AES FUNDACIÓN

Guía Proyectos de seguridad electrónica: ingeniería y diseño

Índice

Guía Proyectos de seguridad electrónica: ingeniería y diseño
Elaborada por el Área de Trabajo de Ingeniería instalación y mantenimiento de AES

Nombre	Empresa	Papel en la elaboración de la guía
Alberto Alonso	AXIS	
Alberto Trigo	SECURITAS DIRECT	Colaborador
Sergio Álvarez	CLECE	Redactor
Álvaro Gil	MICROSEGUR	
Antonio Gómez	ILUNION	
David del Rey	SECURITAS	
Diego Torre	ALTER	
Antonio Fernández	ILUNION	
Francisco Teruel	TRABLISA	
Guillherme Ribeiro	ADVANCIS	
David Alonso	TIS	
José Luis Andrés	SECURITAS DIRECT	Redactor
Juan de la Fuente	PROSEGUR	Redactor / Coordinador
Manuel Pérez	SECURITAS	Redactor
Manuel Rodríguez	PROSEGUR	Coordinador
Manuel Sánchez	ESTUDIOS TÉCNICOS	Redactor
Nacho Jiménez	SECURITAS DIRECT	Colaborador
Oscar Cernuda	TECNOSEFI	
Óscar Téllez	PYCSECA	Redactor
Ricardo Cañizares	AES FUNDACIÓN	Redactor
Simeón Serra	BAUWATCH	
Julio Pérez	EULEN	Redactor
Héctor Carrasco	BAUWATCH	Redactor

Presentación

En la Industria de la Seguridad en España y como asociación decana, AES siempre ha desarrollado un papel vital. Representamos a nuestro país tanto en los Comités Nacionales y Europeos donde se crean las normas como en las dos principales asociaciones europeas como son Eurosafe y Euralarm. Todo ello es posible gracias a la dedicación y conocimiento de nuestros expertos pertenecientes a las diferentes Áreas de Trabajo que disponemos. La información es poder y por supuesto vital para la competitividad de nuestras empresas asociadas. El compromiso social es parte de nuestro ADN y para ello creamos continuamente guías, recomendaciones y publicaciones desde donde transmitimos nuestro conocimiento. En nombre de toda la Junta Directiva de AES esperamos que disfrutes de este trabajo que con tanto cariño hemos realizado.

Iñigo Ugalde Blanco –Presidente de AES.

Después de muchos meses de trabajo y dedicación, el 27 de junio de 2024 quedó registrada AES FUNDACIÓN en el Registro Nacional de Fundaciones. Uno de los objetivos establecidos para la Fundación es la difusión de los documentos elaborados por las áreas de trabajo de AES.

Es por ello por lo que todas las publicaciones de nuestras áreas de trabajo (ya tenemos incorporadas varias guías que puedes consultar sin coste en Publicaciones AES Fundación así como la Newsletter y el Boletín, han empezado a aparecer con el color naranja distintivo de la Fundación, y en el caso de Newsletter y Boletín, con una nueva numeración de segunda época.

Todo ello forma parte del desarrollo #UniversoAES y #HaciendoIndustria. Espero que esta nueva publicación que os traemos hoy sirva de ayuda y siga contribuyendo con nuestra propuesta de valor **"dinamizando la seguridad ciudadana"**

Antonio Escamilla Recio –Presidente de AES FUNDACIÓN.

Esta guía es el resultado del trabajo colaborativo desarrollado en el Área de Trabajo de Ingeniería instalación y mantenimiento de AES, fruto del esfuerzo conjunto de profesionales de distintas empresas asociadas que hemos trabajado de forma coordinada con un objetivo común: aportar al sector un documento de referencia práctico, riguroso y alineado con las mejores prácticas.

A lo largo de este documento abordamos el ciclo completo de un proyecto de seguridad electrónica, desde el análisis y la evaluación de riesgos hasta el diseño, la implementación, la operación y la mejora continua de los sistemas, incorporando aspectos clave como la integración tecnológica, la ciberseguridad y el cumplimiento normativo.

Desde AES queremos agradecer la implicación, dedicación y generosidad de todos los compañeros que han participado en la elaboración de esta guía. Confiamos en que este trabajo contribuya a reforzar el conocimiento compartido y sirva de apoyo a los profesionales y organizaciones que afrontan proyectos de seguridad electrónica.

Juan De La Fuente Sánchez
Co-coordinador del área de ingeniería, instalación y mantenimiento de AES

1 Objeto

El objeto de esta guía de Fases de Diseño para Proyectos de Seguridad Electrónica es proporcionar un marco para crear las bases para la aplicación de sistemas que protejan activos, información y personas, reduciendo riesgos, amenazas y vulnerabilidades.

Objeto de la guía de Fases de Diseño para Proyectos de Seguridad Electrónica.

El propósito principal de la guía es:

Evaluar y reducir riesgos: Crear sistemas que minimicen la exposición a riesgos, amenazas y vulnerabilidades.

Proteger activos: Salvaguardar la integridad de las personas, la información sensible y el patrimonio de una organización.

Establecer un marco de referencia: Ofrecer un conjunto de directrices, principios y procesos para el diseño e implementación de soluciones con sistemas de seguridad.

2 Alcance

Su alcance abarca desde el análisis de riesgos y la selección de tecnologías de protección física y lógica, vigilancia y control hasta la integración con otras plataformas, estableciendo medidas de control, sistemas de instalación, procedimientos para la gestión de dispositivos e incidentes, asegurando el cumplimiento de normativas para garantizar la confidencialidad, integridad y disponibilidad de los sistemas y datos.

Alcance de la guía de Fases de Diseño para Proyectos de Seguridad Electrónica

El alcance de la guía de diseño se extiende a múltiples aspectos del proyecto:

- **Análisis y evaluación de riesgos:** Identificación de riesgos, amenazas, vulnerabilidades y activos a proteger.
- **Diseño e integración de sistemas:** Selección de tecnologías como sistemas de videovigilancia, lectores biométricos, sistemas de control de acceso y cableado estructurado, y cómo integrarlas con otras plataformas.
- **Medidas de control:** Definición de controles para garantizar la confidencialidad, integridad y disponibilidad de la información y los sistemas.
- **Gestión de identidades y accesos:** Controlar quién accede a los recursos y cómo se verifica su identidad.
- **Auditoría y monitoreo:** Implementar sistemas de registro y monitoreo de actividades para la toma de decisiones y la respuesta ante incidentes.
- **Cumplimiento normativo:** Asegurar que los sistemas cumplen con las regulaciones y estándares de seguridad aplicables, como el Esquema Nacional de Seguridad (ENS).
- **Cultura de seguridad:** Fomentar la concienciación y capacitación del personal para promover una cultura de ciberseguridad dentro de la organización.
- **Ciber resiliencia:** Establecer bases para la recuperación y continuidad del negocio tras un incidente de seguridad.

3.1. El análisis de riesgos

Al igual que una buena planificación estratégica empresarial debe ser flexible y dinámica, pero siempre respetando los objetivos finales, la seguridad y por la planificación de la Seguridad Integral de la empresa, debe de adaptarse rápidamente a los cambios de su complejo entorno y proporcionar rapidez de reacción ante los diversos acontecimientos que puedan acaecer.

La elaboración de un Plan y un proyecto de Seguridad debe ir acorde a un correcto Análisis de Riesgos.

No podemos tratar el Análisis de Riesgos en materia de seguridad sin acudir como "referentes" a los documentos de normalización UNE-ISO. Estos son documentos orientados a la gestión del riesgo en general, que afectan por tanto a todo tipo de organizaciones en todas sus áreas, proyectos o actividades específicas. Por este motivo resultan muy genéricos, pues tratan de satisfacer necesidades de muy diversa índole según tipo de Organización y actividades a cubrir.

Como gestores del riesgo en el ámbito de la Seguridad Privada, hemos de ser capaces de filtrar y emplear lo que realmente resulta de aplicación y cumplimiento en la parte que nos corresponde. No obstante, todo lo desarrollado en este temario cumple con las mencionadas normativas.

Normas desarrolladas en Gestión de Riesgos de Seguridad:

- UNE-ISO 31000:2010 Gestión del Riesgo. Principios y directrices.
- UNE-EN 31010:2011 Gestión del Riesgo. Técnicas apreciación.
- UNE-ISO GUIA 73:2010 Gestión Riesgo. Vocabulario.
- UNE-ISO/TR 31400:2015 Gestión del Riesgo. Orientación para la implementación de la norma ISO 31000.
- Especificación AENOR EA0031 Sistema de Gestión del Riesgo.

Y en cuanto a otras áreas se seguridad integral corporativa, que, si bien no son específicas de la gestión del riesgo, pero le asignan un papel primordial, podemos destacar las siguientes:

- UNE-EN ISO 22301:2015 Sistema de Gestión de Continuidad de Negocio. Especificaciones.
- UNE-EN ISO 22313:2015 Sistema de Gestión de Continuidad de Negocio. Directrices.
- UNE-EN ISO 22320:2013 Protección y seguridad de los ciudadanos. Gestión de emergencias. Requisitos para la respuesta a incidentes.
- Conjunto de normas ISO 27000 (ISO27k) sobre técnicas de seguridad aplicadas a la tecnología de la información.
- ISO/IEC 27031 Gestión de la Tecnología de Información y Comunicación y obtención de Continuidad de Negocio.
- UNE 19601:2017 Compliance penal.
- UNE-ISO 19600:2015 Gestión Compliance.
- UNE-ISO 37001:2017 Antisoborno.

Definición de riesgo

Comprender la definición de Riesgo y los conceptos que abarca, es fundamental para poder identificarlo, analizarlo, valorarlo y gestionarlo.

En primer lugar, hemos de conocer como lo definen las normas UNE-ISO que bajo un prisma genérico lo desarrolla para todos los ámbitos de la Organización.

En segundo lugar, definiremos el concepto de riesgo tal y como se emplea en el ámbito de la Seguridad. Concepto mucho más concreto y de aplicación directa a los análisis, pero siempre en concordancia con los documentos de normalización internacionalmente reconocidos anteriormente mencionados.

Para acudir a las normas UNE-ISO, lo primero que debemos tener en cuenta es que a nivel empresarial el concepto resulta más amplio que el utilizado en Seguridad.

La UNE-ISO 31000:2010 Gestión del Riesgo. Principios y directrices define el Riesgo como:

Riesgo: "Efecto de la incertidumbre sobre la consecución de los objetivos"

El riesgo en la planificación de seguridad

Riesgo: "Probabilidad de materialización de una amenaza" x "Daño producido"

Evidentemente es una expresión elemental, pero si analizamos meticulosamente los procedimientos de análisis de riesgos que vamos a estudiar, comprobaremos que es el resultado final que buscan alcanzar tras diversas operaciones aritméticas y resultados parciales.

Estas metodologías de análisis previamente descomponen cada factor considerado en varios, que a su vez proceden de haber efectuado sumas o productos, se emplean tablas..., todo ello buscando descomponer los múltiples factores que influyen en el riesgo para operar con ellos, pero basándose siempre en el concepto anterior.

Podemos dar igualmente por válidas otras definiciones menos "visuales" tales como:

Riesgo: "Medida del potencial impacto (consecuencias negativas) sobre los activos de una Organización, en términos de probabilidad de ocurrencia de un evento no deseado (amenaza)".

O también:

Riesgo: "Contingencia de que un bien sufra un daño".

El Riesgo aumenta con el Impacto (daño) y con la Probabilidad de ocurrencia.

Bienes o activos

Estos términos se emplean indistintamente, según las diferentes circunstancias, entorno estudiado, etc. Realmente el término "bien" es más generalista, y el término "activo" está más relacionado con la actividad empresarial.

Así pues, si recurrimos a las definiciones clásicas nos encontramos:

- **Bien:** Toda persona, animal o cosa que en determinadas circunstancias posee una o varias cualidades benéficas, en virtud de las cuales resulta objeto de valoración.
- Recurso de la empresa o ligado a ésta, necesario para que funcione correctamente y alcance los objetivos propuestos por la Dirección.

El término "activo" resulta más amplio, dado que el posible daño que se puede causar a una Organización no siempre ha de recaer sobre bienes materiales, sino que tan importante o más que éstos resultan otros "intangibles" como la imagen corporativa, confianza generada, información sensible, cotización en bolsa, etc. En este caso términos respecto a los cuales la valoración de un posible daño resulta mucho más complicada que en el caso anterior.

Ejemplos de bienes o activos de una empresa:

- Personal.
  - Trabajadores, colaboradores, socios...
  - Clientes, consumidores...
- Activos Materiales.
  - Edificios e instalaciones...
  - Equipos.
  - Vehículos.
  - Productos, mercancías...
- Activos Inmateriales. (No inventariables, y en muchos casos relacionados con las percepciones que tienen de la empresa los grupos de interés que se relacionan con ella).
  - Imagen, prestigio, reputación...
  - Garantía de seguridad ante los inversores...
  - Actividad desempeñada.
  - Confianza generada en el cliente.
  - Información, bases de datos de clientes, estudios de patentes, etc.

Identificación del Bien: Un bien queda identificado mediante la descripción de sus elementos característicos:

- La cosa valiosa o bien propiamente dicho.
- La cualidad benéfica o característica que posee o se le atribuye al bien.
- Las circunstancias que delimitan o determinan el bien y la cualidad benéfica, así como aquellas que hacen que el bien sea objeto de nuestra responsabilidad.

Daño o impacto

Al igual que ocurría al hablar de "bienes" y "activos", encontramos los términos "daño" e "impacto". El término "daño" empleado de una forma más generalista, e "impacto" más corporativa.

- **Daño:** Toda variación que supone un bien, en virtud de la cual sufre una disminución del valor o precio de que era objeto.
- **Impacto:** Consecuencia negativa producida por la materialización de una amenaza sobre uno o varios activos.

Cabe resaltar de nuevo que no todos los daños tienen una clara valoración económica, y que su cuantificación a veces es muy complicada. ¿Cuánto vale haber perdido la oportunidad de realizar una alianza empresarial, o una fusión, etc., debido a un robo previo de información por parte de competidores? ¿Cómo cuantificamos los daños a los trabajadores, la pérdida de confianza del cliente, etc.?

Identificación del Daño: Un daño queda identificado mediante la descripción de sus elementos característicos:

- Agente dañino o causa del daño.
- La manifestación.
- Las consecuencias negativas o daño propiamente dicho.

Amenazas

Los riesgos existen porque existen las amenazas. Las amenazas en caso de manifestarse son la causa de un daño previsible. Si consideramos la probabilidad de manifestarse una amenaza y el daño que ésta podría producir, es cuando hablamos de riesgo.

La amenaza no es cuantificable (es la causa), el riesgo por el contrario sí que lo es (valor de probabilidad por daño).

Estas amenazas no siempre se materializan, pero existe una probabilidad de que así ocurra y de que en caso de materializarse produzcan un daño o perjuicio de mayor o menor magnitud en los activos de la empresa, sean del tipo que sean. Pues bien, cuando tratamos de cuantificar los aspectos anteriores, estamos realizando ya un análisis de riesgos.

Ejemplos de amenazas en el ámbito de la seguridad son: el robo, hurto, atentado, vandalismo, sabotaje, incendio intencionado, etc., sin dejar nunca de considerar inicialmente otras que puntualmente nos pudieran llegar a afectar de forma indirecta, como la caída de rayo (que pudiera afectar a los medios electrónicos), la inundación, el incendio fortuito, el corte de suministro eléctrico, etc.

Amenaza: "Toda causa previsible de daño a las personas o bienes.

Por sí sola no indica nada más que la causa, sin embargo, el concepto de Riesgo veremos que aporta más información como ya se ha adelantado.

Para facilitar los análisis existen diversos "catálogos generales de amenazas". Si bien nosotros nos centramos en las amenazas a la seguridad, no es menos cierto que todos ellos pueden resultar útiles para evitar cometer errores por omisión, dado que la materialización de una amenaza de otro tipo puede acabar afectándonos, teniendo consecuencias negativas sobre la seguridad, que podríamos haber reducido o evitado de haberla contemplado a tiempo.

Llegado este punto es importante fijarnos en que no es lo mismo amenaza que riesgo, aunque es muy frecuente ver cómo se emplea el término "riesgo" para hablar de "amenaza" o viceversa.

Así pues, sería impreciso decir: "La amenaza de atentado en el edificio es mayor que la de robo", puesto que "amenaza" es sólo una causa, siendo más correcto: "El riesgo de atentado en el edificio es mayor que el de robo", puesto que con el término "riesgo" va implícita la probabilidad de materialización de la amenaza, así como del daño producido, términos ambos cuantificables.

Se pueden utilizar "catálogos generales de amenazas" similares al que a continuación se expone. La finalidad de apoyarse inicialmente en uno de ellos no es otra que ayudar en la confección del catálogo personalizado de amenazas para nuestra Organización, de forma que no se pase por alto accidentalmente alguna de ellas y trabajemos partiendo de una información ya clasificada por su tipología.

Antisociales

- Intrusión.
- Robo.
- Hurto interno.
- Hurto externo.
- Sabotaje.
- Atraco.
- Agresiones.
- Vandalismo.
- Atentado terrorista.
- Secuestro.
- Extorsión.
- Espionaje corporativo.
- Fugas de información.
- Alteración de bases de datos.
- Fraude.
- Blanqueo de capitales.
- Falsificación de moneda.
- Tráfico de drogas.
- Amenaza de bomba.
- Incendio intencionado.

De la Naturaleza

- Inundaciones.
- Seísmos.
- Rayos.
- Nevadas.
- Heladas.
- Granizo.
- Volcanes.
- Corrimiento de tierras.
- Incendios forestales.
- Tornados
- Aludes.
- Maremotos.

Tecnológicas

- Riesgos químicos, escapes y nubes tóxicas.
- Explosión/estallido.
- Transporte de mercancías peligrosas.
- Fuego/combustión.
- Corrosión.
- Riesgos físicos.
- Efectos Mecánicos.
- Efectos Termodinámicos.
- Vibraciones.
- Radiaciones ionizantes.
- Fallo hardware.
- Fallo software.

Biológicas

- Virus.
- Bacterias.
- Enfermedades contagiosas.
- Pandemias.
- Antrópicas
- Manifestaciones.
- Huelgas.
- Grandes concentraciones de masas.
- Ferias, fiestas populares.
- Colapso y bloqueo de servicios básicos.
- Incendios urbanos.
- Colapso de estructuras.

Otras

- Cortes en suministros.
- Incumplimientos legales (LOPD, NBA, Legislación de Seguridad Privada...etc.)
- Impacto de aeronaves.
- Accidentes laborales, en el transporte...etc.
- Desprestigio comercial.
- Pérdida de imagen corporativa.

El riesgo como aspecto cuantificable

Todo Análisis de Riesgos busca obtener como resultado el grado en que se encuentra presente cada uno de ellos con la finalidad de clasificarlos y seguidamente proceder a su gestión.

