- **480E: Mejorar la concienciación y las habilidades** [11]. Prácticas para mejorar la concienciación continua, establecer un marco de formación y el desarrollo de las relaciones laborales.
- **480F: Gestionar el riesgo de terceros** [12]. Trata la identificación de terceras partes, gestión del riesgo de los proveedores, gestión del riesgo de las organizaciones de soporte y la gestión del riesgo en la cadena de suministro.
- **480G: Afrontar proyectos** [13]. Toma otros elementos del marco relacionados con políticas y normas, comprensión del riesgo y observaciones sobre terceros y los incorpora en el proceso de realización de proyectos de seguridad, en un paso previo a la implementación. Trata todas las fases del desarrollo, desde el punto de vista de la seguridad; contratación, especificación del diseño, ciclo de vida del desarrollo, revisiones de seguridad del diseño, pruebas, entrega y baja.
- **480H: Establecer una dirección permanente** [14]. Guía para establecer una dirección formal para la administración de la seguridad en sistemas de control, mediante el establecimiento de un grupo directivo, el desarrollo de políticas y normas, garantizar su cumplimiento, informar a reguladores externos de su cumplimiento y la actualización de políticas y normas.

2.5 España: Centro de Ciberseguridad Industrial

En junio de 2013 surge en España una nueva iniciativa, el Centro de Ciberseguridad Industrial (CCI), cuya misión es la de impulsar y contribuir a la mejora de la Ciberseguridad Industrial en España y Latinoamérica, desarrollando actividades de análisis, desarrollo de estudios e intercambio de información sobre el conjunto de prácticas, procesos y tecnologías, diseñadas para gestionar el riesgo del ciberespacio. Este organismo está apoyado por gran parte del sector, y dará cabida a todo tipo de actores públicos y privados.

Los objetivos del Centro pasan por aglutinar a los principales actores y expertos implicados en la ciberseguridad industrial, proporcionar un ciber-estado de la situación, establecer canales de interlocución con autoridades y reguladores, mejorar la concienciación, cualificar a profesionales en ciberseguridad industrial y fomentar la dinamización y difusión del mercado español de la ciberseguridad industrial.

Un medio para alcanzar sus objetivos, será la creación de grupos de trabajo sectoriales y temáticos, centrados en los aspectos de ciberseguridad de un área industrial determinada o en una cuestión concreta. Previsiblemente, se comenzará con los sectores de Energía, Químico, Agua y Transporte, siempre supeditado a la demanda de los miembros.

3 SEGURIDAD DE LA INFORMACIÓN

La Seguridad de la Información (SI en adelante) tiene como fin la protección dentro de una organización, de la información y de los sistemas que hacen uso de ella, protegiendo el acceso, el uso, la divulgación, la interrupción y la destrucción no autorizada. Dentro de la SI se agrupa el conjunto de medidas preventivas y reactivas de una organización y de los sistemas tecnológicos que permitan resguardar y proteger la información con el fin de preservar la confidencialidad, la disponibilidad e integridad de la información.

3.1 ISO/IEC 27000

ISO (*International Organization for Standardization*) es el organismo encargado de promover el desarrollo de normas internacionales, de cumplimiento voluntario, de fabricación, comercio y comunicación para todas las ramas industriales a excepción de la eléctrica y la electrónica.

La serie ISO/IEC 27000 es un conjunto de estándares y guías de seguridad (la mayoría en fase de desarrollo), que contienen las mejores prácticas recomendadas en el ámbito de la SI para el desarrollo, la implementación y el mantenimiento de un Sistema de Gestión de la Seguridad de la Información (SGSI, en adelante).

Se trata del estándar referente a nivel mundial, y proporciona una norma certificable para aquellas organizaciones que cumplan los requisitos descritos en el documento ISO/IEC 27001 [32].

La serie está compuesta por los siguientes documentos, entre otros de nueva generación en desarrollo [33]:

- ISO/IEC 27000. Vocabulario y términos relacionados con el SGSI.
- ISO/IEC 27001. Norma que contiene los requisitos de implantación de un SGSI, certificable.
- ISO/IEC 27002. Código de buenas prácticas en forma de controles para la gestión de la SI.
- ISO/IEC 27003. Conjunto de directrices para la implementación de un SGSI.
- ISO/IEC 27004. Métricas para medir eficacia, eficiencia y grado de implantación de un SGSI.
- ISO/IEC 27005. Documento con recomendaciones sobre la gestión de riesgos en la SI.
- ISO/IEC 27006:2007. Requisitos para conseguir la acreditación como organización certificadora de ISO 27001.
- ISO/IEC 27007. Guía de auditoría de un SGSI.
- ISO/IEC 27799:2008. Guía de implementación de ISO 27002 en la industria de la salud.
- ISO/IEC 27035:2011. Gestión de incidentes de seguridad.

3.1.1 ISO/IEC 27001

Publicada en 2005 [32], tiene su base en normas anteriores de BSI (*British Standards Institution*), la norma BS7799-1 y BS7799-2. ISO/IEC 27001 es la norma principal de la serie, y contiene el conjunto formal de especificaciones para el establecimiento, implementación, monitorización, revisión, mantenimiento, y mejora, contra las que una organización puede obtener una certificación independiente, de su SGSI.

El estándar es aplicable sobre cualquier tipo y tamaño de organización, y se basa en el ciclo PDCA ("*Plan, Do, Check, Act*"), que se aplica en diferentes procesos.

Incluye un apéndice (Anexo A) que presenta una relación de los objetivos y control y controles que desarrolla el documento ISO/IEC 27002, para que sean seleccionados por las organizaciones dentro de sus SGSI; aunque la implementación de estos controles no es obligatorio, la organización debe argumentar sólidamente su no aplicabilidad.

La norma está publicada en España desde 2007 como UNE-ISO/IEC 27001:2007.

El documento se estructura en secciones, más tres apéndices, tratando las bases y los diferentes aspectos de un SGSI. Estas son las secciones que establecen requisitos:

- **Sección 4**. Sistema de Gestión de la Seguridad de la Información. Compone el grueso del estándar, basado en el ciclo PDCA, en el que, en cada etapa del ciclo requiere, mediante la realización de diferentes actividades:
    - *Plan*: definir los requisitos, evaluar los riesgos, decidir qué controles son aplicables.
    - *Do*: implementar y operar el SGSI (todos los controles elegidos en el paso anterior, más los ya implementados con anterioridad).
    - *Check*: monitorizar y revisar el SGSI.
    - *Act*: mantener y mejorar de manera contínua el SGSI.

  También especifica ciertos documentos que son requeridos y deben ser controlados, y define qué registros que deben ser generados y controlados, como pruebas de la operación del SGSI.
- **Sección 5**. Responsabilidad de la Dirección. La dirección debe demostrar su compromiso con el SGSI, principalmente mediante la asignación adecuada de recursos para implementar y operar el SGSI.
- **Sección 6**. Auditorías Internas del SGSI. La organización debe llevar a cabo auditorías periódicas para asegurar que el SGSI incorpora los controles adecuados y que estos funcionan de manera efectiva.
- **Sección 7**. Revisión por parte de la Dirección. La dirección debe revisar la adecuación y efectividad del SGSI al menos una vez al año, evaluando las oportunidades de mejora y la necesidad de cambios.
- **Sección 8**. Mejora del SGSI. La organización debe mejorar de manera contínua el SGSI mediante la evaluación, y cuando sea necesario, realizar cambios para asegurar la adecuación y efectividad. También debe abordar la no conformidad, y cuando sea posible, prevenir asuntos recurrentes.

3.1.2 ISO/IEC 27002

Este documento [31] presenta una serie buenas prácticas, en forma de técnicas de seguridad de la información, que no conforma un verdadero estándar. Es empleado tanto por organizaciones, para guiarse en la implementación de controles concretos, sin otro ánimo, como para otras que desean seguir la norma 27001 y/o conseguir la certificación de su SGSI.

El documento presenta 33 objetivos de control y 133 controles, donde para cada uno de ellos se presenta una descripción, una guía de implementación, y otras informaciones relativas, agrupados en diferentes categorías y subcategorías. Las categorías principales son:

- Evaluación y Tratamiento del Riesgo
- Política de Seguridad
- Aspectos Organizativos de la SI
- Gestión de Activos
- Seguridad ligada a los Recursos Humanos
- Seguridad Física y del Entorno
- Gestión de Comunicaciones y Operaciones
- Control de Acceso
- Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información

- Gestión de Incidentes de SI
- Gestión de la Continuidad de Negocio
- Cumplimiento

La agrupación en categorías y subcategorías puede verse gráficamente la figura EA.2.

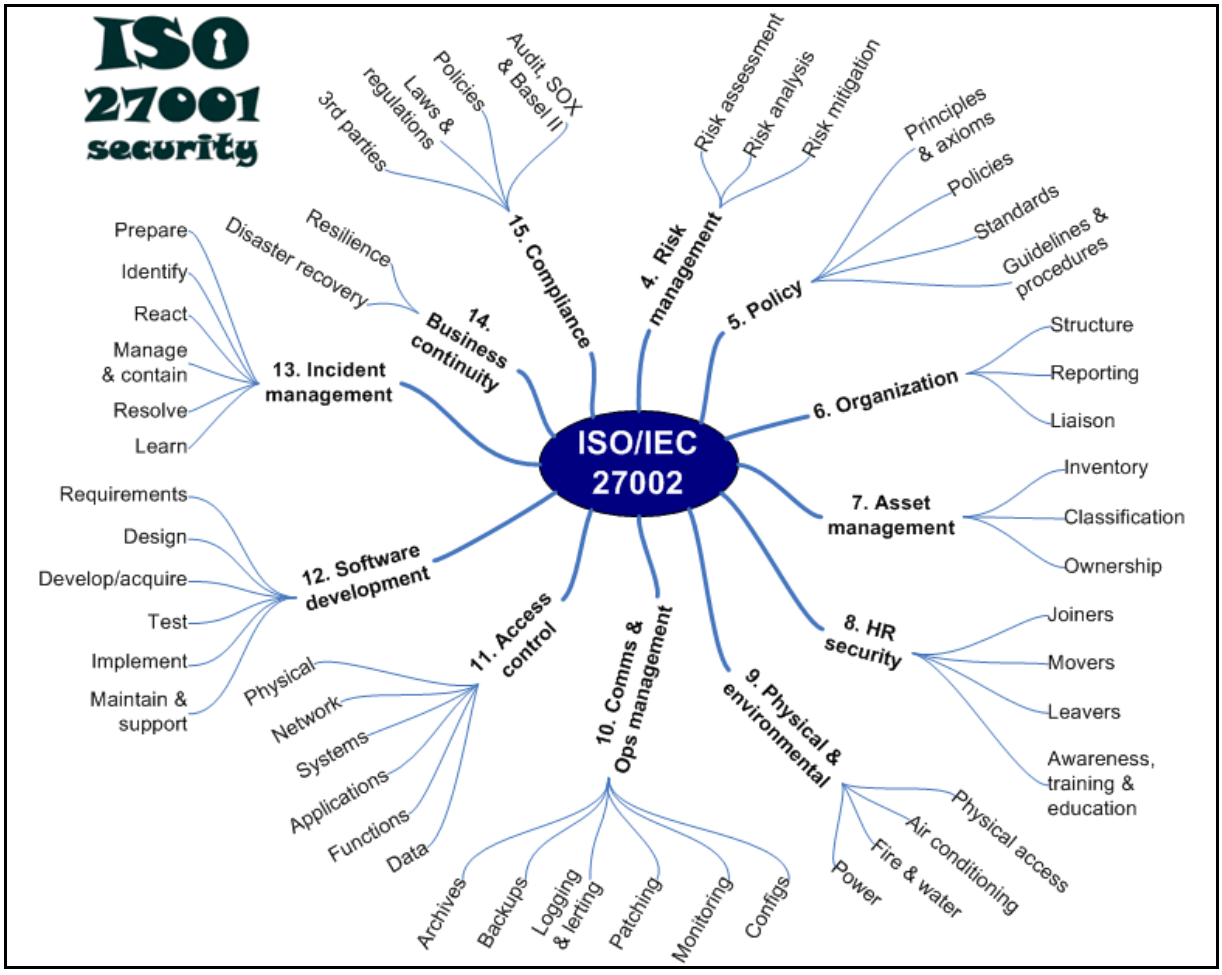
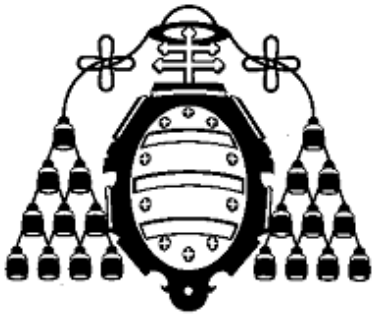


Figura EA.2. Mapa mental de las secciones del estándar que describen las categorías de controles [34]



UNIVERSIDAD DE OVIEDO

ESCUELA POLITÉCNICA DE INGENIERÍA DE GIJÓN

MÁSTER EN INGENIERÍA INFORMÁTICA

TRABAJO FIN DE MÁSTER

SISTEMA DE GESTIÓN DE LA CIBERSEGURIDAD INDUSTRIAL

-SISTEMA DE GESTIÓN DE LA CIBERSEGURIDAD INDUSTRIAL-

Pablo Sánchez Fernández

Junio de 2013

1 INTRODUCCIÓN

1.1 Objetivo y ámbito

Esta norma tiene por objetivo la definición de una guía práctica para el establecimiento de un Sistema de Gestión de la Ciberseguridad Industrial, especificando los requisitos y las apartados necesarios para la gestión integral de la ciberseguridad, considerando las fases de creación, implementación, operación, supervisión, revisión, mantenimiento y mejora del sistema.

Está orientada a organizaciones de cualquier tipo, que cuenten entre sus infraestructuras de información con redes y sistemas de control industrial.

