



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

**SEGURIDAD EN EL CONTROL DE  
PROCESOS Y SCADA**

**Guía 1  
Comprender el riesgo del negocio**

Edita:



© Editor y Centro Criptológico Nacional, 2010  
NIPO: 076-10-072-4

Tirada: 1000 ejemplares  
Fecha de Edición: Enero de 2010

### **LIMITACIÓN ORIGINAL DE RESPONSABILIDAD**

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

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

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

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

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

### **AVISO LEGAL**

Quedan rigurosamente prohibidas, sin la autorización escrita del **Centro Criptológico Nacional**, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

## **PRÓLOGO**

El uso masivo de las tecnologías de la información y las telecomunicaciones (TIC), en todos los ámbitos de la sociedad, ha creado un nuevo espacio, el ciberespacio, donde se producirán conflictos y agresiones, y donde existen ciberamenazas que atentarán contra la seguridad nacional, el estado de derecho, la prosperidad económica, el estado de bienestar y el normal funcionamiento de la sociedad y de las administraciones públicas.

La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información en su artículo 4.e), y de protección de la información clasificada en su artículo 4.f), a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional en su artículo 9.2.f).

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

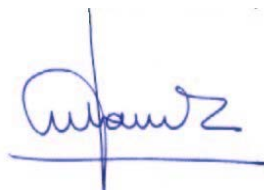
Una de las funciones más destacables del Centro Criptológico Nacional es la de elaborar y difundir normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los sistemas de las tecnologías de la información y las comunicaciones de la Administración, materializada en la existencia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

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

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

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

Febrero de 2010



Félix Sanz Roldán  
Secretario de Estado  
Director del Centro Criptológico Nacional

## ÍNDICE

0. INTRODUCCIÓN A LA TRADUCCIÓN.....	5
0.1. ALCANCE DE ESTA TRADUCCIÓN .....	5
0.2. CAMBIOS EN EL CONTENIDO .....	5
0.3. CAMBIOS EN EL FORMATO .....	6
1. INTRODUCCIÓN .....	7
1.1. TERMINOLOGÍA .....	7
1.2. ANTECEDENTES.....	7
1.3. MARCO DE SEGURIDAD EN EL CONTROL DE PROCESOS .....	8
1.4. FINALIDAD DE ESTA GUÍA.....	8
1.5. DESTINATARIOS .....	9
2. RESUMEN DE “COMPRENDER EL RIESGO DEL NEGOCIO” .....	9
3. ESTUDIAR EL RIESGO DEL NEGOCIO.....	10
3.1. CONTEXTO DE ESTA SECCIÓN DENTRO DEL MARCO GENERAL .....	10
3.2. JUSTIFICACIÓN .....	11
3.3. PRINCIPIOS DE BUENAS PRÁCTICAS.....	12
3.4. ORIENTACIÓN SOBRE LAS BUENAS PRÁCTICAS .....	12
3.4.1. COMPRENDER LOS SISTEMAS .....	13
3.4.2. ESTUDIO DEL RIESGOS DEL NEGOCIO .....	14
3.4.3. COMPRENDER LAS AMENAZAS.....	15
3.4.4. COMPRENDER EL IMPACTO .....	17
3.4.5. COMPRENDER LAS VULNERABILIDADES.....	18
3.4.6. RESULTADOS DE LA COMPRESIÓN DEL RIESGO DEL NEGOCIO .....	19
3.5. APLICANDO ESTA APROXIMACIÓN AL ESTUDIO DEL RIESGO .....	19
3.5.1. PASO 1 - ESTUDIO DEL RIESGO DE LA EMPRESA A ALTO NIVEL .....	19
3.5.2. PASO 2 – ESTUDIO DEL RIESGO DE LOS CENTROS/SISTEMAS INDIVIDUALES .....	20
4. REALIZAR ESTUDIOS CONTINUOS DEL RIESGO DEL NEGOCIO .....	21
4.1. CONTEXTO DE ESTA SECCIÓN DENTRO DEL MARCO GENERAL .....	21
4.2. JUSTIFICACIÓN .....	21
4.3. PRINCIPIOS DE BUENAS PRÁCTICAS.....	21
4.4. ORIENTACIÓN SOBRE LAS BUENAS PRÁCTICAS .....	21
5. AGRADECIMIENTOS .....	23

## ANEXOS

ANEXO A. REFERENCIAS .....	24
A.1. REFERENCIAS GENERALES SCADA .....	24
A.2. REFERENCIAS EN ESTA TRADUCCIÓN .....	26
ANEXO B. GLOSARIO DE TÉRMINOS Y ABREVIATURAS .....	27
B.1. GLOSARIO DE TÉRMINOS .....	27
B.2. GLOSARIO DE SIGLAS .....	27
B.3. TABLA DE EQUIVALENCIAS DE LA TRADUCCIÓN .....	28

## FIGURAS

FIGURA 1: DÓNDE ENCAJA ESTA GUÍA DENTRO DEL MARCO DE BUENAS PRÁCTICAS .....	8
FIGURA 2: ESTRUCTURA DEL DOCUMENTO “COMPRENDER EL RIESGO DEL NEGOCIO” .....	10
FIGURA 3: CÓMO ENCAJA “COMPRENDER EL RIESGO DEL NEGOCIO” EN ESTE MARCO .....	11
FIGURA 4: PRINCIPALES PASOS EN EL ESTUDIO DEL RIESGO DEL NEGOCIO .....	12
FIGURA 5: ESTUDIO DEL RIESGO DE LA EMPRESA A ALTO NIVEL .....	19
FIGURA 6: MATRIZ DE RIESGO DE LA EMPRESA A ALTO NIVEL .....	20

## TABLAS

TABLA 1. TABLA DE RIESGO DE LOS CENTROS .....	20
---	----

## 0. INTRODUCCIÓN A LA TRADUCCIÓN

### 0.1. ALCANCE DE ESTA TRADUCCIÓN

1. Como parte del acuerdo de colaboración entre el Centro para la Protección de la Infraestructura Nacional de Reino Unido (CPNI en adelante) y el Centro Criptológico Nacional de España (CCN en adelante), se han traducido la colección de guías "Process Control and SCADA Security" publicadas por el CPNI. La presente traducción se corresponde con la versión 2 de las guías del CPNI, publicadas en Junio de 2008, y que consta de las siguientes guías:
  - 00752 - Process Control and SCADA Security
  - 00753 - Process Control and SCADA Security Guide 1. Understand the business risk
  - 00754 - Process Control and SCADA Security Guide 2. Implement secure architecture
  - 00755 - Process Control and SCADA Security Guide 3. Establish response capabilities
  - 00756 - Process Control and SCADA Security Guide 4. Improve awareness and skills
  - 00757 - Process Control and SCADA Security Guide 5. Manage third party risk
  - 00758 - Process Control and SCADA Security Guide 6. Engage projects
  - 00759 - Process Control and SCADA Security Guide 7. Establish ongoing governance
2. En el momento de publicación de esta traducción, las guías originales pueden encontrarse en <http://www.cpni.gov.uk/WhatsNew/scada.aspx> ([Ref.- 6])
3. Este documento traduce la siguiente guía:
  - 00753 - Process Control and SCADA Security Guide 1. Understand the business risk
4. El CCN ha publicado la guía CCN-STIC-480 "Seguridad en sistemas SCADA" que, junto con el resto de guías publicadas y utilizando estas traducciones adapta la seguridad al contexto de España.
5. El CCN se adhiere a la cláusula de responsabilidad del CPNI sobre el contenido de la presente guía.