En definitiva, "el riesgo es medible por diversos procedimientos matemáticos, dado que se le puede asignar un «valor relativo respecto a los demás», estimando todos dentro de un mismo escenario de estudio (proyecto, empresa u organización, instalaciones físicas, etc.). Valores que nos sirven para comparar los riesgos entre sí y priorizar su tratamiento.

Estos valores se corresponden con el producto matemático del valor de la probabilidad estimada para su ocurrencia (entre 0 y 1), por otro valor numérico correspondiente al impacto, asignado en función su magnitud o efectos, que habitualmente se obtiene de una tabla elaborada al efecto" (PASCUAL SANZ, O. "Gerencia de Riesgos en la Dirección de Proyectos").

Tal y como se detalla en el apartado correspondiente a las metodologías de análisis, cuando se va a proceder a su realización se debe seguir la siguiente secuencia:

1. Definición del Riesgo: concretar de forma inequívoca lo que vamos a analizar.
2. Análisis: Obtención de resultados bajo criterios de probabilidad y magnitud; normalmente aplicando criterios según tablas.
3. Evaluación: Cuantificación final del riesgo o grado obtenido.
4. Clasificación: Localizar el resultado numérico de la cuantificación anterior dentro de los intervalos de una tabla de asignación, para catalogarlo según diferentes terminologías. Algunos métodos denominan esta parte como valoración.

Mapas de riesgo

Para representar gráficamente los grados o niveles de riesgo a los que están expuestos los activos, se suelen emplear los llamados mapas de riesgo.

Bajo este concepto se agrupan tanto las distribuciones de un riesgo en diferentes escenarios, como diversos riesgos en uno único o diversos riesgos en una Organización determinada.

Incluso a veces la propia tabla de cálculo del grado de riesgo se emplea como mapa de riesgo, especialmente cuando se utiliza el modelo de matriz de análisis de riesgos sobre las entradas de probabilidad e impacto (sin mayor metodología). Algunos modelos de mapas de riesgo, tanto genéricos como por ejemplo para el riesgo de sabotaje serian:

Mapa de Riesgo. Distribución de un tipo de riesgo en múltiples escenarios.
(Método Cuantitativo-Mixto)

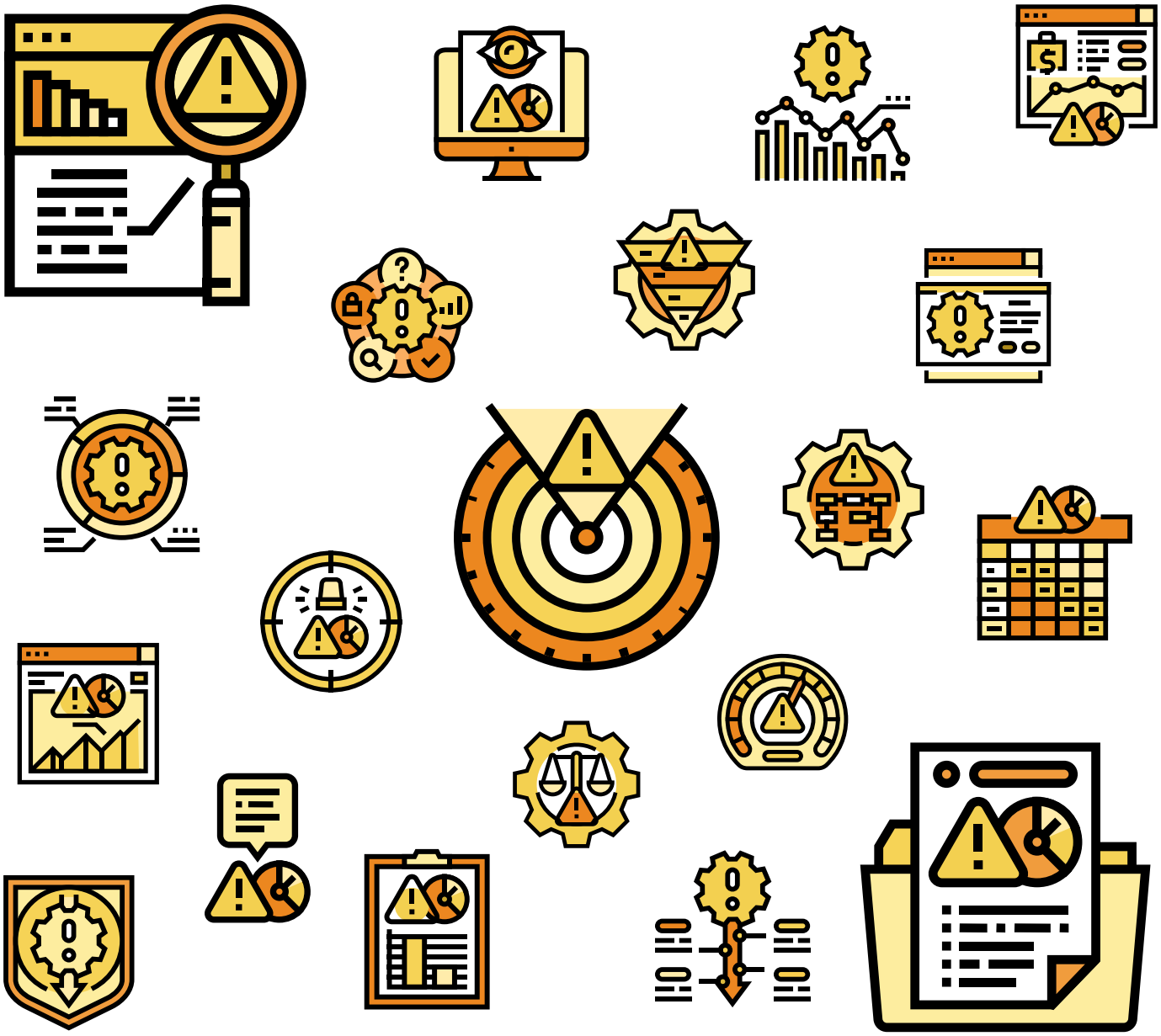
Mapa de riesgo que incluye los valores parciales de cálculo.
(Método Mosler)

Mapa de Riesgo. Múltiples riesgos en una Organización.
(Método Cuantitativo-Mixto)

Identificación de riesgos

Si acudimos a la UNE-ISO Guía 73 Gestión del Riesgo - Vocabulario, encontramos que la identificación de riesgos la define como:

"Proceso que comprende la búsqueda, el reconocimiento y la descripción de los riesgos". Continúa la norma aclarando este concepto, e indica que dicha identificación implica definir las fuentes de riesgo, los sucesos, sus causas y sus consecuencias potenciales. En el ámbito de la seguridad, esto lo trascribimos a una expresión, mediante la que explicamos los términos que lo identifican plenamente, referidos únicamente a las posibles repercusiones negativas que puede causar. Es lo que denominamos "Expresión formal del Riesgo".



Expresión formal del riesgo

Un riesgo queda identificado mediante su expresión formal, que se efectuará con ayuda de la descripción de sus elementos característicos, de forma que se facilite su comprensión:

- Bien (cosa valiosa, con sus cualidades benéficas y circunstancias).
- Daño (con la causa o agente dañino, manifestación del suceso y consecuencias negativas).

Expresión formal:

"Riesgo de que la cualidad benéfica de un bien, en unas determinadas circunstancias, pueda sufrir una manifestación, motivada por una causa con resultados de consecuencias negativas".

Metodología de identificación práctica

Realmente el procedimiento anterior es el más exhaustivo y completo, pero cuando se realizan muchos análisis puede resultar especialmente largo y tedioso, lo que normalmente termina produciendo errores tanto por parte del analista, que cae en acciones a veces demasiado repetitivas, como en quien debe interpretarlo, al exigirle un gran esfuerzo "descifrar" multitud de tablas o resúmenes. Lo importante de una definición de riesgo es plasmar documentalmente lo que se va a analizar, de forma que cualquiera que deba acceder posteriormente a los análisis pueda interpretarlos correctamente. No sirve con que inicialmente el analista tenga muy claro lo que realiza, sino que cualquiera (de su equipo auxiliar, departamento de seguridad, otros gerentes o directivos, personal auditor, etc.) debe comprender lo que realmente ha sido analizado. Está comprobado que si por ejemplo mostramos un análisis de "riego de hurto" a diferentes personas, cada una opina y obtiene conclusiones diferentes porque se imagina escenarios de análisis diferentes... varían los bienes objeto de hurto, varía la interpretación del horario y circunstancias en que se llevan a cabo los hechos, el posible personal ejecutante (interno/externo), las localizaciones donde cada persona interpreta que puede ocurrir... e incluso si quien lo interpreta no pertenece al ámbito de la seguridad, a veces varía incluso la interpretación sobre el propio hecho en sí mismo (en el ejemplo, diferentes interpretaciones sobre lo que es un hurto).

Para evitar esto podemos emplear los conceptos citados en el apartado anterior de una forma flexible, pero alcanzando la misma finalidad. Recodemos que el análisis lo podemos realizar con la profundidad que creamos conveniente, hasta llegar a obtener las conclusiones necesarias para acometer una gestión del riesgo acertada.

Las vulnerabilidades

Otro término que nos encontramos estrechamente relacionado con los anteriores, y no siempre bien utilizado es el de "vulnerabilidad". Sin riesgos no hay vulnerabilidades y sin vulnerabilidades no tenemos riesgos.

“Vulnerabilidad es la ausencia o insuficiencia de elementos de protección que garanticen la Seguridad". Una vulnerabilidad es cualquier situación que pueda desembocar en un problema de seguridad, y un riesgo es la acción específica que aprovecha una vulnerabilidad para crear un problema de seguridad. Recordemos que una vulnerabilidad puede deberse no sólo a la ausencia de un determinado medio de protección (físico o electrónico), o a la falta de medios humanos, sino también a un mal diseño de los subsistemas de seguridad, a su integración deficiente, a la ausencia de medidas organizativas, empleo de procedimientos inadecuados u obsoletos... e incluso al mero hecho de no haber logrado la plena implantación del Plan de Seguridad en la empresa o institución. Cuando una amenaza se puede materializar y causar un determinado daño, decimos que tenemos una vulnerabilidad ante un riesgo determinado. Si, por ejemplo, nuestro subsistema anti-intrusión es deficiente, al estudiar las amenazas posibles, veremos que la amenaza de intrusión nos afecta puesto que se puede materializar, es decir, estamos ante un riesgo y tenemos una vulnerabilidad.

¿En qué grado nos afecta? o ¿Cuál es su magnitud? Calculamos el riesgo mediante el correspondiente análisis, y obtenemos el nivel de riesgo estimado dentro de una escala previamente definida, que además nos permitirá obtener una graduación ordenada de todos los riesgos, y conocer la magnitud de este respecto a los demás. En el ámbito de la seguridad implantamos medidas organizativas e instalamos subsistemas de seguridad con el objetivo de reducir el riesgo. Pero los subsistemas pueden seguir teniendo vulnerabilidades, o aparecer otras nuevas según la evolución de las amenazas o del bien a proteger, por lo que habrá que seguir efectuando análisis cuantas veces sea necesario para mantener "vivo" nuestro Plan de Seguridad.

Los bienes o activos

La primera acción para comenzar un análisis de riesgos es identificar cuáles son los bienes que tenemos que proteger. Para ello nos debemos de plantear dos cuestiones, cuáles son los activos de la empresa (catálogo de activos), y de ellos cuáles son los más importantes. Dicho de otra forma, necesitamos comenzar con una priorización de activos a proteger. La priorización de los bienes no se realiza sólo por coste, sino por todos los factores que le confieren valor en la empresa, pues no hay que olvidar los activos intangibles, tales como la funcionalidad, la imagen, etc. Es decir, se debe priorizar según importancia o criticidad. Para el análisis de riesgos, un activo vale tanto como su importancia en la empresa. Por ejemplo, para una empresa el coste de uno de sus edificios puede ser el bien más valorado económicamente, sin embargo, la inutilización de este a causa de un incendio no impide que continúe su actividad desde otra ubicación. Sin embargo, quizá para esa misma empresa, si lo que pierde es la confidencialidad de sus investigaciones (información) en el desarrollo de unas determinadas patentes, puede significar tales pérdidas económicas, daño en su imagen, pérdida de confianza en sus inversores y clientes... que le lleven a la quiebra.

Una correcta identificación de bienes implica el conocimiento de la actividad empresarial, el personal, los medios, el entorno y circunstancias que le dan valor a determinados activos, etc. Se trata de realizar una recogida de información y elaborar los oportunos estudios. Pero no hemos de olvidar dos aspectos. Que bienes como la vida humana estarán siempre en primer lugar, y que existen interdependencias entre activos que pueden añadir un valor inesperado a algunos de ellos. Si un activo A depende de otro activo B, el valor de B se incrementa. Si por ejemplo resulta de la máxima importancia la prestación de un servicio a los inversores mediante un sistema informático, estarán relacionados entre sí, el personal trabajador, las bases de datos, los equipos informáticos, el suministro eléctrico, las comunicaciones y las propias instalaciones. Considerando esto, quizá el riesgo de sabotaje a cableados telefónicos, o a la instalación eléctrica tenga un impacto mayor del que hubiéramos estimado si no consideramos esta relación. Puede haber interrelaciones de todo tipo. Por ejemplo, los hurtos y robos entre el público que asiste habitualmente a un complejo de ocio pueden suponer un riesgo muy elevado cuando entre los atributos de identidad que la Organización está proyectando, nos encontramos valores como la orientación al cliente, la confianza, o la diversión en un ambiente cordial y seguro. Estudiar la imagen corporativa es algo que a menudo se olvida, o que simplemente se hace de forma intuitiva, pero que no sólo es importante para descubrir posibles interrelaciones entre activos y valorar adecuadamente posibles impactos, sino también para conseguir que el Plan de Seguridad que elaboramos se adapte lo mejor posible a nuestra empresa y su comportamiento corporativo.

Como profesional de la gestión, tras el estudio del entorno externo e interno de la Organización y para valorar convenientemente sus activos y las amenazas a las que están expuestos, resulta aconsejable conocer los siguientes puntos de su Plan Estratégico:

- Filosofía: Razón de ser de la Organización o compromiso de esta ante la sociedad y ante sus grupos de referencia (clientes, accionistas, trabajadores...). Incluye los valores o principios que rigen la actuación de los miembros de la Organización. Establece sus reglas de conducta.
- Visión: Estado que desea la dirección para el futuro.
- Misión: Propósito de la Organización.
- Objetivos estratégicos: Resultados que se desean alcanzar para lograr la misión, medibles y cuantificables en el tiempo.
- Políticas: Pautas que orientan a la toma de decisiones. Lógicamente en este ámbito, conocer la política de seguridad de la Organización resulta de vital importancia.
- Presupuestos: Recursos económicos para alcanzar los diferentes planes. En materia de seguridad, hay que tener presente que además del presupuesto en seguridad, existe otro concepto importante: el esfuerzo empresarial en esta materia, que incluye todo aquello fuera de presupuestos asignados y que supone una inversión en seguridad para la empresa. Por ejemplo, horas de trabajo del personal en plantilla o personal involucrado en el apoyo del Departamento de Seguridad, horas dedicadas a la formación del personal e implantación del Plan de Seguridad Integral (horas no trabajadas), etc. Estos aspectos no sólo se deben conocer para realizar correctamente el análisis de riesgos, sino para adecuar todo lo posible los medios y procedimientos de seguridad que implantemos posteriormente con los procedimientos organizacionales.

Además del estudio de la Organización, previo al Análisis de Riesgos, tanto para la identificación y priorización de bienes como para la identificación de amenazas, resulta de gran ayuda disponer de un Encargo Empresarial, (o Mandato Empresarial), en el que la Dirección de la Organización nos indique entre otras cosas, los objetivos que desea alcanzar en materia de seguridad, la tolerancia al riesgo, así como sus prioridades. Disponer de una relación priorizada nos servirá para seleccionar las amenazas que nos afecten, y estimar con más precisión el impacto corporativo al realizar el análisis.

Las amenazas

La identificación de amenazas es un proceso clave en el análisis de riesgos. Cualquier amenaza que no identifiquemos ahora, no será analizada posteriormente, por lo que tenemos que realizar un trabajo meticuloso. No se trata de hacer un análisis de riesgos contemplando todas las amenazas existentes, sino sólo aquellas que afecten a nuestros activos a proteger. Para ello necesitamos confeccionar un catálogo de riesgos particularizado para nuestra empresa o institución.

Debemos tener presente cuáles son los bienes o activos que pueden sufrir algún tipo de daño, y preparar un proceso de identificación y selección bien estructurado. Identificaremos causas, y consideraremos los posibles escenarios actuales y futuros para realizar los estudios con un enfoque amplio. Para ello procederemos considerando cada uno de los siguientes métodos:

- Apoyándonos en los catálogos de amenazas existentes (de una relación lo más amplia posible), de entre las cuales identificaremos aquellas que nos puedan afectar según lo explicado hasta ahora.
- Estudiando todos los incidentes de seguridad acaecidos en nuestra empresa. Recurriremos para ello a historiales, estadísticas, etc.
- Estudiando los incidentes de seguridad acaecidos en otras empresas bajo circunstancias similares.
- Mediante un análisis documental de balances, planes, informes, memorias, resultados de auditorías, pólizas de seguros, etc. Finalizada la identificación y selección de amenazas, todavía debemos considerar las posibilidades de identificación que nos ofrecen.
- El estudio de las actividades: amenazas que tiene la propia actividad de la corporación y las derivadas de sus instalaciones de riesgo (por ejemplo, ante el caso de incendio).
- La inspección física que de las instalaciones y entorno realicemos
- El tener en consideración las opiniones y experiencia del resto del personal de la empresa. Puede resultar conveniente el empleo de encuestas, entrevistas con responsables de las diversas áreas o departamentos, etc.

3.2. Métodos de análisis de riesgos

Métodos Cuantitativos

Los riesgos tienen una probabilidad de ocurrencia y unos daños perfectamente cuantificables. El análisis cuantitativo emplea valores numéricos (en lugar de las escalas descriptivas empleadas en los análisis cualitativos) tanto para las consecuencias, como para la probabilidad. Estos métodos se basan en modelos matemáticos y bases de datos de históricos. Son métodos muy objetivos, pues para todo se emplean cifras que eliminan cualquier posibilidad de valoración subjetiva por parte del analista. Estas metodologías son muy empleadas por las aseguradoras.

Métodos Cualitativos

La probabilidad de ocurrencia, y el impacto sobre los múltiples aspectos de la Organización, se estiman o valoran por el analista, asignándoles unos valores relativos de forma totalmente subjetiva basados en su experiencia, formación e información disponible. El análisis cualitativo emplea escalas descriptivas para estimar la magnitud de las consecuencias potenciales, y la posibilidad de que estas consecuencias ocurran. Resultan especialmente útiles en el ámbito de la seguridad, porque normalmente o no hay suficientes datos numéricos disponibles, o bien son inadecuados para elaborar un análisis cuantitativo.

