TLP:WHITE

GOBIERNO DE ESPAÑA MINISTERIO DEL INTERIOR

GOBIERNO DE ESPAÑA MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL

Esquema Nacional de Seguridad Industrial

ENSI_ARLI-CIB_01- Modelo de Análisis de Riesgos Ligero de Ciberseguridad en Sistemas de Control Industrial (ARLI-CIB)

certsi_

CERT DE SEGURIDAD E INDUSTRIA

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

NOVIEMBRE 2016

1. OBJETO DEL DOCUMENTO

Este documento establece la Metodología de Análisis de Riesgos Ligero de Ciberseguridad en Sistemas de Control Industrial (ARLI-CIB) del Esquema Nacional de Seguridad Industrial (ENSI).

Como tal, desarrolla el modelo ARLI-CIB y los pasos esenciales para su aplicación haciendo referencia a las plantillas que lo instrumentan y facilitan su implementación de forma homogénea.

A lo largo del texto aparecen una serie de cuadros sombreados en color o tono gris.
Se trata de referencias a (extractos de) la Resolución Publicada en el BOE de 8 de septiembre de 2015, de la Secretaría de Estado de Seguridad [1], por la que se aprueban los nuevos contenidos mínimos de los Planes de Seguridad del Operador y Planes de Protección Específicos.
Su inclusión pretende ayudar al lector a identificar los requisitos exigidos por la legislación en materia de protección de infraestructuras críticas con los diferentes pasos del modelo ARLI-CIB aquí presentado.

2. ACERCA DEL ENSI

La promulgación de la Ley 8/2011, de 28 de abril, por la que se establecen medidas para la Protección de las Infraestructuras Críticas (Ley PIC), puso de manifiesto la importancia de la seguridad de las Infraestructuras Críticas dentro de la Seguridad del Estado. Por su parte, la Estrategia de Seguridad Nacional [2] de 2013 reconoce, por primera vez, las ciberamenazas como uno de los riesgos y amenazas a la seguridad nacional. Complementando la anterior, la Estrategia de Ciberseguridad Nacional [3] de 2013 completa la apuesta por la protección de los sistemas de control industrial como elemento clave en un enfoque integral de la ciberseguridad

En este contexto, el Instituto Nacional de Ciberseguridad (INCIBE), del Ministerio de Energía, Turismo y Agenda Digital, y el Centro Nacional de Infraestructuras Críticas del Ministerio del Interior, de la mano del acuerdo suscrito en 2012 y renovado en 2015 entre la Secretaría de Estado para la Sociedad de la Información y la Agenda Digital (SESIAD) y la Secretaría de Estado de la Seguridad (SES), promueven el Esquema Nacional de Seguridad Industrial (ENSI), como instrumento para mejorar la seguridad de las infraestructuras críticas industriales y con una vocación global en tanto que es aplicable en sistemas de control industrial de cualquier organización.

Para ello, favorecer el tratamiento homogéneo de la seguridad y extender su aplicación a toda la cadena de valor de las organizaciones industriales, reconociendo el papel de proveedores y clientes, son las claves para dibujar el panorama completo al que responde el ENSI, que podría conformar la base para nuevas iniciativas que permitieran al ENSI ampliarse e incluir la seguridad desde un punto de vista más integral.

El ENSI se concreta en cuatro elementos esenciales que se configuran para atender a las necesidades específicas de su ámbito de aplicación:

- ARLI-SI: Metodología de Análisis de Riesgos Ligero de Seguridad Integral como punto de partida y piedra angular del proceso de mejora de la seguridad. Con entidad propia, dentro de esta metodología, ARLI-CIB permite un acercamiento específico, y también ligero, al Análisis de Riesgos de Ciberseguridad en sistemas de control industrial.
- IMC: Indicadores para la Mejora de Ciberresiliencia, como instrumento de diagnóstico y medición de la capacidad para soportar y sobreponerse a desastres y perturbaciones procedentes del ámbito digital.
- C4V: Modelo de Construcción de Capacidades en Ciberseguridad de la Cadena de Valor como elemento imperante en la operativa y actividad de la prestación de servicio del operador: proveedores y clientes.
- SA: Sistema de Acreditación en Ciberseguridad, garantía de la aplicación de unas medidas de seguridad mínimas equivalentes en todas las arquitecturas que prestan servicios equiparables o semejantes.

La aproximación práctica y ligera predomina en todos los elementos del ENSI y dibuja un marco completo para la mejora de la ciberseguridad en sistemas de control industrial.

Aquí, las diferentes guías y documentos de articulación, siempre alineados con todo lo establecido para los Planes de Seguridad del Operador, Planes de Protección Específicos

y Planes Estratégicos Sectoriales, aportarán las instrucciones, criterios y herramientas para facilitar su aplicación por parte de los diferentes agentes.

3. ANTECEDENTES

Una característica del riesgo es su naturaleza subjetiva; esto es, lo que en unas determinadas condiciones pudiera tildarse de riesgo admisible, bajo una diferente coyuntura podría resultar completamente inaceptable. Esa es la razón fundamental por la que toda organización -los individuos al frente de la misma, de sus operaciones, de sus infraestructuras, procesos etc.- ha de ser capaz de comprender y fijar, adecuadamente, un umbral de riesgo tolerable y aceptable desde el punto de vista de la actividad (negocio) de la propia organización, para lo cual el análisis de riesgos deberá estar basado en un modelo con criterios de valoración, objetivos y homogéneos, que permitan obtener valores comparables.

De ese modo, se podrá saber si se está sobrepasando, o no, el referido umbral; y, en su caso, ello permitirá decidir la mejor respuesta para: i) evitar, en la medida de lo posible, la materialización de la amenazas; ii) corregir las vulnerabilidades; o, iii) reducir las consecuencias de los previsibles impactos. Además, conocer el grado de riesgo frente al umbral servirá como criterio para priorizar y ajustar las medidas de tratamiento.

La ciberseguridad en los entornos industriales más dependientes de las tecnologías ha tomado una gran relevancia, motivada por el impacto que podría tener un ciberataque a gran escala en estos sistemas y en las infraestructuras a las que dan soporte. Los ciberataques a infraestructuras estratégicas son una realidad diaria, y por ello los países están haciendo un esfuerzo por mejorar sus niveles de ciberseguridad.

Desde INCIBE y el CERTSI se está trabajando en la elaboración del Esquema Nacional de Seguridad Industrial (ENSI), que abordará un catálogo completo de guías, procedimientos, normativas de buenas prácticas y estándares de ciberseguridad, de los que forma parte este Modelo de Análisis de Riesgos, el cual está basado en guías y estándares reconocidos por la industria, como las familias de normas internacionales ISA/IEC 62443 e ISO/IEC 27000 y el marco de referencia sobre Métricas de Ciberresiliencia de INCIBE.

4. MODELO DE ANÁLISIS DE RIESGOS LIGERO

4.1. Definición

El Modelo de Análisis de Riesgos Ligero de Ciberseguridad en Sistemas de Control Industrial (ARLI-CIB) ha sido elaborado al objeto de proporcionar un modelo sencillo y práctico de análisis de riesgos de ciberseguridad en sistemas de control industrial que permita:

- identificar
- analizar
- evaluar
- tratar

Oportunamente aquellos riesgos que afecten a infraestructuras con sistemas de control industrial; y, al mismo tiempo, obtener resultados comparables y reproducibles.

El modelo estará dirigido, por tanto, a organizaciones industriales con infraestructuras o procesos productivos automatizados. Resulta, por ello, de especial aplicación a los operadores de infraestructuras críticas (en el plano de la ciberseguridad), quienes están obligados a cumplir los dictados de la *Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas*, desarrollada en el *Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas*.

Los operadores a que se refiere el párrafo anterior están obligados a elaborar un Plan de Seguridad del Operador (PSO) y Planes de Protección Específicos (PPE) que habrán de incluir análisis de riesgos, tanto a nivel organizativo como de cada infraestructura crítica.

Resolución de 8 de septiembre de 2015

Anexo I. Guía Contenidos Mínimos PSO

Apartado 1.1. Base legal

El artículo 13 de la Ley explicita una serie de compromisos para los operadores críticos públicos y privados, entre los que se encuentra la necesidad de elaboración de un Plan de Seguridad del operador (en adelante, PSO) y de los Planes de Protección Específicos que se determinen (en adelante, PPE).

Apartado 4. Metodología del análisis de riesgos

En virtud de lo establecido en el artículo 22.3 del Real Decreto 704/2011, en el PSO se plasmará la metodología o metodologías de análisis de riesgos empleadas por el operador crítico.

Resolución de 8 de septiembre de 2015

Anexo II. Guía Contenidos Mínimos PPE

Apartado 1.1. Base legal

En el PPE, el operador crítico aplicará los siguientes aspectos y criterios incluidos en su PSO, que afecten de manera específica a esa instalación:

- *… Desarrollo de la metodología de análisis de riesgos que garantice la continuidad de los servicios proporcionados por dicho operador a través de esa infraestructura crítica …*

En todo caso los análisis de riesgos deberán basarse en una metodología en la que los valores que se utilicen y las estimaciones de los diferentes parámetros (vulnerabilidad, impacto...) sean homogéneos. Ello permitirá que sean repetibles, manteniendo un mismo criterio a lo largo del tiempo, lo cual favorecerá, la obtención de resultados comparables.

4.2. Marco Conceptual

El marco conceptual del Modelo de Análisis de Riesgos de Ciberseguridad en Sistemas de Control Industrial queda resumido en la Figura 1, que muestra sus principales componentes y las relaciones entre ellos.

Figura 1: Marco conceptual del Modelo de Análisis de Riesgos de Ciberseguridad en SCI

Los principales componentes que habrán de ser identificados y analizados, dentro del modelo, se enumeran a continuación:

Activos: Recursos -habitualmente de naturaleza técnica- vinculados con las actividades de operación o de información de la organización, que resultan necesarios para que las infraestructuras o procesos productivos de aquella funcionen correctamente, y puedan prestar los servicios esenciales previstos.

Estos últimos podrán verse afectados por amenazas de carácter negligente o intencionado -por ejemplo, de origen terrorista u otro-; y, consecuentemente, sufrir algún tipo de impacto de menor o mayor gravedad.

Vulnerabilidades: Constituyen una característica intrínseca de los activos: se dice de un activo que es vulnerable o presenta vulnerabilidades.
La vulnerabilidad se define como la estimación de la exposición efectiva de un activo a una amenaza y puede determinarse por medio de dos medidas: frecuencia de ocurrencia/aparición o degradación causada.

Amenazas: Son eventos que pueden desencadenar un incidente sobre los activos subyacentes a los servicios esenciales, produciendo pérdidas materiales o daños inmateriales y afectando al funcionamiento correcto de la infraestructura o proceso productivo. Las amenazas se derivan de la existencia de vulnerabilidades.

Impactos: Son las consecuencias que, sobre un activo, tiene la materialización de una o más amenazas.

4.3. Componentes del Modelo

El Modelo de Análisis de Riesgos de Ciberseguridad en Sistemas de Control Industrial está formado por los siguientes componentes:

Documentación del Modelo de Análisis de Riesgos de Ciberseguridad en SCI	
Modelo de Análisis de Riesgos de Ciberseguridad en SCI	Documento que contiene el marco conceptual y la metodología del análisis de riesgos.
Plantilla Alcance	Plantilla que permite **describir** la compañía y el Alcance sobre el que se aplicará el Análisis de Riesgos de Ciberseguridad en Sistemas de control industrial.
Plantilla Análisis de Riesgos	Plantilla que permite **identificar** cada servicio esencial, sus activos, amenazas, así como su valoración y medidas de ciberseguridad necesarias para tratar el riesgo.

