LA GESTIÓN DE LA CIBERSEGURIDAD DE LOS SISTEMAS DE SEGURIDAD FÍSICA

RECOMENDACIONES Y CASOS DE USO

FORO NACIONAL DE CIBERSEGURIDAD

2024

Catálogo de publicaciones de la Administración General del Estado
https://cpage.mpr.gob.es

Edita:

GOBIERNO DE ESPAÑA
MINISTERIO DE LA PRESIDENCIA, JUSTICIA Y RELACIONES CON LAS CORTES

NIPO (edición on-line): 143-24-070-X
Fecha de edición: Diciembre 2024

LA GESTIÓN DE LA CIBERSEGURIDAD DE LOS SISTEMAS DE SEGURIDAD FÍSICA

RECOMENDACIONES Y CASOS DE USO

FORO NACIONAL DE CIBERSEGURIDAD

EL FORO NACIONAL DE CIBERSEGURIDAD

MOTOR DE LA COLABORACIÓN PÚBLICO-PRIVADA

La Estrategia Nacional de Ciberseguridad, aprobada por el Consejo de Seguridad Nacional en abril de 2019, considera la colaboración público-privada como un elemento clave para impulsar la seguridad y confiabilidad del ciberespacio.

La propia Estrategia establece específicamente que dicha colaboración se articule a través del Foro Nacional de Ciberseguridad, que integre a representantes de la sociedad civil, expertos independientes, sector privado, la comunidad académica, asociaciones, organismos sin ánimo de lucro, entre otros, con el fin de para potenciar y crear sinergias público-privadas, particularmente en la generación de conocimiento sobre las oportunidades y amenazas para la seguridad en el ciberespacio.

El Foro Nacional de Ciberseguridad se constituye oficialmente en julio del año 2020, siguiendo el mandato de su creación acordado en el Consejo Nacional de Ciberseguridad.

La composición del Foro responde a la pretensión de contar con la mayor representatividad posible de organismos públicos y de la sociedad civil en el ámbito de la ciberseguridad. Bajo la presidencia del Departamento de Seguridad Nacional y las vicepresidencias del Instituto Nacional de Ciberseguridad (INCIBE) y del Centro Criptológico Nacional (CCN), el Foro está constituido por 18 organizaciones representantes de la sociedad civil, además de otros organismos con competencia en ciberseguridad.

El documento "**La gestión de la ciberseguridad de los sistemas de seguridad física. Recomendaciones y casos de uso**", elaborado por el Foro Nacional de Ciberseguridad, responde a la línea de acción 7 de la Estrategia Nacional de Ciberseguridad: desarrollar una cultura de ciberseguridad.

LA GESTIÓN DE LA CIBERSEGURIDAD DE LOS SISTEMAS DE SEGURIDAD FÍSICA

RECOMENDACIONES Y CASOS DE USO

AGRADECIMIENTOS

Coordinadora institucional:

Departamento de Seguridad Nacional

Coordinadora sociedad civil:

Ana Isabel Borredá Caballero (Presidenta de la Fundación Borredá)

Autores y colaboradores:

Centro Criptológico Nacional*
Raúl Aguilera Sares
Alberto Alonso
Jordi Alonso
Mariano J. Benito Gómez
Alfonso Bilbao *
Enrique Bilbao
Julio Camino
Juan Carlos Gámez Granados
Aitor Goicoechea
Enrique González Herrero *
Francisco Lázaro Anguís
José Ricardo López García *
Gustavo Lozano García
José Antonio Márquez
Julio Pérez Carreño
Javier Rodríguez
Ignacio Rojo
Raúl Siles
Benjamín Suárez
Gonzalo Suárez
Rosa María Tourís López
Alberto Tovar Ropero
Alberto Trigo Viejo

*Coordinadores de los grupos de trabajo

ÍNDICE

1.RESUMEN EJECUTIVO 8

2.NECESIDAD Y OPORTUNIDAD 11

3.SISTEMAS DE SEGURIDAD FÍSICA: ANÁLISIS DEL ÁMBITO 15

4.ANÁLISIS DE CIBERRIESGOS 19

- 4.1- Identificación de activos 19
- 4.2- Identificación de amenazas 21
- 4.3- Valoración del ciberriesgo 23

5.MEDIDAS DE CIBERSEGURIDAD 27

- 5.1 – Propuesta de salvaguardas 27
- 5.2 – Propuesta de correspondencia con los grados de los Sistemas de Seguridad Física 29

6.CASOS DE USO 31

- 6.1 – Ataques contra la red de comunicaciones 32
- 6.2 – Modificación de sensores de detección de intrusión 34
- 6.3 – Ataques a elementos de control de acceso, interfonía y televigilancia 36
- 6.4 – Ataques al subsistema de supervisión y control 38
- 6.5 – Explotación de vulnerabilidades en los protocolos de comunicaciones 40
- 6.6 – Ataques de inyección de comandos en el subsistema de supervisión y control 42
- 6.7 – Escalada de privilegios 44
- 6.8 – Denegación de servicio distribuido 46
- 6.9 – Manipulación de las fuentes de alimentación 48
- 6.10 – *Ransonware* *50*

7.DOCUMENTOS DE REFERENCIA 52

8.GLOSARIO 55

ANEXOS 58

- ANEXO I: CATÁLOGO DE AMENAZAS 59
- ANEXO II: MARCO DE REFERENCIA GENERAL DE MEDIDAS DE CIBERSEGURIDAD 72

RESUMEN EJECUTIVO

Los sistemas de seguridad física, como tantos otros sistemas de distintos sectores económicos, dependen cada vez más de las tecnologías de la información y las comunicaciones. A pesar de que estos sistemas están destinados a proteger los activos de las compañías o administraciones, adolecen en no pocas ocasiones de carencias en relación con las medidas de ciberseguridad o mantienen configuraciones deficitarias que los hacen vulnerables y pueden perder la funcionalidad de seguridad física de los activos a los que protegen. Teniendo en cuenta que estos sistemas están interconectados con el resto de la organización y con terceros, su laxa protección los convierte en una puerta abierta a los activos críticos de una organización.

Las necesidades y carencias mencionadas han motivado la elaboración del presente documento, que persigue dar visibilidad a este problema y orientar a los responsables de los sistemas de seguridad física para decidir qué medidas de seguridad deben implantarse para limitar su exposición ante los riesgos cibernéticos.

Para ello, este documento está enfocado a sistemas de interés para el ámbito físico y el cibernético, esto es, las **centrales receptoras de alarmas y centros de control de seguridad** a los que se conectan los diferentes sistemas y subsistemas de seguridad física. Concretamente, se han tomado en consideración los sistemas de intrusión, control de accesos, videovigilancia, interfonía y megafonía, así como los de supervisión y control, que pueden integrarse en las propias instalaciones que protegen, u ofrecerse desde instalaciones remotas o en la nube.

Teniendo en cuenta estas apreciaciones, se plantea un conjunto de recomendaciones y casos de uso para la gestión de la ciberseguridad de los sistemas de seguridad física. En primer lugar, se facilita la identificación de los activos de seguridad física, estableciendo un listado de elementos que requieren la atención de los responsables de seguridad, ya sean más o menos críticos para la protección de la organización.

Seguidamente, se analiza y describe un catálogo de amenazas relevantes sobre los activos de seguridad física identificados. Esto permitirá al lector visualizar de manera clara y estructurada cómo cada amenaza impacta sobre los diferentes conjuntos de activos, facilitando así la identificación de prioridades en la implementación de medidas de protección y mitigación.

Finalmente, se formula una propuesta general de salvaguardas o medidas de ciberseguridad para proteger y robustecer los sistemas de seguridad física, reducir sus vulnerabilidades, asegurar su operatividad y preservar la información que contienen.

El documento ilustra el resultado obtenido con casos de uso de posibles incidentes de ciberseguridad en los sistemas de seguridad física, aportando, en definitiva, un marco de trabajo para incorporar la ciberseguridad a estos sistemas.

Con todo ello, se espera que el lector sea más sensible a las necesidades de ciberseguridad de los sistemas de seguridad física y que el presente documento le sirva de soporte para alcanzar una mayor protección de su organización a través de dichos sistemas.

NECESIDAD Y OPORTUNIDAD

2.NECESIDAD Y OPORTUNIDAD

La tradicional distancia entre el mundo de la ciberseguridad y el de la seguridad física ha tenido como consecuencia que ésta ni se diseñe, ni se instale, ni se mantenga teniendo en cuenta la ciberseguridad.

No hubo problema mientras las redes de seguridad física vivían separadas del resto de redes o sistemas de la organización; pero ahora que los sistemas analógicos han sido sustituidos por los digitales en las redes de las empresas, es preciso hacer una llamada de atención sobre la necesidad de actuar tanto sobre el parque de dispositivos ya instalado, como sobre los que deban instalarse en el futuro.

Para cuantificar la importancia de esta amenaza, se ha recogido la opinión de responsables de seguridad de empresas pertenecientes a diversas asociaciones, que indica claramente el vacío sobre el que se llama la atención en este documento.

Como resultado, puede afirmarse que existe un número significativo de empresas que consideran insuficientes o totalmente insuficientes sus evaluaciones de riesgos de ciberseguridad para elementos de seguridad física. Igualmente, las opiniones obtenidas demuestran que, aunque muchas organizaciones han comenzado a priorizar la ciberseguridad en sus sistemas de seguridad física, otras aún no le otorgan la relevancia necesaria.

En este contexto, el propósito de este documento es destacar las siguientes cuestiones clave:

1. Los sistemas de seguridad física conectados son una puerta de acceso a la red corporativa de una compañía si no están protegidos, de manera que su vulnerabilidad pone en riesgo tanto la información de la organización –incluida la más crítica– como la propia continuidad del negocio. Un ciberataque a estos sistemas podría desde paralizar las operaciones hasta destruir o afectar a activos digitales, pasando por el robo de información, sabotaje u otras acciones perjudiciales.
2. Es necesario establecer medidas de ciberseguridad técnicas y organizativas para garantizar el correcto funcionamiento de los dispositivos de seguridad física conectados en su función de proteger de amenazas físicas los activos e infraestructuras.
3. La seguridad de la información tiene un componente físico que no puede dejar de tomarse en consideración porque las organizaciones procesan su información en soportes físicos, incluyendo servidores y otros sistemas. Una seguridad física adecuada protege estos activos contra robos, daños y accesos no autorizados, garantizando la confidencialidad, integridad y disponibilidad de los datos.
4. La normativa de seguridad privada, exhaustiva en las características exigidas a los dispositivos de seguridad física, no contempla los requisitos de ciberseguridad exigibles a estos sistemas.
5. El control físico desempeña un papel esencial en la prevención de intrusiones o accesos no autorizados a áreas críticas. Además de la atención a las amenazas cibernéticas, es igualmente vital abordar la posibilidad de intrusiones físicas para evitar daños directos a equipos o infraestructuras.
6. La complementariedad entre medidas de ciberseguridad y de seguridad física permite afrontar amenazas multifacéticas con una mayor probabilidad de éxito.

En definitiva, es necesario fomentar la cultura de ciberseguridad en el sector de la seguridad física (fabricantes, instaladores, mantenedores y prestadores de servicios de seguridad) así como concienciar:

- A la administración para que impulse las acciones necesarias en el ámbito regulatorio.

- A la industria para que ofrezca soluciones con la ciberseguridad por diseño.
- A los directores de seguridad y a los responsables de ciberseguridad para que tengan en cuenta estos riesgos y actuando conjuntamente pongan los medios necesarios para anularlos o mitigarlos.

Para la creación de un escudo de ciberseguridad 360º que proteja los activos de las organizaciones es imprescindible que todas las partes trabajen de forma coordinada. En este aspecto, es importante señalar que la cultura de la ciberseguridad debe permear desde la propia dirección de las empresas. Solo así se podrá impulsar la acción de los responsables de todas las áreas de seguridad encargadas de aplicar las políticas definidas por la dirección.

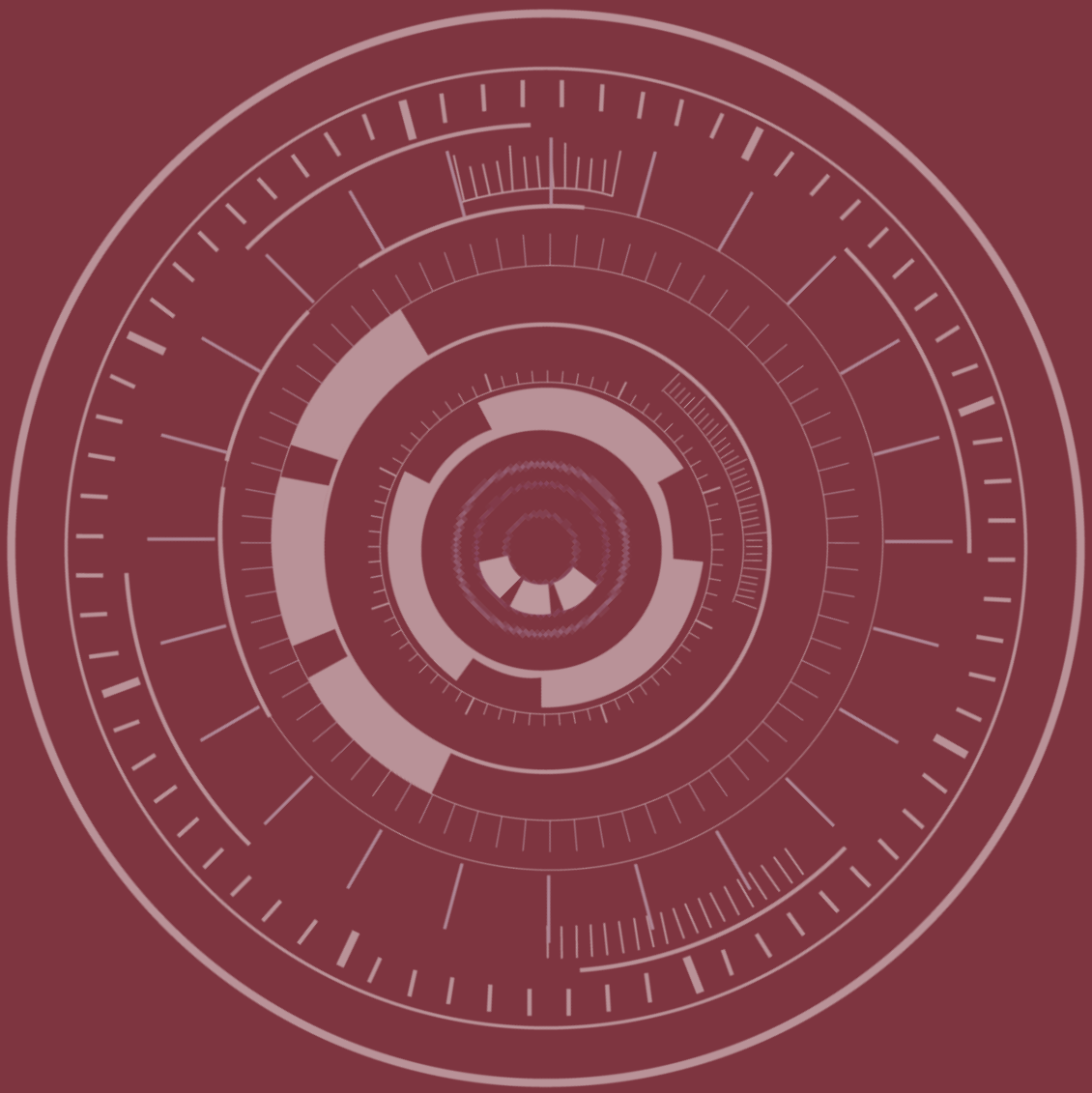
Además, es esencial contar con el apoyo tanto del personal interno como del externo, en el marco de un modelo de gobenanza de la seguridad implantado al mas alto nivel de la organización. En esta línea, la directiva conocida como NIS2[1], relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, establece que los órganos de dirección de las empresas bajo su ámbito de aplicación deben disponer de formación en ciberseguridad y ofrecer a su vez formación a sus empleados.

Dado el volumen y la importancia de los dispositivos de seguridad física actualmente en funcionamiento, resulta fundamental aplicar una estrategia de ciberseguridad que abarque tanto el parque instalado actualmente como a los sistemas que se desplegarán en los próximos años. Además, la proliferación de dispositivos *IoT* y la adopción de sistemas en la nube, junto con las capacidades emergentes de la inteligencia artificial, anticipan un crecimiento exponencial en el número de equipos que deberán integrarse en un marco de ciberseguridad robusto. En este sentido, cabe señalar la actividad en el ámbito regulatorio que se está produciendo en la Unión europea, en concreto, el Reglamento de ciberresiliencia, relativo a los requisitos horizontales de ciberseguridad para los productos con elementos digitales[2]. Este Reglamento tiene como objetivo garantizar que los productos consistentes en equipos y programas informáticos se introduzcan en el mercado con menos vulnerabilidades y que los fabricantes se tomen en serio la seguridad a lo largo de todo el ciclo de vida de un producto.

