AES FUNDACIÓN

MANIFIESTO 2030: GESTIÓN INTEGRAL DE LAS SEÑALES DE ALARMA

Índice

1 Objeto del Manifiesto

Propósito y Visión Estratégica

El presente Manifiesto 2030, impulsado por expertos en gestión y tratamiento de alarmas en CRA, protección contra incendios y seguridad integral, constituye la hoja de ruta estratégica para la consolidación y evolución de la industria de la seguridad integral. En un ecosistema marcado por la interconectividad y la complejidad tecnológica, esta iniciativa busca fortalecer el mercado único europeo, garantizar un crecimiento sostenible y fomentar una cultura proactiva orientada a la protección de vidas y bienes.

Una de las necesidades más básicas de la sociedad actual es la protección frente a las amenazas, en cualquiera de las formas en las que se produzcan. Sin las medidas de protección adecuadas, los ciudadanos que conforman la sociedad afrontan riesgos. Durante décadas, la industria de la seguridad integral ha trabajado eficazmente en el desarrollo de soluciones para prevenir y mitigar las consecuencias de amenazas tales como robos, incendios, daños a la propiedad, accidentes y otros, con una misión: la protección de vidas y bienes. Nuestra industria trabaja para abordar las necesidades de seguridad y protección de la sociedad en colaboración con las Administraciones Públicas y conforme a la legislación vigente, organismos de normalización y certificación y asociaciones profesionales de la industria, respetando los códigos éticos y de cumplimento de prácticas empresariales.

Impulsando la **industria de la Seguridad,** y comprometidos con la sociedad y la ciudadanía, queremos contribuir a fomentar un crecimiento sostenible que fortalezca el mercado único de la UE, atraer inversiones a España y ampliar los mercados globales para las empresas españolas. Para ello, estamos evaluando continuamente las oportunidades y los desafíos a los que nos enfrentamos para identificar las prioridades que nos permitirán avanzar como una sociedad próspera, segura y en nuestra condición de actor global.

El Manifiesto 2030 que ahora presentamos, tiene las siguientes prioridades:

- **desarrollar la industria** de la Seguridad en Europa y ampliar los mercados globales para productos y servicios de calidad;
- **elevar los estándares** para los profesionales de la industria a través de la formación y la cualificación;
- **convertir las tecnologías emergentes en soluciones sostenibles**;
- **avanzar en el conocimiento y la innovación**;
- **desarrollar productos y servicios respetuosos** con el medio ambiente y fomentando la economía circular.

Nuestro objetivo es lograrlo orientados a las siguientes áreas:

- estándares orientados al mercado para productos y servicios;
- pruebas paneuropeas y certificación de productos;
- formación y cualificación;
- digitalización incluyendo ciberseguridad, internet de las cosas y la personas e inteligencia artificial;
- asociarse con organismos de investigación;
- alianzas estratégicas con otras asociaciones de la industria;
- participación en Asociaciones Europeas representativas de la industria, como Euralarm y Eurosafe.

Trabajando juntos, podemos lograr una sociedad más segura para España y construir una industria que contribuya al crecimiento sostenible en España y Europa.

1 Objeto del Manifiesto

Antecedentes

Las empresas miembros de AES que lideran la industria de la Seguridad en España son miembros del Patronato de AES FUNDACIÓN[1]. La participación en el mercado español de dichas empresas es muy relevante, específicamente en conexiones a CRA. En ese sentido de las 3.502.718 conexiones existentes a finales de diciembre de 2024, la cuota de mercado representada por nuestros asociados nos permite compartir experiencia con otros actores de la industria. Por otro lado, estos datos junto con la interlocución con todos los actores de la industria avalan una experiencia en la gestión de la totalidad de las alarmas (incendio, robo, intrusión, atraco, asistencial, técnica...) y en todos los verticales (doméstico, comercial, industrial, bancario, infraestructuras críticas...).

La nuestra es una industria con visión de futuro, que se basa en la innovación y el desarrollo constante y una gran inversión para proporcionar las mejores soluciones y servicios que garanticen la seguridad integral y la protección de la sociedad.

Representamos los intereses de instaladores, compañías de mantenimiento, centrales receptoras de alarmas, fabricantes, distribuidores, ingenierías y laboratorios. Todos nuestros miembros con sus plantillas cualificadas confían en las áreas prioritarias enumeradas anteriormente para diseñar, instalar y mantener esas soluciones y proporcionar los servicios necesarios para garantizar unas prestaciones del más alto nivel.

Con estos antecedentes impulsamos, la elaboración del presente **Manifiesto 2030 sobre la gestión integral de las señales de alarma** como una iniciativa estratégica orientada a reforzar el papel esencial que desempeñan los sistemas de seguridad en la protección de la sociedad. Este documento aborda de manera integral la gestión de señales de alarma (incluyendo las relacionadas con incendios, atracos e intrusiones) en un contexto marcado por la evolución tecnológica, la creciente interconectividad y la necesidad de respuestas más eficientes, centralizadas, coordinadas y fiables.

El Manifiesto se enmarca dentro de nuestro compromiso con la promoción de un modelo de seguridad integral, acorde con la actividad de las empresas de la industria, y con la vocación de anticiparse a los desafíos presentes y futuros. Asimismo, responde a nuestro propósito de fomentar una sólida cultura de la seguridad, sensibilizando a la sociedad sobre su importancia y contribuyendo activamente a la protección de las vidas y de los bienes. En este sentido, el documento aspira a convertirse en una referencia en la industria de la Seguridad Integral, para el desarrollo de buenas prácticas, la colaboración público-privada y la innovación en la gestión de las señales de alarma de cara al horizonte 2030.

[1] AES FUNDACIÓN es una Fundación corporativa perteneciente a la Asociación Española de empresas de Seguridad (AES)

En línea con los objetivos de este Manifiesto 2030, una evaluación de riesgos adecuada, tal y como se profundiza en el apartado correspondiente, es fundamental para desarrollar soluciones proporcionadas y adaptadas al contexto de cada cliente. Este proceso requiere integrar medidas organizativas, tales como la formación especializada del personal y el establecimiento de protocolos de atención e intervención claramente definidos.

En los últimos años, la Unión Europea ha introducido dos directivas clave para reforzar la protección de las infraestructuras críticas: la Directiva sobre la Resiliencia de las Entidades Críticas (CER 2022/2557) y la Directiva sobre Ciberseguridad (NIS2 2022/2555). Ambos marcos buscan garantizar la continuidad de los servicios esenciales y aumentar la resiliencia ante amenazas diversas, afectando directa e indirectamente a gran parte de la economía. El liderazgo que nuestras empresas ejercen en la gestión de infraestructuras estratégicas en nuestro país es prueba de este compromiso.

El concepto de seguridad integral que impulsamos, prevé la implementación de todas las medidas necesarias contra amenazas naturales, fallos técnicos, actos malintencionados o delictivos. En la gestión de las Centrales Receptoras de Alarmas (CRA), contamos con una amplia experiencia y un enfoque que combina medidas estructurales, técnicas y organizativas. Solo mediante la coordinación de la seguridad física (protección contra intrusión e incendios, tecnologías avanzadas de vídeo, seguridad perimetral y control de accesos), ciberseguridad e inteligencia artificial, se puede alcanzar la solvencia necesaria en la gestión remota de señales.