Tabla 1: Kit documental del Modelo de Análisis de Riesgos de Ciberseguridad en SCI

El Modelo de Análisis de Riesgos dispone de dos plantillas que facilitan la identificación de activos, su valoración, así como la evaluación de escenarios de riesgos y aplicación de medidas. En la siguiente figura se muestra la relación entre ellos:

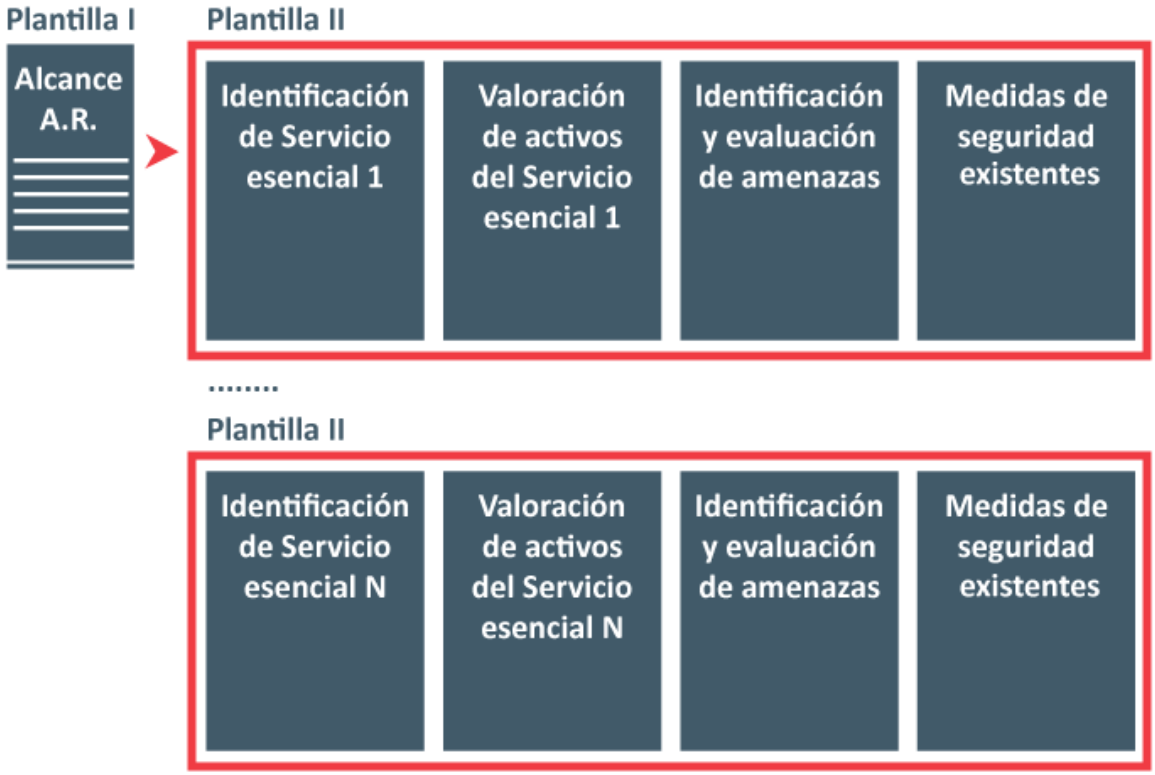


Figura 2: Plantillas del Modelo de Análisis de Riesgos y la relación entre ellos

4.4. Descripción de la Metodología de Análisis

El enfoque propuesto por el Modelo de Análisis de Riesgos de Ciberseguridad en Sistemas de Control Industrial desarrollado a lo largo de esta guía, pasa por: i) delimitar el alcance del análisis; ii) identificar los activos y las amenazas a que puedan estar sujetos; iii) estimar el impacto potencial de las mismas; iv) evaluar la probabilidad de que los escenarios de riesgo, construidos a partir de esas amenazas, se materialicen; y v) sugerir una serie de medidas de protección, de aplicación a la instalación objeto de análisis, dentro del alcance definido.

Resolución de 8 de septiembre de 2015

Anexo I. Guía Contenidos Mínimos PSO

Apartado 4.1. Descripción de la metodología de análisis

Se describirá de forma genérica la metodología empleada por la Organización para la realización de los análisis de riesgos de los diferentes Planes de Protección Específicos (PPE) que se deriven tras la designación de sus infraestructuras críticas. Al menos, se aportará la siguiente información:

- *Pasos esenciales.*
- *Algoritmos de cálculo empleados.*
- *Método empleado para la valoración de los impactos.*
- *Métricas de medición de riesgos aceptables, residuales, etc.*
- *En particular, se harán constar las relaciones entre los análisis de riesgos realizados a distintos niveles: A nivel de corporación, a nivel de servicios y el más concreto, a nivel de infraestructuras críticas.*

La siguiente figura muestra los pasos esenciales referidos en la *figura* 2 en orden.

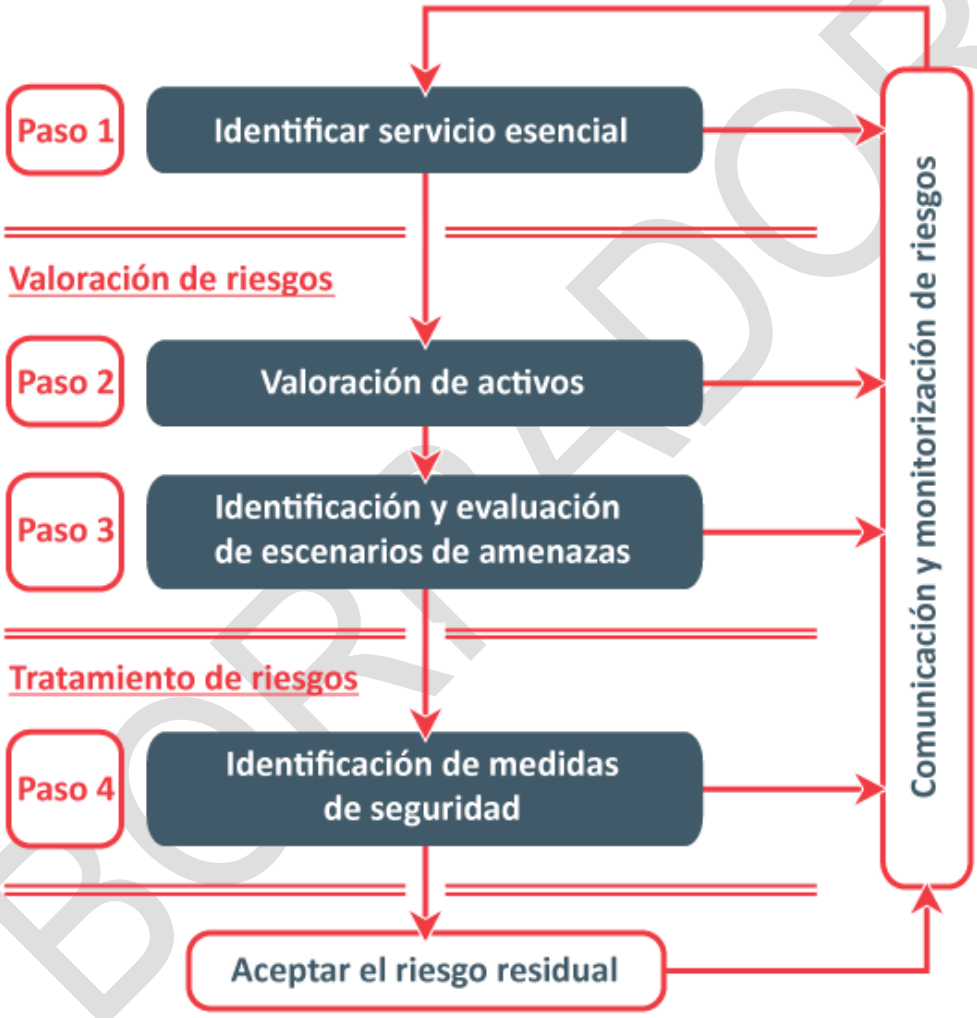


Figura 3: Enfoque general del Modelo de Análisis de Riesgos de Ciberseguridad en Sistemas de Control Industrial (ARLI-CIB)

Consecuentemente, quedarán fuera del ámbito de esta guía las actividades específicamente vinculadas a la gestión de los riesgos obtenidos, esto es, vinculadas al tratamiento propiamente dicho, de aquellos. Un tratamiento que comenzará con la toma de una decisión por parte de los responsables de la instalación, sobre qué hacer con el riesgo -evitarlo, reducirlo, transferirlo o retenerlo- y que seguirá, en su caso, con la adopción y

puesta en marcha de las medidas sugeridas por este modelo (o una parte de ellas) para su mitigación.

De igual modo, resultarán una responsabilidad exclusiva de quienes estén al frente de la instalación -escapando, de nuevo, al ámbito de esta guía- la aceptación del riesgo residual tras el tratamiento, y las actividades transversales de comunicación y supervisión del riesgo, que facilitarán la adopción de una cultura de la ciberseguridad industrial y la mejora continua.

Finalmente, cabe señalar que la aplicación, como base del análisis de escenarios de alto riesgo permitirá realizar hipótesis, tanto sobre la probabilidad de que tales riesgos se materialicen, como sobre la capacidad de la organización para resistir y recuperarse de los impactos/consecuencias asociados.

A fin de atajar la previsible escasez de datos históricos sobre incidentes, el enfoque seguido por el modelo se basará en una **aproximación cualitativa**, en la que se emplearán un conjunto de niveles de probabilidad y severidad (impacto) que resultarán de aplicación a los distintos componentes del modelo.

4.5. Responsabilidades

A la vista de las diferentes actividades que, de forma genérica, intervendrán en el análisis de riesgos de ciberseguridad en SCI, y posterior gestión de riesgos, será oportuno señalar que diferentes actores o roles tendrán una participación concreta en cada una de ellas. Así se refleja en la tabla que se muestra a continuación.

	Propietario	Usuario	Mantenimiento	Experto en ciberseguridad	Otras entidades de referencia
Establecer alcance	●			●	●
Identificación y valoración de activos	●	●	●	●	●
Identificación de vulnerabilidades	●	●	●	●	●
Identificación de amenazas	●	●	●	●	●
Análisis de impacto	●			●	●
Evaluación de escenarios				●	●
Tratamiento del riesgo	●			●	
Aceptación del riesgo residual	●				
Supervisión y monitorización de riesgos			●	●	

Figura 4: Responsabilidades en el marco de las actividades genéricas del análisis y gestión de riesgos de ciberseguridad para SCI

Propietario: Rol responsable del servicio y/o infraestructura objeto del análisis de riesgos.
Usuario: Rol destinatario del servicio y/o infraestructura, en muchos casos corresponderá con el operador.
Mantenimiento: Rol que se encarga de supervisar y mantener el servicio y/o infraestructura.
Experto en Ciberseguridad: Es el rol especialista en ciberseguridad que dará soporte en la interpretación de las amenazas, vulnerabilidades y criterios de valoración CID.
Otras entidades de referencia: Corresponde a entidades relacionadas con la operación de la infraestructura, fabricantes de tecnología o integradores, así como entidades reconocidas por su conocimiento y experiencia.

5. PASOS ESENCIALES DEL ANÁLISIS DE RIESGOS

Al objeto de facilitar la ejecución del análisis de los riesgos, se describen, a continuación, los pasos propuestos para este modelo:

5.1. Paso 1: Identificación de Servicios Esenciales

Este modelo de análisis de riesgos está diseñado para contemplar dentro de su alcance todos los activos relacionados con la automatización y control industrial que den soporte a servicios esenciales gestionados por un operador, en el caso de ser infraestructuras críticas, aquellos servicios necesarios para garantizar funciones sociales básicas como la sanidad, la seguridad o el bienestar social y económico de los ciudadanos, a través de un conjunto de infraestructuras estratégicas del operador ubicadas en el territorio nacional. Y ello sin obviar sus posibles interdependencias con servicios prestados por otros operadores, o terceros, dentro o fuera del país.

Resolución de 8 de septiembre de 2015

Anexo I. Guía Contenidos Mínimos PSO

Apartado 1.1. Base legal

En dicho apartado se define: *El normal funcionamiento de los servicios esenciales que se prestan a la ciudadanía descansa sobre una serie de infraestructuras de gestión tanto pública como privada, cuyo funcionamiento es indispensable y no permite soluciones alternativas: las denominadas infraestructuras críticas.*

Resolución de 8 de septiembre de 2015

Anexo II. Guía Contenidos Mínimos PPE

Apartado 3.1. Datos generales de la infraestructura crítica

El operador crítico deberá incluir los siguientes datos e información sobre la infraestructura a proteger:

- *Generales, relativos a la denominación y tipo de instalación, propiedad y gestión de la misma.*
- *Sobre localización física y estructura (localización, planos generales, fotografías, componentes, etc.)*
- *Sobre los sistemas TIC que gestionan la infraestructura crítica y su arquitectura.*
- *Datos estratégicos:*
  - *Descripción del servicio esencial que proporciona y el ámbito geográfico o poblacional del mismo.*
  - *Relación con otras posibles infraestructuras necesarias para la prestación de ese servicio esencial.*
  - *Descripción de sus funciones y de su relación con los servicios esenciales soportados.*

El Modelo incluye la **plantilla I** "**ENSI_ARLI-CIB_02_Plantilla-Alcance**" que proporcionará la descripción del operador crítico, sus servicios esenciales, y los medios materiales y recursos, que determinarán el alcance del análisis de riesgos.