Para ayudar a la aplicación de esta norma, y contribuyendo con el enfoque práctico de la misma, se incluyen una serie de anexos sobre controles de seguridad, lista de documentación a generar por el SGCI y listas de amenazas y vulnerabilidades.

1.2 Estándares y guías consideradas

Para la elaboración de esta norma, se han tenido en cuenta multitud de estándares y guías, tanto del ámbito de la protección de los sistemas de control industrial, como de la seguridad de las tecnologías de la información.

Parte de la redacción de la norma, es una adaptación y traducción de alguna de estos estándares y guías, adecuándose a la estructura del Sistema de Gestión de la Ciberseguridad Industrial. Aquellos puntos del documento que resulten de alguna manera de la adaptación, de forma parcial o total, o estén íntimamente relacionados con aspectos de la documentación tenida en consideración, aparecerá una referencia al documento y apartado correspondientes.

A continuación se listan los documentos de los que se ha adaptado alguno de sus contenidos para la redacción de esta norma, y sus abreviaturas, tal y como aparecerán en el texto:

- ANSI/ISA-99.02.01-2009 Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program. Referenciado por [ANSI/ISA 99] y los apartados y subapartados correspondientes..
- CCN-STIC-480 Guía de Seguridad de las TIC . Referenciado por [CCN-STIC-480] y los apartados y subapartados correspondientes.
- ISO/IEC 27001 Information technology - Security techniques - Information security management systems - Requirements . Referenciado por [SO/IEC 27001] y los apartados y subapartados correspondientes.
- NIST SP 800-82 Guide to Industrial Control Systems (ICS) Security. Referenciado por [NIST SP 800-82] y los apartados y subapartados correspondientes.

1.3 Ciclo de Vida

Este documento se basa en el modelo PDCA ("*Plan, Do, Check, Act*"), que marcará las cuatro etapas de ciclo de vida del proceso general del SGCI (Creación, Implementación y Operación, Supervisión y Revisión, y Mantenimiento y Mejora) y de todos sus procesos. Este modelo está orientado a la mejora contínua de la calidad, mediante la repetición de las cuatro fases del ciclo de manera que las salidas de cada una de las fases, serán las entradas de la siguiente, y finalmente, los resultados obtenidos en la fase final de un ciclo ("*Act*"), aportarán las entradas necesarias para la primera fase de la siguiente iteración del ciclo.

2 TÉRMINOS Y ACRÓNIMOS

Relación de los términos utilizados en el presente documento, adoptados de fuentes industriales, de documentación técnica y de guías y estándares.

1. **Acceso remoto**: comunicación o uso de activos o sistemas dentro de un determinado perímetro desde cualquier localización fuera de dicho perímetro.
2. **Activo**: objeto físico o lógico perteneciente o bajo custodia de una organización, que posee un cierto valor real o percibido para la organización.
3. **Ataque**: método por el que un individuo, mediante un sistema informático, intenta tomar el control, desestabilizar o dañar otro sistema informático.
4. **Autenticación**: medida de seguridad diseñada para establecer la validez de una transmisión, mensaje u origen, o los medios para verificar una autorización individual para acceder a categorías específicas de información.
5. **Autorización**: derecho o permiso que es otorgado a una entidad del sistema para acceder a un recurso del sistema.
6. **Backup**: copia de los datos originales que se realiza con el fin de disponer de un medio de recuperarlos en caso de su pérdida.
7. **Bot-net**: conjunto de robots informáticos que se ejecutan de manera autónoma y automática, normalmente de manera inadvertida para sus propietarios, y controlada de manera remota, con el propósito de utilizar los equipos infectados para envío de spam, descarga de ficheros de gran volumen, o realización de ataques de denegación de servicio.
8. **Brecha de seguridad**: 1. acto desde el exterior de la organización que esquiva o contraviene las políticas de seguridad, las prácticas o los procedimientos.
9. **Ciberseguridad**: es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno.
10. **Control**: procedimiento o mecanismo tecnológico que reduce el riesgo
11. **Cuenta de acceso**: función de control de acceso que permite a un usuario acceder a un conjunto particular de datos, funciones o cierto equipamiento.
12. **DCS**: acrónimo de Distributed Control System. Sistema de control en el que los elementros que realizan el control no se encuentran en una ubicación centralizada sino distribuidos sobre todo el sistema, donde cada subsistema se encuentra controlado por uno o más controladores.
13. **DHCP**: acrónimo de Dynamic Host Configuration Protocol. Protocolo para la asignación parámetros de red a dispositivos dentro de una red de manera automática.
14. **DNS**: acrónimo de Domain Name System. sistema de nomenclatura jerárquica para computadoras, servicios o cualquier recurso conectado a Internet o a una red privada.
15. **Equipamiento ambiental:**
16. **Firewall**: puerta de enlace entre redes que restringe el tráfico de datos desde y hacia una de las redes conectadas, considerada la interna al firewall, y de dicha forma es capaz de proteger los recursos conectados a la red contra amenazas de la otra red, la considerada externa al firewall.
17. **HSE**: acrónimo de Health, Safety, and Environment. Responsabilidad de proteger la salud de los trabajadores y de la comunidad circundante (surrounding), y mantener la gestión ambiental.
18. **ICS**: acrónimo de Industrial Control System.Sistemas de control industrrial, abarcando varios tipos de sistemas de control, incluyendo sistemas SCADA, sistemas DCS y otras configuraciones basadas en PLCs.

19. **IDS**: acrónimo de Intrusion Detection System. Servicio de seguridad que monitoriza y analiza los eventos de la red o el sistema con el propósito de encontrar y proporcionar avisos en tiempo real, o casi, sobre los intentos de acceso a recursos no autorizados.
20. **IED**: acrónimo de Intelligent Electronic Device. Dispositivo electrónico multifunción que presenta algún tipo de inteligencia local.
21. **Incidente**: evento que no es parte de la operación que se espera de un sistema o servicio, que causa o puede causar una interrupción o una reducción en la calidad del servicio proporcionada por el sistema.
22. **IPS**: acrónimo de Intrusion Protection System. Sistema que puede detectar actividades de intrusión y es capaz de detener la actividad, idealmente antes de que dicha actividad alcance su objetivo.
23. **Log**: registro oficial de eventos durante un rango de tiempo en particular.
24. **Malware**: software que tiene como objetivo infiltrarse o dañar una computadora o Sistema de información sin el consentimiento de su propietario.
25. **Norma**: regla que se debe seguir o a que se deben ajustar las conductas, tareas, actividades, etc.
26. **Parche**: pieza de software diseñada para solventar problemas mediante el cambio o actualización de un programa o sus datos de soporte, incluyendo la solución de vulnerabilidades de seguridad y otros fallos, y la mejora de la usabilidad y el rendimiento.
27. **Phishing**: envío de mensajes electrónicos que, aparentando provenir de fuentes fiables , intentan obtener datos confidenciales del usuario,con el ánimo de ser usados posteriormente en algún tipo de fraude.
28. **PLC**: acrónimo de Programmable Logic Controller. Dispositivo programable basado en microprocesador usado en la industria para controlar líneas de ensamblaje, maquinaria y otros tipos de equipamiento mecánico, eléctrico y electrónico de planta.
29. **PSM**: acrónimo de Process Safety Management. Gestión de la seguridad de los procesos en relación a la liberación accidental de líquidos y gases en procesos en los que estén implicados productos químicos o biológicos peligrosos.
30. **RTU**: acrónimo de Remote Terminal Unit. Dispositivo basado en microprocesador que sirve de interfaz entre objetos del mundo físico y un sistema de control mediante la transmisión de datos de telemetría.
31. **SGCI**: acrónimo de Sistema de Gestión de la Ciberseguridad Industrial
32. **SO**: acrónimo de Sistema Operativo. Programa o conjunto de programas que en un sistema informático gestiona los recursos de hardware y provee servicios a los programas de aplicación, ejecutándose en modo privilegiado respecto de los restantes.
33. **Spamming**: abuso de cualquier tipo de sistema de mensajería electrónica
34. **Spyware**: software que recopila información de un ordenador y después transmite esta información a una entidad externa sin el conocimiento o el consentimiento del propietario del ordenador.
35. **VLAN**: Virtual Local Area Network. Grupo de dispositivos en una o más LANs que son configurados de tal manera que se pueden comunicar como si estuvieran conectados al mismo cable, cuando en realidad están localizados en un segmento diferente de LAN
36. **VPN**: Virtual Private Network. Una red privada virtual o VPN, es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada, como por ejemplo Internet.

3 ESTRUCTURA DEL DOCUMENTO

El documento está estructurado en cuatro partes principales:

- **Sistema de Gestión de la Ciberseguridad Industrial**. Contiene los requisitos y directivas del propio sistema de gestión, y se divide en cuatro capítulos, según las cuatro fases del ciclo de vida del SGCI.
- **Anexo A. Controles de Seguridad**. Contiene una lista no exhaustiva de controles de seguridad que pueden ser implementados por la organización para mitigar los riesgos que se hayan considerado.
- **Anexo B: Lista de documentos del SGCI**. Lista de documentos a implementar durante el ciclo de vida del SGCI.
- **Anexo C: Listas de amenazas y vulnerabilidades**. Listas de los agentes y categorías de amenazas, y los tipos de vulnerabilidades.

4 SISTEMA DE GESTIÓN DE LA CIBERSEGURIDAD INDUSTRIAL

4.1 Creación del SGCI

4.1.1 Alcance

4.1.1.1 Definir el alcance del SGCI

La organización debe poner por escrito de manera formal el ámbito y alcance del programa de ciberseguridad industrial, explicando los objetivos estratégicos, los procesos y la planificación temporal del SGCI.

4.1.2 Política del SGCI

4.1.2.1 Definir la política del SGCI

La organización debe redactar una política del SGCI acorde con otras políticas de seguridad existentes de la organización, y que tenga en cuenta: [ISO/IEC 27001 4.2.1b]

a. Orientación general sobre directrices y principios de actuación en materia de ciberseguridad industrial.
b. La tolerancia al riesgo de la organización.
c. Los requisitos de la actividad de la organización, así como otros requisitos legales, o reglamentarios del sector.
d. Las estrategias de gestión de riesgos de la organización.

4.1.3 Organización de la seguridad [ANSI/ISA 99 4.3.2.3]

4.1.3.1 Obtener el apoyo de la dirección [ANSI/ISA 99 4.3.2.3.1], [ISO/IEC 27001 5.1]

La organización debe contar con el apoyo de los órganos de gestión y personas encargadas de la gestión de los ICS para la creación de un programa de ciberseguridad industrial. La dirección debe apoyar el programa de ciberseguridad industrial proporcionando y gestionando los recursos necesarios para llevar a cabo todas sus fases.

4.1.3.2 Establecer las organizaciones involucradas [ANSI/ISA 99 4.3.2.3.2]

Debe crearse una red o estructura de las partes interesadas, establecido por la dirección, con el propósito de proporcionar supervisión y orientación sobre ciberseguridad industrial.

4.1.3.3 Definir el equipo de ciberseguridad, roles y responsabilidades [ANSI/ISA 99 4.3.2.3.3], [ANSI/ISA 99 4.3.2.4]

Debe definirse la composición de un equipo de ciberseguridad, integrado por miembros de las partes interesadas, con conocimientos de distintas áreas, para quienes se han de definir los roles y las responsabilidades en materia de ciberseguridad industrial y las actividades de seguridad física relacionadas, así como las de otras personas o entidades fuera del equipo, involucradas en la ciberseguridad industrial.

4.1.4 Identificación, clasificación y evaluación de riesgos [ANSI/ISA 99 4.2.3], [ISO/IEC 27001 4.2.1 c-f]

4.1.4.1 Seleccionar una metodología de evaluación de riesgos [ANSI/ISA 99 4.2.3.1], [ISO/IEC 27001 4.2.1 c]

La organización debe seleccionar una metodología de análisis y evaluación de riesgos, que identifique y priorice los riesgos, basados en las amenazas, vulnerabilidades y consecuencias específicos de los activos ICS.

4.1.4.2 Determinar los factores desencadenantes de la evaluación de riesgos [ANSI/ISA 99 4.2.3.10]

La organización debe determinar los factores que desencadenarán una nueva evaluación de riesgos, que deben tener en cuenta, los cambios de envergadura en los sistemas y la adaptación a nuevas normativas y leyes.

4.1.4.3 Desarrollar listas de amenazas y vulnerabilidades del sector

La organización debe desarrollar listas de amenazas y vulnerabilidades específicas de su sector de actividad, que ayuden a determinar los riesgos (ver tabla de categorías de amenazas y vulnerabilidades sobre ICS del Anexo B).

4.1.4.4 Desarrollar criterios de aceptación de riesgo y determinar niveles aceptables de riesgo. [ISO/IEC 270014.2.1 c2]

La organización debe desarrollar unos criterios para aceptar los riesgos de seguridad, y determinar los niveles aceptables de riesgo, teniendo en cuenta la criticidad de su actividad y de las consecuencias para terceras partes.

4.1.4.5 Realizar una evaluación de riesgos de alto nivel [ANSI/ISA 99 4.2.3.3]

La organización debe desarrollar unos criterios para aceptar los riesgos de seguridad, y determinar los niveles aceptables de riesgo, teniendo en cuenta la criticidad de su actividad y de las consecuencias para terceras partes.

4.1.4.6 Identificar e inventariar los sistemas de automatización industrial, los sistemas de control, y los activos de red: [ANSI/ISA 99 4.2.3.4], [NIST SP 800-82 4.2.5]

La organización debe identificar todos los activos ICS y de red involucrados, reunir datos sobre los dispositivos para caracterizar la naturaleza del riesgo, y agrupar los dispositivos en sistemas lógicos.

