Norma Española

UNE-EN 50518

Centro de supervisión y recepción de alarmas

Esta norma ha sido elaborada por el comité técnico CTN 108 *Seguridad física y electrónica. Sistemas de protección y alarma*, cuya secretaría desempeña AES.

Asociación Española
de Normalización
Génova, 6 - 28004 Madrid
915 294 900
info@une.org
www.une.org

UNE-EN 50518

Centro de supervisión y recepción de alarmas

Monitoring and Alarm Receiving Centre.

Centre de contrôle et de réception d'alarme.

Esta norma es la versión oficial, en español, de la Norma Europea EN 50518:2019.

Esta norma anulará y sustituirá a las Normas UNE-EN 50518-1:2014, UNE-EN 50518-2:2014 y UNE-EN 50518-3:2013 antes de 2022-02-07.

Las observaciones a este documento han de dirigirse a:

Asociación Española de Normalización
Génova, 6
28004 MADRID-España
Tel.: 915 294 900
info@une.org
www.une.org

NORMA EUROPEA
EUROPEAN STANDARD
NORME EUROPÉENNE
EUROPÄISCHE NORM

EN 50518

Agosto 2019

ICS 13.320

Sustituye a EN 50518-1:2013, EN 50518-2:2013, EN 50518-3:2013 y a todas sus modificaciones y corrigendum (si los hay)

Versión en español

Centro de supervisión y recepción de alarmas

Monitoring and Alarm Receiving Centre. **Centre de contrôle et de réception d'alarme.** **Alarmempfangsstelle.**

Esta norma europea ha sido aprobada por CENELEC el 2019-02-06. Los miembros de CENELEC están sometidos al Reglamento Interior de CEN/CENELEC que define las condiciones dentro de las cuales debe adoptarse, sin modificación, la norma europea como norma nacional.

Las correspondientes listas actualizadas y las referencias bibliográficas relativas a estas normas nacionales, pueden obtenerse en el Centro de Gestión de CEN/CENELEC, o a través de sus miembros.

Esta norma europea existe en tres versiones oficiales (alemán, francés e inglés). Una versión en otra lengua realizada bajo la responsabilidad de un miembro de CENELEC en su idioma nacional, y notificada al Centro de Gestión de CEN/CENELEC, tiene el mismo rango que aquéllas.

Los miembros de CENELEC son los comités electrotécnicos nacionales de normalización de los países siguientes: Alemania, Austria, Bélgica, Bulgaria, Chipre, Croacia, Dinamarca, Eslovaquia, Eslovenia, España, Estonia, Finlandia, Francia, Grecia, Hungría, Irlanda, Islandia, Italia, Letonia, Lituania, Luxemburgo, Malta, Noruega, Países Bajos, Polonia, Portugal, Reino Unido, República Checa, República de Macedonia del Norte, Rumanía, Serbia, Suecia, Suiza y Turquía.

CENELEC

COMITÉ EUROPEO DE NORMALIZACIÓN ELECTROTÉCNICA
European Committee for Electrotechnical Standardization
Comité Européen de Normalisation Electrotechnique
Europäisches Komitee für Elektrotechnische Normung
CENTRO DE GESTIÓN: Rue de la Science, 23, B-1040 Brussels, Belgium

Índice

Prólogo europeo

Esta Norma EN 50518:2019 fue preparada por el Comité Técnico TC 79, *Sistemas de alarma*, de CENELEC.

Se fijaron las siguientes fechas:

– Fecha límite en la que la norma debe adoptarse a nivel nacional por publicación de una norma nacional idéntica o por ratificación	(dop)	2020-02-06
– Fecha límite en la que deben retirarse las normas nacionales divergentes con esta norma	(dow)	2022-02-06

Esta norma sustituye a las Normas EN 50518-1:2013, EN 50518-2:2013 y EN 50518-3:2013.

La Norma EN 50518:2017 incluye los siguientes cambios técnicos significativos con respecto a las Normas EN 50518-1:2013, EN 50518-2:2013 y EN 50518-3:2013:

– las normas de las referencias se han actualizado a las últimas versiones;

– se han actualizado las definiciones;

– se ha ampliado el campo de aplicación para incluir alarmas de detección de incendios, de control de accesos, circuitos cerrados de televisión (CCTV), alarmas sociales y otras alarmas;

– se describen dos categorías de centro de recepción de alarmas (ARC), la categoría I y la categoría II. Los centros de recepción de alarmas (ARC) de categoría I se deben diseñar, construir y manejar siguiendo un nivel de construcción, seguridad e integridad más alto que para un centro de recepción de alarmas de categoría II;

– se ha añadido un capítulo que describe las herramientas de gestión con las que debe contar el centro de recepción de alarmas (ARC);

– se ha añadido un anexo informativo en el que se describen las repercusiones técnicas y de seguridad del acceso remoto a los datos del centro de recepción de alarmas (ARC);

– se ha añadido un anexo informativo en el que se describen los requisitos para un sistema de gestión de alarmas.

El objetivo de esta revisión es actualizar los procedimientos para reflejar los avances técnicos actuales, teniendo en cuenta los cambios en las normas básicas y la experiencia adquirida en el uso de la norma.

0 Introducción

Esta norma europea se aplica a todos los centros de supervisión y recepción de alarmas (MARC, por sus siglas en inglés) que supervisan, reciben y/o procesan mensajes (de alarma) que requieren una respuesta de emergencia.

La abreviatura MARC describe todo el campo de aplicación funcional de un centro de supervisión y recepción de alarmas. Sin embargo, en todas las normas existentes de la serie de Normas EN 50131 elaboradas por el Comité Técnico CLC/TC 79, "Sistemas de Alarma", se utiliza la abreviatura ARC. Con el fin de evitar confusiones y lograr coherencia en la terminología, se utilizará la abreviatura ARC a lo largo de esta norma, siempre que MARC sea equivalente a ARC.

La función de recibir, procesar e iniciar acciones de respuesta mediante intervención (humana o no humana) no se limita únicamente a los mensajes generados por los sistemas de alarma de intrusión y atraco (I&HAS). La serie completa de normas elaboradas por el Comité Técnico CLC/TC 79, "Sistemas de alarma", comprende los sistemas de vigilancia por vídeo (Norma EN 62676), los sistemas de alarma social (Norma EN 50134), los sistemas de control de acceso (Norma EN 60839-11) y los sistemas de audio y vídeo de puertas de entrada. Todos los sistemas mencionados pueden enviar información, incluyendo alarmas, a uno o más centros de recepción de alarmas (ARC) para su posterior procesamiento, evaluación e intervención.

La información de alarma generada por otros sistemas, como por ejemplo sistemas de detección y alarma de incendios, sistemas de seguimiento y localización (de vehículos), vigilancia de personas o supervisión de redes de telecomunicación, se transmite regularmente a uno o más centros de recepción de alarmas (ARC) para su posterior procesamiento, evaluación e intervención.

En todas las circunstancias anteriores, las acciones criminales y/o las situaciones de emergencia pueden poner en peligro la seguridad de las personas y/o de las propiedades. Las ubicaciones de los centros en los que tiene lugar la recepción, procesamiento e inicio de las intervenciones deberían cumplir con los requisitos de esta norma.

