La evolución hacia la gestión integral del riesgo: análisis analítico del Manifiesto 2030 de AES (Parte III de IV)

La vertebración de un posible modelo unificado para la gestión remota de alarmas invitaría a trascender la mera parametrización técnica para adentrarse en el dominio estratégico de la toma de decisiones. En esta tercera iteración del estudio normativo del sector, se somete a un riguroso escrutinio el documento titulado **«Manifiesto 2030: Gestión integral de las señales de alarma», impulsado por AES Fundación**.

Para comprender la magnitud de este texto, resultaría necesario contextualizar previamente la evolución teórica de la figura de la central receptora de alarmas (CRA) y, por extensión, de las centrales receptoras de ncendios (CRI). El manifiesto sugiere que los tiempos en los que un sistema de seguridad se limitaba a emitir una señal unidireccional, carente de posibilidad de verificación o coordinación, estarían ampliamente superados.

En el escenario contemporáneo, la CRI se conceptualizaría no como un mero nodo pasivo de recepción, sino como un centro avanzado, permanente y operativo las 24 horas del día, cuya función esencial radicaría en la protección integral de las personas, los bienes y la continuidad de las

actividades corporativas y comerciales. Desde esta óptica, la conexión a una central receptora de alarmas actuaría teóricamente como una salvaguarda transversal y altamente eficiente diseñada para mitigar activamente el riesgo.

Es precisamente bajo este prisma donde el documento de AES Fundación podría erigirse conceptualmente como una declaración de intenciones que plantea la hipótesis de un cambio de paradigma insoslayable para la industria. El texto propondría distanciarse de la ingeniería puramente prescriptiva para abordar la seguridad desde la alta gestión estratégica y la resiliencia.

Dado su carácter fundacional, resultaría imperativo analizar sus postulados generales, diseccionando, a través de diversas interrogantes, cómo la disciplina de la gestión del riesgo podría superponerse a la estricta tipología de las emergencias para redefinir teóricamente la operatividad y el propósito mismo de estas centrales receptoras de alarmas.

¿Cuál sería el fundamento epistemológico que invalidaría la clasificación tradicional basada en la tipología de la señal?

Históricamente, la arquitectura operativa de la seguridad electrónica parece haberse fundamentado en un modelo de clasificación rígidamente condicionado por la naturaleza tecnológica de la señal, categorizando los eventos en compartimentos estancos predefinidos tales como fuego, atraco o intrusión, en observancia de los estándares técnicos habituales.

El manifiesto sugiere que este enfoque podría resultar obsoleto e insuficiente para responder con la debida eficacia a la fenomenología de **la sociedad contemporánea, caracterizada por su extrema complejidad e interconectividad**. La disrupción conceptual radicaría en proponer la superación de esta categorización estática para transitar hacia una segmentación dinámica que estaría sustentada, de forma íntegra, en el nivel de riesgo asociado al evento.

Bajo esta nueva perspectiva, el vector que debería gobernar la priorización y el tratamiento de una señal de alarma en la central receptora ya no sería de forma exclusiva la etiqueta del sensor que la origina, sino la evaluación prospectiva del impacto potencial del incidente.

Esta redefinición perseguiría alinear la respuesta operativa con la protección efectiva de las personas y la continuidad de la actividad, sugiriendo que el despliegue de recursos habría de ser estrictamente proporcional a la gravedad que el contexto, la vulnerabilidad y la ubicación del evento pudiesen indicar de forma combinada.

¿Cómo redefiniría la norma UNE-ISO 31000 el concepto de riesgo en el ecosistema propuesto para las centrales receptoras de alarmas?

Para dotar de un hipotético rigor métrico y metodológico a esta declaración de intenciones, el modelo estratégico de AES propone anclarse de forma indubitada en los **principios rectores de la norma UNE-ISO 31000:2018**.

Este estándar internacional proporciona un marco teórico que define el riesgo, en su acepción más pura y analítica, como el efecto de la incertidumbre sobre la consecución de los objetivos de una organización.

Al extrapolar esta definición dogmática al entorno operativo propuesto para una central receptora de alarmas, el objetivo principal e inalienable se centraría en la protección eficaz y eficiente de las vidas y los bienes. Por consiguiente, la incertidumbre se materializaría en la probabilidad de que aconteciesen eventos no deseados —ya fuesen actos malintencionados como intrusiones, o bien amenazas fortuitas como incendios— que impidieran o degradaran el cumplimiento de dicho objetivo protector.

La norma establece que la gestión del riesgo no debería ser un ente aislado, sino que su propósito nuclear sería la creación y la protección del valor, debiendo estar integrada, ser estructurada, exhaustiva, adaptada a la organización, inclusiva y dinámica frente a los cambios del contexto. Desde este punto de vista, la central receptora abandonaría su rol tradicional de mero canalizador de avisos para intentar erigirse en un instrumento fundamental para la protección del valor organizacional del cliente.