4.1.4.7 Identificar e inventariar dependencias de terceras partes [CCN-STIC-480 5.1.5 88]

Se debe identificar y registrar las empresas externas, clientes, proveedores y empresas de soporte, que tengan relación en la cadena de suministro del servicio o producto y que puedan afectar a los sistemas ICS, para poder identificar los riesgos relacionados con terceras partes.

4.1.4.8 Desarrollar diagramas simples de red [ANSI/ISA 99 4.2.3.5]

La organización debe desarrollar diagramas simples de red para cada uno de los sistemas integrados de manera lógica, mostrando los dispositivos más relevantes tipos de red y ubicaciones generales del equipamiento.

4.1.4.9 Priorizar sistemas [ANSI/ISA 99 4.2.3.6]

La organización debe desarrollar un criterio y asignar una prioridad en base a él para cada sistema lógico de control, para mitigar el riesgo.

4.1.4.10 Identificar los riesgos [ISO/IEC 27001 4.2.1 d]

Teniendo en cuenta la prioridad establecida para los sistemas, el ámbito del SGCI y sus activos y las dependencias de las terceras inventariadas:

a. Identificar las amenazas, generales y específicas del sector y sobre los ICS de la organización

b. Identificar las vulnerabilidades, generales y específicas del sector y de los ICS de la organización

c. Identificar los impactos en cuanto a pérdida de confidencialidad, integridad y disponibilidad sobre dichos activos.

4.1.4.11 Analizar y valorar los riesgos [ISO/IEC 27001 4.2.1 c]

a. Evaluar las consecuencias en la actividad de la empresa de los posibles fallos de seguridad

b. Evaluar la probabilidad de que se produzcan dichos fallos

c. Evaluar los impactos asociados a los activos y controles implementados

d. Estimar los niveles de riesgo

e. Clasificar los riesgos como aceptables o no, de acuerdo con los criterios establecidos en 4.1.4.4.

4.1.4.12 Evaluar las opciones de tratamiento de riesgos [ISO/IEC 27001 4.2.1 f]

La organización debe decidir, para los riesgos identificados, y en base a los criterios de aceptación de riesgos, si se desarrollarán y aplicarán controles para mitigarlos, se asumirán, se evitarán, se transferirán a otras partes, u otras acciones que pueda llevar a cabo.

4.1.4.13 Integrar los resultados de evaluación de riesgos [ANSI/ISA 99 4.2.3.11]

Otras evaluaciones realizadas por la organización, en materia de seguridad física, de salud, de medio ambiente y de ciberseguridad deben ser integradas en la evaluación de para comprender el riesgo absoluto sobre los activos.

4.1.4.14 Documentar la evaluación de riesgos [ANSI/ISA 99 4.2.3.13]

La metodología de evaluación de riesgos y los resultados obtenidos deben ser documentados.

4.1.5 Aprobación del SGCI

4.1.5.1 Aprobación del riesgo residual [ISO/IEC 27001 4.2.1 h]

La dirección debe aprobar los riesgos residuales que resultarán de las decisiones tomadas de tratamiento de riesgos, en la fase de evaluación.

4.1.5.2 Autorización del SGCI [ISO/IEC 27001 4.2.1 i]

La dirección debe autorizar a los miembros del equipo de ciberseguridad (4.1.3.3) así como la implementación y operación del SGCI.

4.2 Implementación y Operación del SGCI

4.2.1 Selección de controles de seguridad [ISO/IEC 27001 4.2.1 g]

4.2.1.1 Seleccionar controles de seguridad

Deben definirse los controles adecuados para satisfacer los requisitos resultantes de la evaluación de riesgos, teniendo en cuenta:

a. La evaluación de tratamiento de riesgos (4.1.4.14)

b. Los requisitos de la actividad de la organización, así como otros requisitos legales, o reglamentarios del sector.

La lista de controles del Anexo A comprende una relación no exhaustiva de controles de seguridad, de entre los cuales deben seleccionarse los adecuados, así como otros controles no descritos en dicho anexo y que resultaran oportunos.

4.2.1.2 Redactar una lista de controles [ISO/IEC 27001 4.201 j]

Debe elaborarse una lista que incluya:

a. Los controles ya implementados
b. Los controles seleccionados y su relación con el riesgo o riesgos a mitigar.

4.2.1.3 Establecer métodos de medición [ISO/IEC 27001 4.2.2 d]

Deben definirse e implementarse métricas y métodos de medición de la eficacia para cada uno de los controles implementados.

4.2.2 Tratamiento de riesgos

4.2.2.1 Redactar plan de tratamiento de riesgos [ISO/IEC 27001 4.2.2 a]

Debe redactarse un documento que recoja el plan de tratamiento de riesgos, para gestionar los riesgos evaluados, y debe incluir las acciones a realizar, los recursos a utilizar, las responsabilidades y las prioridades.

4.2.2.2 Implementar plan de tratamiento de riesgos [ISO/IEC 27001 4.2.2 b]

Deben implementarse las medidas recogidas en el plan de tratamiento de riesgos, teniendo en cuenta las condiciones reflejadas en dicho plan.

4.2.2.3 Implementar controles seleccionados [ISO/IEC 27001 4.2.2 c]

Implementar los controles seleccionados (4.2.1.1, 4.2.1.2) y operarlos para que cumplan su cometido.

4.2.3 Formación y concienciación [ANSI/ISA 99 4.3.2.4], [ISO/IEC 27001 5.2.2]

4.2.3.1 Determinar competencias necesarias del personal y determinar sus carencias [ISO/IEC 27001 5.2.2 a]

Deben examinarse las competencias relacionadas con la ciberseguridad industrial necesarias para todo el personal de la organización, y determinar las carencias existentes.

4.2.3.2 Elaborar e impartir un plan de formación y concienciación

A partir de las carencias encontradas, elaborar un plan, teniendo en cuenta los siguientes aspectos:

a. Proporcionar formación general sobre procedimientos e instalaciones [ANSI/ISA 99 4.3.2.4.2]: debe proporcionarse formación sobre los procedimientos correctos de seguridad y el uso correcto de las instalaciones de procesamiento de información a todo el personal.
b. Proporcionar formación específica para el personal involucrado en SGCI [ANSI/ISA 99 4.3.2.4.3]: el personal involucrado en la gestión de riesgos, ingeniería de ICS, administración, mantenimiento, y otras tareas que tengan impacto sobre el SGCI deben ser formados sobre los objetivos de seguridad y las operaciones industriales de la organización, para dichas tareas.
c. Emprender iniciativas de concienciación [ISO/IEC 27001 5.2.2 párrafo final]: deben tenerse en cuenta otras iniciativas adicionales a la formación para que el personal sea consciente de la trascendencia de las actividades de ciberseguridad industrial.

4.2.3.3 Mantener registros de formación [ANSI/ISA 99 4.3.2.4.9], [ISO/IEC 27001 5.2.2 d]

Deben crearse y mantenerse registros de la formación impartida, los períodos y las aptitudes y cualificaciones obtenidas.

4.2.3.4 Establecer métodos de medición

Deben definirse e implementarse métricas y métodos para medir la eficacia de la formación impartida a los empleados de la organización dentro del plan de formación y concienciación.

4.2.4 Mantener el inventario de activos del SGCI [CCN-STIC-480 5.3.1]

4.2.4.1 Mantener actualizado el inventario de activos

Debe mantenerse actualizado el inventario de activos, bien por medios automáticos o mediante procedimientos adecuados que garanticen que se registren todos los cambios realizados sobre los activos.

4.2.5 Establecer métodos de medición del SGCI [ISO/IEC 27001 4.2.2 f]

4.2.5.1 Establecer métodos de medición de conformidad [ANSI/ISA 99 4.4.2.3]

Deben definirse e implementarse métricas y métodos de medición de la conformidad y cumplimiento de políticas, procesos y procedimientos del SGCI.

4.2.6 Gestionar la respuesta ante incidentes [ISO/IEC 27001 4.2.2 h], [ANSI/ISA 99 4.3.4.5]

4.2.6.1 Implementar un plan de respuesta ante incidentes [ANSI/ISA 99 4.3.4.5.1]

La organización debe implementar un plan de respuesta ante incidentes que identifique el personal responsable implicado y defina las acciones a realizar por las personas indicadas.

4.2.6.2 Comunicar el plan de respuesta ante incidentes [ANSI/ISA 99 4.3.4.5.2]

El plan de respuesta ante incidentes debe ser comunicado a todas las personas y organizaciones apropiadas.

4.2.6.3 Establecer un procedimiento de informe y tratamiento ante eventos o actividades inusuales [ANSI/ISA 99 4.3.4.5.3]

La organización debe establecer un procedimiento de informe y tratamiento de eventos o actividades que se consideren fuera de lo normal, y que pudieran ser en realidad, incidentes de ciberseguridad.

4.2.6.4 Instruir a los empleados en el informe de incidentes de ciberseguridad [ANSI/ISA 99 4.3.4.5.4]

Los empleados deben ser instruidos en los procedimientos para el informe de incidentes de ciberseguridad y su responsabilidad ante ellos.

4.2.6.5 Informar de incidentes de ciberseguridad de manera temprana [ANSI/ISA 99 4.3.4.5.5]

El personal debe informar de todos los incidentes de ciberseguridad producidos de manera puntual.

4.2.6.6 Identificar y responder a incidentes [ANSI/ISA 99 4.3.4.5.6]

Si tras un informe, el personal responsable identifica un incidente, la organización debe responder a la mayor brevedad de acuerdo con los procedimientos establecidos.

4.2.6.7 Identificar brechas de ciberseguridad exitosas y fallidas [ANSI/ISA 99 4.3.4.5.7]

La organización debe implementar procedimientos para identificar las brechas o incidentes de seguridad detectados que resultaron no tener impacto, y los que resultaron exitosas y con algún impacto.

4.2.6.8 Documentar el detalle de los incidentes [ANSI/ISA 99 4.3.4.5.8]

Los detalles de cada incidente identificado deben ser documentados para registrar el incidente, la respuesta, las lecciones aprendidas, y cualquier acción llevada a cabo que modifique el SGCI a la luz del incidente.

4.2.6.9 Comunicar el detalle de los incidentes [ANSI/ISA 99 4.3.4.5.9]

Los detalles documentados de cada incidente identificado deben ser comunicados a todas las personas y organizaciones apropiadas, de manera puntual.

4.2.6.10 Abordar y corregir problemas descubiertos [ANSI/ISA 99 4.3.4.5.10]

La organización debe tener una metodología para tratar problemas que hayan sido descubiertos y asegurar que se corrigen.

4.2.6.11 Efectuar simulacros [ANSI/ISA 99 4.3.4.5.11]

Deben llevarse a cabo simulacros de manera periódica, para testear la gestión de respuesta ante incidentes.

4.2.7 Gestionar implementaciones y mantenimientos de sistema [ANSI/ISA 99 4.3.4.3], [CCN-STIC-480 5.1.4]

4.2.7.1 Gestionar implementaciones y mantenimientos de sistema [ANSI/ISA 99 4.3.4.3], [CCN-STIC-480 5.1.4]

Deben definirse políticas generales y procedimientos sobre nuevos componentes e implementaciones, y los requisitos de ciberseguridad concretos para cada nuevo componente, dispositivo, o implementación a incluir dentro de los sistemas de control industrial, teniendo en cuenta las políticas y procedimientos definidos para la zona/entorno en la que se llevarán a cabo.

4.2.7.2 Testear funciones de seguridad y capacidades de componentes[ANSI/ISA 99 4.3.4.3.1]

Las funciones y capacidades de seguridad de cada nuevo componente a integrar en el sistema, deben ser testeadas de manera conjunta con los componentes existentes, para asegurar que el sistema entero alcanza los niveles de seguridad deseados.

4.2.7.3 Realizar pruebas de seguridad de implementaciones [CCN-STIC-480 5.1.4.2 82]

Deben llevarse a cabo pruebas para asegurar que las nuevas implementaciones alcanzan los niveles de seguridad deseados, en todas las fases del ciclo de vida del proyecto.

4.2.7.4 Desarrollar e implementar un sistema de gestión de cambios [ANSI/ISA 99 4.3.4.3.2]

Debe desarrollarse e implementarse un sistema para gestionar los cambios que hayan de realizarse sobre el entorno de ICS. El proceso de gestión de cambios debe seguir los principios de la segregación de tareas para evitar problemas de conflictos de interés.

4.2.7.5 Evaluar todos los riesgos de cambios de ICS [ANSI/ISA 99 4.3.4.3.3]

Los cambios propuestos a realizar sobre el entorno de ICS deben ser revisados, usando criterios bien definidos, para controlar el potencial impacto sobre los riesgos de HSE y ciberseguridad por personal conocedor de las operaciones industriales y los sistemas ICS.

4.2.7.6 Integrar los procedimientos de gestión de cambios de ciberseguridad y gestión de seguridad de procesos [ANSI/ISA 99 4.3.4.3.5]

El procedimiento de gestión de cambios de ciberseguridad deberá integrarse con los procedimientos de gestión seguridad de procesos (PSM).

4.2.7.7 Establecer y documentar un procedimiento de gestión de parches [ANSI/ISA 99 4.3.4.3.7], [CCN-STIC-480 5.3.4.1]

Debe establecerse, documentarse y seguirse, un procedimiento para la gestión de parches que tenga en cuenta:

a. Mecanismos de vigilancia de actualizaciones de proveedores
b. Parcheo en entornos de alta disponibilidad o preproducción
c. Soporte de los proveedores
d. Programación de calendarios y horarios de parcheo
e. Pruebas previas
f. Procedimiento habitual y de emergencia, y de regresión en caso de fallo

4.2.7.8 Establecer y documentar un procedimiento de gestión de antivirus/malware [ANSI/ISA 99 4.3.4.3.8]

Debe establecerse, documentarse y seguirse, un procedimiento para la gestión de antivirus/malware que tenga en cuenta:

a. Definición de la lista de activos que requieran de software antivirus e instalación
b. Frecuencia y modo de actualización
c. Comunicación y tratamiento de las alertas generadas por la gestión de incidentes

4.2.7.9 Establecer un procedimiento de backup y restauración[ANSI/ISA 99 4.3.4.3.9]

Debe establecerse un procedimiento para realizar backup y restauración de sistemas y proteger las copias de backup, y dicho procedimiento debe ser usado.