---

[1] DIRECTIVA (UE) 2022/2555 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 14 de diciembre de 2022.

[2] REGLAMENTO (UE) 2024/2847 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 23 de octubre de 2024.



SISTEMAS DE SEGURIDAD FÍSICA: ANÁLISIS DEL ÁMBITO

3.SISTEMAS DE SEGURIDAD FÍSICA: ANÁLISIS DEL ÁMBITO

Como paso previo al análisis de los ciberriesgos el estudio del ámbito es fundamental para delimitar su alcance, así como el de la propuesta de medidas, tanto técnicas como organizativas que sería necesario implementar.

En este trabajo se han considerado dos escenarios típicos de los Sistemas de Seguridad Física (SSF):

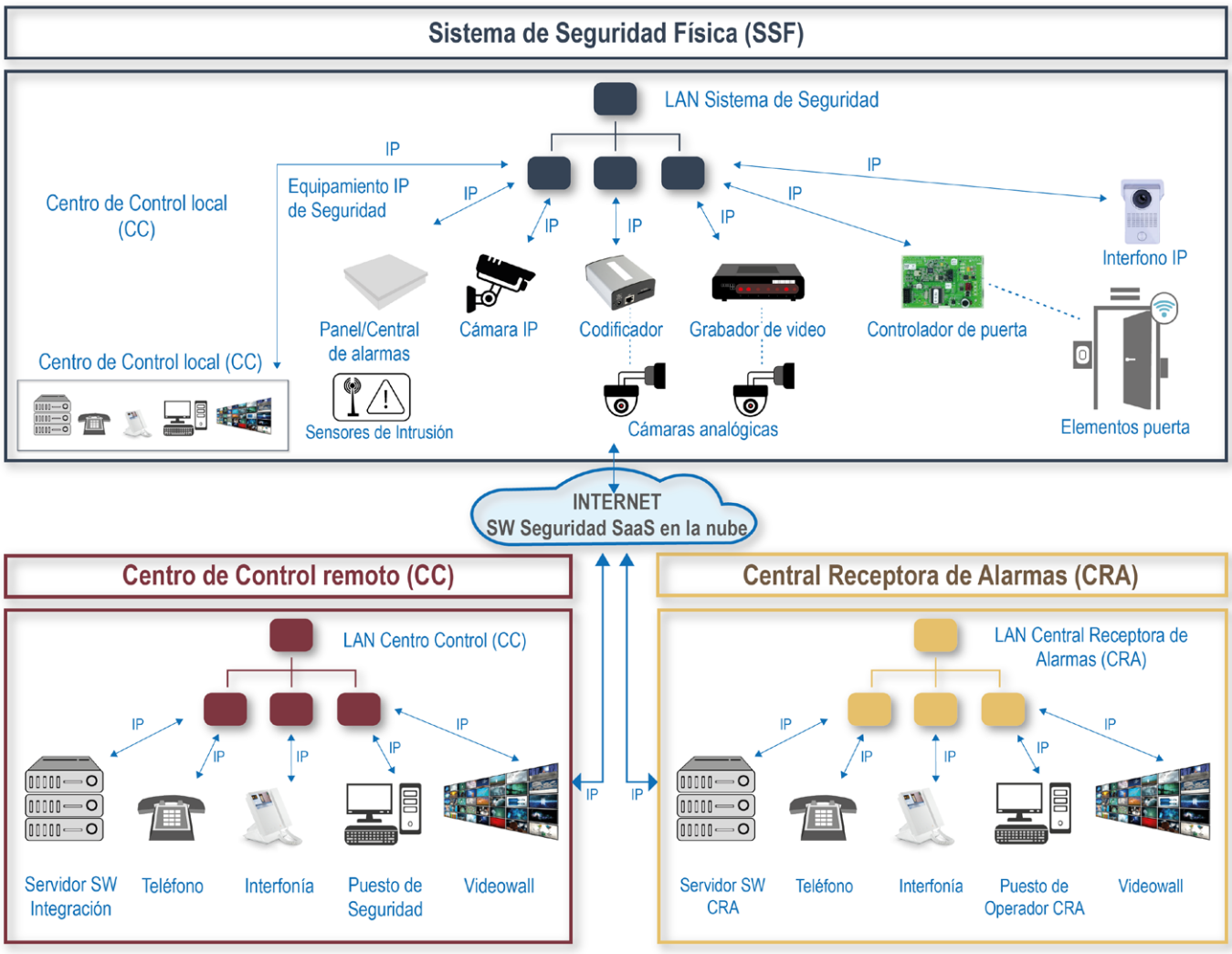
- Sistemas, normalmente sencillos, conectados a Centrales Receptoras de Alarmas (CRA) externas.
- Sistemas de una cierta complejidad dotados de Centros de Control propios (CC), de los que, en algunos casos, tienen parte de sus recursos de *hardware* y *software* en una nube externa.

No se han tenido en cuenta los dispositivos de seguridad que no están regulados por la Ley de Seguridad Privada, como los instalados en viviendas o pequeños comercios que envían sus señales de alarma de intrusión o de vídeo a los propietarios particulares a través de aplicaciones informáticas que utilizan servicios en la nube, sin conexión con Centrales receptoras de alarmas o Centros de control.

En ese mismo sentido es importante resaltar que, aunque otros subsistemas pueden estar conectados a un SSF, compartiendo incluso red de datos, como por ejemplo señales de climatización, de gestión de ascensores, etc., se ha decidido limitar el estudio a los elementos más comunes en los SSF que tengan una relación directa con la seguridad. Por ello, no se han incluido entre los subsistemas del SSF objeto de análisis los relacionados con el BMS (*Building Management Systems*), como protección de incendios, gestión de clima, etc.

Para la descripción de los elementos y estructuras que componen SSF se ha utilizado la nomenclatura del *Cybersecurity Framework* (CSF) de NIST, de modo que los "Perfiles" del CSF se correspondan con los dos escenarios que se han descrito, las "Categorías"se correspondan con los subsistemas que componen un SSF (detección de intrusión, control de accesos, televigilancia, supervisión y control e interfonía y megafonía) y las "Subcategorías" consistan en los tipos de elementos de estos subsistemas (*hardware*, *software*, personas, etc.).

En el diagrama que se expone a continuación se representa la arquitectura típica de los dos escenarios considerados.



Algunos de los elementos o conexiones podrían no existir dependiendo del sistema

ANÁLISIS DE CIBERRIESGOS

4.ANÁLISIS DE CIBERRIESGOS

Con objeto de identificar el conjunto de salvaguardas necesarias para incrementar las garantías de ciberseguridad en los SSF, se ha llevado a cabo un proceso de análisis de ciberriesgos siguiendo las fases comunes que componen este tipo de análisis:

- Identificación de activos.
- Identificación de amenazas.
- Valoración del ciberriesgo.

4.1- Identificación de activos

En la siguiente tabla se describen los activos identificados en los SSF considerados en este trabajo. Se consideran 36 componentes distintos, agrupados en 5 categorías de activos:

- Detección de intrusión (DI).
- Control de accesos (CA).
- Televigilancia (TV).
- Supervisión y control (SC).
- Interfonía y megafonía (ITM).

Para cada uno de los activos se han identificado los servicios que presta, con el objetivo de poder evaluar el impacto de cada una de las amenazas que le afectan.

Categoría	Tipo de Componentes en la categoría	Servicios
DI: Detección de intrusión	DI 1. Detectores.	Detectar puertas abiertas, movimiento, rotura o vibración en estructuras.
	DI 2. Dispositivos de captura de datos / información.	Recopilar datos de presión, humedad, niveles de gases, líquido, etc.
	DI 3. Elementos de análisis y tratamiento de señales.	Gestión de la comunicación y almacenaje de las señales de los detectores.
	DI 4. Elementos de respuesta.	Avisan localmente de las alarmas y aportan disuasión.
	DI 5. Elementos de gestión de señales e información.	Recepción de alarmas, verificación de las mismas y gestión de la reacción adecuada.
	DI 6. Elementos de comunicación y redes.	Comunicación de alarmas.
	DI 7. Elementos auxiliares.	Alimentación de equipos.
CA : Control de accesos	CA 1. Detectores.	Monitorización del estado del punto de acceso (por ejemplo, abierto o cerrado) y alarmas.
	CA 2. Dispositivos de captura de datos / información.	Lectura de credenciales.
	CA 3. Elementos de análisis y tratamiento de señales.	Gestión de la comunicación y procesamiento de las señales de los lectores, cerraduras y otros dispositivos conectados a las UCAs.
	CA 4. Elementos de respuesta.	Apertura de puertas, envío de señales a dispositivos conectados/integrados.
	CA 5. elementos de gestión de señales e información.	*Software* de gestión de accesos, interfaz de control, Monitor de accesos, recepción de alarmas, verificación de las mismas y gestión de la reacción adecuada.
	CA 6. Elemento de almacenamiento de datos.	Almacenamiento de información de usuarios, sistemas permisos, eventos, etc.
	CA 7. Elementos de intercomunicación audio/vídeo.	Facilitar el reconocimiento e identificación de los usuarios por parte del operador del sistema. Interfonía.
	CA 8. Elementos de comunicación y redes.	Transmisión de credenciales, datos de los usuarios y eventos del sistema.
	CA 9. Elementos auxiliares.	Alimentación del sistema, apertura libre del punto de acceso Otros servicios auxiliares.
TV: Televigilancia	TV 1. Detectores.	Mediante análisis de la imagen o del audio detectan situaciones definidas como potencialmente peligrosas.
	TV 2. Dispositivos de captura de datos / información.	Captura y almacenaje de imágenes, Captura de datos contenidos en la imagen (objetos, credenciales, etc), tranmisión de la señal de vídeo (puede incluir audio) y transmisión de alarmas.
	TV 3. Elementos de análisis y tratamiento de señales.	Generación de eventos en función de la captado por las cámaras de video o drones y en función de su programación.
	TV 4. Elementos de respuesta.	Avisan localmente de las alarmas y aportan disuasión.
	TV 5. Elementos de gestión de señales e información.	Recepción en tiempo real de vídeo, audio y eventos/alarmas. Control de cámaras móviles. Reproducción de vídeo y audio grabado.
	TV 6. Elemento de almacenamiento de datos.	Almacenamiento de audio, vídeo, eventos y log de usuarios.
	TV 7. Elementos de intercomunicación audio/vídeo.	Añaden ví deo a la comunicación verbal y audio a la vigilancia visual.
	TV 8. Elementos de comunicación y redes.	Transmisión de vídeo y audio. Comunicación de alarmas.
	TV 9. Elementos auxiliares.	Alimentación de equipos.
SC: Supervisión y control	SC 1. Estaciones de monitorización y operación. SC 2. Servidores de aplicaciones. SC 3. Estaciones de megafonía / Interfonía. SC 4. Estaciones de radio comunicación. SC 5. Sistemas unidades de almacenamiento de datos/vídeo.	Monitorización de imágenes y señales de alarma. Protocolos de respuesta. Revisión de video grabado. Investigación de eventos.
ITM: Interfonía y megafonía	ITM 1. Estación llamada intefonía.	Posibilitar comunicación bidireccional con CC.
	ITM 2. Estación/puesto de recepción de llamadas.	Recepción de llamadas y establecimiento de comunicación bidoreccional con las estaciones de llamada ITM1.1.
	ITM 3. Proyectores / Altavoces de Megafonía.	Emisión de mensajes de audio grabado o en tiempo real.
	ITM 4. Amplificadores Megafonía.	Amplificación de las señales de audio generadas en ITM1. 5 o ITM 1,6 para su difusión a través de los proyectores de ITM1,3.
	ITM 5. Grabadores /Reproductores de mensajes de voz.	Almacenamiento y reproducción de los mensajes pregrabados.
	ITM 6. Estación /Puesto de Control de Interfonía y Megafonía.	Gestión integral de las comunicaciones con posible interaccción con la comunicación con los ITM1.1 y ITM1.2, emisión mensajes conITM1.3 y ITM1.5 , a traves de ITM1.4.

4.2- Identificación de amenazas

Con el fin de disponer de una identificación clara de amenazas, en el **Anexo I** se presenta un catálogo de amenazas junto con su descripción. Para determinar el listado de amenazas aplicable se han utilizado fuentes basadas en metodologías como Magerit 3.0 y la *Interoperable EU Risk Management Toolbox* propuesta por ENISA (Agencia de la Unión Europea para la Ciberseguridad).

A continuación, se ha analizado el posible impacto que tienen de las amenazas identificadas en el Anexo I en los activos identificados en la tabla del apartado anterior, estudiando qué dimensiones de las establecidas en las metodologías de análisis de riesgos de base (disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad) resultan más críticas. Esta actividad persigue la identificación de prioridades en la implementación de medidas de protección y mitigación.

Disponibilidad

De manera general y para todos los subsistemas, sin excepción, la disponibilidad es crítica, dado que, si el subsistema no está operativo para desempeñar su función, las capacidades y funcionalidad de detección y observación del entorno, de restricción de acceso, de supervisión y de comunicación, se verán significativamente (o completamente) mermadas, inutilizando las medidas de seguridad física establecidas. Es por tanto fundamental establecer salvaguardas para asegurar que los subsistemas están continuamente operativos y funcionales, y disponer de capacidades redundantes de respaldo y de operación, aunque sean reducidas, incluso en caso de incidencias o incidentes graves.

Integridad

La **integridad** tiene un papel muy relevante en varios subsistemas:

- **Detección de intrusión**: se debe evitar que se manipulen los eventos de detección dando lugar a falsos positivos o falsos negativos, que dificulten la detección temprana de intrusiones o la identificación de la potencial vulneración de otras medidas de seguridad física.
- **Control de accesos**: se debe evitar la suplantación de la identidad de usuarios, proporcionando certeza sobre las actividades de acceso.
- **Televigilancia**: se debe asegurar que no se manipulen o modifiquen las grabaciones y de la adquisición de información del estado del entorno.

- **Supervisión y control**: se deben evitar interferencias sobre las capacidades de gestión del entorno.
- **Interfonía y megafonía**: se debe evitar la manipulación y modificación de las grabaciones y mensajes que se difundan en el entorno.

Autenticidad

Para todos los subsistemas en los que la integridad es relevante, la **autenticidad** también lo es, pero especialmente en **control de accesos e interfonía y megafonía**, de cara a poder llevar a cabo una identificación y autentificación precisa y confiable para poder aplicar mecanismos de autorización efectivos.

Confidencialidad

Los subsistemas de **control de accesos y de televigilancia** se ven directamente afectados por las amenazas a la confidencialidad, siendo necesario evitar la divulgación de actividades de identificación, acceso, monitorización y observación del entorno.

Igualmente, las amenazas a la confidencialidad afectan a la **supervisión y control**, al centralizarse en este subsistema la mayor parte del intercambio y recolección de datos, telemetría e información del entorno, muchos de ellos de carácter muy sensible y privado.

Trazabilidad

Para el subsistema de **supervisión y control** es igualmente crítica la **trazabilidad** ya que el mismo centraliza todas las actividades de gestión y monitorización de todo el entorno, por lo que requiere disponer de un histórico de eventos y registros que permitan conocer en todo momento y con suficiente granularidad y nivel de detalle las actividades, acciones y operaciones que han tenido lugar, tanto a nivel de auditoría como a nivel de la investigación y análisis de potenciales incidentes.

De forma sucinta se podría decir que la **disponibilidad** e **integridad** son necesarias para que los subsistemas cumplan con su función, que la **confidencialidad** y **autenticidad** deben garantizar el acceso sólo al personal autorizado y para aquello que están autorizados a tratar y conocer, y finalmente que la **trazabilidad** se requiere para supervisar, auditar el uso, y como gestionar incidentes de ciberseguridad.

4.3- Valoración del ciberriesgo

Para la valoración del ciberriesgo se ha tenido en cuenta la consulta realizada a responsables de seguridad física, tanto de empresas instaladoras como propietarias de SSF.

A partir de los resultados de la consulta, se ha estimado la **probabilidad** de ocurrencia de cada amenaza, así como el **impacto** causado por la degradación que supondría su materialización.

Para el cálculo del **ciberriesgo** se ha tenido en cuenta la combinación del impacto y la probabilidad, utilizando las siguientes escalas cualitativas especificadas en la metodología Magerit:

IMPACTO	PROBABILIDAD	RIESGO
MA: muy alto	MA: prácticamente seguro	MA: crítico
A: alto	A: probable	A: importante
M: medio	M: posible	M: apreciable
B: bajo	B: poco probable	B: bajo
MB: muy bajo	MB: muy raro	MB: despreciable

RIESGO		PROBABILIDAD				
		MB	B	M	A	MA
IMPACTO	MA	A	MA	MA	MA	MA
	A	M	A	A	MA	MA
	M	B	M	M	A	A
	B	MB	B	B	M	M
	MB	MB	MB	MB	B	B

La evaluación del impacto es el componente más importante en el proceso de análisis de ciberriesgos, permitiendo a las organizaciones poder clasificarlos en función del efecto que produce la materialización de la amenaza sobre la operatividad, seguridad y viabilidad del activo a largo plazo.