La **plantilla I** "**ENSI_ARLI-CIB_02_Plantilla-Alcance**" es un documento de alto nivel que permite la identificación de los servicios esenciales y áreas de actividad que son o pueden ser esenciales para los ciudadanos, así como, los medios de los que se dispone para la prestación del servicio y su ubicación. Se emplearán, para ello, los siguientes campos, en la **pestaña** "**Alcance**" que habrán de ser cumplimentados:

Nombre del operador: Este campo deberá identificar el nombre del operador de los servicios esenciales objeto del Análisis de riesgos.

Razón Social y Matriz: Este campo deberá identificar la razón social o nombre legal de la empresa propietaria de los servicios esenciales, y su matriz o sede social.

Desglose de estructura societaria: Este campo deberá contener la estructura societaria de la empresa propietaria de los servicios esenciales, así como su composición accionarial y los porcentajes de participación de cada uno de los accionistas.

Sedes sociales y ubicación geográfica: Este campo identificará las ubicaciones físicas que corresponderán al alcance del análisis de riesgos.

Actividades desarrolladas: Se identificará en este campo las actividades desarrolladas por el operador y los recursos que contribuyen a realizar dichas actividades.

Sector/es y Subsectores a los que pertenece: Se identificará los sectores y subsectores a los que pertenece el operador crítico en función de la/s actividad/es desarrollada/s.

Servicios esenciales: Este campo identificará los servicio/s que por sus características son considerado/s esencial/es.

Resolución de 8 de septiembre de 2015

Anexo I. Guía Contenidos Mínimos PSO

Apartado 3.4. Interdependencias

En relación con el concepto de interdependencias recogido en el artículo 2. j) de la Ley, pueden existir efectos y repercusiones que afecten los servicios esenciales y las infraestructuras críticas propias y/o de otros operadores, tanto dentro del mismo sector como en otros sectores diferentes. Estas interdependencias deberán ser en todo caso consideradas en el análisis de riesgos que realicen los operadores en el marco global de su organización.
El operador crítico deberá hacer referencia a las interdependencias que identifique, explicando en líneas generales el motivo que origina dichas dependencias:

- *Entre sus propias instalaciones o servicios.*
- *Con operadores del mismo sector.*

- *Con operadores de distintos sectores.*
- *Con operadores de otros países, del mismo sector o no.*
- *Con sus proveedores de servicio dentro de la cadena de suministros.*
- *Con los proveedores de servicios TIC contratados, tales como: proveedor(es) de telecomunicaciones, Centros de Proceso de Datos, servicios de seguridad (Centro de Operaciones de Seguridad, CERT privado, etcétera) y cualesquiera otros que se considere, especificando para cada uno de ellos el nombre del proveedor, los servicios contratados, acuerdos de nivel de servicio (SLA) y cumplimiento del servicio provisto con la política general de seguridad del operador.*

Resolución de 8 de septiembre de 2015

Anexo II. Guía Contenidos Mínimos PPE

Apartado 3.3. Interdependencias

En relación con el concepto de interdependencias recogido en el artículo 2. j) de la Ley, pueden existir efectos y repercusiones que afecten los servicios esenciales y las infraestructuras críticas propias y/o de otros operadores, tanto dentro del mismo sector como en ámbitos diferentes. Estas interdependencias deberán ser en todo caso consideradas en el análisis de riesgos que realicen los operadores para la infraestructura crítica de que se trate, en el marco del PPE.
El operador crítico deberá hacer referencia dentro de sus diferentes PPE a las interdependencias que, en su caso, identifique, explicando brevemente el motivo que las origina:

- *Con otras infraestructuras críticas del propio operador.*
- *Con otras infraestructuras estratégicas del propio operador que soportan el servicio esencial.*
- *Entre sus propias instalaciones o servicios.*
- *Con sus proveedores dentro de la cadena de suministro.*
- *Con los proveedores de servicios TIC contratados para esa infraestructura, tales como: proveedor(es) de telecomunicaciones, Centros de Proceso de Datos, servicios de seguridad (Centro de Operaciones de Seguridad, CERT privado, etcétera) y cualesquiera otros que se considere, especificando para cada uno de ellos el nombre del proveedor, los servicios contratados, acuerdos de nivel de servicio (SLA) y cumplimiento del servicio provisto con la política general de seguridad del operador.*
- *Con los proveedores de servicios de seguridad física, indicando los servicios prestados y el personal y medios empleados.*

Resolución de 8 de septiembre de 2015

Anexo I. Guía Contenidos Mínimos PSO

Apartado 3.2. Mantenimiento del inventario de servicios esenciales

Periódicamente, al menos bienalmente, el operador crítico deberá revisar la relación de servicios esenciales que figuran en su PSO, como consecuencia de la evolución normal que cualquier empresa experimenta respecto a los servicios que ofrece.
Así, en este mantenimiento deberá incorporar aquel/-los cambio/-s que se produzcan:

• Por causas endógenas (por ejemplo, ajuste de cartera de servicios, fusiones, adquisiciones o ventas de activos, cambios técnicos, modificación de infraestructuras, cambio de instalaciones, etc.).
• Como consecuencia de la adecuación a los períodos establecidos en el Plan conforme al punto 1.4 de esta guía.

Y los siguientes campos, en la **pestaña** "**MEDIOS MATERIALES Y UBICACIONES**" que habrán de ser cumplimentados, empezando por la información correspondiente a medios materiales, personales y recursos:

Objetivo y Misión: Este campo identificará el objetivo del servicio y su misión.

Propietario: Identificará el rol responsable del servicio y la organización a la que pertenece, si no fuera la misma del operador.

Destinatario del servicio: Este campo identificará a los usuarios del servicio.

Entradas del servicio: Este campo identificará cuales son los elementos de entrada necesarios para poder prestar el servicio.

Actividades del servicio: Este campo deberá identificar los nombres de los procedimientos, registros e instrucciones relativos al servicio y de interés para el objeto del análisis.

Recursos y sistemas: Este campo identificará aquellos sistemas y recursos que pueden ser afectados por el alcance del análisis de riesgos, y que deberán formar parte del mismo para su valoración.

También deberá cumplimentarse la información relativa a Fronteras y Ubicaciones:

Ubicaciones: Este campo identificará las ubicaciones que pueden ser afectadas por el alcance del análisis de riesgos, y que deberán formar parte del mismo para su valoración.

Empresas con las que comparte ubicación geográfica: Este campo identificará los límites del servicio, indicando proveedores de servicios adicionales que comparten ubicación

5.2. Paso 2: Identificación y valoración de activos

El segundo paso en la realización del análisis de los riesgos es la identificación y descripción de cada servicio esencial prestado por el operador a través del conjunto de sus infraestructuras estratégicas ubicadas en el territorio nacional. Así como del inventariado de activos, así como su clasificación y agrupación para facilitar, en la medida de lo posible, la realización del análisis.

Resolución de 8 de septiembre de 2015

Anexo I. Guía Contenidos Mínimos PSO

Apartado 4.2. Tipologías de activos que soportan los servicios esenciales

Se denominan activos los recursos necesarios para que la Organización funcione correctamente y alcance los objetivos propuestos por su Dirección.
Sobre la base de los servicios identificados en el apartado 3.1 anterior, se incluirán en este apartado, para cada servicio esencial, los tipos de activos que los soportan, diferenciando aquéllos que son críticos de los que no lo son.

Cada servicio esencial del alcance estará compuesto por N "Activos" que darán soporte al servicio, y que a su vez cada uno de ellos estará identificado en uno de los niveles de la pirámide de automatización industrial, según se muestra en la *figura 5*.

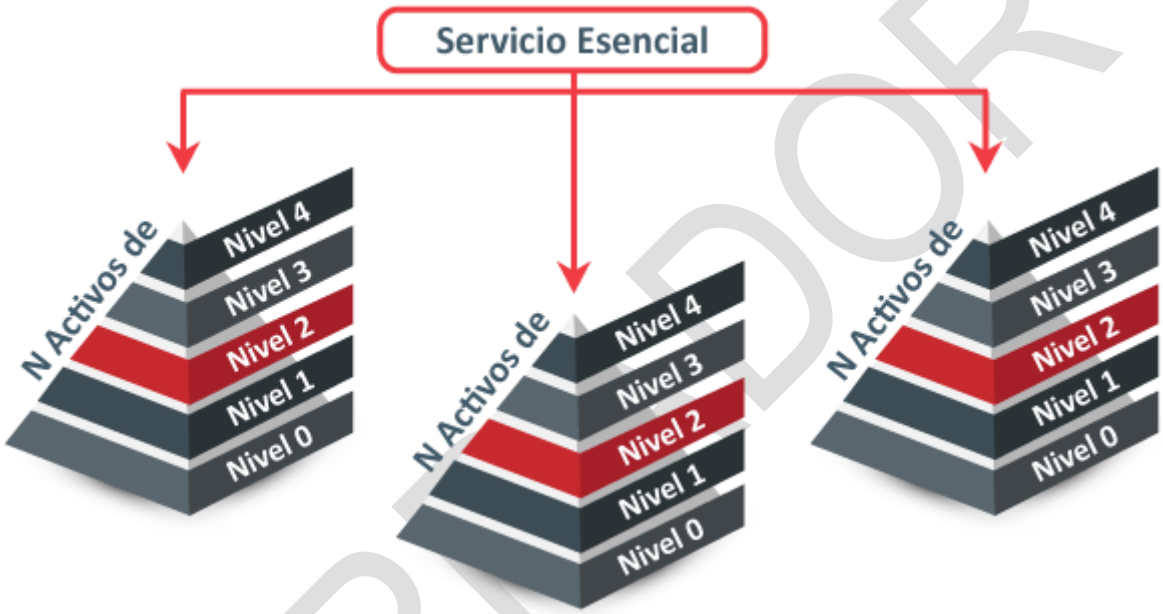


Figura 5: Jerarquía de activos de un servicio esencial automatizado

Así por ejemplo, el "*Servicio Esencial 1*" podría tener quince activos, repartidos entre los niveles 0 y 2 de la pirámide de automatización, de los cuales cinco activos podrían ser de tipo hardware, tres de tipo software, dos de tipo redes de comunicaciones, una de tipo instalaciones físicas, y cuatro de tipo personal.

Todos los activos dentro del alcance deberán ser estudiados, dado que la identificación de sus amenazas, permitirá determinar cómo estas últimas podrían afectar al funcionamiento del servicio esencial al que subyacen, **considerando que son activos críticos aquellos cuya valoración de impacto CID, en cualquiera de sus dimensiones sea de 3 (véase apartado 4.2.3).**

Resolución de 8 de septiembre de 2015

Anexo II. Guía Contenidos Mínimos PPE

Apartado 3.2. Activos/elementos de la infraestructura crítica

Se incluirán en este apartado todos los activos que soportan la infraestructura crítica, diferenciando aquellos que son vitales de los que no lo son. En concreto se detallarán:

• Las instalaciones o componentes de la infraestructura crítica que son necesarios y por lo tanto vitales para la prestación del servicio esencial.
• Los sistemas informáticos (hardware y software) utilizados, con especificación de los fabricantes, modelos y, versiones, etcétera.
• Las redes de comunicaciones que permiten intercambiar datos y que se utilicen para dicha infraestructura crítica:
- *Arquitectura de red, rangos de IP públicas y, dominios.*
- *Esquema(s) de red completo y detallado, de tipo gráfico y con descripción literaria, donde se recojan los flujos de intercambio de información que se realizan en las redes, así como sus perímetros electrónicos.*
- *Descripción de componentes de la red (servidores, terminales, hubs, switches, nodos, routers, firewalls,…) así como su ubicación física.*

• Las personas o grupos de personas que explotan u operan todos los elementos anteriormente citados, indicando y detallando de forma particular si existe algún proceso externalizado a terceros.
• Los proveedores críticos que en general son necesarios para el funcionamiento de dicha infraestructura crítica, y específicamente:
- *De suministro eléctrico.*
- *De comunicaciones (telefonía, internet, etc.).*
- *De tratamiento y almacenamiento de información (CPDs, etc.).*
- *De Ciberseguridad (CERTs privados, SOCs, etc.).*

• Sobre los proveedores nombrados por el operador, se especificarán los distintos Acuerdos de Nivel de Servicios que se tienen contratados y que son considerados esenciales.