La interdependencia de las infraestructuras críticas es aplicable a todos nuestros clientes. Sectores como el energético o las comunicaciones son vitales, pero también lo es la industria de la Seguridad Privada, tal como establece la propuesta del anteproyecto de Ley de la directiva CER al confirmarlo como sector estratégico.

Independientemente de los plazos de transposición de la directiva CER, la tendencia es clara: el futuro exige la convergencia entre seguridad física de manera integral y la ciberseguridad. Esto tendrá un impacto significativo en nuestras empresas, requiriendo conocimientos especializados tanto en protección de activos como en arquitecturas de red seguras.

Una CRA debe integrar en sus servicios conceptos de seguridad holísticos, vinculando la monitorización informática con los planes de contingencia. Es nuestra responsabilidad asesorar eficazmente a los clientes, elaborando análisis de necesidades individuales que no solo aborden los riesgos actuales, sino que anticipen las amenazas futuras.

1 Objeto del Manifiesto

Visión en la gestión de señales de alarma

Adicionalmente a la legislación vigente y desde nuestra experiencia y visión estratégica, entendemos que la actual tipificación de señales de alarma por tipo, según la norma UNE-EN 50518:2020, debe ser superada para adaptarse a la realidad y complejidad de la sociedad actual. El modelo tradicional, basado en la clasificación de señales de alarma según el tipo de señal (fuego, atraco, intrusión...), resulta cada vez menos adecuado para responder de forma eficaz y eficiente a los riesgos reales que se producen en los entornos protegidos.

En este contexto, proponemos avanzar hacia un modelo de gestión basado en la segmentación del riesgo asociado al evento, en línea con los principios recogidos en la normativa *UNE-ISO 31000:2018, Gestión de riesgos. Principios y directrices*, que se recogen en el apartado 3 de este Manifiesto. Por tanto, el criterio principal de priorización y gestión será el impacto potencial del incidente y su nivel de riesgo, y no únicamente el tipo de señal de alarma.

Este cambio de paradigma permitirá que la respuesta operativa se centre en la protección efectiva de las personas, los bienes y la continuidad de la actividad, priorizando aquellos eventos que, por su contexto o ubicación, puedan generar situaciones de mayor gravedad o afectar a un número elevado de personas.

En particular, resulta evidente que los incidentes que se producen en espacios de pública concurrencia deben ser gestionados de forma remota atendiendo principalmente al nivel de riesgo del evento, y no exclusivamente al tipo de señal de alarma que los origina. En estos casos, la capacidad de análisis, verificación y coordinación resulta crítica para garantizar una respuesta adecuada y proporcional.

Por ello, entendemos que este tipo de señales y eventos deben ser gestionados desde centrales de Categoría I, conforme a los requisitos de resiliencia, redundancia y capacidad operativa establecidos en la norma, UNE-EN 50518:2020 garantizando así los más altos niveles de disponibilidad, excelencia, continuidad de servicio y capacidad de gestión de incidentes críticos.

De igual forma, y con independencia de la naturaleza del riesgo, la gestión de cualquiera de ellos que queden evaluados con un valor medio o alto, deberán ser gestionados desde una CRA de Categoría I conforme a la norma UNE-EN 50518:2020.

La resistencia frente a ataques físicos, la ubicación del equipo de procesamiento de datos, la protección de los cables de comunicación, las fuentes de alimentación y generadores de reserva asociados a la actividad, así como el resto de las instalaciones en general hacen imprescindible que los servicios de gestión integral de señales de alarmas se presten desde una CRA de Categoría I conforme a la norma UNE-EN 50518:2020.

Este enfoque representa una evolución necesaria hacia un modelo de gestión inteligente de eventos de seguridad, donde la tecnología, la normativa y la operación converjan para ofrecer una respuesta eficaz, eficiente, proporcional y alineada con los riesgos reales y necesidades de la sociedad contemporánea.

2 Papel de una Central Receptora de Alarmas

Una Central Receptora de Alarmas (CRA) cumple hoy una función esencial en la seguridad de las personas, los hogares, los bienes y las actividades económicas. Su labor ha evolucionado de forma significativa gestionando actualmente todo tipo de incidencias que ayudan a prevenir riesgos y a reaccionar ante situaciones de emergencia.

Una CRA puede recibir señales de sistemas de seguridad de intrusión y atraco, de cumplimiento de medidas impuestas (órdenes de alejamiento, permisos penitenciarios y en general todo aquello que un juzgado considere que tiene que ser monitorizado), de protección contra incendios, alarmas asistenciales o sanitarias, dispositivos móviles, de protección personal y avisos técnicos procedentes de instalaciones. Esta variedad de información permite que una CRA actúe como un centro preparado para dar una respuesta rápida, especializada y clara ante cualquier necesidad.

Los tiempos en los que un sistema únicamente enviaba una señal sin posibilidad de verificación o coordinación están superados. Hoy, una CRA es un centro avanzado donde cualquier tipo de cliente puede conectar distintos sistemas para lograr una protección completa y adaptada a su día a día. Esta visión integral permite ofrecer seguridad real tanto a las personas como a las actividades que desarrollan.

En línea con la propuesta de valor de AES FUNDACIÓN[2] — **'dinamizando la seguridad ciudadana'** — la CRA no solo impulsa esta industria, sino que contribuye al desarrollo de la economía circular y de la sociedad en su conjunto. Un entorno seguro ayuda a que las personas vivan con tranquilidad y a que las empresas operen con confianza, lo que favorece el crecimiento y el progreso.

En el ámbito residencial, la CRA ofrece un elemento clave para lograr una seguridad completa, combinando la tecnología con la protección física. Gracias a ello, los hogares y sus habitantes cuentan con un respaldo permanente tanto dentro como fuera de su vivienda.

En el entorno corporativo, industrial y comercial, la CRA ayuda a proteger la actividad diaria de las empresas. Integra la seguridad electrónica con la supervisión de procesos, la protección contra incendios y la coordinación ante emergencias, creando espacios más seguros que permiten a cada organización centrarse en su labor principal.

En cualquiera de estos entornos la CRA es, en definitiva, el centro de atención operativo 24 horas al día, los 365 días del año, donde los clientes y usuarios se pueden apoyar para dar atención continua a cualquiera que sea la necesidad que tengan.