La figura 1 muestra la cadena de eventos del conjunto del proceso de alarma.

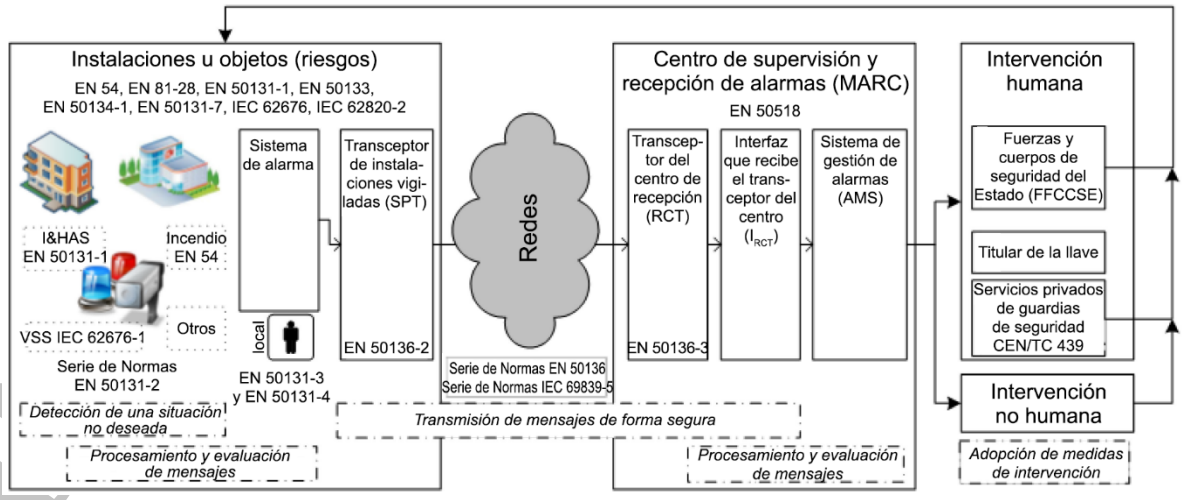


Figura 1 – Diagrama de cadena del proceso total de alarma

Se advierte que esta norma europea no puede sustituir a ningún requisito legislativo que un gobierno nacional haya juzgado necesario para controlar el sector de la seguridad a nivel nacional. Esta norma no puede interferir con los aspectos regulados mediante reglamentos (inter)nacionales relativos a servicios externos (por ejemplo, agua, aguas residuales, suministro de combustible para gas y/o petróleo y fuentes de alimentación de la red eléctrica).

1 Objeto y campo de aplicación

En este documento se especifican los requisitos mínimos para la supervisión, recepción y procesamiento de los mensajes de alarma generados por los sistemas de alarma que tienen lugar como parte del proceso total de protección contra incendios y seguridad.

A los efectos de este documento, el término "alarma" se utiliza en sentido amplio para incluir los mensajes de avería, estado y otros mensajes recibidos por parte de uno o varios sistemas de alarma de seguridad, que pueden incluir, entre otros, sistemas de detección y alarma de incendios, sistemas fijos de lucha contra incendios, sistemas de alarma de intrusión y atraco, sistemas de control de acceso, sistemas de videovigilancia, sistemas de alarma social y combinaciones de dichos sistemas.

En este documento se establecen requisitos para dos categorías de centros de recepción de alarmas (ARC), la categoría I y la categoría II. Los centros de recepción de alarmas (ARC) de categoría I se deben diseñar, construir y manejar siguiendo un nivel de construcción, seguridad e integridad más alto que para un centro de recepción de alarmas de categoría II.

La elección de la categoría se basa en el tipo o tipos de mensajes de alarma que se manejen.

Categoría I: Centros de recepción de alarmas (ARC) que gestionen mensajes de las aplicaciones de seguridad:

- sistemas de alarma de intrusión y atraco (I&HAS);
- sistemas de control de acceso;
- sistemas de videovigilancia en aplicaciones de seguridad que requieren una respuesta de emergencia (por ejemplo, prevención de pérdidas);
- seguimiento de personas, trabajadores en solitario y sistemas de rastreo de objetos para aplicaciones de seguridad;
- mensajes de alarma gestionados por centros de recepción de alarmas (ARC) de categoría II;
- combinaciones de los sistemas anteriores.

Categoría II: Centros de recepción de alarmas (ARC) que gestionen mensajes de aplicaciones que no estén relacionadas con la seguridad:

- sistemas de alarma de incendios;
- sistemas fijos de lucha contra incendios;
- sistemas de alarma social;

- sistemas de audio/vídeo de puertas de entrada;
- sistemas de videovigilancia en aplicaciones no relacionadas con la seguridad (por ejemplo, circulación del tráfico);
- seguimiento de personas, trabajadores en solitario y sistemas de rastreo de objetos para aplicaciones no relacionadas con la seguridad;
- sistemas de emergencia de ascensores;
- combinaciones de los sistemas anteriores.

Los requisitos se aplican a las alarmas de supervisión y procesamiento de los centros de recepción de alarmas (ARC, ya estén ubicados en uno o varios lugares) generadas por sistemas instalados en otras ubicaciones y a las alarmas de supervisión de los centros de recepción de alarmas (ARC) emitidas por los sistemas que se encuentran en sus propias instalaciones.

Este documento incluye los requisitos funcionales y específicos que se necesitan para facilitar los servicios de un centro de recepción de alarmas (ARC). El documento NO se aplica a:

- sistemas de alarma utilizados con fines no civiles;
- sistemas de alarma para aplicaciones médicas o de salud.

2 Normas para consulta

En el texto se hace referencia a los siguientes documentos de manera que parte o la totalidad de su contenido constituyen requisitos de este documento. Para las referencias con fecha, solo se aplica la edición citada. Para las referencias sin fecha se aplica la última edición (incluida cualquier modificación de esta).

EN 54 (series), *Sistemas de detección y alarma de incendios.*

EN 179, *Herrajes para la edificación. Dispositivos de emergencia accionados por una manilla o un pulsador para recorridos de evacuación. Requisitos y métodos de ensayo.*

EN 356, *Vidrio de construcción. Vidrio de seguridad. Ensayo y clasificación de la resistencia al ataque manual.*

EN 1063, *Vidrio de construcción. Vidrio de seguridad. Ensayo y clasificación de la resistencia al ataque por balas.*

EN 1125, *Herrajes para la edificación. Dispositivos antipánico para salidas de emergencia accionadas por una barra horizontal. Requisitos y métodos de ensayo.*

EN 1522, *Ventanas, puertas, persianas y celosías. Resistencia a la bala. Requisitos y clasificación.*

EN 1627, *Puertas peatonales, ventanas, fachadas ligeras, rejas y persianas. Resistencia a la efracción. Requisitos y clasificación.*

EN 13501-2, *Clasificación en función del comportamiento frente al fuego de los productos de construcción y elementos para la edificación. Parte 2: Clasificación a partir de datos obtenidos de los ensayos de resistencia al fuego excluidas las instalaciones de ventilación.*

EN 13637, *Herrajes para la edificación. Sistemas de salida controlados eléctricamente para su uso en recorridos de evacuación. Requisitos y métodos de ensayo.*