En el ámbito de la seguridad, tenemos una seria la dificultad para obtener cifras exactas de probabilidad de ocurrencia, pues la materialización de una amenaza depende de muchos factores como el tipo de empresa, su ubicación, entorno externo (competitivo, político, legal, etc.), entorno interno, evolución de las amenazas, etc., ocurriendo lo mismo con la magnitud del posible impacto, algo difícilmente cuantificable con cifras como ya hemos explicado anteriormente. No hay dos organizaciones iguales y además el impacto a considerar no se refiere únicamente a pérdidas económicas ocasionadas sobre un bien físico tangible. Por este motivo, cuando nos estamos refiriendo a los análisis de riesgos, estamos hablando de riesgos relativos y no de riesgos absolutos. Porque lo que podemos hacer es estimar el "nivel" de un riesgo con respecto a los demás analizados, y de una forma sobre todo "cualitativa" decidir si es preciso o no tomar acciones correctivas, o bien sobre qué riesgos debemos de actuar con mayor prioridad o urgencia. Al emplear métodos cualitativos, necesitamos de personal muy preparado y competente en la materia que nos ocupa.

En esta guía vamos a desarrollar los métodos "Mosler" y Williams T. Fine, más conocido como "Cuantitativo-Mixto", este último tratando de conseguir una mayor objetividad en sus resultados mediante la asignación de valores numéricos a las escalas cualitativas y abandonando la ponderación igualitaria de sus factores. El empleo de la metodología de análisis de riesgos no debe hacerse de forma aislada, sino que debe estar plenamente integrada en la planificación de Seguridad, pudiendo distinguirse a estos efectos tres fases totalmente diferenciadas:

- Fase 1: Identificación de bienes y amenazas.
- Fase 2: Análisis y Evaluación de riesgos (aplicación de un método de análisis).
- Fase 3: Tratamiento y Gestión del riesgo.

La Fase 1 es necesaria para facilitar el correcto análisis metodológico a realizar en la Fase 2, y la Fase 3 empleando los resultados anteriores, para manejar y administrar el riesgo mediante estrategias y recursos gerenciales, así como para ayudar a definir el procedimiento más adecuado de mitigación.

Mitigación

Reducción del Riesgo alcanzada mediante la disminución de la probabilidad de materialización de su correspondiente amenaza o bien del impacto o daño que podría ocasionar.

Apreciación del riesgo

Según la norma UNE-ISO 31000, ésta incluye la Identificación o definición de este, su Análisis y su posterior Evaluación. Es la norma UNE-ISO 31010 la que incluye directrices sobre posibles técnicas de apreciación del riesgo. Tras el análisis por la correspondiente metodología, la evaluación cuantifica el riesgo o grado resultante. El análisis como herramienta técnica nos proporciona el dato.

Sin embargo, la evaluación: "nos ayuda en la toma de decisiones, determinando los riesgos a tratar y la prioridad en su tratamiento" (Norma UNE-ISO 31000).

3 Fase Inicial

Ya hemos comentado que debemos ser perfectos conocedores de la Organización, sus procedimientos, su Plan estratégico y su Política de Seguridad. Es ahora cuando estos aspectos que definen el contexto existente en la misma deben ayudar en nuestra percepción del riesgo, de forma que se pueda evaluar su aceptación o no, así como su posible forma de gestión. No debe confundirnos el hecho de que la normativa UNE-ISO establece identificación, análisis y evaluación, mientras que las metodologías que vamos a estudiar marcan la pauta con las fases de identificación, análisis, evaluación y clasificación. Lo que ocurre es que la normativa UNE-ISO incluye la clasificación como parte de la evaluación. El resultado es el mismo. De una forma genérica la normativa UNE-ISO propone que a partir del dato numérico del análisis se determinen los riesgos a tratar y su prioridad. De otra forma más pormenorizada las metodologías Mosler y Cuantitativo-Mixto establecen que a partir del dato numérico del análisis se clasifique el riesgo acudiendo a la correspondiente tabla de valoración y se encuentre cómo lo clasifican, que según el método lo hace con diferentes denominaciones, por ejemplo: muy bajo, pequeño, normal, grande o elevado en Mosler.

En definitiva, las metodologías propuestas (Mosler o Cuantitativo Mixto) ya nos orientan sobre si los riesgos son aceptables o no añadiendo una fase específica de clasificación. La normativa UNE-ISO indica que la propia fase de evaluación se determine lo mismo.

Por ejemplo, métodos de análisis basados en matrices genéricas de probabilidad e impacto no proporcionan este apoyo inicial pero la fase de evaluación sea como sea debe concluir con el mismo tipo de decisiones sobre qué riesgos se deben tratar y sus prioridades. Lógicamente y con independencia de la terminología empleada en cualquier método, debemos traducir los datos resultantes del análisis a términos de negocio para la Organización. Es lo que la norma UNE-ISO 31010 explica diciendo que hay que comparar estos niveles con los criterios de riesgo definidos cuando se estableció el "Contexto". Precisamente el contexto referido es el que abarca todos los condicionantes existentes externos e internos en el momento del análisis y quien nos servirá de referente para evaluar correctamente el riesgo.

Podemos tener una visión global estudiando la terminología que se explica conjuntamente:

1. Contexto:

   Condicionantes externos e internos que marcarán la política de gestión del riesgo.

2. Identificación del Riesgo:

   Amenazas que pueden materializarse y deben de ser analizadas.

3. Análisis de Riesgos:

   Cuantifica los riesgos de forma que posteriormente se puedan ordenar por su magnitud (Riesgo Estimado). Es la herramienta técnica que nos proporciona el "dato" para trabajar.

4. Evaluación de Riesgos:

   Valora las consecuencias en función del contexto y nos proporciona la información sobre los riesgos que hay que tratar y sus prioridades (cuáles alcanzan un nivel intolerable, cuáles son asumibles, etc.). De forma implícita realiza una clasificación del riesgo, que algunas metodologías extraen como fase independiente.

5. Tratamiento del Riesgo:

   Gestión del riesgo de forma fundamentada (según las opciones que se estudiaran en su correspondiente apartado).

6. Planes de Comunicación y Consulta:

   Procedimientos que facilitan la integración de la Seguridad en las diferentes áreas de la empresa. Están referidas a todas las consultas e intercambios de información que se han de realizar con la Organización (dirección, departamentos, equipos de trabajo, etc.) y con sus partes interesadas afectadas también por las decisiones (subcontratas, socios, inversores, clientes, accionistas, trabajadores, proveedores, etc.). Afectan especialmente al proceso de toma de decisiones conjuntas sobre la aceptabilidad o no de un riesgo (retención), posible cese de alguna actividad por su elevado riesgo... y en general a la evaluación y aceptabilidad del tratamiento de los diferentes riesgos.

7. Seguimiento y revisión:

   Integración del análisis en un procedimiento de mejora continua como cualquier otro de la organización, tal y como se explica más adelante.

3.3. Tratamiento de los riesgos

El tratamiento de cada riesgo debe realizarse en función de los resultados obtenidos tras el análisis y evaluación de estos. Hay que tener en cuenta las prioridades asignadas en función de los resultados y dentro de éstas incluso los diferentes valores de Riesgo Estimado. Por este motivo la fase de "Evaluación" del riesgo es justamente la anterior a la de "Tratamiento". Las metodologías de análisis Mosler y Cuantitativo Mixto incluyen sistemáticamente tras la fase de Evaluación una de Clasificación según criterios de valoración de una tabla en función de que entren dentro de un intervalo numérico u otro.

Y pese a que otros métodos tales como el Cuantitativo-Mixto recomienden incluso acciones correctivas según los resultados de la evaluación que proporciona el propio método, resulta obvio que aunque válido de forma orientativa, se queda totalmente corto y limitado a la hora de gestionar un conjunto de riesgos con una mínima complejidad (por ejemplo debido a su interrelación, la dependencia de los activos e incluso la forma en que un mismo medio de seguridad pueda afectar a varios riesgos simultáneamente). Además, tampoco orienta sobre la forma de abordar el tratamiento correspondiente. Este aspecto debe conocerse por las consultas realizadas a la Organización y a las partes interesadas.

3.4. Gestión del riesgo

El Análisis y Evaluación de Riesgos no son un fin en sí mismos, sino que forman parte de la planificación y diseño del sistema de seguridad, pudiendo gracias a ellos realizar una gestión metódica del riesgo de forma fundamentada. La gestión del riesgo implica tomar decisiones sobre su tratamiento en virtud de la actitud de la Organización frente al mismo. Por este motivo se ve fuertemente afectada por la tolerancia al riesgo que tenga, referida al criterio existente para soportar el riesgo después de su tratamiento. La aceptación del riesgo puede deberse en ocasiones a compromisos contractuales o decisiones políticas y directivas al más alto nivel. "La Gestión del riesgo es un componente integral de la gestión, ya que involucra actividades coordinadas relacionadas con el efecto de la incertidumbre sobre estos objetivos. Esta es la razón por la cual, para ser eficaz, es importante que la gestión del riesgo esté integrada completamente en el sistema y los procesos de gestión de la organización". (Informe UNE-ISO/TR 31004:2015 Gestión del Riesgo.

Orientación para la implementación de la Norma ISO 31000).

Debemos alinear la gestión del riesgo a la estrategia corporativa u organizacional. "La sinergia -objetivo fundamental del diseño organizativo- requiere vincular e integrar las distintas unidades de negocio y/o departamentos, eliminando las correspondientes barreras funcionales". SAEZ DE VICUÑA ANCÍN, JOSE MARÍA. El plan estratégico en la práctica. Ed. ESIC.

Existen diversas formas de tratamiento del riesgo, pudiéndose aplicar en algunos casos más de una de simultáneamente:

Transferencia

Se cede el riesgo a otra empresa u Organización, que asume la vulnerabilidad existente. Esto ocurre cuando se hace un seguro, o cuando se subcontrata a una empresa para que realice una actividad que suponga un riesgo para nuestra seguridad, como por ejemplo el transporte de fondos.

Retención

Se decide no actuar ante determinados riesgos, y se asume el posible impacto o daño causado. Supone que existe un equilibrio entre inversión en seguridad y posibles pérdidas. Normalmente esto se produce cuando nos encontramos ante muchos riesgos de diversa índole, pero cuyos daños son de escasa cuantía. Se considera entonces que la inversión en seguridad, o bien no compensa las pérdidas ocasionadas, o bien se puede retrasar en el tiempo hasta que otros riesgos de mayor nivel ya se hayan reducido. Generalmente los gastos de gestión de una compañía aseguradora resultan excesivamente costosos, y por ello tampoco se recurre al seguro, aunque debe ser objeto de valoración y estudio.

Reducción

Son acciones de mitigación dirigidas a reducir la Probabilidad de materialización de la amenaza que lo origina, o bien en ocasiones a reducir el Impacto que se pudiera producir. Este tipo de acciones son las que llevamos a cabo con la elaboración e implantación de nuestro Plan de Seguridad.

Evitar el Riesgo

Acción que en ocasiones puede suponer eliminar la actividad sujeta al riesgo, pero que en otras se puede lograr eliminando la amenaza. Por ejemplo, el riesgo de "caída del sistema informático" debido a daños causados por una inundación, se puede evitar si el cuarto de servidores se traslada de la planta sótano del edificio a la cuarta planta. Estas formas de tratamiento se pueden agrupar en dos tipos. Aquellas que buscan el control del riesgo, tales como la eliminación y la reducción y las que realizan una financiación del riesgo, como son la transferencia y la retención. En este caso tanto la transferencia como la retención implican la asignación de una dotación presupuestaria específica para pagos de seguros, contingencias, etc. Hay que tener presente que cuando implantamos un Plan de Seguridad, los riesgos se están gestionado de forma que todos ellos con su aplicación deberían permanecer en un nivel asumible para la Organización. Es decir, los riesgos residuales (que siempre van a existir) deben de quedar tras la implantación, plenamente asumibles para la Organización, que los retiene de forma consciente. Denominamos riesgo intrínseco a aquel analizado de forma previa a la aplicación de medidas de seguridad y riesgo residual el estimado tras el correspondiente tratamiento del riesgo o medidas de seguridad implantadas. Por tanto, el riesgo residual ha de ser menor que el intrínseco medido antes de la aplicación de controles para la reducción de la probabilidad o el impacto. Excepcionalmente puede darse el caso de que el un determinado riesgo residual no sea justamente el deseable (por resultar demasiado elevado), en cuyo caso quedará pendiente de tratamiento con máxima prioridad. De darse esta circunstancia se debe informar y justificar convenientemente.

En cualquier caso, siempre hay que tener una monitorización continua de los riesgos dado que un simple cambio en el contexto puede incrementarlos exponencialmente de forma desapercibida. El coste total del riesgo sería la suma de los costes que suponen:

- Las primas de los seguros.
- Las transferencias o cesiones de actividades a otras empresas.
- Las pérdidas ocasionadas por el riesgo retenido.
- Las inversiones totales en personal y/o medios de seguridad.
- El mantenimiento de los sistemas de seguridad.
- La propia administración del programa de gerencia de riesgos, gastos en peritación y ajustes de reclamaciones, pérdidas en caso de siniestro, etc.

Vemos que, desde el punto de vista de la seguridad en toda su extensión, pese a lo que podría parecer a priori, la gestión del riesgo no se limita únicamente a su reducción, sino que incluye todas las posibilidades que hemos mencionado. Se debe insistir una vez más, en que, para actuar sobre el riesgo de forma óptima y eficaz, el resultado del análisis debe incardinarse en el proceso de gerencia del riesgo empresarial, lo que obliga a una estrecha relación entre el director de Seguridad (experto en los riesgos de su competencia) y quienes tengan la responsabilidad de su aseguramiento o de asumir la retención. No olvidemos tampoco que la disponibilidad de determinados sistemas de seguridad puede tener una repercusión directa en el aseguramiento modificando la prima.

3.5. Seguimiento y revisión

El Seguimiento del Riesgo consiste en una vigilancia rutinaria del contexto interno y externo, así como de todos los factores cuyas variaciones puedan implicar cambios en el resultado de los análisis realizados o en la eficacia de su tratamiento. Es un proceso sistemático que nos obliga a realizar nuevos análisis una vez se detectan posibles cambios que puedan afectar al resultado final. La Revisión del Riesgo abarca comprobaciones bien esporádicas o de forma periódica que se realizan para verificar que no se han producido cambios no detectados, o bien cuando se tiene conocimiento de modificaciones de cualquier tipo, que pudieran dejar desactualizados los análisis existentes.

"El seguimiento y la revisión están dirigidos a aportar seguridad razonable de que los riesgos se gestionan adecuadamente, a identificar deficiencias en la gestión del riesgo, y a identificar oportunidades de mejora de la gestión de los riesgos" (UNE-ISO/TR 31004 Gestión del riesgo. Orientación para la implementación de la Norma ISO 31000).

El seguimiento y la revisión resultan especialmente útiles cuando:

- Aparecen riesgos emergentes.
- Se producen cambios en el entorno interno o externo.
- Los controles pierden su eficacia.
- Se desean sacar conclusiones de incidentes ocurridos.

Para que el seguimiento y la revisión de la gestión de riesgos sean eficaces, hay que planificar cómo y cuándo se realizarán los controles de comprobación, designar responsables y establecer los protocolos de comunicación necesarios.

3.6. Nivel de justificación

Una vez analizados los riesgos y concretados los medios necesarios para reducirlos, este método nos proporciona un criterio sobre la posible justificación o no de las acciones correctoras e inversiones que vamos a realizar. Para ello emplea una expresión matemática que relaciona el valor de los medios de seguridad, su coste y el grado de corrección del riesgo:

$$J = R / (CM \times FC)$$

J: Justificación
R: Riesgo ($R = P \times E \times C$)
CM: Coste de los medios
FC: Factor de corrección

Evidentemente la justificación es mayor cuanto mayor sea el riesgo, menor el coste de los medios empleados, y menor sea el FC o factor de corrección. Para introducir los valores CM y FC acudimos al empleo de las correspondientes tablas.

Con todos los parámetros ya definidos y cuantificados, podemos calcular el nivel de la justificación (J): $J = R / (CM \times FC)$ y en función de este valor obtener el correspondiente criterio sobre nuestra decisión:

Nivel de justificación	Decisión
$0 \leq J < 10$	No se justifican acciones correctoras.
$10 \leq J < 20$	Zona de dudas, revisar CM y FC.
$20 \leq J$	Se justifican las acciones correctoras

3.7. Obligatoriedad del análisis de riesgos

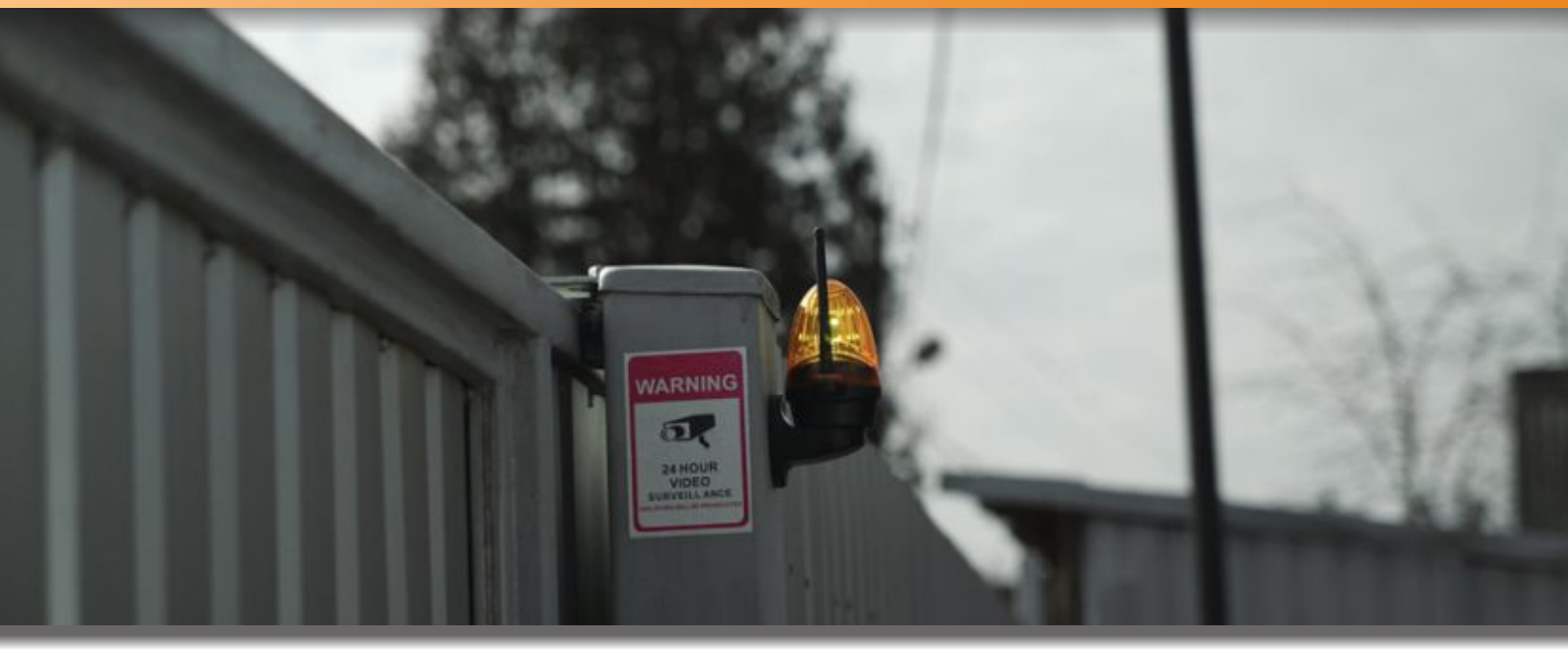
Cuando elaboramos un diseño de un sistema de seguridad, así como en cada una de sus revisiones e incluso en sus posibles auditorias, hemos de apoyarnos obligatoriamente en una evaluación previa de los riesgos existentes.