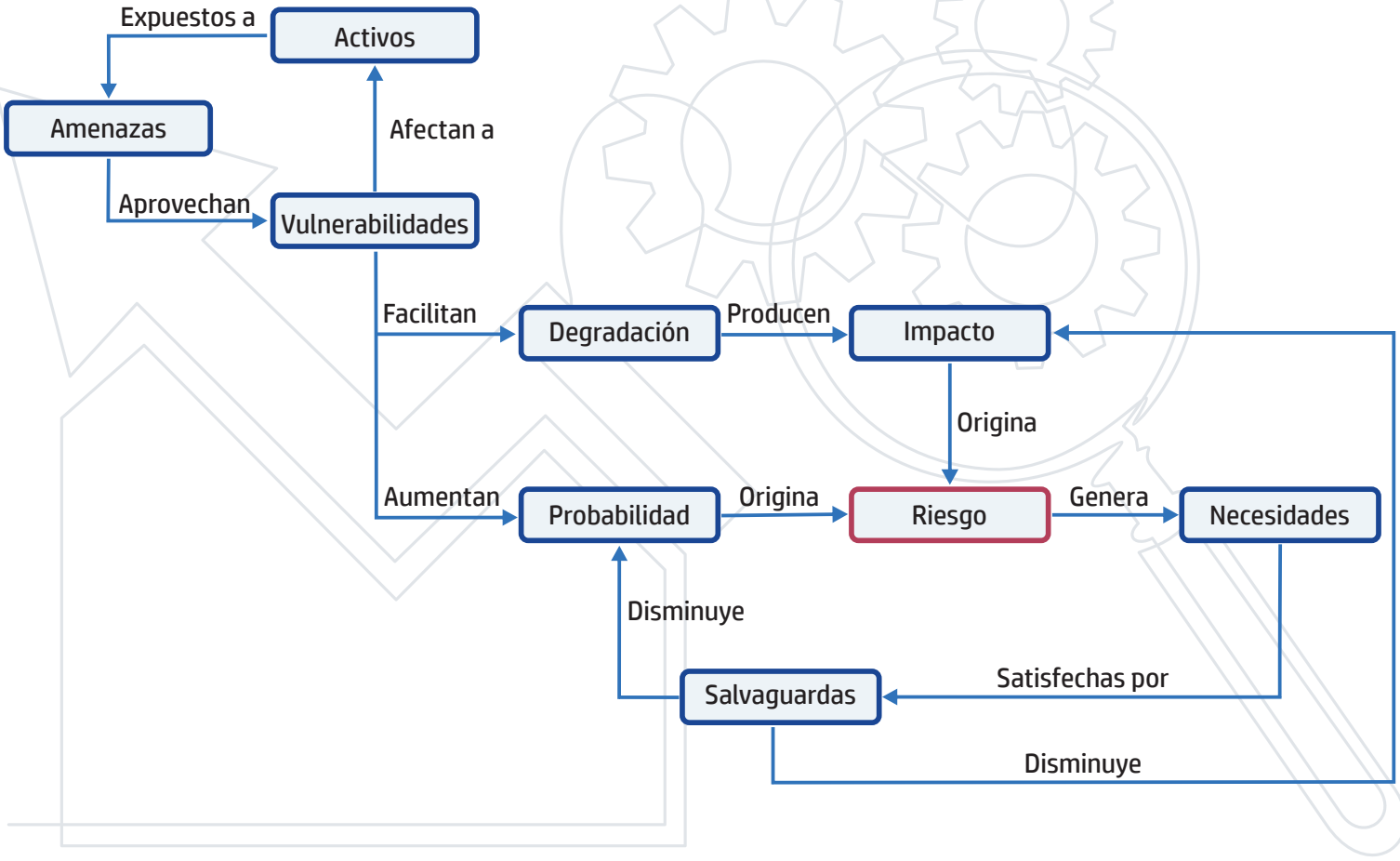
AES reúne a las CRAs más grandes de España que gestionan la mayoría de las conexiones de sistemas de seguridad del país. Este liderazgo permite ofrecer soluciones integrales de calidad, garantizar un servicio continuo y avanzar hacia un modelo de seguridad integral moderno, sencillo de entender y orientado al bienestar de toda la sociedad.

[2] AES FUNDACIÓN es una Fundación corporativa perteneciente a la Asociación Española de empresas de Seguridad (AES)

3 La gestión del Riesgo desde una CRA

Teniendo en cuenta que el objetivo de la CRA es la protección de personas y bienes, resulta imprescindible abordar su diseño y operación desde un enfoque de gestión del riesgo. La norma UNE-ISO 31000:2018 "Gestión del riesgo. Principios y directrices" define el riesgo como el "efecto de la incertidumbre sobre la consecución de los objetivos". En el contexto de la CRA, esta incertidumbre se traduce en la posibilidad de que se materialicen eventos no deseados (intrusiones, sabotajes, incendios, fallos técnicos, incidentes operativos, etc.) que le impidan alcanzar su objetivo principal: proteger de forma eficaz y eficiente a las vidas y los bienes objeto de su protección.

Existen distintos modelos para representar y analizar el riesgo. Un modelo ampliamente aceptado, y especialmente útil en seguridad, parte de la relación entre activos, amenazas y vulnerabilidades, y conecta estos elementos con el impacto y la probabilidad de ocurrencia. Este enfoque permite traducir un concepto abstracto (riesgo) a decisiones concretas (medidas de seguridad), lo que facilita justificar inversiones, priorizar actuaciones y definir niveles de servicio acordes al riesgo.



En este modelo, los activos (personas, instalaciones, mercancías, información, continuidad del negocio, etc.) están expuestos a amenazas que pueden causarles daño. Las amenazas pueden ser malintencionadas (intrusión, robo, sabotaje, agresiones, incendio provocado, etc.), técnicas (fallos de equipos, cortes de suministro, errores de transmisión) o fortuitas/naturales (incendios accidentales, inundaciones, condiciones meteorológicas adversas, etc.). Las amenazas aprovechan las vulnerabilidades del activo o de su entorno: debilidades físicas (localización, construcción, cerramientos, accesos, etc.), tecnológicas (equipos obsoletos, mala configuración, etc.), organizativas (procedimientos insuficientes o ineficaces, falta de formación, etc.) o humanas (errores, prácticas inseguras).

Cuando una amenaza se materializa (es decir, ocurre el evento), puede producir un impacto sobre el activo: daños personales, pérdidas económicas, interrupción de la operativa, deterioro reputacional, sanciones, etc. La magnitud del impacto depende de factores como el valor del activo, el grado de exposición, el tiempo de respuesta y la capacidad de recuperación. Por otra parte, cada amenaza tiene una probabilidad (o posibilidad) de materializarse, que aumenta cuando existen vulnerabilidades y cuando la exposición es alta (por ejemplo, instalaciones aisladas, horarios sin presencia, entornos con mayor criminalidad, equipamiento sin mantenimiento, etc.).

De forma simplificada, el riesgo se puede considerar función de impacto y probabilidad. A partir de la estimación del riesgo surgen necesidades de protección que deben satisfacerse mediante salvaguardas o medidas de seguridad. Estas medidas actúan de dos formas: por una parte, reduciendo la probabilidad de que la amenaza se materialice (disuasión, detección temprana) y por otra minimizando el impacto si la amenaza llega a materializarse (verificación, detección y respuesta rápida, coordinación con recursos, mitigación y recuperación). En consecuencia, la aplicación adecuada de medidas de seguridad contribuye a disminuir el riesgo hasta niveles aceptables.