### 0.2. CAMBIOS EN EL CONTENIDO

6. Por coherencia con el resto de guías CCN-STIC, se han añadido la portada, la Limitación de Responsabilidad y el Prólogo el presente capítulo 0 de introducción.
7. Se ha traducido de todos los apartados desde el 1 hasta el final, incluyendo la Cláusula Original de Exención de Responsabilidad, y los Agradecimientos. Se respeta el contenido original, con las siguientes salvedades:
  - Cuando una traducción requiere una explicación, (ej., cuando el conocimiento de los términos del documento original pueda suponer algún matiz), se incluyen notas a pie

de página, precedidas de “N.T.”, indicando matices de la traducción. Debido a este hecho, el orden de las notas al pie no se corresponde con el orden en la guía original

- Siempre que aparece una referencia a un recurso en inglés y exista un recurso equivalente en español o relativo a España, se habrá sustituido. Las referencias a recursos del CPNI han sido convertidas a referencias del CCN-CERT siempre que ha sido posible. La referencia original se indicará a pie de página como una N.T.
  - Los nombres propios y las siglas se han traducido. Las equivalencias entre referencias en inglés y en español se lista en el apartado “B.3. Tabla de equivalencias de la traducción” del Glosario de Términos y Abreviaturas”. No se han traducido las siglas CPNI, SCADA, PA Consulting Group.
8. Se han añadido los Anexos comunes a las guías CCN-STIC, con el siguiente contenido:
9. **ANEXO A. Referencias:** Contiene todas las referencias que aparecen tanto en el documento original en inglés como en el documento actual. Los Anexos originales de referencias se han integrado en este Anexo. Las referencias se han numerado en base al resto de guías CCN-STIC.
- A.1. Referencias generales SCADA: Contiene el Anexo “*General SCADA References*” del documento original del CPNI.
  - A.2. Referencias en esta traducción: Contiene las nuevas referencias añadidas en este documento de traducción.
10. **ANEXO B. Glosario de Términos y Abreviaturas:** Contiene las definiciones de los términos y abreviaturas que aparecen en el texto.
- Incluye las definiciones que en el original se incluían al final del apartado 2 “Resumen de “Comprender el Riesgo del Negocio””
  - B.3. Tabla de equivalencias de la traducción: Contiene las equivalencias entre los términos técnicos en inglés, utilizados en el documento original, y los términos en español usados en la traducción.

### 0.3. CAMBIOS EN EL FORMATO

11. El formato de la guía original se ha adaptado al formato utilizado en el resto de guías CCN-STIC editadas por el CCN. Esto implica algunas adaptaciones que se explican a continuación:
12. Todos los párrafos han sido numerados.
13. El formato de algunos títulos, especialmente de cuarto nivel y sucesivos, ha sido adaptado.

## 1. INTRODUCCIÓN

### 1.1. TERMINOLOGÍA

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

### 1.2. ANTECEDENTES

15. Los sistemas de control de procesos y SCADA hacen uso y se están volviendo progresivamente más dependientes de las tecnologías de la información (TI) estándar. Estas tecnologías, como Microsoft Windows, TCP/IP, navegadores Web y las tecnologías inalámbricas, en uso creciente, están reemplazando a las tecnologías propietarias convencionales y más a medida que los sistemas de control de procesos son sustituidos por software comercial .
16. A pesar de que existen beneficios empresariales positivos derivados de este desarrollo, esta transformación conlleva dos principales preocupaciones:
17. Primero, tradicionalmente los sistemas de control de procesos han sido diseñados sólo con el propósito de controlar y proteger. Debido a la necesidad de conectividad, por ejemplo para extraer información bruta sobre la planta o para poder realizar descargas directas a la producción, estos sistemas, que estaban aislados, se están conectando a redes abiertas. De ese modo se exponen a nuevas amenazas no esperadas, como gusanos<sup>1</sup>, virus y hackers). La seguridad a través del secreto ya no es un tipo de defensa válido.
18. Segundo, el software comercial y el hardware de propósito general se está usando para sustituir sistemas de control de procesos propietarios. Muchas medidas estándar de protección de la seguridad en TI utilizadas normalmente en estas tecnologías no han sido adaptadas a un entorno de control de procesos. Por tanto, las medidas de seguridad disponibles para proteger los sistemas de control y mantener el entorno seguro pueden ser insuficientes.
19. En caso de que se explotaran estas vulnerabilidades habría consecuencias potencialmente serias. Los efectos de un ataque electrónico en los sistemas de control de procesos pueden incluir, por ejemplo: denegación del servicio, pérdida de la integridad, pérdida de confidencialidad, pérdida de imagen (reputación) empresarial, y el impacto en las condiciones de trabajo y el medio ambiente.

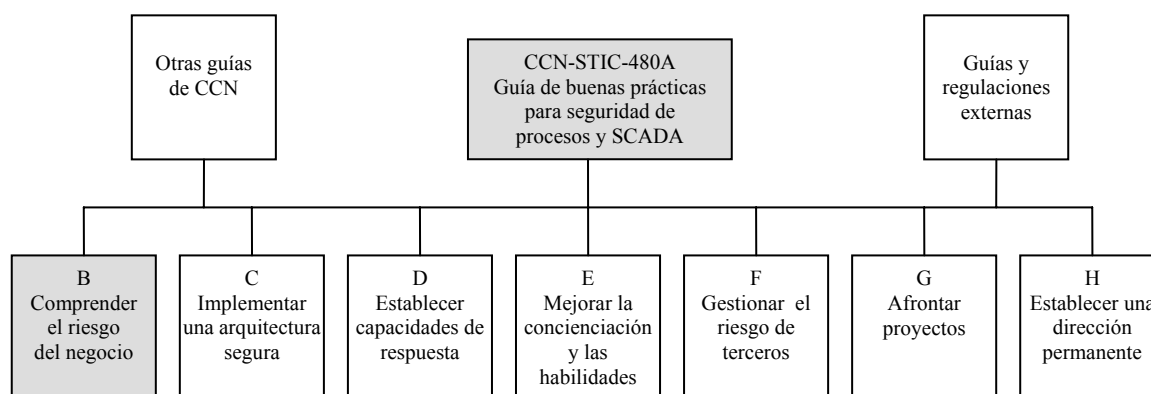
---

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



### 1.3. MARCO DE SEGURIDAD EN EL CONTROL DE PROCESOS

20. Aunque los sistemas de control de procesos están a menudo basados en tecnologías TI estándar, sus entornos operacionales difieren significativamente de un entorno TI corporativo. Pueden aprovecharse muchas lecciones de la experiencia adquirida por los expertos de seguridad en TI y, tras la adaptación de algunas herramientas y técnicas de seguridad estándar, se pueden usar para proteger sistemas de control de procesos. Otras medidas de seguridad estándar pueden ser completamente inapropiadas o no estar disponibles para su uso en un entorno de control.
21. Este marco de seguridad en el control de procesos se basa en las buenas prácticas de la industria para seguridad en el control de procesos y en TI. Está centrado en siete temas clave para el uso de las tecnologías TI estándar en el entorno de control de procesos y SCADA. Este marco pretende ser un punto de referencia para que una organización comience a desarrollar y adaptar la seguridad en el control de procesos adecuado a sus necesidades. Los siete módulos del marco se muestran a continuación en la Figura 1.



**FIGURA 1: DÓNDE ENCAJA ESTA GUÍA DENTRO DEL MARCO DE BUENAS PRÁCTICAS**

22. Cada uno de estos módulos es descrito con mayor detalle en su documento aparte, este documento ofrece una visión general de todas las guías de este marco. Todas las guías de este marco pueden encontrarse en la página Web de CCN en <https://www.ccn-cert.cni.es> ([Ref.- 43]<sup>2</sup>).

### 1.4. FINALIDAD DE ESTA GUÍA

23. La colección de guías “**Seguridad en el Control de Procesos y SCADA**” del CCN<sup>3</sup>, proponen un marco que consta de siete módulos para abordar la seguridad en el control de procesos. Esta guía “**Comprender el riesgo del negocio**” se basa en los fundamentos explicados en la guía de buenas prácticas y proporciona orientación para estudiar el riesgo del negocio y el estudio continuo de este riesgo.
24. En esta guía no incluye técnicas ni metodologías detalladas de estudio del riesgo.

<sup>2</sup> N.T.: [Ref.- 6]

<sup>3</sup> N.T.: Traducción de las guías del CPNI([Ref.- 6]) y complementadas con la guía “Seguridad en Sistemas SCADA” (**¡Error! No se encuentra el origen de la referencia.**)

## 1.5. DESTINATARIOS

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

- Ingenieros de telemetría SCADA y de control y automatización de procesos.
- Especialistas en la seguridad de la información.
- Especialistas en seguridad física.
- Líderes empresariales.
- Gestores de riesgos.
- Encargados de las condiciones de trabajo.
- Ingenieros que operan los sistemas.
- Auditores.

## 2. RESUMEN DE “COMPRENDER EL RIESGO DEL NEGOCIO”

26. El primer paso para mejorar la seguridad de los sistemas de control de procesos es obtener una comprensión exhaustiva de los riesgos de negocio en el contexto de la seguridad electrónica. Los riesgos de negocio son una función de las amenazas, impactos y vulnerabilidades. Sólo con un buen conocimiento de los riesgos de negocio, una organización puede tomar decisiones informadas sobre lo que deberían ser los niveles apropiados de protección.