¿De qué manera debería ejecutarse teóricamente el proceso de evaluación del riesgo (identificación, análisis y valoración) en el contexto de una emergencia?

La norma ISO 31000 articula un proceso secuencial e iterativo que resultaría de vital importancia diseccionar para comprender el alcance que persigue el manifiesto. El primer paso teórico sería el establecimiento del alcance, contexto y criterios, seguido de la evaluación del riesgo, la cual se subdividiría en tres fases ineludibles: identificación, análisis y valoración.

En la **fase de identificación**, el propósito radicaría en encontrar y describir las fuentes de riesgo, asumiendo que los activos protegidos estarían expuestos a amenazas que, aprovechando vulnerabilidades, tendrían el potencial de generar un incidente.

Posteriormente, la **fase de análisis** del riesgo exigiría comprender la naturaleza del mismo, implicando una consideración de la probabilidad de los eventos y la magnitud de sus potenciales consecuencias.

Finalmente, la **fase de valoración del riesgo** requeriría comparar los resultados del análisis con los criterios previamente establecidos para determinar qué nivel de tratamiento se requeriría. Es precisamente en la fase de «tratamiento del riesgo» donde la conexión a una central receptora de alarmas se justificaría, según la guía, como una salvaguarda.

El tratamiento buscaría modificar el riesgo, actuando tanto sobre la probabilidad como sobre las consecuencias. En el análisis hipotético de una emergencia, el manifiesto ilustra que la gestión remota intentaría alterar positivamente los modelos temporales del siniestro, con la premisa de que el tiempo total de respuesta debería ser inferior al tiempo necesario para que un incendio generase condiciones críticas inasumibles. Por lo tanto, el marco de la norma ISO transformaría teóricamente la monitorización en una ciencia mensurable de la mitigación.

¿Por qué la mitigación de riesgos de alto impacto exigiría, según el documento, la transición hacia una infraestructura de Categoría I?

La derivación lógica de aplicar exhaustivamente el proceso de evaluación de riesgos llevaría a la premisa de que no todas las infraestructuras tolerarían el mismo grado de latencia o indisponibilidad.

Aquí es donde el manifiesto introduce su proposición operativa de mayor calado: la hipótesis de que **los incidentes producidos en espacios de pública concurrencia, así como aquellos eventos tipificados con un nivel de riesgo medio o alto, deberían ser gestionados de manera exclusiva desde centrales operativas de Categoría I, conforme a los parámetros de la norma UNE-EN 50518:2020**.

Esta exigencia se fundamentaría en una necesidad de resiliencia estructural. Operar bajo la Categoría I implicaría someter la infraestructura a estrictas garantías de blindaje frente a ataques físicos, protección de las comunicaciones, ubicación segura para el procesamiento de datos y un sistema de generadores de reserva que pudiesen soportar crisis energéticas prolongadas de forma autónoma.

El postulado argumentaría que, ante una contingencia crítica en una infraestructura estratégica, el centro táctico encargado de gestionar la coordinación no debería presentar fisuras, requiriendo en teoría el máximo grado de continuidad de servicio.

¿Cuál sería el rol estrictamente proporcional de las directivas europeas de ciberseguridad (NIS2 y CER) en esta ecuación operativa?

El manifiesto introduce en su perímetro de análisis el contexto regulatorio paneuropeo, referenciando la **Directiva sobre la Resiliencia de las Entidades Críticas (CER) y la Directiva relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad (NIS2)**.

Resultaría imprescindible delimitar analíticamente la importancia de estos textos en el ecosistema específico de las alarmas de incendio. Estas normativas podrían concebirse como un telón de fondo legal que **obligaría a las corporaciones a proteger sus infraestructuras lógicas frente a amenazas híbridas y ataques informáticos** que pudieran comprometer la disponibilidad de la red.

Un sistema de detección de incendios conectado a una central receptora de alarmas en remoto constituiría un activo de red susceptible de sufrir ataques de denegación de servicio. Sin embargo, la preeminencia operativa continuaría centrándose en el plano físico: las directivas europeas instarían a la central receptora a blindar sus propios sistemas informáticos y canales de telemetría para intentar asegurar que el dato fluyera de manera ininterrumpida, pero no alterarían el análisis táctico fundamental del operador frente a un conato de incendio real.

La ciberseguridad actuaría como el escudo lógico que protegería el canal de información, pero la mitigación del riesgo térmico se seguiría rigiendo metodológicamente por la dinámica de fluidos y los protocolos de evacuación derivados del análisis ISO 31000.

¿De qué manera la Inteligencia Artificial optimizaría la capacidad analítica sin comprometer, en teoría, la supervisión humana?