En este entorno, la conexión a la CRA actúa como una salvaguarda especialmente eficaz y eficiente para reducir el riesgo, porque incorpora capacidades que normalmente no están disponibles en el propio emplazamiento de forma continua: detección, verificación, gestión del tiempo y respuesta coordinada. Su aportación es transversal: mejora tanto la protección frente a amenazas intencionadas (intrusión, robo, sabotaje o incendio provocado) como frente a amenazas fortuitas o técnicas (incendios accidentales, averías, cortes de suministro o fallos de comunicación).

- Ante una intrusión, la transmisión inmediata de señales, junto con procedimientos de verificación (video verificación, audio, verificación secuencial o presencial según el caso), reduce el tiempo hasta la activación de la respuesta, limitando el daño y aumentando la probabilidad de intervención.
- Ante un incendio (provocado o accidental), la recepción temprana de alarmas (detectores automáticos, pulsadores y señales técnicas asociadas) permite activar protocolos y recursos antes de que el incidente evolucione, reduciendo el impacto sobre personas e instalaciones.
- Ante un fallo técnico (pérdida de alimentación, sabotaje de línea, avería de comunicaciones o fallo de supervisión), la CRA gestiona señales técnicas para activar acciones preventivas (comprobación de estado, aviso a mantenimiento y escalados), reduciendo la probabilidad de indisponibilidad del sistema.

3 La gestión del Riesgo desde una CRA

Desde la perspectiva de la gestión del riesgo, la CRA contribuye a reducir la probabilidad, como una medida de disuasión, y el impacto mediante la detección temprana del evento, la verificación y clasificación para decidir el protocolo adecuado, la activación y coordinación de recursos de respuesta (internos y externos) y la trazabilidad para analizar incidencias y mejorar el desempeño. En la práctica esto se traduce en una mejora directa del factor tiempo: se reduce el tiempo desde el inicio del evento hasta la intervención efectiva.

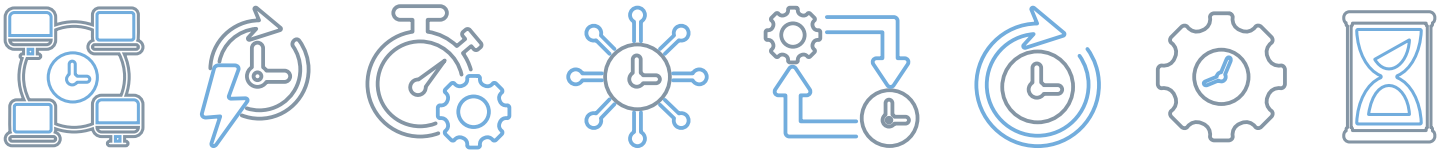
El factor tiempo tiene particulares dependiendo del tipo de amenaza, por ello, resulta útil describir cada tipo de evento mediante modelos temporales que permitan identificar dónde se gana o se pierde tiempo, y qué parte de ese tiempo depende de la instalación, de la CRA y de los recursos de respuesta. Como ejemplo tenemos los modelos de tiempo de una intrusión y de un incendio.

Modelo de tiempos en caso de intrusión

- Tiempo de retardo: tiempo que aportan las medidas de protección (físicas y/o electrónicas) para dificultar el avance del intruso: cerramientos, control de accesos, rejas, puertas, retardos mecánicos, etc.
- Tiempo de ataque: tiempo que necesita el intruso para lograr el éxito inicial del ataque (por ejemplo, franquear el perímetro, abrir un hueco o acceder a una zona protegida).
- Tiempo de detección: tiempo transcurrido desde que se inicia la acción de intrusión hasta que el sistema la detecta y la información llega al primer nivel de respuesta (incluida la transmisión a la CRA cuando aplique).
- Tiempo de consecución del objetivo: tiempo que necesita el intruso para materializar el impacto deseado tras el éxito inicial del ataque (por ejemplo, sustraer bienes, acceder a un objetivo, causar daños o sabotear).
- Tiempo de reacción: tiempo desde la detección hasta que se inicia la respuesta operativa (gestión en CRA, verificación, llamadas, escalado y activación de recursos).
- Tiempo de eficacia: tiempo desde el inicio de la respuesta hasta que esta alcanza un nivel suficiente para impedir el éxito del ataque o, al menos, minimizar su impacto (llegada e intervención efectiva).
- Tiempo de retirada: tiempo que necesita el intruso, una vez alcanzado su objetivo, para abandonar el lugar y reducir la probabilidad de identificación (huida, ocultación de evidencias, etc.).
- Tiempo de respuesta: suma de los tiempos de detección, reacción y eficacia. Es el tiempo total que tarda la organización en pasar de “evento iniciado” a “intervención efectiva”.

El objetivo es impedir que el intruso alcance el impacto deseado. Para ello, la respuesta debe ser efectiva antes de que transcurra el tiempo que el intruso necesita para completar el ataque y explotar sus efectos. En términos operativos:

Tiempo de respuesta < Tiempo de ataque + Tiempo de consecución del objetivo



Modelo de tiempos en caso de incendio

T0 - Inicio (ignición): instante en el que se inicia la combustión (normalmente no observable).

T1 - Crecimiento hasta señal detectable: intervalo desde T0 hasta que el incendio genera señales detectables (humo, temperatura o llama) en el punto de detección. Depende del escenario (carga de fuego, ventilación, geometría, etc.).

T2 - Detección: tiempo desde que existe una condición detectable hasta que el sistema la detecta y genera la alarma (detectores, pulsadores, aspiración, etc.).

T3 - Transmisión a CRA / primer nivel de respuesta: tiempo desde la generación de la alarma hasta su recepción por la CRA o por el primer nivel de respuesta definido (comunicaciones, encaminamiento, redundancias).

T4 - Verificación y clasificación: tiempo desde la recepción hasta identificar el tipo de evento y activar el protocolo (confirmación por doble tecnología, vídeo, audio, llamada al emplazamiento, aplicación del plan, etc.).

T5 - Aviso / despacho: tiempo desde la decisión de actuación hasta el aviso efectivo (112/bomberos, responsable de emergencias, personal interno, vigilantes, etc.).

T6 - Movilización y llegada: tiempo desde el despacho hasta la llegada del primer recurso al emplazamiento (brigada interna, vigilancia, mantenimiento, bomberos).

T7 - Intervención inicial efectiva: tiempo desde la llegada hasta el comienzo de acciones eficaces (reconocimiento, acceso, corte de suministros, primer ataque con extintores/BIE, activación de evacuación y sectorización).

T8 - Control: tiempo desde el inicio de la intervención hasta detener el crecimiento (incendio controlado, sin propagación).

T9 - Extinción y rehabilitación: extinción completa, ventilación, comprobación de puntos calientes, restablecimiento seguro del servicio y retorno progresivo a la normalidad.

TCC - Tiempo hasta Condiciones Críticas tiempo desde el inicio del incendio hasta que se supera un umbral que compromete la vida, la evacuación o la continuidad (p. ej., visibilidad insuficiente por humo, temperatura elevada, colapso de elementos, pérdida de compartimentación, propagación a zonas críticas, etc.).

