



Informe de Amenazas

CCN-CERT IA-04/16

Amenazas y análisis de riesgos en
Sistemas de Control Industrial (ICS)

Enero 2016



S2 Grupo ha participado en la elaboración y modificación del presente documento y sus anexos.

LIMITACIÓN DE RESPONSABILIDAD

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

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.

ÍNDICE

1	SOBRE EL CCN-CERT	5
2	INTRODUCCIÓN	6
2.1	Antecedentes	6
2.2	Justificación de la necesidad	7
2.3	Objetivos	7
3	METODOLOGÍA	8
3.1	Punto de partida y referencias	8
3.2	Clasificación por subsectores	9
3.3	Descripción de la ficha técnica	10
3.3.1	Activos	10
3.3.2	Agentes	11
3.3.3	Escenarios de Riesgo (ER)	11
4	CATÁLOGO DE ERS EN ICS	13
4.1	ER 1: Uso inadecuado de dispositivos portátiles	13
4.2	ER 2: Trabajo de terceros	15
4.3	ER 3: Interconexiones con otras redes	18
4.4	ER 4: Gestión deficiente de copias de seguridad	20
4.5	ER 5: Falta de concienciación del personal	22
4.6	ER 6: Inadecuada gestión de cambios	24
4.7	ER 7: Inexistencia de planes adecuados de gestión de incidentes y continuidad	26
4.8	ER 8: Gestión deficiente de la información	28
4.9	ER 9: Gestión deficiente del software	30
4.10	ER 10: Asignación deficiente de responsabilidades y gestión de la seguridad	32
4.11	ER 11: Gestión deficiente de usuarios y contraseñas	34
4.12	ER 12: Falta de gestión técnica de la seguridad y sistemas	36
5	CRITERIOS PARA LA REALIZACIÓN DE ANÁLISIS DE RIESGOS	37

5.1	Aproximación al análisis de riesgos y diferencias específicas IT/OT_____	37
5.2	Criterios para la estimación de la probabilidad por subsectores_____	39
5.3	Criterios para la estimación de impacto por subsectores _____	43

1 SOBRE EL CCN-CERT

El CCN-CERT (www.ccn-cert.cni.es) es la Capacidad de Respuesta a incidentes de Seguridad de la Información del **Centro Criptológico Nacional**, CCN. Este servicio se creó en el año 2006 como **CERT Gubernamental Nacional español** y sus funciones quedan recogidas en la Ley 11/2002 reguladora del Centro Nacional de Inteligencia, el RD 421/2004 de regulación del CCN y en el RD 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad, modificado por el RD 951/2015, de 23 de octubre.

De acuerdo a todas ellas, el CCN-CERT tiene responsabilidad en ciberataques sobre **sistemas clasificados** y sobre sistemas de las **Administraciones Públicas** y de **empresas y organizaciones de interés estratégico** para el país. Su misión, por tanto, es contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas.

2 INTRODUCCIÓN

2.1 Antecedentes

En la actualidad, existen multitud de documentos publicados por diferentes organismos que abordan amenazas y riesgos en sistemas de control industrial (ICS¹, por sus siglas en inglés). A continuación se hace referencia a los que, a juicio de los autores, son los más relevantes.

El Centro Criptológico Nacional español dispone de una serie de guías (CCN-STIC-480) orientadas a "Seguridad en sistemas SCADA²" y basadas en un conjunto de documentos publicados por el Centro para la Protección de la Infraestructura Nacional de Reino Unido (CPNI³). En concreto la guía CCN-STIC-480B⁴ "Comprender el riesgo del negocio" hace mención a una serie de amenazas genéricas.

El documento *Smart Grid Threat Landscape and Good Practice Guide*⁵ fue publicado por ENISA⁶ en diciembre de 2013 y está especialmente dirigido a las *smart grid*⁷. ENISA presenta una lista muy extensa de amenazas que es de difícil aplicación práctica puesto que las describe de forma excesivamente prolija y con poca consideración con las características del ámbito industrial.

NIST 800-82 rev.2 ⁸ es una amplia guía publicada por el National Institute of Standards and Technology (NIST) dependiente del Departamento de Comercio de EEUU. Este documento profundiza más en las posibles vulnerabilidades que pueden afectar a los ICS y no tanto en las amenazas a las que pueden estar sometidos estos sistemas.

Por su parte, la Oficina Federal para la Seguridad de la Información alemana (BSI⁹ por su siglas en alemán) publicó en 2014 una nueva versión de su documento *Industrial Control System Security – Top Threats and Countermeasures*¹⁰ en el que se presentan una serie de amenazas donde se incluyen posibles escenarios y medidas para la protección.

¹ Industrial Control System (ICS)

² Supervisory Control and Data Acquisition (SCADA)

³ Centre for the Protection of National Infrastructure (CPNI)

⁴ https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/400-Guias_Generales/480B-SCADA-Comprender_%20el_riesgo_del_negocio/480B-SCADA-Comprender_el%20riesgo_del_negocio-ene10.pdf

⁵ <https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-thematic-landscapes/sqtl/smart-grid-threat-landscape-and-good-practice-guide>

⁶ European Union Agency for Network and Information Security(ENISA)

⁷ Red eléctrica inteligente

⁸ <http://csrc.nist.gov/publications/PubsSPs.html>

⁹ Bundesamt für Sicherheit in der Informationstechnik (BSI),

¹⁰ https://www.bsi.bund.de/DE/Themen/weitereThemen/ICS-Security/Empfehlungen/Betreiber/Betreiber_node.html

La experiencia en la realización de auditorías de ciberseguridad en el ámbito industrial y la elaboración posterior de planes de iniciativas, muestra que existen una serie de situaciones frecuentes y comunes en distintos sectores de la industria. Una parte importante de las mismas son consecuencia del modo en que se trabaja en este ámbito. Además, la forma de corregir esta situación no es trivial. No basta con trasladar directamente las soluciones del mundo de las Tecnologías de la Información (TI) a esta área.

Existen muchos catálogos de amenazas dirigidas al ámbito TI puesto que, históricamente, han sido el objetivo principal de los ciberataques. El estado en que se encuentra el ámbito industrial en esta cuestión es considerablemente distinto. En la actualidad, para la mayoría de los casos, un pequeño número de amenazas supone un porcentaje muy elevado del riesgo al que se exponen los ICS. Por ello, centrarse en la resolución de las mismas puede generar una mejora significativa en el estado de ciberseguridad del sistema de control.

2.2 Justificación de la necesidad

Aunque algunos de los documentos nombrados en el apartado anterior cuentan con un elevado nivel de detalle y pueden llegar a ser muy útiles, detectamos la ausencia, por un lado, de un documento que haga especial hincapié en las amenazas a las que están sometidos los ICS. Por otro lado, de un documento más práctico y que tenga en cuenta específicamente el modo en el que se operan este tipo de sistemas.

Uno de los planteamientos principales del presente documento parte de la certeza de que uno de los mayores problemas, al menos tan importante como las propias amenazas tecnológicas, es la barrera cultural que existe entre el mundo de la ciberseguridad y el industrial de control de procesos. Se parte de la idea de que la ciberseguridad de los sistemas de control industrial se encuentra en un terreno a caballo entre dos culturas profesionales y que lo más frecuente es que no los diseñen, construyan ni exploten expertos en seguridad.

Hasta la fecha existen pocos documentos que, con un enfoque eminentemente práctico, sirvan de ayuda a los profesionales del sector para conocer cuál es el estado de ciberseguridad de sus ICS y afrontar de modo inicial un análisis de riesgos en los mismos.

2.3 Objetivos

El objetivo principal de este documento es ofrecer de manera muy práctica herramientas que ayuden llevar a cabo una aproximación inicial a la situación en la que se encuentran los sistemas de control industrial de su organización en materia de ciberseguridad.

Así pues, nos dirigimos principalmente a dos perfiles distintos. En primer lugar, a personas no necesariamente acostumbradas a trabajar con ICS pero entre cuyas responsabilidades está la seguridad de estos sistemas. En segundo lugar, el perfil inverso: personal del ámbito industrial acostumbrado a trabajar con ICS pero que no dispone de conocimientos profundos de ciberseguridad.

Para facilitar la aplicación del presente documento, se incluye en el apartado 5 una aproximación a los análisis de riesgos así como una serie de criterios para la evaluación de la probabilidad y el impacto ante la materialización de amenazas en ICS. Adicionalmente se ha incluido también en ese último bloque una particularización para la clasificación por subsectores del apartado 3.2.

Como se ha comentado en el punto 2.1, en este documento se presenta una selección de amenazas que, según el criterio y experiencia de los autores, son más frecuentes y características en el ámbito industrial y que por tanto deben constituir el principal objeto de atención a la hora de abordar un análisis de los riesgos de un sistema de control industrial.

Nótese que existe una gran diversidad de sistemas en el sector industrial. Por ello, la selección presentada no excluye la existencia de otras amenazas que, en casos particulares, puedan representar riesgos significativos.

3 METODOLOGÍA

3.1 Punto de partida y referencias

Es importante recalcar que los conceptos sistema de control industrial (ICS) e infraestructura crítica (IC) no son intercambiables.

En España es la Ley 8/2011, de 28 de abril, de Protección de Infraestructuras Críticas la que establece la definición, a efectos legales, de infraestructura crítica: aquella infraestructura estratégica cuyo funcionamiento es indispensable y no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales prestados a la sociedad.

El concepto de ICS es mucho más genérico. Un sistema de control industrial es un conjunto de equipos dispuestos en diferentes niveles (nivel de campo, nivel de control, nivel de supervisión), que están conectados en una misma red y que permiten, mediante acciones en tiempo real, gestionar procesos físicos. Entre estos equipos existe una serie de elementos que disponen de una lógica de control programada y que son los responsables de que este tipo de sistemas sean, en buena parte, automáticos. Un ICS puede ser responsable de un proceso muy complejo, pero que no sea necesariamente crítico para la sociedad aunque sí lo sea para la organización propietaria del mismo.

Así pues, existen infraestructuras críticas que no cuentan en su operación con sistemas de control industrial y sistemas de control industrial que, por el proceso que llevan a cabo, no son infraestructuras críticas.

Téngase en cuenta que, para llevar a cabo este análisis, se han definido una serie de ER,s a las que una red de control industrial se puede ver expuesta con una cierta probabilidad. Con el fin de hacer más operativo y comprensible el análisis, se ha incluido en cada una de ellas ejemplos prácticos que describen el modo en que se trabaja en este tipo de entornos. Como resulta lógico, se han descartado escenarios que, a juicio de los autores, no tienen relevancia en el entorno de trabajo de este tipo de sistemas.

Además, se ha llevado a cabo en primer lugar una clasificación de los ICS partiendo de los diferentes subsectores estratégicos de la industria que están incluidos en la Ley de Protección de Infraestructuras Críticas española, modificándola y completándola para abarcar todos los sistemas posibles. Finalmente se ha definido un conjunto de activos y agentes asociados a este tipo de sistemas.

Cabe destacar que este documento debe servir para abordar de manera simple los primeros pasos de un proyecto de mejora del estado de la ciberseguridad en una red de

control industrial. En este tipo de proyectos no sólo se lleva a cabo una valoración del estado en el que se encuentra el ICS en cuestión, sino que también se realiza un estudio de la estimación del riesgo específico asociado para cada una de los ERs así como un plan de iniciativas en el que se detallan las acciones que la organización debe seguir y su prioridad para avanzar hacia los objetivos que se han marcado.

