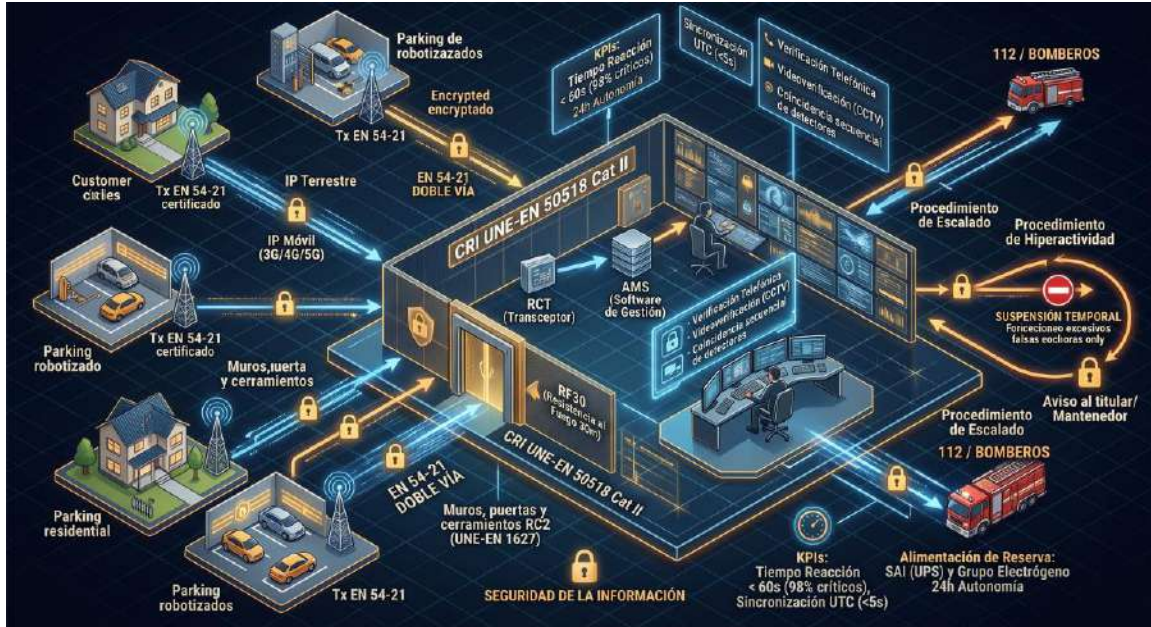


La ingeniería del servicio operativo: análisis pormenorizado del estándar técnico de Tecnifuego (Parte II de IV)



¿Cómo podemos construir un modelo unificado y realmente fiable para la gestión remota de alarmas de incendio?

Para lograrlo, necesitamos una base tecnológica y de procedimientos que asegure la trazabilidad y la resistencia de las comunicaciones operativas. En esta segunda entrega sobre la transición normativa de nuestro sector, analizamos a fondo el documento técnico de la Asociación Española de Sociedades de Protección Contra Incendios. Este texto propone un marco muy completo que define la ingeniería, la arquitectura y el funcionamiento que debe tener una central receptora de alarmas de incendio, a la que llamaremos CRI. Su objetivo es solucionar el actual vacío legal marcando reglas estrictas para el hardware, el software y los procesos frente a eventos críticos.

¿Por qué no sirve cualquier panel de seguridad para gestionar un incendio?

El documento parte de una idea fundamental: vigilar la seguridad física contra robos no es lo mismo que proteger contra incendios. El fuego avanza a una velocidad exponencial y genera subproductos tóxicos rápidamente, lo que exige un modelo de atención ininterrumpida y de altísima especialización.

Por ello, la guía aplica exclusivamente a los sistemas regulados por el Reglamento de Instalaciones de Protección contra Incendios (RIPCI), dejando fuera las señales de intrusión, los controles de accesos o los sistemas de circuito cerrado de televisión propios de la seguridad privada.

La guía deja claro que es técnicamente incompatible canalizar señales de incendio a través de paneles de intrusión, imposibilitando que ambas señales usen el mismo transmisor, ya que un panel de robo no ofrece la identificación exacta e imprescindible que requiere una emergencia de esta naturaleza.

¿Qué tecnología necesitamos realmente para que la comunicación sea infalible?