Este análisis siempre será previo a la toma de decisiones en materia de seguridad y en muchas ocasiones resultará incluso conveniente repetirlo tras nuestra labor de planificación (adecuación de medios, implantación de procedimientos, etc.) para verificar resultados y obtener información sobre la mejora obtenida o sobre el nivel de riesgo residual que permanece.

Resulta evidente que cuando pensamos en un sistema de seguridad, en su efectividad, diseño, mejora, ampliación, etc., de una forma intuitiva ya estamos efectuando un pequeño e informal "análisis de riesgos" para encontrar la solución más adecuada. A veces nos parece evidente lo que hay que hacer. ¿Debemos entontes efectuar igualmente un análisis de riesgos?

La respuesta es siempre afirmativa, considerando que:

- Mediante un enfoque metodológico es como mejor evitamos cometer errores.
- Es la única forma en la que podemos cuantificar un riesgo respecto a los demás analizados, y establecer así prioridades de inversión o esfuerzo empresarial en materia de seguridad.
- Posibilita una adecuada gestión del riesgo, proporcionando criterios para la justificación de inversiones en medios de seguridad.
- Evita las discusiones especulativas al proporcionar cifras justificativas.
- Nos ayuda a tomar decisiones lo más objetivas posibles.



4.1. Enfoque del diseño por capas

El diseño por capas de un sistema de seguridad contra intrusión física es una estrategia integral que busca proteger propiedades mediante la implementación de múltiples niveles de defensa. Este enfoque se basa en la idea de que no existe una única solución que pueda garantizar la seguridad total, por lo que se combinan diversas técnicas y tecnologías para crear un entorno seguro. A continuación, se presentan los clave sobre este diseño:

- Capa de disuasión: La primera línea de defensa es la disuasión, que busca prevenir la intrusión antes de que ocurra. Esto incluye medidas visibles como cámaras de seguridad, iluminación exterior, letreros de advertencia y cercas. La presencia de estos elementos puede hacer que los intrusos potenciales lo piensen dos veces antes de intentar ingresar a la propiedad.
- Capa de detección perimetral: Esta capa se centra en detectar cualquier intento de intrusión en el perímetro de la propiedad. Incluye sensores de movimiento, barreras infrarrojas y sistemas de alarma perimetral. Estos dispositivos alertan a los centros de control o CRA´s en caso de una posible intrusión, permitiendo una respuesta rápida.
- Capa de control de acceso: Una vez que se ha detectado una intrusión, es crucial controlar el acceso a las áreas más sensibles de la propiedad. Esto incluye el uso de cerraduras reforzadas, puertas y ventanas de seguridad, y sistemas de control de acceso electrónico como tarjetas de proximidad o códigos de acceso. Estas medidas dificultan el ingreso de intrusos a las áreas protegidas.
- Capa de monitorización y vigilancia: Esta capa implica la vigilancia continua de la propiedad para identificar cualquier actividad sospechosa. Los sistemas de cámaras de seguridad, tanto internas como externas, y sistemas de detección de intrusión, permiten visualizar en tiempo real y grabar las incidencias en zonas interiores y/o restringidas, para que en caso necesario, los servicios de vigilancia remotos y CRA´s pueden alertar a las fuerzas y cuerpos de seguridad en caso de una intrusión confirmada.

Perímetro Exterior

Evaluación de barreras físicas y electrónicas.

La integración de sistemas de seguridad física en la capa de detección perimetral es esencial para crear una barrera efectiva contra intrusiones. Estos elementos físicos proporcionan una primera línea de defensa que, combinada con tecnologías de detección, mejora significativamente la seguridad de la propiedad.

- Muros y cercas: Los muros y cercas son estructuras físicas que delimitan el perímetro de la propiedad y dificultan el acceso no autorizado. Para aumentar su eficacia, se pueden equipar con sensores de vibración que detectan cualquier intento de escalamiento o manipulación. Además, las barreras infrarrojas pueden instalarse a lo largo de estas estructuras para que se activen alarmas al ser cruzado el perímetro.

- Puertas y portones: Las puertas y portones de seguridad son cruciales para controlar el acceso a la propiedad. Estas estructuras pueden estar reforzadas con materiales resistentes y equipadas con cerraduras electrónicas que requieren códigos de acceso o tarjetas de proximidad. Sensores de movimiento y cámaras de seguridad pueden instalarse cerca de estas entradas para monitorizar cualquier actividad sospechosa y activar alarmas en caso de intento de intrusión.

- Ventanas de seguridad: Las ventanas son puntos vulnerables en cualquier propiedad. Para protegerlas, se pueden utilizar vidrios reforzados y cerraduras adicionales. Sensores de vibración y de apertura pueden instalarse en las ventanas para detectar cualquier intento de manipulación. Además, las cámaras de seguridad pueden monitorizar las áreas cercanas a las ventanas para proporcionar una supervisión continua.

- Iluminación exterior: La iluminación exterior es una medida disuasoria efectiva. Luces de seguridad con sensores de movimiento pueden instalarse alrededor del perímetro de la propiedad. Estas luces se activan cuando detectan movimiento, iluminando el área y disuadiendo a los intrusos. La iluminación adecuada también mejora la visibilidad de las cámaras de seguridad durante la noche.

- Barreras físicas adicionales: En propiedades más grandes, se pueden utilizar barreras físicas adicionales como bolardos y barreras automáticas para controlar el acceso de vehículos. Estas barreras pueden integrarse con sistemas de control de acceso electrónico y sensores de movimiento para proporcionar una protección adicional.

Sistemas de detección de intrusos en el perímetro.

Para identificar cualquier intento de intrusión en el perímetro de la propiedad se incluyen diversos dispositivos y tecnologías diseñados para alertar a CRA´s o servicios de vigilancia:

- Sensores de movimiento: Estos sensores se instalan en puntos estratégicos alrededor del perímetro de la viviendas, locales o edificios, como jardines, entradas y patios. Detectan el movimiento de personas y activan alarmas o luces para disuadir a los intrusos.

- Barreras infrarrojas: Estas barreras consisten en un emisor y un receptor. Si alguien cruza la línea imaginaria que los une, se activa una alarma.

Estos sistemas se pueden combinar (movimiento + barreras infrarrojas), para crear una red de detección alrededor del inmueble a proteger.

Acceso al Edificio

La capa de control de acceso al edificio se encarga de gestionar y supervisar quién puede entrar y salir del edificio, así como de verificar la identidad de las personas que acceden.

Control de accesos en entradas y salidas.

El control de accesos en entradas y salidas es esencial para mantener la seguridad del edificio. Este apartado incluye diversas medidas y tecnologías que regulan el flujo de personas y vehículos, asegurando que solo los individuos autorizados puedan acceder a la propiedad.

- Puertas y portones de seguridad: Las puertas y portones son los puntos de acceso principales al edificio. Para garantizar su seguridad, se utilizan cerraduras electrónicas y mecánicas de alta resistencia. Las cerraduras electrónicas pueden requerir códigos de acceso, tarjetas de proximidad o incluso datos biométricos para desbloquearse. Además, los portones automáticos pueden estar equipados con sensores de movimiento y cámaras de seguridad para controlar el acceso de vehículos.

- Torniquetes y barreras físicas: En edificios comerciales y oficinas, los torniquetes y barreras físicas son comunes en las entradas principales. Estos dispositivos regulan el flujo de personas, permitiendo el acceso solo a aquellos que presentan una identificación válida. Los torniquetes pueden estar integrados con sistemas de control de acceso electrónico, como tarjetas de proximidad o lectores de huellas dactilares.

- Vigilantes de seguridad: La presencia de vigilantes de seguridad en las entradas y salidas proporciona una capa adicional de protección. Los vigilantes pueden verificar las identificaciones, realizar inspecciones visuales y responder rápidamente a cualquier incidente de seguridad. Además, pueden supervisar los sistemas de control de acceso y coordinar con las autoridades en caso de emergencia.

Sistemas de identificación y autenticación.

Los sistemas de identificación y autenticación son utilizados para verificar la identidad de las personas que acceden al edificio. Estos sistemas aseguran que solo los individuos autorizados puedan entrar, minimizando el riesgo de intrusión.

- Tarjetas de proximidad: Las tarjetas de proximidad son una forma común de identificación en edificios comerciales y residenciales. Estas tarjetas contienen un chip que se comunica con los lectores de proximidad instalados en las puertas y torniquetes. Al acercar la tarjeta al lector, se verifica la identidad del usuario y se permite el acceso. Las tarjetas de proximidad son fáciles de usar y pueden ser desactivadas rápidamente en caso de pérdida o robo.
- Lectores biométricos: Los lectores biométricos utilizan características físicas únicas, como huellas dactilares, reconocimiento facial o escaneo de iris, para autenticar la identidad de los usuarios. Estos sistemas ofrecen un alto nivel de seguridad, ya que las características biométricas son difíciles de falsificar. Los lectores biométricos pueden integrarse con otros sistemas de control de acceso para proporcionar una autenticación multifactorial.
- Códigos de acceso: Los códigos de acceso son otra forma de autenticación utilizada en edificios. Los usuarios deben ingresar un código numérico en un teclado para desbloquear las puertas. Estos códigos pueden ser cambiados regularmente para mantener la seguridad y pueden ser asignados individualmente a cada usuario para un control más preciso.

Áreas Internas

La capa de áreas internas combina medidas de seguridad física, electrónica y humana para crear un entorno seguro y controlado.

Protección de áreas críticas y sensibles.

La protección de áreas críticas y sensibles es fundamental para evitar el acceso no autorizado y proteger los activos más valiosos del edificio. Este apartado incluye diversas medidas y tecnologías que aseguran que solo las personas autorizadas puedan acceder a estas áreas.

- Puertas de seguridad reforzadas: Las áreas críticas, como salas de servidores, oficinas de alta dirección y almacenes de productos valiosos, deben estar protegidas con puertas de seguridad reforzadas. Estas puertas pueden estar equipadas con cerraduras electrónicas que requieren códigos de acceso, tarjetas de proximidad o datos biométricos para desbloquearse. Además, pueden incluir sensores de vibración para detectar cualquier intento de manipulación.
- Videovigilancia: La instalación de cámaras de seguridad en las áreas críticas permite una vigilancia continua y la grabación de cualquier actividad sospechosa. Las cámaras pueden estar conectadas a un sistema de monitorización central que supervisa las imágenes en tiempo real y envía alertas en caso de incidentes. Por ejemplo, una cámara en la sala de servidores puede ayudar a detectar y prevenir accesos no autorizados.

- Sistemas de control de acceso: Los sistemas de control de acceso electrónico, como lectores de tarjetas de proximidad y lectores biométricos, son esenciales para regular quién puede entrar en las áreas críticas. Estos sistemas registran cada acceso, proporcionando un historial detallado de quién ha entrado y salido de la zona. Esto ayuda a identificar cualquier actividad sospechosa y a tomar medidas rápidas.

Monitorización y vigilancia interna.

La monitorización y vigilancia interna es crucial para mantener la seguridad dentro del edificio. Este apartado combina medidas de seguridad física, electrónica y humana para asegurar una vigilancia continua y una respuesta rápida ante cualquier incidente.

- Cámaras de seguridad internas: incluidas en el sistema de videovigilancia, vinculadas a sistemas de detección de intrusión, o como circuito cerrado de televisión, CCTV. Las características de estas cámaras pueden ser menos robustas en cuanto a estanqueidad o elementos ambientales externos, al estar instaladas en entornos interiores.

- Sistemas de alarma: Los sistemas de alarma internos, como los sensores de movimiento y los detectores de apertura de puertas y ventanas, detectan cualquier intento de intrusión. Estos sistemas pueden estar integrados con las cámaras de seguridad y los sistemas de control de acceso para proporcionar una respuesta rápida y coordinada.

- Vigilantes de seguridad: La presencia de vigilantes de seguridad dentro del edificio proporciona una capa adicional de protección. Los vigilantes pueden realizar patrullas regulares, supervisar los sistemas de seguridad y responder rápidamente a cualquier incidente. Además, pueden coordinar con el personal de seguridad electrónica para asegurar una vigilancia efectiva.

4.2. Diseño de la Arquitectura del Sistema

El diseño de la arquitectura de un sistema de seguridad electrónica no solo establece cómo los componentes interactúan entre sí, sino que también define los parámetros de escalabilidad, robustez y eficiencia operativa del sistema. Este proceso debe considerar múltiples factores, desde las necesidades específicas del entorno hasta las tecnologías disponibles y las restricciones presupuestarias.

Identificación de Requisitos

El primer paso en el diseño de la arquitectura del sistema consiste en recopilar y analizar los requisitos específicos del proyecto. Esto incluye entender las características del entorno, como el tamaño de la instalación, el tipo de amenazas a mitigar y las normativas aplicables. Por ejemplo, una instalación industrial puede requerir monitoreo constante en áreas críticas, mientras que un edificio corporativo podría priorizar el control de acceso y la integración con sistemas de gestión de edificios (BMS).

Los requisitos funcionales, como la necesidad de grabaciones continuas, notificaciones en tiempo real y acceso remoto, deben estar claramente definidos. De igual manera, es esencial considerar las limitaciones, como el presupuesto, el espacio disponible para la instalación de equipos y la infraestructura existente.

Selección del Modelo de Implementación

Una vez definidos los requisitos, es fundamental seleccionar el modelo de implementación adecuado. Los sistemas on-premise ofrecen mayor control y personalización, pero requieren una inversión inicial significativa y un equipo técnico dedicado para su mantenimiento. Por otro lado, los sistemas basados en la nube son ideales para organizaciones que buscan flexibilidad y escalabilidad, aunque implican consideraciones adicionales de conectividad y seguridad de datos.

Las arquitecturas híbridas han ganado popularidad por su capacidad de combinar lo mejor de ambos mundos. En este enfoque, los datos críticos se procesan localmente, mientras que las funcionalidades adicionales, como análisis avanzado o almacenamiento secundario, se gestionan en la nube. Este diseño ofrece un equilibrio entre seguridad, rendimiento y costos.

Integración de Tecnologías Emergentes

La adopción de tecnologías como el Edge Computing y la inteligencia artificial está transformando el diseño de sistemas de seguridad. El Edge Computing permite procesar datos localmente en dispositivos como cámaras y sensores, reduciendo la latencia y mejorando la capacidad de respuesta. Por ejemplo, una cámara equipada con análisis de video basado en inteligencia artificial puede identificar comportamientos sospechosos en tiempo real, desencadenando alertas inmediatas sin depender de un servidor central.

La integración de inteligencia artificial también permite predecir patrones de comportamiento y optimizar la asignación de recursos. Un sistema puede analizar datos históricos para identificar puntos críticos de vulnerabilidad y recomendar ajustes en la configuración o la ubicación de los dispositivos.

Diseño Modular y Escalable

Una buena arquitectura debe ser modular y escalable, permitiendo la incorporación de nuevos componentes y funcionalidades sin afectar el rendimiento del sistema. Esto es especialmente relevante en proyectos a largo plazo, donde las necesidades pueden evolucionar con el tiempo. Por ejemplo, un diseño modular permite agregar cámaras adicionales o integrar sistemas de análisis facial sin necesidad de reemplazar la infraestructura existente.

El uso de protocolos estándar y plataformas interoperables facilita esta escalabilidad, asegurando que los nuevos dispositivos sean compatibles con los sistemas actuales. Además, un diseño escalable debe prever la capacidad de la red y los recursos de almacenamiento necesarios para manejar volúmenes crecientes de datos.

Consideraciones de Seguridad y Resiliencia

La seguridad debe ser una prioridad en el diseño de la arquitectura. Esto incluye la protección de datos mediante cifrado avanzado, la implementación de medidas de autenticación robustas y la segmentación de redes para minimizar el impacto de posibles brechas de seguridad. Adicionalmente, un diseño resiliente debe incluir redundancias, como fuentes de alimentación ininterrumpida (UPS) y enlaces de comunicación secundarios, para garantizar la continuidad operativa en caso de fallos.

El monitoreo continuo y las actualizaciones regulares también son esenciales para mantener la integridad del sistema frente a amenazas emergentes. Herramientas de gestión centralizada pueden simplificar estas tareas, permitiendo supervisar el estado del sistema y aplicar parches de seguridad de manera eficiente.

Documentación y Validación del Diseño

Una vez definido el diseño, es crucial documentarlo detalladamente. Esto incluye planos de instalación, diagramas de conexión, especificaciones técnicas de los componentes y flujos de operación. Esta documentación no solo facilita la implementación, sino que también sirve como referencia para el mantenimiento y futuras actualizaciones.

La validación del diseño debe realizarse mediante simulaciones y pruebas piloto, asegurando que cumple con los requisitos establecidos y que todos los componentes funcionan correctamente en conjunto. Esta etapa también permite identificar y resolver posibles problemas antes de la implementación completa.

4.3. Selección de Tecnologías y Equipos

Evaluación de Tecnologías

En la actualidad los proyectos de seguridad, sobre todo cuando su objetivo es la integración, abarcan otros tipos de sistemas como son:

- De protección contra incendios,
- IOT ligado a la gestión de la climatización, la iluminación, o el ahorro energético,
- De producción.
- Etc.

Por ello, en primer lugar, vamos a definir los sistemas a los que nos vamos a referir:

Detección de intrusión - Control de Accesos - Videovigilancia

Por otro lado, es conveniente diferenciar entre la selección de soluciones de centralización de estos sistemas y la selección de los sensores asociados.

Detección de Intrusión. Centralización.

Evidentemente los criterios técnicos de selección estarán ligados a características y/o funcionalidades que proporcionan cada gama de producto de centralización de cada fabricante como son número de:

- Entradas
- Salidas
- Particiones
- Usuarios
- Comunicación IP a red local para integración On site y por Fibra, 4/5G, VPN, para conexión exterior
- Comunicación con los sensores por cable o vía radio
- La disponibilidad de APIS, SDKS, protocolos para integración
- Etc.