Impacto muy alto: Daños severos y, a menudo, irreparables que afectan profundamente a la infraestructura y a la operatividad de la organización. Implica pérdidas catastróficas, crisis de reputación y requiere replantear las estrategias de seguridad y operación.

Impacto alto: Consecuencias serias y posiblemente irreversibles en los SSF, con pérdidas financieras altas. Aunque la recuperación es posible, exige un esfuerzo significativo y posibles cambios estratégicos a largo plazo.

Impacto medio: Compromete la seguridad y operatividad del SSF en áreas críticas, pero permite una recuperación manejable con esfuerzos sostenidos. La respuesta inmediata controla los daños, evitando mayores consecuencias

Impacto bajo: Incidentes de impacto limitado que causan inconvenientes menores o pérdidas financieras manejables. La recuperación es sencilla, sin comprometer significativamente la operatividad general del SSF.

Impacto muy bajo: Incidentes insignificantes con impacto casi despreciable en la operatividad y en las finanzas. La recuperación es inmediata y no requiere acciones correctivas importantes.

Los resultados de la valoración del ciberriesgo se han incorporado en cada uno de los casos de uso incluidos en el capítulo 6.

MEDIDAS DE CIBERSEGURIDAD

5.MEDIDAS DE CIBERSEGURIDAD

Partiendo de los resultados de las fases anteriores, se han identificado las medidas de ciberseguridad o salvaguardas pertinentes para mitigar los riesgos detectados.

5.1 – Propuesta de salvaguardas

En la tabla que se presenta a continuación se incluye una propuesta genérica de aplicación de salvaguardas para cada categoría o subsistema teniendo en cuenta el nivel de seguridad demandado[3] .

En este punto, se hace necesario considerar que obviamente no todos los SSF protegen activos de la misma importancia y que la adopción de las medidas de ciberseguridad debe forzosamente venir condicionada por este factor, tanto en la selección de las salvaguardas que se apliquen como en el grado de su utilización. Consecuentemente, se debe hacer corresponder la criticidad de un ciberataque a un sistema con la importancia y criticidad de aquello que el sistema protege. Con esa premisa se han establecido niveles de exigencia de aplicación de las salvaguardas en función del nivel de seguridad que el sistema demande.

En consecuencia, en la tabla se incluye una referencia a los distintos **niveles de seguridad** del SSF considerados: **bajo** (verde), **medio** (amarillo) y **alto** (rojo), con la indicación de las salvaguardas recomendadas para cada nivel.

---

[3] En el anexo II se incluye la descripción completa de las salvaguardas, utilizado como marco de referencia el conjunto de medidas establecido por el Esquema Nacional de Seguridad (ENS). A efectos de trazabilidad se ha mantenido la codificación original, salvo para aquellas medidas codificadas como pro.*, que son específicas de producto y no tienen correspondencia con ninguna del ENS.

MEDIDAS		Detccion de intrusión	Control de accesos	Videovigilancia	Interfonía y megafonía	Supervisión y control
MEDIDAS ORGANIZATIVAS						
Política de seguridad	org.1					
Normativa de seguridad	org.2					
Procedimientos de seguridad	org.3					
Proceso de autorización	org.4					
MEDIDAS OPERACIONALES						
Análisis de riesgos	op.pl.1					
Arquitectura de seguridad	op.pl.2					
Adquisición nuevos componentes	op.pl.3					
Dimensionado/gestión capacidad	op.pl.4					
Componentes certificados	op.pl.5					
Identificación	op.acc.1					
Requisitos de acceso	op.acc.2					
Segregación	op.acc.3					
Gestión derechos de acceso	op.acc.4					
Autenticación de usuarios	op.acc.6					
Inventario de activos	op.exp.1					
Configuración de seguridad	op.exp.2					
Gestión de la configuración	op.exp.3					
Mantenimiento y actualizaciones	op.exp.4					
Gestión de cambios	op.exp.5					
Protección código dañino	op.exp.6					
Gestión de incidentes	op.exp.7					
Registro de actividad	op.exp.8					
Registro gestión de incidentes	op.exp.9					
Protección claves criptográficas	op.exp.10					
Acuerdos nivel de servicio	op.ext.1					
Protección cadena de suministro	op.ext.3					
Interconexión de sistemas	op.ext.4					
Protección servicios en la nube	op.nub.1					
Análisis de impacto	op.cont.1					
Plan de continuidad	op.cont.2					
Pruebas periódicas continuidad	op.cont.3					
Medios alternativos continuidad	op.cont.4					
Detección intrusión informática	op.mon.1					
MEDIDAS DE PROTECIÓN						
Áreas separadas y control acceso	mp.inf.1					
Identificación de personas	mp.inf.2					
Acondicionamiento de locales	mp.inf.3					
Energía eléctrica	mp.inf.4					
Registro entrada salida equipamiento	mp.inf.7					
Caracterización puesto de trabajo	mp.per.1					
Concienzación	mp.per.3					
Formación	mp.per.4					
Bloqueo puesto de trabajo	mp.eq.2					
Otros dispositivos conectados a la red	mp.eq.4					
Perímetro seguro	mp.com.1					
Protección confidencialidad	mp.com.2					
Protección autenticidad e integridad	mp.com.3					
Separación flujos información en red	mp.com.4					
Desarrollo de aplicaciones	mp.sw.1					
Aceptación y puesta en servicio	mp.sw.2					
Datos personales	mp.info.1					
Calificación de la información	mp.info.2					
Copias de seguridad	mp.info.6					
Protección correo electrónico	mp.s.1					
Protección servicios y aplicaciones web	mp.s.2					
Protección navegación web	mp.s.3					
Protección frente denegación de servicio	mp.s.4					
MEDIDAS DE PRODUCTOS						
Canales confiables	pro.1					
Auditoría	pro.2					
Actualización confiable	pro.3					
Gestión de usuarios, mínimos privilegios	pro.4					
Autentificación robusta	pro.5					
Mecanismos antiDos	pro.6					
Control de acceso informático	pro.7					
Protección de los equipos y los servicios	pro.8					
Cifrado “at rest”	pro.9					
Firma digital	pro.10					
Borrado seguro	pro.11					
Soberanía	pro.12					
SLA en la nube	pro.13					

Medida exigible para sistemas que demanden un nivel de seguridad bajo o superior
Medida exigible para sistemas que demanden un nivel de seguridad medio o superior
Medida exigible para sistemas que demanden un nivel de seguridad alto

5.2 – Propuesta de correspondencia con los grados de los Sistemas de Seguridad Física

En el ámbito de la seguridad física la reglamentación existente (Reglamento de Seguridad Privada[4] y órdenes ministeriales[5]) contempla la categorización de las instalaciones con criterio del riesgo y activos a proteger. Apoyándose en la norma UNE-EN 50131-1 se determina una categorización en base a diferentes grados (1,2,3 y 4) que se hacen corresponder con los riesgos estimados en cada entorno de aplicación:

- El **grado 1,** el más básico, corresponde a instalaciones no conectadas a centrales receptoras de alarma o centros de control, y por lo tanto estaría fuera del ámbito de este documento.
- Los **grados 2,3 y 4** podrían hacerse corresponder con los niveles de exigencia de salvaguardas utilizados en la tabla de recomendaciones.

Un simple traslado de la categorización incluida en la tabla hacia el modelo de grados (Bajo=Grado 2, Medio=Grado 3, Alto=Grado 4) facilitará la comprensión de qué salvaguardas son recomendadas en función del tipo de instalación y activos a proteger. Todo ello sin intención alguna de entrar en una correspondencia exhaustiva entre los niveles establecidos en este documento y los fundamentos técnicos de las normas UNE-EN en las que se sustenta la categorización de grados en los SSF.

[4] Ley 5/2014, de 4 de abril, de Seguridad Privada. Real Decreto 2364/1994, de 9 de diciembre, por el que se aprueba el Reglamento de Seguridad Privada.

[5] Orden INT/1504/2013, de 30 de julio. Orden INT/314/2011, de 1 de febrero. Orden PRE/2914/2009, de 30 de octubre.

CASOS DE USO

6.CASOS DE USO

Como cierre del proceso, se presentan en este capítulo a modo de ejemplo algunos posibles casos de uso o escenarios de ataque más comunes contra los SSF. El objetivo es proporcionar una visión de las principales amenazas en las que sería necesario poner más atención, así como una lista de salvaguardas para mitigar los riesgos, sin pretender que esta lista sea exhaustiva.

Para la valoración del impacto y la probabilidad de cada escenario se ha tenido en cuenta la aportación de los expertos de empresas tanto instaladoras como propietarias de SSF. La valoración del ciberrriesgo se ha realizado conforme a la metodología Magerit expuesta en el apartado 4.3.

6.1 – Ataques contra la red de comunicaciones

1 ATAQUES CONTRA LA RED DE COMUNICACIONES

Este escenario describe una interrupción o interceptación de la comunicación entre controladores y actuadores de SSF. Este ataque prueba la seguridad de la red y la resiliencia de los sistemas críticos de control.

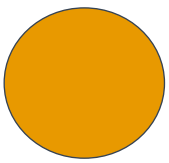
Este tipo de ataque compromete la operatividad de los sistemas al interrumpir o interceptar comunicaciones clave. Afecta la capacidad de respuesta y control en tiempo real, lo que puede conllevar riesgos significativos para la seguridad física y cibernética.

APLICACIÓN A LOS ESCENARIOS DE CONTEXTO

CRA: La interrupción o interceptación compromete la recepción y el procesamiento de señales de alarma, retrasando o impidiendo la respuesta a emergencias. El impacto es alto debido a la pérdida de capacidad de respuesta en tiempo real.

Centro de Control: Afecta la coordinación y el control de operaciones. La interrupción en la comunicación puede tener consecuencias graves en la seguridad y la eficiencia operativa.

AMENAZAS	SALVAGUARDAS
[I.4] Contaminación electromagnética [I.5] Avería de origen físico o lógico [I.6] Corte del suministro eléctrico [I.8] Fallo de servicios de comunicaciones [E.2] Errores del administrador [E.3] Errores de monitorización (log) [E.4] Errores de configuración [E.20] Vulnerabilidades de los programas [A.11] Acceso no autorizado	[mp.if.3] Acondicionamiento de los locales [pro.8] Protección de los equipos y servicios [mp.if.4] Energía eléctrica [mp.if.1] Áreas separadas y control de acceso [op.exp.4] Mantenimiento y actualizaciones de seguridad [op.exp.6] Protección frente al código dañino [op.ext.4] interconexión de sistemas [op.exp.8] Registro de actividad

[A.12] Análisis de tráfico [A.14] Interceptación de información (escucha) [A.23] Manipulación de los equipos [A.24] Denegación de servicio	[pro.2] Auditoría [op.acc.2] Requisitos de acceso [op.acc.4] Proceso de gestión de derechos de acceso [pro.7] Control de acceso informático [mp.com.1] Perímetro seguro [mp.com.2] Protección de la confidencialidad [mp.com.3] Protección de la integridad y de la autenticidad [mp.com.4] Separación de flujos de información en la red [pro.1] Canales confiables
VALORACIÓN	RIESGO
Este ataque tiene **un riesgo importante** debido a la combinación de una **probabilidad probable** y un **impacto alto**. La interrupción de la comunicación entre los dispositivos de seguridad compromete la operatividad, afectando la capacidad de respuesta en tiempo real y generando un escenario crítico para las empresas que dependen de sistemas conectados.	

6.2 – Modificación de sensores de detección de intrusión

2 MODIFICACIÓN DE SENSORES DE DETECCIÓN DE INTRUSIÓN

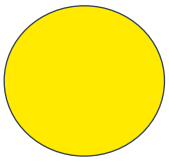
Este escenario describe una alteración de los valores leídos por los sensores un cambio en sus configuraciones. Este tipo de ataque compromete la autenticidad y la integridad de la información crítica recopilada por los sensores, impactando en la toma de decisiones basada en datos y la respuesta automática de los sistemas.

APLICACIÓN A LOS ESCENARIOS DE CONTEXTO

CRA: La modificación de los valores leídos puede llevar a respuestas inadecuadas a eventos no ocurridos o a la ignorancia de eventos reales, comprometiendo la seguridad y la confiabilidad del sistema.

Centro de Control: Afecta la toma de decisiones basada en datos erróneos, pudiendo resultar en acciones operativas incorrectas con posibles consecuencias materiales o humanas.

AMENAZAS	SALVAGUARDAS
[I.8] Fallo de servicios de comunicaciones	[pro.8] Protección de los equipos y servicios
[E.2] Errores del administrador	[op.exp.4] Mantenimiento y actualizaciones de seguridad
[E.3] Errores de monitorización (log)	[op.exp.8] Registro de actividad
[E.4] Errores de configuración	[pro.2] Auditoría
[E.20] Vulnerabilidades de los programas	[op.acc.2] Requisitos de acceso
[A.11] Acceso no autorizado	[op.acc.4] Proceso de gestión de derechos de acceso
[A.12] Análisis de tráfico	[pro.7] Control de acceso informático
[A.14] Interceptación de información (escucha)	[mp.com.2] Protección de la confidencialidad
[A.22] Manipulación de programas	[mp.com.3] Protección de la integridad y de la autenticidad
[A.23] Manipulación de los equipos	[pro.1] Canales confiables
[A.24] Denegación de servicio	

	[mp.if.1] Áreas separadas y control de acceso [mp.s.4] Protección frente a denegación de servicio [pro.6] Mecanismos antiDoS
VALORACIÓN	RIESGO
Este escenario presenta un **riesgo apreciable,** con una **probabilidad poco probable** y un **impacto medio,** ya que la manipulación de los sensores afecta la confiabilidad del sistema de seguridad, pero su impacto está relativamente contenido debido a la posible detección temprana o mitigación de los efectos antes de que se produzcan daños graves.	

6.3 – Ataques a elementos de control de acceso, interfonía y televigilancia

3 ATAQUES A ELEMENTOS DE CONTROL DE ACCESO, INTERFONÍA Y TELEVIGILANCIA

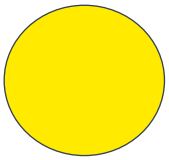
Este escenario describe una modificación indebida o inhabilitación de las configuraciones normales de los actuadores. Evalúa la seguridad de los componentes que ejecutan acciones físicas en respuesta a señales de control, poniendo a prueba la integridad operativa de los sistemas.

APLICACIÓN A LOS ESCENARIOS DE CONTEXTO

CRA: Indirectamente afectado, ya que la manipulación de elementos de respuesta puede resultar en fallos de los sistemas de seguridad que deberían ser monitorizados por la CRA.

Centro de Control: Compromete la ejecución de operaciones críticas y la integridad física de la infraestructura.

AMENAZAS	SALVAGUARDAS
[I.8] Fallo de servicios de comunicaciones	[pro.8] Protección de los equipos y servicios
[E.2] Errores del administrador	[op.exp.4] Mantenimiento y actualizaciones de seguridad
[E.3] Errores de monitorización (log)	[op.exp.8] Registro de actividad
[E.4] Errores de configuración	[pro.2] Auditoría
[E.20] Vulnerabilidades de los programas	[op.acc.2] Requisitos de acceso
[A.11] Acceso no autorizado	[op.acc.4] Proceso de gestión de derechos de acceso
[A.12] Análisis de tráfico	[pro.7] Control de acceso informático
[A.14] Interceptación de información (escucha)	[mp.com.2] Protección de la confidencialidad
[A.22] Manipulación de programas	[mp.com.3] Protección de la integridad y de la autenticidad
[A.23] Manipulación de los equipos	

[A.24] Denegación de servicio	[pro.1] Canales confiables [mp.if.1] Áreas separadas y control de acceso [mp.s.4] Protección frente a denegación de servicio [pro.6] Mecanismos antiDoS
VALORACIÓN	RIESGO
Este escenario tiene un **riesgo apreciable** dado por la **probabilidad de ocurrencia posible** mientras que el **impacto** es **medio,** ya que la manipulación de estos sistemas puede afectar a la operación de control de acceso y televigilancia, sus consecuencias no son tan graves en términos de disrupción general de la seguridad.	

6.4 – Ataques al subsistema de supervisión y control

4 ATAQUES AL SUBSISTEMA DE SUPERVISIÓN Y CONTROL

Este escenario describe un compromiso de los sistemas que gestionan la seguridad global. Aquí se prueba la robustez de las políticas y herramientas de seguridad implementadas, identificando vulnerabilidades en la gestión y administración de la seguridad.

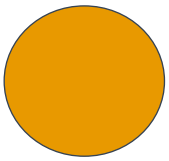
Esta tipología de ataque compromete los sistemas de administración de seguridad y pone en riesgo la capacidad de gestionar adecuadamente las operaciones y responder a incidentes de manera eficiente, afectando tanto la operatividad como la seguridad general.