EN 14846, *Herrajes para edificación. Cerraduras y pestillos. Cerraduras y cerraderos electromecánicos. Requisitos y métodos de ensayo.*

EN 15713, *Destrucción segura del material confidencial. Código de buenas prácticas.*

EN 50131-1, *Sistemas de alarma. Sistemas de alarma contra intrusión y atraco. Parte 1: Requisitos del sistema.*

EN 50134-7, *Sistemas de alarma. Sistemas de alarma social. Parte 7: Guía de aplicación.*

EN 50136-1, *Sistemas de alarma. Sistemas y equipos de transmisión de alarmas. Parte 1: Requisitos generales para los sistemas de transmisión de alarmas.*

EN 50136-3, *Sistemas de alarma. Sistemas y equipos de transmisión de alarmas. Parte 3: Requisitos para los transceptores del centro de recepción (RCT).*

EN 50272-2, *Requisitos de seguridad para las baterías e instalaciones de baterías. Parte 2: Baterías estacionarias.*

EN 50600 (series), *Tecnología de la información. Infraestructuras e instalaciones de centros de datos.*

EN 62040-1, *Sistemas de alimentación ininterrumpida (SAI) Parte 1: Requisitos generales y de seguridad para los SAI (IEC 62040-1).*

EN 62305-2, *Protección contra el rayo. Parte 2: Evaluación del riesgo.*

EN 62676-4, *Sistemas de videovigilancia para utilización en aplicaciones de seguridad. Parte 4: Directrices de aplicación.*

3 Términos, definiciones y abreviaturas

3.1 Términos y definiciones

Para los fines de este documento, se aplican los términos y definiciones siguientes.

ISO e IEC mantienen bases de datos terminológicas para su utilización en normalización en las siguientes direcciones:

- Electropedia de IEC: disponible en http://www.electropedia.org/
- Plataforma de búsqueda en línea de ISO: disponible en http://www.iso.org/obp

3.1.1 empresa de sistemas de alarma:
Organización que suministra servicios para sistemas de alarmas (AS).

[FUENTE: EN 50131-1:2006, 3.1.7, modificado]

3.1.2 condición de alarma:
Condición de un sistema de alarmas (AS), o parte del mismo, que resulta de la respuesta del sistema a la presencia de un peligro.

[FUENTE: EN 50131-1:2006, 3.1.8, modificado]

3.1.3 retraso en la gestión de la alarma:
Procedimiento por el cual las condiciones de alarma señaladas se retrasan intencionadamente en el centro de recepción de alarmas (ARC) y se revisa su estado con el fin de evitar llamadas innecesarias al servicio de respuesta pertinente mediante la cancelación de determinadas condiciones de alarma, siempre que el usuario autorice dicha cancelación en las instalaciones vigiladas.

3.1.4 sistema de gestión de alarmas; AMS:
Sistema que almacena, organiza, controla, gestiona y permite la recuperación de los datos de los clientes y que está conectado a un equipo receptor de alarmas para la notificación automática de mensajes para cada sistema de alarma.

3.1.5 centro de recepción de alarmas; ARC:
Centro gestionado de manera permanente por personas a las que se envía toda la información relativa al estado de uno o más sistemas de alarmas (AS).

[FUENTE: EN 50136-1:2012, 4.1.2]

3.1.6 operador del centro de recepción de alarmas; operador del ARC:
Persona responsable del tratamiento de los mensajes presentados al sistema de gestión de alarmas (AMS).

[FUENTE: CLC/TS 50136-4:2004, 3.3, modificado]

3.1.7 estructura del centro de recepción de alarmas; estructura del ARC:
Todos los elementos estructurales del perímetro del centro de recepción de alarmas (ARC) (muros, vestíbulo de entrada, ventanas, zonas acristaladas, suelos, techos, puertas de entrada y salida, puntos de entrada y salida de los conductos de ventilación, puntos de entrada y salida de otros cables y conductos de servicio, ventanilla de transferencia).

3.1.8 equipo de transmisión de alarmas; ATE:
Término colectivo que describe el transceptor de instalaciones vigiladas (SPT), el transceptor del centro de supervisión (MCT) y el transceptor del centro de recepción (RCT).

[FUENTE: EN 50136-1:2012, 4.1.4]

3.1.9 sistema de transmisión de alarmas; ATS:
Equipo de transmisión de alarmas (ATE) y redes utilizadas para transferir información relacionada con el estado de uno o más sistemas de alarma (AS) al sistema de gestión de alarmas (AMS) de uno más centros de recepción de alarmas (ARC).

NOTA 1 Un sistema de transmisión de alarmas (ATS) puede consistir en vías de transmisión de alarmas de diferentes clases, como por ejemplo para su uso en los llamados "sistemas de doble vía".

[FUENTE: EN 50136-1:2012, 4.1.8, modificado]

3.1.10 verificación de alarmas:
Proceso para proporcionar información adicional a la alarma notificada que aumenta la probabilidad de que se haya producido una auténtica alarma.

3.1.11 cliente:
Entidad individual o corporativa con la que el centro de recepción de alarmas (ARC) tiene un contrato para el suministro de servicios de supervisión de alarmas.

3.1.12 detector:
Dispositivo diseñado para generar un mensaje de alarma en respuesta a la detección de una condición anormal que indique la presencia de un peligro.

[FUENTE: CLC/TS 50131-7:2010, 3.1.12, modificado]

3.1.13 incidencia disruptiva:
Cualquier incidente natural o provocado por el hombre que pueda causar la interrupción de las actividades ordenadas del centro de recepción de alarmas (ARC) de acuerdo con los procedimientos habituales de funcionamiento y que requiera la ejecución de procedimientos especiales.

NOTA 1 Algunos ejemplos incluyen:

- fallo en el suministro de energía;
- fallo de los sistemas de comunicación entrantes;
- fallo de los sistemas de comunicación de salida;
- fallo de los sistemas informáticos, pérdida de datos;
- incendio;
- condiciones climatológicas extremas, como tormentas, inundaciones, tormenta eléctrica;
- desastres naturales, como terremotos o deslizamientos de tierra;
- daños causados por vehículos de tierra y aire;
- gases peligrosos y reducción de los niveles de oxígeno en el aire ambiente;
- intrusión en las instalaciones, ataque físico, incluyendo la coacción;
- intrusión en los sistemas informáticos y de comunicación, ataque virtual y ciberdelincuencia;
- sabotaje por parte de personas con autorización de acceso (empleados, socios comerciales).

3.1.14 vestíbulo de entrada:
Espacio entre el exterior y el centro de recepción de alarmas (ARC) que proporciona una entrada/salida controlada y segura al centro.

3.1.15 mensaje previsto:
Mensaje que tiene que llegar al centro de recepción de alarmas (ARC) de acuerdo con los horarios predeterminados (en particular, los mensajes de estado de los sistemas de alarma y los sistemas de comunicación).

3.1.16 comunicación externa:
Todas las comunicaciones entrantes y salientes con el centro de recepción de alarmas (ARC).