4.2.8 Gestión de empresas externas [CCN-STIC-480 5.1.5]

4.2.8.1 Mantener actualizado el inventario de terceros

Debe mantenerse actualizado el inventario de terceros, y la información relativa a ellos.

4.2.8.2 Suscribir y registrar acuerdos y cláusulas de seguridad

Deben suscribirse y registrarse acuerdos con los terceros cuando sea necesario, que garanticen los requisitos de ciberseguridad, y debe tenerse en cuenta:

a. Acuerdos de no divulgación de información sensible: si la empresa externa tiene acceso a información sensible, no debe utilizarla sin el permiso de la organización propietaria de la información.
b. Existencia de procedimientos y controles de seguridad interna del tercero: petición de garantías al tercero sobre los procedimientos y controles de seguridad de la información y ciberseguridad.
c. Derecho a auditar: si se considera necesario el derecho a auditar los servicios y locales de terceros.
d. Acuerdos de nivel de servicio: asegurar mediante acuerdos de nivel de servicio las necesidades de la organización de una manera adecuada.
e. Responsabilidad: donde los sistemas o conexiones superan los límites de la organización, se necesitan acuerdos de responsabilidad de seguridad del proveedor.
f. Pruebas/certificaciones de seguridad: exigencia de que el tercero realice pruebas u obtenga certificaciones respecto de sus sistemas de seguridad.
g. Garantía de conexiones y dependencias remotas: exigencia de asegurar las conexiones remotas entre la organización y terceros. Tanto la información que transcurre a través de la conexión, como los almacenados en dependencias remotas debe estar debidamente protegida.

4.2.9 Plan de Continuidad del Negocio [ANSI/ISA 99 4.3.2.5]

4.2.9.1 Definir y priorizar objetivos de recuperación [ANSI/ISA 99 4.3.2.5.1]

La organización debe primeramente especificar cuáles son los objetivos de recuperación para los sistemas involucrados, y priorizarlos, basándose en las necesidades del negocio.

4.2.9.2 Determinar el impacto y las consecuencias para cada sistema [ANSI/ISA 99 4.3.2.5.2]

La organización debe determinar el impacto sobre cada sistema debido a una interrupción de importancia, y las consecuencias asociadas a la pérdida de uno o más sistemas.

4.2.9.3 Desarrollar e implementar un plan de continuidad del negocio [ANSI/ISA 99 4.3.2.5.3]

Debe desarrollarse e implementarse un plan (o varios planes) de continuidad del negocio para asegurar que los procesos de negocio puedan ser restablecidos de acuerdo con los objetivos de recuperación establecidos. El plan debe tener en cuenta:

a. Formación de un equipo de continuidad del negocio [ANSI/ISA 99 4.3.2.5.4]: debe formarse un equipo de continuidad de negocio, incluyendo propietarios de procesos de ICS y otros procesos. En caso de una interrupción de importancia, el equipo deberá determinar la prioridad de los sistemas críticos para restablecer la operación.

b. Definición y comunicación de roles y responsabilidades [ANSI/ISA 99 4.3.2.5.5]: deben definirse y comunicarse los roles y responsabilidades específicos para cada parte del plan.

c. Procedimientos de backup de soporte al plan de continuidad [ANSI/ISA 99 4.3.2.5.6]: la organización debe crear procedimientos de backup y restauración que den soporte al plan de continuidad del negocio.

4.2.10 Gestión de la Información y Documentos [ANSI/ISA 99 4.3.4.4], [ISO/IEC 27001 4.3.2, ISO/IEC 27001 4.3.3]

4.2.10.1 Establecer una política general de gestión de activos de información

Debe establecerse una política que proporcione guía sobre los objetivos de seguridad a alcanzar en materia de gestión de activos de información, el ámbito de aplicación, y los recursos a utilizar.

4.2.10.2 Definir niveles de clasificación de activos de información [ANSI/ISA 99 4.3.4.4.2]

Deben definirse diferentes niveles de clasificación de información, con el fin de otorgar el nivel de protección adecuada a la información, limitando su acceso y control, incluyendo compartición, copia, transmisión, y distribución de la información.

4.2.10.3 Desclasificar y reclasificar los activos de información

Para cada activo de información debe mantenerse el nivel de clasificación durante un período de tiempo establecido, de manera que sea desclasificada o degradada tan pronto como sea posible sin poner en riesgo la seguridad. El período de tiempo para la reclasificación, puede depender del nivel de clasificación, y debe revisarse la clasificación de todos los activos de información de manera regular.

4.2.10.4 Clasificar los activos de información del SGCI [ANSI/ISA 99 4.3.4.4.3]

Todos los activos de información, lógicos y físicos dentro del alcance del SGCI, deben ser clasificados mediante la aplicación del nivel de clasificación apropiado, teniendo en cuenta las consecuencias de una posible revelación o modificación de dichos activos.

4.2.10.5 Asegurar un control apropiado de los activos de información [ANSI/ISA 99 4.3.4.4.4]

Deben desarrollarse políticas y procedimientos detallando la retención, la protección física, la destrucción y la eliminación de todos los activos de información, basándose en su clasificación, incluyendo los activos electrónicos y papel, considerando además requisitos legales o regulatorios.

4.2.10.6 Asegurar la recuperación de activos de información a largo plazo [ANSI/ISA 99 4.3.4.4.5]

Deben tomarse las medidas adecuadas para asegurar que los documentos, registros y cualquier activo de información, pueda ser recuperado a largo plazo, convirtiendo los datos a nuevos formatos, reteniendo equipamiento antiguo para poder leer los datos, u otras medidas a tal efecto.

4.3 Supervisión y revisión del SGCI

4.3.1 Revisión de la Eficacia

4.3.1.1 Revisar la eficacia de los controles [ISO/IEC 27001 4.2.3 c]

Debe revisarse la eficacia de todos los controles implementados en la organización, basándose en las mediciones de eficacia tomadas, para asegurar que los controles cumplen con su cometido de manera eficaz, e identificar las mejoras a realizar en caso contrario.

4.3.1.2 Revisar el grado de conformidad y cumplimiento

Deben revisarse los resultados de las mediciones de conformidad y cumplimiento de políticas, procesos y procedimientos del SGSI, identificando los incumplimientos.

4.3.2 Formación y concienciación [ANSI/ISA 99 4.3.2.4], [ISO/IEC 27001 5.2.2]

4.3.2.1 Evaluar el programa de formación [ISO/IEC 27001 5.2.2 c], [ANSI/ISA 99 4.3.2.4.4]

Debe evaluarse la eficiencia del programa de formación para asegurar que se ha impartido la formación de manera adecuada y que el personal ha adquirido los conocimientos necesarios, basándose en las mediciones de eficacia tomadas, e identificar las mejoras a realizar en caso contrario.

4.3.2.2 Revisar el programa de formación [ANSI/ISA 99 4.3.2.4.5]

Debe revisarse el programa de formación para adaptarlo a las nuevas necesidades, y las nuevas amenazas y vulnerabilidades.

4.3.3 Revisión de la Medición del SGCI [ISO/IEC 27001 4.2.2 f]

4.3.3.1 Revisar métodos de medición de conformidad

Deben revisarse las métricas y métodos de medición de la conformidad y cumplimiento de políticas, procesos y procedimientos del SGCI, con el fin de adaptarlas de la mejor manera posible a la organización y su actividad, y detectar las posibles mejoras.

4.3.3.2 Revisar métodos de medición de eficacia de los controles [ISO/IEC 27001 4.2.2 d]

Deben revisarse las métricas y métodos de medición de la eficacia definidos e implementados para los controles, para identificar deficiencias y posibles mejoras.

4.3.4 Gestionar la respuesta ante incidentes [ISO/IEC 27001 4.2.2 h], [ANSI/ISA 99 4.3.4.5]

4.3.4.1 Revisar el plan de respuesta ante incidentes

La organización debe revisar periódicamente el plan de respuesta ante incidentes para asegurarse de que sigue siendo válido, teniendo en cuenta los posibles cambios organizativos, funcionales y de sistemas.

4.3.5 Gestionar implementaciones y mantenimientos de sistema [ANSI/ISA 99 4.3.4.3], [CCN-STIC-480 5.1.4], [CCN-STIC-480 5.3.4.1]

4.3.5.1 Revisar y mantener políticas y procedimientos de nuevos componentes e implementaciones [ANSI/ISA 99 4.3.4.3.6]

Las políticas y procedimientos de implementaciones y cambios deben ser revisadas para asegurar que las alteraciones en el sistema no incrementen los riesgos o la continuidad del negocio.

4.3.5.2 Revisar el procedimiento de gestión de cambios

Debe revisarse el procedimiento de gestión de cambios, teniendo en cuenta los cambios organizativos, funcionales o de sistemas, e identificando posibles mejoras.

4.3.5.3 Revisar el procedimiento de gestión de parches

Debe revisarse el procedimiento de gestión de parches, teniendo en cuenta los cambios organizativos, funcionales o de sistemas, así como los cambios en la entrega de parches y actualizaciones de los fabricantes, e identificar posibles mejoras.

4.3.5.4 Revisar el procedimiento de gestión de antivirus/malware

Debe revisarse el procedimiento de gestión de antivirus/malware, e identificar posibles mejoras.

4.3.5.5 Revisar el procedimiento de backup y restauración [ANSI/ISA 99 4.3.4.3.9]

Debe revisarse y probarse el procedimiento de backup y restauración con el fin de asegurar de que en caso necesario, puedan restaurarse las copias adecuadamente, e identificar posibles mejoras.

4.3.6 Gestión de empresas externas [CCN-STIC-480 5.1.5]

4.3.6.1 Revisión del cumplimiento de acuerdos y cláusulas de seguridad

Debe revisarse el cumplimiento de los acuerdos y las cláusulas de seguridad firmadas con terceras partes, y detectar aquellas partes que no han sido cumplidas.

4.3.7 Plan de Continuidad del negocio [ANSI/ISA 99 4.3.2.5]

4.3.7.1 Revisar el plan de continuidad del negocio

Debe revisarse el plan de continuidad del negocio, así como sus objetivos y prioridades, e identificar posibles mejoras.

4.3.7.2 Testear el plan de continuidad de negocio [ANSI/ISA 99 4.3.2.5.7]

El plan debe ser testeado de manera regular, redactar informes de resultados, e identificar las anomalías y mejoras.

4.3.8 Gestión de la información y documentos [ANSI/ISA 99 4.3.4.4], [ISO/IEC 27001 4.3.2], [ISO/IEC 27001 4.3.3]

4.3.8.1 Revisar procedimientos de gestión de activos de información [ANSI/ISA 99 4.3.4.4.1]

Deben revisarse los mecanismos y procedimientos de gestión de activos de información, relacionados con la clasificación, el control y la recuperación, con el objetivo de encontrar deficiencias y posibles mejoras.

4.3.8.2 Auditar las políticas y procedimientos de gestión de activos de información [ANSI/ISA 99 4.3.4.4.7]

Deben llevarse a cabo revisiones periódicas para verificar el cumplimiento de las políticas y procedimientos de gestión de activos de información y documentos.

4.3.9 Análisis externo de la Ciberseguridad

4.3.9.1 Monitorizar y evaluar las estrategias de CSMS de la industria [ANSI/ISA 99 4.4.3.6]

La organización debe monitorizar las buenas prácticas y recomendaciones que aparezcan en el sector industrial, para la evaluación y la mitigación de riesgos, y evaluar su aplicabilidad en el negocio y las actividades de la organización.

4.3.9.2 Monitorizar y evaluar la legislación aplicable relevante para la ciberseguridad [ANSI/ISA 99 4.4.3.7]

La organización debe monitorizar e identificar la legislación aplicable en materia de ciberseguridad y los cambios que se produzcan.

4.3.10 Sugerencias del personal

4.3.10.1 Requerir e informar de la realimentación del personal sobre sugerencias de seguridad [ANSI/ISA 99 4.4.3.8]

Debe procurarse la realimentación del personal sobre sugerencias en materia de seguridad, y debe informarse a la dirección de los defectos y oportunidades que de ellas se concluya.

4.3.11 Tratamiento de riesgos

4.3.11.1 Revisar las evaluaciones de riesgos [ISO/IEC 27001 4.2.3 d], [ANSI/ISA 99 4.2.3.12]

La organización debe revisar periódicamente las evaluaciones de riesgos e identificar aquellos riesgos que no consiguieron reducirse según lo previsto.

4.3.11.2 Revisar la frecuencia de evaluación de riesgos y los factores desencadenantes [ANSI/ISA 99 4.2.3.10]

La organización debe revisar la frecuencia con la que se realizan las evaluaciones de riesgos y los factores que desencadenan otras evaluaciones adicionales, para determinar si son adecuados.

4.3.11.3 Revisar la tolerancia de riesgo [ISO/IEC 27001 4.2.3 d], [ANSI/ISA 99 4.4.3.5]

La organización debe revisar la tolerancia al riesgo, para asegurarse de que los umbrales siguen siendo los aceptables.

4.3.11.4 Revisar la evaluación de vulnerabilidades [ANSI/ISA 99 4.2.3.13]

Debe revisarse la evaluación de vulnerabilidades del SGCI con el fin de identificar los cambios.