En el apartado 5 se incluye información que, desde esta perspectiva, puede ser útil para ayudar a estimar la probabilidad y el impacto que podría generar la materialización de estos ERs en diferentes subsectores a personas no necesariamente familiarizadas, bien con el ámbito industrial, bien con la ciberseguridad.

3.2 Clasificación por subsectores

Existen multitud de sectores de naturaleza muy distinta en los que se hace uso de sistemas de control industrial. Por ello, el modo en que les afectan cierto tipo de amenazas puede variar de manera significativa.

Por su interés, se ha utilizado el listado de sectores estratégicos anexo en la Ley 8/2011 del 28 de abril por la que se establecen medidas para la protección de infraestructuras críticas (BOE-A-2011-7630). Adicionalmente se han incluido también el sector de manufactura y el sector de servicios por estar sus sistemas afectados por las amenazas que se describen en el presente documento y se ha excluido del listado el sector espacial por entender que éste está representado tanto en los sectores de manufactura como en el de tecnologías de la información y las comunicaciones.

Para poder hacer una explicación más precisa del modo en que estos ERs afectan a cada sector se ha realizado una clasificación en cuatro grupos distintos atendiendo a la naturaleza de los mismos. Téngase en cuenta que una clasificación de estas características presenta diversas dificultades puesto que los diferentes sectores podrían figurar en más de uno de los grupos. Con esta consideración presente, por simplicidad, cada sector se ha incluido únicamente en un grupo.

Forman parte del grupo 1 aquellos sectores en los que los sistemas de control industrial no son parte de su proceso principal de negocio pero en los que se dispone de este tipo de sistemas en elementos auxiliares que sirven de sostén en procesos esenciales para la organización. Por ejemplo, el sistema de control de climatización de un Centro de Procesamiento de Datos de una entidad financiera. Los sectores incluidos en este grupo son el sistema financiero y tributario, las instalaciones de investigación, la administración pública y las organizaciones del sector de la tecnología de la información y las comunicaciones.

En el grupo 2 se encuentran aquellos sectores en los que los sistemas de control industrial forman parte de su proceso principal de negocio y que, por la naturaleza del mismo, se encuentran físicamente distribuidos por un área geográfica extensa y, en algunos casos, cuentan con instalaciones sin personal permanente. Pueden servir de ejemplo el sistema de control de bombeo de una red de saneamiento o de una red de abastecimiento de agua potable. En este grupo están los sectores de transporte, agua y energía.

Los sectores que forman parte del grupo 3 son aquellos en los que los ICS se encuentran localizados en espacios físicos acotados y en los que las consecuencias de un incidente en sus sistemas estarían limitadas a sus instalaciones. Por ejemplo, un hospital. Entrarían dentro de este grupo los sectores de la alimentación, manufactura, salud y servicios.

Por último, se han incluido en el grupo 4 los sectores en los que, aunque sus sistemas de control industrial se encuentran localizados también en áreas geográficas limitadas, las consecuencias de incidentes en sus ICS pueden afectar a la vida o a la salud de la población o al medio ambiente. Están incluidos en este grupo el sector químico y el sector nuclear.

En la siguiente tabla se incluye un resumen de los grupos y sectores asociados.

GRUPO	SECTOR
Grupo 1	Sistema financiero y tributario
	Instalaciones de investigación
	Administración
	Tecnologías de la Información y las Comunicaciones
Grupo 2	Transporte
	Agua
	Energía
Grupo 3	Alimentación
	Manufactura
	Salud
	Servicios
Grupo 4	Industria química
	Industria nuclear

3.3 Descripción de la ficha técnica

Para cada ER se ha elaborado una ficha técnica. A continuación se detalla la estructura y contenido de estas fichas.

3.3.1 Activos

Los activos susceptibles de sufrir la materialización de las amenazas pueden ser tanto propios de la organización como externos. Además, y esto es algo que diferencia los ICS de los sistemas TI, el impacto también puede afectar a amplios grupos de población cuando, por ejemplo, las amenazas se materializan en infraestructuras críticas (tal y como se definen en la Ley). En particular se han considerado como activos:

- Archivos de proyecto
- Lógica en ejecución en controladores y/o PC SCADA
- Equipos, máquinas y/o instalaciones
- Materia prima, material en proceso y/o producto terminado
- Información del proceso y/o de la organización
- Red y elementos de la arquitectura de comunicación
- Medio Ambiente
- Personal propio y/o de terceros
- Terceras personas

3.3.2 Agentes

A su vez, pueden existir diversos agentes que provoquen que los ERs se materialicen. Nótese que, atendiendo a las motivaciones de los mismos, podría llevarse a cabo una clasificación más detallada. Sin embargo, se ha considerado una lista simplificada que, según el criterio de los autores, es suficientemente precisa para este caso. Teniendo esto presente, los agentes considerados son los siguientes:

- Ciberdelincuentes.
- Personal propio y de terceras partes. El daño se puede causar de forma voluntaria o involuntaria.
- Estados.
- Terroristas.

3.3.3 Escenarios de Riesgo (ER)

Los escenarios de riesgos (ER) listados en el presente documento son aquellas que se han considerado más frecuentes y características dentro del ámbito industrial. En cualquier caso, dada la extensa variedad de sistemas en este sector, la selección realizada no excluye la existencia de otras amenazas que, en sistemas concretos, pueden constituir riesgos relevantes.

- Uso inadecuado de dispositivos portátiles
- Trabajo de terceros
- Interconexiones con otras redes
- Gestión deficiente de copias de seguridad
- Falta de concienciación del personal
- Inadecuada gestión de cambios
- Inexistencia de planes adecuados de gestión de incidentes y continuidad
- Gestión deficiente de la información
- Gestión deficiente del software
- Asignación deficiente de responsabilidades y gestión de la seguridad
- Gestión deficiente de usuarios y contraseñas
- Falta de gestión técnica de la seguridad y sistemas

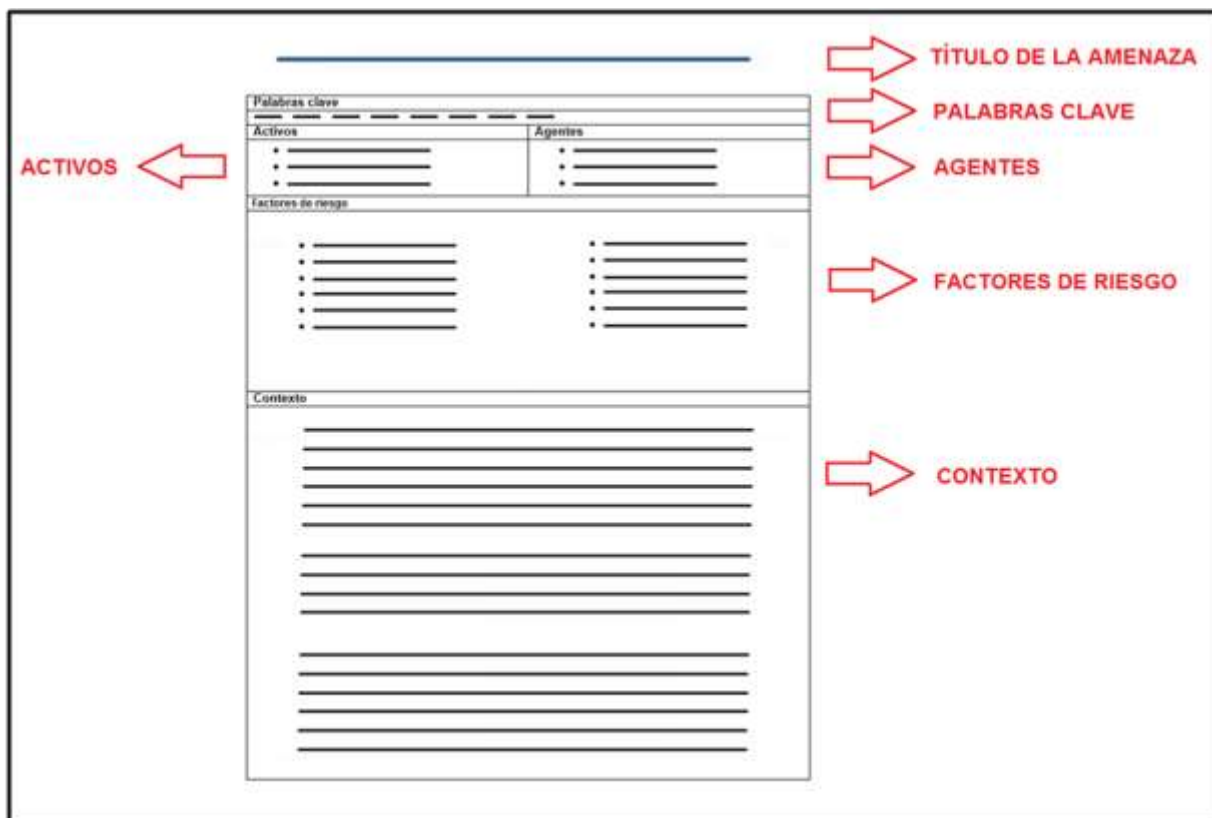
Para cada una de los ER se presenta una ficha técnica con diferentes apartados.

En primer lugar se enumeran una serie de palabras clave relacionadas con el ER que pueden servir para encontrar rápidamente cuestiones que se abordan en el apartado de contexto.

En los dos apartados siguientes se enumeran los activos que se pueden ver afectados si el ER se materializa y los agentes responsables de llevarla a cabo.

En el apartado "factores de riesgo" se enumera de manera resumida una serie de factores que pueden introducir riesgos en los ICS y que se abordan de manera más detallada en el punto de "contexto".

En el apartado "contexto" se describe con detalle el ER y se proporciona al lector información específica del entorno industrial que caracteriza de manera concreta el modo en que ese ER se puede hacer presente en un ICS.



The diagram shows a form template for threat analysis. It includes sections for 'Palabras clave', 'Activos', 'Agentes', 'Factores de riesgo', and 'Contexto'. Red arrows point from labels to these sections: 'ACTIVOS' points to the 'Activos' section, 'TÍTULO DE LA AMENAZA' points to the top of the form, 'PALABRAS CLAVE' points to the 'Palabras clave' section, 'AGENTES' points to the 'Agentes' section, 'FACTORES DE RIESGO' points to the 'Factores de riesgo' section, and 'CONTEXTO' points to the 'Contexto' section.