27. Todas las mejoras de la seguridad deben basarse en el nivel de riesgo a que se enfrenta un sistema en concreto para garantizar un nivel adecuado de protección. Por ejemplo, un sistema de bajo riesgo es probable que exija menos protección que un sistema de alto riesgo. Sin embargo, estas medidas de protección necesitan ser desplegadas correctamente para lograr el beneficio completo de la seguridad. La comprensión de los riesgos de negocio es un factor clave para determinar dónde se aplican estas medidas de protección.

28. Comprender el riesgo del negocio no es un ejercicio único, es un proceso continuo. Una vez que se ha llevado a cabo un estudio del riesgo y se han aplicado las medidas relevantes de mejora de la seguridad, es importante mantener vigilados los riesgos de negocio a medida que pasa el tiempo, las amenazas cambian y se identifican más vulnerabilidades.

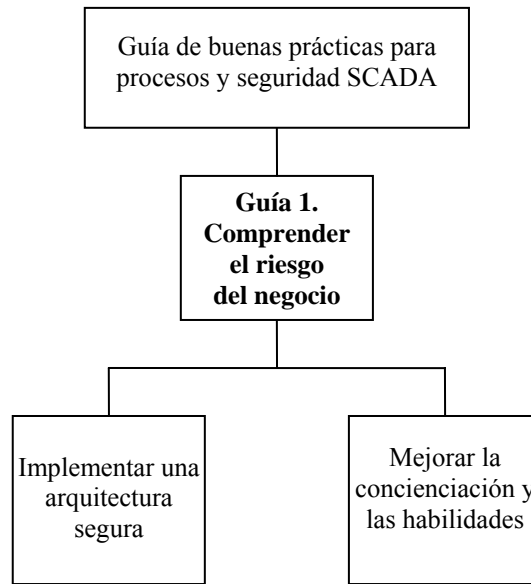


FIGURA 2: ESTRUCTURA DEL DOCUMENTO "COMPRENDER EL RIESGO DEL NEGOCIO"

29. Definiciones<sup>4</sup>.

### 3. ESTUDIAR EL RIESGO DEL NEGOCIO

#### 3.1. CONTEXTO DE ESTA SECCIÓN DENTRO DEL MARCO GENERAL

30. Estudiar el riesgo del negocio precede a todos los temas en este marco de seguridad en el control de procesos, y los resultados de esta tarea se utilizan en muchos otros módulos del marco.

---

<sup>4</sup> N.T.: Las traducciones aquí incluidas en el original se han movido al "ANEXO B. Glosario de Términos y Abreviaturas"

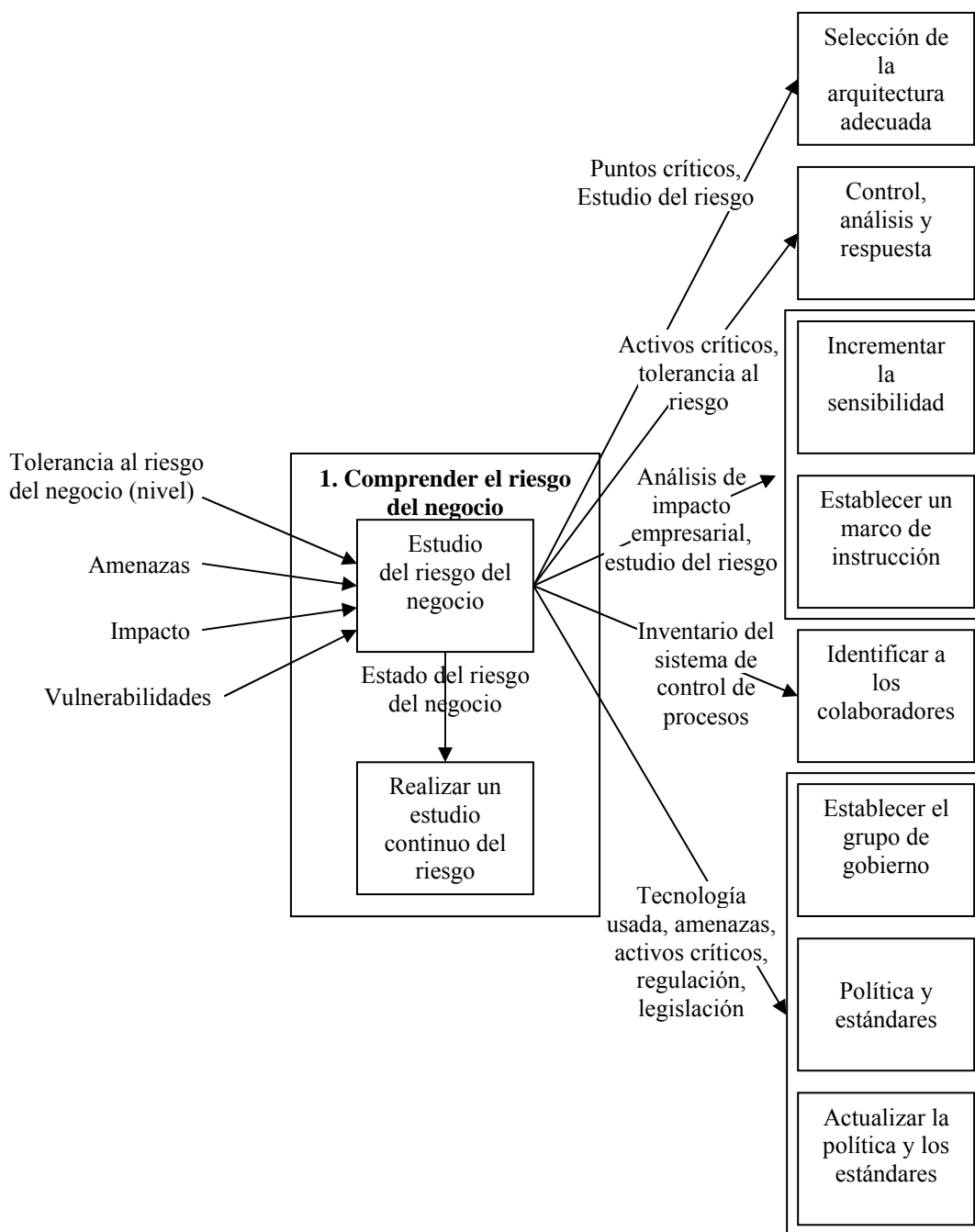


FIGURA 3: CÓMO ENCAJA “COMPRENDER EL RIESGO DEL NEGOCIO” EN ESTE MARCO

### 3.2. JUSTIFICACIÓN

31. Las organizaciones necesitan comprender el riesgo al que se enfrentan para determinar qué tolerancia del riesgo es adecuada y qué mejoras en seguridad se necesitan para reducir el nivel de exposición a los riesgos y alcanzar la tolerancia al riesgo.

### 3.3. PRINCIPIOS DE BUENAS PRÁCTICAS

32. Los principios generales de buenas prácticas del documento general “CCN-STIC-480A – Guía de buenas prácticas – Seguridad en el Control de Procesos y SCADA” ([Ref.- 45]), son los siguientes:

33. Realizar un estudio formal del riesgo de los sistemas de control de procesos para:

- **Comprender los sistemas:** realizar una auditoría y una evaluación formal del inventario de los sistemas de control de procesos. Es importante capturar, documentar y tener bajo control de cambios: qué sistemas existen, cuál es el papel de cada sistema, sus tareas y sus puntos críticos de seguridad, dónde se encuentran, quién es el propietario designado de cada sistema, quién gestiona cada sistema, quién da soporte a cada sistema y cómo los sistemas interactúan. Identificar el alcance de los sistemas y la identidad de todas las interfaces, *hardware* y *software*<sup>5</sup>.
- **Comprender las amenazas:** Identificar y evaluar las amenazas a las que se enfrentan los sistemas de control de procesos. Las posibles amenazas incluyen: denegación de servicio, ataques dirigidos, incidentes accidentales, accesos y controles no autorizados, o infecciones de virus, código malicioso instalado en las máquinas, gusanos o troyanos.
- **Comprender el impacto:** Identificar los posibles impactos y las consecuencias que una amenaza puede producir en los sistemas de control de procesos. Ejemplos de tales consecuencias incluyen: pérdida de imagen (reputación), violación de requisitos reglamentarios (ej., de condiciones de trabajo, medioambientales), incapacidad para cumplir compromisos empresariales o pérdidas financieras.

Nota: Cuando los sistemas de control de procesos son elementos críticos de suministro para otros servicios clave, el impacto no debe limitarse a la empresa, pues pueden tener graves consecuencias que pongan vidas en peligro en otros sitios.