4.3.12 Auditorias [ANSI/ISA 99 4.4.2], [ISO/IEC 27001 6], [CCN-STIC-480 5.1.3]

4.3.12.1 Especificar la metodología del proceso de auditoría [ANSI/ISA 99 4.4.2.1]

El programa de auditoría debe especificar la metodología a usar para el proceso de auditoría.

4.3.12.2 Establecer un programa de auditoría

Debe establecerse un programa de auditoría, teniendo en cuenta las condiciones específicas en que se llevará a cabo la auditoría (dispersión geográfica de las plantas, lugares de reunión con personal de planta, entrada a entornos industriales, etc.)

4.3.12.3 Elaborar una lista de documentos del registro de auditoría [ANSI/ISA 99 4.4.2.4]

Debe elaborarse una lista de los documentos e informes necesarios que compondrán el registro de auditoría.

4.3.12.4 Llevar a cabo auditorías del SGCI periódicamente [ANSI/ISA 99 4.4.2.2]

De manera periódica, la organización debe realizar auditorías sobre el SGCI.

4.3.13 Revisión del SGCI

4.3.13.1 Revisión del SGCI por parte de la dirección: [ANSI/ISA 99 4.4.3], [ISO/IEC 27001 4.2.3 f]

La dirección debe:

a. Revisar la política del SGCI, con el fin de que se alinee con el contexto actual del negocio
b. Revisar el alcance del SGCI, para actualizar los objetivos y el ámbito del SGCI
c. Revisar el equipo de ciberseguridad, los roles y responsabilidades
d. Revisar los resultados de las auditorías
e. Identificar posibles mejoras del SGCI

4.4 Mantenimiento y Mejora del SGCI

4.4.1.1 Implementar en el SGCI las mejoras identificadas [ISO/IEC 27001 4.2.4 a]

Deben implementarse en el SGCI las mejoras identificadas mediante revisiones, pruebas y auditorías.

4.4.1.2 Aplicar las medidas correctivas y preventivas adecuadas [ISO/IEC 27001 4.2.4 b], [[ISO/IEC 27001 8.2, 8.3]

Deben llevarse a cabo las acciones correctivas y/o preventivas adecuadas para paliar las no conformidades detectadas, respecto de los requisitos del SGSI.

4.4.1.3 Comunicar medidas y mejoras a las partes interesadas [ISO/IEC 27001 4.2.4 c]

Deben comunicarse las medidas adoptadas así como las mejoras implementadas a las partes involucradas o interesadas, con un nivel de detalle adecuado para cada una de ellas.

4.4.1.4 Asegurar que las medidas y las mejoras alcancen los objetivos previstos [ISO/IEC 27001 4.2.4 d]

Debe mantenerse un control sobre las medidas y mejoras implementadas para verificar que cumplen su cometido y alcanzan los objetivos previstos.

4.4.1.5 Actualizar planes, políticas y procedimientos [ISO/IEC 27001 4.2.3 g], [ANSI/ISA 99 4.3.4.3.6]

Deben actualizarse los planes implementados dentro del SGCI, conforme a las mejoras identificadas, o según los cambios provocados por las medidas correctivas o preventivas.

4.4.1.6 Mantener registros de evaluación de vulnerabilidades [ANSI/ISA 99 4.2.3.13]

Deben mantenerse actualizados los registros de evaluación de vulnerabilidades de todos los activos ICS, con el fin de ver la evolución en el tiempo.

5 ANEXO A. CONTROLES DE SEGURIDAD

Este anexo es una ayuda para la selección de controles de seguridad por parte de la organización tras la fase de evaluación de riesgos. Contiene una lista no exhaustiva de controles de seguridad que pueden ser implementados por la organización para mitigar los riesgos que se hayan considerado.

Los controles de esta lista pueden ser completados con las listas de controles de seguridad descritas en los documentos NIST Special Publication 800-53 [6], en sus apéndices D y F, en la serie de documentos NERC CIP [5] y en los controles que proporciona el estándar ISO/IEC 27002 [4].

5.1 Seguridad de Recursos Humanos

5.1.1.1 Establecer una política de seguridad de personal [ANSI/ISA 99 4.3.3.2.1]

La política de seguridad del personal ha de declarar el compromiso de la organización para con la seguridad del personal y las responsabilidades de seguridad del personal.

5.1.1.2 Examinar al personal al inicio [ANSI/ISA 99 4.3.3.2.2]

Debe examinarse al personal durante la fase de selección, validando su identidad y sus antecedentes, a menos que alguna regulación lo prohíba.

5.1.1.3 Examinar al personal regularmente [ANSI/ISA 99 4.3.3.2.3]

El personal debe ser objeto de revisión, sobre cambios que puedan indicar un conflicto de interés o asuntos que puedan afectar al rendimiento en el trabajo de la manera apropiada.

5.1.1.4 Abordar responsabilidades de seguridad [ANSI/ISA 99 4.3.3.2.4]

La política de seguridad de personal debe abordar las responsabilidades de seguridad del personal, desde la etapa de reclutamiento hasta el fin del empleo, especialmente para puestos que manejen información sensible.

5.1.1.5 Documentar y comunicar expectativas y responsabilidades de seguridad [ANSI/ISA 99 4.3.3.2.5]

Las expectativas de seguridad y responsabilidades del personal deben ser documentadas de forma precisa y comunicadas regularmente.

5.1.1.6 Establecer términos de ciberseguridad y condiciones de empleo de manera precisa [ANSI/ISA 99 4.3.3.2.6]

Los términos y condiciones de empleo deben ser definidos de manera precisa en cuanto a la responsabilidad del empleado para con la ciberseguridad.

5.1.1.7 Segregar deberes y tareas para mantener el equilibrio de poderes [ANSI/ISA 99 4.3.3.2.7]

Los deberes y tareas deben ser segregadas entre el personal para mantener un equilibrio de poderes apropiado, de manera que ningún individuo tenga control total sobre acciones que puedan cambiar la operación funcional de los ICS.

5.2 Seguridad Física y del Entorno

5.2.1.1 Establecer políticas complementarias de seguridad física y ciberseguridad [ANSI/ISA 99 4.3.3.3.1]

Deben establecerse políticas y procedimientos que aborden la seguridad física y la ciberseguridad en la protección de los activos.

5.2.1.2 Establecer un perímetro físico de seguridad [ANSI/ISA 99 4.3.3.3.2], [NIST SP 800-82 6.2.2]

Deben establecerse uno o más perímetros físicos de seguridad para proporcionar barreras, activas y/o pasivas, como vallas, muros, zanjas anti-vehículos, puertas, etc. ante accesos no autorizados para proteger los activos.

5.2.1.3 Establecer controles de entrada [ANSI/ISA 99 4.3.3.3.3], [NIST SP 800-82 6.2.2]

Deben establecerse controles de entrada apropiados en cada barrera o límite físico de manera que sólo personas autorizadas tengan acceso a los espacios controlados.

5.2.1.4 Rastrear situación del personal y activos [NIST SP 800-82 6.2.2]

Deben establecerse mecanismos para conocer la localización de personas y ciertos activos de la organización, dentro de una planta, para asegurar que se encuentran en las áreas autorizadas, y localización de recursos en caso de emergencia.

5.2.1.5 Proteger activos contra daños ambientales [ANSI/ISA 99 4.3.3.3.4], [NIST SP 800-82 6.2.2]

Los activos deben protegerse frente daños ambientales, de amenazas como el fuego, agua, humo, polvo, radiación, corrosión, e impactos.

5.2.1.6 Protección del cableado [NIST SP 800-82 6.2.2.3]

Debe asegurarse la protección del cableado frente al entorno de planta, como campos magnéticos, ondas de radio, temperaturas extremas, humedad, polvo, vibraciones, o las condiciones que presente la actividad industrial de la organización. Las conducciones de cable deben además protegerse contra accesos a personal no autorizado.

5.2.1.7 Establecer política sobre dispositivos portátiles [NIST SP 800-82 6.2.2.2]

Debe establecerse una política de uso de los dispositivos electrónicos o computerizados portátiles usados para realizar funciones de los ICS, como la programación de PLCs, asegurando que dichos dispositivos no abandonen nunca el área segura de ICS, o en caso de necesidad, lo hagan de manera segura.

5.2.1.8 Requerir a los empleados el seguimiento de los procedimientos de seguridad [ANSI/ISA 99 4.3.3.3.5]

Debe requerirse a los empleados que sigan y cumplan los procedimientos de seguridad física que han sido establecidos.

5.2.1.9 Proteger conexiones [ANSI/ISA 99 4.3.3.3.6]

Todas las conexiones bajo el control de la organización deben ser protegidas adecuadamente frente a la manipulación y el daño.

5.2.1.10 Mantener activos de equipamiento [ANSI/ISA 99 4.3.3.3.7]

Todos los activos de equipamiento, incluyendo el equipamiento ambiental, debe ser mantenido de manera adecuada para asegurar su correcto funcionamiento.

5.2.1.11 Establecer procedimientos de monitorización y alarma [ANSI/ISA 99 4.3.3.3.8]

Deben establecerse procedimientos para monitorizar y disparar alarmas, cuando la seguridad física o ambiental se ve comprometida.

5.2.1.12 Establecer procedimientos para añadir, suprimir y eliminar activos físicos [ANSI/ISA 99 4.3.3.3.9]

Deben establecerse y auditarse procedimientos con respecto a la adición, supresión y eliminación de todos los dispositivos.

5.2.1.13 Establecer procedimientos para la protección temporal de activos críticos [ANSI/ISA 99 4.3.3.3.10]

Deben establecerse procedimientos para asegurar la protección de componentes críticos durante la interrupción de las operaciones, por ejemplo, debido al fuego, agua, brechas de seguridad, o cualquier otro tipo de desastre.

5.3 Segmentación y Protección de Red

5.3.1.1 Desarrollar una arquitectura de red segmentada [ANSI/ISA 99 4.3.3.4.1]

Debe desarrollarse una estrategia de segmentación de red, empleando zonas de seguridad, para los dispositivos ICS, en base al nivel de riesgo de ICS.

5.3.1.2 Emplear aislamiento o segmentación en ICS de alto riesgo [ANSI/ISA 99 4.3.3.4.2]

Los ICS de alto riesgo deben ser aislados o debe emplearse algún dispositivo que funcione como barrera para separarlos de otras zonas con diferentes niveles de seguridad o riesgos.

5.3.1.3 Bloquear comunicaciones no esenciales con dispositivos barrera [ANSI/ISA 99 4.3.3.4.3]

Dispositivos barrera deben bloquear todas las comunicaciones no esenciales en sentido de entrada y salida de la zona de seguridad que contiene el equipamiento crítico de control.

5.3.1.4 Utilizar sistemas de protección de red [NIST 800-82 6.2.6.2]

Deben emplearse dispositivos IDS y/o IPS, así como firewalls, debidamente configurados, entre las redes de control y la red corporativa.

5.3.1.5 Uso de protocolos seguros para servidores web [NIST 800-82 6.3.2.2]

Los servidores web (incluyendo web, ftp, email, etc.) dentro del entorno de ICS deben usar protocolos seguros (como HTTPS, SFTP o SCP, etc.)

5.4 Control de Acceso: Administración de Cuentas

5.4.1.1 Cuentas de acceso de acuerdo a la política de seguridad de autorización [ANSI/ISA 99 4.3.3.5.1]

Los privilegios de acceso implementados para las cuentas de acceso deben ser establecidos en concordancia con la política de autorización de la organización (5.6.1.1).

5.4.1.2 Identificar individuos [ANSI/ISA 99 4.3.3.5.2]

Debe evaluarse y escogerse el tipo de acceso, por individuos o por grupos, considerando los riesgos y vulnerabilidades, incluyendo los riesgos HSE de controles individuales, mitigación de riesgos usando controles de seguridad física complementarios, requisitos de responsabilidad, y necesidades administrativas/operacionales.

5.4.1.3 Autorizar acceso a las cuentas [ANSI/ISA 99 4.3.3.5.3]

El acceso a las cuentas debe ser otorgado, cambiado o finalizado, bajo la autoridad de un director adecuado.

5.4.1.4 Crear y mantener registros de cuentas [ANSI/ISA 99 4.3.3.5.4]

Debe mantenerse un registro de todas las cuentas de acceso, incluyendo detalles de los individuos, y los dispositivos autorizados para usar la cuenta, sus permisos y la persona que otorgó la autorización.

5.4.1.5 Suspender o eliminar cuentas innecesarias [ANSI/ISA 99 4.3.3.5.5]

Las cuentas de acceso deben ser suspendidas o eliminadas tan pronto como sea posible, si no van a ser usadas nunca más.

5.4.1.6 Revisar permisos de cuentas [ANSI/ISA 99 4.3.3.5.6]

Todas las cuentas de acceso establecidas deben ser revisadas regularmente para asegurar que los individuos y dispositivos tienen el mínimo de permisos necesarios.

5.4.1.7 Cambiar contraseñas por defecto [ANSI/ISA 99 4.3.3.5.7]

Las contraseñas por defecto para las cuentas de acceso, deben cambiarse antes de que los activos ICS sean puestos en servicio.

5.4.1.8 Auditar administración de cuentas [ANSI/ISA 99 4.3.3.5.8]

Deben llevarse a cabo revisiones periódicas de cumplimiento de la política de administración de cuentas.

5.5 Control de Acceso: Autenticación

5.5.1.1 Desarrollar estrategia de autenticación [ANSI/ISA 99 4.3.3.6.1]

La organización debe tener una estrategia de autenticación o un enfoque que defina los métodos de autenticación a emplear.

5.5.1.2 Autenticar todos los usuarios antes del uso de sistemas [ANSI/ISA 99 4.3.3.6.2]

Todos los usuarios deben autenticarse antes de usar la aplicación que hayan requerido, a menos que exista una combinación complementaria de controles de entrada y prácticas administrativas.