Tiempo de Respuesta: desde la detección del incendio hasta la intervención inicial efectiva

El objetivo es actuar antes de que el incendio sea incontrolable y alcance un punto en el que el impacto sobre las personas y los bienes sea inaceptable. En términos operativos:

Tiempo de Respuesta Total < Tiempo hasta Condiciones Criticas

Si comparamos los modelos de tiempos vemos sus similitudes

Modelo	Objetivo
Intrusión	Tiempo de respuesta < Tiempo de ataque + Tiempo de consecución del objetivo
Incendio	Tiempo de respuesta total < Tiempo hasta condiciones críticas

La CRA ayuda a dar respuesta a una de las cuestiones críticas en seguridad, independientemente de la amenaza, llegar a tiempo: actuar antes de que una amenaza se materialice (prevención) o, si ya se ha materializado, intervenir con la suficiente rapidez para limitar su impacto (mitigación).

Además, la CRA aporta trazabilidad (registro de eventos), disciplina operativa (procedimientos estandarizados), y mejora continua (análisis de incidencias y tiempos de respuesta), lo que facilita el ciclo de gestión del riesgo: identificar amenazas y vulnerabilidades, analizar y evaluar el riesgo, tratarlo mediante medidas adecuadas, y monitorizar el desempeño para ajustar niveles de protección.

Entender el riesgo como la combinación de probabilidad e impacto permite justificar el papel de la CRA como salvaguarda clave. No se limita a “recibir señales”, sino que habilita una respuesta organizada y medible que reduce tiempos, mejora la detección y ayuda a minimizar las consecuencias en caso de materialización de una amenaza, contribuyendo a que el riesgo se mantenga dentro de umbrales aceptables para la organización.

Por último, hay que tener en cuenta que los registros de eventos y las comunicaciones telefónicas de una CRA cumplen con todos los requisitos que establece la legislación de Seguridad Privada y la referente a protección de datos, garantizando la confidencialidad, integridad y disponibilidad de las mismas, y aportan información fundamental tanto en las investigaciones de las Fuerzas y Cuerpos de Seguridad, como en las actuaciones judiciales en procesos penales y civiles.

4 La normativa en una CRA

Teniendo en cuenta que las Centrales Receptoras de Alarma constituyen uno de los pilares esenciales sobre los que se sustenta no sólo el sistema actual de seguridad privada sino la seguridad ciudadana en general, su función no solo trascienden de la mera recepción de señales, sino que representan un punto crítico de coordinación, verificación y respuesta ante situaciones que pueden afectar gravemente a personas, bienes e infraestructuras y especialmente en un entorno cada vez más digitalizado y expuesto a mayores riesgos, el cumplimiento de la normativa vigente en seguridad privada no debe ser tenida en cuenta como una mera obligación legal, sino como un compromiso de calidad en el servicio.

Su funcionamiento está regulado principalmente por la Ley 5/2014 de Seguridad Privada, la Orden INT/316/2011, que establece las reglas de funcionamiento de los sistemas de alarma y la Norma EN 54-21, que establece la normativa para la conexión de los sistemas de protección contra incendios.

LEY 5/2014

La Ley 5/2014, de 4 de abril, de Seguridad Privada, regula las actividades, servicios y funciones de seguridad privada en España, incluyendo de forma expresa a las Centrales Receptoras de Alarma. De acuerdo con la Ley 5/2014, la actividad de la centralización de alarmas constituye un servicio reservado a empresas de seguridad autorizadas.

Para poder operar con una CRA, las empresas deben cumplir los siguientes requisitos:

- Autorización precisa del Ministerio de Interior.
- Estar inscrita en el Registro Nacional de Seguridad Privada.
- Disponer de medios técnicos y humanos adecuados para el desarrollo de la actividad.
- Garantizar la solvencia económica y organizativa.

La Ley 5/2014 establece que una CRA puede realizar las siguientes funciones por normativa:

- Recepción y gestión de señales de alarma.
- Verificación de las alarmas recibidas.
- Transmisión de alarmas verificades a las Fuerzas y Cuerpos de Seguridad.
- Comunicación con los titulares de los sistemas de seguridad.

A continuación, se describen brevemente los artículos de la legislación vigente que establecen las funciones:

- Los servicios de verificación de alarmas consisten en la recepción, verificación, y en caso necesario, transmisión a las Fuerzas y Cuerpos de Seguridad de las señales de alarma que se produzcan en los dispositivos de seguridad de los usuarios (Artículo 15. Servicios de verificación de alarmas).
- Las empresas de seguridad que presten servicios de central de alarmas deben disponer de un sistema de verificación de las señales recibidas, con el fin de evitar las falsas alarmas y asegurar la intervención policial solo cuando sea necesario. (Artículo 39. Características de los Servicios).
- Las centrales receptoras de alarmas están obligadas a recibir y verificar las señales de alarma, comunicar de inmediato a las Fuerzas y Cuerpos de Seguridad competentes las alarmas que hayan sido verificades como reales y, por último, prestar servicios de respuesta ante alarmas, mediante el desplazamiento de vigilantes de seguridad y, en su caso, la apertura y custodia de llaves. (Artículo 47. Funciones de las centrales receptoras de alarmas).
- A la vez, también tienen prohibiciones tales como la transmisión a las Fuerzas y Cuerpos de Seguridad de señales de alarma que no se hayan verificado como reales siguiendo la normativa de desarrollo. (Artículo 51. Prohibiciones).

También se establece que el personal en una CRA debe estar debidamente habilitado cuando la normativa lo exija, actuar conforme a los principios de legalidad, integridad y profesionalidad y estar sujeto a la confidencialidad respecto a la información manejada. Adicionalmente, el operador de CRA u operador de seguridad, debe tener la consideración de personal acreditado conforme a lo que se establezca regulatoriamente.

Las medidas de seguridad y control tienen que garantizar la continuidad del servicio, la protección contra accesos no autorizados y el registro y conservación de las señales y actuaciones realizadas.

Por último, la Ley 5/2014 establece un régimen de responsabilidad y sanciones (clasificadas en leves, graves y muy graves) que pueden incluir sanciones económicas, suspensión temporal de funciones y sueldo y la cancelación de la autorización.

Orden INT/316/2011

La Orden INT/316/2011, tiene por objeto regular el funcionamiento de los sistemas de alarmas en la seguridad privada, establece los requisitos técnicos, operativos y procedimentales que deben cumplir los sistemas y las Centrales Receptoras de Alarma.

Esta orden se aplica a las empresas de seguridad que prestan servicios de conexión a Centrales Receptoras, a las propias receptoras al ser centros de recepción, verificación y transmisión de señales y a los usuarios conectados.

La CRA debe recibir y gestionar todas las señales procedentes de los sistemas conectados, registrar las señales y las actuaciones realizadas y garantizar la trazabilidad de las mismas. Esta gestión debe realizarse de forma continua, permanente y con sistemas que aseguren la disponibilidad del servicio.

Un aspecto central de la ORDEN INT/316/2011, es la regulación de la verificación de alarmas. Estas verificaciones pueden ser realizadas por diferentes métodos:

- ✓ Verificación secuencial: confirmación mediante la activación de varios elementos del sistema.
- ✓ Verificación mediante vídeo: comprobación visual en tiempo real.
- ✓ Verificación mediante audio: escucha de sonidos en el lugar protegido.
- ✓ Verificación personal: intervención directa de personal de seguridad.