Los sistemas de intrusión en general o se conectarán a una Central Receptora de Alarma o un Centro de Control, pero además debemos resaltar, que en estos momentos todas las soluciones están ligadas a conexión Cloud (en nube) del propio fabricante permitiendo la posibilidad de actuaciones remotas sobre los sistemas como:

- Supervisión constante de fuentes de alimentación, líneas de comunicación y de todos los elementos conectados a la central de intrusión.
- Actualización remota de firmware de la central de intrusión.
- Tele mantenimiento
- ...

Estas actuaciones remotas facilitan el correcto funcionamiento del sistema y garantizan su continua protección frente a vulnerabilidades, así como la actuación sobre el mismo desde las App previstas para trabajar con dispositivos móviles.

Pero dado que los equipos comunican con su plataforma en nube, en internet, otro punto a considerar es la necesidad o no, de comunicación segura por VPN y si la solución a seleccionar permitirá esta opción

Otro aspecto para tener en cuenta a la hora de elegir una solución de intrusión es su capacidad para incluir sistemas de Vídeo vigilancia, Control de Accesos, dispositivos Iot, etc., que permite soluciones con todos los sistemas integrados de manera sencilla. Siendo algo que cobra especial relevancia en pequeñas y medianas instalaciones pues facilita de manera sencilla toda la información de la instalación de los distintos sistemas.

Detección de Intrusión. Sensores de interior

Los criterios técnicos de selección se basarán en el escenario o elemento a proteger, de este modo tendremos que elegir entre sensores:

- De apertura, como los contactos magnéticos para puertas y ventanas
- De rotura de cristal para la protección de ventanas y escaparates
- Sísmicos e inerciales para protección de muros o cajas fuertes
- Volumétricos de Microondas, Infrarrojos Pasivos o Doble Tecnología dependiendo del área y alcance a proteger.

Cabe destacar que los sensores volumétricos con cámara incorporada son cada vez más utilizados dado que el mismo elemento facilita la imagen del momento de alarma, fundamental para poder verificar que una señal de alarma es real y desencadenar el procedimiento de actuación previsto, ganando eficiencia en centros de control y centrales receptoras de alarma.

Detección de Intrusión. Sensores de exterior

La elección del tipo de tecnología para la detección en exteriores tiene tres criterios fundamentales a considerar:

- La infraestructura ligada a su instalación
- El alcance del sensor
- La posibilidad de ser afectada su detección de eventos reales de alarma por el entorno: Condiciones meteorológicas, movimiento de vegetación, proximidad de animales...

Según el escenario se optará, entre otros, por:

- Barreras de infrarrojos
- Barreras de microondas
- Sensores enterrados de presión, radiofrecuencia, o fibra óptica
- Sensores sísmicos
- Sensores ligados a un cerramiento con valla
- Analítica de vídeo

En cada caso la tecnología a adoptar dependerá de:

- Si existe un perímetro cerrado, una valla o un muro, donde pueda ser detectado con antelación el inicio de la intrusión antes de llegar a su objetivo.
- Si deben ser cubiertas grandes superficies de terreno abierto.
- Si existen barreras arquitectónicas, desniveles, etc., que dificulten la utilización de posibles opciones.

Si bien estas soluciones han ido mejorando en efectividad, ninguna ha evolucionado tanto como la Analítica de Vídeo donde con la mejora de algoritmos, la introducción de IA para clasificación de objetos y su reducción en costes la sitúan como una de las preferidas para la detección en exterior ligada tanto a cámaras de visión convencional como de cámaras térmicas.

Control de Accesos

En el caso del Control de Accesos, una de las primeras elecciones que deberemos tomar está relacionada con la arquitectura de la solución: Ubicación de la BBDD con la información, tipo de conexión entre los elementos, tecnologías de los lectores.

- Centralización de la información. La tendencia, como en otras soluciones de la industria donde está desapareciendo el CPD local, son las soluciones Cloud (en nube) para albergar la plataforma de gestión. Así que, uno de los primeros criterios es determinar si se realizará una implantación On site (sobre servidor virtualizado o no) o Cloud (en nube). Como en el caso de los sistemas de intrusión las soluciones Cloud facilitan la ciberseguridad de los sistemas de CCAA y el fácil acceso a la gestión y a los informes desde dispositivos móviles.
- La conexión entre las electrónicas de gestión y conexión con los lectores, pudiendo ser por: Bus, IP o Wifi
- El protocolo de comunicación con los lectores: Wiegand o OSDP
- La tecnología del lector: RFID, biometría...
- En su caso la tecnología de la credencial: Física o Virtual en dispositivo móvil.

También deberemos seleccionar la solución en base:

Al número de:

- Accesos que gestionar.
- Usuarios.
- Posibilidad de calendarios para los grupos de usuarios
- Otras soluciones con las que se interactuará:
- Control de presencia
- Lectores de matrículas de vehículos
- Gestión de reserva de plazas de aparcamiento
- Gestión de reserva de taquillas, salas de reuniones...
- Gestión de visitas
- Máquinas de vending, máquinas de impresión, fotocopiadoras...
- Soluciones CAE
- Etc.

Los sistemas de control de acceso son, dentro de la seguridad, los que más han evolucionado en la integración con otros sistemas del edificio incluidos los relacionados con la gestión del clima y ahorro energético. A la hora de seleccionar una solución de CCAA es importante considerar este punto sobre todo en edificios corporativos, entornos industriales y en general grandes instalaciones como hospitales, universidades...

Videovigilancia

Al igual que en el caso del Control de Accesos la actual tecnología de los sistemas de Videovigilancia nos obliga a considerar en primer lugar donde estará ubicada la plataforma de gestión del vídeo (VMS - Video Management System) y en estos momentos todos los fabricantes contemplan una solución Cloud (en nube) permitiendo el acceso remoto a:

- Las imágenes de cualquier cámara de cualquier instalación
- Video grabado
- Programación del sistema incluso a las analíticas ligadas al video cuando se decida que estas sean remotas y estén alojadas en la nube.

También habrá que decidir sobre las analíticas a utilizar y si estas estarán en la nube, en servidores locales o alojadas en las cámaras desplegada en la instalación. Todo ello dependerá de la capacidad, entre otras cosas, de computación de los elementos seleccionados o el tráfico de datos permitido por la red. La realidad es que un sistema de Videovigilancia se ha convertido en una red IP que en muchos casos debe ser dimensionada específicamente para no interferir con la red de trabajo del cliente o depender de las tareas de mantenimiento que realice el departamento de IT del cliente.

Otros criterios para considerar correspondientes al VMS que puede estar incluido en el NVR de grabación o ser un software instalado en un servidor:

- El número de canales de vídeo (licencias) a conectar
- Capacidad de almacenamiento de imágenes
- Nivel de gestión (Visualización) de eventos en tiempo real y de análisis forense sobre vídeo grabado
- Su grado de integración con sistemas de intrusión y control de accesos para presentar imágenes de eventos reportados por estos sistemas: detección de intrusión, apertura de una puerta del CCAA...

Cámaras:

El abanico de cámara es realmente grande y todos los fabricantes presentan catálogos de producto con opciones para cualquier situación.

A la hora de establecer criterios de selección tendremos que elegir entre modelos:

- Para interior, para exterior, de aplicación en entornos industriales extremos
- Fijas o móviles
- N.º de megapíxeles, iluminación mínima, entornos de contraluz, etc.
- Cámaras de luz visible, térmicas, termográficas...
- Formato y tipo de sujeción

Pero quizás lo más importante es determinar su uso:

- Protección perimetral
- Visualización de interiores
- Visualización de entornos exteriores como el tráfico de vehículos
- Analíticas con las que debe trabajar.
  - Detección o identificación de posible intruso, detección de merodeo
  - Detección de grito, disparo
  - Cuenta personas, detección de aforo…
  - Velocidad de un vehículo, marca, modelo, color, LPR
  - Zonas de paso, mapas de calor
  - etc.

Integración entre sistemas y con terceros elementos

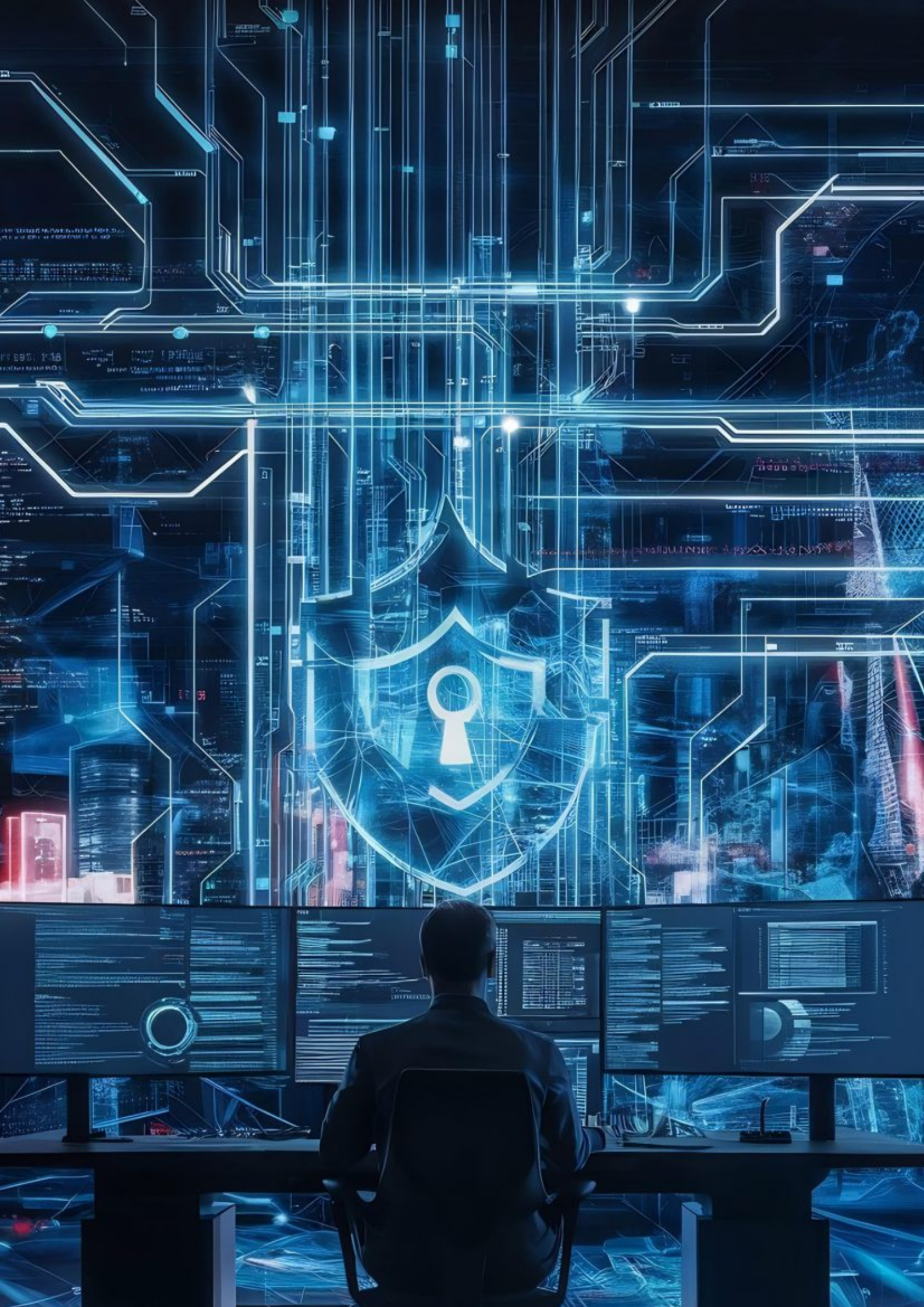
La necesidad de considerar opciones de integración entre distintos sistemas nos lleva a tener que valorar como se realizará esta cuando seleccionamos elementos y por tanto a considerar que en el caso de los equipos de intrusión estos serán compatibles, en general entre distintos fabricantes salvo que su comunicación se realice por bus o vía radio ya que cada fabricante tiene su protocolo.

En el caso del Control de accesos habrá que analizar las opciones integración ya disponibles o en su defecto si existen APIS, SDKS o protocolos para desarrollar las integraciones. Como norma general entre lectores y controladoras se deben considerar protocolos OSDP o Wiegand.

Para los sistemas de Videovigilancia la situación es la misma similar al control de accesos, aunque aquí la integración por RTSP u ONVIF en sus distintas opciones suelen ser opciones disponibles.

Situación actual

En el pasado los sistemas de seguridad han sido soluciones estancas con dificultades de integración. En estos momentos la tendencia es su acercamiento a las redes IP de comunicación y su convergencia al mundo IT, adoptando soluciones similares a las de otras industrias y por lo tanto a las soluciones Cloud con los mismos riesgos y necesidades que cualquier otra industria: Ciberseguridad, garantía de privacidad, necesidad de continuas actualizaciones, rápida obsolescencia tecnológica, búsqueda de integraciones para ofrecer valor añadido.



4.4. Ciberseguridad

La ciberseguridad es un elemento esencial en todo proyecto de diseño de instalación de un Sistema Electrónico de Seguridad, ya que estos sistemas no sólo protegen activos físicos, sino que también generan, almacenan y procesan una gran cantidad de información sensible. Hoy en día, los sistemas de videovigilancia, de control de accesos y de intrusión han pasado de utilizar tecnología exclusivamente analógica a ser sistemas que utilizan mayoritariamente tecnología digital, lo que ha incrementado los ciber riesgos a los que están expuestos, haciendo imprescindible la incorporación de estrategias, protocolos y políticas que garanticen la ciberseguridad de los propios sistemas y de la confidencialidad, integridad y disponibilidad de la información que estos almacenan, procesan y transmiten.

El cumplimiento de la normativa vigente es un pilar fundamental en la gestión de la ciberseguridad dentro de un proyecto de Sistemas Electrónicos de Seguridad. Tanto la legislación nacional como la europea establecen obligaciones específicas para la protección de los datos de carácter personal y la seguridad de los sistemas. Entre las principales normas destacan:

- Reglamento General de Protección de Datos (RGPD) –UE 2016/679: establece directrices para el tratamiento, protección y libre circulación de los datos personales de personas físicas en la Unión Europea. Impone obligaciones sobre la legitimidad del tratamiento, el consentimiento, la transparencia, la minimización de datos y el derecho a la portabilidad, así como la necesidad de adoptar medidas técnicas y organizativas para garantizar la seguridad de los datos.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales: establece los derechos y obligaciones relacionados con los datos de carácter personal, adaptando y complementando el RGPD. Incluye disposiciones concretas sobre el consentimiento, la información a las personas titulares de datos, la gestión de brechas de seguridad y el régimen sancionador.
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad: marco normativo que establece los principios y requisitos mínimos para una protección adecuada de la información y los servicios en las administraciones públicas y en entidades que gestionan información del sector público. Obliga a implantar medidas y controles alineados al nivel de riesgo, asegurando la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad.
- Directiva NIS2 (UE) –2022/2555: establece requisitos de ciberseguridad para operadores de servicios esenciales y proveedores de servicios digitales en la Unión Europea, obligando a implementar mecanismos de gestión de riesgos, notificación de incidentes y cooperación transfronteriza.
- Directiva CER (UE) –2022/2557: regula la resiliencia de entidades críticas en la Unión Europea, obligando a las organizaciones de sectores esenciales a identificar riesgos, adoptar medidas de protección, notificar incidentes graves y cooperar con autoridades nacionales y europeas en la gestión de crisis.
- Reglamento DORA, Reglamento (UE) 2022/2554 sobre resiliencia operativa digital del sector financiero: impone obligaciones específicas en materia de gestión de riesgos TIC, incidentes, pruebas, gestión de la cadena de suministro y notificación, orientadas a la banca, seguros y otros sectores financieros dentro de la UE.

El cumplimiento de estas normativas implica la realización de análisis de riesgos, la designación de responsables de protección de datos, la elaboración de registros de actividades de tratamiento, la gestión de brechas de seguridad y la garantía de los derechos de las personas usuarias, así como la adopción de medidas de seguridad apropiadas y la formación continua del personal involucrado.

La ciberseguridad en proyectos de diseño e instalación de Sistemas Electrónicos de Seguridad demanda un enfoque integral y proactivo. El diseño e implementación de protocolos sólidos de cifrado, políticas estrictas de acceso y robustas estrategias de redundancia, monitoreo y recuperación, junto con el cumplimiento de las obligaciones legales y reglamentarias, permiten mitigar riesgos y garantizar tanto la continuidad operativa como la confianza de las personas usuarias y responsables del sistema.

Confidencialidad e Integridad de los Datos

En el caso de los Sistemas Electrónicos de Seguridad la prioridad es garantizar la confidencialidad y la integridad de la información, debe asegurarse que la información que procesan, almacenan y transmiten estos sistemas sólo sea accesible por personas autorizadas y que no sea alterada de forma no autorizada.

Para garantizar la confidencialidad e integridad de los datos, debemos aplicar tanto medidas técnicas como organizativas.

Protocolos de encriptación y protección de datos

- Cifrado de datos en tránsito: toda comunicación entre dispositivos, servidores y usuarios debe estar protegida mediante protocolos de cifrado robustos como TLS (Transport Layer Security) o SSL (Secure Sockets Layer). Esto garantiza que datos sensibles como credenciales, imágenes de videovigilancia o registros de accesos no puedan ser interceptados ni manipulados por terceros durante su transmisión.
- Cifrado de datos en reposo: la información almacenada en servidores, dispositivos de grabación o sistemas en la nube debe ser cifrada utilizando algoritmos como AES (Advanced Encryption Standard) de al menos 256 bits. Esto protege los datos ante cualquier acceso físico no autorizado o robo de dispositivos.
- Gestión de claves: es fundamental la implementación de políticas seguras para la creación, almacenamiento, rotación y destrucción de claves criptográficas. El acceso a estas claves debe estar limitado al personal autorizado, utilizando módulos de seguridad de hardware (HSM) cuando sea posible.
- Protección de datos personales: se deben cumplir las normativas de protección de datos de carácter personal utilizando mecanismos de anonimización y minimización de datos, especialmente en el caso de datos sensibles.

Políticas de acceso y control de datos

- Principio de mínimo privilegio: los usuarios y los sistemas deben contar únicamente con los permisos estrictamente necesarios para desempeñar sus funciones, limitando el acceso a los datos sensibles.
- Identificación y autenticación robusta: el acceso a aplicaciones y dispositivos debe requerir mecanismos robustos de autenticación y, si técnicamente es posible, debe requerir de una autenticación multifactorial.
- Control de acceso basado en roles (RBAC): se debe implementar una gestión de roles clara que determine qué personas pueden acceder, modificar o eliminar información específica con una trazabilidad completa de las acciones realizadas.
- Registros de auditoría: es necesario mantener y revisar bitácoras detalladas de accesos, cambios y eventos relevantes para detectar y responder a incidentes de seguridad.
- Revisión periódica de accesos: se deben auditar regularmente los permisos y accesos concedidos, retirando privilegios innecesarios y ajustando los perfiles ante cambios en las funciones del personal.