5.5.1.3 Requerir métodos de autenticación fuerte para administración de sistema y configuración de aplicación [ANSI/ISA 99 4.3.3.6.3]

Deben emplearse prácticas de autenticación fuerte (como requerir contraseñas fuertes) en todas las cuentas de acceso a la administración del sistema y la configuración de aplicaciones.

5.5.1.4 Registrar y revisar todos los intentos de acceso a sistemas críticos [ANSI/ISA 99 4.3.3.6.4]

Deben registrarse todos los intentos de acceso a sistemas críticos mediante archivos de log, y deben ser revisados los intentos de acceso satisfactorios y fallidos.

5.5.1.5 Autenticar usuarios remotos con un nivel apropiado [ANSI/ISA 99 4.3.3.6.5]

La organización debe emplear un esquema de autenticación con un nivel apropiado de fortaleza con el fin de identificar positivamente a los usuarios remotos interactivos.

5.5.1.6 Desarrollar una política para inicio de sesión remota y conexiones [ANSI/ISA 99 4.3.3.6.6]

La organización debe desarrollar una política que trate el inicio de sesión remota de un usuario y/o las conexiones remotas al sistema de control (por ejemplo de conexiones entre tareas), que defina las respuestas adecuadas a los intentos fallidos de acceso y los períodos de inactividad.

5.5.1.7 Implementar autenticación múltiple para accesos remotos [NIST SP 800-82 6.3.1.3]

Debe emplearse un método de autenticación basado en más de un factor para el acceso a las aplicaciones de forma remota.

5.5.1.8 Deshabilitar cuenta de acceso tras número fallido de intentos de inicio de sesión remota [ANSI/ISA 99 4.3.3.6.7]

Tras un número establecido de intentos de acceso de un usuario remoto, el sistema debería deshabilitar el acceso a la cuenta durante un cierto período de tiempo.

5.5.1.9 Requerir re-autenticación tras inactividad de sesión remota [ANSI/ISA 99 4.3.3.6.8]

Tras un período de inactividad, el usuario remoto debería ser emplazado a re-autenticarse antes de que pueda re-acceder al sistema.

5.5.1.10 Emplear autenticación para comunicaciones entre aplicaciones y dispositivos [ANSI/ISA 99 4.3.3.6.9]

Los sistemas deberían emplear un esquema de autenticación apropiado para la comunicación de tarea a tarea, entre aplicaciones y dispositivos.

5.6 Control de Acceso: Autorización

5.6.1.1 Definir una política de autorización [ANSI/ISA 99 4.3.3.7.1]

Debe definirse de manera precisa una política de autorización que aplique sobre todo el personal, en la que deben establecerse reglas que definan los privilegios autorizados bajo las cuentas de acceso de personal de varios roles de trabajo.

5.6.1.2 Establecer métodos apropiados de permisos lógicos y físicos para el acceso a dispositivos ICS [ANSI/ISA 99 4.3.3.7.2]

El permiso de acceso a dispositivos ICS debe ser lógico (reglas que otorguen o denieguen el acceso a usuarios conocidos, basándose en sus roles), físico (cierres, cámaras, y otros controles que restrinjan el acceso a una consola activa), o ambos.

5.6.1.3 Control de acceso a sistemas o información mediante cuentas de acceso basadas en roles [ANSI/ISA 99 4.3.3.7.3]

Las cuentas de acceso deben ser basadas en roles, para gestionar el acceso a la información apropiada, o a los sistemas para dicho rol de usuario. Deben tenerse en cuenta implicaciones de seguridad humana al definir los roles.

5.6.1.4 Emplear múltiples métodos de autorización para ICS críticos [ANSI/ISA 99 4.3.3.7.4]

En entornos de control críticos, deben emplearse múltiples métodos de autorización para limitar el acceso a los ICS.

6 ANEXO B. LISTA DE DOCUMENTOS DEL SGCI

Este anexo presenta una lista de documentos, registros o contenidos a implementar durante las distintas fases del ciclo de vida del SGCI, sirviendo a la organización de guía o lista de comprobación. La organización deberá decidir el medio y el formato lógico o físico a emplear para cada uno de los documentos de la lista.

Tabla SGCI.1. Lista de documentos del SGCI

Id. Documento	Nombre	Descripción	Correspondencia con apartado SCGI
Creación del SGCI			
C.1	Alcance del SGCI	Ámbito del SGCI, objetivos estratégicos, procesos y planificación temporal del SGCI	4.1.1.1
C.2	Política del SGCI	Política del SGCI con directrices, requisitos, orientación, etc.	4.1.2.1
C.3	Composición del equipo de ciberseguridad	Lista del personal, roles y responsabilidades del equipo de ciberseguridad	4.1.3.3
C.4	Lista de amenazas	Lista de amenazas del sector de la organización	4.1.4.3
C.5	Lista de vulnerabilidades	Lista de vulnerabilidades del sector de la organización	4.1.4.3
C.6	Criterios de aceptación del riesgo:	Detalle de los criterios de aceptación de los riesgos de seguridad	4.1.4.4
C.7	Inventario de activos	Lista de los activos dentro del alcance del SGCI, e información asociada a cada uno	4.1.4.6
C.8	Inventario de terceros	Lista de los terceros relacionados con los sistemas ICS, e información asociada a cada uno	4.1.4.7
C.9	Diagramas de red	Diagramas simples de red de los sistemas ICS	4.1.4.8
C.10	Evaluación de riesgos	Resultados de la	4.1.4.14, 4.1.4.1

Id. Documento	Nombre	Descripción	Correspondencia con apartado SCGI
		evaluación de riesgos y la metodología utilizada	
C.11	Documento de aprobación del riesgo residual	Aprobación firmada por la dirección	4.1.5.1
C.12	Documento de autorización del SGCI	Autorización firmada por la dirección	4.1.5.2
Implementación y Operación del SGCI			
IO.1	Lista de controles	Lista de controles implementados y a implementar y la relación con los riesgos a mitigar	4.2.1.2
IO.2	Documento de métodos de medición de controles	Métodos y métricas de medición de la eficacia de los controles	4.2.1.3
IO.3	Plan de tratamiento de riesgos	Acciones a realizar, recursos a utilizar, responsabilidades y prioridades para gestionar los riesgos evaluados	4.2.2.1
IO.4	Plan de formación y concienciación	Acciones, recursos, prioridades y planificación temporal de las acciones formativas y de concienciación	4.2.3.2
IO.5	Registros de formación	Registros de formación impartida, reflejando períodos, aptitudes y cualificaciones obtenidas	4.2.3.3
IO.6	Documento de métodos de medición de la eficacia de la formación y concienciación	Métricas y métodos para medir la eficacia de la formación y concienciación	4.2.3.4
IO.7	Documento de métodos de medición de conformidad	Métricas y métodos para medir la conformidad y el cumplimiento de políticas, procesos y	4.2.5.1

Id. Documento	Nombre	Descripción	Correspondencia con apartado SCGI
		procedimientos del SGCI	
IO.8	Plan de respuesta ante incidentes	Plan de respuesta ante incidentes de seguridad, responsabilidades y acciones a realizar	4.2.6.1
IO.9	Procedimiento de informe y tratamiento de eventos inusuales	Procedimiento de informe y tratamiento de eventos o actividades inusuales	4.2.6.3
IO.10	Registro de incidentes de seguridad	Incidentes producidos, con nivel de detalle suficiente, acciones llevadas a cabo, y lecciones aprendidas.	4.2.6.8
IO.11	Procedimiento de simulacro de incidentes	Procedimiento para llevar a cabo simulacros de incidentes de prueba	4.2.6.11
IO.12	Política de seguridad de componentes e implementaciones	Política general sobre nuevos componentes e implementaciones y sus requisitos de seguridad	4.2.7.1
IO.13	Procedimiento sobre nuevos componentes e implementaciones	Procedimiento de seguridad para incluir los nuevos componentes al sistema de control industrial y las nuevas implementaciones.	4.2.7.1
IO.14	Procedimiento de gestión de cambios	Responsabilidades, consideraciones y acciones a llevar a cabo, antes, durante y después de los cambios sobre los sistemas.	4.2.7.4
IO.15	Procedimiento de gestión de parches	Responsabilidades, consideraciones y acciones a llevar a cabo, antes, durante y después de las actualizaciones de sistemas mediante	4.2.7.7

Id. Documento	Nombre	Descripción	Correspondencia con apartado SCGI
		parches.	
IO.16	Procedimiento de gestión de antivirus/malware	Procedimiento para el uso y actualización del software antivirus	4.2.7.8
IO.17	Procedimiento de backup y restauración	Procedimiento de realización de backup y la restauración del mismo	4.2.7.9
IO.18	Documento de objetivos de recuperación	Objetivos de recuperación de sistemas, priorizados.	4.2.9.1
IO.19	Plan de continuidad del negocio	Plan que considere el equipo de continuidad, los roles y responsabilidades y los procedimientos y acciones de recuperación.	4.2.9.3
IO.20	Política de gestión de activos de información	Política sobre objetivos de seguridad, ámbito de aplicación y recursos para la gestión de activos de información	4.2.10.1
IO.21	Documento de definición de niveles de clasificación de activos de información	Definición de los niveles de clasificación sobre activos de información y sus restricciones	4.2.10.2
IO.22	Procedimiento de gestión de activos de información	Procedimiento para la retención, protección, destrucción y eliminación de activos de información.	4.2.10.2, 4.2.10.3, 4.2.10.4, 4.2.10.5
Supervisión y Revisión del SGCI			
SR.1	Informe de la revisión de eficacia de los controles	Resultados de la revisión de eficacia de los controles, identificando deficiencias y mejoras	4.3.1.1
SR.2	Informe de la revisión del grado de conformidad y	Resultados de la revisión del grado de conformidad y	4.3.1.2

Id. Documento	Nombre	Descripción	Correspondencia con apartado SCGI
	cumplimiento	cumplimiento, e identificación de los incumplimientos	
SR.3	Informe de la evaluación del programa de formación	Resultados de la evaluación del programa de formación, identificando deficiencias y mejoras	4.3.2.1
SR.4	Informe de la revisión del programa de formación	Resultados de la revisión del programa de formación, identificando nuevas necesidades de formación	4.3.2.2
SR.5	Informe de la revisión de los métodos de medición de conformidad	Resultados de la revisión de los métodos de medición de conformidad y cumplimiento de políticas, procesos y procedimientos del SGCI, identificando mejoras.	4.3.3.1
SR.6	Informe de la revisión de los métodos de medición de eficacia de los controles	Resultados de la revisión de los métodos de medición de eficacia de los controles, identificando deficiencias y mejoras.	4.3.3.2
SR.7	Informe de la revisión del plan de respuesta ante incidentes	Resultado de la revisión del plan de respuesta ante incidentes	4.3.4.1
SR.8	Informe de la revisión de políticas y procedimientos de nuevos componentes e implementaciones	Resultado de la revisión de políticas y procedimientos de nuevos componentes e implementaciones	4.3.5.1
SR.9	Informe de la revisión del procedimiento de gestión de cambios	Resultado de la revisión del procedimiento de gestión de cambios e identificación de mejoras	4.3.5.2

Id. Documento	Nombre	Descripción	Correspondencia con apartado SCGI
SR.10	Informe de la revisión del procedimiento de gestión de parches	Resultado de la revisión del procedimiento de gestión de parches e identificación de mejoras	4.3.5.3
SR.11	Informe de la revisión del procedimiento de gestión de antivirus/malware	Resultado de la revisión del procedimiento de gestión de antivirus/malware e identificación de mejoras	4.3.5.4
SR.12	Informe de la revisión del procedimiento de backup y restauración	Resultado de la revisión del procedimiento de backup y restauración e identificación de mejoras	4.3.5.5
SR.13	Informe de la revisión del cumplimiento de acuerdos y cláusulas de seguridad	Resultado de la revisión del cumplimiento de acuerdos y cláusulas de seguridad e identificación de incumplimientos	4.3.6.1
SR.14	Informe de la revisión del plan de continuidad del negocio	Resultado de la revisión del plan de continuidad del negocio e identificación de mejoras	4.3.7.1
SR.15	Informe de resultados de test de continuidad de negocio	Resultados del test de continuidad de negocio e identificación de anomalías y mejoras	4.3.7.2
SR.16	Informe de la revisión de los procedimientos de gestión de activos de información	Resultado de la revisión de los procedimientos de gestión de activos de información e identificación de mejoras	4.3.8.1
SR.17	Informe de la auditoría sobre políticas y procedimientos de gestión de activos de	Resultado de la auditoría sobre políticas y procedimientos de gestión de activos de	4.3.8.2

Id. Documento	Nombre	Descripción	Correspondencia con apartado SCGI
	información	información, identificando los incumplimientos.	
SR.18	Informe del Análisis externo de la Ciberseguridad	Nuevas buenas prácticas, recomendaciones y nueva legislación que afecte a la actividad	4.3.9.1, 4.3.9.2
SR.19	Informe de la revisión de la evaluación de vulnerabilidades	Resultado de la revisión de la evaluación de vulnerabilidades y los cambios identificados respecto de evaluaciones anteriores	4.3.11.1
SR.20	Programa de auditoría	Objetivos, alcance, identificación del responsable, recursos, procedimientos, miembros del equipo auditor, métodos de auditoría y gestión de los registros y los resultados	4.3.12.1, 4.3.12,2
SR.21	Informe de las auditorías	Resultado de las auditorías realizadas, incluyendo no conformidades, observaciones e identificación de mejoras	4.3.12.4
SR.22	Lista de documentos del registro de auditoría	Lista de documentos de registros que se generarán mediante la auditoría	4.2.12.3
SR.23	Informe de la revisión del SGCI por parte de la dirección	Resultado de la revisión del SGCI por parte de la dirección e identificación de mejoras	4.3.13.1

7 ANEXO C. LISTAS DE AMENAZAS Y VULNERABILIDADES

Este anexo trata de servir de ayuda a la organización, a la hora identificar, clasificar y evaluar los riesgos, presentando listas de categorías de amenaza, agentes de amenaza, vulnerabilidades potenciales de ICS y de redes industriales.