NOTA 1 La comunicación incluye toda la información pertinente para el funcionamiento del centro de recepción de alarmas (ARC), como número teléfono, correo electrónico, fax, información escrita, audio, todas las imágenes del sistema de videovigilancia y otros datos electrónicos, pero excluye los mensajes de alarma.

3.1.17 resistencia al fuego:
Capacidad de un elemento de la construcción, componente o estructura de un edificio para cumplir, durante un período de tiempo determinado, las condiciones requeridas de estabilidad, integridad al fuego y/o aislamiento térmico y/u otros servicios previstos en un ensayo normalizado de resistencia al fuego.

3.1.18 dispositivo contra atracos:
Dispositivo que, cuando se activa manualmente, hace que se genere un mensaje de alarma.

[FUENTE: EN 50131-1:2006, 3.1.29, modificado]

3.1.19 sistema de alarma contra intrusos:
Sistema de alarma (AS) para detectar e indicar la presencia, entrada o tentativa de entrada de un intruso en un local protegido.

[FUENTE: EN 50131-1:2006, 3.1.36]

3.1.20 instalador:
Entidad jurídica que instala sistemas.

NOTA 1 Puede formar parte de la entidad jurídica que presta servicios al centro de recepción de alarmas (ARC) o estar afiliada a la misma o puede ser una entidad jurídica independiente no relacionada.

3.1.21 indicador clave del rendimiento; KPI:
Estadísticas empresariales que miden el rendimiento de una organización.

NOTA 1 Los indicadores clave del rendimiento muestran los progresos (o la falta de ellos) en la consecución de los objetivos o planes estratégicos de la organización mediante la supervisión de las actividades que, si no se realizan adecuadamente, probablemente causen una degradación del rendimiento del centro de recepción de alarmas (ARC).

3.1.22 mensaje:
Conjunto de señales transportadas a través de interconexiones y que incluyen la identificación, los datos relativos a la función y diversos medios destinados a asegurar su propia integridad, inmunidad y correcta recepción.

[FUENTE: EN 50131-1:2006, 3.1.43]

3.1.23 alarma notificada:
Condición de alarma que se ha transmitido al centro de recepción de alarmas (ARC).

3.1.24 transceptor del centro de recepción; RCT:
Equipo situado en una ubicación segura que cuenta, como mínimo, con la capacidad de enviar y recibir mensajes de alarma a/desde el sistema de gestión de alarmas (AMS).

NOTA 1 El transceptor del centro de recepción (RCT) puede incluir funciones de gestión para los sistemas de transmisión de alarmas (ATS).

[FUENTE: EN 50136-1:2012/A1:2018, 4.1.28]

3.1.25 empleo relevante:
Empleo que implica o puede implicar la adquisición de o el acceso a información o equipamiento cuya utilización indebida pueda suponer un riesgo para la seguridad de la organización, de cualquier cliente de la organización o de un tercero.

[FUENTE: EN 15602:2008, 2.2.3]

3.1.26 respondedor:
Organización o persona que ejecuta acciones a petición de un centro de recepción de alarmas (ARC).

3.1.27 aplicación de seguridad:
Aplicación(es) diseñada(s) para detectar un peligro que pueda causar daño o perjuicio por acciones delictivas a personas, propiedades, objetos o bienes.

3.1.28 verificación de seguridad:
Procedimiento de comprobación del historial y antecedentes de los empleados y empleados potenciales.

[FUENTE: EN 15602:2008, 2.2.6]

3.1.29 verificación de antecedentes penales:
Comprobación por parte de la autoridad nacional de los registros judiciales y penales de los empleados y empleados potenciales.

[FUENTE: EN 15602:2008, 2.2.7]

3.1.30 fuente de alimentación de reserva:
Fuente de energía que es capaz de suministrar energía a un centro de recepción de alarmas (ARC) durante largos períodos de tiempo.

3.1.31 instalaciones vigiladas:
Parte de un edificio y/o área en la que un sistema de alarma puede detectar un peligro.

[FUENTE: EN 50131-1:2006, 3.1.66, modificado]

3.1.32 marca de tiempo:
Valor que asigna un tiempo único a un evento.

3.1.33 ventanilla de transferencia:
Dispositivo para pasar llaves, documentos u otros objetos.

3.1.34 sistema de alimentación ininterrumpida SAI:
Combinación de convertidores, interruptores y dispositivos de almacenamiento de energía (como baterías) que constituye un sistema de alimentación para mantener la continuidad de la potencia de carga en caso de fallo en la potencia de entrada.

NOTA 1 La continuidad de la potencia de carga se produce cuando la tensión y la frecuencia se encuentran dentro de las bandas asignadas de tolerancia de estado estacionario y transitorio y cuando la distorsión y las interrupciones se sitúan dentro de los límites especificados para la carga. Se puede producir un fallo en la potencia de entrada cuando la tensión y la frecuencia están fuera de las bandas asignadas de tolerancia de estado estacionario y transitorio o cuando la distorsión o las interrupciones no se sitúan dentro de los límites especificados para el sistema de alimentación ininterrumpida (SAI).

[FUENTE: EN 62040-1:2008, 3.1.1]

3.1.35 usuario:
Persona autorizada por el cliente para hacer uso de un sistema (de alarma).

[FUENTE: EN 50131-1:2006, 3.1.80, modificado]

3.2 Abreviaturas

Para los propósitos de este documento, se aplican las siguientes abreviaturas.

AMS	Sistema de gestión de alarmas (*Alarma management system*)
ARC	Centro de recepción de alarmas (*Alarm receiving centre*)
AS	Sistema de alarma (*Alarm s*ystem)
ATE	Equipo de transmisión de alarmas (*Alarm transmission equipment*)
ATP	Vía de transmisión de alarmas (*Alarm transmission path*)
ATS	Sistemas de transmisión de alarmas (*Alarm transmission system*)
I&HAS	Sistema de alarma de intrusión y atraco (*Intruder and hold-up alarm system*)
KPI	Indicador clave del rendimiento (*Key performance indicator*)
RCT	Transceptor del centro de recepción (*Receiving centre transceiver*)
SOP	Procedimiento habitual de funcionamiento (*Standard operating procedure*)
SPT	Transceptor de instalaciones vigiladas (*Supervised premises transceiver*)
SAI	Sistema de alimentación ininterrumpida
UTC	Tiempo universal coordinado (*Coordinated Universal Time*)
VSS	Sistema de videovigilancia (antes llamado CCTV) (*Video surveillance system*)

4 Planificación

4.1 Categorización

La planificación para la construcción de un centro de recepción de alarmas (ARC) debería basarse en la categorización prevista.

Los centros de recepción de alarmas (ARC) se categorizan según el tipo o tipos de mensajes de alarma que se gestionen y los consiguientes requisitos de integridad y seguridad relativos a la construcción, las comunicaciones, el funcionamiento y la información. Esta norma contiene recomendaciones para dos categorías de centros de recepción de alarmas (ARC), tal y como se describe en el campo de aplicación.

A menos que se indique lo contrario, los requisitos de esta norma se aplican tanto a los centros de recepción de alarmas (ARC) de categoría I como a los de categoría II.

4.2 Elección de la ubicación

Se debe completar una evaluación de riesgos documentada que incluya la ubicación del centro de recepción de alarmas (ARC).