APLICACIÓN A LOS ESCENARIOS DE CONTEXTO

CRA: Impacto muy alto, ya que compromete la capacidad general de monitorización y respuesta a alarmas, afectando la confianza en el sistema de seguridad global.

Centro de Control: Afecta la gestión de la seguridad operacional, pudiendo llevar a una gestión deficiente de las amenazas y riesgos.

AMENAZAS	SALVAGUARDAS
[I.9] Interrupción de otros servicios y suministros esenciales [E.1] Errores de los usuarios [E.2] Errores del administrador [E.3] Errores de monitorización (log) [E.4] Errores de configuración [E.8] Difusión de *software* dañino [E.20] Vulnerabilidades de los programas (*software*) [E.21] Errores de mantenimiento / actualización de programas (*software*)	[mp.if.3] Acondicionamiento de los locales [mp.if.4] Energía eléctrica [op.exp.8] Registro de actividad [pro.2] Auditoría [pro.8] Protección de los equipos y servicios [op.exp.6] Protección código dañino [op.pl.5] Componentes certificados [op.exp.4] Mantenimiento y actualizaciones de seguridad

[E.23] Errores de mantenimiento / actualización de equipos (*hardware*) [A.4] Manipulación de la configuración [A.8] Difusión de *software* dañino [A.14] Interceptación de información (escucha) [A.22] Manipulación de programas [A.23] Manipulación de los equipos	[pro.3] Actualización confiable [mp.if.1] Áreas separadas y control de acceso [op.acc.2] Requisitos de acceso [op.acc.4] Proceso de gestión de derechos de acceso [pro.7] Control de acceso informático [mp.com.2] Protección de la confidencialidad [mp.com.3] Protección de la integridad y de la autenticidad [pro.1] Canales confiables
VALORACIÓN	RIESGO
Este escenario representa un **riesgo importante** con una **probabilidad de ocurrencia probable** y un **impacto alto,** ya que los sistemas de administración son críticos para la gestión global de la seguridad. Un ataque que comprometa estos sistemas puede generar una gran disrupción en la operatividad de la organización y en su capacidad para gestionar amenazas y riesgos.	

6.5 – Explotación de vulnerabilidades en los protocolos de comunicaciones

5 EXPLOTACIÓN DE VULNERABILIDADES EN LOS PROTOCOLOS DE COMUNICACIONES

Este escenario describe la identificación o explotación de debilidades en los protocolos de comunicación utilizados por la red y los dispositivos. Este ataque revela las carencias en la seguridad de las comunicaciones y la necesidad de fortalecer la protección de los datos en tránsito.

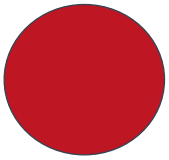
Al explotar estas vulnerabilidades, se ve afectada la integridad y confidencialidad de los datos en tránsito, comprometiendo la seguridad de las operaciones.

APLICACIÓN A LOS ESCENARIOS DE CONTEXTO

CRA: Puede permitir el acceso no autorizado a datos sensibles a la manipulación de señales de alarma, comprometiendo la confidencialidad y la integridad de la información.

Centro de Control: Expone a riesgos similares, afectando a la seguridad de las comunicaciones operativas y posiblemente a la integridad de los sistemas controlados.

AMENAZAS	SALVAGUARDAS
[E.4] Errores de configuración [E.20] Vulnerabilidades de los programas (*software*) [A.14] Interceptación de información (escucha) [A.22] Manipulación de programas [A.24] Denegación de servicio	[op.exp.8] Registro de actividad [pro.2] Auditoría [pro.8] Protección de los equipos y servicios [op.pl.5] Componentes certificados [mp.com.2] Protección de la confidencialidad [mp.com.3] Protección de la integridad y de la autenticidad [pro.1] Canales confiables

VALORACIÓN	RIESGO
Este escenario tiene un **riesgo crítico**. La **probabilidad de ocurrencia es probable** y el **impacto** es **muy alto**. Explotar vulnerabilidades en los protocolos de comunicación puede comprometer la confidencialidad y la integridad de los datos en tránsito, lo que tiene efectos graves sobre la seguridad de las operaciones.	

6.6 – Ataques de inyección de comandos en el subsistema de supervisión y control

6 ATAQUES DE INYECCIÓN DE COMANDOS EN EL SUBSISTEMA DE SUPERVISIÓN Y CONTROL

Este escenario describe una ejecución de comandos maliciosos en la consola de sistema de dispositivos críticos. Plantea ataques que buscan obtener control no autorizado sobre los dispositivos, desafiando la seguridad perimetral y las defensas internas.

La inyección de comandos compromete el control de sistemas críticos y afecta a la toma de decisiones operativas en los sistemas de seguridad.

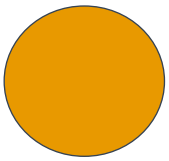
APLICACIÓN A LOS ESCENARIOS DE CONTEXTO

CRA: La inyección de comandos puede comprometer directamente la integridad de los sistemas de procesamiento de alarmas, permitiendo a un atacante modificar configuraciones o desactivar alarmas. Este ataque presenta un impacto es alto debido al riesgo de fallos en la respuesta a incidentes críticos.

Centro de Control: Este ataque podría permitir el control no autorizado sobre procesos operativos críticos, impactando directamente la seguridad y eficiencia de las operaciones. La capacidad para mantener operaciones seguras se ve seriamente comprometida.

AMENAZAS	SALVAGUARDAS
[I.8] Fallo de servicios de comunicaciones [E.2] Errores del administrador [E.3] Errores de monitorización (log) [E.4] Errores de configuración [E.20] Vulnerabilidades de los programas (*software*) [A.11] Acceso no autorizado	[pro.8] Protección de los equipos y servicios [op.exp.4] Mantenimiento y actualizaciones de seguridad [op.exp.8] Registro de actividad [pro.2] Auditoría [op.acc.2] Requisitos de acceso [op.acc.4] Proceso de gestión de derechos de acceso

[A.12] Análisis de tráfico [A.14] Interceptación de información (escucha)	[pro.7] Control de acceso informático [mp.com.2] Protección de la confidencialidad [mp.com.3] Protección de la integridad y de la autenticidad [pro.1] Canales confiables

VALORACIÓN	RIESGO
Este escenario representa un **riesgo importante,** con una **probabilidad de ocurrencia probable**. El **impacto** es **alto,** ya que la inyección de comandos maliciosos afecta la capacidad de control de los sistemas críticos, comprometiendo la toma de decisiones operativas y poniendo en peligro la integridad del sistema de seguridad.	

6.7 – Escalada de privilegios

7 ESCALADA DE PRIVILEGIOS EN LOS SUBSISTEMAS DE SEGURIDAD FÍSICA PARA ACCEDER A LOS SUBSISTEMAS DE SUPERVISIÓN Y CONTROL

Este escenario describe el uso de dispositivos o sistemas comprometidos como paso previo a un ataque más complejo. Este tipo de ataque pone a prueba la cadena de seguridad, desde el perímetro hasta los sistemas internos, destacando la importancia de la protección de los activos implementando el modelo de seguridad por capas.

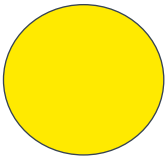
Aprovecha vulnerabilidades en los sistemas de detección e intrusión para escalar a otras partes críticas de la infraestructura, afectando a la seguridad global.

APLICACIÓN A LOS ESCENARIOS DE CONTEXTO

CRA: El uso de dispositivos intermedios comprometidos puede facilitar ataques indirectos, como el espionaje de datos o la introducción de *malware*. Esto afecta a la confidencialidad y la integridad de las comunicaciones y datos procesados.

Centro de Control: Podría permitir a un atacante obtener acceso escalonado a sistemas críticos, comprometiendo desde las operaciones hasta la seguridad de datos, con un impacto medio en la continuidad operacional.

AMENAZAS	SALVAGUARDAS
[E.2] Errores del administrador [E.4] Errores de configuración [E.8] Difusión de *software* dañino [E.20] Vulnerabilidades de los programas (*software*) [E.21] Errores de mantenimiento / actualización de programas (*software*) [A.8] Difusión de *software* dañino	[op.exp.8] Registro de actividad [pro.2] Auditoría [pro.8] Protección de los equipos y servicios [op.exp.6] Protección código dañino [op.pl.5] Componentes certificados [op.exp.4] Mantenimiento y actualizaciones de seguridad

[A.11] Acceso no autorizado [A.12] Análisis de tráfico [A.14] Interceptación de información (escucha) [A.24] Denegación de servicio	[pro.3] Actualización confiable [mp.if.1] Áreas separadas y control de acceso [op.acc.2] Requisitos de acceso [op.acc.4] Proceso de gestión de derechos de acceso [pro.7] Control de acceso informático [mp.com.2] Protección de la confidencialidad [mp.com.3] Protección de la integridad y de la autenticidad [pro.1] Canales confiables [mp.s.4] Protección frente a denegación de servicio [pro.6] Mecanismos antiDoS [mp.com.1] Perímetro seguro
VALORACIÓN	RIESGO
Este escenario representa un **riesgo apreciable,** con una **probabilidad posible** y un **impacto** es **medio,** ya que la explotación de vulnerabilidades en los sistemas de detección permite a un atacante escalar su acceso y comprometer otras áreas críticas del sistema, aumentando significativamente el riesgo para la organización.	

6.8 – Denegación de servicio distribuido

8 DENEGACIÓN DE SERVICIO DISTRIBUIDO

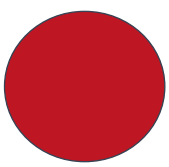
Este escenario describe un ataque de denegación de servicio distribuido (DDdos) que busca sobrecargar los sistemas y la infraestructura de red, comprometiendo principalmente la disponibilidad de servicios críticos. Pone a prueba la capacidad de absorber y mitigar ataques masivos de tráfico no deseado.

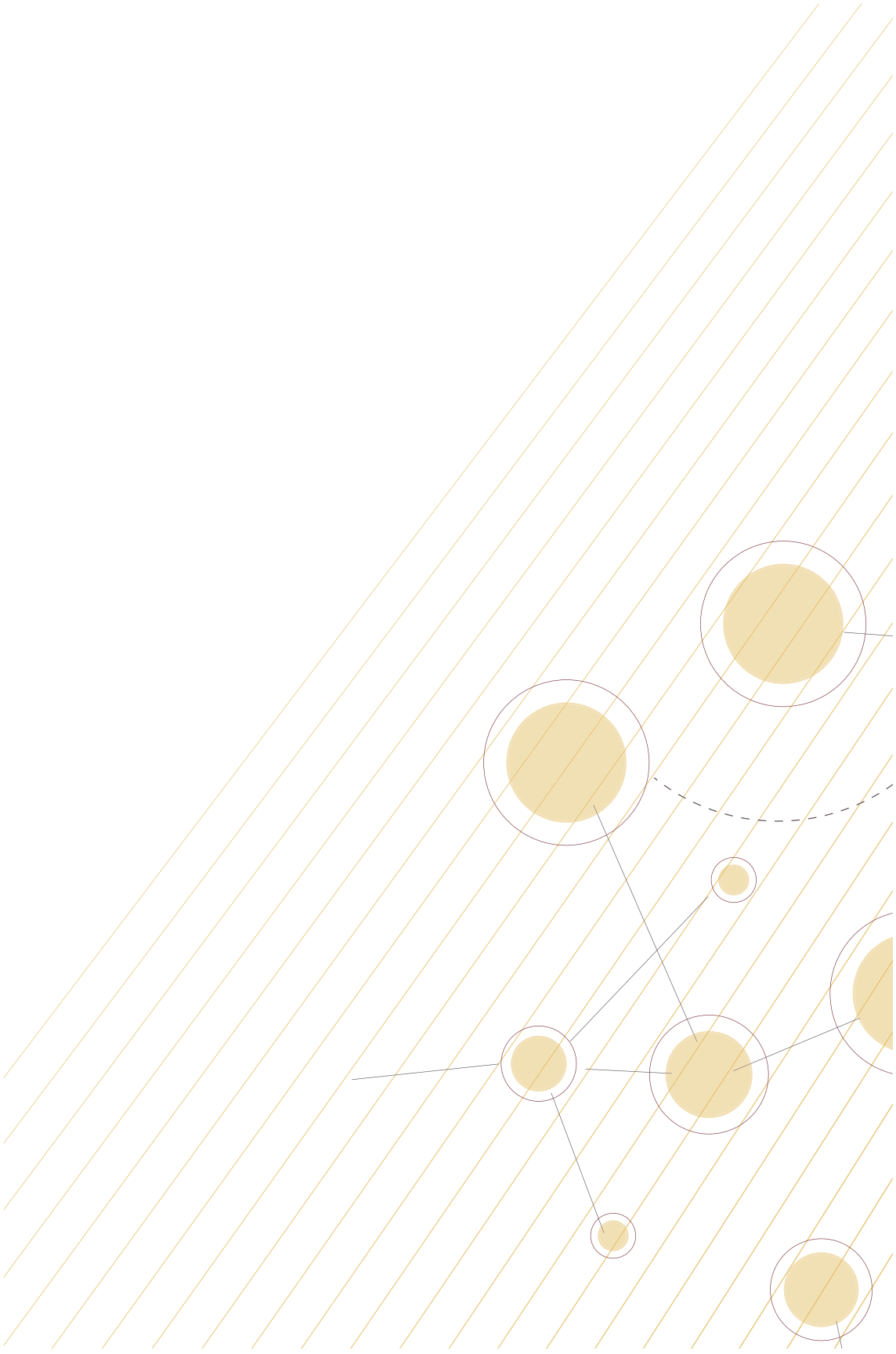
APLICACIÓN A LOS ESCENARIOS DE CONTEXTO

CRA: Un ataque de DDoS podría saturar la red, impidiendo la comunicación efectiva con dispositivos de seguridad o la recepción de señales de alarma. El impacto es crítico por la potencial pérdida de funcionalidad en situaciones de emergencia.

Centro de Control: La sobrecarga de las redes de comunicación puede interrumpir la monitorización y control de operaciones, llevando a una parálisis operativa con consecuencias potencialmente catastróficas.

AMENAZAS	SALVAGUARDAS
[A.24] Denegación de servicio	[mp.s.4] Protección frente a denegación de servicio [pro.6] Mecanismos antiDoS [mp.com.1] Perímetro seguro

VALORACIÓN	RIESGO
Este escenario implica un **riesgo crítico** con una **probabilidad probable**. El **impacto** es **muy alto**, ya que un ataque de denegación de servicio podría interrumpir la operación de sistemas de seguridad en situaciones de emergencia, afectando gravemente la disponibilidad de servicios críticos.	



6.9 – Manipulación de las fuentes de alimentación

9 MANIPULACIÓN DE LAS FUENTES DE ALIMENTACIÓN

Este escenario describe ataques dirigidos a la fuente de alimentación y a la explotación de vulnerabilidades en la monitorización de energía. Este tipo de ataque desafía la seguridad física y la estabilidad operacional de los sistemas, poniendo en riesgo la continuidad de las operaciones.

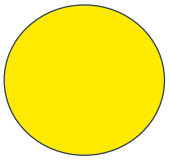
Este ataque compromete temporalmente los sistemas de seguridad al manipular la fuente de alimentación, aunque las medidas de respaldo suelen mitigar sus efectos de forma significativa.

APLICACIÓN A LOS ESCENARIOS DE CONTEXTO

CRA:Los ataques a la fuente de alimentación pueden desactivar temporalmente los sistemas de procesamiento de alarmas, comprometiendo la disponibilidad. Aunque existan sistemas de respaldo, el impacto es significativo.

Centro de Control: La estabilidad operativa se ve comprometida, con el riesgo de pérdida de control de los procesos esenciales. La dependencia de sistemas de alimentación ininterrumpida se pone a prueba, destacando la necesidad de medidas de contingencia robustas.

AMENAZAS	SALVAGUARDAS
[E.20] Vulnerabilidades de los programas (*software*) [A.4] Manipulación de la configuración [A.5] Suplantación de la identidad del usuario [A.14] Interceptación de información (escucha) [A.18] Destrucción de información	[mp.if.3] Acondicionamiento de los locales [mp.if.4] Energía eléctrica [op.exp.8] Registro de actividad [pro.2] Auditoría [op.pl.5] Componentes certificados [pro.4] Gestión de usuarios. Mínimo privilegio

	[op.acc.2] Requisitos de acceso [op.acc.4] Proceso de gestión de derechos de acceso [pro.7] Control de acceso informático [mp.com.2] Protección de la confidencialidad [mp.com.3] Protección de la integridad y de la autenticidad [pro.1] Canales confiables [mp.info.6] Copias de seguridad
VALORACIÓN	RIESGO
Este escenario representa un **riesgo apreciable,** con una **probabilidad posible** de ocurrencia. El **impacto** es **medio,** ya que aunque puede desactivar temporalmente sistemas de procesamiento de alarmas, las medidas de respaldo permiten mitigar en gran medida los efectos.	