7.1 Amenazas

Tabla SGCI.2. Categorías y ejemplos de amenazas [ISO/IEC 27005 Anexo C]

Categoría	Ejemplos de amenazas
Daño físico	Fuego, agua, polución, corrosión, destrucción de equipamiento
Desastres naturales	Fenómenos volcánicos, fenómenos meteorológicos, inundación
Pérdida de servicios esenciales	Fallo del sistema de aire acondicionado, fallo del equipo de telecomunicaciones
Perturbación debida a radiaciones	Radiación electromagnética, radiación térmica
Compromiso de la información	Robo de documentos, revelación de información, recuperación de medios desechados
Fallos técnicos	Fallo del equipamiento, saturación del sistema de información
Acciones no autorizadas	Uso no autorizado del equipamiento, copia fraudulenta del software
Compromiso de las funciones	Errores de uso, abuso de los derechos, denegación de acciones

Tabla SGCI.3. Agentes de amenaza [NIST SP 800-82, ISO/IEC 27005 Anexo C]

Agente de Amenaza	Descripción
Atacantes	Individuos que intervienen las redes, con distinto propósito, ayudados normalmente de sofisticadas herramientas.
Operadores de bot-net	Atacantes, que toman el control de múltiples sistemas distribuidos para coordinar y realizar sus ataques.
Grupos criminales	Grupos criminales de individuo cuyo propósito es la ganancia de dinero.
Servicios de inteligencia extranjeros	Grupos organizados de inteligencia, que usan herramientas cibernéticas para recopilar información y espiar.
Infiltrados	Personas pertenecientes a la organización que tienen fines contrarios, normalmente trabajadores descontentos.
Phishers	Individuos o pequeños grupos que realizan ataques de phishing con intereses monetarios.
Spammers	Individuos o pequeños grupos que distribuyen información falsa, que conlleva ataques de phishing, distribución de spyware/malware u otros ataques.
Autores de	Individuos u organizaciones con fines maliciosos que pretenden llevar a

spyware/malware	cabo ataques mediante software malicioso.
Terroristas	Individuos u organizaciones terroristas que pretenden destruir, incapacitar o aprovecharse de infraestructuras críticas.
Espias industriales	Individuos que trabajan para otras organizaciones que buscan hacerse con la propiedad intelectual y el conocimiento técnico de la organización mediante métodos clandestinos.

7.2 Vulnerabilidades

7.2.1 Vulnerabilidades Potenciales de ICS [NIST SP 800-82 3.3]

Tabla SGCI.4. Vulnerabilidades de políticas y procedimientos [NIST SP 800-82 3.3.1 Table 3-3]

Vulnerabilidad	Descripción
Política de seguridad inadecuada para ICS	Políticas de seguridad para ICS inadecuadas o inexistentes
No existencia de formación de seguridad en ICS y programa de concienciación	La falta de formación en políticas y procedimientos de ICS, hace que el personal no pueda mantener un entorno ICS seguro
Arquitectura y diseño de seguridad inadecuados	Falta de consideración de la seguridad por parte de los ingenieros de control
No existencia de procedimientos de seguridad	Falta de existencia de procedimientos de seguridad derivados a partir de la política de seguridad de ICS
Ausencia o deficiencia en las directrices de implementación de ICS	Las directrices de implementación del equipamiento ICS no están actualizadas o disponibles
Falta de mecanismos administrativos para hacer cumplir la seguridad	Los responsables de hacer cumplir las políticas y procedimientos de seguridad no tienen la autoridad suficiente
Escasez o inexistencia de auditorías de seguridad sobre ICS	Falta de auditorías sobre ICS o ejecutadas con baja periodicidad o que no tienen en cuenta factores desencadenantes
Falta de plan de recuperación ante desastres	Inexistencia o incompletitud de un plan de recuperación ante desastres, para reducir los tiempos de parada y las pérdidas en caso de desastre
Falta de gestión de cambios específica para ICS	Inexistencia de procesos específicos para gestionar las modificaciones de hardware, firmware, software y documentación de ICS

Política de seguridad inadecuada para ICS	Políticas de seguridad para ICS inadecuadas o inexistentes

Tabla SGCI.5. Vulnerabilidades de configuración [NIST SP 800-82 3.3.2 Table 3-4]

Vulnerabilidad	Descripción
Parches del SO y del software no desarrollados hasta tiempo después de encontrarse vulnerabilidades	La complejidad de los sistemas ICS hace que posiblemente los parches que solventen una vulnerabilidad de seguridad encontrada, no estén disponibles para su uso hasta tiempo después, presentando así una ventana de vulnerabilidad.
Soporte de parches de seguridad de SO y aplicación no mantenido	Aplicaciones y SOs anticuados puede que no dispongan de un soporte de mantenimiento que desarrolle parches para las vulnerabilidades descubiertas
Parches de SO y aplicación implementados sin tests exhaustivos	Falta de pruebas antes del despliegue de los parches que puedan comprometer la operación de los ICS
Uso de configuraciones por defecto	Uso de configuraciones de los ICS por defecto que conlleva puertos abiertos, servicios y aplicaciones explotables ejecutándose en los equipos, contraseñas por defecto, etc.
Configuraciones críticas no almacenadas	Falta de procedimientos para almacenar y restaurar configuraciones de ICS
Datos no protegidos en dispositivos portátiles	Falta de protección de información sensible en dispositivos portátiles como ordenadores portátiles o PDAs
Falta de una política adecuada de contraseñas	Falta de una política de contraseñas, sobre cuándo deben ser empleadas, la fortaleza y el mantenimiento de las mismas
Falta de contraseñas	Falta de contraseñas para acceder a funciones críticas
Revelación de contraseñas	Falta de confidencialidad de las contraseñas, debido a comunicación de la misma a otras personas, compartición de la misma contraseña, envío por medios no protegidos, etc.
Adivinación de contraseñas	Contraseñas mal escogidas pueden ser adivinadas por individuos o por algoritmos informáticos para conseguir acceso no autorizado
Aplicación no adecuada de controles de acceso	Controles de acceso mal especificados pueden resultar en otorgar a un usuario un nivel de privilegios demasiado alto o bajo

Tabla SGCI.6. Vulnerabilidades de hardware [NIST SP 800-82 3.3.2 Table 3-5]

Vulnerabilidad	Descripción
Pruebas inadecuadas ante cambios de	Pruebas insuficientes o no existentes debido a la falta de plataformas de

seguridad	prueba de entornos ICS
Protección física inadecuada para sistemas críticos	Control y monitorización inadecuados para acceder al centro de control, los dispositivos de campo u otros componentes ICS
Personal no autorizado tiene acceso físico al equipamiento	El acceso al equipamiento ICS no está restringido solo al personal necesario
Acceso remoto inseguro a componentes ICS	Falta de controles de seguridad para el acceso remoto a componentes ICS como módems y otros dispositivos
Tarjetas de red duales conectando varias redes	Máquinas con varias tarjetas de red conectadas a diferentes redes pueden permitir el acceso no autorizado y el traspaso de datos entre redes
Activos no documentados	La existencia de activos ICS no documentados podría resultar en la existencia de puntos de acceso al sistema que no se están teniendo en cuenta
Radiofrecuencias y pulso electromagnético	El hardware de ICS es vulnerable a la radiofrecuencia y a los pulsos electromagnéticos
Falta de energía auxiliar	Si no existe un sistema de energía auxiliar, y ante una caída de la energía principal, se apagarían los ICS y podría crearse una situación insegura
Pérdida del control sobre el entorno ambiental	La pérdida del control sobre las condiciones del entorno ambiental puede producir consecuencias como el sobrecalentamiento de equipos
Falta de redundancia de componentes críticos	La falta de redundancia de componentes críticos puede aumentar las posibilidades de un fallo general debido al fallo en único punto

Tabla SGCI.7. Vulnerabilidades de software [NIST SP 800-82 3.3.2 Table 3-6]

Vulnerabilidad	Descripción
Overflow de búffer	El software usado para implementar un ICS puede ser vulnerable a overflows de búffer, de manera que sea explotable
Capacidades de seguridad instaladas no habilitadas por defecto	Los ICS disponen de capacidades de seguridad pero no están identificadas o no se han habilitado
Denegación de Servicio (DoS)	Los ICS pueden ser vulnerables a ataques DoS, resultando que se inhabilite el acceso autorizado o producir retrasos en las operaciones
Tratamiento erróneo de condiciones mal definidas o “ilegales”	Algunas implementaciones de ICS son vulnerables a paquetes malformados o que contienen valores “ilegales” o inesperados
OLE for Process Control (OPC)	Sin los parches de actualización, OPC es vulnerable a las conocidas

confía en llamadas a procedimientos remotos (RPC) y en el Modelo de Objetos de Componentes Distribuidos (DCOM)	vulnerabilidades de RPC/DCOM
Uso de protocolos inseguros de la industria	DNP 3.0, Modbus, Profibus y otros protocolos comúnmente usados en diversas industrias tienen pocas o ninguna capacidad de seguridad
Uso de texto plano	Muchos protocolos de ICS transmiten los mensajes en texto plano, haciéndolos susceptibles de ser interceptados por adversarios
Uso de software propietario que ha sido tratado por conferencias y medios	El software propietario, es debatido en conferencias, artículos, listas de correo, etc. y los manuales suelen estar disponibles al público lo que facilita a los adversarios crear sus ataques hacia los ICS
Autenticación y control de acceso al software de configuración y programación inadecuados	El acceso no autorizado al software de configuración y programación puede conllevar la posibilidad de corromper un dispositivo
Software de detección/prevención de intrusiones no instalado	La no existencia de software IDS/IPS puede resultar en incidentes que provoquen pérdidas de disponibilidad, captura, modificación y borrado de datos, etc.
Falta de mantenimiento de logs	Logs no almacenados o poco precisos, hacen que sea muy difícil determinar las causas de un evento de seguridad

Tabla SGCI.8. Vulnerabilidades de malware [NIST SP 800-82 3.3.2 Table 3-7]

Vulnerabilidad	Descripción
Software de protección ante el malware no instalado	El software malicioso puede provocar pérdidas de rendimiento, pérdidas de disponibilidad del sistema, captura, modificación o borrado de datos
Software de protección ante el malware no actualizado	El software de protección ante el malware no actualizado deja al sistema abierto a nuevas amenazas de malware
Software de protección ante el malware no probado de manera exhaustiva	El software de protección ante el malware es desplegado sin las adecuadas pruebas lo que podría resultar en un impacto en la operación normal de los ICS

7.2.2 Vulnerabilidades de Red [NIST 800-82 3.3.3]

Tabla SGCI.9. Vulnerabilidades de configuración de red [NIST SP 800-82 3.3.3 Table 3-8]

Vulnerabilidad	Descripción
Arquitectura de seguridad de red débil	La infraestructura de red es diseñada y modificada a lo largo del tiempo según requisitos operativos y no de seguridad, creando huecos de seguridad
Controles de flujo de datos no empleados	Controles de flujo de datos como, listas de control de acceso (ACL) no utilizados, por lo que el acceso a los dispositivos de red no queda restringido
Equipamiento de seguridad mal configurado	Configuraciones por defecto pueden suponer la apertura de puertos innecesarios y explotables. Reglas de firewalls y routers mal configuradas pueden permitir el paso de tráfico innecesario.
Configuraciones de dispositivos de red no se almacenan	No existen o no se implementan procedimientos para guardar y restaurar configuraciones de los dispositivos de red en caso necesario
Contraseñas no encriptadas en tránsito	Contraseñas transmitidas en texto plano son susceptibles de ser interceptadas por los adversarios
Contraseñas existentes por tiempo indefinido en dispositivos de red	Las contraseñas no son cambiadas cada cierto período de tiempo, lo que permite un acceso indefinido en el tiempo a terceras partes si logran conocer dichas contraseñas
Controles de acceso inadecuados	El acceso no autorizado a los dispositivos de red y a funciones administrativas podría permitir a un usuario interrumpir las operaciones de ICS o monitorizar la actividad de red

Tabla SGCI.10. Vulnerabilidades de hardware de red [NIST SP 800-82 3.3.3 Table 3-9]

Vulnerabilidad	Descripción
Protección física inadecuada del equipamiento de red	El acceso al equipamiento de red debe ser controlado para prevenir daños
Puertos físicos no asegurados	Puertos físicos como USB o PS/2 pueden permitir una conexión no autorizada de memorias USB, registradores de pulsaciones de teclas, etc.
Pérdida de control del entorno ambiental	La pérdida de control del entorno ambiental puede producir que los procesadores se sobrecalienten
Personal no crítico tiene acceso al equipamiento y las conexiones de red	El acceso no restringido solo al personal necesario al equipamiento y las conexiones de red puede puede resultar en robo, daño, cambios no autorizados, etc.
Falta de redundancia de redes críticas	La falta de redundancia en redes críticas puede resultar en puntos de fallo únicos

Tabla SGCI.11. Vulnerabilidades de perímetro de red [NIST SP 800-82 3.3.3 Table 3-10]

Vulnerabilidad	Descripción
Perímetro de seguridad no definido	Sin un perímetro de la red de control bien definido no podrá asegurarse que los controles de seguridad estén correctamente desplegados y configurados
Firewalls inexistentes o mal configurados	La falta de firewalls configurados adecuadamente puede permitir el paso de datos entre redes, como por ejemplo entre la red de control y la red corporativa, lo que puede permitir ataques y propagación de malware
Redes de control utilizadas para tráfico que no es de control	La coexistencia de tráfico de control y otros tráficos en la misma red dificulta la configuración de la red, a la vez que el tráfico que no es de control puede consumir recursos
Servicios de control de red fuera de la red de control	Servicios como DNS o DHCP, usados por las redes de control, implementadas fuera dichas redes, pueden suponer no alcanzar los requisitos de disponibilidad y fiabilidad de los ICS