- **Comprender las vulnerabilidades:** Llevar a cabo un estudio de las vulnerabilidades de los sistemas de control de procesos. Dicha revisión debe incluir: evaluación de la infraestructura, sistemas operativos, aplicaciones, *software* usado, conexiones de red, accesos remotos, y procesos y procedimientos.

### 3.4. ORIENTACIÓN SOBRE LAS BUENAS PRÁCTICAS

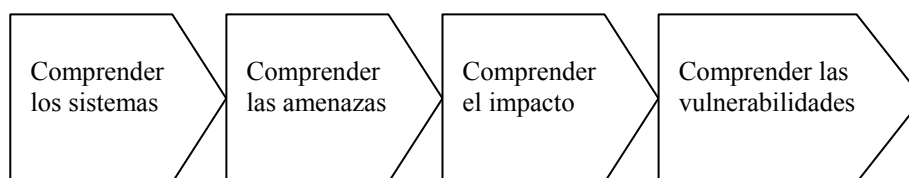


FIGURA 4: PRINCIPALES PASOS EN EL ESTUDIO DEL RIESGO DEL NEGOCIO

<sup>5</sup> N.T. Original: *hard and soft*.

### 3.4.1. COMPRENDER LOS SISTEMAS

34. Con el fin de entender los riesgos de seguridad de los sistemas de control de procesos a que se enfrenta una empresa, es necesaria una comprensión profunda de los sistemas que constituyen esa empresa. El primer paso en este proceso es acordar el ámbito que cubrirá este análisis de riesgos. Los límites del ámbito de aplicación necesitan ser dibujados claramente y los sistemas que se identifiquen fuera de ese ámbito deben tenerse claro en qué ámbito se encuentran. También debe buscarse una garantía adecuada del nivel de protección de la seguridad en estos sistemas.
35. Puede que los sistemas de control de procesos fueran instalados hace muchos años y puede que un conocimiento detallado de su funcionamiento y configuración no sea de fácil obtención. Con el fin de comprender el riesgo del negocio esta información debe determinarse (aunque no esté disponible inmediatamente), e incluirse en un completo inventario del sistema.
36. Hay una serie de cuestiones que deben considerarse al realizar un inventario:
- ¿Cuántas localizaciones, centros<sup>6</sup>, sistemas y activos existen?
  - ¿Qué sistemas hay en cada centro?
  - ¿Dónde encajan cada centro y sistema en el ‘valor’ global o en la cadena de ‘suministro’?
  - ¿Cuáles son los puntos críticos de negocio y operativos de cada centro o sistema?
  - ¿Qué contribuciones hace el sistema a la seguridad del proceso y del personal?
  - ¿Qué producción y otras operaciones son llevadas a cabo por el centro?
  - ¿Hay alguna implicación de condiciones de trabajo y medio ambiente o de otro reglamento?
  - ¿Los activos forman parte de la Infraestructura Crítica Nacional (ICN)? Para más información acerca de lo que puede considerarse ICN, consultar el portal web donde se proporciona más información sobre el Catálogo de Infraestructuras Críticas Nacionales en ([Ref.- 43]<sup>7</sup>).
  - ¿Quién es el responsable único (RU) para cada centro, sistema y activo?
  - ¿Quiénes son los principales proveedores y colaboradores relacionados con los sistemas?
  - ¿Cuáles son las organizaciones de apoyo en el centro (TI, control de procesos, colaboradores remotos, en el centro o externos)?
  - ¿Cuáles son los activos críticos del sistema en el centro?
  - ¿Qué conexiones y alimentaciones de entran y salen del sistema de control (incluyendo tanto alimentaciones manuales de datos como conexiones electrónicas)?
  - ¿Hay algún problema conocido con los sistemas?

---

<sup>6</sup> N.T.: Aunque la traducción literal de *site* es “sitio”, no resulta lo bastante descriptivo en el entorno tecnológico, en el que se aplica a oficinas, CPD, etc., y se ha optado por la palabra “centro”

<sup>7</sup> N.T.: Este portal se acaba de abrir y esta en proceso de proporcionar información.

- ¿Cuáles son los proyectos en curso o programados?
  - ¿Cuáles son los datos de contacto para el personal local y los proveedores?
  - ¿Qué dependencias tiene el centro?
  - ¿Hay resúmenes y diagramas detallados de los sistemas y la red?
  - ¿Está protegida toda la documentación y se siguen procedimientos de gestión de cambios?
37. Las respuestas a estas preguntas permiten a la organización crear un inventario de control de procesos. El inventario es un bloque fundamental para construir el marco de seguridad de control de procesos y es el punto de partida de muchos otros temas y secciones. Este inventario debe estar suficientemente detallado como para proporcionar una adecuada apreciación del riesgo.
38. Los inventarios son muy difíciles de generar y mantener actualizados. Una situación ideal consiste en mantener un inventario único podría ser el que pudiera proporcionar un resumen único con un nivel detallado de información. Si esto se hace para una gran organización puede no ser práctico realizar un único inventario detallado. Un inventario jerárquico puede ser más apropiado, donde un inventario central contiene referencias a los inventarios de los centros locales, que contienen el detalle.
39. Cabe señalar que estos inventarios son una fuente de información sensible, que puede ser muy útil para un atacante. En consecuencia, estos inventarios deben protegerse. El acceso a estos inventarios debe limitarse al mínimo número de personas que necesiten acceder a esta información.
40. Dependencias: Es importante comprender cualquier dependencia entre sistemas (tanto para sistemas estudiados como fuera de estudio). Algunas partes de un sistema industrial pueden depender de los resultados de otro sistema en la cadena de suministro. Por ejemplo, una refinería de petróleo puede ser dependiente del gasoducto que le alimente. Por consiguiente, al determinar el riesgo del negocio de una refinería, las dependencias hijo-padre<sup>8</sup> tales como las tuberías de suministro deben considerarse adecuadamente en el estudio del riesgo. Del mismo modo, las dependencias padre-hijo<sup>9</sup> también deben ser consideradas. Si se amplía el ejemplo anterior para incluir una planta de productos químicos que utilizan un producto de la refinería, la planta química serían una dependencia padre-hijo y debería estar sujeta a un cierto nivel de control en el estudio del riesgo.

### 3.4.2. ESTUDIO DEL RIESGO DEL NEGOCIO

41. El riesgo del negocio se puede definir de muchas maneras. Una definición útil consiste en expresar el riesgo en función de la probabilidad de que se produzca ese riesgo y el impacto que tendría lugar si ese riesgo se produjera. El riesgo es la suma de todos los riesgos individuales de las amenazas identificadas.

---

<sup>8</sup> N.T.: El original *upstream* presenta un símil con el flujo de un río.

<sup>9</sup> N.T.: El original *downstream* presenta un símil con el flujo de un río.

**42. Riesgo del negocio = F (Probabilidad x Impacto)<sup>10</sup>. (1)**

43. La probabilidad de que se produzca un riesgo puede ser expresada en términos de amenaza, atractivo del blanco y vulnerabilidad,

**44. Probabilidad = F (Amenaza x Atractivo x Vulnerabilidad). (2)**

45. El término “atractivo” se refiere a cuan atractivo un blanco puede ser para un atacante potencial. Por ejemplo, ¿un atacante puede encontrar una planta de energía nuclear como un objetivo más atractivo que una planta de fabricación de bolsas de papel! Este término, atractivo, puede no ser aplicable a ciertos riesgos, como la infección de un gusano. La mayoría de los gusanos infectan de manera indiscriminada y, por tanto, cualquier sistema vulnerable está en peligro. En consecuencia, el término no es relevante en este caso.

46. El término atractivo contribuye a la probabilidad de que se produzca un riesgo (es decir, un objetivo atractivo es más probable que sea atacado) y por sencillez, a menudo puede incorporarse dentro del término amenaza.

47. Combinando (1) y (2) se obtiene una expresión para el riesgo del negocio en términos de amenaza, atractivo, impacto y vulnerabilidades.

**48. Riesgo del negocio = F(Amenaza x Impacto x Atractivo x Vulnerabilidad) (3)**

49. Las siguientes secciones describen el resto de elementos necesarios para entender el riesgo del negocio.

**3.4.3. COMPRENDER LAS AMENAZAS**

50. Las amenazas a la seguridad del control de procesos son numerosas y pueden surgir de una variedad de fuentes. Es importante tener en cuenta las amenazas comunes, pero también deben tenerse en cuenta una empresa en particular o un tipo de organización. Por ejemplo, una compañía petrolera que opera en las regiones del mundo especialmente sensibles puede tener un perfil de amenazas distinto al de una empresa de transporte que opere exclusivamente en el Reino Unido.