6.10 – *Ransonware*

10 *RANSONWARE*

Este escenario describe el despliegue e implementación de *ransomware* dirigido a cifrar datos críticos y sistemas, exigiendo un rescate para su liberación. Pone a prueba todas las defensas perimetrales, las defensas anti-*malware*, la eficacia de las copias de seguridad y los planes de respuesta ante incidentes de seguridad.

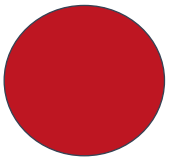
El *ransomware* cifra datos críticos, paraliza operaciones y exige un rescate para recuperar el control de los sistemas, con graves consecuencias financieras y operativas.

APLICACIÓN A LOS ESCENARIOS DE CONTEXTO

CRA:Un ataque de *ransomware* que cifre datos críticos o sistemas de procesamiento de alarmas puede tener un impacto muy alto, interrumpiendo las operaciones y exigiendo una respuesta inmediata para recuperar la funcionalidad.

Centro de Control: El cifrado de sistemas operativos o datos críticos no solo interrumpe las operaciones, sino que también plantea un riesgo significativo de pérdida de datos operativos esenciales, requiriendo esfuerzos extensivos para la recuperación y el restablecimiento de operaciones.

AMENAZAS	SALVAGUARDAS
[E.20] Vulnerabilidades de los programas (*software*) [A.4] Manipulación de la configuración [A.8] Difusión de *software* dañino [A.24] Denegación de servicio	[op.exp.8] Registro de actividad [pro.2] Auditoría [op.pl.5] Componentes certificados [op.exp.6] Protección código dañino [mp.com.1] Perímetro seguro [mp.info.6] Copias de seguridad

VALORACIÓN	RIESGO
Este escenario representa un **riesgo crítico** debido a la **probabilidad posible** de que se implemente *ransomware*. El **impacto** es **muy alto,** ya que el cifrado de datos y la exigencia de rescates pueden paralizar las operaciones y generar graves disrupciones operativas y pérdidas financieras.	

7.DOCUMENTOS DE REFERENCIA

- MAGERIT v.3 : Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.

  Visto en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

- Interoperable EU Risk Management Toolbox.

  Visto en: https://www.enisa.europa.eu/publications/interoperable-eu-risk-management-toolbox

- The NIST Cybersecurity Framework (CSF) 2.0.

  Visto en: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

- Cyber Assurance of Physical Security Systems (CAPSS). National Proactive Security Agency de Reino Unido, 2024.

  Visto en: https://www.npsa.gov.uk/resources/capss-guidance

- Recommandations sur la sécurisation des systèmes de contrôle d'accès physique et de vidéoprotection. Agence nationale de la sécurité des systèmes d'information, 2023.

  Visto en: https://cyber.gouv.fr/sites/default/files/document/Recommandations%20sur%20la%20s%C3%A9curisation%20des%20syst%C3%A8mes%20de%20contr%C3%B4le%20d%27acc%C3%A8s%20physique%20et%20vid%C3%A9oprotection%20-%20v2.1.pdf

- Cybersecurity and Physical Security Convergence. Cibersecurity & Infraestructure Security Agency de EEUU (CISA), 2021.

  Visto en: https://www.cisa.gov/sites/default/files/publications/Cybersecurity%20and%20Physical%20Security%20Convergence_508_01.05.2021_0.pdf

- 800-82 Guide to Industrial Control Systems (ICS) Security. National Institute of Standards and Technology US Department of Commerce (NIST), 2015.

  Visto en: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

- Baseline Security Recommendations for IoT (ENISA) 2017.

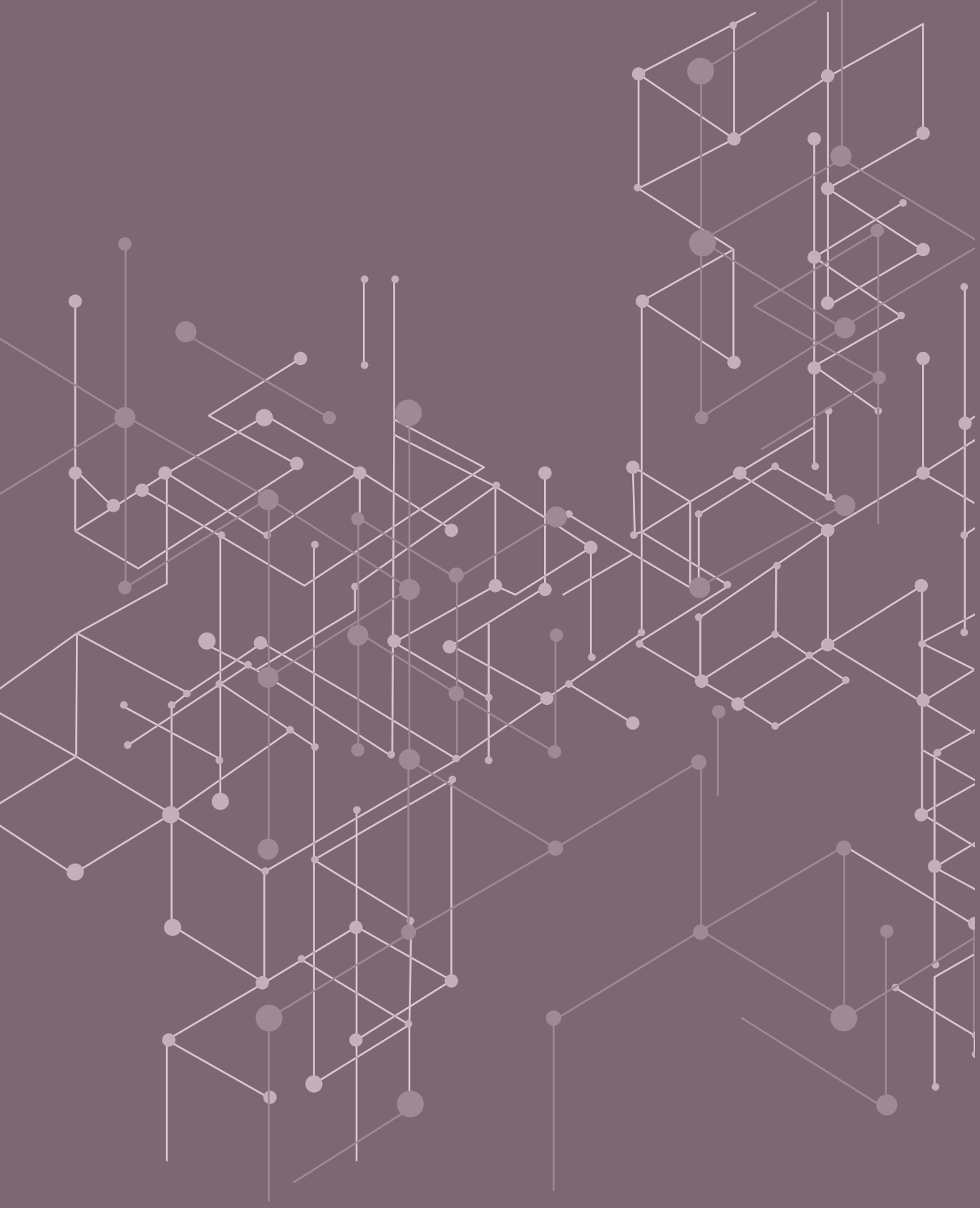
  Visto en https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot

- Best Practices for Cyber Crisis Management (ENISA) 2024.

  Visto en https://www.enisa.europa.eu/publications/best-practices-for-cyber-crisis-management

- Cyber/Physical Security Framework (Cyber Security Division , Ministry of Economy Trade and Industry, Japón) 2019.

  Visto en https://www.meti.go.jp/policy/netsecurity/wg1/CPSF_ver1.0_eng.pdf



GLOSARIO

8.GLOSARIO

Anti-*malware*: Aplicación informática cuya finalidad es la detección, detención y eliminación de virus y demás códigos maliciosos.

Autenticación: Proceso de verificación de la identidad de un usuario, dispositivo o sistema antes de permitir el acceso a recursos protegidos.

Autorización: Proceso mediante el cual se otorgan o deniegan permisos a un usuario, dispositivo o sistema para acceder a recursos específicos tras haberse autenticado.

Centro de Control (CC): Referido a un Sistema de Seguridad Física. Unidad central donde se monitorizan y gestionan los sistemas de seguridad de una organización. Comprende el conjunto de dispositivos, redes, aplicaciones y bases de datos, que permiten recibir la información del sistema de seguridad (imágenes, alarmas, registros de acceso, etc.), normalmente a través de una red local, para su presentación a los operadores del sistema, el archivo de los registros correspondientes y, en su caso, el envío de comandos de actuación (posicionamiento de cámaras, aceptación de alarmas, apertura de puertas, etc.) al sistema que se controla.

Central Receptora de Alarmas (CRA): Instalación dedicada a la recepción, verificación y gestión de señales de alarma provenientes de sistemas de seguridad instalados en distintas ubicaciones, permitiendo una respuesta rápida ante incidentes. Comprende el conjunto de dispositivos, redes, aplicaciones y bases de datos, que permiten recibir la información de múltiples sistemas de seguridad, ubicados de forma remota (imágenes, alarmas, registros de acceso, etc.) para su presentación a los operadores del sistema, el archivo de los registros correspondientes y, en su caso, el envío de comandos de actuación (posicionamiento de cámaras, aceptación de alarmas, apertura de puertas, etc.) a los sistemas que se controlan. Referido también al prestador de servicios de recepción y respuesta de alarmas.

Ciberamenaza: Cualquier actividad maliciosa realizada en el ciberespacio con la intención de comprometer la seguridad de sistemas de información, redes o dispositivos.

Ciberriesgos: Probabilidad de que una organización o individuo sufra pérdidas financieras, daños reputacionales o interrupciones operativas debido a incidentes cibernéticos.

Ciberseguridad: Conjunto de actividades dirigidas a proteger el ciberespacio contra el uso indebido del mismo, defendiendo su infraestructura tecnológica, los servicios que prestan y la información que manejan.

Cifrado *at rest* (en reposo): Técnica o tecnología (ya sea de *software* o *hardware*) que se utiliza para cifrar todos los datos almacenados en un dispositivo.

Codificador: En el entorno de la video vigilancia, es un dispositivo que permite digitalizar flujos de vídeo de cámaras analógicas e incorporarlos a la red de datos IP.

Controlador de puerta: Referido al sistema de control de accesos, es un dispositivo que supervisa y controla los elementos instalados en la puerta (sensores, lectores, cerradura, etc.) y aplica las reglas de acceso de acuerdo con lo programado, comunicando con el *software* de gestión a través de redes de datos.

Confidencialidad: Propiedad que garantiza que la información no sea accesible o divulgada a individuos, entidades o procesos no autorizados.

Cookies: Pequeños archivos de datos enviados desde un sitio web y almacenados en el navegador del usuario, que permiten recordar información sobre la visita y facilitar la identificación del usuario en sesiones sucesivas .

Cortafuegos: Dispositivo de red físico o lógico que se utiliza para permitir, denegar o analizar las comunicaciones entre redes de datos, de acuerdo con las políticas de seguridad de la organización o del usuario.

DDoS (*Distributed Denial of Service***)**: Ataque de denegación de servicio (DoS) que se realiza utilizando múltiples puntos de ataque simultáneamente.

Disponibilidad: Propiedad que garantiza que los sistemas y la información estén accesibles y utilizables por los usuarios autorizados cuando lo requieran.

DMZ (Zona Desmilitarizada): Subred con un nivel de protección intermedio entre dos áreas de seguridad diferentes, que actúa como zona intermedia entre una red interna segura y una red externa insegura, como Internet.

DoS (*Denial of Service***)**: Acción de impedir el acceso, estando autorizado, a recursos o retrasar las operaciones.

DPD: Delegado de Protección de Datos. Garante del cumplimiento de la normativa de protección de datos en las organizaciones.

Entornos ciberseguros: Conjunto de instalaciones de un sistema que tienen medidas de ciberseguridad que le confieren un cierto nivel de protección frente a ataques cibernéticos.

Firmware: *Software* integrado en dispositivos de *hardware* que controla sus funciones básicas y que puede ser actualizado para corregir vulnerabilidades o mejorar su rendimiento.

Integridad: Propiedad que asegura que la información y los sistemas son exactos y completos, y no han sido alterados de forma no autorizada.

IoT (Internet of things): Internet de las cosas. Dispositivos u objetos cotidianos que se encuentran conectados entre sí o a Internet.

Malware: *Software* malicioso diseñado para dañar o infiltrarse en sistemas informáticos sin el conocimiento o consentimiento del usuario.

Ransomware: Código malicioso para secuestrar datos, una forma de explotación en la cual el atacante encripta los datos de la víctima y exige un pago por la clave de descifrado.

RGPD: REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

Salvaguardas: Prácticas, procedimientos o mecanismos que tratan y mitigan los riesgos. Medidas de ciberseguridad.

SaaS (*Software as a Service*): Modalidad de explotación de un *software* que implica un pago recurrente durante el tiempo en que se utiliza en lugar de un pago por adquisición de licencias y *hardware*. Habitualmente este *software* está alojado en la nube.

Seguridad física: Conjunto de medidas usadas para proporcionar protección física a los bienes y personas contra amenazas intencionadas o accidentales.

Seguridad privada: Ámbito de disposiciones regulatorias, empresas de prestación de servicios, actividad interna de empresas para su propia protección, y órganos de la Administración, que tratan sobre las funciones de Seguridad, definidas como tal en la Ley de Seguridad Privada (Ley 5/2014 de 4 de abril).

Sistema de Seguridad Física (SSF): conjunto de dispositivos, tecnologías y procedimientos destinados a proteger instalaciones, personas y activos físicos contra amenazas como intrusión, robo o vandalismo.

Spyware: Programa espía. Tipo de *software* malicioso que se usa para recoger información sobre una persona o empresa, o información referente a equipos o a redes, sin su conocimiento o consentimiento.

Vulnerabilidad: Debilidad o defecto en un sistema, aplicación o red que puede ser explotado por una amenaza para comprometer la seguridad.

ANEXOS

CATÁLOGO DE AMENAZAS

Categoría de la amenaza	Código	Amenaza (Magerit 3.0)	Amenaza (Interoperable EU Risk Management Toolbox)	Definición
De origen industrial [I]	[I.10]	Degradación de los soportes de almacenamiento de la información	Media/equipment degradation	La degradación de los soportes de almacenamiento compromete la **integridad** y **disponibilidad** de los datos debido al desgaste físico, obsolescencia o daños en los dispositivos. Además, afecta la confidencialidad si no se manejan correctamente los soportes dañados, exponiendo información sensible al no ser debidamente eliminados o protegidos.
	[I.11]	Emanaciones electromagnéticas	Electromagnetic emanations	Las emanaciones electromagnéticas no controladas de dispositivos electrónicos pueden comprometer la **confidencialidad** de la información, ya que podrían ser interceptadas a distancia, permitiendo el acceso a datos sensibles sin contacto físico directo con el sistema.electrónicos emiten radiaciones al exterior que pudieran ser interceptadas por otros equipos (receptores de radio) derivándose una fuga de información. Esta amenaza se denomina, incorrecta pero frecuentemente, ataque TEMPEST (del inglés “Transient Electromagnetic Pulse Standard”). Abusando del significado primigenio, es frecuente oír hablar de que un equipo disfruta de "TEMPEST protection", queriendo decir que se ha diseñado para que no emita, electromagnéticamente, nada de interés por si alguien lo captara. No se contempla en esta amenaza la emisión por necesidades del medio de comunicación: redes inalámbricas, enlaces de microondas, etc. que estarán amenazadas de interceptación.

Categoría de la amenaza	Código	Amenaza (Magerit 3.0)	Amenaza (Interoperable EU Risk Management Toolbox)	Definición
Errores y fallos no intencionados [E]	[E.1]	Errores de los usuarios	User errors	Los errores de usuario afectan la **integridad** y **disponibilidad** de la información, ya que acciones involuntarias como el borrado, modificación incorrecta o acceso no autorizado pueden alterar o eliminar datos críticos, comprometiendo la continuidad y seguridad de los sistemas.
	[E.2]	Errores del administrador	System/security administrator errors	Los errores de los administradores de sistemas o seguridad pueden impactar gravemente la **confidencialidad**, **integridad** y **disponibilidad** de la información, ya que una configuración incorrecta o una acción errónea en sistemas críticos puede abrir vulnerabilidades, provocar fallos de seguridad o interrumpir servicios esenciales.
	[E.3]	Errores de monitorización (log)	Monitoring errors (logs)	Los errores en la monitorización de logs en sistemas de seguridad física, como CCTV, controles de acceso y alarmas, pueden comprometer la **integridad y disponibilidad** de los registros de eventos de seguridad. Esto afecta la capacidad de detectar incidentes y rastrear actividades sospechosas, dejando vulnerables los sistemas físicos ante posibles intrusiones o fallos de seguridad.
	[E.4]	Errores de configuración	Configuration errors	Los errores de configuración en sistemas de seguridad física, como CCTV, controles de acceso y alarmas, pueden comprometer la **confidencialidad**, **integridad** y **disponibilidad** de estos sistemas. Una configuración incorrecta puede dejar puntos de acceso desprotegidos, permitir accesos no autorizados o causar fallos en la captura y almacenamiento de eventos de seguridad.
	[E.7]	Deficiencias en la organización	Organisational deficiencies	Las deficiencias organizativas en la gestión de los sistemas de seguridad física (SSF) pueden comprometer la **eficacia** de la seguridad general. La falta de procedimientos claros, asignación de roles o formación adecuada aumenta el riesgo de errores operativos y vulnerabilidades, dejando los SSF expuestos a incidentes y fallos de protección.