Tabla SGCI.12. Vulnerabilidades de monitorización y registro de red [NIST SP 800-82 3.3.3 Table 3-11]

Vulnerabilidad	Descripción
Logs de firewalls y routers inadecuados	Sin logs apropiados y precisos, resulta difícil determinar las causas de un incidente de seguridad
No existencia de monitorización en la red ICS	Sin una monitorización de seguridad de manera regular, pueden producirse incidentes que pasen desapercibidos, conllevando daños e interrupciones

Tabla SGCI.13. Vulnerabilidades de comunicación [NIST SP 800-82 3.3.3 Table 3-12]

Vulnerabilidad	Descripción
No están identificadas las monitorizaciones críticas	Conexiones malintencionadas o desconocidas pueden dejar en los ICS una puerta trasera disponible para ataques
Uso de protocolos de comunicación estándar en texto plano bien documentados	Los adversarios que puedan monitorizar la actividad de red de ICS, podrían acceder a la información que transcurre por la red mediante protocolos como telnet o FTP
Autenticación de usuarios, datos o dispositivos, deficiente o inexistente	Muchos protocolos ICS no presentan mecanismos de autenticación a ningún nivel, y potencialmente vulnerables por tanto a la modificación de datos y la suplantación
Falta de comprobación de integridad de las comunicaciones	No existen comprobaciones de integridad de datos en la mayoría de los protocolos de control

Tabla SGCI.14. Vulnerabilidades conexiones inalámbricas [NIST SP 800-82 3.3.3 Table 3-13]

Vulnerabilidad	Descripción
Autenticación inadecuada entre clientes y puntos de acceso	La falta de mutua autenticación fuerte entre clientes inalámbricos y puntos de acceso podría permitir la conexión a un punto de acceso malintencionado o la conexión de un adversario
Protección de datos inadecuada entre clientes y puntos de acceso	Falta de mecanismos fuertes de encriptación entre clientes inalámbricos y puntos de acceso que pueden permitir a los adversarios acceder a los datos

8 BIBLIOGRAFÍA

[1]. ANSI/ISA-99.02.01-2009 Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program.

[2]. CCN-STIC-480 Guía de Seguridad de las TIC.

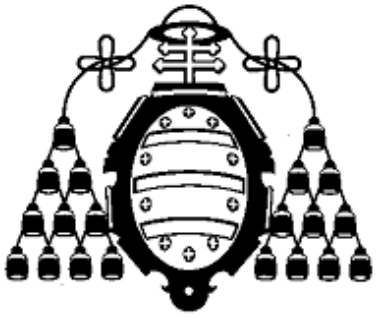
[3]. ISO/IEC. ISO/IEC 27001. Information technology - Security techniques - Information security management systems – Requirements (ISO/IEC 27001:2005).

[4]. ISO/IEC. ISO/IEC 27002. Information technology. Security techniques. Code of practice for information security management (ISO/IEC 27002:2005).

[5]. NERC. NERC CIP-001-009 Cyber Security

[6]. NIST. NIST SP 800-53 Revision 4 Final Public Draft. Security and Privacy Controls for Federal Information Systems and Organizations.

[7]. NIST. NIST SP 800-82 Guide to Industrial Control Systems (ICS) Security.



UNIVERSIDAD DE OVIEDO

ESCUELA POLITÉCNICA DE INGENIERÍA DE GIJÓN

MÁSTER EN INGENIERÍA INFORMÁTICA

TRABAJO FIN DE MÁSTER

SISTEMA DE GESTIÓN DE LA CIBERSEGURIDAD INDUSTRIAL

-RESULTADOS Y CONCLUSIONES FINALES-

Pablo Sánchez Fernández

Junio de 2013

1 PRUEBAS Y RESULTADOS

Los resultados del trabajo han sido revisados por expertos en seguridad de la información y ciberseguridad industrial, como son Ignacio Paredes y Samuel Linares (Centro de Ciberseguridad Industrial) verificando el cumplimiento de los objetivos propuestos del trabajo, de manera que el trabajo pueda sirva de norma práctica para el establecimiento de un Sistema de Gestión de Ciberseguridad Industrial, a falta de la prueba que supondría la puesta en práctica por una organización.

2 CONCLUSIONES

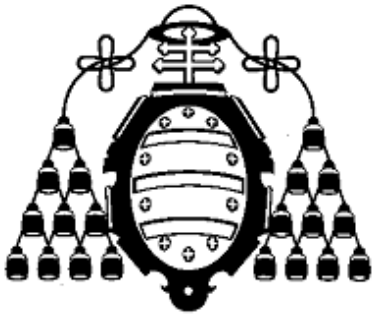
Las conclusiones extraídas tras la realización del trabajo, teniendo en cuenta todas las fases, son las siguientes:

- Actualmente existen numerosas iniciativas de protección de infraestructuras críticas e infraestructuras de información críticas, aunque no tantas sobre sistemas de control industrial, de carácter nacional, o promovidas por instituciones, pero generalmente inmaduras, que presentan muchos aspectos que no están definidos de manera práctica. El retraso en materia de protección de estas infraestructuras es notable respecto al mundo de las tecnologías de la información.
- Como consecuencia del punto anterior, existe poca documentación específica, como por ejemplo controles o contramedidas específicos para sistemas de control industrial, o catálogos de amenazas y vulnerabilidades específicos para diferentes sectores industriales.
- Actualmente existe un riesgo alto para los sistemas de control industrial, debido principalmente a que estos sistemas, con sus especiales características que se describen en este trabajo, quedan expuestos a múltiples riesgos hasta hace poco no considerados, se encuentran ahora interconectados con redes corporativas e internet.
- Las lecciones aprendidas mediante el presente trabajo abarcan:
    - Conocimiento sobre sistemas de control industrial e infraestructuras críticas
    - Iniciativas de protección sobre sistemas de control industrial e infraestructuras críticas
    - La relación actual de las tecnologías de la información con los sistemas de control industrial, sus riesgos y la manera de tratarlos

3 TRABAJO FUTURO

Como trabajo futuro a desarrollar a partir del presente trabajo se encuentran:

- La implementación de la norma descrita por parte de una organización como prueba práctica, llevando a cabo cada una de las fases del SGCI, y la recogida de datos sobre dicha implementación, su análisis, para determinar éxitos y mejoras, y el posterior refinamiento de la norma.
- El desarrollo de catálogos de amenazas y vulnerabilidades específicos para diferentes sectores industriales, que faciliten la laborar a la hora de analizar y evaluar los riesgos de una determinada organización.
- El desarrollo o la adaptación de más controles de seguridad dentro del Anexo A de la norma, de cara a que la organización que la implemente, tenga una recopilación exhaustiva de las medidas que podría implementar, sin tener que recurrir a otras guías.



UNIVERSIDAD DE OVIEDO

ESCUELA POLITÉCNICA DE INGENIERÍA DE GIJÓN

MÁSTER EN INGENIERÍA INFORMÁTICA

TRABAJO FIN DE MÁSTER

SISTEMA DE GESTIÓN DE LA CIBERSEGURIDAD INDUSTRIAL

-BIBLIOGRAFÍA-

Pablo Sánchez Fernández

Junio de 2013

1 BIBLIOGRAFÍA

[1]. Australian Government. Critical Infrastructure Resilience Strategy.

[2]. BSI. BS 7799-1:1999. Information security management. Code of practice for information security management.

[3]. BSI. BS 7799-2:2002. Information security management. Specification with guidance for use.

[4]. Cabinet Office. Strategic Framework and Policy Statement on Improving the Resilience of Critical Infrastructure to Disruption from Natural Hazards.

[5]. Cabinet Office. The UK Cyber Security Strategy. Protecting and promoting the UK in a digital world.

[6]. CCN. Guía de Seguridad de las TIC (CCN-STIC-480) Seguridad en Sistemas SCADA.

[7]. CCN. Guía de Seguridad de las TIC (CCN-STIC-480A) Seguridad en Sistemas SCADA. Guía de buenas prácticas.

[8]. CCN. Guía de Seguridad de las TIC (CCN-STIC-480B) Seguridad en Sistemas SCADA. Comprender el riesgo del negocio.

[9]. CCN. Guía de Seguridad de las TIC (CCN-STIC-480C) Seguridad en Sistemas SCADA. Implementar una arquitectura segura.

[10]. CCN. Guía de Seguridad de las TIC (CCN-STIC-480D) Seguridad en Sistemas SCADA. Establecer capacidades de respuesta.

[11]. CCN. Guía de Seguridad de las TIC (CCN-STIC-480E) Seguridad en Sistemas SCADA. Mejorar la concienciación y las habilidades.

[12]. CCN. Guía de Seguridad de las TIC (CCN-STIC-480F) Seguridad en Sistemas SCADA. Gestionar el riesgo de terceros.

[13]. CCN. Guía de Seguridad de las TIC (CCN-STIC-480G) Seguridad en Sistemas SCADA. Afrontar proyectos.

[14]. CCN. Guía de Seguridad de las TIC (CCN-STIC-480H) Seguridad en Sistemas SCADA. Establecer una dirección permanente.

[15]. Comisión de las Comunidades Europeas. Comunicación de la Comisión al Consejo y al Parlamento Europeo. Protección de las infraestructuras críticas en la lucha contra el terrorismo. COM(2004) 702.

[16]. Comisión de las Comunidades Europeas. Comunicación de la Comisión sobre un Programa Europeo para la Protección de Infraestructuras Críticas. COM(2006) 786.

[17]. Comisión de las Comunidades Europeas. Comunicación de la Comisión: una agenda digital para Europa. COM(2010) 245.

[18]. Comisión de las Comunidades Europeas. Comunicación de la Comisión: protegiendo Europa de ciberataques a gran escala e perturbaciones, promoviendo la preparación, seguridad y resiliencia. COM(2009) 149.

[19]. Comisión de las Comunidades Europeas. Libro Verde sobre un programa europeo para la Protección de Infraestructuras Críticas. COM(2005) 576.

[20]. Consejo de la Unión Europea. Directiva 2008/114/CE sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección.

[21]. CPNI. Good Practice Guide. Process Control and SCADA Security.

[22]. Department of Homeland Security. National Infrastructure Protection Plan.

[23]. Enisa. Protecting Industrial Control Systems.

[24]. ENISA. Protecting Industrial Control Systems. Recommendations for Europe and Member States.

[25]. ETH Zurich. International CIIP Handbook 2008/2009.

[26]. ETH Zurich. Strategic Trends 2012. Key Developments in Global Affairs.

[27]. Eugene Nickolov. Critical Information Infrastructure Protecion: Analysis, Evaluation and Expectations.

[28]. Heung Youl Youm, Euisun Paik. Knowledge Sharing Series. Issue 2. Cybersecurity.

[29]. ISA. ANSI/ISA–99.00.01–2007 Security for Industrial Automation and Control Systems Part 1: Terminology, Concepts, and Models.

[30]. ISA. ANSI/ISA–99.02.01–2009 Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program.

[31]. ISO. Information technology. Security techniques. Code of practice for information security management (ISO/IEC 27002:2005).

[32]. ISO. Information technology. Security techniques. Information security management systems. Requirements (ISO/IEC 27001:2005).

[33]. iso27000.es. http://www.iso27000.es/iso27000.html#section3c

[34]. iso27001security.com. http://www.iso27001security.com.

[35]. ITU. A Generic National ieee.es. Framework For Critical Information Infrastructure Protection (CIIP).

[36]. María José Caro Bejarano. La protección de las infraestructuras críticas.

[37]. Ministerio del Interior. Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.

[38]. Ministerio del Interior. Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas.

[39]. National Information Security Policy Council. The Second National Strategy on Information Security.

[40]. NERC. CIP-001-2a. Sabotage Reporting.

[41]. NERC. CIP-002-3. Cyber Security - Critical Cyber Asset Identification.

[42]. NERC. CIP-003-3. Cyber Security - Security Management Controls.

[43]. NERC. CIP-004-3a. Cyber Security - Personnel & Training.

[44]. NERC. CIP-005-3a. Cyber Security - Electronic Security Perimeter(s).

[45]. NERC. CIP-006-3c. Cyber Security - Physical Security of Critical Cyber Assets.

[46]. NERC. CIP-007-3a. Cyber Security — Systems Security Management.

[47]. NERC. CIP-008-3 Cyber Security - Incident Reporting and Response Planning.

[48]. NERC. CIP-009-3. Cyber Security - Recovery Plans for Critical Cyber Assets.

[49]. NIST. Special Publication 800-53 Revision 4 Final Public Draft. Security and Privacy Controls for Federal Information Systems and Organizations.

[50]. NIST. Special Publication 800-82. Guide to Industrial Control Sistems (ICS) Security.

[51]. OECD. Development of Policies for Protection of Critical Information Infrastructures.

[52]. S2Grupo. Protección de Infraestructuras Críticas 2011.

[53]. Securityfocus.com. http://www.securityfocus.com/news/6767.

[54]. The Information Security Policy Council. The Second Action Plan on Information Security Measures for Critical Infrastructures.

[55]. The Scottish Government. Secure and Resilient. A Strategic Framework for Critical National Infrastructure in Scotland.

[56]. The White House. Presidential Decision Directive (PDD) 39, U.S. Policy on Counterterrorism.

[57]. Ministerio de Defensa. Ciberseguridad. Retos y amenazas a la seguridad nacional en el ciberespacio.

[58]. Gabriel Jaime Correa Henao. Identificación y evaluación de amenazas a la seguridad de infraestructuras de transporte y distribución de electricidad.