[…] La información anterior deberá ser la suficiente para recoger de manera explícita el alcance de la infraestructura a proteger y con el mismo nivel de detalle que se haya establecido dentro del PSO.

5.2.1. Identificación del servicio esencial

En la **Plantilla II "ENSI_ARLI-CIB_03_Plantilla-AARR"** de este modelo se incluye una pestaña "Instrucciones" donde se facilitará un formulario para la identificación de cada servicio esencial y los activos de que soportan dicho servicio, sus amenazas y las medidas necesarias para el tratamiento del riesgo.

A continuación se describen los campos de información que deberán ser indicados en la pestaña "**Identificación de S.E**" para el servicio esencial del alcance:

Nombre del Servicio Esencial: Se identificará el nombre del servicio necesario para el mantenimiento de las funciones sociales básicas, la salud, la seguridad, el bienestar social económico de los ciudadanos.

Descripción del Servicio Esencial: Se describirá el servicio esencial.

Tipología de los activos del servicio esencial: Se identificará de manera general la tipología de los activos e infraestructuras críticas sobre las que descansa el servicio esencial. Las tipologías de activos a considerar serán al menos:

- Instalaciones necesarias para la prestación del servicio esencial.
- Sistemas informáticos (Hardware y software necesarios para dar soporte al servicio)
- Redes de comunicaciones necesarias para la prestación del servicio.
- Personas que administran u operan todos los elementos citados anteriormente.

Ubicación geográfica: Se identificará la ubicación/es en las que se presta el servicio y donde se encuentran los activos que lo soportan:

- Laboratorio interno
- Laboratorio externo
- Oficina interna
- Oficina externa
- Planta industrial local
- Instalación
- CPD Interno
- CPD externo
- Otra ubicación (Especificar)

Empresas con las que comparte ubicación geográfica: Se identificará el nombre de las empresas con las que el operador comparte ubicación geográfica.

Interdependencias: En este campo se deberán incluir las interdependencias entre los servicios e infraestructuras críticas que los soportan, así como los de otros operadores dentro del mismo sector o diferente y que deben ser consideradas en el análisis de riesgos.

5.2.2. Identificación y valoración de activos

La recopilación, identificación y valoración de activos debería realizarse mediante entrevistas en las que participen los propietarios de los activos. La identificación de activos en infraestructuras o procesos productivos puede resultar muy compleja dado el elevado número de activos potenciales que existen. Por ello, es recomendable la clasificación de los distintos dispositivos involucrados atendiendo a su participación en distintos procesos de producción, ubicaciones geográficas y otros factores e intentar mantener un equilibrio entre el detalle con el que se realiza el modelado del servicio esencial y la operatividad del análisis, para ello es imprescindible utilizar categorías y grupos de activos.

Los **grupos de activos** permiten disminuir la complejidad del análisis mediante la agrupación de los activos que están dentro de la misma instalación sujetos a las mismas condiciones de operación y funcionamiento; y por tanto a las mismas amenazas. En este modelo de análisis de riesgos se ha establecido como niveles de agrupación de activos, la división en niveles de automatización industrial de la arquitectura propuesta por ISA-99/IEC 62443.

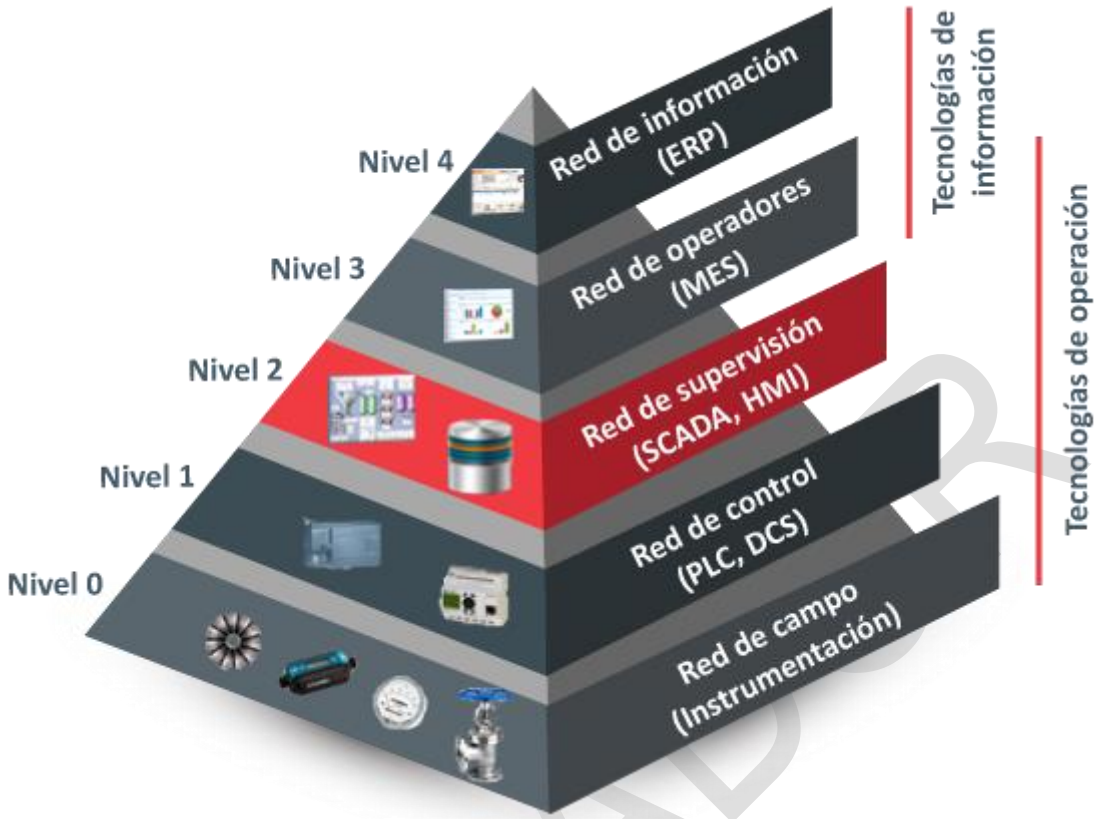


Figura 6. Jerarquía de niveles de automatización industrial, según la norma ISA 99/IEC 62443

De tal modo que se tendrán cinco grupos de activos:

- **Nivel 4**: Nivel de sistemas de información, donde se encuentran sistemas ERP, …
- **Nivel 3**: Nivel de operación, donde se encuentran sistemas MES, MOM,…
- **Nivel 2**: Nivel de supervisión, donde se encuentran sistemas SCADA, HMI…
- **Nivel 1**: Nivel de control básico, donde se encuentran los controladores PLC, DCS, …
- **Nivel 0**: Nivel de instrumentación, donde se encuentran sensores, actuadores, analizadores…

Resolución de 8 de septiembre de 2015

Anexo I. Guía Contenidos Mínimos PSO

Apartado 4.2. Tipologías de activos que soportan los servicios esenciales

Las tipologías de activos a considerar serán, al menos:

- *Las instalaciones necesarias para la prestación del servicio esencial.*
- *Los sistemas informáticos necesarios para dar soporte a los servicios esenciales (hardware y software).*
- *Las redes de comunicaciones necesarias para la prestación del servicio esencial.*
- *Las personas que explotan u operan todos los elementos anteriormente citados.*

Las **categorías (tipologías) de activos** servirán de guía a la hora de determinar las amenazas y vulnerabilidades a las que están expuestos los activos mediante el uso de catálogos que clasifican amenazas y vulnerabilidades para cada categoría (tipo) de activo.

- **Servicios Prestados**: Los servicios necesario para la prestación del servicio esencial.
- **Personal**: Las personas que explotan u operan el servicio esencial.
- ***Hardware***: Los sistemas informáticos físicos necesarios para dar soporte a los servicios esenciales.
- ***Software***: Los sistemas informáticos lógicos necesarios para dar soporte a los servicios esenciales.
- **Redes de comunicaciones**: Las redes de comunicaciones, internas o externas, necesarias para la prestación del servicio esencial.
- **Instalaciones físicas**: Las instalaciones necesarias para la prestación del servicio esencial.

Un servicio esencial estará formado por uno o varios activos que estarán implicados en el proceso del servicio y que deberán ser contemplados en el análisis. Estos activos pertenecerán a las diferentes tipologías enumeradas en el párrafo anterior.

Resolución de 8 de septiembre de 2015

Anexo I. Guía Contenidos Mínimos PSO

Apartado 4.2. Tipologías de activos que soportan los servicios esenciales

El objeto de esta sección es la identificación genérica de tipologías de activos asociadas a los servicios esenciales prestados por dicho operador, y sobre los que se focalizará el análisis de riesgos que efectúe el operador. El nivel de detalle será aquel que permita una comprensión del funcionamiento de los servicios, así como las interrelaciones entre activos y servicios.

Los activos no serán necesariamente espacios físicos concretos, pudiendo por ejemplo considerarse como activos sistemas distribuidos, tales como una red de datos.

La información que deberá ser reflejada para cada uno de los campos en la pestaña "**Valoración de Activos**" de la **Plantilla II "ENSI_ARLI-CIB_03_Plantilla-AARR"** es la siguiente:

Nombre: Este campo deberá ser completado con el nombre del activo incluido en el alcance del ARC-SCI.

Tipo de activo: Este campo permitirá seleccionar el tipo de activo al que pertenece de la lista presentada de tipologías.

Subtipo: Este campo identificará el subtipo de la tipología de activo, el cual deberá ser seleccionado de la lista presentada. Todos los tipos de activo tienen subtipo, excepto el tipo servicio prestado.

C: Este campo se refiere a la valoración de la criticidad del activo en cuanto a su "**Confidencialidad**" y podrá seleccionarse uno de los siguientes valores: 1- Bajo, 2-

Medio, 3-Alto. Es importante que su valoración se base en los criterios de valoración CID establecidos en la tabla inferior de la figura 7.

I: Este campo se refiere a la valoración de la criticidad del activo en cuanto a su "**Integridad**" y podrá seleccionarse uno de los siguientes valores: 1- Bajo, 2-Medio, 3-Alto. Es importante que su valoración se base en los criterios de valoración CID establecidos en la tabla inferior de la figura 7.

D: Este campo se refiere a la valoración de la criticidad del activo en cuanto a su "**Disponibilidad**" y podrá seleccionarse uno de los siguientes valores: 1- Bajo, 2-Medio, 3-Alto. Es importante que su valoración se base en los criterios de valoración CID establecidos en la tabla inferior de la figura 7.

Resolución de 8 de septiembre de 2015

Anexo II. Guía Contenidos Mínimos PPE

Apartado 4.2. Medidas de seguridad integral existentes

El operador deberá describir las medidas de seguridad integral (medidas de protección de las instalaciones, equipos, datos, software de base y aplicativos, personal y documentación) implantadas en la actualidad, con las que se ha contado para la realización del análisis de riesgos. Deberá distinguir entre las medidas de carácter permanente, y aquellas temporales y graduales.

[…] En concreto, el operador deberá describir las medidas específicas de que dispone relativas a:

4.2.1. Organizativas o de gestión
4.2.2. Operacionales o procedimentales
4.2.3. De protección o técnicas.

La valoración de los activos estriba, principalmente, en la estimación de las consecuencias derivadas de la interrupción del servicio.

Criterios horizontales de criticidad

La criticidad, la gravedad y las consecuencias de la perturbación o destrucción de una infraestructura crítica se evaluarán en función de:

1. El número de personas afectadas, valorado en función del número potencial de víctimas mortales o heridos con lesiones graves y las consecuencias para la salud pública.