Palabras clave	
Activos	Agentes
•	•
•	•
•	•

Factores de riesgo	
•	•
•	•
•	•
•	•
•	•

Contexto

4 CATÁLOGO DE ERS EN ICS

4.1 ER 1: Uso inadecuado de dispositivos portátiles

Palabras clave	
Almacenamiento extraíble, USB ¹¹ , HDD ¹² , copias de seguridad, Back Up, aislamiento de redes	
Activos	Agentes
<ul style="list-style-type: none">• Lógica en ejecución en controladores y/o PC¹³ SCADA• Equipos, máquinas y/o instalaciones• Información del proceso y/o de la organización	<ul style="list-style-type: none">• Ciberdelincuentes• Personal propio y de terceras partes• Estados• Terroristas
Factores de riesgo	
<ul style="list-style-type: none">• Copias de seguridad de información de la lógica en ejecución en discos duros externos.• Extracción de información de la red de control con dispositivos USB para la realización de informes.• Uso de dispositivos USB para el intercambio de información relevante para el proceso productivo (precios de producto, información de proveedores, diagramas de proceso, planos, arquitectura de la red de control, marcas y modelos de equipos en producción, etc.)• PC portátiles con aplicaciones específicas empleadas en el mantenimiento de equipos de los ICS.• Existencia de hardware específico de configuración o mantenimiento.	
Contexto	

¹¹ Memoria USB (Universal Serial Bus USB)

¹² Unidad de disco rígido (Hard Disk Drive HDD)

¹³ Ordenadores personales (Personal Computer PC)

El uso de dispositivos extraíbles es común en todo tipo de entornos, también el industrial. Es frecuente que las redes de control no se encuentren conectadas a otras redes, tampoco a la red corporativa de la organización. Por esta razón, el uso de este tipo de elementos es todavía más necesario cuando se requiere trabajar con información que se encuentra en la red de control.

Esta situación se da, por ejemplo, cuando el departamento de producción de una planta ha de extraer información real del proceso para analizar datos. Puesto que no existe acceso desde los PC corporativos de los empleados, se hace imprescindible trasladar información directamente en un dispositivo extraíble. En principio, esta situación no debería tener mayor repercusión en la seguridad del sistema. Sin embargo, como no suelen existir procedimientos para el uso, análisis previo y posterior de estos dispositivos, se introducen una serie de riesgos. Por ejemplo, es frecuente que estos dispositivos de almacenamiento se usen en equipos que luego pueden llevarse o conectarse a otras redes. Es el caso de PC portátiles corporativos que los empleados se llevan a casa y conectan a redes personales o utilizan en viajes y conectan a WiFi públicas o de otras organizaciones. Adicionalmente, estas situaciones facilitan que se ejecute el robo de información con el hurto de dispositivos o el acceso a los mismos a través de redes comprometidas.

Este ER es una de las que rompe el falso mito del aislamiento completo de las redes de control industrial, pues a través de este tipo de dispositivos existe la opción de que se produzcan conexiones asíncronas a la red del ICS. Es decir, que cierto tipo de datos viaje de la red de control hacia fuera y viceversa (información confidencial o código dañino (malware), por ejemplo) de manera secuencial.

Así mismo, es común que en el entorno industrial se haga uso de este tipo de dispositivos para llevar a cabo copias de seguridad de la lógica en ejecución de equipos del sistema de control, a menudo distribuidos por la planta. Es frecuente que un disco duro externo sea el único soporte en el que se almacenan todas las copias de seguridad de los programas en ejecución del nivel de control. Además del peligro de las conexiones asíncronas comentadas anteriormente, se introduce el riesgo de la pérdida de información crítica para la continuidad de la operación si el dispositivo en cuestión deja de funcionar correctamente o, sencillamente, se extravía.

4.2 ER 2: Trabajo de terceros

Palabras clave	
Terceros, terceras empresas, subcontratación, mantenimiento remoto, conexiones asíncronas	
Activos	Agentes
<ul style="list-style-type: none">• Archivos de proyecto/programas• Lógica en ejecución en controladores y/o PC SCADA• Equipos, máquinas y/o instalaciones• Información del proceso y/o de la organización	<ul style="list-style-type: none">• Ciberdelincuentes• Personal propio y de terceras partes• Estados• Terroristas
Factores de riesgo	
<ul style="list-style-type: none">• Existencia de conexiones con un módem de radio o celular (tecnologías 2G/ 3G /4G/ CDMA¹⁴ o GSM¹⁵) en subsistemas de la red de control con o sin conocimiento por parte de la organización.• Conexión con equipos PC portátiles no revisados al sistema de control.• Archivos de proyectos o copias de seguridad únicamente en manos de proveedores.• Existencia de conexiones para mantenimiento remoto de las que no se guarda ningún tipo de registro en el sistema o sobre el que no hay un control de acceso adecuado• Personal de mantenimiento de terceras empresas al que no se le aplican políticas de seguridad para terceros.• Equipos conectados a subsistemas del ICS sobre los que la organización no tiene ningún tipo de control o sobre los que no se accede porque son utilizados para el mantenimiento remoto por parte de proveedores.	

¹⁴ Multiplexación por división de código (Code Division Multiple Access CDMA)

¹⁵ Sistema global de comunicaciones móviles (Global System for Mobile communications GSM)

Contexto

El grado de especialización en el sector industrial suele ser muy alto. Por ello, es frecuente que la organización cuente de manera continua con terceras empresas para llevar a cabo tareas que, sin ser parte del proceso industrial principal, son imprescindibles para el correcto funcionamiento del mismo.

Es frecuente que terceras empresas dispongan de retenes permanentes en plantas industriales de la organización o acudan con mucha regularidad a las mismas. De este modo, es común que se olvide o se ignore que estos trabajadores son, en realidad, externos, y no se aplique sobre ellos las políticas indicadas para terceros.

Por otro lado, no es extraño que exista cierta información de operación del proceso (lógicas en ejecución o pantallas del SCADA, por ejemplo) de la que la propia organización no tiene respaldo. Se confía en que es la empresa tercera que se encargó de proveer dicha parte del sistema, la que cuenta con una copia de todo; con el riesgo asociado que esto conlleva.

Adicionalmente, el trabajo que los terceros llevan a cabo dentro de la organización introduce una serie de riesgos que deben ser considerados para evitar que se produzcan incidentes.

Es el caso de las conexiones para el mantenimiento remoto. Esta situación se tiene, por ejemplo, cuando los equipos se encuentran todavía en garantía y es el propio proveedor de los mismos el que ha de encargarse del mantenimiento en caso de que surja algún tipo de problema. Se pueden dar a través de líneas independientes que se instalan en determinadas partes del sistema de control para que dicho proveedor pueda acceder al sistema del que es especialista y pueda monitorizar los equipos y resolver incidencias sin necesidad de acudir físicamente a las instalaciones de la organización. A veces, los proveedores instalan conexiones en tecnologías 2G/ 3G /4G/ CDMA o GSM de los que la organización no tiene si quiera conocimiento.

También deben considerarse las conexiones ocasionales al sistema de control. Cuando se lleva a cabo mantenimiento presencial, es común que los técnicos encargados de llevarlo cabo conecten sus PC directamente por serie o ethernet¹⁶ a equipos de la red de control para poder configurarlos, cargar programas, etc. Se abre la vía a conexiones asíncronas a la red de control por parte de un atacante. Los equipos de los terceros no suelen revisarse antes de conectarse a la red de control por lo que se desconoce si dichos equipos llevan algún tipo de código dañino que puede ser introducido en el sistema de manera involuntaria durante esos trabajos.

El trabajo de terceros introduce también el riesgo de incumplimiento de políticas de

¹⁶ También conocido como estándar IEE 802.3 es un estándar de transmisión de datos para redes de área local

seguridad de la información: intercambio de ficheros de modo no adecuado, acceso a información crítica, etc. A menudo, las empresas terceras trabajan con información relevante del proceso de negocio como pueden ser arquitecturas de red, planos de la planta, lógica en ejecución, esquemas del proceso industrial, etc. Debe hacerse un control exhaustivo del modo en que los terceros trabajan con dicha información y la intercambian a su vez con otras personas. En este caso hablamos no sólo de empresas responsables de tareas de mantenimiento sino también todo el conjunto de proveedores que intervienen, por ejemplo, cuando se llevan a cabo cambios que requiere la ejecución de obras o nuevas instalaciones eléctricas, de climatización, etc.

4.3 ER 3: Interconexiones con otras redes

Palabras clave	
Interconexiones, red de control, red corporativa, internet, centros de control, aislamiento de redes	
Activos	Agentes
<ul style="list-style-type: none"> • Lógica en ejecución en controladores y/o PC SCADA • Equipos, máquinas y/o instalaciones • Información del proceso y/o de la organización • Procesos industriales 	<ul style="list-style-type: none"> • Ciberdelincuentes • Personal propio y de terceras partes • Estados • Terroristas
Factores de riesgo	
<ul style="list-style-type: none"> • Segmentación inadecuada de la red corporativa con la red ICS. • Control de acceso no adecuado en la gestión remota de dispositivos. • Segmentación inadecuada en el acceso de terceros para el mantenimiento de sistemas. • Línea independiente en subsistema del proceso sin monitorización por parte de la organización. • Actualizaciones en la arquitectura de la red de control que no están bien documentadas y que han introducido interconexiones sin ser éstas advertidas. • Segmentación inadecuada entre los niveles de control y supervisión en la red de control. • Integración de procesos con socios (partners). • Uso de redes públicas de comunicación. • Organizaciones con centros de control centralizados y sistemas con amplia distribución geográfica. 	
Contexto	

Probablemente, la creencia del aislamiento de las redes de control industrial es uno de los motivos que proporciona con más frecuencia la falsa sensación de protección que se tiene en este sector.

Es relativamente frecuente encontrar segmentaciones incorrectas entre los niveles de control y supervisión o conexiones que se han introducido al realizar cambios en la arquitectura que no han sido revisados convenientemente. Puede ser el caso, por ejemplo, de una sala de control centralizada desde la que se visualiza el estado de varias plantas simultáneamente. Si el tráfico de datos no viaja convenientemente cifrado o no están bien limitadas las acciones permitidas, se introducen riesgos que la organización no puede asumir. Existen organizaciones sin redes propias o que tienen interconexiones con socios con los que se integra un proceso industrial (p.ej, gestión "Just In Time").

En un ICS no es extraño encontrarse con distintas interconexiones con otras redes, a menudo, desconocidas para los propios operadores del sistema.

Es el caso de las conexiones remotas que los terceros establecen para el mantenimiento de ciertos equipos que se encuentran en la red de control. Estas conexiones remotas no siempre se establecen a través de líneas propias de la organización si no que a menudo se habilita líneas independientes que carecen de todo tipo de control por parte de los responsables del proceso. A veces se tiene un conocimiento más claro de estas conexiones porque es necesario instalar una línea física independiente. En otros casos, el proveedor habilita un acceso remoto a través de, por ejemplo, un dispositivo 3G.

Rara vez se es consciente de los riesgos que introducen estos elementos. Por un lado no se controla el tráfico de dichas conexiones ni se revisa cuándo se llevan a cabo ni por parte de quién. No se conocen los controles de autenticación que se realizan para poder conectarse a esa parte de la red de control. No es común que existan elementos como firewalls que sean capaces de registrar información del modo adecuado de las conexiones que se establecen.