La Orden establece, con carácter general, que solo las alarmas verificadas podrán ser comunicadas a las Fuerzas y Cuerpos de Seguridad.

A continuación, se describen brevemente los métodos de verificación:

- Se podrá confirmar una señal de alarma si hay la recepción sucesiva de tres o más señales de detección procedentes de la misma, de elementos de detección diferentes en un tiempo determinado (Artículo 15. Verificación mediante confirmación secuencial).
- En la verificación de la señal de alarma por vídeo, la receptora deberá de disponer de imágenes, en tiempo real o grabadas, que permitan identificar de forma precisa e inequívoca la presencia de personas o circunstancias que motiven la activación del sistema (Artículo 16. Verificación mediante vídeo).
- En la verificación por audio se realizará una escucha activa de lo que sucede en el inmueble, siempre que el sistema permita la transmisión de sonido y este aporte elementos suficientes para confirmar la intrusión (Artículo 17. Verificación mediante audio).
- La verificación personal consistirá en el desplazamiento de vigilantes de seguridad al lugar de los hechos para realizar las comprobaciones oportunas, pudiendo estos acceder al interior si disponen de las llaves del inmueble (Artículo 18. Verificación personal).

La CRA debe de cumplir diferentes requisitos técnicos según la Orden INT/316/2011, estos son disponer de sistemas redundantes de alimentación y alimentaciones, equipos capaces de gestionar múltiples señales simultáneamente, medidas de seguridad física y lógica y sistemas de grabación y almacenamiento de información.

Las obligaciones de responsabilidad y control de una CRA se resumen en la correcta aplicación de los procedimientos de verificación anteriormente descritos, la adecuada gestión de las señales y el cumplimiento de los requisitos técnicos.

EN 54-21

La norma EN 54-21 forma parte de la serie de normas europeas EN 54, relativas a los sistemas de detección y alarma de incendios, y en particular, la 54-21, regula los equipos de transmisión de alarmas y avisos de fallo para comunicar eventos desde un sistema de detección de incendios hasta una Central Receptora de Alarmas.

Los equipos de transmisión conectados a una CRA, en el contexto de la EN 54-21, deben garantizar la transmisión fiable de señales de alarma y fallo, supervisar continuamente el estado de la conexión, detectar e informar de interrupciones en la comunicación y disponer de protección frente a interferencias y sabotajes.

4 La normativa en una CRA

La CRA debe tener una supervisión continua de la comunicación entre el sistema de incendio, así como una monitorización permanente, cualquier fallo debe detectarse dentro de un tiempo máximo preestablecido y la recepción inmediata de los fallos críticos. También debe de ser compatible con los equipos de transmisión normativos, interpretar correctamente las señales recibidas y un procedimiento de actuación inmediata predefinido.

Por último, la norma exige que las señales de alarma recibidas de los sistemas de detección y alarma de incendios tengan prioridad sobre otras, se garantice la integridad de los datos recibidos y se evite la pérdida o alteración de la información.

La gestión de señales como pilar del modelo de seguridad integral

El Manifiesto 2030, parte de una premisa clara: la seguridad moderna no puede entenderse como un conjunto de elementos aislados, sino como un sistema integrado donde la información, la tecnología, la profesionalidad del personal y la capacidad de respuesta operativa deben estar plenamente alineadas.

En este modelo, la gestión de señales actúa como nexo entre los sistemas de detección y la respuesta operativa, permitiendo transformar eventos técnicos en decisiones que tienen un impacto directo en la protección de personas y bienes.

Esta visión se apoya en un marco normativo ya consolidado en España, encabezado por la Ley 5/2014 de Seguridad Privada, el Reglamento de Seguridad Privada y las Órdenes INT/314/2011 e INT/316/2011, y resto de normas que sean de aplicación y que establecieron las bases para una gestión rigurosa, profesional y trazable de las alarmas, y del que se habla en el apartado anterior.

Lejos de limitarse a una función de recepción, la CRA asume un papel activo y constante como centros de análisis, verificación y coordinación permanente, en los que cada señal, del tipo que sea, es evaluada conforme a procedimientos definidos y protocolos específicos, garantizando una respuesta ajustada a su nivel de criticidad.

Normativa y estándares: fundamentos de fiabilidad y confianza

El desarrollo de este modelo se sustenta en la aplicación de estándares técnicos armonizados que aseguran la calidad y fiabilidad de los sistemas. Normas como la UNE-EN 50131 para intrusión, la UNE-EN 50136 para transmisión de alarmas o la serie UNE-EN 54 para detección de incendios establecen los requisitos que deben cumplir tanto los equipos como las infraestructuras de comunicación.

En instalaciones de alto riesgo (entidades financieras, joyerías o infraestructuras críticas...), estos requisitos se intensifican, exigiendo sistemas de grado 3 o 4, comunicaciones redundantes y supervisadas, y una elevada capacidad de integración entre subsistemas.

Este enfoque normativo no solo garantiza la robustez técnica, sino que también refuerza la confianza en el sistema, un elemento clave en el planteamiento del Manifiesto 2030, que aspira a consolidar un modelo de seguridad integral, fiable, interoperable y orientado a la protección efectiva.

5 Conexiones de señales de alarma: fuego, atraco e intrusión.

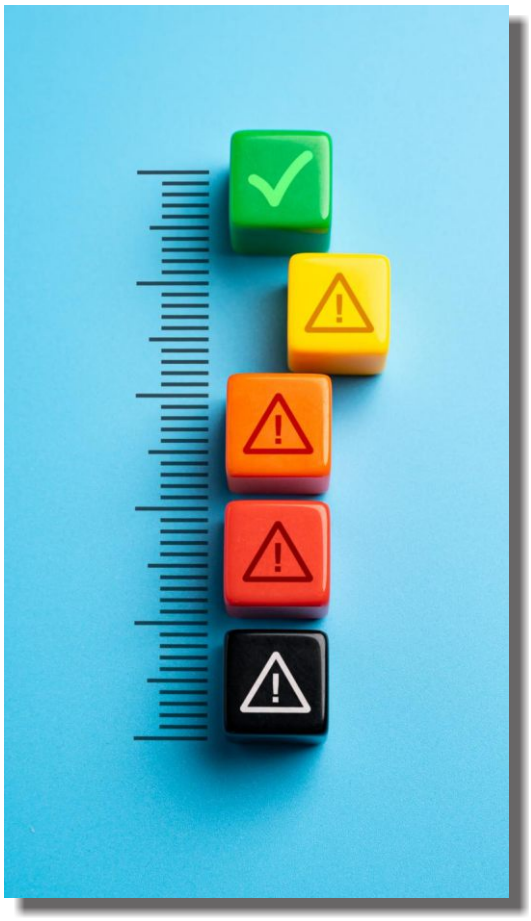
La naturaleza de la señal define la respuesta

Uno de los aspectos tradicionales en la gestión de alarmas es la diferenciación operativa en función del tipo de señal, una cuestión ampliamente abordada tanto en la normativa como en las publicaciones técnicas del sector. Queremos abordar, en este enfoque, una aproximación diferente en la gestión de alarmas, priorizando una clasificación por nivel de riesgo que aporte un mayor nivel de seguridad y fiabilidad de los distintos subsistemas de seguridad establecidos.