51. Las fuentes de amenazas que deben considerarse incluyen (pero no deben limitarse a):

- *Hackers*
- Atacantes internos
- Delincuentes
- Asesores informativos<sup>11</sup> ilegales
- Personal descontento
- Personal realizando acciones no autorizadas (ej., acceder a Internet)
- Inteligencia corporativa

<sup>10</sup> Guía para analizar y gestionar vulnerabilidades de seguridad en centros químicos. AIChE - 2003

N.T. Original: Guidelines for analysing and managing the security vulnerabilities of fixed chemical sites. AIChE - 2003.

N.T.: AIChE es el Instituto Americano de Ingenieros Químicos ([www.aiche.org](http://www.aiche.org))

<sup>11</sup> N.T.: *Information brokers*



- Contratistas
- Servicios de inteligencia extranjeros
- Crimen organizado
- Terroristas
- Manifestantes y activistas (ej, medioambientales, políticos, pro-derechos de los animales)

52. Los tipos de amenazas que deben considerarse incluyen (pero no deben limitarse a):

- Gusanos (genéricos y específicos)
- *Hackers* (internos, externos, externos con ayuda interna)
- Virus
- Troyanos o puertas traseras
- *Bots* y *spyware*
- Pérdida de integridad
- Pérdida de disponibilidad (denegación de servicio)
- Pérdida de confidencialidad
- Control no autorizado

53. Estas amenazas son genéricas, por lo que es útil aplicarlas en escenarios de ejemplo para que su impacto y las vulnerabilidades relacionadas puedan considerarse más específicamente, teniendo especial cuidado en garantizar que los escenarios escogidos son lo suficientemente amplios para incluir todas las amenazas. Los escenarios de ejemplo de consecuencias incluyen, pero no se limitan a:

- Pérdida sistémica de todas las máquinas basadas en un sistema operativo (ej., Windows, Unix, VMS, etc).
- Pérdida sistémica de tecnologías de red Ethernet/IP.
- Pérdida (o reducción) de la funcionalidad de los sistemas de control de procesos.
- Pérdida de conectividad entre los sistemas de control de procesos y
  - Redes corporativas
  - Otros sistemas (ej., cadena de suministro, sistemas de laboratorio u otras empresas)
  - Dispositivos de mando a distancia.
- Cambio no autorizado de puntos de ajuste o configuración por acciones maliciosas o inadvertidas.
- Cambio accidental de la configuración del sistema por un usuario autorizado.
- Ataque por un empleado descontento.
- Pérdida de integridad o disponibilidad de datos históricos
- Pérdida de la confidencialidad del proceso y su información relacionada.

### 3.4.4. COMPRENDER EL IMPACTO

54. Una vez que las amenazas se han convertido en escenarios de amenaza es mucho más fácil examinar el impacto que pueden causar. Hay que considerar cada escenario para cada centro, sistema o subsistema y considerar cuál sería el impacto en la vida real, no sólo en ese sistema, sino también para cualquier sistema del que dependan. Por ejemplo, al considerar un SCD que controla una central eléctrica para una planta de productos químicos, habría que examinar el impacto que tendría la pérdida dicho sistema en el funcionamiento de la planta de productos químicos, incluidos los efectos sobre seguridad. Al determinar el impacto, hay que hacer referencia a los inventarios y a las dependencias ya identificadas.
55. **Clasificación del impacto:** Es habitual en el estudio del riesgo cuantificar los posibles impactos o consecuencias de una amenaza en términos de valor monetario. Se da este caso particularmente al considerar el riesgo financiero. Sin embargo, al considerar el riesgo para la seguridad del control de procesos puede ser difícil determinar los impactos financieros exactos de los incidentes de seguridad. Esta cuantificación de las consecuencias financieras supone un campo completo de especialización por sí mismo y puede ser excesivo para estudiar los riesgos para la seguridad del control de procesos a fin de determinar las medidas de seguridad adecuadas.
56. Con el fin de evitar un esfuerzo excesivo en la determinación de los impactos de un riesgo, a menudo es posible expresar el impacto en términos de lenguaje de negocio en vez de cómo una cifra monetaria. Por ejemplo, ser capaz de comunicar el impacto de una posible amenaza a la que enfrenta un sistema de control de procesos en términos del efecto que tendría en el sistema hace el riesgo mucho más comprensible. Por ejemplo, el impacto de la infección por un gusano en un sistema de control podría dar como resultado la decisión de detener las operaciones de una planta.
57. Ejemplos de posibles descripciones de impactos en la ‘vida real’ son los siguientes:
58. **Eventos de condiciones de trabajo, medioambientales o daños a la planta:** un caso que provoque como resultado daños a las personas, el medio ambiente y la planta.
59. **Incumplimiento de los requisitos reglamentarios o eventos menores de condiciones de trabajo y medioambientales:** un caso que provoque que el centro no cumplan los requisitos reglamentarios. Por ejemplo, un incumplimiento (por ejemplo, la quema excesiva en una planta de productos químicos o el arranque o apagado de una refinería) o la pérdida de datos históricos reglamentarios.
60. **Cierre forzoso controlado de operaciones:** un evento que provoque que el sistema de apagado de emergencia sea ejecutado automáticamente sin intervención humana. Por ejemplo, cuando se pierde la visibilidad de todos o algunos de los procesos de producción.
61. **Cierre voluntario controlado de operaciones:** un caso que provoque que un centro decida parar sus operaciones. Por ejemplo, cuando se pierde la visibilidad de todos o algunos de los procesos de producción.
62. **Reducción en la eficiencia operativa:** un caso que pueda provocar que la planta continúe funcionando de un modo menos eficaz o rentable o produzca una reducción en la producción. Por ejemplo, si la mezcla de materias primas se cambia provocando que el producto se produzca de manera menos eficiente.

63. **Sin impacto:** Ningún impacto en las operaciones.
64. Otros impactos que deben ser considerados son los siguientes:
- Pérdida de información confidencial
  - Daños a la Infraestructura Crítica Nacional
  - Pérdida de la continuidad del negocio
  - Reputación
  - Cadena de valores o suministro.
65. **Variación del impacto con el tiempo:** Al considerar el impacto de una amenaza particular, es importante considerar cómo la amenaza puede variar con el tiempo. Por ejemplo, un incidente puede tener inicialmente un menor impacto pero si se le permite que continúe un largo período de tiempo la gravedad del impacto podría ser mayor. Un ejemplo de ello es la pérdida de la información de vigilancia medioambiental que puede no ser grave a corto plazo, pero probablemente que sea mucho más crítica a largo plazo debido los requisitos legales y regulativos de disponibilidad e integridad de la información.
66. **Impactos sucesivos:** Debe ser considerado el efecto de impactos coincidentes o sucesivos, especialmente cuando pueden ser producidos por una causa común.

#### 3.4.5. COMPRENDER LAS VULNERABILIDADES

67. Comprender las vulnerabilidades implica un examen detallado de todos los elementos del sistema (ej., servidores, estaciones de trabajo, infraestructura de red, etc.), para determinar las vulnerabilidades que existen. Ejemplos de áreas de vulnerabilidad común incluyen, pero no están limitadas a:
- Conexiones a otros sistemas
  - Acceso remoto
  - Seguridad física
  - Protección antivirus
  - Control de acceso
  - Contraseñas y cuentas
  - Parcheados de seguridad
  - Monitorización del sistema
  - Resistencia y continuidad del sistema
  - Terceros que producen código para los sistemas de la planta.
68. Al considerar la seguridad del sistema completo es importante recordar que es un sistema sólo está tan protegido como el eslabón más débil. Por ejemplo, hay poco beneficio en tener un cortafuegos bien configurado y administrado si tiene una conexión con módem poco protegida al mundo exterior que evita el cortafuegos.

### 3.4.6. RESULTADOS DE LA COMPRENSIÓN DEL RIESGO DEL NEGOCIO

69. Los principales resultados son:

- Inventario.
- Centros y sistemas priorizados.
- Lista de las principales amenazas basada en el estudio del impacto.
- Vulnerabilidades priorizadas.

### 3.5. APLICANDO ESTA APROXIMACIÓN AL ESTUDIO DEL RIESGO

70. La mayor parte de esta guía se centra en el nivel de centro o de sistema. En una gran organización con muchos centros y geografías a considerar, puede no ser práctico trabajar a este nivel. Por lo tanto, es necesario dividir el problema en tareas más manejables. Esto se puede hacer realizando un estudio somero del riesgo, a alto nivel, que incluya toda la organización o empresa y, a continuación, realizar un estudio más detallado para cada uno de los sistemas o centros existentes (Figura 5).