4.4 ER 4: Gestión deficiente de copias de seguridad

Palabras clave	
BackUp, copia de seguridad, restauración de copias, revisión de copias	
Activos	Agentes
<ul style="list-style-type: none">Archivos de proyectoPersonasMedio ambienteProcesos industrialesLógica en ejecución en controladores y/o PC SCADAInformación del proceso y/o de la organización	<ul style="list-style-type: none">Personal propio y de terceras partes
Factores de riesgo	
<ul style="list-style-type: none">No verificación de las copias de seguridad del ICS.Copias no actualizadas de la lógica en ejecución en el ICSInexistencia de copias de seguridad. Dependencia de los archivos que se encuentran en manos proveedor.No ejecución de copias de seguridad previas a actualizaciones de cualquier tipo.Diversidad de repositorios para copias de seguridad, etiquetado inadecuado de las mismas u otras situaciones que crean confusión en caso de tener que reestablecer una copia.Imposibilidad de acceso a la lógica de control en PLC¹⁷ para llevar a cabo copias de seguridad porque el proveedor ha protegido el programa con una contraseña que la organización desconoce.Periodos de garantías en los que la organización depende de un proveedor para resolver incidentes en ciertos equipos del ICS.	
Contexto	

¹⁷ Conmutador lógico programable (Programmable Logic Controller PLC)

Debe tenerse en cuenta que la información que contienen las copias de seguridad es crítica para cualquier organización. No sólo porque su pérdida puede generar problemas en el proceso de producción si no porque, cuando hablamos de la lógica de procesos industriales, es en muchos casos en esa lógica donde se encuentra el modo de subsistencia de la organización y una parte muy importante de su conocimiento y modo de proceder que puede estar bajo propiedad industrial o puede ser usada para preparar un ataque.

En el ámbito industrial no sólo se ven afectados por este ER los equipos PC que se encuentran dentro del ICS (en la sala de control, por ejemplo), sino también equipos propios del proceso que contienen algún tipo información almacenada o lógica programada. Es el caso, por ejemplo de PLC y otro tipo de controladores lógicos o configuraciones de equipos de medición o calibración. Y a menudo llevar a cabo estas copias de seguridad no es sencillo.

Puesto que es frecuente que partes del ICS se subcontraten a terceros que a su vez se encargan del mantenimiento, es común que en la propia planta no se disponga de los recursos o los conocimientos necesarios para restaurar el sistema o algunos de sus componentes sin que necesariamente intervenga un tercero. En muchos casos, frente a esta dificultad, las copias acaban por no hacerse o se confía en que el proveedor disponga de las mismas y sea capaz de restaurarlas.

El supuesto ideal es que exista una configuración automática de copias de seguridad. Sin embargo, esto no siempre es posible en las redes de control pues algunos elementos que contienen información relevante o lógicas programadas están distribuidos por la planta o no se encuentran siempre conectados por lo que no se dispone de esa posibilidad. De este modo es necesario que las copias se hagan de modo manual conectándose físicamente a los equipos.

En los casos en los que es posible llevar a cabo las copias de modo automático, por supuesto, no se trata únicamente de tenerlas sino de ser capaces de restaurarlas en caso de ser necesario. Rara vez se comprueba que en caso de tener que restaurarse no se producirán pérdidas de información. No suele verificarse que las copias se están llevando a cabo correctamente ni que éstas se pueden restaurar sin problemas. En caso de que éstas sean manuales, no es común que los responsables de llevarlas a cabo sean estrictos en su almacenamiento y etiquetado, lo que puede generar problemas a la hora de saber cuál es la copia que debe utilizarse en caso de ser necesario.

Es frecuente que, sobre todo para las copias que se llevan a cabo de manera manual, se usen como único soporte dispositivos extraíbles para su almacenamiento. De este modo se introducen a su vez los riesgos asociados a estos dispositivos. No sólo por la posibilidad de perder la información sino porque no es común que se establezca en estos equipos ningún tipo de controles de acceso con contraseña a dichas copias. Tanto para hacerlas o borrarlas como para su restauración. Existe el riesgo, por ejemplo, de que con fines maliciosos, un atacante restaure copias modificadas.

4.5 ER 5: Falta de concienciación del personal

Palabras clave	
Concienciación, phishing ¹⁸ , pharming ¹⁹ , ingeniería social, percepción del riesgo	
Activos	Agentes
<ul style="list-style-type: none">Personas	<ul style="list-style-type: none">CiberdelincuentesEstadosTerroristas
Factores de riesgo	
<ul style="list-style-type: none">Personal del ICS que, por desconocimiento del riesgo que supone, antepone un mantenimiento rápido del sistema a que las conexiones remotas para llevarlo a cabo se realicen de manera segura.Desconocimiento de que, si se accede directamente a las comunicaciones entre los dispositivos, hay acciones que se pueden llevar a cabo sobre el ICS aunque el software que se utiliza habitualmente no lo permita.Uso inadecuado de los equipos del ICS.Publicación de excesiva información sobre la organización en perfiles personales en redes sociales de los empleados.No conciencia de la existencia de información pública detallada sobre los propios sistemas (artículos técnicos, casos de éxito de proveedores, etc.)Incapacidad para reconocer un incidente y/o desconocimiento de cómo comunicarlo o actuar.	
Contexto	
<p>El personal que trabaja en el ámbito industrial tiene amplios conocimientos de los procesos que maneja, sin embargo, generalmente, no posee formación en el ámbito de la seguridad de la información.</p> <p>La evolución tecnológica ha provocado que en muchas de las tareas que estos</p>	

¹⁸ Método de ataque que busca obtener información personal del usuario por medio del engaño o la picaresca.

¹⁹ Consiste en modificar la dirección IP de la página web de una entidad legítima (por ejemplo un banco) de forma que el navegador del usuario le dirija a un página falsa para obtener así sus claves de acceso.

trabajadores llevan a cabo intervengan multitud de elementos que introducen riesgos relacionados con las tecnologías de la información y las comunicaciones: uso de correo electrónico, intercambio de ficheros a través de la nube, uso de dispositivos de almacenamiento extraíble, etc.

Además, la utilización que estos mismos empleados hacen de la tecnología en el ámbito privado puede llegar a generar, así mismo, riesgos en la organización si no se dispone de la formación adecuada. Este ER podría materializarse de diferentes formas: descarga de archivos infectados con malware, phishing, ingeniería social, etc.

Generalmente, en el ámbito industrial, se tiene una percepción limitada del peligro que suponen ciertas prácticas habituales en estos entornos: no se tiene consciencia de la debilidad de los sistemas de protección lógica que hay implementados en sus sistemas, se tiene una confianza excesiva en las protecciones físicas de los mismos y se desconoce que la convergencia de las tecnologías ha eliminado barreras de conocimiento para cierto tipo de atacantes.

Por ejemplo, los enclavamientos eléctricos o mecánicos que impedían la operación incorrecta de ciertos equipos y que obligaban a ser rearmados físicamente. Estos elementos han sido sustituidos, en muchos casos, por enclavamientos lógicos que son mucho más flexibles a la hora de realizar cambios o implementar lógicas complejas pues no exigen nuevos dispositivos físicos ni es necesario volver a cablear. La introducción de este tipo de cambios genera muchos beneficios pero introduce, a su vez, riesgos que anteriormente no habían sido contemplados.

El control sobre la lógica de programación y los enclavamientos asociados ha de ser mucho más fuerte ahora para evitar que personas no autorizadas modifiquen el funcionamiento y provoquen situaciones no deseadas. Y eso exige, necesariamente, que el personal responsable perciba que existe un riesgo real para que cumplan las políticas que la organización establezca.

4.6 ER 6: Inadecuada gestión de cambios

Palabras clave	
Cambios, actualizaciones, terceros, ingeniería	
Activos	Agentes
<ul style="list-style-type: none">• Archivos de proyecto• Información del proceso y/o de la organización	<ul style="list-style-type: none">• Ciberdelincuentes• Personal propio y de terceras partes• Estados• Terroristas
Factores de riesgo	
<ul style="list-style-type: none">• Actualizaciones de seguridad en equipos de la red de control sin verificar que no se producen incompatibilidades con el software del ICS.• Cambios en la arquitectura por la introducción de nuevos subsistemas que no se han reflejado en la documentación.• Políticas de gestión de cambios que no incluyen o excluyen explícitamente del procedimiento modificaciones o actualizaciones de software específico del ICS (lógica de control, SCADA, etc.)• No se realiza borrado seguro de los equipos del ICS (PLC, HMI²⁰, etc.) tras ser retirados.• La política de gestión de cambios no incluye la ejecución de copias de seguridad previa a la actualización de cualquier tipo de software de la red de control.	
Contexto	
<p>Es frecuente en la industria que cuando se habla de gestión de cambios se haga referencia a aquellos cambios que tienen que ver directamente con el proceso y que están relacionados generalmente con los departamentos de ingeniería, producción o mantenimiento: cambio de equipos, adición de nuevos elementos, construcción de nuevas áreas, acciones correctivas que generan modificaciones en el sistema, etc. Sin embargo, también es habitual que en esa gestión de cambios no se tengan en cuenta los elementos de software bien por omisión o, incluso a veces, por exclusión explícita en el procedimiento correspondiente. En el ámbito industrial deben tenerse en cuenta en la</p>	

²⁰ Interfaz hombre máquina (Human Machine Interface HMI)

gestión de cambios no sólo los sistemas operativos y actualizaciones de PC sino también otro tipos de software propio de los ICS como son, por ejemplo: la lógica en ejecución en el proceso (tanto la lógica del proceso principal, como la de sistemas de control de utilities), pantallas de SCADA, sistemas operativos de PLC, HMI, etc.

Aunque esencial, tampoco es común que, antes de llevar a cabo un cambio, se hagan las evaluaciones pertinentes para asegurarse de que la introducción de las modificaciones no producirá incompatibilidades con el proceso o con equipos o software auxiliar crítico para el mismo.

Es el caso, por ejemplo, de los equipos PC que se suelen usar en el departamento de mantenimiento. En este tipo de PC suele haber software específico para llevar a cabo tareas críticas del sistema de control como ejemplo la programación de PLC, o la calibración de instrumentación y equipos.

Si bien una actualización de sistema operativo puede parecer trivial, el software que se utiliza en estos ordenadores tiene un coste muy elevado y adquirir licencias nuevas suele requerir grandes inversiones. Se puede dar el caso, incluso, de que no existan versiones para un sistema operativo concreto pues, como el número de usuarios de este tipo de programas no es muy grande, el mantenimiento que hacen los desarrolladores no siempre es el adecuado.

Así mismo, debe contemplarse que en cierto tipo de cambios intervienen terceras empresas subcontratadas especialistas en llevar a cabo determinadas tareas y se generan residuos (por ejemplo equipos antiguos retirados) que contienen información del proceso y que deben ser borrados de manera segura. Entre esos equipos se incluyen PC pero también otro tipo de elementos susceptibles de contener información: dispositivos de almacenamiento extraíble, PLC, HMI, etc.

Es frecuente que, tras llevar a cabo cierto tipo de modificaciones, no se actualice la documentación asociada como planos, arquitecturas de red, diagramas de proceso, etc. Dicha actualización es esencial para poder detectar cambios no autorizados y para la planificación de futuras modificaciones en la instalación.

Nótese que la gestión de cambios debe incluir copias de seguridad que permitan revertir la modificación en caso de que surja algún tipo de incompatibilidad o problema posterior.