2. El impacto económico en función de la magnitud de las pérdidas económicas y el deterioro de productos y servicios.

3. El impacto medioambiental, degradación en el lugar y sus alrededores.

4. El impacto público y social, por la incidencia en la confianza de la población en la capacidad de las Administraciones Públicas, el sufrimiento físico y la alteración de la vida cotidiana, incluida la pérdida y el grave deterioro de servicios esenciales.

Los criterios verticales de la valoración de criticidad de los activos estarán basada en la valoración del impacto, es decir, de las consecuencias causadas por incidentes en cada una de las tres dimensiones CID de la seguridad (Confidencialidad, Integridad y Disponibilidad) que pueden afectar a un servicio esencial. La valoración de activos requiere que sus propietarios identifiquen las consecuencias que tendría para el negocio la pérdida de su confidencialidad, integridad o disponibilidad, en el peor caso posible, sin tener en cuenta medidas de seguridad existentes en la organización.

A continuación se incluye una tabla con el criterio de valoración de impacto CID para cada activo del inventario:

Valor	Confidencialidad	Integridad	Disponibilidad
3	La supervivencia del servicio esencial está amenazada por la revelación de información sensible debido a una: A. Coste mayor [X] millones € B. Daño a la imagen grave C. Por delito grave D. Por citación de autoridad nacional	La supervivencia del servicio esencial está amenazada por la modificación o manipulación de la operación o la información debido a: A. Coste mayor de [X] millones € B. Daño a la imagen grave C. Por delito grave D. Por citación por autoridad nacional E. Pérdida de vidas humanas	Si la supervivencia del servicio esencial está amenazada por la indisponibilidad de la operación: A. Coste mayor de [X] millones € B. Daño de imagen grave C. Por delito grave D. Por citación por autoridad nacional E. Pérdida de vidas humanas
2	El servicio está amenazada de un daño grave por la revelación de información sensible ocasionando una: A. Coste mayor de [Y] millones € B. Perdida confianza clientes C. Por delito grave D. Por citación por autoridad local E. Heridos graves	El servicio está amenazada de un daño grave por la modificación o manipulación de información ocasionando: A. Coste mayor de [Y] millones € B. Perdida confianza clientes C. Por delito grave D. Por citación por autoridad local E. Heridos graves	El servicio está amenazado por la indisponibilidad de la operación: A. Coste mayor de [Y] millones € B. Daño de imagen grave C. Por delito menor D. Por citación por autoridad local E. Heridos graves
1	El servicio está amenazada de un daño considerable por la revelación de información sensible ocasionando una: A. Coste menor de [Y] millones € B. Daños pequeños y contenidos	El servicio está amenazada de un daño considerable por la modificación o manipulación de información ocasionando: A. Coste menor de [Y] millones € B. Perdida confianza clientes C. Daños pequeños y contenidos D. Heridos leves	El servicio está amenazado por la indisponibilidad de operación: A. < 1 día en una ubicación B. < 1 hora en múltiples ubicaciones C. Por daños pequeños y contenidos D. Heridos leves

Figura 7. Criterio de valoración del impacto CID

5.3. Paso 3: Identificación y evaluación de escenarios de amenaza

El tercer paso consistirá en la identificación de escenarios de amenaza. La existencia de una vulnerabilidad por sí misma no es dañina, ya que requiere la presencia de una amenaza para que sea explotada. Las vulnerabilidades que no tengan amenazas asociadas no requieren la implantación de medidas o controles, pero deben ser documentadas y monitorizadas para detectar posibles cambios.

El modelo de análisis aquí presentado clasifica las vulnerabilidades, proponiendo, para cada una de aquellas, amenazas capaces de explotar dichas vulnerabilidades. La categorización permite realizar, de manera sencilla, la asociación de grupos de vulnerabilidades a tipos de activos, como aparece en la figura, a continuación.

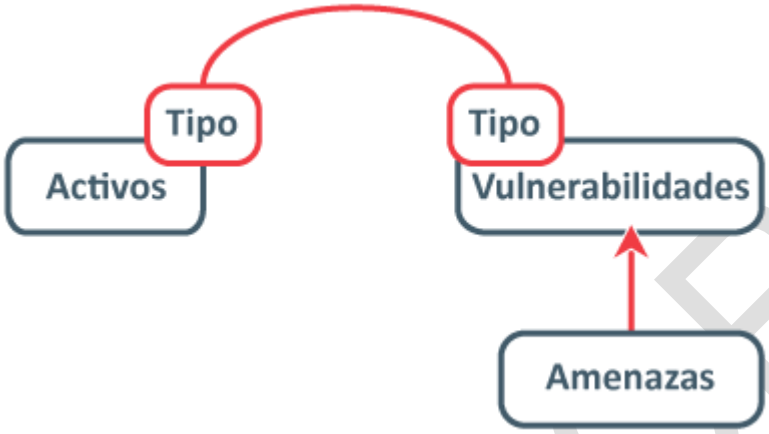


Figura 8. Relación ACTIVOS-VULNERABILIDADES-AMENAZAS

Este paso tiene por objetivo identificar las amenazas, las cuales tienen la capacidad de dañar activos tales como servicios prestados, sistemas informáticos, entre otros, que pueden afectar el correcto funcionamiento del servicio esencial.

Resolución de 8 de septiembre de 2015

Anexo I. Guía Contenidos Mínimos PSO

Apartado 4.3. Identificación y evaluación de amenazas

En el marco de la normativa de protección de infraestructuras críticas y de cara a garantizar la adecuada protección de aquellas infraestructuras que prestan servicios esenciales, el operador crítico deberá tener como referencia el árbol de amenazas proporcionado por el CNPIC, considerando de forma especial aquellas amenazas de origen terrorista o intencionado. El operador deberá indicar expresamente las amenazas que ha considerado para la realización de los análisis de riesgos, plasmando al menos:

• Las intencionadas, de tipo tanto físico como lógico, que puedan afectar al conjunto de sus infraestructuras, las cuales deberán identificarse de forma específica en sus respectivos PPE, en su caso.
• Las procedentes de interdependencias, que puedan afectar directamente a los servicios esenciales, sean estas deliberadas o no.

Resolución de 8 de septiembre de 2015

Anexo II. Guía Contenidos Mínimos PPE

Apartado 4.1. Amenazas consideradas

En el marco de la normativa de protección de infraestructuras críticas, y de cara a garantizar la adecuada protección de las infraestructuras críticas, el operador crítico deberá tener como referencia el árbol de amenazas proporcionado por el CNPIC, considerando de forma especial aquellas amenazas de origen terrorista o intencionado. El operador deberá indicar expresamente las amenazas que ha considerado para la realización de los análisis de riesgos, plasmando al menos:

- *Las amenazas intencionadas, tanto de tipo físico como a la ciberseguridad, que afecten de forma específica a alguno de los activos que soportan la infraestructura crítica.*
- *Las amenazas que puedan afectar directamente a la infraestructura procedente de las interdependencias identificadas, sean éstas deliberadas o no.*
- *Las dirigidas al entorno cercano o elementos interdependientes tanto del ante-perímetro físico como lógico que puedan afectar a la infraestructura.*
- *Las amenazas que afecten a los sistemas de información que den soporte a la operación de la infraestructura crítica y todos los que estén conectados a dichos sistemas sin contar con las adecuadas medidas de segmentación.*
- *Las amenazas que afecten a los sistemas y servicios que soportan la seguridad integral.*

Resolución de 8 de septiembre de 2015

Anexo I. Guía Contenidos Mínimos PSO

Apartado 4. Metodología de análisis de riesgos

[…] Dichas metodologías deberán estar internacionalmente reconocidas, garantizar la continuidad de los servicios proporcionados por dicho operador y contemplar, de una manera global, tanto las amenazas físicas como lógicas existentes contra la totalidad de sus activos críticos. Todo ello, con independencia de las medidas mínimas que se puedan establecer para los Planes de Protección Específicos conforme a lo establecido por el artículo 25.

La identificación de las amenazas y la probabilidad de su materialización requiere del conocimiento experto que deberá ser aportado por los propietarios de los activos, los usuarios, personal implicado en la utilización o mantenimiento de los activos, expertos en ciberseguridad y profesionales o entidades capacitadas para aportar opiniones bien formadas sobre la materia.

Este paso del modelo de análisis de riesgo consistirá en la valoración de los escenarios de alto riesgo que han sido definidos en la “Plantilla II. Análisis de riesgos”. Al ser el riesgo resultado de la interacción de factores de vulnerabilidad con factores de amenaza -esto es, dinámico y cambiante en la medida en que también lo son los elementos que lo producen-, ha de pensarse que los referidos escenarios podrán variar y, consecuentemente, habrán de ser actualizados.

La probabilidad de que se materialice un escenario de alto riesgo se obtendrá tras evaluar la exposición de los activos y de la capacidad de respuesta del operador para resistir y recuperarse del evento de alto riesgo.

Los escenarios de alto riesgo se han definido a partir del análisis de cada tipo de amenaza (evento que podría desencadenar un incidente) y de cuál puede ser su potencial impacto para cada activo que soporta el servicio esencial, teniendo en cuenta los posibles efectos y la capacidad actual para resistir y recuperarse de las pérdidas.

Existen varios aspectos fundamentales que se han tenido en consideración para establecer los escenarios de alto riesgo:

- Se han definido un número de escenarios de riesgo que permitan reflejar la realidad y complejidad de los sistemas o aplicaciones de cada servicio esencial.
- Se han definido escenarios realistas y adecuados para permitir tomar decisiones.
- Facilita la revisión periódica para contemplar y reflejar los cambios que se puedan haber producido.

Los campos de la pestaña "**Amenazas**" permitirán identificar cada uno de los elementos de los escenarios de alto riesgo que han sido definidos en la ***Plantilla II "ENSI_ARLI-CIB_03_Plantilla-AARR"*** para los tipos de activos valorados, incluyéndose los siguientes campos:

Tipo de Activo: Identifica el tipo de activo afectado por el evento.

Tipo Amenaza: Identifica el tipo de amenaza principal que podría dañar los activos afectados por el evento. Los tipos de amenazas posibles son:

- Acciones no autorizadas
- Compromiso de funciones
- Daño físico
- Fallo de servicio de soporte
- Fallo técnico
- Información

Tipo de evento: Es la clasificación de los escenarios de riesgo en función del área donde podría materializarse el incidente que desencadena el evento. Se han identificado 9 categorías que son:

- Diseño y Arquitectura
- Infraestructura (Software y hardware)
- Operación del Personal TI y TO
- Dirección de la organización
- Cadena de suministro
- Cumplimiento normativo
- Medioambiente y Seguridad Industrial
- Ciberataques y Malware
- Geopolítico

Evento: Describe la situación del evento del escenario de riesgo.

Nivel de madurez de respuesta: Es la capacidad actual de resistir y recuperarse frente al evento, es decir, las medidas que se han adoptado actualmente para proteger los activos.

Probabilidad: Es el valor (3,2,1) de ocurrencia del evento en función de los antecedentes de ocurrencia del evento, duración del evento y la capacidad de respuesta del operador al evento.

Criticidad CID: Corresponde al grado de impacto que tendrían los activos afectados si se materializara el evento del escenario de riesgo. Este impacto corresponde al valor de las dimensiones afectadas (Disponibilidad, Integridad y/o Confidencialidad) de la seguridad que se obtiene de la valoración CID de los aspectos de protección.

Riesgo potencial del evento: Es un valor que se calculará automáticamente y que corresponde al producto del valor de impacto por el valor de probabilidad de ocurrencia del evento del escenario.

Riesgo real del evento: Es un valor que corresponde al producto del valor de impacto por el valor de probabilidad de ocurrencia del evento del escenario, teniendo en cuenta el nivel de madurez de respuesta.