Las **señales de incendio**, reguladas por el Reglamento de Instalaciones de Protección Contra Incendios (RD 513/2017) y las normas UNE-EN 54, se gestionan bajo el principio de máxima prioridad, dado su impacto potencial sobre la vida de las personas. Su transmisión a la CRA debe ser automática e inmediata, y su tratamiento requiere garantizar la recepción, verificación y escalado sin demora hacia los servicios de emergencia.

Paralelamente, las **señales de intrusión** requieren un proceso más diverso de verificación previo a su comunicación a las Fuerzas y Cuerpos de Seguridad, conforme a lo establecido en la Orden INT/316/2011. Este proceso, que debe realizarse desde la CRA mediante verificación secuencial, audio y vídeo e incluso activando el desplazamiento de personal de seguridad al lugar de la alarma, procedimientos de los que se ha hablado con anterioridad, tiene como objetivo reducir las falsas alarmas y optimizar la intervención policial, pero garantizando una respuesta en caso de alarma confirmada, constituyendo uno de los pilares operativos del sistema.

Las **señales de atraco**, sin embargo, presentan una lógica distinta. Al tratarse de activaciones manuales asociadas a situaciones de riesgo inmediato para las personas, los procedimientos contemplan, en la mayoría de los casos, la comunicación directa a las Fuerzas y Cuerpos de Seguridad sin verificación previa, lo que refleja su carácter crítico y la necesidad de una respuesta inmediata.



Instalaciones de alto riesgo: exigencia operativa y tecnológica

El Manifiesto 2030 quiere poner especial énfasis en la gestión de señales en entornos de alta criticidad, donde la complejidad técnica y la exigencia operativa alcanzan su máximo nivel.

En estos escenarios, la infraestructura debe garantizar una comunicación continua, supervisada y redundante, mientras que la operativa en CRA debe apoyarse en protocolos específicos adaptados a cada instalación, sistemas avanzados de verificación y una capacidad de priorización dinámica de eventos.

Además, la prestación de servicios complementarios y de valor añadido, como la aplicación de los planes de acción y seguridad acordados con los titulares de los inmuebles, la interacción con el personal de seguridad en el mismo o la coordinación con Fuerzas y Cuerpos de Seguridad y con los servicios de emergencia, refuerza el carácter integral del modelo, siempre conforme a los requisitos de verificación e intervención establecidos regulatoriamente y conforme a procedimientos auditables.

Innovación y futuro: hacia un modelo de seguridad inteligente impulsado por IA

Uno de los ejes estratégicos de este Manifiesto 2030 es la anticipación a los desafíos derivados de la creciente digitalización y complejidad de los entornos de seguridad. En este escenario, la evolución de las Centrales Receptoras de Alarma hacia modelos de centros de gestión y operaciones de seguridad no puede entenderse sin el papel creciente de la tecnología y sobre todo de la inteligencia artificial (IA) en los procesos de gestión y verificación de señales.

La incorporación de IA está transformando de manera progresiva el modelo operativo tradicional, introduciendo capacidades avanzadas de análisis, automatización y apoyo a la toma de decisiones. En el ámbito de la gestión de señales, su impacto se materializa principalmente en tres dimensiones clave.

En primer lugar, la IA permite una mejora sustancial en la clasificación y priorización de alarmas. Mediante el análisis de patrones históricos, comportamiento de dispositivos y contexto operativo, los sistemas pueden identificar anomalías de una manera rápida y precisa, reduciendo significativamente el volumen de falsas alarmas y optimizando la carga de trabajo en la CRA. Este aspecto resulta especialmente relevante en entornos de alta actividad, donde la eficiencia en la discriminación de eventos es crítica.

En segundo lugar, la inteligencia artificial está impulsando una evolución en los métodos de verificación, particularmente a través de la analítica de vídeo. Las soluciones basadas en IA permiten detectar intrusiones reales, identificar comportamientos sospechosos o discriminar eventos no relevantes (movimientos ambientales, animales, etc.), reforzando los procesos de vídeo verificación establecidos en la Orden INT/316/2011. De este modo, la verificación se vuelve más robusta, objetiva y escalable.

En tercer lugar, la IA introduce capacidades de automatización operativa, facilitando la ejecución de acciones predefinidas en función del tipo de señal y su nivel de criticidad. Esto incluye desde la generación automática de flujos de trabajo hasta la activación de protocolos de comunicación, siempre bajo supervisión humana. Este enfoque híbrido (automatización supervisada) se alinea con los principios normativos vigentes, en los que la responsabilidad última de la gestión sigue recayendo en personal habilitado.

Adicionalmente, el uso de modelos analíticos avanzados permite avanzar hacia una gestión predictiva de la seguridad, anticipando posibles incidencias a partir del análisis de tendencias, fallos recurrentes o comportamientos anómalos en los sistemas. Esta capacidad supone un cambio relevante en el paradigma operativo, evolucionando desde un modelo reactivo hacia uno proactivo.

No obstante, la integración de IA en la gestión de alarmas debe abordarse desde un enfoque responsable, garantizando la transparencia de los algoritmos, la protección de datos y el cumplimiento del marco normativo aplicable. En este sentido, AES FUNDACIÓN[3] subraya la importancia de que **la innovación tecnológica vaya acompañada de estándares, buenas prácticas y un marco ético que refuerce la confianza en el sistema**, así como evoluciones regulatorias acordes a estas realidades.

En definitiva, la inteligencia artificial se posiciona como un elemento habilitador clave en la transformación de las CRA, permitiendo mejorar la eficiencia, la precisión y la capacidad de respuesta, y consolidando su papel como núcleo de un modelo de seguridad integral, avanzado y preparado para los retos del horizonte 2030.

[3] AES FUNDACIÓN es una Fundación corporativa perteneciente a la Asociación Española de empresas de Seguridad (AES)

6 Aportaciónes de una CRA

Las Centrales Receptoras de Alarma aportan un valor social fundamental reforzando la protección de personas, bienes e infraestructuras. Su contribución no se limita a la detección y gestión de señales críticas: desempeñan un papel clave en la eficiencia de las fuerzas de seguridad ciudadana.

Tanto si vemos la Seguridad como una sensación como si hacemos un cálculo metódico de riesgos, probabilidad e impacto de los mismos, en cualquier caso, la CRA ofrece una manera directa de incrementar ese nivel o sensación de seguridad de una manera altamente eficiente.

Cuando un ciudadano, empresa u organismo público contrata servicios de seguridad privada (conexión a CRA, un servicio de acuda o cualquier solución especializada) está contribuyendo indirectamente a optimizar el uso de los recursos públicos. Al gestionar de manera profesional un número elevado de incidencias, verificaciones y alarmas, la CRA reduce la carga operativa que de otro modo recaería en Fuerzas y Cuerpos de Seguridad o servicios de emergencia.