4.7 ER 7: Inexistencia de planes adecuados de gestión de incidentes y continuidad

Palabras clave	
Continuidad, incidentes, ciberataque, parada de emergencia, protocolo de actuación	
Activos	Agentes
<ul style="list-style-type: none"> • Equipos, máquinas y/o instalaciones • Materia prima, material en proceso y/o producto terminado • Medio Ambiente • Personal propio y/o de terceros • Terceras personas 	<ul style="list-style-type: none"> • Ciberdelincuentes • Estados • Terroristas
Factores de riesgo	
<ul style="list-style-type: none"> • Organizaciones sin gestión de la ciberseguridad o donde el alcance no incluye los ICS. • Planes de emergencias que no contemplan un incidente de ciberseguridad como causa de la situación de emergencia. 	
Contexto	
<p>Es común que en la industria se disponga de procedimientos exhaustivos que se ensayan con cierta regularidad ante la aparición de diferentes clases de incidentes que pongan en juego la continuidad del proceso. En función del grado de criticidad del sistema en cuestión se contempla desde la pérdida de suministro eléctrico hasta fallos y parada de equipos críticos o pérdida de comunicaciones con diferentes elementos del sistema de control.</p> <p>Para ello se dispone de equipos físicos y comunicaciones redundantes que aseguran la continuidad del proceso frente a diferentes tipos de incidentes.</p> <p>En todos estos procedimientos no es frecuente que se piense en el caso de un ciberataque. La naturaleza de un ciberataque en infraestructuras industriales puede, en muchos casos, generar situaciones imprevistas no contempladas dentro de los incidentes clásicos que se pueden dar en una instalación de esas características.</p> <p>Pongamos como ejemplo una organización que gestiona una gran cantidad de instalaciones distribuidas geográficamente y, en muchos casos, sin personal presente de manera continua. Imaginemos que se pone en modo de defecto un equipo en una de esas instalaciones. Seguramente esta situación estará contemplada en la gestión de incidentes de la organización y existirá un protocolo de actuación en ese caso. Lo más probable es que movilice a un retén de mantenimiento que acudirá a dicha instalación y tratará de reparar el equipo. Mientras tanto el sistema se operará en manual o se detendrá, según proceda.</p>	

La situación es considerablemente más complicada si todos los equipos de un mismo modelo de todas las instalaciones se ponen en modo de defecto simultáneamente un día a una hora determinada. Como la probabilidad de que un escenario como éste se presente de manera fortuita es extremadamente baja, la gestión de incidentes no lo contempla. Sin embargo es verosímil que un ciberataque pueda provocar una situación similar. Por ejemplo, como consecuencia de un malware introducido de manera involuntaria al conectar el PC de mantenimiento en una de las revisiones periódicas.

En una situación como esa el problema puede persistir incluso tras conmutar a equipos redundantes y donde, incluso, no exista otra opción que una parada de emergencia. En cualquier caso, es responsabilidad de la organización incluir procedimientos de gestión de incidentes que contemplen situaciones provocadas como consecuencia de un ataque de estas características y es necesario un conocimiento profundo del sistema en cuestión para llevar a cabo una evaluación adecuada.

4.8 ER 8: Gestión deficiente de la información

Palabras clave	
Intercambio de ficheros, cifrado, información, clasificación, marcado, destrucción segura	
Activos	Agentes
<ul style="list-style-type: none"> Archivos de proyecto Lógica en ejecución en controladores y/o PC SCADA Información del proceso y/o de la organización 	<ul style="list-style-type: none"> Ciberdelincuentes Personal propio y de terceras partes Estados Terroristas
Factores de riesgo	
<ul style="list-style-type: none"> En los pliegos de condiciones técnicas se proporciona excesiva información sobre el ICS (pantallas del SCADA y ubicaciones de instalaciones, etc.) La información que se comparte con los proveedores se envía en claro a través de correo electrónico o se utilizan plataformas no verificadas por la organización. Se proporciona a través de internet, para hacer publicidad de la organización, información excesiva de una planta en producción: detalles del proceso, proveedores, ubicaciones de equipos, respaldos existentes, etc. Obligación legal de publicar cierta información Los proveedores utilizan el nombre de la organización para mostrar casos de éxito (proporcionando de este modo información sobre protocolos o equipos utilizados en el proceso). Existe documentación sobre el proceso o las instalaciones distribuida por los equipos de la planta. No se clasifican ni se marcan los documentos relativos al ICS. 	
Contexto	
<p>Existen múltiples situaciones en las que una gestión no adecuada de la información puede introducir riesgos en la organización.</p> <p>A veces, no existen normas para el marcado y clasificación adecuadas de los documentos de modo que se sepa quién debe acceder a cierta información y cuál debe</p>	

ser el nivel de publicidad de la misma.

Es frecuente que no existan políticas adecuadas para el intercambio de la información entre departamentos. Es el caso, por ejemplo, de los dispositivos extraíbles que se utilizan para exportar información del ICS y que se conectan tanto a equipos de la red de control como a equipos del entorno corporativo y sobre los que no se aplica ningún procedimiento de revisión previa o posterior o de borrado seguro.

Situaciones similares se dan también cuando se intercambia información con proveedores que intervienen en algún punto del proceso con los que se comparten documentos a través del correo electrónico sin ningún tipo de cifrado o se intercambian documentos a través de sistemas en la nube que no han sido revisados por la organización. Esta situación se da, por ejemplo, cuando el departamento de ingeniería de una organización lleva a cabo tareas en las que es necesario compartir información como archivos de proyecto o planos de las instalaciones. Documentos de estas características pueden presentar una gran cantidad de detalles: ubicación de equipos, situación de los accesos a la planta, unifilares de los circuitos eléctricos, etc. Información que en manos no adecuadas podría facilitar un posible ataque. Además, es común encontrar gran cantidad de documentos de este tipo diseminados por varios equipos del ICS sin ningún tipo de control sobre los mismos.

Con frecuencia la propia organización es la que pone a disposición pública excesiva información sobre los sistemas de control. Se puede dar esta situación, por ejemplo en los pliegos de contratación del sector público. A menudo se pueden descargar de la página web de la propia organización. No es extraño encontrar pliegos de condiciones técnicas que incluyen detalladas explicaciones del proceso que lleva a cabo el sistema de control, ubicación geográfica de las instalaciones, equipos con marcas y modelos utilizados o capturas de las pantallas del sistema SCADA.

También puede ocurrir con documentos que por requerimiento legal han de ser públicos, como es, por ejemplo, una autorización ambiental integrada. Si dichos documentos proporcionan excesivos detalles sobre el proceso y el sistema de control, pueden introducir riesgos para la seguridad de la organización.

4.9 ER 9: Gestión deficiente del software

Palabras clave	
Actualizaciones, SCADA, antivirus, software, inventario	
Activos	Agentes
<ul style="list-style-type: none"> • PC, controladores y otro hardware 	<ul style="list-style-type: none"> • Ciberdelincuentes • Personal propio y de terceras partes • Estados • Terroristas
Factores de riesgo	
<ul style="list-style-type: none"> • No se actualiza el software con parches de seguridad en equipos del ICS como consecuencia, por ejemplo, de la dificultad de hacerlo en sistemas distribuidos en un territorio amplio. • No existe un inventario de programas y versiones de cada equipo. • No se verifica previamente que las actualizaciones de sistema operativo (SO) en equipos que se utilizan en la red de control (tanto en el proceso como en mantenimiento) pueden generar incompatibilidades con software crítico para el funcionamiento del proceso. • No se revisan de manera periódica los equipos en búsqueda de documentación o software no pertinente. • No se llevan a cabo copias de seguridad antes de cualquier actualización de software. 	
Contexto	
<p>En el ámbito industrial, no es práctica habitual que exista un inventario de software necesario para cada equipo dentro del ICS así como de las versiones probadas de modo que, en caso de requerirse, pueda disponerse en poco tiempo de un equipo con el software adecuado y sus versiones correspondientes.</p> <p>Es frecuente encontrar, por ejemplo, programas que se han instalado para una necesidad puntual, que no han sido verificados y que se han dejado allí indefinidamente.</p> <p>Además, el software que se instala dentro de la red donde opera el sistema de control industrial no siempre se verifica previamente. Esto es esencial para asegurarse de que, además de verificar que no se introduce ningún tipo de código dañino o malware en</p>	

ellos, no se producirán interacciones no deseadas con el proceso o con otro software necesario para la organización por ser incompatible. Eso incluye tanto todo tipo de software hecho a medida para la organización (como puede ser, por ejemplo, el SCADA), como el sistema operativo de autómatas programables o los antivirus.

Deben incluirse también en estas verificaciones todas las actualizaciones, aunque provengan del propio fabricante, así como todos aquellos equipos con los que, sin estar continuamente conectados a la red de control, se llevan a cabo operaciones puntuales en equipos de la misma o en otros elementos críticos que pueden influir en la continuidad de la operación.

Es el caso de los equipos del departamento de mantenimiento con los que se lleva a cabo la carga de programas en los PLC (esenciales para el funcionamiento de todo el sistema), equipos con los que se revisan las configuraciones de la instrumentación distribuida en campo (sin la que no es posible monitorizar partes del proceso) o equipos corporativos situados en algún sistema anexo al proceso principal. No es extraño encontrarse con multitud de archivos descargados de internet como imágenes o documentos PDF²¹ o software no verificado como programas de mensajería instantánea.

De modo adicional debe tenerse en cuenta que, habitualmente, las redes de control evitan estar conectadas a internet, por lo que los antivirus no se actualizan de manera automática. Puesto que la efectividad de un antivirus no actualizado disminuye considerablemente, esto exige por parte de la organización una tarea continua de verificación de software.

²¹ Formato de documento portátil (Portable Document Format PDF)

4.10 ER 10: Asignación deficiente de responsabilidades y gestión de la seguridad

Palabras clave	
Propiedad de activos, responsable de seguridad, transferencia de propiedad	
Activos	Agentes
<ul style="list-style-type: none"> • Lógica en ejecución en controladores y/o PC SCADA • Información del proceso y/o de la organización 	<ul style="list-style-type: none"> • Ciberdelincuentes • Personal propio y de terceras partes • Estados • Terroristas
Factores de riesgo	
<ul style="list-style-type: none"> • No existe un responsable de ciberseguridad de los ICS. • No existen propietarios de los activos del ICS. • No existen procedimientos para la transferencia de propiedad de activos • No existen procedimientos para el borrado seguro de equipos de sistema de control 	
Contexto	
<p>En el ámbito industrial, existen responsables de la seguridad física y de "safety" o de medio ambiente. Sin embargo, rara vez existe una asignación clara de responsabilidades en cuanto a seguridad de la información se refiere. Esto genera que aunque dentro de la organización haya normas al respecto, éstas no se apliquen dentro del ámbito industrial por la inexistencia de un responsable claro de las mismas.</p> <p>Por ejemplo, los equipos corporativos cuentan siempre con contraseña y ésta debe actualizarse de manera regular y cumplir con una serie de requisitos (longitud, caracteres especiales, etc.) sin embargo es muy frecuente que en equipos de la sala de control o equipos que se encuentran distribuidos en campo no sea necesario introducir ningún tipo de credencial para operar el sistema o éstos dispongan de autologin en el arranque. Esto a menudo es así por requerimientos del modo en el que se operan estos equipos, pero muchas otras veces se debe a la inexistencia de un responsable claro de aplicar políticas sobre los mismos.</p> <p>Del mismo modo, es común que los activos no tengan asignados un propietario y no exista entre los diferentes departamentos dentro del ámbito industrial una transferencia de la propiedad de los activos. Esto incluye todos los elementos del sistema de control industrial: desde equipos PC hasta PLC, conversores de comunicaciones, instrumentación, switches,</p>	

equipos propios de mantenimiento, etc.