El Modelo de Análisis de Riesgos basa su evaluación de probabilidad de ocurrencia de un escenario de alto riesgo en criterios de valoración de tres condiciones; antecedentes de ocurrencia, duración y capacidad de respuesta, tal y como se indica en la siguiente tabla:

VALOR	CONDICIÓN
3	La amenaza se considera como posible que suceda o se materialice y además con probabilidad **ALTA** de que explote la vulnerabilidad dentro del alcance por la falta de capacidad de respuesta: A. Ha ocurrido ya anteriormente en la organización. B. La duración del evento será larga (Días). C. No existen condiciones de respuesta internas o externas que eviten el desastre, accidente, incidente o ataque.
2	La amenaza se considera como posible que suceda o se materialice y además con probabilidad **MEDIA** de que explote la vulnerabilidad dentro del alcance por la capacidad de respuesta: A. Ha ocurrido anteriormente en el sector. B. La duración del evento será media (Horas). C. Existen medidas suficientes que eviten el desastre, accidente, incidente o ataque, pero no han sido probadas.
1	La amenaza se considera como posible que suceda o se materialice y además con probabilidad **BAJA** de que explote la vulnerabilidad dentro del alcance por la capacidad de respuesta: A. Ha ocurrido anteriormente en algún operador de otro sector. B. La duración del evento será muy corta (Minutos). C. Existen medidas suficientes que eviten el desastre, accidente, incidente o ataque, y las medidas han sido probadas.

Figura 9. Criterios de valoración de la probabilidad

El riesgo es un valor que combina el impacto (Consecuencia) que producirá el deterioro o pérdida de un activo (o grupo de activos) junto con la probabilidad de que una vulnerabilidad existente en el activo sea explotada por una amenaza.

Resolución de 8 de septiembre de 2015

Anexo I. Guía Contenidos Mínimos PSO

Apartado 4.4. Valoración y gestión de riesgos

Los PSO recogerán la estrategia de gestión de riesgos implementada por el operador en cuanto a:

• Criterios utilizados para la valoración de las categorías de clasificación de los riesgos.

Resolución de 8 de septiembre de 2015

Anexo II. Guía Contenidos Mínimos PPE

Apartado 1.3. Finalidad y contenido del PPE

Además de un índice referenciado a los contenidos del Plan, los PPE deberán contener, al menos, la siguiente información específica sobre la infraestructura a proteger:

• […] Resultado del análisis de riesgos.

Apartado 4. Resultados del análisis de riesgos

El operador crítico deberá reflejar en su PPE los resultados del análisis de riesgos integral realizado sobre la infraestructura crítica.

El cálculo del riesgo en este modelo de análisis de riesgo corresponderá a la siguiente formula:

Riesgo = Impacto (Consecuencias) X Probabilidad (Amenazas/Vulnerabilidades, Capacidad)

	Criticidad/Impacto (Consecuencias)		
Probabilidad	**3**	**2**	**1**
3	**9 (Riesgo Alto)**	**6 (Riesgo Alto)**	**3 (Riesgo Medio)**
2	**6 (Riesgo Alto)**	**4 (Riesgo medio)**	**2 (Riesgo Bajo)**
1	**3 (Riesgo medio)**	**2 (Riesgo Bajo)**	**1 (Riesgo Bajo)**

Figura 10. Tabla de cálculo del riesgo

5.4. Paso 4: Identificación de medidas de seguridad

En este punto, los responsables de la instalación estarán en disposición de proceder con la gestión concreta (tratamiento) que deseen hacer de los riesgos obtenidos. La ejecución de un determinado tratamiento requerirá la toma, por parte de aquellos, de una decisión previa sobre qué hacer con dichos riesgos - evitarlos, reducirlos, transferirlos o retenerlos-
.

Resolución de 8 de septiembre de 2015

Anexo I. Guía Contenidos Mínimos PSO

Apartado 4.4. Valoración y gestión de riesgos

Los PSO recogerán la estrategia de gestión de riesgos implementada por el operador en cuanto a:

• Metodología de selección de estrategia (reducción, eliminación, transferencia, etc.).
• Plazos para la implantación de medidas, en el caso de elegir una estrategia de minimización del riesgo con indicación, si existe, de mecanismos de priorización de acciones.
• Tratamiento dado a las amenazas de ataques deliberados y, en particular, a aquellas que tengan una baja probabilidad pero un alto impacto debido a las consecuencias por su destrucción o interrupción en la continuidad de los servicios esenciales.
• Mecanismos de seguimiento y actualización periódicos de niveles de riesgo.

Resolución de 8 de septiembre de 2015

Anexo II. Guía Contenidos Mínimos PPE

Apartado 1.3. Finalidad y contenido del PPE

[…] los PPE deberán contener, al menos, la siguiente información específica sobre la infraestructura a proteger:

• Medidas de seguridad integral (tanto las existentes como las que sea necesario implementar) permanentes, temporales y graduales para las diferentes tipologías de activos a proteger y según los distintos niveles de amenaza declarados a nivel nacional de acuerdo con lo establecido por el Plan de Prevención y Protección Antiterrorista y por el Plan Nacional de Protección de Infraestructuras Críticas.
• Plan de acción propuesto (por cada activo evaluado en el análisis de riesgos).
Los PPE deberán estar alineados con las pautas establecidas en la Política General de Seguridad del operador reflejada en el PSO. Así mismo, los análisis de riesgos, vulnerabilidades y amenazas que se lleven a cabo, estarán sujetos a las pautas metodológicas descritas en el PSO.

Como se ha señalado, el modelo descrito en esta guía no pretende sino servir de herramienta que facilite la ejecución de análisis de riesgos y, en ningún caso, suplantar la figura de los responsables de una u otra instalación.

Resolución de 8 de septiembre de 2015

Anexo I. Guía Contenidos Mínimos PSO

Apartado 5. Criterios de aplicación de medidas de seguridad integral

Dentro del ámbito de la seguridad integral, el operador definirá a grandes rasgos los criterios utilizados en su organización para la aplicación y administración de la seguridad. En este sentido, incluirá de forma genérica las medidas de seguridad implantadas en el conjunto de activos y recursos sobre los que se apoyan los servicios esenciales y que se recogerán en sus respectivos PPE, al objeto de hacer frente a las amenazas físicas y lógicas identificadas en los oportunos análisis de riesgos efectuados sobre cada una de las tipologías de sus activos.

Resolución de 8 de septiembre de 2015

Anexo II. Guía Contenidos Mínimos PPE

Apartado 1.1. Base legal

En el PPE, el operador crítico aplicará los siguientes aspectos y criterios incluidos en su PSO, que afecten de manera específica a esa instalación:

• […] Desarrollo de los criterios de aplicación de las diferentes medidas de seguridad que se implanten para hacer frente a las amenazas, tanto físicas como aquellas que afectan a la ciberseguridad, identificadas en relación con cada una de las tipologías de los activos existentes en esa infraestructura.

Por tal motivo, queda recogida, tanto en este apartado, como en la **Plantilla II** que lo acompaña, únicamente, una serie de medidas de aplicación al tratamiento de los riesgos, en particular, en el marco de los escenarios de alto riesgo contemplados en el presente modelo que permitirá identificar la aplicación de las mismas para cada uno de los sistemas/aplicación del alcance.

Resolución de 8 de septiembre de 2015

Anexo II. Guía Contenidos Mínimos PPE

Apartado 5. Plan de acción propuesto (por activo)

En caso de ser pertinente y preverse la disposición de medidas complementarias a las existentes a implementar en los próximos tres años, se deberá describir, como parte integrante del PPE:

• Listado de las medidas complementarias a disponer (físicas o de ciberseguridad).
• Una explicación de la operativa resultante para cada tipo de protección (físico y lógico).

El operador deberá especificar el conjunto detallado de medidas a aplicar para proteger el activo como consecuencia de los resultados obtenidos en el análisis de riesgos. En concreto, deberá incluir la siguiente información:
• Activo de aplicación.
• Acción propuesta, con detalle de su ámbito (alcance) de aplicación.
• Responsables de su implantación, plazos, mecanismos de coordinación y seguimiento, etc.
• Carácter de la medida, permanente, temporal o gradual.

La batería de medidas de tratamiento que ofrece la pestaña “Medidas” de la **Plantilla II** constituye, una colección de buenas prácticas para la mitigación de ciberriesgos de una instalación industrial. Ello es debido a que en su elaboración se han tenido en cuenta algunas de las normas y marcos de referencia de más amplia aceptación en el ámbito de la ciberseguridad -y de la ciberseguridad industrial, en particular-, como las normas ISA/IEC 62443 (anteriormente, ISA 99) o ISO/IEC 27002.

Por tanto, el lector encontrará en la pestaña “**Medidas**” de la **Plantilla II**, una colección de medidas de mitigación del riesgo, para cada una de las cuales se ofrecerá la siguiente información:

Medida: Medidas de seguridad (medidas de protección de las instalaciones, hardware, software, redes de comunicaciones, personal). Deberá distinguir entre las medidas de carácter permanente, y aquellas temporales y graduales. En concreto, el operador deberá describir las medidas concretas relativas a: a) medidas organizativas o de gestión; b) medidas operacionales o procedimentales; y c) medidas de protección, propiamente dichas, o técnicas.

TEn (con ‘n’ tomando valores de 1 a 9): El Modelo ARC-SCI propone nueve categorías de escenarios de alto riesgo:

- Diseño y Arquitectura
- Infraestructura (Software y hardware)
- Operación del Personal TI y TO
- Dirección de la organización
- Cadena de suministro
- Cumplimiento normativo
- Medioambiente y Seguridad Industrial
- Ciberataques y Malware
- Geopolítico

Además se asocia cada una de las medidas de tratamiento con una o más categorías de escenarios (por ejemplo, TE1, TE4, TE5), indicando para cada uno de ellos el/los evento/-s concreto/-s (subescenario/-s) al/a los que la media da cobertura. Por ejemplo, la medida M024-Seguridad del cableado estaría ligada a los escenarios tipo TE3 y TE7; y, dentro de ellos, daría cobertura a los “sub-escenarios” TE305-TE306 y TE701-TE702, respectivamente.

La elección de las medidas para su incorporación a este catálogo de medidas de tratamiento ha seguido un doble criterio:

- por un lado, se han primado aquellas medidas que ofrecen una mayor garantía de disponibilidad de los SCI, según el paradigma CIA (Confidencialidad, Integridad, Disponibilidad) adaptado al contexto industrial; y,
- por otro, se han tenido en cuenta las “Amenazas Principales” que caracterizan a cada uno de los escenarios. Sin excluir ninguna de dichas amenazas, en este caso, se ha procurado identificar medidas que diesen respuesta a las del tipo ‘Acciones no autorizadas’ y ‘Funciones comprometidas’.

Evento: Eventos para los cuales dicha medida reduciría el riesgo.

Activo: Activo afectado por el evento y cuya medida reducirá el riesgo.

Amenaza Principal: Amenaza más significativa del escenario o escenarios a los que la medida da respuesta.

Riesgo real del Evento: Indicará el valor del riesgo real en cada una de las dimensiones de Confidencialidad, Integridad y Disponibilidad.

Tratamiento del Riesgo: Permitirá seleccionar el tratamiento que se dará, especificando el estado de aplicación de cada medida con los siguientes posibles valores:

- **Completa**: Indica que la medida se ha aplicado internamente y está gestionada y auditada.
- **Parcial**: Indica que la medida se ha aplicado internamente y su aplicación es parcial.
- **Externalizada Completa**: Indica que la medida se ha aplicado externamente y está gestionada y auditada.
- **Externalizada Parcial**: Indica que la medida se ha aplicado internamente y su aplicación es parcial.
- **Transferida**: Indica que no se ha aplicado la medida por estar el riesgo transferido a una aseguradora.
- **Planificada**: Indica que la aplicación de la medida está prevista y se ha planificado.
- **No Planificada**: Indica que la aplicación de la medida no está prevista y se asume el riesgo.

Descripción: Es un campo opcional que permitirá especificar más detalle o aclaraciones sobre la aplicación de las medidas.

6. ACRÓNIMOS

ARLI-CIB: Análisis de Riesgos Ligero de Ciberseguridad

ARLI-SI: Análisis de Riesgos Ligero de Seguridad Integral

C4V: Construcción de Capacidades de Ciberseguridad de la Cadena de Valor.

CERT: *Computer Emergency Response Team*.

CERTSI: CERT de Seguridad e Industria.

CIS: *Center for Internet Security.*

CNPIC: Centro Nacional para la Protección de las Infraestructuras Críticas.

ENISA: *European Network and Information Security Agency*.

ENSI: Esquema Nacional de Seguridad Industrial.

IEC: *International Elecrotechnical Commission*.

IMC: Indicadores para la Mejora de la Ciberresiliencia

INCIBE: Instituto Nacional de Ciberseguridad.

ISA: *International Society for Automation*.

NIST: *National Institute of Standards and Technology*.