El centro de recepción de alarmas (ARC) se debe ubicar en un lugar que tenga en cuenta los riesgos de incendio, explosión, inundación, vandalismo y exposición a los peligros de otros sitios. Si el centro de recepción de alarmas no ocupa todo el edificio en el que se encuentra, debe estar separado del resto del edificio mediante una barrera física que consista en muros, suelos, techos y aperturas imprescindibles.

5 Construcción – Estructura del centro de recepción de alarmas (ARC)

5.1 Generalidades

Todos los elementos descritos en el capítulo 5 se refieren a la estructura del centro de recepción de alarmas (ARC) (véase 3.1.7 y el anexo A).

5.2 Muros, suelo y techo – Resistencia frente a ataques físicos

5.2.1 Categoría I

La estructura del centro de recepción de alarmas (ARC) tiene como objetivo proporcionar la misma protección para todos los elementos estructurales del centro. Se deben respetar los requisitos que recoge la tabla 1 para poder proporcionar resistencia frente al ataque físico.

Tabla 1 – Resistencia mínima frente a ataques físicos para la estructura del centro de recepción de alarmas (ARC)

Elementos de construcción	Materiales	Espesor
Muros de la estructura del ARC y muros del vestíbulo de entrada (véase el anexo A)	Mampostería maciza	≥ 200 mm
	Hormigón	≥ 150 mm
	Hormigón armado	≥ 100 mm
	Acero macizo	≥ 8 mm
Muros internos	No hay requisitos	No hay requisitos
Suelos y techos	Hormigón	≥ 150 mm
	Hormigón armado	≥ 100 mm
	Acero macizo	≥ 8 mm [a]
Si el centro de recepción de alarmas (ARC) está situado en un piso a más de 4 m sobre el nivel del suelo o en cualquier plano adyacente, el espesor del muro puede reducirse en un 50%.		
a El espesor del acero puede reducirse en un 50% cuando no sea directamente accesible al público en general.		

Los elementos de construcción que figuran en la tabla 1 cubren los requisitos mínimos para ofrecer resistencia frente a ataques físicos. Si se aplican otros métodos o materiales de construcción, se debe garantizar la misma resistencia frente a ataques físicos y con balas que la que recoge la tabla 2.

5.2.2 Categoría II

La estructura del centro de recepción de alarmas (ARC) debe consistir en una barrera física capaz de impedir el acceso no autorizado, como la que proporcionan los muros, las puertas, el suelo y el techo.

5.3 Puertas perimetrales – Resistencia frente a ataques físicos y con balas

Al menos una de las puertas del vestíbulo de entrada, así como el resto de puertas perimetrales, debe ofrecer una resistencia frente a ataques físicos y con balas que cumpla con los requisitos previstos en la tabla 2.

Tabla 2 – Ataque físico y ataque con balas

	Ataque físico	**Ataque con balas**
Puertas de categoría I	Clase de resistencia 3 (RC3) de acuerdo con la Norma EN 1627	Clasificación FB3 de acuerdo con la Norma EN 1522
Puertas de categoría II	Clase de resistencia 2 (RC2) de acuerdo con la Norma EN 1627	No hay requisitos

5.4 Zonas acristaladas

5.4.1 Categoría I

Las ventanas de la estructura del centro de recepción de alarmas (ARC) se deben bloquear desde el interior en todo momento, excepto cuando se haya iniciado un procedimiento de salida de emergencia o con fines de mantenimiento. Asimismo, deben ofrecer resistencia frente a ataques físicos y con balas, tal y como se especifica en la tabla 3.

Tabla 3 – Ataque físico y con balas de categoría I

	Ataque físico	**Ataque con balas**
Ventanas	Clase de resistencia 3 (RC3) de acuerdo con la Norma EN 1627	Clasificación FB3 de acuerdo con la Norma EN 1522
Acristalamiento	Clasificación P5A de acuerdo con la Norma EN 356	Clasificación BR 3 – S de acuerdo con la Norma EN 1063

El interior del centro de recepción de alarmas (ARC) no debe ser visible desde el exterior de la estructura del centro.

Las ventanas y los cristales deben proporcionar resistencia a incendios y al humo de al menos 30 min.

5.4.2 Categoría II

No hay requisitos.

5.5 Resistencia frente a incendios y humo

La estructura del centro de recepción de alarmas (ARC), excluyendo las zonas acristaladas, debe ofrecer una resistencia al fuego que cumpla con lo establecido en la Norma EN 13501-2, pero nunca inferior a 30 min.

5.6 Protección contra el impacto de rayos

Se debe llevar a cabo un análisis de riesgos de conformidad con la Norma EN 62305-2 o con los reglamentos nacionales, así como adoptar las medidas adecuadas para proteger el centro de recepción de alarmas (ARC) contra el impacto de rayos.

5.7 Aperturas

5.7.1 Generalidades

Las únicas aperturas permitidas en la estructura de un centro de recepción de alarmas (ARC) deben ser:

- áreas acristaladas (véase 5.4);
- punto de acceso al centro de recepción de alarmas (ARC) (véase 5.7.2);
- salida de emergencia (véase 5.7.4);
- puntos de ventilación (véase 5.7.5);
- puntos de entrada y salida de servicios (véase 5.7.6);
- ventanilla de transferencia (véase 5.7.7).

5.7.2 Punto de acceso al centro de recepción de alarmas (ARC)

5.7.2.1 Categoría I – Vestíbulo de entrada

Se debe permitir el acceso al centro de recepción de alarmas (ARC) a través de dos puertas separadas por un vestíbulo de entrada cuya superficie no debe exceder los 6 m^2. Una de las puertas del vestíbulo de entrada debe ofrecer un nivel de resistencia al fuego que se ajuste a lo previsto en el apartado 5.5. La segunda puerta debe cumplir con los requisitos que recoge la tabla 2 para la categoría I.

Las puertas deben estar interbloqueadas para evitar que se abran al mismo tiempo en condiciones normales de entrada y salida. Se puede anular el dispositivo de bloqueo en casos excepcionales, como en una situación de emergencia, de forma que ambas puertas se puedan abrir a la vez. Ambas puertas se deben abrir hacia el exterior del centro de recepción de alarmas (ARC) (véase el anexo A) y deben disponer de dispositivos de autocierre y de bloqueo automáticos.

Ambas puertas deben estar protegidas por dispositivos electromecánicos de bloqueo/desbloqueo, según lo dispuesto en la Norma EN 14846 y con un código de clasificación mínimo de acuerdo con la tabla 4, que se puedan accionar solo desde el interior del centro de recepción de alarmas (ARC).

Tabla 4 – Código de clasificación del dispositivo electromecánico de bloqueo

Dígito	1	2	3	4	5	6	7	8	9
Norma EN 14846	3	S	2	D	0	L	6	1	3

Se debe disponer de un dispositivo mecánico para activar el desbloqueo de emergencia, que debe protegerse contra el uso accidental. Si el dispositivo de bloqueo se instala en la puerta, se debe colocar el cable eléctrico del dispositivo dentro de un protector blindado de metal para puertas. De lo contrario, se debe proteger mecánicamente en aquellos lugares en los que esté expuesto.