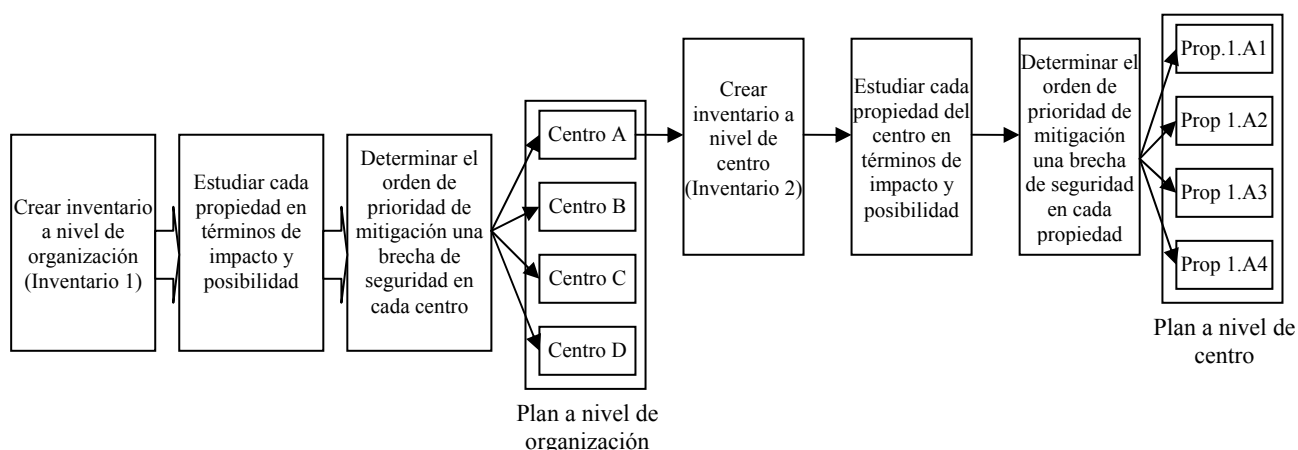


FIGURA 5: ESTUDIO DEL RIESGO DE LA EMPRESA A ALTO NIVEL

#### 3.5.1. PASO 1 - ESTUDIO DEL RIESGO DE LA EMPRESA A ALTO NIVEL

71. La primera iteración del estudio del riesgo proporciona visibilidad a nivel empresarial del riesgo para la seguridad del control de procesos. Proporcionará una indicación de las brechas de seguridad con mayor impacto para la empresa, teniendo en cuenta la “cadena de valores”, interdependencias e impactos que tienen importancia a nivel empresarial. El análisis proporcionará a la empresa los problemas prioritarios de seguridad y los centros que deberán abordar primero.

72. Una manera fácil de determinar el orden de prioridad es situar las puntuaciones de los activos en una Rejilla de Boston (matriz de riesgo). Los parámetros de riesgo señalados anteriormente pueden ser puestos en una Tabla de Riesgos de los Centros, Tabla 1. En algunos casos, cada uno de los factores (Amenaza, Atractivo y Vulnerabilidad), recibe la misma ponderación, en otras ocasiones pueden ser ponderadas para reflejar la situación.

Se debe tener cuidado al agregar diferentes centros para garantizar que se está utilizando el mismo estudio del riesgo, o el perfil de riesgo se verá distorsionado.

Centros	Amenaza (Am)	Atractivo (At)	Vulnerabilidad (V)	Probabilidad (Am x At x V)	Impacto (I)
Centro A	Medio	Bajo	Bajo	Bajo	Bajo
Centro B	Alto	Alto	Alto	Alto	Alto
Centro C	Bajo	Bajo	Bajo	Bajo	M
Centro D	Medio	Medio	Bajo	Medio	Alto

Tabla 1. TABLA DE RIESGO DE LOS CENTROS

73. Desde esta tabla de riesgos, los centros pueden ubicarse en una Rejilla de Boston (Figura 6) utilizando la probabilidad y el valor del impacto para indicar los centros de alto riesgo y permitir que se defina una adecuada prioridad para el centro.

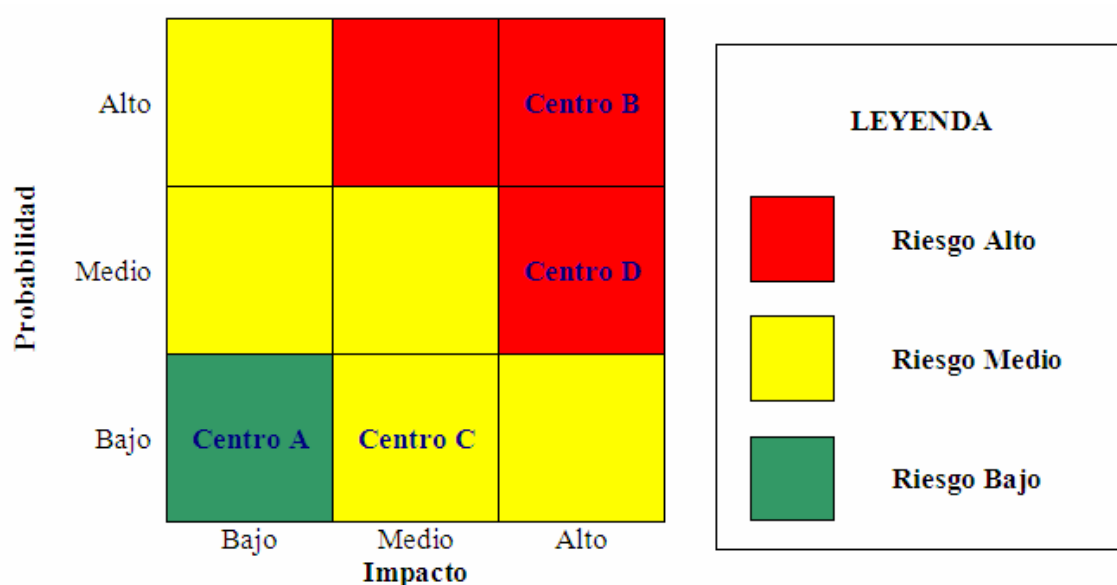


FIGURA 6: MATRIZ DE RIESGO DE LA EMPRESA A ALTO NIVEL

### 3.5.2. PASO 2 – ESTUDIO DEL RIESGO DE LOS CENTROS/SISTEMAS INDIVIDUALES

74. El estudio del riesgo de los centros se basa en el estudio del riesgo de la empresa a alto nivel y desarrolla las principales áreas de riesgo identificadas. El estudio del riesgo de los centros analiza el riesgo en el siguiente nivel de detalle y considera los activos críticos detalladamente.

75. Tras seleccionar la prioridad inicial del centro para la organización, el mismo proceso puede ser utilizado en a nivel de centro para ayudar a que cada centro determine sus prioridades. Cada centro crea un inventario más detallado y a continuación, se estudia cada uno de los activos en términos de las amenazas, impactos y vulnerabilidades. De esta manera un centro puede dar prioridad a los activos o servicios que debe abordarse en primer lugar.

76. Una vez que se ha llevado a cabo un estudio del riesgo de la empresa, debería seguirse un proceso similar de comprensión de sistemas, amenazas, impactos y vulnerabilidades a nivel de centro, sistema y activo para entender el riesgo de negocio existente en ese nivel.

## 4. REALIZAR ESTUDIOS CONTINUOS DEL RIESGO DEL NEGOCIO

### 4.1. CONTEXTO DE ESTA SECCIÓN DENTRO DEL MARCO GENERAL

77. Esta sección trata sobre convertir el estudio del riesgo del negocio en un “todo sigue igual”<sup>12</sup> o una garantía continua de que todo sigue igual. El proceso está vinculado a la dirección para asegurar que los sistemas cumplen los estándares en vigor, y garantizar que no se han introducido cambios no autorizados en los sistemas.

### 4.2. JUSTIFICACIÓN

78. Asegurar que la seguridad adecuada de los sistemas sea compatible con la tolerancia acordada al riesgo del negocio.

### 4.3. PRINCIPIOS DE BUENAS PRÁCTICAS

79. El principio general de buenas prácticas extraído del documento “Guía de Buenas Prácticas: Seguridad en el Control de Procesos y SCADA” es el siguiente:

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

### 4.4. ORIENTACIÓN SOBRE LAS BUENAS PRÁCTICAS

80. Un estudio del riesgo del negocio puede ser un proceso muy largo y necesita información de un número importante de partes interesadas y recursos. Definiendo “factores desencadenantes”<sup>13</sup> que pongan en marcha el proceso de estudio se garantiza que el proceso se ejecute sólo cuando sea necesario. Tales factores desencadenantes pueden variar de una organización a otra dependiendo del tipo de proceso, el nivel de seguridad vigente, la arquitectura vigente, los recursos, etc. Ejemplos típicos de factores desencadenantes son:

- Cambios en:
  - Nivel de amenaza.
  - Tolerancia al riesgo.
- Criticidad y riesgo de sistema.