La anticipación a los desafíos tecnológicos del horizonte 2030 exigiría escudriñar el **papel que estaría llamada a jugar la Inteligencia Artificial (IA) en las centrales receptoras de alarmas**. El manifiesto proyecta una transformación gradual desde el modelo reactivo tradicional hacia una gestión que podría llegar a ser predictiva.

El valor teórico de esta tecnología se materializaría en su capacidad para procesar patrones históricos y ejecutar analíticas de vídeo avanzadas, lo que podría dotar al sistema de la aptitud para discriminar anomalías legítimas y descartar falsas alarmas originadas por factores ambientales, descongestionando así las colas de eventos.

No obstante, el manifiesto parece establecer **un principio inquebrantable: el paradigma de la «automatización supervisada»**. Aunque los modelos algorítmicos pudieran asumir la generación de flujos de trabajo iniciales o la activación preliminar de protocolos, el documento sugiere que la responsabilidad sobre la verificación última de la emergencia y el escalado hacia las fuerzas públicas debería recaer inalterablemente en el criterio final del personal humano habilitado.

A modo de síntesis, el **Manifiesto 2030 no se limitaría a proponer una mera actualización técnica**, sino que configuraría un ambicioso paraguas conceptual que invitaría a toda la industria a interiorizar una verdadera cultura de la seguridad integral. Al proponer la adopción de una metodología de evaluación del impacto, inspirada en la norma ISO 31000, el sector intentaría posicionarse para ofrecer una respuesta verdaderamente proporcional a la amenaza real.

El documento concluiría delineando varios ejes de acción innegociables para alcanzar esta excelencia operativa. Entre ellos, el texto destacaría la exigencia de una profesionalización y formación continua de los operadores, técnicos e ingenieros, así como una adaptación constante al dinámico marco legislativo europeo.

Adicionalmente, el manifiesto introduciría una reflexión sobre el valor social de las centrales receptoras de alarmas: al filtrar, verificar y gestionar profesionalmente un elevado volumen de incidencias, la CRA contribuiría de manera indirecta a optimizar los recursos públicos de emergencia.

Bajo esta hipótesis, **una gestión privada eficiente reduciría la carga operativa del Estado, permitiendo a los servicios de extinción y cuerpos de seguridad mejorar sus tiempos de respuesta ante emergencias reales sin necesidad de incrementar el gasto público**.

Finalmente, el texto reafirmaría que esta amalgama de seguridad física, ciberseguridad e inteligencia artificial requeriría, como condición indispensable para la gestión integral de señales, operar bajo el máximo estándar de resiliencia, es decir, la categoría I de la norma UNE-EN 50518.

Si el análisis previo de la guía de Tecnifuego nos proporcionó la certidumbre técnica de la ingeniería, este manifiesto nos aportaría ahora la visión panorámica y estratégica del riesgo. El engranaje final para cerrar este círculo virtuoso demandaría, sin embargo, un consenso ineludible con la Administración Pública.

Ese indispensable modelo de gobernanza territorial, centrado en la depuración del ruido, la calidad del dato y la colaboración sinérgica con los bomberos será el objeto de estudio de la cuarta y última entrega de esta serie, dedicada a desgranar el borrador estratégico del Clúster de Seguretat de Cataluña.

Referencias

AES Fundación. (2026). Manifiesto 2030: Gestión integral de las señales de alarma. Asociación Española de Empresas de Seguridad.

Asociación Española de Normalización. (2018). Gestión del riesgo. Principios y directrices (Norma UNE-ISO 31000:2018).

Unión Europea. (2022). Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión (Directiva NIS2). Diario Oficial de la Unión Europea, L 333, 80-152.

Unión Europea. (2022). Directiva (UE) 2022/2557 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a la resiliencia de las entidades críticas (Directiva CER). Diario Oficial de la Unión Europea, L 333, 164-198.

Por **Alberto José Galdón Carreño** es Graduado en Ciencias de la Seguridad (Universidad Isabel I) Máster en Protección Civil y Gestión de Emergencias (Universitat de Valencia). Diploma de Especialización. Universitaria en Dirección de Seguridad Integral. (Universitat de VIC). Diploma de Especialista Profesional. Universitario Servicios de Prevención, Extinción de Incendios y Salvamento. (Universitat de Valencia). Diploma de Especialista Profesional Universitario en Gestión e Implantación de Planes de Autoprotección. (Universitat de Valencia). Experto Universitario en Investigación de Incendios (UNED). Director de Seguridad Corporativa en Rotonda Grupo Empresarial (desde 2016 y en la actualidad). Vocal en la Junta Directiva de la Asociación Española de Centrales de Alarmas. Bombero del Consorcio de Emergencias de Ciudad Real (2011-2016).