El centro de recepción de alarmas (ARC) debe contar con medios para anular los dispositivos de bloqueo en caso de salida de emergencia.

Está permitido tener más de un vestíbulo de entrada/salida siempre que cumplan con los requisitos establecidos en este capítulo.

5.7.2.2 Categoría II

Se deben asegurar las puertas de acceso con un dispositivo de bloqueo que cumpla con los requisitos de clase RC2 de la Norma EN 1627.

5.7.3 Entrada de emergencia

Si la entrada al centro de recepción de alarmas (ARC) está controlada por operadores que trabajen dentro del centro, se debería proporcionar un mecanismo o procedimiento para permitir el acceso a las instalaciones sin la ayuda de las personas que se encuentran dentro. Se deben guardar las llaves, códigos o tarjetas que se utilicen para entrar en un lugar seguro, como por ejemplo en una caja fuerte, cuyo acceso debería estar restringido a una lista de personas encargadas. Este mecanismo no se debe utilizar como método habitual de entrada, sino solo en circunstancias excepcionales, como en una situación de emergencia.

5.7.4 Salida(s) de emergencia

La puerta o puertas de las salidas de emergencia se deben abrir hacia el exterior y deben estar provistas de dispositivos de desbloqueo, de conformidad con las Normas EN 179, EN 1125 o EN 13637, según proceda, previstos para activarse solo en caso de emergencia. Los dispositivos de desbloqueo se deben poder accionar únicamente desde el interior del centro de recepción de alarmas (ARC).

5.7.5 Ventilación

5.7.5.1 Categoría I

Los sistemas de ventilación del centro de recepción de alarmas (ARC) se deben controlar desde el interior del centro. Todos los conductos de ventilación se deben proteger con rejillas herméticas que se puedan cerrar fácilmente, ya sea manualmente desde el interior del centro de recepción de alarmas (ARC) o automáticamente en caso de que se sospeche que se está introduciendo gas o humo en el centro.

Si el área de la sección transversal de una entrada o salida de ventilación excede los 0,02 m^2, se debe instalar un equipo de detección de alarmas adecuado para detectar cualquier intento de acceso a la entrada o salida de ventilación.

5.7.5.2 Categoría II

No hay requisitos.

5.7.6 Puntos de entrada y salida de servicios

5.7.6.1 Categoría I

Si la estructura del centro de recepción de alarmas (ARC) cuenta con alguna apertura para la entrada de cables de servicios o tuberías, esta no debe exceder los 0,02 m^2 en el área de la sección transversal. Todas las aperturas en la estructura del centro de recepción de alarmas (ARC) se deben rellenar con material resistente al fuego para minimizar la propagación del fuego y el humo desde el exterior hacia el interior de la estructura del centro.

5.7.6.2 Categoría II

No hay requisitos.

5.7.7 Ventanilla o tolva de transferencia

5.7.7.1 Categoría I

Se puede colocar una ventanilla o tolva de transferencia en la estructura del centro de recepción de alarmas (ARC).

La ventanilla o la tolva de transferencia se debe construir con un material que proporcione resistencia frente a ataques físicos y con balas, de acuerdo con los datos de la tabla 2. Los puntos de acceso deben estar interbloqueados para evitar que se pueda acceder directamente al centro de recepción de alarmas (ARC) en cualquier momento. Por otra parte, la apertura y el cierre de los accesos se deben controlar desde el interior del centro. El punto de acceso externo se debe abrir hacia el exterior desde centro de recepción de alarmas (ARC).

Se debe disponer de sistemas de comunicación por voz entre el área de explotación del centro de recepción de alarmas (ARC) y la entrada externa de la ventanilla o de la tolva.

5.7.7.2 Categoría II

No hay requisitos.

5.8 Ubicación del equipo de procesamiento de datos

5.8.1 Categoría I

5.8.1.1 Generalidades

El siguiente equipamiento del centro de recepción debe estar bajo la responsabilidad del centro y situarse dentro de la estructura del mismo:

- interfaz del sistema de gestión de alarmas (AMS) para la interconexión con el transceptor del centro de recepción (I_{RCT});
- servidores del sistema de gestión de alarmas (bases de datos, dispositivos de almacenamiento);

- equipo de grabación de voz;
- componentes activos de red (enrutadores, conmutadores);
- componentes pasivos de red (paneles de conexión, cableado);
- equipos de comunicación (centralita automática privada, PABX);
- punto de transferencia interna LAN/WAN (proveedor de red).

NOTA La necesidad de contar con transceptores (RCT) dentro de un centro de recepción de alarmas (ARC) de categoría I y la responsabilidad de dichos transceptores puede depender de una solución llamada "alojada" o "no alojada" proporcionada por el proveedor del sistema de transmisión de alarmas (ATSP), tal y como se describe en la Norma EN 50136-1.

Se deberían tener en cuenta los apartados 9.1.12 y 9.1.20.

5.8.1.2 Cuarto técnico situado en el mismo edificio o local que el centro de recepción de alarmas (ARC)

Si el equipo descrito en el apartado 5.8.1 o parte de él no se encuentra dentro de la estructura del centro de recepción de alarmas (ARC), se debe cumplir con los siguientes requisitos en el mismo edificio o en el mismo local donde se ubique el centro:

- se debe completar una evaluación de riesgos documentada de conformidad con el apartado 4.2;
- los requisitos de construcción deben proporcionar resistencia frente a ataques físicos de acuerdo con los apartados 5.2.1, 5.3 y 5.4.1 y con la tabla 2;
- se debe proporcionar resistencia frente al fuego y el humo de acuerdo con el apartado 5.5;
- protección contra el impacto de rayos de acuerdo con el apartado 5.6;
- sistemas de alarma de acuerdo con lo dispuesto en los apartados 6.1.2, 6.1.3, 6.1.4 y 6.1.9;
- fuentes de energía eléctrica de acuerdo con el capítulo 7;

NOTA Las fuentes de alimentación de reserva del centro de recepción de alarmas descritas en el apartado 7.2 también pueden utilizarse para la ubicación del equipo de procesamiento de datos.

- se deben proteger los cables de energía externos, así como el cableado de comunicación con la estructura del centro de recepción de alarmas (ARC), contra ataques físicos y los daños provocados por el fuego.

No se requiere un vestíbulo de entrada. El centro de recepción de alarmas (ARC) debe controlar y autorizar el acceso a dicha zona, incluyendo un sistema de vigilancia por vídeo cuyas imágenes se puedan ver desde el interior del centro para identificar a las personas autorizadas antes de permitirles entrar en el lugar donde se encuentra el equipo de procesamiento de datos.

5.8.1.3 Cuarto técnico situado en una ubicación distinta a la del centro de recepción de alarmas (ARC)

Si el equipo descrito en el apartado 5.8.1 o parte de él no se encuentra dentro de la estructura del centro de recepción de alarmas (ARC), sino que se sitúa en una ubicación remota del centro, se debe cumplir con los siguientes requisitos:

- se debe disponer de un centro de datos diseñado y mantenido de acuerdo con la Norma EN 50600 o de otro centro de recepción de alarmas (ARC) de categoría I de acuerdo con la Norma EN 50518;

- el rendimiento de la conexión entre la ubicación remota y el centro de recepción de alarmas (ARC) en cuanto a la seguridad de los datos, la protección de sustitución y la disponibilidad debe ser igual o superior a los valores definidos por la categoría DP4 de la Norma EN 50136-1.