Accesibilidad y Disponibilidad de los Datos

Otro pilar de la ciberseguridad es asegurar la accesibilidad y la disponibilidad de la información de la información, garantizar que esta esté al alcance de las personas autorizadas cuando se requiera, incluso en situaciones adversas. Esto es especialmente crítico en los Sistemas Electrónicos de Seguridad, donde la falta de acceso a los datos puede comprometer la respuesta ante incidentes que pongan en riesgo la protección de personas y bienes. Para garantizar la accesibilidad y disponibilidad de los datos, debemos aplicar tanto medidas técnicas como organizativas.

Estrategias de redundancia y recuperación

- Redundancia de hardware y software: se recomienda la instalación de sistemas redundantes (servidores, discos duros, fuentes de poder, enlaces de red, etc.) que permitan la continuidad operativa ante fallos de componentes clave.
- Replicación geográfica: la información crítica debe ser replicada en ubicaciones físicas distintas, ya sea dentro de la propia infraestructura de la organización o mediante servicios de nube, para prevenir la pérdida de datos ante desastres.
- Copias de seguridad (backups): es imprescindible implementar políticas de respaldo periódicas y automáticas, probando de forma regular la integridad y capacidad de restauración de los backups.
- Planes de recuperación ante desastres (DRP): se deben definir y documentar procedimientos claros para la restauración de servicios y datos con tiempos de recuperación (RTO y RPO) alineados con los requerimientos establecidos durante el diseño del Sistema Electrónico de Seguridad.

Procesos de monitorización y gestión de accesos

- Monitorización en tiempo real: se deben implantar sistemas de monitorización que permitan detectar anomalías en el propio funcionamiento del sistema, así como en el acceso al mismo, caídas de servicios, intentos de intrusión o cualquier evento que ponga en riesgo la disponibilidad de los datos.

4.5. Elaboración de Especificaciones Técnicas

Sistemas de Intrusión

Dentro del proyecto de instalación, se deberán definir todos los elementos que integrarán el sistema de seguridad. Una vez analizados los riesgos inherentes a la protección del bien a resguardar, se determinará el Grado de Seguridad de los componentes que lo conformarán, conforme a la norma UNE EN-50131-1.

Los siguientes elementos constituyen el mínimo requerido para integrar un sistema de intrusión, y el proyecto de seguridad deberá incluir las siguientes especificaciones técnicas:

Central de alarma - Es un dispositivo electrónico cuya función principal es la protección de un espacio, mediante la recepción de señales de unos sensores y trasmitirlas a una Central Receptora de Alarmas donde se coordine las actuaciones necesarias con el servicio de vigilancia privada o las FFCCSE. Deberá definirse:

- Certificación EN 50131 Grado
- Nº de zonas cableadas e inalámbricas que dispone para la conexión de detectores
- Nº de máximo de particiones en las que se podrá subdividir la protección del recinto.
- Tipo y protección de caja envolvente.
- Tipo de conexión a CRA (IP, wifi, GSM,)
- Si dispone de conexión a nube y método de actualización del firmware.

Teclado - Es un dispositivo situado al principio del recinto protegido, que permite des/armar el sistema o parte de este. Su especificación técnica incluirá:

- Certificación EN 50131 Grado.
- Grado de anti-vandalización y tipo de protección anti-sabotaje.
- Si dispone de lector de proximidad.

Fuente de Alimentación - Es el dispositivo cuya función es la de suministrar alimentación eléctrica a todos los elementos que integran el sistema de intrusión. Dentro del mismo, incluye una batería de respaldo, que permite que el sistema sigua funcionando en caso de un fallo de suministro eléctrico externo al sistema. El proyecto deberá incluir el estudio de consumos de toda la instalación para que el dimensionamiento de duración de la batería sea óptimo y que dependerá del Grado definido para el sistema.

Sirena - Dispositivo electrónico de disuasión acústica diseñado para alertar de una intrusión y evitar la intrusión mediante la emisión de un sonido fuerte y penetrante. Se deberá definir el nivel de sonoridad y si dispone de señalización óptica.

Sensores y detectores de intrusión - Dispositivos electrónicos diseñado para identificar y alertar sobre intentos de acceso no autorizado sobre el área que protege. A continuación, se pueden diferenciar los distintos tipos de detectores que existen en el mercado:

- **Detectores de Movimiento infrarojo-** Un detector de movimiento Infrarrojo o PIR, es un dispositivo capaz de detectar una persona utilizando un sensor piroeléctrico, que generará una señal cuando detecte los cambios en la radiación infrarroja emitida por los objetos en su campo de visión. Es el más utilizado para la detección de intrusiones, aunque no es recomendable su uso en entornos de altas o cambios bruscos de temperaturas.
- **Detectores de Movimiento Ultrasónicos-** Un detector de movimiento ultrasónico es un dispositivo que detecta el movimiento de personas u objetos dentro de un área específica mediante el análisis de ondas sonoras en su entorno, al recibir variación en el eco de la onda trasmitida.
- **Detectores de Movimiento microondas-** Es un detector cuyo funcionamiento es similar al ultrasónico, pero utilizando ondas de microondas, en lugar de ultrasonidos.
- **Detectores de tecnologías múltiples –**Combinan un detector de Infrarrojo y uno microondas para tener una mayor precisión en la detección.

La especificación técnica de estos sensores deberá incluir el Grado de seguridad, altura de instalación, cobertura de detección y si dispone de seguridad anti-enmascaramiento.

- **Detector de vibraciones y sísmico –**Es un dispositivo diseñado para detectar y analizar las vibraciones y movimientos en estructuras por herramientas utilizadas en intentos de intrusión, como taladros, explosivos o lanzas térmicas. Dentro de sus especificaciones se definirá el tipo de anclaje a utilizar (según el tipo de superficie a proteger), cobertura en m2 de protección, rango de temperatura para ataques con lanza térmica y si dispone de elementos de activación remota para comprobar su funcionamiento.
- **Detectores de rotura de cristal activo –**Es un dispositivo instalado sobre una superficie acristalada, que generará una señal cuando detecte cualquier golpe o rotura sufrida por la misma. El proyecto recogerá sus especificaciones sobre la cobertura en m2 de protección y el adhesivo necesario para su correcta instalación.
- **Detectores de rotura de cristal acústico –**Es un dispositivo capaz de analizar el espectro sonoro de un emplazamiento y detectar la frecuencia de sonido característica de la rotura de un cristal. El proyecto recogerá sus especificaciones sobre la cobertura en m2 de protección, altura de instalación y distancia hasta la superficie acristalada a proteger.
- **Dispositivos de interrupción de rayos infrarrojos –**La barrera infrarroja consta de dos componentes principales: un emisor y un receptor. El emisor envía haces de luz infrarroja al receptor y se generará una señal de alarma cuando algún objeto corte dicho haz. Se suele utilizar para proteger perímetros exteriores y en el proyecto se definirá el tipo de barrera a utilizar, distancia de separación emisor/receptor y alturas de instalación.
- **Interruptores protectores (contactos magnéticos) –**Son dispositivos que generan una señal al detectar la apertura o manipulación de puertas, ventanas u otras entradas. Dentro de las especificaciones técnicas se tendrá que detallar:
  - Si es posible su utilización sobre superficies férricas
  - Método de instalación en superficie o embutida en el marco de la puerta
  - Potencia del imán según la puerta sobra la que se utilice.
  - Distancias de conmutación de señal.

- **Analizador de imágenes –** Las cámaras y analizadores de imágenes actuales disponen de algoritmos de análisis que permiten la discernir el acceso no autorizado de personas en un recinto protegido. Para la especificación técnica.

Integración con sistemas de alarma

La interconexión entre la central de alarmas y los detectores de intrusión es fundamental para garantizar una protección eficaz y una respuesta rápida ante cualquier anomalía detectada. Las interconexiones pueden realizarse de las siguientes maneras:

Cableadas por detección de resistencias: Este es el método tradicional de integración de detectores en la central o en distintos expansores del emplazamiento. En el detector se instalan una serie de resistencias que permiten a la central analizar la resistividad del cable de interconexión e identificar las siguientes incidencias:

- Sabotaje mediante el corte del cable.
- Alarma de intrusión.
- Sabotaje del detector de intrusión.
- Sabotaje por enmascaramiento del detector.

Cableadas por bus: En este método de interconexión, la central dispone de uno o varios buses/canales de comunicación a los que se conectan los detectores. Esto tiene la ventaja de reducir la cantidad de cableado necesario en una instalación, ya que no es necesario que cada detector esté cableado directamente a la central o a los expansores, sino que puede conectarse a otro detector. Sin embargo, presenta el inconveniente de que no existe un estándar en la comunicación por bus de los dispositivos, por lo que es necesario que todos los detectores sean de la misma marca que la central.

Inalámbrica: El protocolo de comunicación mediante ondas de radio, normalmente dentro de la frecuencia de 868 MHz, permite la comunicación inalámbrica bidireccional entre la central de alarma y los detectores. Este método es adecuado para instalaciones de tamaño pequeño y mediano, con un coste bajo y fácilmente ampliables mediante la inclusión de repetidores de señal. No obstante, tiene el inconveniente de que no existe un estándar en la comunicación vía radio de los dispositivos, por lo que es necesario que todos los detectores sean de la misma marca que la central.

IP: Con la introducción de la inteligencia artificial, la inclusión de cámaras de videovigilancia dentro de los sistemas de intrusión permite que el análisis de imagen pueda discernir el acceso no autorizado a una región de la imagen. Para ello, tanto la central de alarma como la cámara deben compartir la misma red Ethernet o Wi-Fi, o estar conectado a la nube del fabricante.

CCTV

Tipos de cámaras y ubicaciones estratégicas.

En un proyecto de video vigilancia es esencial definir el tipo de cámaras que integrarán el sistema CCTV. A continuación, se presentan los principales tipos de cámaras que existen en el mercado:

Cámaras Turrent/Minidomo –Es una cámara con forma de cúpula, de pequeñas dimensiones y discreta presentación, utilizada habitualmente para la protección interior del edificio. Se suele ubicar para la protección interior de accesos, vestíbulos, zonas de acceso a distintas plantas y zonas establecidas como ruta de salida de emergencia. En el proyecto de instalación se expondrán, al menos, las siguientes especificaciones técnicas:

- Resolución de imagen y óptica elegida. Esta dependerá de la función que se designe, ya que para la búsqueda posterior de objetos será necesario una resolución mayor que si sólo se desea ver el si hay alguna persona en la imagen.
- Tecnología de conexión al sistema: IP, coaxial, GSM.
- Sensibilidad a la luz.
- Tecnologías de reducción de ruido y de compensación de luces.
- Tecnologías de análisis de imágenes, como cruce de línea.
- Conformidad con respecto a normas de ciberseguridad, como NDAA y NIS2.

Cámaras bullet – Son cámaras encerradas dentro de carcasas, de forma cilíndrica, resistentes a la intemperie, lo que las hace ideales para su implementación en exteriores. En el proyecto de instalación se expondrán, al menos, las siguientes especificaciones técnicas:

- Resolución de imagen y óptica elegida. Esta dependerá de la función que se designe, ya que para la búsqueda posterior de objetos será necesario una resolución mayor que si sólo se desea ver el si hay alguna persona en la imagen.
- Altura y ángulo de instalación.
- Tecnología de conexión al sistema: IP, coaxial, GSM.
- Sensibilidad a la luz.
- Tecnologías de reducción de ruido y de compensación de luces.

  Tecnologías de análisis de imágenes, como cruce de línea.
- Conformidad con respecto a normas de ciberseguridad, como NDAA y NIS2.
- Indice de Protección (IP). Debe ser al menos IP65.
- Grado de protección antivandálico IK.

Cámaras domo –Son cámaras de tipo cúpula, diseñadas para el barrido de grandes espacios, interiores o exteriores, y disponen de motorización de alta precisión que les permite posicionarse en una panorámica de 360º, con zoom y autoenfoque. Las especificaciones técnicas a definir deberán de ser idénticas a las cámaras bullet, pero añadiendo:

Aumentos de la óptica zoom.

Si dispone de tecnología de auto tracking para el seguimiento automático de un determinado objetivo.

Cámaras panorámicas

Cámaras térmicas – Por sus especiales cualidades de captación de imágenes, basada en la firma térmica de la radiación infrarroja, está indicada específicamente para su uso con el dispositivo de análisis de la señal de vídeo, para la detección perimetral del recinto protegido. Dentro de las especificaciones técnicas se deberá definir:

- Resolución del sensor FPA microbolómetrico no refrigerado. Para un correcto funcionamiento no debería ser menor a 320x240 pixeles.
- Nivel de sensibilidad de captación de radiación térmica NETD.
- Rango de temperatura de trabajo.
- Tecnologías de análisis de imágenes, como cruce de línea.
- Conformidad con respecto a normas de ciberseguridad, como NDAA y NIS2.
- Indice de Protección (IP). Debe ser al menos IP65.
- Grado de protección antivandálico IK

Control de Accesos

Tecnologías de control de accesos (biométricos, tarjetas, etc.).

Las tecnologías de control de accesos son un conjunto de sistemas y métodos que permiten o restringen el acceso a áreas físicas, sistemas de información o recursos en función de las políticas de seguridad establecidas. Implican la identificación, autenticación y autorización de usuarios o dispositivos antes de conceder el acceso, garantizando que solo aquellos con permisos adecuados puedan ingresar.

Tipos de tecnologías de control de accesos:

Sistemas biométricos: Utilizan características físicas únicas para identificar y verificar a los usuarios, como huellas dactilares, reconocimiento facial, iris o reconocimiento de venas en la palma de la mano. Este tipo de sistema de acceso identifica rasgos únicos de la persona que se almacenan en un base de datos, por lo que su utilización será restringida a casos de muy determinados. En su uso deberá definirse los métodos de protección de la base de datos, periodo de conservación y personas que tienen acceso al mismo, tal y como se recoge en la LOPD.

Tarjetas de acceso: Permiten el acceso a través de tarjetas de identificación física que contienen información de identificación y permisos de acceso. Se tendrá que especificar en el proyecto:

- Tecnología de lectura (proximidad, RFID o media distancia)
- Tamaño de memoria y cifrado de datos
- Diagramas de conexión de la lectora
- Indice de Protección (IP) de las lectoras y grado de protección antivandálico IK

Sistemas de identificación de placas vehiculares: Permiten el acceso de vehículos a través del reconocimiento automático de placas.

- Resolución de imagen y óptica elegida.
- Altura y ángulo de instalación. Posicionamiento del área de reconocimiento.
- Sensibilidad a la luz.
- Tecnologías de reducción de ruido y de compensación de luces.
- Conformidad con respecto a normas de ciberseguridad, como NDAA y NIS2.
- Indice de Protección (IP). Debe ser al menos IP65.
- Grado de protección antivandálico IK

Sistemas de acceso mediante Bluetooth: Utilizan la tecnología Bluetooth para autenticar a los usuarios mediante dispositivos móviles.

Lector de códigos QR: Identifica a los usuarios a través de códigos QR almacenados en dispositivos móviles o tarjetas.

Según el tipo y dimensión del recinto a proteger nos encontraremos con los siguientes tipos de sistema de control de accesos:

Controles de accesos autónomos: Sistemas que controlan una o más puertas sin estar conectados a un sistema central. En la memoria se debe especificar qué tecnología de control de accesos utiliza y la securización ante posibles extracciones de datos.

Sistemas de gestión de identidad (IAM): Centralizan la administración de accesos y credenciales de usuarios en un servidor de la entidad corporativa. En la memoria se tendrá que definir todos los aspectos relacionados con la localización del servidor y el acceso/modificación de la base de datos.

Sistemas de control de acceso en la nube: Sistemas que se almacenan y gestionan en la nube, permitiendo acceso remoto y centralizado. En necesario identificar todas certificaciones de seguridad de la información que dispone la nube utilizada.

Los sistemas de control de accesos anteriormente citados, para la gestión de permisos dentro del sistema, se pueden emplear las siguientes estrategias, que deberá definirse dentro del proyecto de instalación:

Control de accesos basado en roles (RBAC): Otorgan permisos de acceso en función de las responsabilidades laborales de los usuarios.

Control de acceso basado en atributos (ABAC): Considera múltiples atributos del usuario y del recurso para determinar el acceso.

Control de acceso discrecional (DAC): Permite a los usuarios asignar permisos de acceso a otros usuarios.

4.6. Redacción de la Memoria Técnica

La memoria técnica de un sistema de seguridad electrónica es un documento estratégico que integra los aspectos más relevantes del diseño, implementación y operación del sistema. Este documento tiene como propósito principal servir como guía comprensible y detallada, abarcando todos los componentes y funcionalidades del sistema, y como herramienta para la evaluación y toma de decisiones. Su elaboración debe combinar un enfoque narrativo para facilitar la comprensión y un perfil técnico que respalde la precisión y utilidad del contenido.

La memoria debe concluir con una síntesis de las capacidades del sistema, su alineación con las necesidades del entorno y su preparación para adaptarse a futuros desafíos. La mención explícita de normas tales como las UNE, por ejemplo, la UNE 50131-7 refuerza el compromiso con los estándares de calidad y seguridad.

Estructura y Contenido

El desarrollo de la memoria técnica debe seguir una estructura lógica y modular, que abarque los aspectos esenciales del proyecto. La integración de estándares normativos, como la UNE 50131-7 en el caso de sistemas de intrusión, garantiza que el diseño cumpla con los requisitos más estrictos de calidad, seguridad y funcionalidad.

Introducción y Objetivos del Sistema

Este apartado presenta el alcance del proyecto, definiendo los objetivos principales que guían el diseño e implementación del sistema. Se deben describir las amenazas específicas que el sistema busca mitigar y cómo estas se alinean con las necesidades del cliente o la normativa aplicable.

Por ejemplo, un sistema implementado en un complejo industrial puede priorizar la prevención de accesos no autorizados y la monitorización perimetral. Este contexto se relaciona directamente con la necesidad de integrar soluciones avanzadas que cumplan con normas internacionales, como la UNE 50131-7, que establece los requisitos mínimos para los sistemas de alarma contra intrusión y robo.

Diseño y Arquitectura del Sistema

Se debe narrar cómo se diseñó la arquitectura, destacando las decisiones clave tomadas para asegurar la funcionalidad, escalabilidad y eficiencia del sistema. En el caso de los sistemas de intrusión, el cumplimiento de la UNE 50131-7 garantiza que se respeten estándares de instalación, operación y mantenimiento, proporcionando un marco de referencia confiable para la validación de la solución.