Además, con frecuencia, no existen procedimientos claros para la gestión de la información almacenada en los mismos que contemple de manera adecuada todas las posibles situaciones en las diferentes fases dentro de la vida de los equipos: desde su adquisición, almacenamiento, puesta en marcha y retirada.

El siguiente ejemplo podría servir de referencia en una situación ideal. Si se ejecuta una modificación en una planta en la que es necesario instalar nuevos equipos, mientras el proyecto se encuentra en ejecución, es el departamento de ingeniería el encargado de asegurarse de que se cumplen todos los procedimientos asociados a dichos equipos. Cuando la ejecución de la ampliación finaliza y el nuevo sistema entra en producción la propiedad de todos los activos pasa a ser del departamento de operación y es éste el que se asegura de que se cumplen a partir de ese momento todas las políticas que correspondan. Cuando los equipos deben ser retirados al finalizar su vida útil, la propiedad se transfiere al departamento de mantenimiento que será el encargado de que, por ejemplo, se realice un borrado seguro de la información que contienen antes de ser desguazados.

4.11 ER 11: Gestión deficiente de usuarios y contraseñas

Palabras clave	
Usuario, contraseña, autologin, bloqueo	
Activos	Agentes
<ul style="list-style-type: none">• Lógica en ejecución en controladores y/o PC SCADA• Información del proceso y/o de la organización• Procesos industriales	<ul style="list-style-type: none">• Ciberdelincuentes• Personal propio y de terceras partes• Estados• Terroristas
Factores de riesgo	
<ul style="list-style-type: none">• No se renuevan las contraseñas del ICS.• Se utilizan usuarios y contraseñas comunes en todas las instalaciones que son análogas.• No existe control de acceso en los equipos que contienen lógica en ejecución del proceso• No existe control de acceso en los equipos que son responsables de la ejecución y restauración de copias de seguridad.• Los operadores usan usuarios genéricos en vez de nominales.• Existen equipos de la sala de control o distribuidos por la planta que tienen autologin.• Existen usuarios y contraseñas escritas junto a los equipos del ICS.• Existen programas específicos desarrollados por proveedores o a medida• Existen equipos o software desfasado• La organización trabaja por turnos	
Contexto	

Como consecuencia del modo en que se trabaja dentro del ámbito industrial, es frecuente que no exista una gestión adecuada de usuarios de los equipos ni de las contraseñas asociadas a los mismos.

No es extraño encontrarse con contraseñas pegadas en pantallas, poco robustas, fácilmente deducibles o que no se cambian desde el día en que los equipos se instalaron. Es habitual que existan equipos PC con usuarios genéricos compartidos en los que trabajan de manera continuada varios empleados. Es el caso, por ejemplo, de los equipos de operación de las salas de control donde, en muchos procesos, hay trabajadores a turnos las 24 horas del día y personas distintas utilizan los mismos equipos de manera continuada.

Algo similar ocurre en los casos en los que existe una estación de ingeniería en la sala de control. Generalmente, este equipo contiene información crítica de la lógica de control en ejecución o incluso dispone de la posibilidad de realizar cambios y cargarlos al sistema en producción. Por lo tanto, modificaciones en los documentos que en él se encuentran pueden generar cambios críticos en el sistema. No es extraño encontrarse equipos como éste desbloqueados o con usuarios que no son personales. A veces, el software utilizado para la programación de la lógica permite incluir un control de acceso, pero rara vez está activo. Situaciones como esta no sólo aumentan la probabilidad de que se produzca un incidente si no que, en caso de que ocurra, complican la posibilidad de averiguar quién se encontraba en un equipo en un momento determinado.

En otros equipos propios del sistema de control (PLC, equipos específicos de mantenimiento, pasarelas de comunicaciones, etc.) ocurre exactamente lo mismo. Lo más habitual es que no dispongan de contraseñas o que, si existen, éstas sean contraseñas por defecto. Es el caso, por ejemplo, de muchos PLC que se encuentran en producción. Para descargar o modificar el programa que se encuentra en ejecución sólo es necesario conectarse al mismo utilizando el software del fabricante que, en la mayoría de las ocasiones, es accesible sin demasiados inconvenientes puesto que no se solicita ningún tipo de credencial.

Esto es especialmente relevante cuando, en muchos casos, es precisamente en esa lógica en ejecución donde reside una parte fundamental de la estrategia de la organización llegando incluso a ponerse en jaque su supervivencia si dicha información es vulnerada de algún modo.

4.12 ER 12: Falta de gestión técnica de la seguridad y sistemas

Palabras clave	
Gestión técnica, sistemas, redes, comunicaciones, seguridad	
Activos	Agentes
<ul style="list-style-type: none"> • Lógica en ejecución en controladores y/o PC SCADA • Equipos, máquinas y/o instalaciones • Información del proceso y/o de la organización • Medio Ambiente • Personal propio y/o de terceros • Terceras personas 	<ul style="list-style-type: none"> • Ciberdelincuentes • Personal propio y de terceras partes • Estados • Terroristas
Factores de riesgo	
<ul style="list-style-type: none"> • No se lleva a cabo ningún tipo de control sobre el tráfico de la red del ICS. • Se desconocen las vulnerabilidades o no se lleva a cabo su parcheo en los equipos del ICS. • No se gestionan adecuadamente o no existen cortafuegos (firewalls) en la red de control. • Las reglas de los cortafuegos no son adecuadas. • La segmentación de la red de control y la red corporativa es deficiente. • No se hace uso de protocolos cifrados en la red de control. • No se hacen evaluaciones periódicas de ciberseguridad. 	
Contexto	
<p>La importancia que se da a la seguridad lógica en el ámbito industrial es, por desgracia y en la práctica, limitada. Más allá de la gestión que se pueda hacer de la seguridad a nivel de procedimientos por parte del personal propio de la organización y de terceros subcontratados, se lleva a cabo, en general, una gestión técnica deficiente de la seguridad y los sistemas. Esto es consecuencia, por un lado, de la falta de percepción del peligro que existe en este tipo de ambientes. Por otro lado, también tiene una gran influencia la imposibilidad de implantar medidas de protección clásicas del mundo IT.</p>	

Pongamos como ejemplo el uso de protocolos cifrados, ampliamente utilizados en el ámbito corporativo. En la industria es, en la práctica, muy difícil implantar este tipo de comunicaciones. La vida útil de los equipos industriales es mucho más elevada que la de los equipos IT. Esto provoca que en la industria se cuente con frecuencia con equipos de cierta antigüedad que no fueron concebidos para utilizar este tipo de protocolos. Adicionalmente, muchos sistemas, debido a su modo de funcionamiento o a su criticidad, no pueden operar con los retardos que introducen en las comunicaciones el uso de protocolos cifrados. Además, en la gran mayoría de los casos, cambiar los protocolos de comunicaciones implica a su vez cambiar los equipos, con los inconvenientes y el coste económico que ello conlleva.

Adicionalmente, tampoco es frecuente que se lleve a cabo el guardado ni revisión sistemática de los registros de actividad o bitácora (logs) de los diferentes equipos del sistema ni que se instalen cortafuegos y se establezcan configuraciones adecuadas de los mismos y es común encontrar segmentaciones deficientes en la red de control y generalmente no se llevan a cabo revisiones de la arquitectura ni auditorías periódicas de las mismas.

Otro ejemplo que muestra la dificultad de implantar cierto tipo de medidas puede ser el uso de sistemas de detección automática de intrusos (IDS²²) en la red de control. Se trata de un sistema automático que analiza el tráfico de la red y genera un aviso en caso de detectar situaciones anómalas. Mientras que en el ámbito corporativo no es extraña su instalación y se cuenta con amplios repositorios de reglas de detección, poner en marcha un sistema de estas características en la red corporativa no es tarea sencilla. Las reglas que deben generarse para operar dentro de una red de control industrial deben ser específicas para cada sistema y exigen un conocimiento profundo del proceso y el modo en que los diferentes equipos interactúan entre sí.

5 CRITERIOS PARA LA REALIZACIÓN DE ANÁLISIS DE RIESGOS

5.1 Aproximación al análisis de riesgos y diferencias específicas IT/OT²³

A la hora de llevar a cabo un análisis de riesgos al que están sometidos los activos de un ICS determinado, se consideran **dos factores agregados: probabilidad e impacto**.

- **Probabilidad:** para calcular la probabilidad de que una amenaza se materialice hay que considerar diversos aspectos. Por un lado, la **frecuencia** con que se

²² Intrusion Detection System (IDS)

²³ Tecnologías de la Información / Tecnologías Operacionales (Information Technology/ Operational Technology IT/OT)

puede dar una amenaza o la relevancia para la imagen corporativa de los activos. Por otro lado, hay que tener en cuenta las características o particularidades del objetivo potencial, pues éstas influyen en la probabilidad. Para ello deben tenerse en cuenta criterios como la accesibilidad física y lógica o la existencia de protocolos que puedan mitigar las posibles consecuencias de un ataque.

- **Impacto:** es el grado de repercusión que tendría la materialización de el ER sobre la organización. El impacto se calcula considerando la criticidad de los procesos de la organización que se verían afectados. Para ello, se analiza dicha criticidad y se traslada a los objetivos potenciales en que se sustentan dichos procesos. Dicho de otro modo, los activos "heredan" la criticidad de los procesos a los que dan soporte. Los factores a tener en cuenta para el estudio de las consecuencias varían en función de la organización y del objetivo que se persigue al realizar el análisis de riesgos. Es habitual considerar, entre otros, los siguientes factores: pérdidas económicas, implicaciones legales o daño a la imagen. Además, en el caso de infraestructuras críticas, debe considerarse no sólo el impacto sobre la organización sino también sobre la sociedad.

Nótese que, aunque en la teoría la metodología para evaluar el riesgo puede parecer similar en el ámbito IT y en el ámbito OT o industrial, en la práctica, el modo en que estos se aplican presenta ciertas diferencias específicas.

En la estimación de la frecuencia, por ejemplo, se tiene en cuenta la periodicidad en la que una amenaza se puede materializar. Mientras los tiempos considerados en el entorno IT pueden determinar, por ejemplo, que la probabilidad es alta si el ER se materializa varias veces al día, no es razonable aplicar el mismo criterio en el entorno industrial puesto que los tiempos son, en general, mucho más dilatados. Es el caso, por ejemplo, de las actualizaciones de firmware²⁴. Mientras en un PC, un servidor o, incluso, un teléfono inteligente o smartphone (ámbito IT) se llevan a cabo actualizaciones de seguridad casi diarias, en un Controlador Lógico Programable (PLC ámbito industrial) no es probable que haya que llevar a cabo actualizaciones más de dos o tres veces en toda su vida útil. Por tanto, la probabilidad de que se materialice un riesgo durante la vida del activo es muy distinta.

Por otra parte, mientras los equipos de entornos IT operan en entornos limpios y con condiciones ambientales controladas, en el entorno industrial es frecuente que los equipos trabajen con polvo y sometidos a temperaturas y humedades elevadas. Incluso la protección física de los equipos es distinta: es altamente improbable que, por ejemplo, una transpaleta golpee un rack de servidores en un Centro de Proceso de Datos (CPD), mientras que en una planta industrial es una situación verosímil.

²⁴ Firmware funciona como el nexo de unión entre las instrucciones (software) que llegan al dispositivo desde el exterior y las diversas partes electrónicas (hardware)

Adicionalmente a éstas y otras diferencias IT/OT, la estimación tanto de la probabilidad como del impacto varía también en función del subsector que se esté considerando. En los siguientes apartados, utilizando la clasificación realizada en el punto 3.2, se afronta esta cuestión de manera detallada.