OC: Operador Crítico.

PES: Plan Estratégico Sectorial.

PIC: Protección de Infraestructuras Críticas.

PPO: Plan de Protección del Operador.

SCI: Sistemas de Control Industrial.

SEE: Secretaría de Estado de Energía.

SES: Secretaría de Estado de Seguridad.

SESIAD: Secretaría de Estado para la Sociedad de la Información y la Agenda Digital.

7. REFERENCIAS

[1] Boletín Oficial del Estado, “Resolución de 8 de septiembre de 2015, de la Secretaría de Estado de Seguridad, por la que se aprueban los nuevos contenidos mínimos de los Planes de Seguridad del Operador y de los Planes de Protección Específicos.,” 18 Septiembre 2015. [Online]. Available: http://www.boe.es/diario_boe/txt.php?id=BOE-A-2015-10060.

[2] Gobierno de España, “ESTRATEGIA DE SEGURIDAD NACIONAL,” 2013. [Online]. Available: http://www.lamoncloa.gob.es/documents/seguridad_1406connavegacionfinalaccesiblebpdf.pdf.

[3] Gobierno de España, “ESTRATEGIA NACIONAL DE CIBERSEGURIDAD,” 2013. [Online]. Available: http://www.dsn.gob.es/es/file/146/download?token=Kl839vHG.

[4] CNPIC, “GUÍA DE BUENAS PRÁCTICAS Plan de Protección Específico (PPE),” [Online]. Available: http://cnpic.es/Biblioteca/Noticias/GUIA_BUENAS_PRACTICAS_PPE.pdf.

[5] CNPIC, “GUÍA DE BUENAS PRÁCTICAS Plan de Seguridad del Operador (PSO),” [Online]. Available: http://cnpic.es/Biblioteca/Noticias/GUIA_DE_BUENAS_PRACTICAS_PSO.pdf.

8. ANEXO: PLANTILLAS

PLANTILLA I: ENSI_ARLI-CIB_02 PLANTILLA ALCANCE

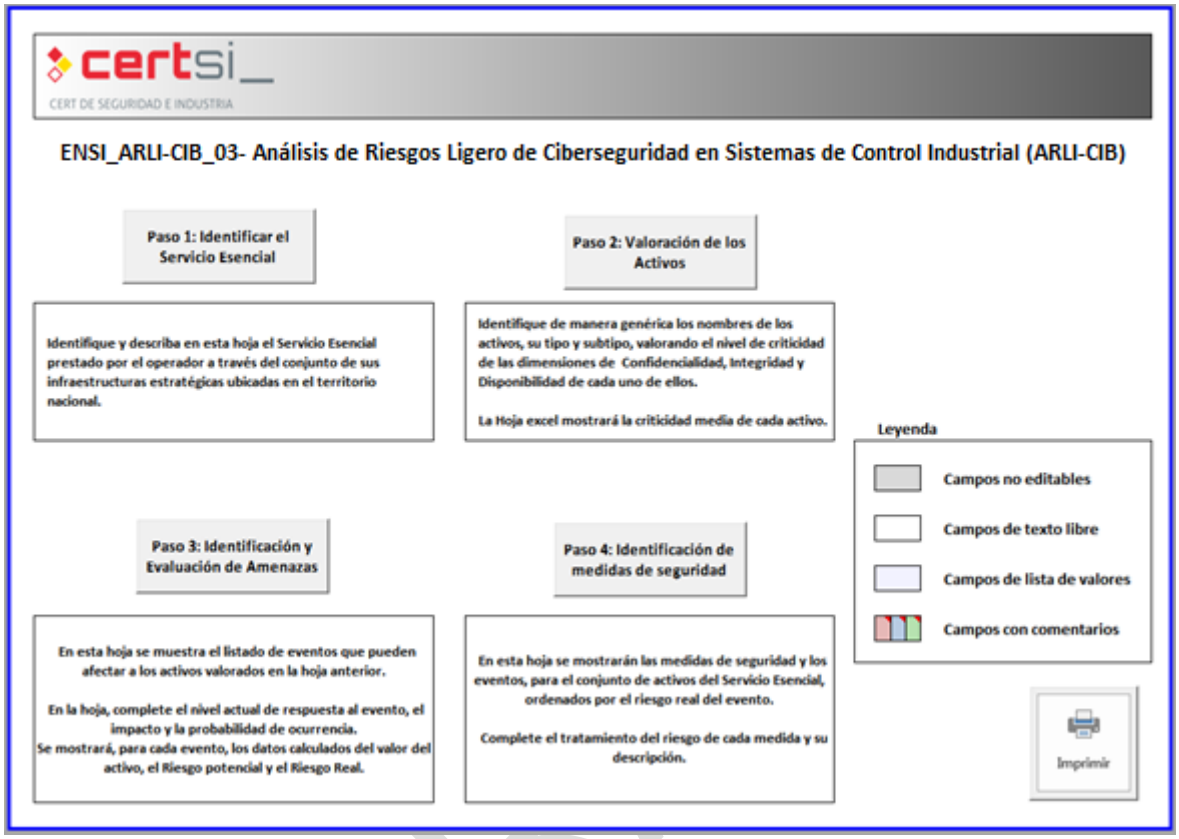
certsi_
CERT DE SEGURIDAD E INDUSTRIA

DESCRIPCIÓN DEL OPERADOR CRÍTICO

Rellene los campos con fondo azul claro para disponer de una breve descripción de la compañía o grupo al que pertenece dicho operador

Nombre del operador
Razón social y matriz
<<Indicar aquí la razón social y matríz del operador>>
Desglose de la estructura societaria, composición accionarial y grado de participación
<<Indicar aquí la estructura societaria del operador>>
Sedes sociales y ubicación geográfica
Las ubicaciones físicas que quedan dentro del alcance del ARC-SCI son: - - -
Actividades desarrolladas
<<Indicar aquí las actividades desarrolladas por el operador>> - - -
Sector/es y subsectores a los que pertenece
Los sectores a los que pertenece en función de la actividad desarrollada son: - - - Los subsectores a los que pertenece en función de la actividad desarrollada son: - - -
Servicios Esenciales
<<Indicar aquí, sin entrar en detalles, un listado de los servicios Esenciales ofrecidas por el operador>> - - - -

PLANTILLA II: ENSI_ARLI-CIB_03 PLANTILLA AARR



GOBIERNO DE ESPAÑA MINISTERIO DEL INTERIOR | GOBIERNO DE ESPAÑA MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL

certsi_ CERT DE SEGURIDAD E INDUSTRIA

certsi_ CERT DE SEGURIDAD E INDUSTRIA

PASO 1: IDENTIFICACIÓN DEL SERVICIO ESENCIAL

Paso 2

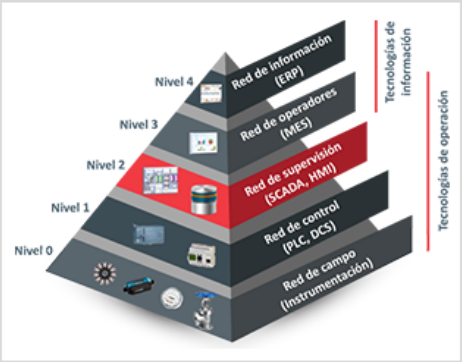
Identifique y describa el Servicio Esencial prestado por el operador a través del conjunto de sus infraestructuras estratégicas ubicadas en el territorio nacional.

Volver

Nombre del Servicio Esencial

Descripción del Servicio Esencial

Tipología de los Activos del Servicio Esencial

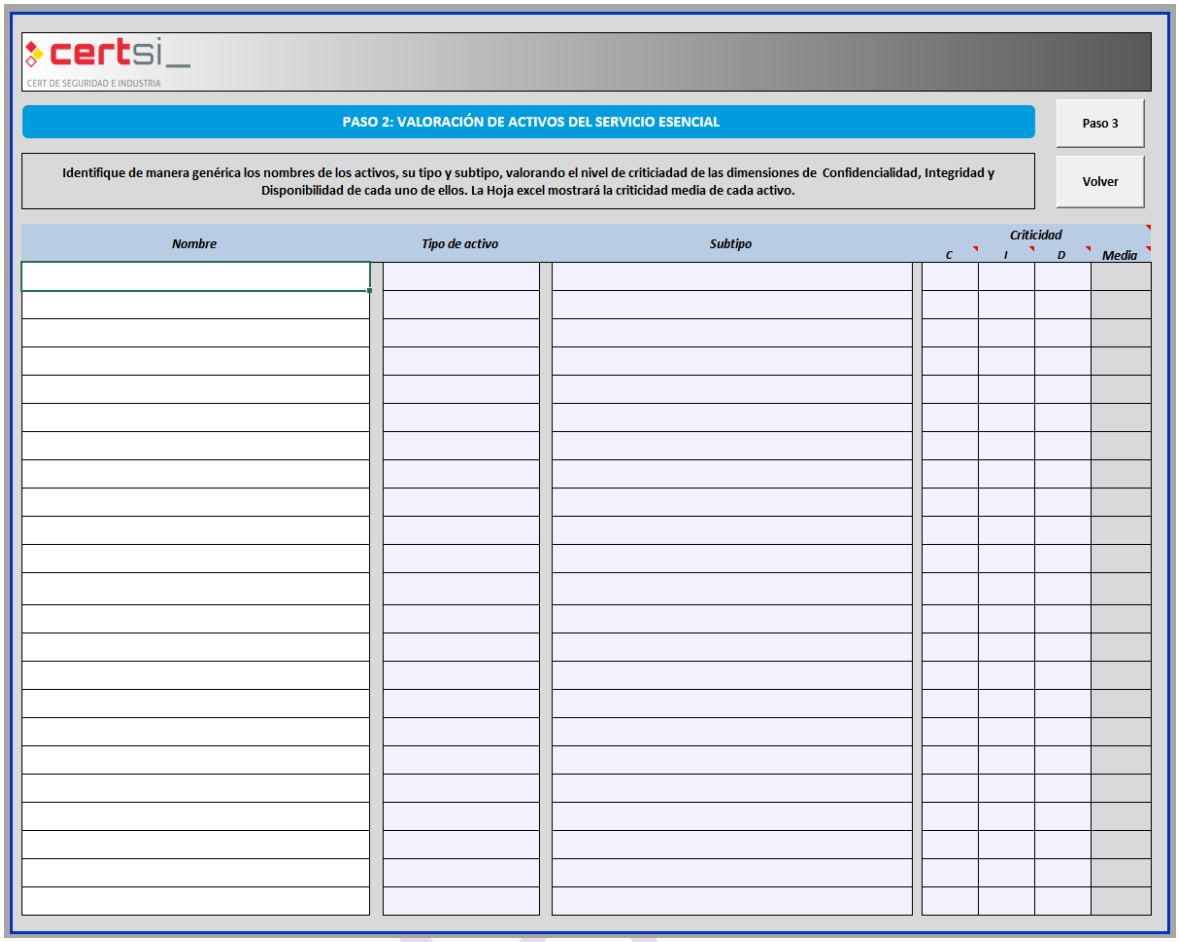


Medios materiales, personales y recursos de los que dispone para la prestación del servicio