Categoría de la amenaza	Código	Amenaza (Magerit 3.0)	Amenaza (Interoperable EU Risk Management Toolbox)	Definición
Errores y fallos no intencionados [E]	[E.8]	Difusión de *software* dañino	Malware diffusion	La propagación de *software* malicioso en sistemas de seguridad física (SSF) puede comprometer la **confidencialidad, integridad** y **disponibilidad** de estos sistemas, permitiendo acceso no autorizado, alteración de registros o incluso la desactivación de componentes críticos, lo cual debilita la protección de instalaciones.
	[E.9]	Errores de [re-] encaminamiento	(Re)routing errors	Los errores en el encaminamiento o reenrutamiento de datos en sistemas de seguridad física (SSF) pueden afectar la **disponibilidad** e **integridad** de la información transmitida, provocando retrasos, pérdida de datos críticos o envío incorrecto de información, lo cual dificulta la supervisión y respuesta ante incidentes de seguridad.
	[E.10]	Errores de secuencia	Sequence errors	Los errores de secuencia en sistemas de seguridad física (SSF) pueden afectar la **integridad** y **eficacia** de los procedimientos de seguridad, al ejecutar eventos en un orden incorrecto. Esto puede resultar en el mal funcionamiento de procesos críticos, como el acceso a áreas restringidas o la activación de alarmas, comprometiendo la seguridad del entorno.
	[E.14]	Escapes de información		Los escapes de información en sistemas de seguridad física (SSF) comprometen la **confidencialidad** de datos sensibles, exponiendo detalles como configuraciones de seguridad, ubicaciones de cámaras o credenciales de acceso. Esta filtración puede facilitar intrusiones o sabotajes, poniendo en riesgo la efectividad de los SSF.
	[E.15]	Alteración accidental de la información	Accidental alteration of the information	La alteración accidental de información en sistemas de seguridad física (SSF) afecta la **integridad** de los datos, como registros de acceso o grabaciones de CCTV, lo cual puede dificultar la reconstrucción de eventos, obstaculizar investigaciones y comprometer la capacidad de respuesta ante incidentes de seguridad.

Categoría de la amenaza	Código	Amenaza (Magerit 3.0)	Amenaza (Interoperable EU Risk Management Toolbox)	Definición
Errores y fallos no intencionados [E]	[E.18]	Destrucción de información	Destruction of information	La destrucción de información en sistemas de seguridad física (SSF) compromete la **disponibilidad** e **integridad** de datos críticos, como registros de acceso o grabaciones, lo que impide el análisis y respuesta ante incidentes de seguridad, además de dificultar la **trazabilidad** de eventos pasados.
	[E.19]	Fugas de información	Information leaks	Las fugas de información en sistemas de seguridad física (SSF) comprometen la **confidencialidad** de datos sensibles, como configuraciones de seguridad, planos de instalaciones o credenciales de acceso, lo cual podría ser explotado por actores malintencionados para evadir o sabotear las medidas de protección establecidas.
	[E.20]	Vulnerabilidades de los programas (*software*)	Software vulnerabilities	Las vulnerabilidades en el *software* de los sistemas de seguridad física (SSF) pueden comprometer la **confidencialidad, integridad** y **disponibilidad** de estos sistemas, permitiendo que atacantes exploten debilidades para obtener acceso no autorizado, manipular registros o desactivar funcionalidades críticas.
	[E.21]	Errores de mantenimiento / actualización de programas (*software*)	Defects in software maintenance / updating	Los errores en el mantenimiento o actualización del *software* en sistemas de seguridad física (SSF) pueden afectar la **disponibilidad** y **seguridad** de estos sistemas, exponiéndolos a fallos operativos o dejando vulnerabilidades sin corregir que podrían ser explotadas por atacantes.
	[E.23]	Errores de mantenimiento / actualización de equipos (*hardware*)	Defects in hardware maintenance / updating	Los errores en el mantenimiento o actualización de los equipos de sistemas de seguridad física (SSF) pueden comprometer la **disponibilidad** y **fiabilidad** de estos dispositivos, aumentando el riesgo de fallos, interrupciones en el servicio y exposición a vulnerabilidades físicas o técnicas no atendidas.

Categoría de la amenaza	Código	Amenaza (Magerit 3.0)	Amenaza (Interoperable EU Risk Management Toolbox)	Definición
Errores y fallos no intencionados [E]	[E.24]	Caída del sistema por agotamiento de recursos	System failure due to exhaustion of resources	El agotamiento de recursos en sistemas de seguridad física (SSF) puede causar la **indisponibilidad** de servicios críticos, como cámaras de vigilancia o controles de acceso, al no poder procesar la carga de trabajo, lo que deja zonas vulnerables a incidentes y afecta la continuidad de la protección.
	[E.25]	Pérdida de equipos	Retrieval of recycled or discarded media	La pérdida de equipos en sistemas de seguridad física (SSF) compromete la **disponibilidad** y **confidencialidad** de los datos, ya que dispositivos extraviados o robados pueden contener información sensible o dejar zonas sin protección, exponiendo las instalaciones a posibles amenazas.
	[E.28]	Indisponibilidad del personal	Breach of personnel availability	La indisponibilidad del personal responsable de los sistemas de seguridad física (SSF) afecta la **operatividad** y **respuesta** ante incidentes, dificultando la supervisión y el mantenimiento adecuado de los sistemas, lo cual puede dejar brechas en la seguridad y retrasar la resolución de fallos críticos.
Ataques intencionados [A]	[A.3]	Manipulación de los registros de actividad (log)	Manipulation of activity records (log)	La manipulación de los registros de actividad en sistemas de seguridad física (SSF) compromete la **integridad** y **trazabilidad** de los eventos, dificultando la detección de incidentes, la investigación de actividades sospechosas y la capacidad de auditar adecuadamente el funcionamiento del sistema.
	[A.4]	Manipulación de la configuración	Manipulation of the configuration files	La manipulación no autorizada de la configuración en sistemas de seguridad física (SSF) afecta la **integridad** y **eficacia** de las medidas de seguridad, pudiendo desactivar protecciones, alterar permisos de acceso o modificar el funcionamiento de dispositivos, lo que incrementa el riesgo de vulnerabilidades y compromete la seguridad de las instalaciones.

Categoría de la amenaza	Código	Amenaza (Magerit 3.0)	Amenaza (Interoperable EU Risk Management Toolbox)	Definición
Ataques intencionados [A]	[A.5]	Suplantación de la identidad del usuario	Masquerading of identity	La suplantación de identidad en sistemas de seguridad física (SSF) compromete la **confidencialidad** e **integridad** del acceso, permitiendo que individuos no autorizados accedan a áreas restringidas o realicen acciones en nombre de usuarios legítimos, lo cual aumenta significativamente el riesgo de intrusiones y manipulaciones no detectadas.
	[A.6]	Abuso de privilegios de acceso	Abuse of access privileges	El abuso de privilegios en sistemas de seguridad física (SSF) compromete la **integridad** y **confidencialidad** del sistema, ya que usuarios con permisos elevados pueden acceder, modificar o desactivar componentes de seguridad de manera indebida, exponiendo las instalaciones a riesgos internos y debilitando los controles de protección.
	[A.7]	Uso no previsto	Misuse	El uso no previsto de sistemas de seguridad física (SSF) afecta la **integridad** y **fiabilidad** del sistema, ya que operar dispositivos o funciones fuera de sus fines originales puede generar vulnerabilidades, provocar fallos en la seguridad o dejar zonas desprotegidas, exponiendo las instalaciones a riesgos no considerados.
	[A.8]	Difusión de *software* dañino	Malware diffusion	La difusión de *software* dañino en sistemas de seguridad física (SSF) compromete la **confidencialidad**, **integridad** y **disponibilidad** de estos sistemas, permitiendo que atacantes accedan, alteren o deshabiliten dispositivos críticos, debilitando la protección de las instalaciones y facilitando posibles intrusiones.
	[A.9]	[Re-]encaminamiento de mensajes	(Re)routing of messages	El reenrutamiento o encaminamiento incorrecto de mensajes en sistemas de seguridad física (SSF) compromete la **disponibilidad** e **integridad** de la comunicación entre dispositivos, pudiendo causar retrasos, pérdida de información crítica o desvío de datos sensibles, lo cual afecta la coordinación y efectividad de las respuestas de seguridad.

Categoría de la amenaza	Código	Amenaza (Magerit 3.0)	Amenaza (Interoperable EU Risk Management Toolbox)	Definición
Ataques intencionados [A]	[A.10]	Alteración de secuencia	Sequence alteration	La alteración de la secuencia en sistemas de seguridad física (SSF) compromete la **integridad** y **coherencia** de los procesos de seguridad, causando que eventos críticos ocurran en un orden incorrecto, lo cual puede desactivar protecciones, interrumpir el control de accesos o generar registros inexactos, debilitando la seguridad global.
	[A.11]	Acceso no autorizado	Unauthorised access	El acceso no autorizado en sistemas de seguridad física (SSF) compromete la **confidencialidad** e **integridad** del entorno, permitiendo que personas sin permiso ingresen a áreas restringidas, manipulen dispositivos o accedan a información sensible, lo cual incrementa el riesgo de intrusiones, sabotajes o robos.
	[A.12]	Análisis de tráfico	Traffic analysis	El análisis de tráfico en sistemas de seguridad física (SSF) puede comprometer la **confidencialidad** de la información, ya que al observar los patrones de comunicación entre dispositivos, un atacante podría inferir horarios, ubicaciones de cámaras y patrones de actividad, facilitando el diseño de ataques o elusión de medidas de seguridad.
	[A.13]	Repudio	Repudiation (denial of actions)	El repudio en sistemas de seguridad física (SSF) se refiere a la capacidad de un usuario de negar haber realizado una acción específica, comprometiendo la **integridad** y **trazabilidad** de los registros. Esto dificulta la responsabilidad y el seguimiento de eventos, afectando la efectividad de las auditorías y respuestas ante incidentes de seguridad.
	[A.14]	Interceptación de información (escucha)	Eavesdropping	La interceptación de información en sistemas de seguridad física (SSF) compromete la **confidencialidad** de los datos transmitidos, permitiendo a terceros no autorizados capturar comunicaciones sensibles entre dispositivos, como cámaras y controles de acceso, lo que facilita posibles intrusiones o manipulación de la seguridad.

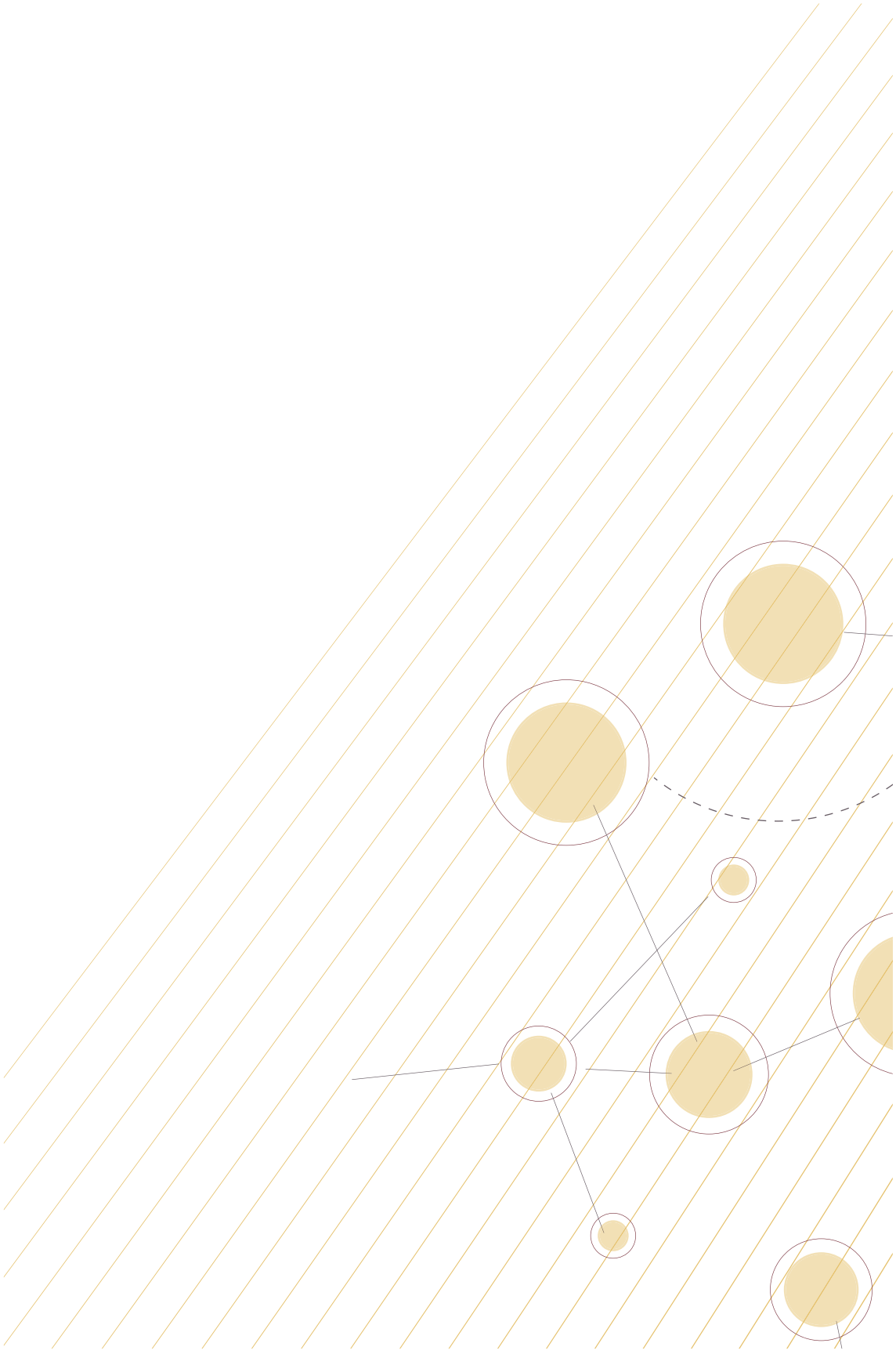
Categoría de la amenaza	Código	Amenaza (Magerit 3.0)	Amenaza (Interoperable EU Risk Management Toolbox)	Definición
Ataques intencionados [A]	[A.15]	Modificación deliberada de la información	Deliberate alteration of information	La modificación intencionada de información en sistemas de seguridad física (SSF) compromete la **integridad** y **confiabilidad** de los datos, permitiendo que actores malintencionados alteren registros, desactiven alarmas o cambien configuraciones críticas, lo cual debilita las defensas de seguridad y facilita acciones no autorizadas.
	[A.18]	Destrucción de información	Destruction of information	La destrucción de información en sistemas de seguridad física (SSF) afecta la **disponibilidad** e **integridad** de datos críticos, como registros de acceso y grabaciones, dificultando el análisis de incidentes y la capacidad de respuesta ante eventos de seguridad, además de obstaculizar futuras auditorías y verificaciones.
	[A.19]	Divulgación de información	Disclosure of information	La divulgación de información en sistemas de seguridad física (SSF) compromete la **confidencialidad** de datos sensibles, como configuraciones de seguridad, ubicaciones de dispositivos o credenciales, lo cual podría ser aprovechado por actores malintencionados para planificar intrusiones o sabotajes, debilitando la efectividad de las medidas de protección.
	[A.22]	Manipulación de programas	Tampering with software	La manipulación de programas en sistemas de seguridad física (SSF) compromete la **integridad** y **fiabilidad** del *software*, permitiendo que se alteren funcionalidades, se desactiven controles de seguridad o se introduzcan vulnerabilidades, lo cual expone los sistemas a fallos operativos y posibles intrusiones.
	[A.23]	Manipulación de los equipos	Tampering with hardware	La manipulación de equipos en sistemas de seguridad física (SSF) compromete la **integridad** y **funcionalidad** de los dispositivos, permitiendo que se alteren sus configuraciones, se desactiven componentes o se interfiera en su operación, lo cual reduce la efectividad de las medidas de protección y aumenta el riesgo de intrusión o sabotaje.