Si el centro de recepción de alarmas (ARC) cuenta con una ubicación secundaria para el equipo de procesamiento de datos como medida de redundancia, esta debe cumplir con los requisitos previstos para un cuarto técnico de categoría I.

5.8.2 Categoría II

El equipo que se enumera a continuación debe estar bajo la responsabilidad del centro de recepción de alarmas (ARC):

- transceptor del centro de recepción (RCT);
- interfaz en el sistema de gestión de alarmas (AMS) para la interconexión con el transceptor del centro de recepción (I_{RCT});
- servidores del sistema de gestión de alarmas (bases de datos, dispositivos de almacenamiento);
- equipo de grabación de voz;
- componentes activos de red (enrutadores, conmutadores);
- componentes pasivos de red (paneles de conexión, cableado);
- equipos de comunicación (centralita automática privada, PABX);
- punto de transferencia interna LAN / WAN (proveedor de red).

Si el equipo o parte de él no se encuentra dentro de la estructura del centro de recepción de alarmas (ARC), se debe disponer de los siguientes elementos en una ubicación segura que cumpla con una de las siguientes normas publicadas para los centros de datos:

- un centro de datos diseñado y mantenido según la Norma EN 50600, o
- un centro de recepción de alarmas (ARC) de acuerdo con la Norma EN 50518 de categoría I o II, cuyo cuarto técnico esté ubicado en el mismo edificio o local en el que se encuentre el centro.

El rendimiento de la conexión entre la ubicación segura y el centro de recepción de alarmas (ARC) en cuanto a la seguridad de los datos, la protección de sustitución y la disponibilidad debe ser igual o superior a los valores definidos por la categoría DP4 de la Norma EN 50136-1.

5.9 Cables de comunicación

5.9.1 Categoría I

Se deben proteger todos los cables de comunicación entre el punto de acceso del edificio y la estructura contra daños físicos y provocados por el fuego.

Se deben proteger todas las conexiones basadas en cables y las conexiones inalámbricas que transporten mensajes de alarma hacia y desde el centro de recepción de alarmas (ARC) y los sistemas de alarma de intrusión y atraco (I&HAS) remotos conectados al centro de acuerdo con la Norma EN 50136-1.

Debe haber un servicio de asistencia disponible las 24 h del día para todos los circuitos de telecomunicaciones, ya que si estos fallan, la supervisión de las señales de alarma o a la extensión de las señales o mensajes de alarma a los servicios de emergencia se verían afectadas.

5.9.2 Categoría II

No hay requisitos.

5.10 Instalaciones

5.10.1 Categoría I

El centro de recepción de alarmas (ARC) debe contar con baños y aseos dentro de su estructura.

5.10.2 Categoría II

No hay requisitos.

6 Sistemas de alarma del centro de recepción de alarmas (ARC)

6.1 Categoría I

6.1.1 Generalidades

El centro de recepción de alarmas (ARC) debe contar con instalaciones de detección y vigilancia electrónicas de acuerdo con los apartados 6.1.2 a 6.1.10 inclusive.

Todos los sistemas incluidos en este capítulo se deben mantener de acuerdo con las normas pertinentes. Si no se han publicado normas al respecto, el mantenimiento se debe realizar de acuerdo con las directrices del fabricante con el fin de garantizar la fiabilidad en todo momento.

Para las siguientes circunstancias se debe indicar una condición de alarma dentro del centro de recepción de alarmas (ARC), que también se debe notificar a otro centro en cumplimiento con los requisitos previstos para la categoría I de esta norma:

- detección de un ataque externo (véase 6.1.2);
- ventana/área acristalada abierta (véase 6.1.3);
- detección de un incendio (véase 6.1.4);

- falta de seguridad en las puertas de acceso y salida (véase 6.1.5);
- activación del dispositivo contra atracos (véase 6.1.7);
- supervisión de la seguridad (véase 6.1.8);
- mensajes de los sistemas de alarma del centro de recepción de alarmas (ARC) (véase 6.1.9).

6.1.2 Ataque externo

Las medidas de seguridad del centro de recepción de alarmas (ARC) deben incluir un sistema de alarma de intrusión y atraco (I&HAS) de acuerdo con el grado 3 de la Norma EN 50131-1.

El equipo de control y señalización del sistema de alarma de intrusión y atraco (I&HAS) del centro de recepción de alarmas (ARC) debe situarse dentro de la estructura del centro.

Las zonas del edificio ocupadas por la empresa que gestiona el centro de recepción de alarmas (ARC) y aquellas en las que se encuentre el propio centro deben contar con un sistema de alarma de intrusión y atraco (I&HAS) de protección, de acuerdo con la Norma EN 50131-1. Estos sistemas de alarma contra intrusos deben incorporar un dispositivo de aviso para alertar a los operadores del centro de recepción de alarmas (ARC) inmediatamente después de la notificación de una alarma.

La guía de aplicación de la Especificación Técnica CLC/TS 50131-7 recoge las recomendaciones para el diseño, la planificación, el funcionamiento, la instalación y el mantenimiento de dichos sistemas.

6.1.3 Áreas acristaladas

Todas las áreas acristalada que puedan abrirse deben estar dotadas de un sistema de detección de apertura.

6.1.4 Incendios

Las zonas del edificio ocupado por la empresa que gestiona el centro de recepción de alarmas (ARC) y aquellas en las que se encuentre el propio centro deben contar con un sistema de detección de incendios de protección de acuerdo con los requisitos nacionales para el nivel más alto de protección de la propiedad y las personas que incorpore componentes certificados de acuerdo con la serie de Normas EN 54.

6.1.5 Entrada/salida

Se debe activar una alarma acústica o visual dentro del centro de recepción de alarmas (ARC) para notificar a los operadores cuando alguna puerta de entrada o salida del centro o del vestíbulo no esté asegurada, excepto cuando las puertas del vestíbulo de entrada se hayan abierto para una permitir una entrada/salida autorizada.

Se debe emitir una condición de alarma cuando se abra una puerta de salida de emergencia o cuando las dos puertas de entrada al vestíbulo y al centro de recepción de alarmas (ARC) se abran al mismo tiempo.

6.1.6 Gas

El centro de recepción de alarmas (ARC) debe contar con sistemas de detección de al menos monóxido de carbono, que avisarán a los empleados del centro antes de que los niveles alcancen una concentración que haga necesaria la evacuación.

6.1.7 Atraco

Los dispositivos contra atracos instalados de acuerdo con la Norma EN 50131-1 se deben instalar dentro del centro de recepción de alarmas (ARC) en posiciones adyacentes al vestíbulo de entrada, salida(s) de emergencia, ventanilla(s) de transferencia y en todas las posiciones normales de operación del personal del centro.