Ubicación geográfica

Empresas con las que comparte ubicación geográfica

Interdependencias



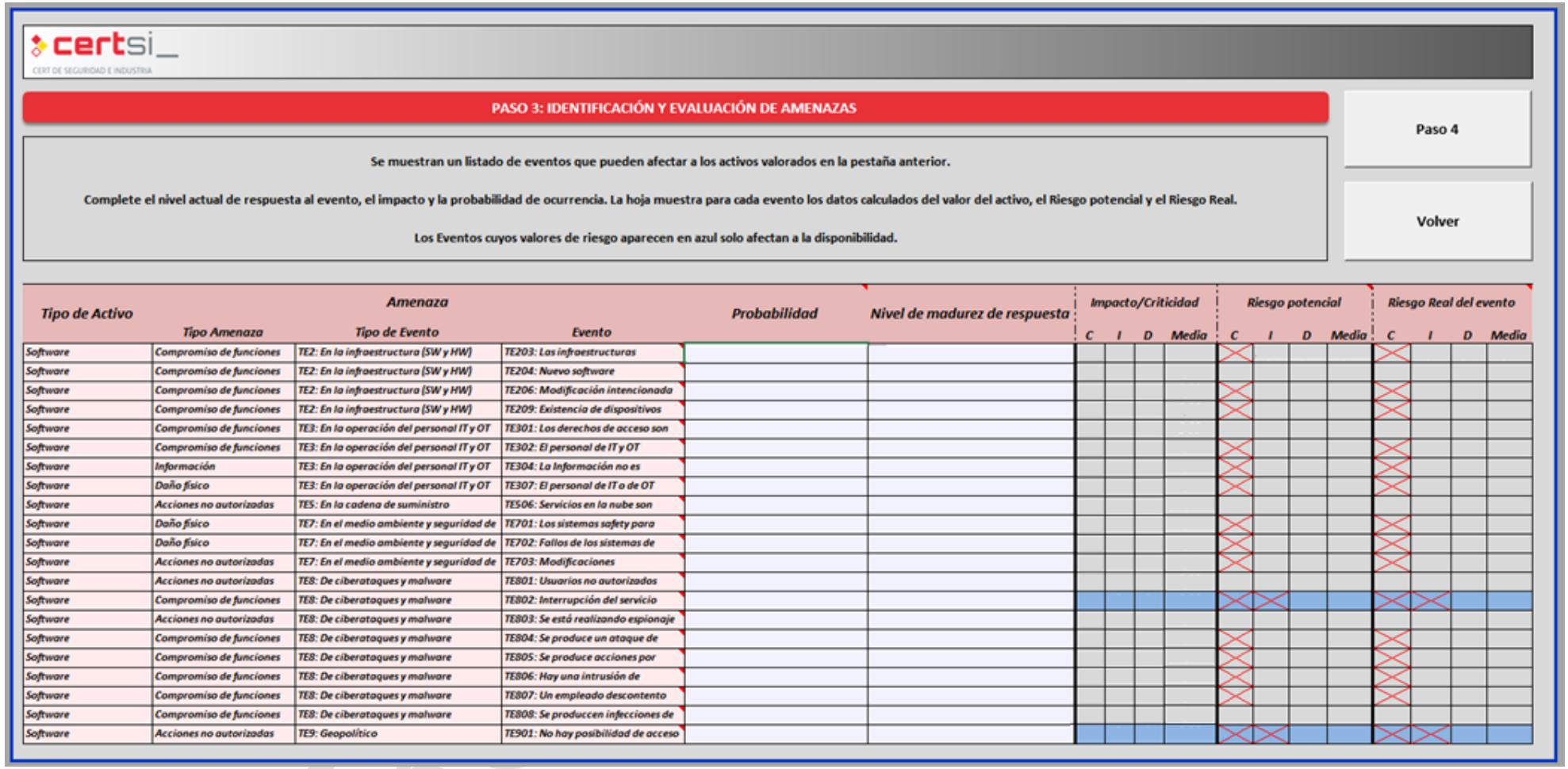
PASO 2: VALORACIÓN DE ACTIVOS DEL SERVICIO ESENCIAL

Paso 3

Volver

Identifique de manera genérica los nombres de los activos, su tipo y subtipo, valorando el nivel de criticidad de las dimensiones de Confidencialidad, Integridad y Disponibilidad de cada uno de ellos. La Hoja excel mostrará la criticidad media de cada activo.

Nombre	Tipo de activo	Subtipo	Criticidad			
			C	I	D	Media



PASO 3: IDENTIFICACIÓN Y EVALUACIÓN DE AMENAZAS

Paso 4

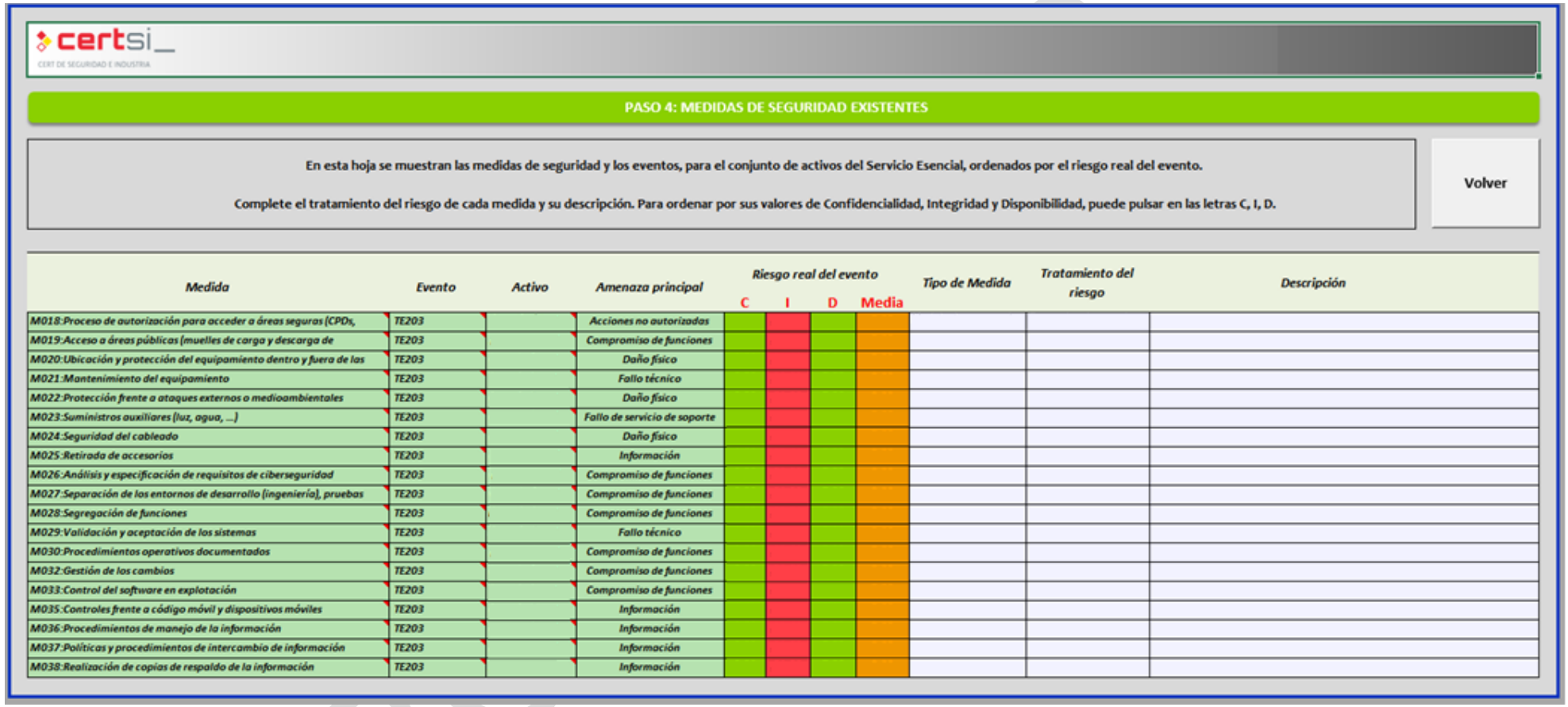
Volver

Se muestran un listado de eventos que pueden afectar a los activos valorados en la pestaña anterior.

Complete el nivel actual de respuesta al evento, el impacto y la probabilidad de ocurrencia. La hoja muestra para cada evento los datos calculados del valor del activo, el Riesgo potencial y el Riesgo Real.

Los Eventos cuyos valores de riesgo aparecen en azul solo afectan a la disponibilidad.

Tipo de Activo	Amenaza			Probabilidad	Nivel de madurez de respuesta	Impacto/Criticidad				Riesgo potencial				Riesgo Real del evento			
	Tipo Amenaza	Tipo de Evento	Evento			C	I	D	Media	C	I	D	Media	C	I	D	Media
Software	Compromiso de funciones	TE2: En la infraestructura (SW y HW)	TE203: Las infraestructuras							X				X			
Software	Compromiso de funciones	TE2: En la infraestructura (SW y HW)	TE204: Nuevo software														
Software	Compromiso de funciones	TE2: En la infraestructura (SW y HW)	TE206: Modificación intencionada							X				X			
Software	Compromiso de funciones	TE2: En la infraestructura (SW y HW)	TE209: Existencia de dispositivos							X				X			
Software	Compromiso de funciones	TE3: En la operación del personal IT y OT	TE301: Los derechos de acceso son														
Software	Compromiso de funciones	TE3: En la operación del personal IT y OT	TE302: El personal de IT y OT							X				X			
Software	Información	TE3: En la operación del personal IT y OT	TE304: La Información no es							X				X			
Software	Daño físico	TE3: En la operación del personal IT y OT	TE307: El personal de IT o de OT							X				X			
Software	Acciones no autorizadas	TE5: En la cadena de suministro	TE506: Servicios en la nube son														
Software	Daño físico	TE7: En el medio ambiente y seguridad de	TE701: Los sistemas safety para							X				X			
Software	Daño físico	TE7: En el medio ambiente y seguridad de	TE702: Fallos de los sistemas de							X				X			
Software	Acciones no autorizadas	TE7: En el medio ambiente y seguridad de	TE703: Modificaciones							X				X			
Software	Acciones no autorizadas	TE8: De ciberataques y malware	TE801: Usuarios no autorizados														
Software	Compromiso de funciones	TE8: De ciberataques y malware	TE802: Interrupción del servicio							X	X			X	X		
Software	Acciones no autorizadas	TE8: De ciberataques y malware	TE803: Se está realizando espionaje														
Software	Compromiso de funciones	TE8: De ciberataques y malware	TE804: Se produce un ataque de							X				X			
Software	Compromiso de funciones	TE8: De ciberataques y malware	TE805: Se produce acciones por							X				X			
Software	Compromiso de funciones	TE8: De ciberataques y malware	TE806: Hay una intrusión de							X				X			
Software	Compromiso de funciones	TE8: De ciberataques y malware	TE807: Un empleado descontento							X				X			
Software	Compromiso de funciones	TE8: De ciberataques y malware	TE808: Se producen infecciones de														
Software	Acciones no autorizadas	TE9: Geopolítico	TE901: No hay posibilidad de acceso							X	X			X	X		



PASO 4: MEDIDAS DE SEGURIDAD EXISTENTES

En esta hoja se muestran las medidas de seguridad y los eventos, para el conjunto de activos del Servicio Esencial, ordenados por el riesgo real del evento.

Complete el tratamiento del riesgo de cada medida y su descripción. Para ordenar por sus valores de Confidencialidad, Integridad y Disponibilidad, puede pulsar en las letras C, I, D.

Volver

Medida	Evento	Activo	Amenaza principal	Riesgo real del evento C	I	D	Media	Tipo de Medida	Tratamiento del riesgo	Descripción
M018:Proceso de autorización para acceder a áreas seguras (CPDs,	TE203		Acciones no autorizadas							
M019:Acceso a áreas públicas (muelles de carga y descarga de	TE203		Compromiso de funciones							
M020:Ubicación y protección del equipamiento dentro y fuera de las	TE203		Daño físico							
M021:Mantenimiento del equipamiento	TE203		Fallo técnico							
M022:Protección frente a ataques externos o medioambientales	TE203		Daño físico							
M023:Suministros auxiliares (luz, agua, ...)	TE203		Fallo de servicio de soporte							
M024:Seguridad del cableado	TE203		Daño físico							
M025:Retirada de accesorios	TE203		Información							
M026:Análisis y especificación de requisitos de ciberseguridad	TE203		Compromiso de funciones							
M027:Separación de los entornos de desarrollo (ingeniería), pruebas	TE203		Compromiso de funciones							
M028:Segregación de funciones	TE203		Compromiso de funciones							
M029:Validación y aceptación de los sistemas	TE203		Fallo técnico							
M030:Procedimientos operativos documentados	TE203		Compromiso de funciones							
M032:Gestión de los cambios	TE203		Compromiso de funciones							
M033:Control del software en explotación	TE203		Compromiso de funciones							
M035:Controles frente a código móvil y dispositivos móviles	TE203		Información							
M036:Procedimientos de manejo de la información	TE203		Información							
M037:Políticas y procedimientos de intercambio de información	TE203		Información							
M038:Realización de copias de respaldo de la información	TE203		Información							

GOBIERNO DE ESPAÑA MINISTERIO DEL INTERIOR

GOBIERNO DE ESPAÑA MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL

certsi_

CERT DE SEGURIDAD E INDUSTRIA