Categoría de la amenaza	Código	Amenaza (Magerit 3.0)	Amenaza (Interoperable EU Risk Management Toolbox)	Definición
Ataques intencionados [A]	[A.24]	Denegación de servicio	Denial of services	La denegación de servicio en sistemas de seguridad física (SSF) afecta la **disponibilidad** de los dispositivos críticos, como cámaras, controles de acceso o alarmas, impidiendo su funcionamiento normal. Esto deja vulnerables las instalaciones al impedir la detección y respuesta ante eventos de seguridad en tiempo real.
	[A.25]	Robo	Theft of equipment	El robo en sistemas de seguridad física (SSF) compromete la **disponibilidad** y **seguridad** de los dispositivos y datos, ya que la sustracción de equipos o componentes críticos puede dejar áreas desprotegidas, exponer información sensible y dificultar la operatividad del sistema de seguridad en su conjunto.
	[A.29]	Extorsión	Extortion	La extorsión en el contexto de sistemas de seguridad física (SSF) afecta la **confidencialidad** e **integridad** de la operación, al utilizar amenazas o coacción para obtener acceso a información sensible o manipular dispositivos, lo cual puede resultar en compromisos de seguridad, filtración de datos o debilitamiento de las defensas de la organización.
	[A.30]	Ingeniería social (picaresca)	Social engineering	La ingeniería social en sistemas de seguridad física (SSF) explota la **confianza vulnerabilidad humana** para obtener acceso no autorizado o manipular a empleados y usuarios, logrando información sensible o acceso a áreas restringidas sin necesidad de violar directamente las barreras técnicas del sistema.

Categoría de la amenaza	Código	Amenaza (Magerit 3.0)	Amenaza (Interoperable EU Risk Management Toolbox)	Definición
Amenazas relacionadas con servicios (servicios en cloud, servicios de terceras personas) [S]	[S.1]	Pérdida de gobernanza	Loss of governance	La pérdida de gobernanza en sistemas de seguridad física (SSF) compromete el **control** y la **coherencia** en la gestión de la seguridad, al no contar con supervisión efectiva, políticas claras o roles bien definidos, lo cual genera vulnerabilidades, inconsistencias en los protocolos y reduce la capacidad de respuesta ante incidentes.
	[S.2]	Bloqueo o dependencia de terceros	Lock-in	La dependencia excesiva de terceros en sistemas de seguridad física (SSF) afecta la **autonomía** y **resiliencia** de la organización, ya que problemas con proveedores o servicios externos pueden limitar el control sobre los sistemas, generar retrasos en mantenimientos y actualizaciones, y comprometer la respuesta efectiva ante incidentes de seguridad.
	[S.3]	Fallos de aislamiento	Isolation failure	Los fallos de aislamiento en sistemas de seguridad física (SSF) comprometen la **integridad** y **seguridad** del sistema al permitir que eventos, señales o interferencias de una zona afecten otras áreas protegidas. Esto puede provocar accesos no autorizados, desactivación de dispositivos o vulnerabilidades en la protección de áreas críticas.
	[S.4]	Interfaz de gestión comprometida	Management interface compromise	La interfaz de gestión comprometida en sistemas de seguridad física (SSF) pone en riesgo la **confidencialidad**, **integridad** y **control** del sistema, permitiendo que atacantes manipulen configuraciones, accedan a datos sensibles o desactiven funciones de seguridad, lo cual expone las instalaciones a intrusiones y fallos en la protección.

Categoría de la amenaza	Código	Amenaza (Magerit 3.0)	Amenaza (Interoperable EU Risk Management Toolbox)	Definición
Amenazas relacionadas con servicios (servicios en cloud, servicios de terceras personas) [S]	[S.5]	Borrado de datos no efectivo o inseguro	Insecure or ineffective deletion of data	El borrado inadecuado de datos en sistemas de seguridad física (SSF) compromete la **confidencialidad** de la información, al dejar rastros de datos sensibles en dispositivos o medios de almacenamiento, lo cual permite que actores malintencionados recuperen y utilicen esa información para explotar vulnerabilidades o planificar intrusiones.
	[S.6]	Core del servicio comprometido	Compromise of service engine	La compromisión del core del servicio en sistemas de seguridad física (SSF) afecta la **integridad**, **disponibilidad** y **confidencialidad** de todo el sistema, permitiendo que atacantes obtengan control centralizado sobre funciones críticas, desactiven medidas de seguridad, alteren configuraciones o accedan a información sensible, lo cual expone las instalaciones a serias vulnerabilidades y fallos en la protección.
	[S.7]	Citación judicial	Subpoena and e-discovery	Una citación judicial en el contexto de sistemas de seguridad física (SSF) puede afectar la **confidencialidad** y **disponibilidad** de los datos, ya que obliga a la organización a compartir registros, grabaciones o información sensible con autoridades, lo cual podría interrumpir operaciones y exponer información que, en manos equivocadas, podría comprometer la seguridad de las instalaciones.
	[S.8]	Riesgo de cambios de la jurisdicción	Risk from changes of jurisdiction	Los cambios en la jurisdicción pueden afectar la **conformidad** y **seguridad legal** de los sistemas de seguridad física (SSF), al introducir nuevas regulaciones o requisitos que obliguen a la organización a adaptar sus prácticas de manejo de datos, privacidad y control de acceso, generando posibles vulnerabilidades y exponiendo la operación a sanciones o restricciones legales.

Categoría de la amenaza	Código	Amenaza (Magerit 3.0)	Amenaza (Interoperable EU Risk Management Toolbox)	Definición
Amenazas relacionadas con servicios (servicios en cloud, servicios de terceras personas) [S]	[S.9]	Riesgo de protección de datos	Data protection risks	El riesgo de protección de datos en sistemas de seguridad física (SSF) compromete la **confidencialidad** y **cumplimiento normativo**, ya que la recopilación y almacenamiento de información personal, como grabaciones y registros de acceso, deben gestionarse conforme a leyes de protección de datos. Un manejo inadecuado puede resultar en filtraciones, sanciones legales y pérdida de confianza por parte de los usuarios.
	[S.10]	Privacidad del usuario y uso de datos para otros propósitos	User privacy and secondary usage of data	El uso de datos de sistemas de seguridad física (SSF) para fines distintos a los previstos compromete la **privacidad** y **confidencialidad** de los usuarios, al emplear información personal, como grabaciones o registros de acceso, sin consentimiento explícito. Esto puede infringir regulaciones de protección de datos, exponiendo a la organización a sanciones legales y pérdida de confianza por parte de los individuos afectados.
	[S.11]	Análisis de incidencias y apoyo forense	Incidence analysis and forensic support	La capacidad de análisis de incidencias y apoyo forense en sistemas de seguridad física (SSF) es crucial para la **integridad** y **trazabilidad** de los eventos, permitiendo investigar incidentes de seguridad de manera efectiva. Una falta de procedimientos forenses o registros completos puede dificultar la reconstrucción de eventos, limitando la capacidad de identificar responsables y aplicar medidas correctivas.
	[S.12]	Interfaces y APIs inseguras	Insecure interfaces and application programming interfaces (APIs)	Las interfaces y APIs inseguras en sistemas de seguridad física (SSF) comprometen la **confidencialidad**, **integridad** y **disponibilidad** de los datos y funciones, al permitir que actores no autorizados exploten vulnerabilidades para acceder, manipular o desactivar dispositivos y servicios críticos, lo cual expone las instalaciones a potenciales intrusiones y fallos de seguridad.



MARCO DE REFERENCIA GENERAL DE MEDIDAS DE CIBERSEGURIDAD

Para la definición del conjunto medidas de ciberseguridad, o controles, se ha utilizado como marco de referencia el conjunto de medidas establecido por el Esquema Nacional de Seguridad (ENS). Por ello, a efectos de trazabilidad se ha mantenido la codificación original, salvo para aquellas medidas codificadas como **pro.***, que son específicas de producto y no tienen correspondencia con ninguna del ENS.

La descripción de las contramedidas ha sido resumida y adaptada al caso de uso específico considerado cuando la contramedida original contemplaba aspectos generales no aplicables a este tipo de sistemas.

Marco organizativo

org.1 Política de seguridad

Deberá considerarse el sistema dentro de la política de seguridad de la organización, especialmente en lo referente a:

- El marco legal y regulatorio en el que se desarrollarán las actividades.
- Los roles o funciones de seguridad, definiendo para cada uno los deberes y responsabilidades del cargo.

org.2 Normativa de seguridad

Se dispondrá de una normativa donde se describa:

- El uso correcto de equipos, servicios e instalaciones, así como lo que se considera uso indebido.
- La responsabilidad del personal con respecto al cumplimiento o violación de la normativa.

org.3 Procedimientos de seguridad

Se dispondrá de un procedimiento donde se detalle de forma clara y precisa cómo operar los elementos del SSF:

- Cómo llevar a cabo las tareas habituales.
- Quién debe hacer cada tarea.
- Cómo identificar y reportar comportamientos anómalos.
- La forma en que se ha de tratar la información en consideración al nivel de seguridad que requiere.

org.4 Proceso de autorización

Se establecerá un proceso formal de autorizaciones para la utilización de las instalaciones.

Marco operacional

op.pl.1 Análisis de riesgos

Deberá realizarse un análisis de riesgos donde se identifiquen los activos más valiosos del sistema, las amenazas más probables, las salvaguardas que debe implementar el SSF para protegerse de dichas salvaguardas y los riesgos residuales tras aplicar dichas amenazas, que deberán ser asumibles.

op.pl.2 Arquitectura de seguridad

Se definirá cual es la arquitectura de seguridad TIC del SSF detallando, al menos, los siguientes aspectos: documentación de las instalaciones, documentación del sistema TIC (equipos, redes internas y conexiones al exterior, y puntos de acceso al sistema), esquemas de líneas de defensa (cortafuegos, DMZ, etc.), sistemas de identificación y autenticación de usuarios.

op.pl.3 Adquisición de nuevos componentes

Se establecerá proceso de adquisición de los nuevos componentes del sistema derivados de las conclusiones del análisis de riesgos y de arquitectura de seguridad

escogida. Contemplará las necesidades técnicas, de formación y de financiación, de forma conjunta.

op.pl.4 Dimensionamiento/gestión de la capacidad

Con carácter previo a la puesta en explotación, se realizará un estudio de las necesidades de procesamiento, almacenamiento de información durante el período que deba retenerse, necesidades de comunicación, de personal, de instalaciones y medios auxiliares. Se recomienda realizar este análisis de manera periódica durante todo el ciclo de vida del sistema.

op.pl.5 Componentes certificados

Todos los elementos que componen la arquitectura de seguridad del sistema deberán contar con una certificación de seguridad bajo alguna metodología reconocida por el Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información (ENECSTI) o por el Esquema Europeo de la Certificación de la Ciberseguridad.

op.acc.1 Identificación

La identificación de los usuarios del sistema se realizará asignado un identificador mediante los sistemas previstos en la normativa de aplicación. Este identificador no podrá ser compartido con otros usuarios/procesos/entidades. Un usuario deberá tener tantos identificadores singulares como roles dentro del sistema y se delimitarán los privilegios correspondientes a cada perfil.

Cada cuenta de usuario estará asociada a un identificador. Las cuentas deberán deshabilitarse cuando finalice su uso y se retendrán durante el período necesario para garantizar las exigencias de trazabilidad.

op.acc.2 Requisitos de acceso

Deberá restringirse el acceso a los recursos del sistema únicamente a usuarios con privilegios para ellos. El control de acceso se establecerá teniendo en cuenta, al menos, el **usuario** que desea acceder, el **recurso** al que desea acceder y la **operación** que desea realizar (lectura, escritura, modificación, borrado, etc.), aunque podrían añadirse otros atributos.

Particularmente, se controlará el acceso a los componentes del sistema operativo y a sus ficheros o registros de configuración.

op.acc.3 Segregación de funciones y tareas

El sistema de control de acceso se organizará de forma que se exija la concurrencia de dos o más personas para realizar tareas críticas. Además, se segregarán tareas de tal forma que, por ejemplo, las personas que autorizan y controlan no sean las mismas, de cara a impedir que una única persona pueda realizar tareas ilícitas sin ser detectado.

op.acc.4 Proceso de gestión de derechos de acceso

Los derechos de acceso de cada entidad, usuario o proceso serán gestionados y supervisados por personal habilitado para ello y atenderán a los principios de:

- Todo acceso estará prohibido, salvo autorización expresa.
- Los privilegios se reducirán al mínimo imprescindible.

op.acc.6 Mecanismos de autenticación de usuarios de la organización

Las credenciales de autenticación estarán bajo el control exclusivo del usuario y se cambiarán con una periodicidad marcada por la política de seguridad de la organización. Serán inhabilitadas cuando conste su pérdida, hayan sido comprometidas o reveladas a entidades no autorizadas o el usuario finalice su relación con el sistema.

Para el acceso se recomienda utilizar alguno de los siguientes mecanismos de autenticación:

- Contraseñas con una complejidad y robustez mínima.
- Contraseña más otro factor de autenticación tal como «algo que se tiene», es decir, un dispositivo, un certificado, una contraseña de un solo uso (OTP, en inglés) o «algo que se es».
- Certificado y PIN.

El número de intentos permitidos será limitado y deberán registrarse, a efectos de trazabilidad.

Para el acceso desde o a través de zonas no controladas (ej.: acceso que requiera el uso de internet, acceso desde fuera de la organización, etc.) se requerirá un doble factor de autenticación.

Cuando el acceso sea remoto:

- Deberá ser autorizado por la autoridad correspondiente.
- El tráfico deberá ser cifrado.

- Si la utilización no se produce de manera constante, el acceso remoto deberá encontrarse inhabilitado y habilitarse únicamente cuando sea necesario.

op.exp.1 Inventario de activos

Se mantendrá un inventario actualizado de todos los elementos del sistema, el etiquetado del equipamiento y el cableado.

Se dispondrá de herramientas que permitan visualizar de forma continua el estado de todos los equipos en la red, en particular, los servidores y los dispositivos de red y de comunicaciones.

op.exp.2 Configuración de seguridad

Todos los equipos estarán configurados de forma que se retiren cuentas y contraseñas estándar, se apliquen las reglas de mínima funcionalidad y seguridad por defecto.

op.exp.3 Gestión de la configuración de seguridad

Se gestionará de forma continua la configuración de los componentes del sistema de forma que se mantenga en todo momento la regla de "funcionalidad mínima" y "mínimo privilegio".

Se realizarán copias de seguridad de la configuración del sistema de forma que sea posible reconstruirlo en parte o en su totalidad tras un incidente.

op.exp.4 Mantenimiento y actualizaciones de seguridad

Para mantener el equipamiento físico y lógico que constituye el sistema, se atenderá a las especificaciones y recomendaciones de los fabricantes, lo que incluirá un seguimiento continuo de los anuncios de defectos.

Se dispondrá de un procedimiento para analizar, priorizar y determinar cuándo aplicar las actualizaciones de seguridad, parches, mejoras y nuevas versiones.

op.exp.5 Gestión de cambios

Se mantendrá un control continuo de los cambios realizados en el sistema, cuya implementación se planificará para reducir el impacto sobre la prestación de los servicios afectados, teniendo en cuenta la posibilidad de revertirlos ante efectos adversos.

Mediante un análisis de riesgos se determinará si los cambios son relevantes para la seguridad del sistema. Aquellos cambios que impliquen un riesgo de nivel ALTO deberán ser aprobados por el Responsable de la Seguridad.

op.exp.6 Protección frente a código dañino

Se instalará *software* de protección frente a código dañino en todos los equipos: puestos de usuario, servidores y elementos perimetrales. Se recomienda utilizar herramientas de seguridad orientadas a detectar, investigar y resolver actividades sospechosas en puestos de usuario y servidores (EDR - *Endpoint Detection and Response*) e implementar protección en tiempo real.

Solamente se podrán ejecutar aquellas aplicaciones previamente autorizadas. Todo fichero procedente de fuentes externas será analizado antes de trabajar con él.

op.exp.7 Gestión de incidentes

Se dispondrá de un proceso integral para hacer frente a los incidentes que puedan tener un impacto en la seguridad del sistema. La gestión de incidentes que afecten a datos personales tendrá en cuenta lo dispuesto en el Reglamento General de Protección de Datos, así como el resto de normativa de aplicación.

Este proceso deberá contemplar, entre otras cosas, la implantación de medidas urgentes, la asignación de recursos para resolver el incidente, así como medidas para prevenir que se repita.

op.exp.8 Registro de actividad

Se activarán los registros de actividad en los servidores y se revisarán de forma periódica, buscando patrones anormales. El sistema deberá disponer de una referencia de tiempo (*timestamp*) para facilitar las funciones de registro de eventos y auditoría.