Para garantizar esta especialización, la normalización técnica se plantea como un requisito obligatorio. La arquitectura de captación de datos debe basarse, sin excepciones, en sistemas de alarma que cumplan la norma UNE 23007-2, conectados a equipos de transmisión certificados bajo la norma UNE-EN 54-21. El viaje de los datos hacia la CRI funciona como una cadena de validaciones lógicas ininterrumpida. La señalización, preferiblemente encriptada, es procesada por un módulo transductor de señales (RCT) que decodifica la trama y la envía al *software* de gestión de alarmas de la CRI, conocido como AMS.

Gracias a esta topología, la pantalla del operador muestra variables perfectamente estructuradas, dándole la capacidad de distinguir con precisión milimétrica si se trata de un detector automático, un pulsador manual, una evacuación en curso o el disparo de un sistema de extinción.

¿Qué nivel de blindaje y resistencia debe tener la propia central receptora?

Analizando los riesgos de la propia instalación, se establece que los edificios destinados a operar como una CRI deben cumplir, como mínimo, con el diseño de la Categoría II de la norma UNE-EN 50518 sobre centros de supervisión y recepción de alarmas. Esto exige que el recinto acredite una resistencia certificada frente a ataques físicos, lo que se traduce en utilizar cerramientos y puertas homologadas con un nivel de resistencia RC2, según la norma UNE-EN 1627.

Además, se exige una resistencia pasiva al humo y al fuego de al menos treinta minutos, junto con análisis de riesgos frente naturales, antrópicos y un control de accesos auditable, medidas pensadas para proteger el núcleo de procesamiento frente a problemas climáticos o sabotajes.

¿Y si hay un corte de luz o fallan las comunicaciones?

El colapso del suministro eléctrico representa una vulnerabilidad inaceptable para el servicio. Por ello, la instalación debe contar con sistemas de alimentación ininterrumpida capaces de asumir la carga al instante y sin provocar alteraciones en los equipos. Esta energía actúa como un puente temporal hasta que arrancan automáticamente los generadores de reserva. Estos equipos deben garantizar veinticuatro horas de autonomía continua, soportando un consumo equivalente a 1,2 veces la demanda máxima prevista de la instalación. Además, los generadores necesitan su propio espacio aislado y reservas de combustible in situ, creando una auténtica isla de resiliencia energética.

En cuanto a las telecomunicaciones, depender de una sola vía es demasiado inestable para proteger instalaciones sin vigilancia. Resulta imperativo usar comunicaciones redundantes, combinando infraestructuras terrestres e inalámbricas para mitigar la probabilidad de un fallo general.

La vigilancia de la red es rigurosa: si se pierde la comunicación total en vías dedicadas, el sistema debe avisar en un máximo de noventa segundos, recomendando configurar ciclos interrogativos o «polling» cada diez minutos. Si se detecta una caída del sistema de protección contra incendios, la CRI espera una ventana de quince minutos; si la conexión no se recupera, el sistema avisa automáticamente al titular o al mantenedor, ajustando la urgencia del aviso en función de si sobreviven las vías alternativas.

¿Cómo evita la central saturarse de avisos y distinguir lo urgente de lo que no lo es?

El software de la CRI utiliza un algoritmo lógico para ordenar las señales según su urgencia real de forma autónoma. De este modo, el sistema da prioridad absoluta a las alertas de evacuación, disparos de extinción o prealarmas, dejando en un segundo plano los fallos de periféricos, las rutinas de prueba o los avisos de mantenimiento.

Para medir la eficacia de este trabajo, el modelo marca indicadores clave de rendimiento (KPIs), exigiendo que el tiempo de reacción del operador, desde que salta la alerta en el software hasta su primera intervención, sea inferior a 60 segundos en el 98% de los eventos críticos evaluados a lo largo de un año.

Discriminar las falsas alarmas es fundamental para no amenazar directamente la operatividad de los equipos de emergencia y protección civil. El primer paso para verificar una alerta, y el más habitual, es llamar por teléfono a los responsables del plan de autoprotección del edificio. No obstante, la norma admite otros métodos técnicos, como confirmar si han saltado zonas independientes de forma secuencial, cruzar tecnologías de detección diferentes o usar cámaras para la videoverificación.