Esta colaboración permite que los recursos públicos aumenten su presencia y nivel de servicio para la sociedad en general, en la prevención y persecución del delito, así como que puedan mejorar la respuesta ante emergencias reales sin necesidad de incrementar el gasto público. Como resultado, se eleva el nivel de seguridad general de la sociedad y se mejora la eficiencia del uso de los presupuestos de la Administración pública.

Además, la CRA impulsa el desarrollo tecnológico y la profesionalización de la industria, generando empleo cualificado y contribuyendo a un ecosistema industrial sólido y alineado con la innovación.

Su aportación, por tanto, es doble: proteger de manera directa y fortalecer la capacidad del sistema público sin aumentar su coste, consolidando así un modelo de seguridad moderno, sostenible y beneficioso para toda la sociedad.

1. Representatividad en la Industria de la Seguridad.

Las empresas asociadas a AES representan una parte muy relevante del mercado español de la seguridad física y electrónica, de conexiones a CRA y de instalaciones y mantenimientos.

2. Compromiso con la seguridad integral.

El Manifiesto 2030 se enmarca en nuestro compromiso con la promoción de un modelo de seguridad integral, acorde con la actividad de las empresas de la industria, y con la vocación de anticiparse a los desafíos presentes y futuros. Asimismo, responde a nuestro propósito de fomentar una sólida cultura de la seguridad, sensibilizando a la sociedad sobre su importancia y contribuyendo activamente a la protección de las personas y de los bienes.

3. Cultura de la seguridad.

AES FUNDACIÓN[4] promueve e impulsa la concienciación social y la protección activa de vidas y bienes, realizando acciones de divulgación dirigidas a la sociedad.

Dentro de estas acciones se destaca la publicación de guías de buenas prácticas sectoriales, los boletines informativos y las Newsletters que contribuyen a difundir el mensaje institucional de la Fundación.

4. Marco europeo.

Adicionalmente y dada la participación activa de AES en Asociaciones Europeas representativas de la industria, como Euralarm y Eurosafe, así como su implicación mediante la secretaría del CTN108 en la elaboración de normas europeas, se incorporan al Manifiesto 2030 por su relevancia e impacto en la industria, las dos directivas que la Unión Europea ha introducido para reforzar la protección de las infraestructuras críticas: la Directiva sobre la Resiliencia de las Entidades Críticas (CER 2022/2557) y la Directiva de Ciberseguridad (NIS2 2022/2555).

[4] AES FUNDACIÓN es una Fundación corporativa perteneciente a la Asociación Española de empresas de Seguridad (AES)

5. Modelo integral operativo.

El concepto de seguridad integral que impulsamos en este Manifiesto 2030, prevé la implementación de todas las medidas necesarias contra amenazas naturales, fallos técnicos, actos malintencionados o delictivos. En la gestión de las Centrales Receptoras de Alarmas (CRA), contamos con una amplia experiencia y un enfoque que combina medidas estructurales, técnicas y organizativas. Solo mediante la coordinación de la seguridad física —rotección contra intrusión e incendios, tecnologías avanzadas de vídeo, seguridad perimetral y control de accesos—ciberseguridad e inteligencia artificial, se puede alcanzar la solvencia necesaria en la gestión remota de señales.

6. Evolución del paradigma: de la tipología a la gestión integral del riesgo.

Conforme a la legislación vigente y desde nuestra experiencia y visión estratégica, consideramos que la actual tipificación de señales de alarma por tipo debe ser superada para adaptarse a la realidad y complejidad de la sociedad actual. El modelo tradicional, basado en la clasificación de señales de alarma según el tipo de señal (fuego, atraco, intrusión...), resulta cada vez menos adecuado para responder de forma eficaz y eficiente a los riesgos reales que se producen en los entornos protegidos.

En este contexto, proponemos avanzar hacia un modelo de gestión basado en la segmentación del riesgo asociado al evento, en línea con la normativa UNE-ISO 31000:2018. Por tanto, el criterio principal de priorización y gestión será el impacto potencial del incidente y su nivel de riesgo, y no únicamente el tipo de señal de alarma.

Este cambio de paradigma permitirá que la respuesta operativa se centre en la protección efectiva de las personas, los bienes y la continuidad de la actividad, priorizando aquellos eventos que, por su contexto o ubicación, puedan generar situaciones de mayor gravedad o afectar a un número elevado de personas.

En particular, resulta evidente que los incidentes que se producen en espacios de pública concurrencia deben ser gestionados de forma remota atendiendo principalmente al nivel de riesgo del evento, y no exclusivamente al tipo de señal de alarma que los origina.

Por ello, entendemos que este tipo de señales y eventos deben ser gestionados desde una CRA Categoría I conforme a la norma UNE-EN 50518:2020 garantizando así los más altos niveles de disponibilidad, excelencia, continuidad de servicio y capacidad de gestión de incidentes críticos.

Este enfoque representa una evolución necesaria hacia un modelo de gestión inteligente de eventos de seguridad, donde la tecnología, la normativa y la operación converjan para ofrecer una respuesta eficaz, eficiente, proporcional y alineada con los riesgos reales y necesidades de la sociedad contemporánea.

7. Formación continua.

Impulso a la capacitación especializada de los operadores de seguridad integral de la CRA, de los técnicos instaladores y mantenedores de los sistemas y de los ingenieros de seguridad.

8. Actualización normativa.

Desde AES FUNDACIÓN[5] participamos e impulsamos en la adaptación constante al marco legislativo vigente y emergente, tanto a nivel Europeo como Nacional y Autonómico.

9. Digitalización y colaboración.

Nuestra vocación es liderar, junto con el resto de la industria y mediante el fomento de la colaboración público-privada, el desarrollo y la implementación de herramientas digitales que faciliten la gestión técnico-administrativa y el intercambio de información entre la Seguridad Privada y la Seguridad Pública.

Asimismo, es nuestra intención y forma parte de nuestros objetivos, extender esta colaboración al resto de la Administración Pública, con especial atención a los cuerpos de bomberos y emergencias.

10. Excelencia operativa.

Con objeto de garantizar una protección de vidas y bienes, eficaz, eficiente y alineada con los riesgos y amenazas actuales y futuras, la gestión integral de señales de alarma debe realizarse, como mínimo, desde una CRA de Categoría I conforme a la norma UNE-EN 50518:2020.

[5] AES FUNDACIÓN es una Fundación corporativa perteneciente a la Asociación Española de empresas de Seguridad (AES)

Elaborado por el grupo de trabajo creado ad hoc
por la Junta Directiva de AES incorporando a
expertos en seguridad integral

AES
ASOCIACIÓN ESPAÑOLA
EMPRESAS DE SEGURIDAD

C/Alcalá, 99 2ºA - 28009 Madrid
Telf. 915 765 225

www.aesseguridad.es / aes@aesseguridad.es

www.aesfundacion.es / patronato@aesfundacion.es

@aes_seguridad

ASOCIACIÓN ESPAÑOLA DE
EMPRESAS DE SEGURIDAD

aesseguridad2021

@FundacionAES

AES Fundación

aes_fundacion_