Además, se recomienda:

- Disponer de herramientas para analizar y revisar la actividad del sistema y la información de auditoría, en búsqueda de comprometimientos de la seguridad posibles o reales.
- Disponer de un sistema automático de recolección de registros, correlación de eventos y respuesta automática ante los mismos.

op.exp.9 Registro de la gestión de incidentes

Se registrarán todas las actuaciones relacionadas con la gestión de incidentes, en especial:

- Los reportes iniciales, intermedios y finales de los incidentes, las actuaciones de emergencia y las modificaciones del sistema derivadas del incidente.

- Las evidencias que puedan comportar acciones disciplinarias sobre el personal interno, los proveedores externos o en la persecución de delitos.

op.exp.10 Protección de claves criptográficas

Las claves criptográficas se protegerán durante todo su ciclo de vida: generación, transporte, custodia durante la explotación, archivo y destrucción final.

op.ext.1 Contratación y acuerdos de nivel de servicio

Con anterioridad a la efectiva utilización de los recursos externos se establecerá contractualmente un Acuerdo de Nivel de Servicio, que incluirá las características del servicio prestado, lo que debe entenderse como "servicio mínimo admisible", así como, la responsabilidad del prestador y las consecuencias de eventuales incumplimientos.

op.ext.3 Protección de la cadena de suministro

Se analizará el impacto que puede tener sobre el sistema un incidente accidental o deliberado que tenga su origen en la cadena de suministro, se estimará el riesgo y se tomarán medidas de contención.

El plan de continuidad de la organización deberá tener en cuenta la dependencia de proveedores externos críticos. Se deberán realizar pruebas o ejercicios de continuidad, incluyendo escenarios en los que falla un proveedor.

op.ext.4 Interconexión de sistemas

Todos los intercambios de información y prestación de servicios con otros sistemas deberán ser objeto de una autorización previa. Todo flujo de información estará prohibido salvo autorización expresa.

op.nub.1 Protección de servicios en la nube

Cuando se utilicen servicios en la nube suministrados por terceros, estos deberán estar certificados bajo una metodología de certificación reconocida por el Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de Seguridad de las Tecnologías de la Información.

op.cont.1 Análisis de impacto

Se realizará un análisis de impacto que permita determinar los requisitos de disponibilidad de cada servicio (impacto de una interrupción durante un periodo de

tiempo determinado), así como los elementos que son críticos para la prestación de cada servicio.

op.cont.2 Continuidad del servicio: Plan de continuidad, cont.3 Pruebas periódicas y cont.4 Medios alternativos

Se desarrollará un plan de continuidad que establezca las acciones a ejecutar en caso de interrupción de los servicios prestados con los medios habituales. Dicho plan incluirá, entre otras cosas, una descripción de las funciones, responsabilidades y actividades a realizar, así como una previsión para coordinar la entrada en servicio de los medios alternativos, que estarán planificados y materializados en acuerdos con los proveedores.

Estos medios alternativos cubrirán los servicios contratados a terceros, así como medios propios: instalaciones, personal y equipamiento. Deberán estar disponibles en un tiempo máximo establecido.

Se recomienda realizar pruebas periódicas para localizar corregir los errores y deficiencias que pudieran existir en dicho plan.

op.mon.1 Detección de intrusión

Se dispondrá de herramientas de detección o prevención de intrusiones informáticas. Existirán procedimientos de respuesta a las alertas generadas por dicho sistema.

Medidas de protección

mp.if.1 Áreas separadas y con control de acceso, mp.if.2 Identificación de las personas

El equipamiento del Centro de Proceso de Datos (CPD) se instalará, en la medida de lo posible, en áreas separadas, específicas para su función. Se controlarán los accesos a las áreas indicadas de forma que sólo se pueda acceder por las entradas previstas.

El control de acceso identificará a las personas y registrará las correspondientes entradas y salidas[6] .

[6] Teniendo en cuenta la regulación aplicable de seguridad privada

mp.if.3 Acondicionamiento de los locales

Los locales donde se ubiquen los sistemas de información dispondrán de elementos para asegurar:

- Las condiciones de temperatura y humedad.
- La protección frente a las amenazas identificadas en el análisis de riesgos.
- La protección del cableado frente a incidentes fortuitos o deliberados.

mp.if.4 Energía eléctrica

Los locales donde se ubiquen los sistemas de información y sus componentes esenciales dispondrán de iluminación de emergencia.

En caso de fallo del suministro principal, el abastecimiento eléctrico deberá estar garantizado durante el tiempo suficiente para una terminación ordenada de los procesos y la salvaguarda de la información .

mp.if.7 Registro de entrada y salida de equipamiento

Se llevará un registro pormenorizado de cualquier entrada y salida de equipamiento esencial, incluyendo la identificación de la persona que autoriza el movimiento.

mp.per.1 Caracterización del puesto de trabajo

Para cada puesto de trabajo, relacionado directamente con el manejo de información o servicios, se definirán las responsabilidades en materia de seguridad, que estarán basadas en el análisis de riesgos. Se definirán los requisitos que deben satisfacer las personas que vayan a ocupar el puesto de trabajo.

mp.per.3 Concienciación y mp.per.4 Formación

Se realizarán acciones para concienciar regularmente al personal acerca de su papel y responsabilidad en la seguridad del sistema. En particular, se recordará periódicamente:

- La normativa de seguridad relativa al buen uso de los equipos o sistemas y las técnicas de ingeniería social más habituales.
- La identificación de incidentes, actividades o comportamientos sospechosos que deban ser reportados para su tratamiento por personal especializado.
- El procedimiento para informar sobre incidentes de seguridad, sean reales o falsas alarmas.

Además, se formará regularmente al personal en aquellas materias relativas a seguridad TIC que requiera el desempeño de sus funciones.

mp.eq.2 Bloqueo de puesto de trabajo

El puesto de trabajo se bloqueará al cabo de un tiempo prudencial de inactividad, requiriendo una nueva autenticación del usuario para reanudar la actividad en curso. Pasado un cierto tiempo, superior al anterior, se cancelarán las sesiones abiertas desde dicho puesto de trabajo.

mp.eq.4 Otros dispositivos conectados a la red

Todos los dispositivos conectados a la red que puedan tener en algún momento acceso a la información, tales como impresoras, escáneres, pantallas, dispositivos *IoT*, etc., deberán contar con una configuración de seguridad adecuada, de manera que se garantice el control del flujo definido de entrada y salida de la información.

Los dispositivos presentes en la red que dispongan de algún tipo de almacenamiento temporal o permanente de información proporcionarán la funcionalidad de borrado seguro de la información.

mp.com.1 Perímetro seguro

Se dispondrá de un sistema de protección perimetral TIC que separe el SSF. Todo el tráfico deberá atravesar dicho sistema. Todos los flujos de información a través del perímetro deben estar autorizados previamente.

mp.com.2 Protección de la confidencialidad y mp.com.3 Protección de la integridad y de la autenticidad

Se emplearán redes privadas virtuales cifradas VPN en las comunicaciones que discurran por redes fuera del propio dominio de seguridad.

Estas VPN aportarán protección de la confidencialidad e integridad, así como autenticación extremo a extremo.

Se prevendrán ataques activos garantizando que al ser detectados se activen los procedimientos previstos de tratamiento del incidente. Se considerarán ataques activos:

- La alteración de la información en tránsito.
- La inyección de información espuria.
- El secuestro de la sesión por una tercera parte.

mp.com.4 Separación de flujos de información en la red

Los flujos de información se separarán en segmentos de forma que el tráfico por la red se segregue para que cada equipo solamente tenga acceso a la información que necesita.

Dependiendo del nivel de seguridad que requiera el sistema, se podrán implementar distintos tipos de segmentación:

- Redes de área local virtuales o VLAN (nivel básico).
- Redes privadas virtuales o VPN (nivel medio).
- Segmentación física o utilizando pasarelas de intercambio seguro o diodos (nivel alto). Este tipo de soluciones tienen una alta aplicabilidad en sistemas de control de infraestructuras críticas.

La red que conforma el sistema deberá segregarse en distintas subredes contemplando como mínimo:

- Usuarios.
- Servicios.
- Administración.

Además, si se emplean comunicaciones inalámbricas, será en un segmento separado.

Para las interconexiones entre segmentos se establecerán puntos de interconexión.

mp.sw.1 Desarrollo de aplicaciones

El desarrollo de aplicaciones deberá realizarse sobre un sistema diferente y separado del de producción. Las aplicaciones se desarrollarán respetando el principio de mínimo privilegio y mínima funcionalidad, es decir, accediendo únicamente a los recursos imprescindibles para su función, y con los privilegios que sean indispensables.

Se aplicará una metodología de desarrollo seguro reconocida que tendrá en cuenta aspectos relacionados con todo el ciclo de vida.

mp.sw.2 Aceptación y puesta en servicio

Antes de pasar a producción se comprobará el correcto funcionamiento de la aplicación, en especial que se cumplen los criterios de aceptación en materia de seguridad y que no se deteriora la seguridad de otros componentes del servicio.

mp.info.1 Datos personales

Cuando el sistema trate datos personales, el responsable de seguridad recogerá los requisitos de protección de datos que sean fijados por el responsable del tratamiento, contando con el asesoramiento del DPD, así como los riesgos para los derechos y libertades de acuerdo a lo establecido en los artículos 24 y 32 del RGPD, y de acuerdo a la evaluación de impacto en la protección de datos, si se ha llevado a cabo.

mp.info.2 Calificación de la información

La política de seguridad establecerá quién es el responsable de cada información manejada por el sistema, así como los criterios que, en cada organización, determinarán el nivel de seguridad requerido.

mp.info.6 Copias de seguridad

Se realizarán copias de seguridad de la información que se considere sensible en disponibilidad. La periodicidad y los plazos de retención de estas copias de seguridad se determinarán en la normativa aplicable.

Los procedimientos de respaldo establecidos indicarán la frecuencia de las copias, los dispositivos y lugar de almacenamiento y los controles para el acceso a las copias.

mp.s.1 Protección de correo electrónico

La información distribuida por correo electrónico, así como la información de encaminamiento y el establecimiento de conexiones se protegerá.

Se protegerá a la organización frente a correo no solicitado o spam, código dañino, y código móvil tipo micro-aplicación o *applets.*

Se establecerán normas de uso del correo electrónico para el personal que contendrán limitaciones al uso como soporte de comunicaciones privadas, buenas prácticas, concienciación anti *phishing*, etc.

mp.s.2 Protección de servicios y aplicaciones web

Se realizarán auditorías de seguridad de caja negra o de caja blanca sobre las aplicaciones web durante la fase de desarrollo en donde se compruebe que están protegidos contra las siguientes amenazas:

- Acceso a la información confidencial obviando la autenticación (accesos a documentos por vías alternativas, mediante ataques a la URL).

- Ataques de manipulación de *cookies*.
- Ataques de inyección de código (escalado de privilegios, CSS)

mp.s.3 Protección de la navegación web

El acceso de los usuarios internos a la navegación por internet se protegerá del siguiente modo:

- Se establecerá una normativa de utilización. En particular, se concretará el uso permitido de conexiones cifradas.
- Se llevarán a cabo regularmente actividades de concienciación sobre el uso seguro del navegador.
- Se protegerá la información de resolución de direcciones web y de establecimiento de conexiones.
- Se protegerá contra la actuación de programas dañinos tales como páginas activas, descargas de código ejecutable, etc., previniendo la exposición del sistema a vectores de ataque del tipo *spyware*, *ransomware*, etc.
- Se establecerá una política ejecutiva de control de *cookies*, en particular, para evitar la contaminación entre uso personal y uso organizativo.
- Se registrará el uso de la navegación web.
- Se establecerá una función para la ruptura de canales cifrados a fin de inspeccionar su contenido.
- Se establecerá una lista negra de destinos vetados.

mp.s.4 Protección frente a la denegación de servicio

Se establecerán medidas preventivas frente a ataques de denegación de servicio y denegación de servicio distribuido (DoS y DDoS). Para ello, se planificará y dotará al sistema de capacidad suficiente para atender con holgura a la carga prevista y se desplegarán tecnologías para prevenir los ataques conocidos.

Además, establecerá un sistema de detección y tratamiento de dichos ataques, así como procedimientos de reacción, incluyendo la comunicación con el proveedor de comunicaciones.

Medidas aplicables a productos o servicios de seguridad (pro)

pro.1 Canales confiables

Deberán utilizarse canales de comunicación confiables con protocolos que aporten protección criptográfica de confidencialidad e integridad extremo a extremo (TLS 1.2 o superior, SSHv2, IPSec, Macsec, etc.). Se exigirá autenticación mutua entre cada uno de los elementos del sistema y solamente se establecerán canales con entidades autorizadas, rechazando el resto de conexiones.

pro.2 Auditoría

Deberán generarse registros de auditoría, cuando se produzcan los siguientes eventos:

- Cambios en la configuración del sistema.
- Gestión de usuarios (alta/baja/modificación).
- Tareas de administración del sistema.
- Cambios de claves privadas.
- Lectura, modificación o borrado de información sensible.

pro.3 Actualización confiable

Cada uno de los elementos *firmware/software* del sistema deberán implementar mecanismos de instalación y actualización confiables que garanticen su integridad y autenticidad. Se recomienda que estos mecanismos estén basados en verificación de firma digital o hashes publicados por el fabricante. En caso de no disponer de esta posibilidad, deberían implementarse procedimientos alternativos de actualización que garanticen la integridad del *firmware* o *software*. En ningún caso se instalarán actualizaciones sin tener garantías de su autenticidad e integridad.

pro.4 Gestión de usuarios. Mínimo privilegio

El sistema permitirá diferenciar dos tipos der roles: usuarios no privilegiados y usuarios privilegiados (administradores). De tal forma que a cada usuario se le asignará el rol que con el menor número de privilegios necesarios para desempeñar su funcionalidad. Únicamente los roles de usuarios privilegiados podrán llevar a cabo tareas de administración.

pro.5 Autenticación robusta

El sistema deberá identificar y autenticar a cada usuario antes de otorgarle acceso salvo a aquellas funcionalidades específicamente permitidas. Deberán implementar mecanismos que impidan ataques de autenticación de fuerza bruta.

Se recomienda que los administradores del sistema se autentiquen con doble factor, especialmente en accesos remotos o se implemente una política de contraseñas fuerte para aquellos sistemas que se encuentren instalados en áreas protegidas.

pro.6 Mecanismos antiDoS

Deberán utilizarse mecanismos anti denegación de servicio que impidan que el sistema no pueda ofrecer su funcionalidad.

pro.7 Control de acceso informático

Se establecerán políticas de control de acceso a los sistemas y la información, de tal forma que únicamente los usuarios autorizados y convenientemente identificados y autenticados puedan acceder al sistema o a la información que éste maneje.

pro.8 Protección de los equipos y servicios

Todos los elementos del sistema que se consideren críticos para el desempeño de su funcionalidad deberán implementar autochequeos de arranque y funcionamiento o ser supervisados por un sistema externo. En caso de detección de un mal funcionamiento se generarán alarmas.

pro.9 Cifrado at rest

Deberán utilizarse mecanismos de *cifrado at rest* robustos para toda aquella información de usuario que normativamente requiera ser protegida en confidencialidad.

pro.10 Firma digital

Deberán utilizarse mecanismos de firma digital para proteger la integridad y garantizar la autenticidad de la información de usuario que normativamente así lo requiera.

pro.11 Borrado seguro

Deberán implementarse mecanismos de borrado seguro de la información de usuario cuando sea requerida su destrucción de forma que esta no sea recuperable. Se recomienda utilizar borrado por sobreescritura con herramientas que generen un certificado de borrado.

pro.12 Soberanía

Para aquellos sistemas que manejen información sensible que demande un alto nivel de seguridad en confidencialidad se recomienda que se almacenen en servidores sometidos exclusivamente a la jurisdicción española.

pro.13 SLA (*Service Level Agreement*)

Para aquellos sistemas que utilicen la nube para ofrecer su servicio se definirán acuerdos a nivel de servicio (SLA), en donde se definan cuestiones como:

- Disponibilidad del sistema. Establecimiento de ratios de disponibilidad que el proveedor de servicio deberá asumir, determinación de tiempos máximos de respuesta, recuperación, etc. Con los acuerdos a nivel de servicio, el proveedor de servicio cloud se debe comprometer a ofrecer información vinculante, comprensible y transparente relativa a:
  - Disponibilidad de servicio.
  - Categoría y priorización de incidentes.
  - Tiempos de respuesta ante caídas de la operación normal, de acuerdo a la categorización (tiempo transcurrido entre que se reporta y se resuelve el incidente).
  - Tiempo de recuperación (tiempo transcurrido hasta que el incidente ha sido resuelto).
- Prestaciones: medidas relativas a la capacidad de carga.
- Consecuencias de no cumplimiento.
- Disposiciones que limiten los cambios implementados por el proveedor de servicio que puedan impactar directamente en el servicio ofrecido.

FORO
NACIONAL DE
CIBERSEGURIDAD