Este capítulo también debe incluir:

- **Requisitos técnicos específicos:** Qué necesidades del entorno se abordaron, incluyendo limitaciones presupuestarias, espacio físico disponible e infraestructura existente.
- **Modelos de implementación:** Comparación entre sistemas locales, en la nube o híbridos, justificando la selección con análisis costo-beneficio.
- **Integración de tecnologías emergentes:** Uso de inteligencia artificial o Edge Computing para optimizar la detección de intrusiones y la generación de alertas inmediatas.

Cumplimiento Normativo

Las distintas normas que afectan o participan en el diseño de los sistemas de seguridad, tales como la UNE 50131-7 debe citarse explícitamente como indicador clave en la parte dedicada a los sistemas de intrusión. Estos estándares normativos establecen criterios para garantizar:

- **Fiabilidad** de los sistemas de detección.
- **Mecanismos de prueba** que verifican el rendimiento bajo diferentes condiciones.
- **Directrices de instalación y documentación** que facilitan la operación y el mantenimiento.

Además, la memoria debe documentar cómo el cumplimiento normativo se verificó a través de simulaciones y pruebas piloto, asegurando que el sistema funcione correctamente antes de su puesta en marcha.

Documentación Técnica Complementaria

La memoria debe incluir planos detallados y diagramas que representen gráficamente el sistema. Para los sistemas de intrusión, esto implica ilustrar la disposición de sensores, paneles de control, y zonas críticas monitorizadas, alineándose con las directrices de la UNE 50131-7 u otras posibles normativas o estándares en vigor.

Estrategias de Operación, Mantenimiento y Actualización

Este apartado describe cómo se garantizará la continuidad operativa y la vigencia del sistema a lo largo del tiempo.

- **Planes de mantenimiento:** Incluyen revisiones periódicas según las recomendaciones de la UNE 50131-7, que exige inspecciones regulares de sensores, baterías y conexiones.
- **Gestión de actualizaciones:** La arquitectura modular y escalable permite integrar nuevas tecnologías sin interrupciones operativas, asegurando que el sistema se mantenga vigente frente a nuevas amenazas.

4.7. Elaboración de Planos y Diagramas

La elaboración de planos y diagramas en un sistema de seguridad electrónica es un pilar fundamental para garantizar su correcta instalación, operación y mantenimiento. Estos elementos gráficos actúan como una representación clara y detallada de los componentes del sistema, facilitando la comunicación técnica entre todas las partes involucradas, desde los diseñadores hasta los instaladores y mantenedores.

La elaboración de planos y diagramas es una tarea crítica que debe realizarse con meticulosidad y atención al detalle. No solo son representaciones visuales, sino elementos esenciales para el éxito del proyecto. La integración de estándares normativos como la UNE 50131-7 asegura que estos documentos sean funcionales, comprensibles y completos, consolidando el sistema como una solución robusta y confiable.

Los planos y diagramas no son meros anexos visuales; son herramientas estratégicas que permiten:

- **Optimizar la instalación inicial**, al proporcionar una visión clara de la disposición de los dispositivos.
- **Facilitar futuras expansiones o actualizaciones**, mediante la documentación de la infraestructura existente.
- **Asegurar el cumplimiento normativo**, especialmente en sistemas que deben alinearse con estándares como la UNE 50131-7, que exige documentación precisa para validar la funcionalidad y fiabilidad del sistema.

Tipos de Planos y Diagramas

Planos de Ubicación de Dispositivos

Estos planos ilustran la ubicación exacta de cada componente del sistema dentro del entorno físico. Incluyen:

- Cámaras de videovigilancia, detectores de intrusión y paneles de control.
- Sensores especializados, como detectores de humo o sensores de vibración.
- Áreas de cobertura de cada dispositivo, representadas gráficamente para identificar zonas críticas o posibles puntos ciegos.

Diagramas de Conexión

Estos diagramas explican cómo interactúan los diferentes componentes entre sí, destacando las conexiones físicas y lógicas. Deben incluir:

- Enlaces entre sensores, paneles de control y sistemas de grabación.
- Flujos de datos desde los dispositivos de campo hasta los sistemas de gestión central.
- Integración con otros sistemas, como controles de acceso o plataformas en la nube.

Diagramas Funcionales

Estos diagramas representan los flujos de operación del sistema, explicando cómo se procesan los datos desde la detección hasta la acción.

- **Flujo de detección de intrusión:** Describe cómo un sensor detecta movimiento, genera una señal y activa los mecanismos de respuesta.
- **Gestión de alertas:** Muestra cómo las notificaciones se enrutan a los operadores o usuarios finales, incluyendo los pasos para su escalado si es necesario.

Esquemas Eléctricos

Incluyen detalles sobre el suministro de energía y las conexiones eléctricas de los dispositivos. Este nivel de detalle es esencial para garantizar:

- La compatibilidad de voltajes y corrientes.
- La implementación de medidas de redundancia, como fuentes de alimentación ininterrumpida (UPS).

Consideraciones de Diseño

La calidad de los planos y diagramas depende de un diseño detallado y bien organizado. Algunos principios clave son:

- **Claridad visual:** Uso de símbolos estandarizados y anotaciones que permitan interpretar fácilmente la información, en línea con las directrices de la UNE 50131-7.
- **Escalabilidad:** Los planos deben estar diseñados para admitir futuras expansiones, como la adición de nuevos sensores o la actualización de equipos existentes.
- **Precisión técnica:** Los diagramas deben reflejar la configuración real del sistema, asegurando que cualquier cambio en el diseño se actualice en la documentación.

Beneficios Operativos

Los planos y diagramas no solo son útiles durante la instalación, sino que también:

- Facilitan el diagnóstico de problemas al ofrecer una visión clara de cómo interactúan los componentes.
- Simplifican las auditorías y verificaciones de cumplimiento normativo, demostrando que el sistema se alinea con estándares como la UNE 50131-7.
- Apoyan el mantenimiento al identificar rápidamente las ubicaciones de dispositivos y las rutas de cableado.

4.8. Detalle de Componentes y Funcionamiento

El análisis de los componentes y su funcionamiento es clave para garantizar la operación eficiente del sistema de seguridad electrónica. Este apartado resume los elementos típicos del sistema y su integración para cumplir con los objetivos del proyecto, en este apartado se intenta describir los componentes y su interacción, asi como indicar la necesidad de respaldo del diseño con estándares técnicos, asegurando su eficiencia, seguridad y capacidad de adaptación a futuras necesidades, y basándose en el cumplimiento normativo existente, como por ejemplo la UNE 50131-7.

Componentes Principales

- **Dispositivos de Campo**
  - **Sensores de intrusión:** Detectores de movimiento, contactos magnéticos y sensores especializados, diseñados para detectar accesos no autorizados.
  - **Cámaras de videovigilancia:** Equipadas con análisis de video e inteligencia artificial para generar alertas en tiempo real.
  - **Paneles de control:** Centralizan la información y gestionan respuestas automáticas o manuales.
- **Sistemas de Gestión**
  - **Software de gestión (VMS):** Almacena grabaciones, permite búsquedas avanzadas y genera informes.
  - **Plataformas de monitoreo centralizado:** Facilitan la supervisión remota y la gestión de alertas.
- **Infraestructura de Soporte**
  - **Redes de comunicación:** Interconexión de dispositivos.
  - **Fuentes de energía:** Sistemas primarios y redundantes para garantizar continuidad operativa.

Funcionamiento del Sistema

- **Recopilación de Datos:** Los dispositivos capturan información del entorno y detectan eventos relevantes.
- **Procesamiento y Respuesta:** El sistema central procesa señales y genera respuestas automatizadas (activación de alarmas, notificaciones, grabaciones).
- **Integración:** Los subsistemas trabajan de manera interoperable, optimizando la operación (por ejemplo, integración de control de acceso y videovigilancia).

4.9. Necesidades y Previsión de Futuras Actualizaciones

La previsión de futuras actualizaciones es un componente crítico en el diseño de sistemas de seguridad electrónica. Este enfoque garantiza que el sistema pueda adaptarse a las necesidades cambiantes, avances tecnológicos y nuevas amenazas, maximizando su vida útil y optimizando el retorno de inversión.

Un sistema diseñado con previsión para futuras actualizaciones no solo prolonga su vigencia, sino que también asegura que seguirá cumpliendo con estándares técnicos y normativos. Este enfoque refuerza la inversión inicial y garantiza su capacidad para evolucionar junto con las necesidades del entorno.

Identificación de Necesidades

- **Evolución Tecnológica**
  - Las innovaciones en inteligencia artificial, análisis de video y sistemas en la nube requieren que el sistema esté preparado para integrar nuevas capacidades sin necesidad de reemplazos significativos.
- **Escalabilidad del Proyecto**

  Es esencial prever la expansión del sistema a medida que crecen las instalaciones o aumenta la demanda de seguridad.
- **Adaptación a Normativas**

  Las regulaciones, como la UNE 50131-7, pueden evolucionar, requiriendo que los sistemas se actualicen para mantener el cumplimiento normativo.

Estrategias de Actualización

- **Diseño Modular y Escalable**

  La arquitectura basada en microservicios permite la implementación de mejoras de manera progresiva y sin interrupciones operativas.
- **Compatibilidad e Interoperabilidad**

  Usar protocolos estándar asegura que los nuevos componentes sean compatibles con la infraestructura existente.

Planes de Mantenimiento Preventivo

Implementar revisiones regulares permite identificar componentes obsoletos y planificar su actualización antes de que afecten al sistema.

Esto redundara en los proyectos en una mejora de la vida útil de los mismos asi con en determinados beneficios tales como:

- **Reducción de Costos:** Planificar actualizaciones minimiza inversiones inesperadas y costosas.
- **Mayor Seguridad:** Adaptarse rápidamente a nuevas amenazas o vulnerabilidades.
- **Optimización Operativa:** Mantener el sistema alineado con las mejores prácticas y tecnologías disponibles.

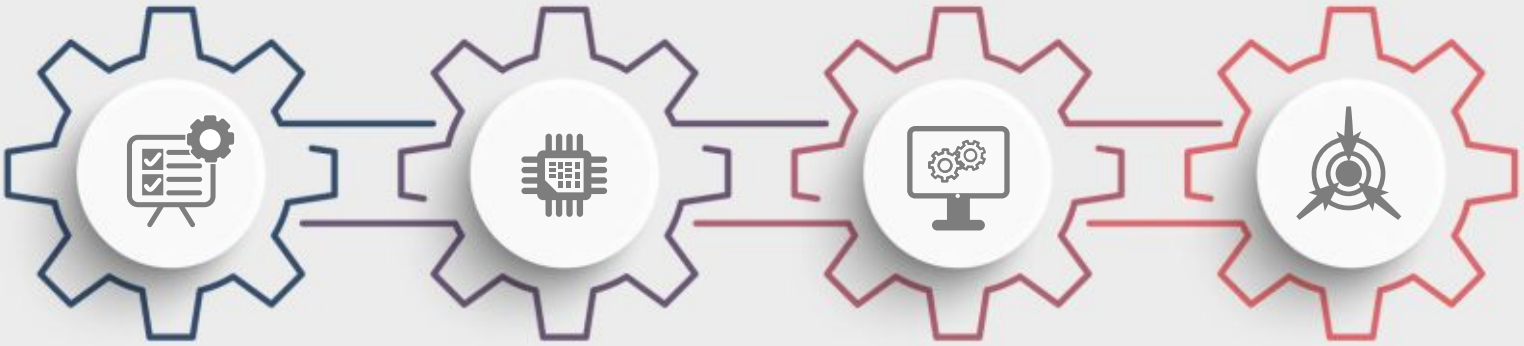
La implementación de un sistema de seguridad electrónica es una etapa crucial que traduce el diseño teórico en una solución funcional y operativa. Este proceso requiere planificación meticulosa, ejecución precisa y validación exhaustiva para garantizar que el sistema cumpla con los objetivos establecidos y se integre correctamente en su entorno.

La fase de implementación transforma el diseño del sistema en una solución tangible y funcional. Su éxito depende de una planificación estructurada, pruebas rigurosas y una integración efectiva. Al finalizar esta etapa, el sistema debe estar preparado para operar de manera confiable, adaptándose a las demandas actuales y futuras del entorno.

5.1. Etapas de la Implementación

- **Planificación Inicial**
  - **Definición del Cronograma:** Se establece un plan de trabajo detallado con hitos claros para cada fase del proyecto.
  - **Revisión de Infraestructura:** Verificar la preparación del sitio, disponibilidad de energía y conectividad de red para evitar contratiempos.
- **Instalación del Hardware**
  - **Montaje de Dispositivos:** Instalación de cámaras, sensores, paneles de control y otros componentes según los planos y diagramas previamente elaborados.
  - **Conexiones Eléctricas y de Comunicación:** Establecer enlaces seguros y confiables entre los dispositivos para garantizar su correcto funcionamiento.
- **Configuración de Software y Sistemas**
  - **Integración de Componentes:** Configurar el software de gestión, asegurando que todos los dispositivos interactúen correctamente.
  - **Pruebas de Interoperabilidad:** Verificar que el sistema funcione como un todo integrado, respetando los flujos de datos y la generación de alertas.
- **Pruebas y Validación**
  - **Pruebas Funcionales:** Comprobar que cada componente cumpla con su función específica.
  - **Pruebas de Estrés:** Simular escenarios críticos para garantizar la resiliencia del sistema frente a posibles fallos o ataques.
  - **Validación Normativa:** Asegurar que el sistema cumpla con estándares como la UNE 50131-7, mediante auditorías y revisiones técnicas.

5 Fase de Implementación



5.2. Capacitación del Personal

Entrenar a los operadores y personal de mantenimiento en el uso del sistema y la interpretación de alertas, asegurando su correcta operación a largo plazo.

5.3. Comunicación Continua

Mantener un flujo constante de información entre diseñadores, instaladores y el cliente, asegurando que todos los involucrados estén alineados en cada etapa.

5.4. Documentación Completa

Generar registros detallados del proceso de implementación, incluyendo cambios realizados y observaciones relevantes.

5.5. Planes de Contingencia

Preparar soluciones alternativas para abordar imprevistos, como fallos en la infraestructura o demoras en la entrega de componentes.

La fase de implementación transforma el diseño del sistema en una solución tangible y funcional. Su éxito depende de una planificación estructurada, pruebas rigurosas y una integración efectiva. Al finalizar esta etapa, el sistema debe estar preparado para operar de manera confiable, adaptándose a las demandas actuales y futuras del entorno.

Si como hemos analizado en los apartados anteriores podemos asegurar lo que vamos a proteger, de qué o de quién vamos a protegernos, las características orográficas, geográficas y climáticas de nuestra instalación, solo nos resta considerar quién y cómo operará el sistema buscando su mayor efectividad. Premisa de efectividad, en la que debemos optimizar criterios como la eficacia (funcionalidad), la eficiencia, la fiabilidad, la facilidad de mantenimiento, la sostenibilidad, la capacidad de adecuación a situaciones cambiantes, la durabilidad, la capacidad de recuperación frente a situaciones no previstas (resiliencia), etc.

Sin duda, el éxito de un sistema bien diseñado y correctamente instalado es que llegue a ser correctamente operado. Hoy por hoy podemos asegurar que esa operación pasa inevitablemente por el factor humano, y que por lo tanto la capacitación del personal constituye un pilar esencial de nuestro sistema de seguridad en su más amplia concepción

Consecuencia de una buena Operación es que el sistema instalado sea mantenido adecuadamente y reparado con un buen servicio de mantenimiento que acorde con el nivel de riesgo de la instalación, garantice la operación del sistema sin solución de continuidad, incorporando las rutinas de mantenimiento preventivas con la periodicidad establecida y unos tiempos de respuesta en las actuaciones correctivas que garantice la operatividad del sistema.

6.1. Capacitación del Personal: El Pilar Humano de la Seguridad

Un sistema de seguridad no es más eficiente que las personas que lo operan. La capacitación efectiva no se limita a un curso inicial; es un proceso continuo que moldea el comportamiento y la mentalidad del personal.

Para profundizar en la **capacitación del personal**, nos enfocaremos en tres aspectos clave: el enfoque estratégico, el contenido de los programas de formación y la importancia de los manuales y guías de usuario. Estos elementos garantizan que el equipo humano no solo sepa cómo usar el sistema, sino que lo entienda y lo gestione con un enfoque de seguridad proactivo e incluso preventivo.

6.2. Enfoque Estratégico de la Formación

La capacitación no debe verse como un simple requisito, sino como una **inversión estratégica** en la capacidad humana de la organización. Un plan de formación bien diseñado convierte a los operadores del sistema en analistas de seguridad, capaces de identificar riesgos y reaccionar de forma inteligente.

- **Formación técnica:** Detallada sobre el funcionamiento del sistema, sus componentes, las interfaces y las capacidades avanzadas.
- **Formación continua:** La tecnología de seguridad evoluciona rápidamente, al igual que las amenazas. Los programas deben incluir sesiones de actualización periódicas para mantener al personal al día sobre nuevas funcionalidades del sistema y tácticas de los atacantes. Esto garantiza que la inversión en el sistema no se quede obsoleta.

- **Simulacros y ejercicios:** La teoría es importante, pero la práctica es crucial. Los simulacros de incidentes (como intrusiones, fallos del sistema o intentos de *phishing*) preparan al personal para actuar bajo presión. Esto mejora los tiempos de respuesta, reduce los errores y valida los protocolos de emergencia.
- **Cultivar una mentalidad de seguridad:** La capacitación debe ir más allá de los aspectos técnicos. Debe fomentar una cultura donde cada miembro del equipo se sienta responsable de la seguridad. Esto incluye la concienciación sobre la importancia de la ciberseguridad y la protección de datos, incluso en las tareas diarias.

6.3. Contenido Detallado de los Programas de Formación

El contenido de la capacitación debe ser exhaustivo y adaptado a los diferentes roles dentro del equipo.

- **Formación técnica:** Esto incluye una comprensión profunda del **hardware y software** del sistema, el uso e incluso la configuración de las interfaces de usuario, la configuración de alarmas y la gestión de los registros de eventos. Se debe enseñar cómo realizar diagnósticos básicos y solucionar problemas comunes.
- **Análisis de datos e inteligencia:** El personal debe aprender a interpretar los datos que genera el sistema. Esto va más allá de ver una alarma; implica analizar patrones, identificar comportamientos anómalos y predecir posibles incidentes. De igual manera el personal debe saber incorporar las variables que pudieran proporcionar los servicios de inteligencia en sus aportaciones periódicas a los efectos oportunos de prever nuevos riesgos emergentes o el crecimiento en la probabilidad de éxito de riesgos ya conocidos.
- **Protocolos de respuesta a incidentes:** Es vital que el equipo conozca el plan de acción paso a paso. Se deben definir claramente las responsabilidades, los canales de comunicación y los procedimientos de escalado para asegurar una respuesta coordinada y rápida.

6.4. Manuales y Guías de Usuario: Herramientas de Referencia Esenciales

Los manuales de usuario no son solo documentos; son la memoria colectiva del proyecto de seguridad. Su diseño y accesibilidad son tan importantes como su contenido.