---

<sup>12</sup> N.T.: Traducción de la frase hecha inglesa *Business As Usual* o BAU

<sup>13</sup> N.T.: Traducción del inglés *triggers* o disparador

- Cumplimiento de las garantías necesarias.
  - Nuevos proyectos.
  - Cambios en un sistema.
  - Fusiones y adquisiciones.
  - Circunstancias políticas (ej., un cambio de gobierno, en particular en un país en desarrollo, puede cambiar la estabilidad de la infraestructura del país y debe ser tenido en cuenta).
  - Tiempo transcurrido.
  - Incidente/s importante/s
81. Tras un re-estudio del riesgo del negocio es necesario volver a estudiar una serie de elementos para garantizar que se encuentran todavía en línea con el riesgo del negocio general. Se incluyen:
- Programa de seguridad del control de procesos - para garantizar que la dirección general sigue estando alineada con el riesgo del negocio.
  - Gobierno - para garantizar que la estructura y la composición se adapta a las necesidades del riesgo del negocio.
  - Inventario – cualquier cambio en el inventario debe cumplir una solicitud firme de cambio y un control de cambios, y se debe comunicar a las partes interesadas.
  - Planes de respuesta - deben reflejar con exactitud los sistemas y procesos existentes.
82. Probablemente el proceso de re-estudio consumirá muchos recursos y debe ser proporcional al riesgo para los sistemas críticos. Hay una tendencia natural a establecer un estándar de rutina en el estudio de la seguridad, como una revisión anual para cada centro, sistema y activo. Sin embargo, puede que éste no sea el uso más eficiente de los recursos, ya que algunos centros pueden ser revisados demasiado frecuentemente mientras otros no lo son lo suficiente. La frecuencia de los re-estudios debe corresponder a la criticidad de los sistemas o su impacto en la empresa y la cadena de suministro. Uno de los principales resultados de cada estudio del riesgo del negocio es una indicación de la frecuencia con la que el re-estudio del riesgo debe llevarse a cabo.

## 5. AGRADECIMIENTOS

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

### Sobre los autores

Este documento<sup>14</sup> ha sido producido conjuntamente por PA Consulting Group y CPNI.

#### **Centre for the Protection of National Infrastructure**

Central Support

PO Box 60628

London

SW1P 9HA

Fax: 0207 233 8182

Email: [enquiries@cpni.gov.uk](mailto:enquiries@cpni.gov.uk)

Web: [www.cpni.gov.uk](http://www.cpni.gov.uk)

Para más información del CPNI sobre la Seguridad en el Control de Procesos y SCADA:

Internet: [www.cpni.gov.uk/ProtectingYourAssets/scada.aspx](http://www.cpni.gov.uk/ProtectingYourAssets/scada.aspx)

#### **PA Consulting Group**

123 Buckingham Palace Road

London

SW1W 9SR

Tel: +44 20 7730 9000

Fax: +44 20 7333 5050

Email: [info@paconsulting.com](mailto:info@paconsulting.com)

Web: [www.paconsulting.com](http://www.paconsulting.com)

Para más información de PA Consulting Group sobre Seguridad en el Control de Procesos y SCADA:

Email: [process\\_control\\_security@paconsulting.com](mailto:process_control_security@paconsulting.com)

Web: [www.paconsulting.com/process\\_control\\_security](http://www.paconsulting.com/process_control_security)

---

<sup>14</sup> N.T.: La versión original de este documento. La traducción ha sido realizada por CCN-CERT ([Ref.- 43]).



## ANEXO A. REFERENCIAS

### A.1. REFERENCIAS GENERALES SCADA

N.T.: Las siguientes referencias se reproducen tal cual aparecen en el documento original en el apartado "General SCADA Referentes".

- [Ref.- 1] BS 7858:2006: Security screening of individuals employed in a security environment. Code of practice  
[www.bsi-global.com/en/Standards-and-Publications/Industry-Sectors/Security/Security-Products/](http://www.bsi-global.com/en/Standards-and-Publications/Industry-Sectors/Security/Security-Products/)
- [Ref.- 2] BS-78582006/BS 8470:2006 Secure destruction of confidential material. Code of practice  
[www.bsi-global.com/en/Shop/Publication-Detail/?pid=00000000030127562](http://www.bsi-global.com/en/Shop/Publication-Detail/?pid=00000000030127562)
- [Ref.- 3] CPNI: Best Practice Guide Commercially Available Penetration Testing  
[www.cpni.gov.uk/Docs/re-20060508-00338.pdf](http://www.cpni.gov.uk/Docs/re-20060508-00338.pdf)
- [Ref.- 4] CPNI: Best Practice Guide on Firewall Deployment for SCADA and Process Control Networks  
[www.cpni.gov.uk/Docs/re-20050223-00157.pdf](http://www.cpni.gov.uk/Docs/re-20050223-00157.pdf)
- [Ref.- 5] CPNI First Responders' Guide: Policy and Principles  
[www.cpni.gov.uk/docs/re-20051004-00868.pdf](http://www.cpni.gov.uk/docs/re-20051004-00868.pdf)
- [Ref.- 6] CPNI SCADA Good Practice Guides  
[www.cpni.gov.uk/ProtectingYourAssets/scada.aspx](http://www.cpni.gov.uk/ProtectingYourAssets/scada.aspx)
- [Ref.- 7] CPNI Information Sharing  
[www.cpni.gov.uk/ProtectingYourAssets/InformationSharing.aspx](http://www.cpni.gov.uk/ProtectingYourAssets/InformationSharing.aspx)
- [Ref.- 8] CPNI Personnel Security measures  
[www.cpni.gov.uk/ProtectingYourAssets/personnelSecurity.aspx](http://www.cpni.gov.uk/ProtectingYourAssets/personnelSecurity.aspx)
- [Ref.- 9] CPNI: Good Practice Guide Patch Management  
[www.cpni.gov.uk/Docs/re-20061024-00719.pdf](http://www.cpni.gov.uk/Docs/re-20061024-00719.pdf)
- [Ref.- 10] CPNI: Good Practice Guide Outsourcing: Security Governance Framework for IT Managed Service Provision  
[www.cpni.gov.uk/Docs/re-20060802-00524.pdf](http://www.cpni.gov.uk/Docs/re-20060802-00524.pdf)
- [Ref.- 11] CPNI: Good Practice Guide on Pre-Employment Screening  
[www.cpni.gov.uk/Products/bestpractice/3351.aspx](http://www.cpni.gov.uk/Products/bestpractice/3351.aspx)
- [Ref.- 12] CPNI: An Introduction to Forensic Readiness Planning  
[www.cpni.gov.uk/docs/re-20050621-00503.pdf](http://www.cpni.gov.uk/docs/re-20050621-00503.pdf)
- [Ref.- 13] CPNI: Personnel Security Measures  
[www.cpni.gov.uk/ProtectingYourAssets/personnelSecurity.aspx](http://www.cpni.gov.uk/ProtectingYourAssets/personnelSecurity.aspx)
- [Ref.- 14] DHS Control Systems Security Program  
<http://csrp.inl.gov/>
- [Ref.- 15] DHS Control Systems Security Program Recommended Practice  
[http://csrp.inl.gov/Recommended\\_Practices.html](http://csrp.inl.gov/Recommended_Practices.html)