Sobre este último punto, la guía hace una advertencia importante: que no veamos humo o llamas en el vídeo no es motivo suficiente para descartar una alerta generada por un equipo homologado, a menos que confirmemos positivamente la existencia de una causa falsa.

¿Cuándo se debe llamar a los bomberos y qué ocurre si un sistema no para de fallar?

Los procedimientos para avisar a las autoridades se formulan de forma muy categórica. Cualquier fuego detectado por un sistema certificado, que no haya podido confirmarse como falso tras intentar verificarlo por todos los medios, debe comunicarse sin dilación al 112 o a los bomberos correspondientes. Pero la red pública de emergencias también necesita salvaguardas frente a equipos informáticos perturbados o mal calibrados. Para ello, el documento introduce el concepto de «hiperactividad».

Si un edificio envía de forma masiva señales falsas, la CRI tiene la potestad de suspender temporalmente y de forma documentada los avisos a los recursos públicos, contactando exclusivamente con los titulares y mantenedores. Esta es una medida coercitiva que busca forzar la reparación técnica del problema antes de permitir que la instalación vuelva a conectar sus avisos con el 112.

¿Cómo garantizamos que todos estos procesos se cumplan a la perfección?

La solidez de toda esta arquitectura se basa en la obligación de implantar y someter a auditoría externa una serie de procedimientos operativos estandarizados (SOP). Estas reglas internas cubren desde cómo dar de alta a un cliente hasta los protocolos de contingencia aplicables si el software falla o si hay que evacuar la propia CRI.

Para proteger los datos, que son un activo crítico, se exige realizar copias de seguridad sincronizadas bajo el estándar UTC, con un margen de error máximo de cinco segundos respecto

al reloj maestro, lo que garantiza la precisión forense al reconstruir un siniestro. Sumado a esto, los sistemas de almacenamiento deben estar bien dimensionados y emitir alertas preventivas cuando lleguen al noventa por ciento de su capacidad.

En definitiva, la conclusión que extraemos de este estándar de Tecnofuego es que basar la telemetría de las alarmas en procedimientos de ingeniería estrictos y auditables es totalmente viable. Aplicar las normas EN 54 para la captación y las exigencias de la EN 50518 resuelve la precariedad y variabilidad tecnológica histórica del sector.

Homogeneizar estos parámetros mejora cualitativamente la fiabilidad de las alertas, creando un filtro capaz de distinguir una verdadera emergencia de un simple ruido electrónico. Sin embargo, la complejidad de las amenazas actuales nos demuestra que tener una buena infraestructura y algoritmos no es suficiente por sí solo. El ecosistema de protección corporativa nos pide combinar esta ingeniería pura con una evaluación integral del contexto y de la naturaleza de los activos protegidos. Esta visión más estratégica, orientada a la gobernanza y al riesgo, será el tema principal de nuestro tercer artículo, donde analizaremos el modelo de segmentación de amenazas del Manifiesto 2030 de AES Fundación.

Referencias

Tecnifuego. (2025, 26 de noviembre). *Documento técnico gestión remota de alarmas de incendios: Servicios asociados a Central Receptora de Alarmas de Incendio (CRI)*. Asociación Española de Sociedades de Protección Contra Incendios.

Legislación

Real Decreto 513/2017, de 22 de mayo, por el que se aprueba el Reglamento de instalaciones de protección contra incendios. *Boletín Oficial del Estado*, 139, de 12 de junio de 2017, pp. 48325-48386.

Normas Técnicas (AENOR)

Asociación Española de Normalización. (1998). *Sistemas de detección y de alarma de incendios. Parte 2: Equipos de control e indicación* (Norma UNE 23007-2:1998).

Asociación Española de Normalización. (2007). *Sistemas de detección y alarma de incendios. Parte 21: Equipos de transmisión de alarmas y avisos de fallo* (Norma UNE-EN 54-21:2007).

Asociación Española de Normalización. (2020). *Centros de supervisión y recepción de alarmas* (Norma UNE-EN 50518:2020).

Asociación Española de Normalización. (2021). *Puertas peatonales, ventanas, fachadas ligeras, rejas y persianas. Resistencia a la efracción. Requisitos y clasificación* (Norma UNE-EN 1627:2021).

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).