5.2 Criterios para la estimación de la probabilidad por subsectores

En este apartado se abordan distintos criterios generales que deben tenerse en cuenta a la hora de estimar la probabilidad de materialización de una amenaza en un entorno industrial.

La probabilidad de una amenaza guarda una fuerte relación con la frecuencia en la que ésta se puede dar en el ICS pero se ve modificada por otros factores. Por ejemplo, también tiene influencia la existencia de contramedidas y salvaguardas en el sistema objeto del estudio. Estas contramedidas reducen la probabilidad de que una amenaza se haga efectiva y/o contribuyen a minimizar las consecuencias derivadas de la materialización de la misma.

Para evaluar todos estos criterios es conveniente definir escenarios de siniestro para cada una de las ubicaciones en las que residen objetivos potenciales. Cuando un activo puede encontrarse en más de una ubicación es conveniente ser conservador y asignar el más desfavorable.

Por ejemplo, la frecuencia es uno de los criterios utilizados para la estimación de la probabilidad, pues se tiene en cuenta la periodicidad de materialización de los ERs. Tal y como se ha introducido en el apartado 55.1, es necesario establecer plazos razonables ajustados a la realidad del sector industrial. Esto implica conocer con profundidad el sistema de control y su grado de criticidad en la organización, pero también disponer de una visión global de con qué frecuencia se dan estas amenazas en la industria. En cualquier caso, la experiencia dicta que, de manera general, se habla de plazos de tiempo más amplios que en el ámbito IT: semestres, años o incluso lustros.

Por otro lado, la naturaleza de ciertos objetivos potenciales los convierte en blancos preferentes frente a la materialización de algunas amenazas. Este hecho se ve reflejado como un agravamiento o incremento de la probabilidad. Se requiere, por tanto, conocer cuál es la importancia de la infraestructura que se está evaluando para la organización, de modo que se pueda determinar la relevancia que tiene a nivel de, por ejemplo, imagen corporativa o si, en caso de verse afectado, se produciría cierta repercusión social.

Además, los elementos que proporcionan seguridad a la organización suelen ser blancos preferentes. Es importante que este tipo de objetivos se mantengan operativos incluso tras la materialización de el ER. Los sistemas de control de acceso, los sistemas de video vigilancia y los cortafuegos son ejemplos de objetivos potenciales. Se produce un incremento de la probabilidad de presentación de un suceso en este tipo de activos como consecuencia de que el objetivo potencial es relevante para la seguridad de la organización (o de la sociedad en el caso de infraestructuras críticas) ya bien sea por que se trate de un elemento de seguridad o por intervenir en funciones de seguridad (ej. equipo de respuesta ante incidentes, control de emergencias, instalaciones de bomberos, etc.)

También debe tenerse en cuenta la accesibilidad, que es una medida de la facilidad con la que es posible llegar al objetivo potencial. Tanto a nivel físico como lógico. Por

ejemplo, a la hora de impedir el acceso a un elemento físico se puede establecer un vallado perimetral. Si hablamos de objetivos potenciales lógicos, se puede impedir el acceso a información confidencial definiendo unas políticas de acceso lógico basadas en la clasificación de la información, definición de roles y asignación de privilegios. También se tiene en consideración la existencia de sistemas de seguridad como cortafuegos (firewalls), sistemas de detección de intrusos (IDS), etc. En el entorno industrial es común que los trabajos de mantenimiento lo realice personal ajeno a la organización. Por ello, la accesibilidad se ve incrementada en estos casos. Además, en algunos sectores es frecuente que existan instalaciones desatendidas.

Así mismo, es conveniente evaluar la resistencia del objetivo potencial frente a las amenazas y las medidas de seguridad implantadas para proteger dicho objetivo. A la hora de evaluar este parámetro se tienen en cuenta la existencia de sistemas redundantes que actúen en caso de que se destruya el sistema principal.

Es frecuente que en infraestructuras críticas (distribución de agua potable, generación y transporte de energía, grandes CPD, etc.) se cuente con sistemas de alta disponibilidad que son seguros a fallos físicos pero en los que no se ha pensado en fallos lógicos. Por ejemplo, se cuenta con equipos redundantes conectados a la misma red para que tomen el relevo en caso de ser necesario. Sin embargo, es probable que no se haya pensado en que si uno de los equipos es infectado por código dañino o malware, es posible que el equipo redundante también se vea afectado. De esta forma, si tuviera lugar un ciberataque de estas características, no bastaría con disponer de equipos redundantes desde el punto de vista de la operación.

Por otro lado hay que valorar el grado de madurez de los procedimientos implantados en la organización para evitar la materialización de las amenazas y/o hacer frente a las mismas una vez se hayan producido. Se debe evaluar si la organización ha definido protocolos para responder ante incidentes, si los ha comunicado al personal implicado y si se realizan pruebas periódicas para verificar que dichos procedimientos son efectivos.

Afortunadamente, el personal industrial está acostumbrado a trabajar de manera procedimentada porque existen multitud de reglamentos técnicos que tienen implicaciones legales y cuyo fin es proteger la seguridad física de las personas y las cosas. Éste es un buen punto de partida que permite introducir nuevos procedimientos relativos a la ciberseguridad en los sistemas de control.

Es común en algunos tipos de industria como la nuclear que existan planes de emergencia, pero es habitual que éstos no contemplen incidentes de ciberseguridad. Por ejemplo, puede que esté prevista la restauración de un sistema con copias de seguridad, pero no se haya previsto que, si lo que está afectando al ICS es código dañino, dichas copias estén también infectadas.

A continuación, se incluye una tabla con consideraciones específicas sobre estos criterios para cada uno de los grupos del apartado 3.2 teniendo en cuenta las características de cada grupo de sectores en cuestión. Téngase en cuenta que dicha particularización se ha hecho en términos generales por subsector y requerirá de aproximaciones concretas para cada activo e instalación evaluada.

CRITERIOS GENERALES PARA LA EVALUACIÓN DEL RIESGO	
SUBSECTOR	Estimación de la probabilidad
Grupo 1 <ul style="list-style-type: none"> • Sistema financiero y tributario • Instalaciones de investigación • Administración • Tecnologías de la Información y las Comunicaciones 	<p>Es frecuente que en este tipo de entornos se lleven a cabo actualizaciones de seguridad en sus sistemas. Aunque, a priori, este proceder es adecuado, debe tenerse en cuenta que, con frecuencia, los equipos industriales (servidores SCADA, por ejemplo) presentan problemas de compatibilidad frente a ciertas actualizaciones. Por lo tanto, las políticas asociadas deben contemplar esta circunstancia.</p> <p>Algunos sectores de este grupo se caracterizan por tener infraestructuras con un carácter simbólico muy elevado. Puede ser el caso, por ejemplo, de los ICS en Centros de Procesamientos de Datos de organizaciones del sector financiero o pertenecientes a la Administración. Las repercusiones sobre la imagen de una organización o un Estado pueden ser muy altas.</p> <p>A pesar de ser una infraestructura IT, como existen ICS que dan soporte al mismo (sistema de refrigeración o control del suministro eléctrico por ejemplo), un CPD hereda los problemas asociados a los sistemas industriales. De este modo, el personal responsable de la infraestructura, generalmente familiarizado con las medidas IT, tiene una falsa sensación de seguridad porque percibe que estas medidas están protegiendo simultáneamente el sistema industrial cuando, generalmente, no suele ser el caso.</p> <p>Por lo que se refiere a los controles de acceso lógicos, este tipo de sectores suele contar con medidas de seguridad elevadas. En cualquier caso, no debe perderse de vista que, por tratarse de sistemas de naturaleza distinta a los que estas organizaciones están acostumbrados a gestionar y a menudo porque se desconocen con exactitud las consecuencias de un incidente, es relativamente común que no se apliquen las mismas políticas de seguridad en los elementos de la red de control que en la red corporativa.</p> <p>En cuanto a la seguridad física, es frecuente que en las instalaciones estos sectores cuenten con vallados perimetrales, videovigilancia, controles de acceso, etc.</p> <p>Es frecuente que los sistemas cuenten con equipos de respaldo a nivel lógico y también a nivel de alimentación eléctrica.</p>
Grupo 2 <ul style="list-style-type: none"> • Transporte • Agua • Energía 	<p>En la medida en que los ICS de las infraestructuras de este grupo controlan elementos que dan servicio a grandes cantidades de población, el carácter simbólico tiende a ser elevado. Puede ser el caso, por ejemplo, de instalaciones pertenecientes al sistema de transporte o distribución de energía eléctrica. Atacar, por ejemplo, al sistema de transporte eléctrico de una nación es atacar a la nación en sí misma.</p>

CRITERIOS GENERALES PARA LA EVALUACIÓN DEL RIESGO	
SUBSECTOR	Estimación de la probabilidad
	<p>Puesto que las instalaciones de este subsector se encuentran diseminadas en amplias extensiones geográficas, como por ejemplo las redes de distribución de agua potable, es lógico pensar que la facilidad de acceso físico a las mismas se ve incrementada. Especialmente cuando en algunos casos muchas de las infraestructuras donde existen equipos de control no hay personal de manera permanente. Es el caso, por ejemplo, de las subestaciones eléctricas. Por esta razón, también es frecuente encontrarse con equipos que permiten ser gestionados de manera remota y de este modo evitar el desplazamiento de personal para llevar a cabo modificaciones menores por lo que hay que ser muy cuidadoso a la hora de evaluar si los controles de acceso lógico son los adecuados.</p> <p>Las redes de suministro de este tipo de organizaciones suelen ser malladas, es decir, permiten el fallo de una o más instalaciones sin que esta situación afecte apreciablemente al servicio. Además, como consecuencia de la amplia distribución a nivel geográfico, no es extraño que las comunicaciones estén redundadas para asegurar que se cuenta con visibilidad remota en caso de fallo. Estas consideraciones tienen como consecuencia que la probabilidad de que un incidente tenga lugar sea menor.</p>
Grupo 3 <ul style="list-style-type: none"> • Alimentación • Manufactura • Salud • Servicios 	<p>En general, las infraestructuras que controlan los ICS en este subsector no tienen un carácter simbólico elevado. Aunque el impacto para la organización puede ser alto, no es común que un incidente en un sistema de control de una instalación de tamaño limitado tenga grandes repercusiones de imagen o relevancia en los medios de comunicación.</p> <p>La situación en cuanto a facilidad de acceso físico a las instalaciones de este subsector es muy heterogéneo y depende de cada organización. Por ejemplo, hay instalaciones que cuentan con video vigilancia exterior, como pueden ser los hospitales, pero donde no se captan imágenes de la sala de control ni del interior de las salas donde se hallan los cuadros eléctricos donde se sitúan habitualmente los equipos del nivel de control de los ICS. Estas salas se encuentran generalmente distribuidas por toda la instalación y es frecuente que las puertas de estas salas estén abiertas o no se cierran con llave. Si, además, el perímetro no está delimitado o protegido convenientemente, aumenta de manera considerable la facilidad de acceso.</p> <p>En función de la criticidad del proceso que el ICS controla, la organización puede disponer de respaldos en alimentación eléctrica o redundancias en equipos y electrónica de red en los niveles de supervisión y control. Si eso es así, la susceptibilidad a la destrucción disminuye</p>