- [Ref.- 16] Guide to Industrial Control Systems (ICS)  
<http://csrc.nist.gov/publications/PubsDrafts.html>
- [Ref.- 17] Securing WLANs using 802,11i  
<http://csrp.inl.gov/Documents/Wireless%20802.11i%20Rec%20Practice.pdf>
- [Ref.- 18] Using Operational Security (OPSEC) to support a Cyber Security Culture in Control Systems Environments  
<http://csrp.inl.gov/Documents/OpSec%20Rec%20Practice.pdf>
- [Ref.- 19] ISA SP99 –DHS Catalog of Control System Security Requirements  
[www.dhs.gov](http://www.dhs.gov)
- [Ref.- 20] Manufacturing and Control Systems Security  
[www.isa.org/MSTemplate.cfm?MicrositeID=988&CommitteeID=6821](http://www.isa.org/MSTemplate.cfm?MicrositeID=988&CommitteeID=6821)
- [Ref.- 21] ISO 17799 International Code of Practice for Information Security Management  
[www.iso.org/iso/iso\\_catalogue/catalogue\\_tc/catalogue\\_detail.htm?csnumber=39612](http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=39612)
- [Ref.- 22] ISO 27001 International Specification for Information Security Management  
[www.iso.org/iso/iso\\_catalogue/catalogue\\_tc/catalogue\\_detail.htm?csnumber=42103](http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42103)
- [Ref.- 23] Cyber Security Procurement Language for Control Systems  
[www.msisac.org/scada/documents/12July07\\_SCADA\\_procurement.pdf](http://www.msisac.org/scada/documents/12July07_SCADA_procurement.pdf)
- [Ref.- 24] MU Security Industrial Control (MUSIC) Certification  
[www.musecurity.com/support/music.html](http://www.musecurity.com/support/music.html)
- [Ref.- 25] Control System Cyber Security Self-Assessment Tool (CS2SAT)  
[www.us-cert.gov/control\\_systems/pdf/CS2SAT.pdf](http://www.us-cert.gov/control_systems/pdf/CS2SAT.pdf)
- [Ref.- 26] Department of Homeland Security Control Systems Security Training  
[www.us-cert.gov/control\\_systems/cstraining.html#cyber](http://www.us-cert.gov/control_systems/cstraining.html#cyber)
- [Ref.- 27] Recommended Practices Guide for Securing ZigBee Wireless Networks in Process Control System Environments  
[www.us-cert.gov/control\\_systems/pdf/Zigbee%20Rec%20Pract%20-%20draft-posted%207-10-07.pdf](http://www.us-cert.gov/control_systems/pdf/Zigbee%20Rec%20Pract%20-%20draft-posted%207-10-07.pdf)
- [Ref.- 28] Achilles Certification Program  
[www.wurldtech.com/index.php](http://www.wurldtech.com/index.php)
- [Ref.- 29] American Gas Association (AGA)  
[www.aga.org](http://www.aga.org)
- [Ref.- 30] American Petroleum Institute (API)  
[www.api.org](http://www.api.org)
- [Ref.- 31] Certified Information Systems Auditor (CISA)  
[www.isaca.org/](http://www.isaca.org/)
- [Ref.- 32] Certified Information Systems Security Professional (CISSP)  
[www.isc2.org/](http://www.isc2.org/)
- [Ref.- 33] Global Information Assurance Certification (GIAC)  
[www.giac.org/](http://www.giac.org/)
- [Ref.- 34] International Council on Large Electric Systems (CIGRE)  
[www.cigre.org](http://www.cigre.org)
- [Ref.- 35] International Electrotechnical Commission (IEC)  
[www.iec.ch](http://www.iec.ch)

- [Ref.- 36] Institution of Electrical and Electronics Engineers (IEEE)  
[www.ieee.org/portal/site](http://www.ieee.org/portal/site)
- [Ref.- 37] National Institute of Standards and Technology (NIST)  
[www.nist.gov](http://www.nist.gov)
- [Ref.- 38] NERC Critical Infrastructure Protection (CIP)  
[www.nerc.com/~filez/standards/Cyber-Security-Permanent.html](http://www.nerc.com/~filez/standards/Cyber-Security-Permanent.html)
- [Ref.- 39] Norwegian Oil Industry Association (OLF)  
[www.olf.no/english](http://www.olf.no/english)
- [Ref.- 40] Process Control Security Requirements Forum  
[www.isd.mel.nist.gov/projects/processcontrol/](http://www.isd.mel.nist.gov/projects/processcontrol/)
- [Ref.- 41] US Cert  
[www.us-cert.gov/control\\_systems/](http://www.us-cert.gov/control_systems/)
- [Ref.- 42] WARPS  
[www.warp.gov.uk](http://www.warp.gov.uk)

## A.2. REFERENCIAS EN ESTA TRADUCCIÓN

- [Ref.- 43] Portal de CCN-CERT  
<https://www.ccn-cern.cni.es>
- [Ref.- 44] CNPIC  
<http://www.cnpic-es.es>
- [Ref.- 45] CCN-STIC-480A Seguridad en el control de procesos y SCADA  
Guía de buenas prácticas
- [Ref.- 46] CCN-STIC-480B Seguridad en el control de procesos y SCADA  
Guía 1: Comprender el riesgo del negocio
- [Ref.- 47] CCN-STIC-480C Seguridad en el control de procesos y SCADA  
Guía 2: Implementar una arquitectura segura
- [Ref.- 48] CCN-STIC-480D Seguridad en el control de procesos y SCADA  
Guía 3: Establecer capacidades de respuesta
- [Ref.- 49] CCN-STIC-480E Seguridad en el control de procesos y SCADA  
Guía 4: Mejorar la concienciación y las habilidades
- [Ref.- 50] CCN-STIC-480F Seguridad en el control de procesos y SCADA  
Guía 5: Gestionar el riesgo de terceros
- [Ref.- 51] CCN-STIC-480G Seguridad en el control de procesos y SCADA  
Guía 6: Afrontar proyectos
- [Ref.- 52] CCN-STIC-480H Seguridad en el control de procesos y SCADA  
Guía 7: Establecer una dirección permanente
- [Ref.- 53]

## ANEXO B. GLOSARIO DE TÉRMINOS Y ABREVIATURAS

### B.1. GLOSARIO DE TÉRMINOS

Las definiciones indicadas con un asterisco aparecían en el apartado 2 “Resumen de “Comprender el Riesgo del Negocio”” del documento original.

<b>Amenaza*</b>	Cualquier circunstancia o hecho que pueda dañar un sistema de control de procesos y SCADA a través de accesos no autorizados, destrucción, divulgación, modificación de datos y/o denegación del servicio.
<b>Riesgo*</b>	Posibilidad de que se produzca un hecho que tendrá un impacto negativo en el sistema de control. El hecho puede ser el resultado de una amenaza o una combinación de amenazas.
<b>Tolerancia al riesgo*<sup>15</sup></b>	Nivel de riesgo, utilizado para determinar lo aceptable que puede ser un riesgo.
<b>Probabilidad*<sup>16</sup></b>	Probabilidad de un determinado resultado.
<b>Impacto*</b>	Consecuencias de que una amenaza ocurra.
<b>Vulnerabilidad*</b>	Grado en que un sistema de <i>software</i> o un componente está abierto a accesos no autorizados, cambio o divulgación de su información y es susceptible a las interferencias o a la interrupción de los servicios del sistema.
<b>Activo<sup>17</sup></b>	Cualquier infraestructura, equipo, edificio, cableado, etc., que suponga parte directa o indirectamente del sistema productivo.
<b>Asunción del Riesgo</b>	La decisión de aceptar un riesgo. [ISO/IEC Guide 73:2002]

### B.2. GLOSARIO DE SIGLAS

<b>CCN</b>	Centro Criptológico Nacional
<b>CPNI</b>	Centro para la Protección de la Infraestructura Nacional de Reino Unido
<b>CSIRTUK</b>	Combined Security Incident Response Team – United Kingdom
<b>ERSCP</b>	Equipo de Respuesta de Seguridad en el Control de Procesos
<b>INC</b>	Infraestructura Nacional Crítica
<b>SCADA</b>	<i>Supervisory Control And Data Acquisition</i> Sistema de Supervisión, Control y Adquisición de Datos
<b>SCD</b>	Sistemas de Control Distribuido
<b>TI</b>	Tecnología de la Información

\* Los términos así señalados se definían en el original al final del apartado 2 “Resumen de “Comprender el Riesgo del Negocio””.

<sup>15</sup> N.T.:Original: *Risk Appetite*

<sup>16</sup> N.T.:Original: *Likelihood*

<sup>17</sup> N.T.:Original: *Asset*

RU	Responsable Único
SCD	Sistema de Control Distribuido
TIC	Tecnologías de la Información y las Comunicaciones
STIC	Seguridad de las Tecnologías de la Información y las Comunicaciones

### **B.3. TABLA DE EQUIVALENCIAS DE LA TRADUCCIÓN**

<b>Traducción al español</b>	<b>Original en inglés</b>
RU: Responsable Único	SPA: Single Point of Accountability
SCD: Sistema de Control Distribuido	DCS, <i>Distributed Control System</i>
Tabla de Riesgos del Centro	SRT: Site Risk Table
TI: Tecnologías de la Información	IT: Information Technologies
Tolerancia del Riesgo	risk appetite