- **Claridad y accesibilidad:** Los manuales deben estar escritos en un lenguaje claro y sencillo, evitando la jerga técnica innecesaria. Deben estar disponibles en formatos de fácil acceso, como una plataforma en línea, una aplicación móvil o una intranet, para que el personal pueda consultarlos al instante.
- **Estructura y contenido:** Un manual eficaz incluye:
  - Una **guía de inicio rápido** para las funciones básicas.
  - Secciones detalladas sobre la **solución de problemas**.
  - **Listas de verificación de emergencia** para los escenarios más críticos.
  - Un **glosario de términos** para asegurar que todos hablan el mismo idioma.

- **Mantenimiento:** Los manuales deben ser **documentos vivos** que se actualicen continuamente con cada cambio en el sistema o cada nueva lección aprendida de un incidente.

La capacitación del personal no es un gasto, sino la **inversión más inteligente** para asegurar la longevidad y la efectividad de cualquier sistema de seguridad.

6.5. Monitoreo y Gestión: De la Vigilancia Reactiva a la Inteligencia Proactiva

El monitoreo de un sistema de seguridad ha evolucionado sustancialmente en los últimos años. Hoy no se trata simplemente de mirar pantallas o de solo de responder a las alarmas generadas en nuestro sistema, sino de anticiparse a los incidentes y a sus consecuencias. Esta transición de una postura reactiva a una proactiva es fundamental para una seguridad eficaz.

En este empeño nacen las **PSIM (Physical Security Information Management)** plataformas de software para integrar sistemas de seguridad como cámaras de vigilancia, alarmas, sistemas de protección contra incendios, control de acceso y sensores, etc., que proporcionan una interfaz única donde monitorizar y gestionar todos los sistemas de seguridad, automatizar flujos de trabajo y mejorar la toma de decisiones.

Esto facilita:

- **Estrategias de Monitoreo Continuo:** Un monitoreo efectivo se basa en el análisis de datos, no solo en la observación. El objetivo es identificar patrones y anomalías que puedan indicar un riesgo potencial antes de que se convierta en una amenaza. Esto se logra mediante:

  Uso de la inteligencia artificial y el *machine learning* para analizar grandes volúmenes de datos y detectar comportamientos inusuales, como accesos a horas no habituales o intentos repetidos de acceso fallidos.

  Integración de sistemas: La seguridad es más fuerte cuando los sistemas se comunican entre sí. Al integrar el sistema de seguridad con otros, como los de control de acceso o gestión de edificios, se obtiene una visión holística y se pueden coordinar las respuestas de manera más eficaz.

  Auditorías y revisiones regulares: No basta con tener un sistema automatizado. El personal debe revisar y auditar los registros y el rendimiento del sistema de forma regular para asegurar su integridad.

- **Gestión de Incidentes y Respuesta Rápida:** La velocidad, la organización y la coordinación de medios disponibles son cruciales en un incidente de seguridad. Un plan de respuesta bien definido minimiza el daño y acelera la recuperación. Este plan debe incluir:

  Roles y responsabilidades claramente definidos: Cada miembro del equipo debe saber exactamente qué hacer y a quién informar en caso de una alerta. Una línea de mando bien definida es imprescindible. La claridad reduce la confusión y acelera la acción.

Procedimientos de escalado: Se deben establecer los pasos a seguir para notificar a los niveles superiores de la dirección y a los equipos externos (como las fuerzas de seguridad), si el incidente lo requiere.

Análisis post-incidente: Después de que un incidente es mitigado, es vital realizar un análisis detallado para entender la causa raíz, actualizar los protocolos y entrenar al equipo para evitar que vuelva a ocurrir. Esta etapa es clave para la mejora continua.

6.6. Evaluación de Desempeño: Medición del Éxito y Mejora Constante

Sin una evaluación continua y rigurosa, no se puede saber si el sistema de seguridad está cumpliendo su función. La medición del rendimiento es fundamental para la mejora continua, para aprender de nuestros errores para realimentar nuestros sistemas y procedimientos.

La evaluación de desempeño convierte la seguridad de una actividad en una inversión cuantificable. Al medir el rendimiento del sistema, se puede demostrar su valor y justificar la necesidad de recursos adicionales.

Con esta finalidad es necesario establecer **métricas adecuadas** que nos ayuden en la medición de unos **Indicadores de rendimiento (KPIs)** que nos ayuden a cuantificar la operatividad del sistema.

Los KPIs deben ser específicos, medibles, alcanzables, relevantes y con un plazo definido (SMART). Algunos ejemplos de KPIs para sistemas de seguridad podrían ser:

- **Tiempo promedio de respuesta:** El tiempo que transcurre desde la detección de un incidente hasta la primera acción de mitigación. Un tiempo de respuesta más corto indica un sistema eficiente.
- **Tasa de falsas alarmas:** Un alto número de falsas alarmas puede generar fatiga en el personal y retrasar la respuesta a incidentes reales.
- **Porcentaje de incidentes resueltos:** La efectividad del equipo para gestionar y cerrar incidentes con éxito.
- **Índice de cumplimiento de protocolos:** Medir con qué frecuencia el personal sigue los procedimientos establecidos.

La presentación de los datos obtenidos con estos KPIs en **Informes periódicos de evaluación,** representan la herramienta de comunicación más importante de las Direcciones de Seguridad, para poner en valor el sistema de seguridad a la alta dirección, dado que deben presentar el estado de la seguridad y la base para la toma de decisiones y justificación de nuevas inversiones.

Deben contener un resumen de manera clara y visual de los incidentes, incluyendo:

- Un **resumen ejecutivo** con los puntos más importantes para la alta dirección.
- **Análisis de los KPIs** con gráficos, tablas y datos claros que muestren el rendimiento del sistema.
- **Recomendaciones para la mejora**, como la necesidad de formación adicional, la actualización de equipos o la modificación de protocolos.

7 Fase de Mejora Continua

En el ámbito de la gestión de proyectos se define la mejora continua como la aplicación sistemática de procesos de análisis, revisión y ajuste de procesos, productos y servicios, con el propósito de incrementar su valor y desempeño. Por ello la Fase de Mejora Continua de cualquier proyecto relacionado con el diseño e instalación de Sistemas Electrónicos de Seguridad representa una etapa fundamental dentro de su ciclo de vida. En este contexto la mejora continua abarca aspectos técnicos, operativos y de gestión, garantizando que los sistemas instalados respondan a los desafíos emergentes y mantengan altos estándares de protección.

Su objetivo central es garantizar que el sistema que se ha diseñado e implantado se mantenga eficiente y actualizado, para ello se debe adoptar un enfoque integral a la hora de optimizar el desempeño del sistema, detectando y corrigiendo vulnerabilidades y deficiencias técnicas y operativas. Manteniendo actualizadas las políticas y procedimientos conforme a los cambios regulatorios y tecnológicos. Fomentando la participación de los usuarios y partes interesadas. Con el objetivo final de mejorar la satisfacción y confianza en el Sistema Electrónico de Seguridad instalado.

Para una correcta mejora continua es necesaria la implementación de mecanismos como auditorías, revisiones periódicas, lecciones aprendidas, gestión de cambios y recopilación de retroalimentación, integrados en un ciclo sistemático de mejora. Para conseguir esta mejora continua tenemos las siguientes buenas prácticas:

- Planificar la mejora continua desde la fase inicial del proyecto: definir métricas, indicadores y procedimientos para evaluar el desempeño y detectar áreas de oportunidad.
- Documentar todos los procesos y resultados: facilita la trazabilidad, la rendición de cuentas y la transferencia de conocimientos.
- Involucrar a todas las partes interesadas: personas usuarias, equipo técnico, gerencia y personal de seguridad deben participar activamente en las auditorías, revisiones y retroalimentaciones.
- Realizar auditorías y revisiones periódicas: analizar el cumplimiento de normativas, políticas internas y estándares de calidad.
- Recopilar y analizar la retroalimentación: utilizar encuestas, entrevistas y análisis de incidentes para identificar mejoras.
- Gestionar adecuadamente los cambios: evaluar el impacto de las mejoras propuestas, planificar su implementación y comunicar de forma efectiva.

La fase de mejora continua en los proyectos de instalación de Sistemas Electrónicos de Seguridad es esencial a la hora de mantener la eficacia, adaptabilidad y vigencia de las soluciones tecnológicas implementadas. Lo que se logra mediante la ejecución sistemática de auditorías, revisiones y la integración de la retroalimentación de los usuarios, es posible anticipar riesgos, corregir debilidades y aprovechar nuevas oportunidades para fortalecer la protección que proporciona el sistema y mejorar la experiencia de quienes interactúan con él. La cultura de mejora continua no solo implica procesos técnicos, sino también la colaboración activa de todas las áreas involucradas, asegurando así que el sistema evolucione en sintonía con las necesidades de la organización y el entorno.

La mejora continua no debe considerarse una fase aislada o final del proyecto, sino un proceso transversal que acompaña todas las etapas del ciclo de vida del sistema. Desde la planificación inicial hasta la operación y mantenimiento, cada decisión debe evaluarse bajo el prisma de su capacidad para ser mejorada en el futuro.

En este sentido, es fundamental establecer una cultura organizacional orientada a la mejora, donde todos los actores involucrados comprendan su rol en la identificación de oportunidades de optimización. Además, la incorporación de tecnologías emergentes como la inteligencia artificial, el análisis predictivo y la automatización de procesos pueden potenciar significativamente la capacidad de los sistemas electrónicos de seguridad para adaptarse a nuevas amenazas y contextos operativos.

A continuación, se describen en detalle las actividades y tareas principales que constituyen a desarrollar esta fase, organizadas en dos grandes bloques: "Auditorías y Revisiones", y "Retroalimentación y Ajustes".

7.1. Auditorías y Revisiones

Las auditorías y revisiones son una herramienta fundamental para garantizar la integridad y eficacia de los Sistemas Electrónicos de Seguridad. Las auditorías deben ser periódicas y abarcar aspectos técnicos, operativos y de cumplimiento normativo. Estas actividades permiten identificar áreas de oportunidad y establecer acciones correctivas o preventivas.

7.2. Auditorías periódicas de seguridad

Las auditorías periódicas se deben realizar conforme a un calendario previamente definido, tanto las internas como las externas. Al realizar la programación se debe asegurar que se cubren todas las áreas críticas del sistema, incluyendo control de accesos, videovigilancia, sistemas de detección de intrusión, etc.

Las auditorias deben incluir:

- Revisión del cumplimiento normativo: evaluación de la conformidad con la legislación vigente, así como con políticas internas de la organización.
- Evaluación de riesgos: identificación continua de nuevos riesgos o vulnerabilidades que puedan afectar la operación del sistema, considerando tanto amenazas tecnológicas como humanas.
- Detección de vulnerabilidades: identificación de posibles fallas de seguridad, accesos no autorizados y riesgos emergentes.
- Análisis de registros y eventos: revisión de bitácoras, logs, estadísticas de uso e informes generados por los sistemas para detectar irregularidades, intentos de acceso no autorizado o fallos recurrentes.
- Revisión de la infraestructura física y electrónica: inspección de equipos, cableado, sensores, cámaras, alarmas y sistemas de control.
- Verificación del funcionamiento y configuración: pruebas de operación, simulacros, revisión de actualizaciones de firmware y software.

  Informe de hallazgos: elaboración de informes detallados con los resultados de la auditoría, identificando hallazgos, no conformidades y oportunidades de mejora.
- Seguimiento de recomendaciones: implementación de planes de acción para atender las observaciones identificadas priorizando en función del nivel de riesgo.

7.3. Revisiones y actualizaciones de políticas y procedimientos

Las revisiones periódicas de políticas y procedimientos son indispensables para garantizar que estas siguen siendo efectivas y aplicables. Las actividades clave incluyen:

- Análisis de políticas vigentes: evaluación recurrente de las políticas de seguridad para asegurar que reflejan los cambios tecnológicos, organizacionales y normativos.
- Actualización de procedimientos: revisión y ajuste de los procedimientos operativos, mantenimientos preventivos y correctivos, protocolos de respuesta ante incidentes y planes de contingencia.
- Capacitación y sensibilización: actualización y refuerzo de la capacitación del personal operativo y técnico respecto a cambios en políticas y procedimientos y en el uso de nuevas tecnologías o herramientas implementadas.
- Documentación y difusión: asegurar que toda la documentación relevante esté actualizada y disponible para quienes la requieran, ya sea en formato físico o digital, y que se comunique oportunamente a todas las partes interesadas.
- Evaluación de impacto: medición del impacto de los cambios realizados en procedimientos y políticas, vigilando su efectividad y ajustándolo en caso de ser necesario.

7.4. Retroalimentación y Ajustes

La mejora continua no puede entenderse sin la participación de las personas que utilizan y operan los Sistemas Electrónicos de Seguridad. La recopilación y análisis sistemático de su retroalimentación es imprescindible para identificar áreas de mejora y permitir realizar ajustes que optimicen la funcionalidad y el rendimiento del sistema.

7.5. Recopilación de retroalimentación del usuario

Las actividades para la obtención de retroalimentación por parte de los usuarios deben incluir lo siguiente:

- Encuestas de satisfacción: se deben realizar periódicamente encuestas estructuradas dirigidas a los usuarios y enfocadas en la funcionalidad, facilidad de uso, rapidez de respuesta y confiabilidad de los sistemas, para así poder evaluar la satisfacción y percepción que tienen los usuarios respecto al sistema en cuestión.
- Entrevistas a grupos de interés: se deben organizar sesiones de trabajo con representantes de los distintos perfiles de usuarios para profundizar en sus experiencias, expectativas y desafíos en el uso diario de los sistemas.
- Canales de comunicación abiertos: se deben implantar buzones físicos o digitales, líneas directas o plataformas electrónicas en las que se puedan recibir sugerencias, informes de fallos o solicitudes de mejora.
- Análisis de tickets e informes de servicio: se deben analizar las solicitudes de soporte técnico e informes de incidentes para identificar patrones recurrentes que ayuden a identificar problemas.
- Monitorización del uso: se deben analizar las métricas y datos generados por el propio sistema respecto a la interacción de los usuarios, identificando funciones poco utilizadas o procesos que generan confusión.

7.6. Ajustes y Mejoras Basadas en la Retroalimentación

Sobre la base de la información recopilada por medio de la retroalimentación, se deben programar y ejecutar acciones de ajuste y mejora que permitan elevar el nivel de seguridad y eficiencia del sistema. Para ello es necesario realizar las siguientes actividades:

- Identificación de oportunidades de mejora: se deben clasificar y priorizar las mejoras a implementar, considerando factores como el impacto en la seguridad, la facilidad de implementación y los recursos disponibles.
- Planificación de las acciones correctivas: se deben definir objetivos, asignar responsables, elaborar cronogramas y dotar de los recursos necesarios para la implementación de mejoras.
- Implementación de ajustes técnicos y operativos: en caso necesario, se deben modificar las configuraciones, actualizar los equipos, proporcionar capacitación adicional e integrar nuevas tecnologías.
- Evaluación post-implementación: se debe medir el éxito de las mejoras aplicadas a través de indicadores de desempeño, auditorías de seguimiento y establecer una nueva recopilación de retroalimentación.
- Comunicación de cambios: se debe informar a todos los usuarios y partes interesadas, de forma oportuna y clara, de los cambios realizados, los beneficios esperados y las modificaciones en los procedimientos de uso.
- Documentación de mejoras: se deben registrar, de forma detallada, todas las mejoras y ajustes realizados asegurando la trazabilidad y facilitando futuras auditorías o revisiones.

8 Conclusiones

8.1. Resumen final

Este marco consolida un **proceso de diseño y gestión del riesgo** para sistemas de seguridad electrónica, abarcando identificación, análisis y evaluación de riesgos, tratamiento, integración tecnológica, operación y **mejora continua**. El alcance integra medidas técnicas y organizativas, IAM, monitorización/auditoría y cumplimiento normativo, reforzando la **confidencialidad, integridad y disponibilidad** y la Ciber resiliencia organizacional.

8.2. Metodología validada

El proceso se articula en **tres fases**: (1) identificación de bienes, amenazas y contextos; (2) análisis y evaluación del riesgo con criterios comparables; y (3) tratamiento y gestión (reducción, transferencia, retención o evitación). Se recomienda el **uso complementario** de metodologías (p. ej., Mosler y enfoque cuantitativo tipo William T. Fine) para mejorar la objetividad, la trazabilidad y la priorización.

8.3. Gobierno e integración corporativa

La gestión del riesgo se integra en el **ciclo PDCA** y en los sistemas de gestión de la organización. La **dirección** define el contexto, los **criterios de aceptación** y los umbrales de decisión. Esto habilitas decisiones justificadas sobre aceptación del **riesgo residual**, priorización de controles y alineamiento con la estrategia y requisitos regulatorios.

8.4. Tratamiento y planificación de la seguridad

El tratamiento se fundamenta en la **magnitud del ER** y su prioridad. Las propuestas deben ser **coherentes con el análisis**, atendiendo sinergias entre riesgos y la **multifuncionalidad** de subsistemas (p. ej., CCTV contribuye a mitigar intrusión, hurto, vandalismo y robo). La planificación incluye diseño modular/escalable, interoperabilidad, pruebas y validación operativa, y un plan de mantenimiento/actualización.

8.5. Medición y mejora continua

Se establecen **KPIs** y reportes periódicos para seguimiento y toma de decisiones: p. ej., **tiempo medio de respuesta (MTTR)**, **tasa de falsas alarmas**, **% de incidentes resueltos**, **disponibilidad del sistema**, **cumplimiento de protocolos** y **% de riesgos en nivel aceptable**. El programa de **auditorías, revisiones y lecciones aprendidas** mantiene la eficacia de los controles y la documentación actualizada.

8.6. Cierre técnico

El resultado es un **modelo repetible y auditable** que optimiza la relación entre **coste de seguridad** y **pérdidas evitadas**, aportando una base común para decisiones de inversión, priorización de controles y evaluación de eficacia a lo largo del ciclo de vida del sistema.

8.7. Recomendación

Adoptar este marco como **estándar corporativo** para proyectos de Seguridad Electrónica, con:

- **Criterios de riesgo y umbrales** aprobados por dirección.
- **Aplicación dual** de metodologías (p. ej., Mosler + cuantitativa) en análisis relevantes.
- **Plan de tratamiento** con responsables, presupuesto, hitos y KPIs.
- **Programa de mejora continua** (auditorías, revisiones post-incidente y gestión de cambios).
- **Memoria técnica** que documente capacidades, cumplimiento y la adaptación a riesgos emergentes.

Guía elaborada por el Área de
Trabajo de Ingeniería instalación
y mantenimiento de:

AES
ASOCIACIÓN ESPAÑOLA
EMPRESAS DE SEGURIDAD

C/Alcalá, 99 2ºA - 28009 Madrid
Telf. 915 765 225
www.aesfundacion.es
patronato@aesfundacion.es

@FundacionAES AES Fundación aes_fundacion_