CRITERIOS GENERALES PARA LA EVALUACIÓN DEL RIESGO	
SUBSECTOR	Estimación de la probabilidad
	considerablemente.
Grupo 4 Industria química Industria nuclear	<p>Las infraestructuras controladas por los ICS de este grupo se caracterizan por tener un carácter simbólico muy elevado por las graves consecuencias que podría tener para la salud o la vida de las personas y el medio ambiente funcionamientos no adecuados o cierto tipo de incidentes. Es el caso de las centrales nucleares o las refinerías, por ejemplo. La relevancia mediática que puede tener un incidente en este tipo de instalaciones las convierte en un blanco perfecto cuando lo que busca el atacante es impacto en los medios de comunicación.</p> <p>Aunque las instalaciones de estos sectores suelen encontrarse alejadas de núcleos urbanos grandes, lo que en principio podría facilitar el acceso físico, suelen contar con medidas de control muy elevadas. Frecuentemente existe CCTV²⁵ supervisado, vallado e incluso patrullas de seguridad privada por el perímetro o el interior de las instalaciones.</p> <p>Generalmente se evita la interconexión con otras redes, pero si éstas existen debe verificarse que la segmentación es adecuada y que se hace una revisión periódica de la misma.</p> <p>Como consecuencia de la criticidad de los procesos que controlan los ICS en este subsector, se cuenta generalmente con redundancias que duplican o incluso triplican todos los niveles del sistema de control. La susceptibilidad a la destrucción de los activos en este tipo de sistemas es reducida.</p> <p>Es frecuente que en este subsector se cuente con planes de emergencia que se ensayan con cierta regularidad pero que, generalmente, no incorporan protocolos de respuesta ante incidentes de ciberseguridad.</p>

5.3 Criterios para la estimación de impacto por subsectores

A través de la estimación de impacto se cuantifican las consecuencias que tiene sobre la organización la materialización de una amenaza. Es más difícil estimar de manera general el

²⁵ Circuito cerrado de televisión (Closed Circuit Television CCTV)

impacto que la probabilidad porque existe una diversidad muy amplia de entornos industriales. Téngase en cuenta que, por ello, esta particularización se ha hecho en términos generales por subsector y requerirá de aproximaciones concretas para cada activo e instalación evaluada.

Se debe valorar el impacto que tendría una pérdida de confidencialidad, integridad y/o disponibilidad de los activos y, en consecuencia, de los procesos de negocio. En aras de simplificar la estimación de las consecuencias, se valoran de manera implícita las distintas dimensiones de la seguridad de la información (confidencialidad, integridad, disponibilidad, etc.) y se estiman las consecuencias considerando factores específicos de cada sector.

Los **factores a tener en cuenta para el estudio de las consecuencias** varían en función de la organización y del objetivo que se persigue al realizar el análisis de riesgos. Es habitual considerar los que se indican a continuación.

Por un lado, **las personas afectadas**. Debe hacerse una estimación del número de empleados, trabajadores de empresas terceras y población en general afectados por la incidencia.

Es conveniente evaluar también **las posibles pérdidas económicas**. Este factor mide el impacto en términos económicos que tiene la materialización de el ER. Se consideran tanto los costes de reposición de elementos destruidos como los asociados al cese de las actividades de negocio.

Por otro lado, un posible criterio es el **tiempo máximo de parada del proceso**, que valora cuantitativamente el tiempo máximo que un proceso de negocio puede estar no disponible. Las consecuencias derivadas de superar este tiempo máximo pueden no ser admisibles para la organización.

El **daño a la imagen** es un factor que estima la pérdida de la reputación corporativa en caso de que un ataque tuviera lugar.

Así mismo, es adecuado tener en cuenta también las **posibles implicaciones legales** derivadas de la materialización de el ER: reglamentos técnicos existentes, consecuencia de daños al medio ambiente, etc.

A la hora de aproximar el impacto que tendría la materialización de una amenaza es necesario conocer la dependencia que existe entre el objetivo potencial (activo) y los procesos de negocio por lo que se requiere que el evaluador disponga de información suficiente al respecto.

Estimar el impacto potencial en sistemas de control industrial puede llegar a ser muy complejo como consecuencia de las **interdependencias** que se pueden dar en este tipo de entornos.

A continuación, se incluye **una tabla con consideraciones específicas sobre estos criterios para cada uno de los grupos** del apartado 3.2 teniendo en cuenta las características de cada grupo de sectores en cuestión.

CRITERIOS GENERALES PARA LA EVALUACIÓN DEL RIESGO	
SUBSECTOR	Estimación del impacto
Grupo 1 <ul style="list-style-type: none"> • Sistema financiero y tributario • Instalaciones de investigación • Administración • Tecnologías de la Información y las Comunicaciones 	<p>En general, estos sectores dan servicio a una cantidad elevada de personas. Un ataque a los ICS que pudiera afectar a la continuidad de los procesos que llevan a cabo podría tener consecuencias directas sobre un amplio grupo de individuos pero, por otra parte, es difícil que impliquen riesgo para la vida de las personas o el medio ambiente.</p> <p>Por el ámbito en el que trabajan las organizaciones incluidas en este subsector, las infraestructuras de que disponen tienen un alto coste y la información con la que trabajan es de alto valor. Es el caso de registros civiles, juzgados o la bolsa. Por ello, las pérdidas económicas asociadas a, por ejemplo, la no disponibilidad de cierta información en un momento determinado podrían llegar a ser muy elevadas.</p> <p>Dado que la relevancia económica o de ciertos servicios es alta, el tiempo máximo de parada que se puede permitir en este tipo de sistemas tiende a ser reducido. Las operadoras de telecomunicaciones pueden ser un ejemplo.</p> <p>Es común que los sectores vinculados a este grupo tengan infraestructuras con un alto valor simbólico, por ello incidentes en activos de estas instalaciones pueden generar un daño importante a la imagen de la organización.</p>
Grupo 2 <ul style="list-style-type: none"> • Transporte • Agua • Energía 	<p>Dado que estos sectores de la industria dan servicio a grandes cantidades de población, el número de personas afectadas en caso de una incidencia puede ser muy elevado.</p> <p>Una gran parte del funcionamiento de la sociedad en general depende de que las organizaciones que pertenecen a este subsector funcionen sin incidentes. Esto provoca que una eventualidad en un ICS dentro de este ámbito que genere, por ejemplo, la detención de parte de los procesos que se llevan a cabo, tenga graves consecuencias económicas no sólo en la organización víctima del ataque sino también en sus clientes. Piénsese, por ejemplo, en la pérdida de suministro de eléctrico o de agua en una gran población.</p> <p>Los sistemas de este tipo de sectores son, en muchos casos, mallados por lo que es frecuente que admitan simultáneamente varios fallos durante plazos de tiempo razonables. Si tiene lugar un incidente en una ubicación concreta, el diseño del proceso es suficientemente robusto como para que el servicio no se vea afectado de manera significativa. Sin embargo, si se produce un incidente a nivel global que es capaz de generar un problema de consecuencias generales en el proceso, el tiempo máximo de parada tiende a cero, puesto que muchos otros servicios</p>

CRITERIOS GENERALES PARA LA EVALUACIÓN DEL RIESGO	
SUBSECTOR	Estimación del impacto
	<p>esenciales dependen en gran medida del funcionamiento de estos sistemas.</p> <p>Por la relevancia que tiene este tipo de industrias en la sociedad, la materialización de una amenaza en sus ICS que tenga consecuencias sobre la continuidad del proceso tiene implicaciones importantes sobre la imagen corporativa e, incluso, en función de la gravedad del suceso, trascendencia en los medios de comunicación.</p>
Grupo 3 <ul style="list-style-type: none"> Alimentación Manufactura Salud Servicios 	<p>El número de personas que pueden verse afectadas como consecuencia de un ataque a un ICS de este subsector es, en general, limitado puesto que el número de empleados propios y de terceros no suele ser elevado y el número de personas externas al que puede afectar está restringido a los clientes de la organización.</p> <p>Las pérdidas económicas varían considerablemente en función de la organización y del tipo de ER que se haya materializado en sus ICS. En cada situación hay que considerar el gasto de reposición de equipos y material destruidos, pero también hay que considerar otro tipo de costes. Por ejemplo, en caso de una industria dedicada a la manufactura, las pérdidas asociadas a la no producción si el incidente afecta a la continuidad del proceso. Si hablamos por ejemplo del sector de la salud deberían tenerse en cuenta los costes adicionales derivados por solicitar la intervención de terceros para proveerse de un servicio necesario del que no se puede prescindir.</p> <p>El tiempo máximo de parada que se puede permitir un sistema de este subsector es muy heterogéneo y depende de nuevo de la criticidad específica del proceso que lleva a cabo. En ocasiones basta una parada breve para causar un impacto no proporcional a la duración de la interrupción. Por ejemplo, una parada en un proceso de inyección de plástico no sólo supone la pérdida de la materia prima, sino también, posiblemente, de las boquillas de inyección. Adicionalmente, se requiere un largo proceso de limpieza hasta poder reanudar la producción. En otros casos el daño se limita a la duración del incidente. Dentro del sector servicios, un parque acuático podría ser un ejemplo de ello.</p> <p>El daño a la imagen corporativa puede producirse en caso de que el incidente en el ICS tenga consecuencias sobre el cliente de la organización. Podría ser, por ejemplo, el caso de situaciones que generan una parada en la producción y por tanto un retraso en la entrega del producto al cliente. Generalmente, por la limitada relevancia para el conjunto de la sociedad que tiene este tipo de organizaciones, incidentes que afectan a los ICS de esas organizaciones no suelen tener excesiva divulgación en los</p>

CRITERIOS GENERALES PARA LA EVALUACIÓN DEL RIESGO	
SUBSECTOR	Estimación del impacto
	medios de comunicación.
Grupo 4 <ul style="list-style-type: none"> Industria química Industria nuclear 	<p>El número de personas afectadas por un incidente en un ICS de este subsector puede ser extremadamente elevado. Además, las consecuencias sobre la salud en el personal de la organización o incluso de población en general pueden ser graves. Por ejemplo, un incendio en una refinería.</p> <p>Es frecuente que el coste asociado a la producción de este tipo de organizaciones sea elevado. A menudo las materias primas con las que se trabaja tienen un precio muy alto o los procesos, si se detienen, no pueden retomarse en el punto en el que se quedaron, si no que implican una pérdida del producto en proceso generación. Por esta razón, las pérdidas económicas pueden ser muy elevadas si se materializa un incidente en un sistema de control de este subsector.</p> <p>El tiempo máximo de parada en este grupo tiende a ser reducido pero depende de la criticidad del proceso. Existen sistemas dentro de este subsector que pueden detenerse durante un periodo determinado sin que esto afecte a la producción de manera significativa. Así mismo, existen otros procesos cuya parada supone un coste muy elevado, como es el caso de las centrales nucleares.</p> <p>Adicionalmente, las implicaciones legales que puede tener un incidente, por menor que éste sea, en una industria de este subsector pueden ser considerables. Por ejemplo, un vertido a cauce por encima de los niveles en ciertos parámetros permitidos puede acarrear multas considerables por las consecuencias al medio ambiente o sobre la salud de las personas.</p>