6.1.8 Supervisión de la seguridad

Se debe comprobar la seguridad del personal del centro de recepción de alarmas (ARC) de manera automática en intervalos de 60 min como máximo. Si no hay respuesta en un plazo de 60 s cuando se haga la comprobación, se debe emitir automáticamente una alarma a otro centro de recepción de alarmas (ARC) que cumpla los requisitos previstos para la categoría I de esta norma.

6.1.9 Mensajes de los sistemas de alarma del centro de recepción de alarmas (ARC)

Se deben notificar los mensajes del sistema de alarma del centro de recepción de alarmas (ARC) (véase 6.1.1) a otro centro que cumpla los requisitos previstos para la categoría I de esta norma. El centro de recepción de alarmas (ARC) que reciba los mensajes no debe estar ubicado en el mismo edificio. El sistema de transmisión de alarmas para el sistema de alarma debe cumplir, como mínimo, con los requisitos previstos para las categorías SP4 o DP3 de la Norma EN 50136-1.

6.1.10 Sistema de videovigilancia

Los sistemas de videovigilancia deben funcionar de tal forma que:

a) Todos los accesos al edificio en el que se encuentra el centro de recepción de alarmas (ARC) puedan supervisarse desde dentro del centro de acuerdo con la guía de aplicación de la Norma EN 62676-4.

b) Los empleados del centro de recepción de alarmas (ARC) puedan identificar a las personas autorizadas antes de permitirles entrar en el vestíbulo de entrada, ver cualquier actividad que se realice en el mismo y garantizar una salida segura.

c) Los empleados del centro de recepción de alarmas (ARC) puedan identificar a cualquier empleado que utilice una ventanilla de transferencia.

6.2 Categoría II

El centro de recepción de alarmas (ARC) debe contar con un sistema de alarma de intrusión y atraco (I&HAS) de grado 2 como mínimo, según la Norma EN 50131-1, que incluya al menos un dispositivo contra atracos.

Las zonas del edificio ocupado por la empresa que gestiona el centro de recepción de alarmas (ARC) y aquellas en las que se encuentre el propio centro deben contar con un sistema de detección de incendios de protección de acuerdo con los requisitos nacionales para el nivel más alto de protección de la propiedad y las personas que incorpore componentes certificados de acuerdo con la serie de Normas EN 54.

7 Fuentes de alimentación eléctrica

7.1 Alimentación de la red eléctrica

La alimentación de la red eléctrica se debe utilizar como la principal fuente de energía eléctrica, aunque también se pueden utilizar alternativas fiables. Se debe indicar cuál es la fuente de alimentación en uso en el área de explotación. Si la alimentación de la red eléctrica falla, se debe emitir una alarma acústica o visual para alertar a los operadores del área de explotación. La alimentación de la red eléctrica debe ser capaz de proporcionar suficiente energía para la carga normal del centro de recepción de alarmas (ARC) y para recargar simultáneamente los dispositivos de almacenamiento de energía de reserva del sistema de alimentación ininterrumpida (SAI) (baterías) hasta la capacidad requerida en un plazo de 24 h.

7.2 Fuentes de alimentación de reserva

7.2.1 Generalidades

El suministro de energía de reserva debe tener la capacidad suficiente para el funcionamiento ininterrumpido de todos los equipos de comunicación, señalización, supervisión, grabación, cerraduras de puertas accionadas eléctricamente, equipo de ventilación y alumbrado esenciales, incluido el equipo requerido para la vigilancia necesaria durante un período de 24 h basado en una demanda de 1,2 veces la carga máxima prevista.

El cambio a o desde una fuente de alimentación de reserva no debe afectar el funcionamiento normal del equipo.

El suministro de energía de reserva debe realizarse a través de un generador o generadores apoyados por un sistema de alimentación ininterrumpida (SAI) de acuerdo con la Norma EN 62040-1.

7.2.2 Sistema de alimentación ininterrumpida (SAI)

El sistema de alimentación ininterrumpida (SAI) y cualquier equipo de cambio de estado automático deben estar ubicados dentro de la estructura del dentro de recepción de alarmas (ARC). Como excepción, si el sistema de alimentación ininterrumpida (SAI) y/o el equipo de cambio de estado automático no están instalados dentro de la estructura del centro de recepción de alarmas (ARC), se debe aplicar lo siguiente:

a) Categoría I – el sistema de alimentación ininterrumpida (SAI) y/o el equipo de cambio de estado automático deben situarse en un área que cumpla con los requisitos de construcción de un centro de recepción de alarmas (ARC) de categoría I, tal como se describe en los apartados 5.2.1, 5.3, 5.4.1, 5.5, 5.6, mientras que el sistema de alarma debe cumplir con los apartados 6.1.2, 6.1.4 y 6.1.5.

b) Categoría II – el sistema de alimentación ininterrumpida (SAI) y/o el equipo de cambio de estado automático deben situarse en un área que cumpla con los requisitos de construcción de un centro de recepción de alarmas (ARC) de categoría II, como se describe en el capítulo 5, mientras que el sistema de alarma debe cumplir con el apartado 6.2.

Cuando el sistema de alimentación ininterrumpida (SAI) se encuentre fuera de la estructura del centro de recepción de alarmas (ARC), el propio centro debe autorizar el acceso a dicha zona e incluir un sistema de videovigilancia cuyas imágenes se puedan ver desde el interior del centro.

El sistema de alimentación ininterrumpida (SAI) debe entrar en funcionamiento de manera automática inmediatamente después de que la tensión primaria caiga por debajo del nivel requerido para operar el centro de recepción de alarmas (ARC). El centro de recepción de alarmas (ARC) debe volver a funcionar con la fuente de alimentación primaria, mientras que los dispositivos de almacenamiento de energía del sistema de alimentación ininterrumpida (SAI) deben recargarse de manera automática cuando se restablezca la tensión primaria.

Las instalaciones de las baterías deben cumplir con la Norma EN 50272-2.

Cuando se utilice un generador de reserva, la capacidad del sistema de alimentación ininterrumpida (SAI) debe ser suficiente para alimentar el equipo del centro de recepción de alarmas (ARC) durante al menos 10 min, según lo previsto en el apartado 7.2.1.

7.2.3 Generadores de reserva

Un generador situado dentro de la estructura del centro de recepción de alarmas (ARC) debe estar separado de la zona de explotación por una construcción que ofrezca una resistencia al fuego de acuerdo con los requisitos establecidos en el apartado 5.5.

Todos los generadores de reserva deben contar con un suministro de combustible *in situ* suficiente como para hacer funcionar el generador durante al menos 24 h.

Todos los generadores de reserva deben disponer de un medio de arranque independiente que se active de manera automática cuando falle el suministro de la red eléctrica. El funcionamiento de los generadores de reserva se debe indicar dentro del centro de recepción de alarmas (ARC). La batería necesaria para poner en marcha un generador de reserva debe recargarse a través de la red eléctrica.

Como excepción, si el generador de reserva no está instalado en la estructura del centro de recepción de alarmas (ARC), se aplican las siguientes condiciones:

a) Categoría I – el generador de reserva debe situarse en una zona que cumpla con los apartados 6.1.2, 6.1.4 y 6.1.5.

b) Categoría II – el generador de reserva debe situarse en una zona que cumpla con el apartado 6.2.

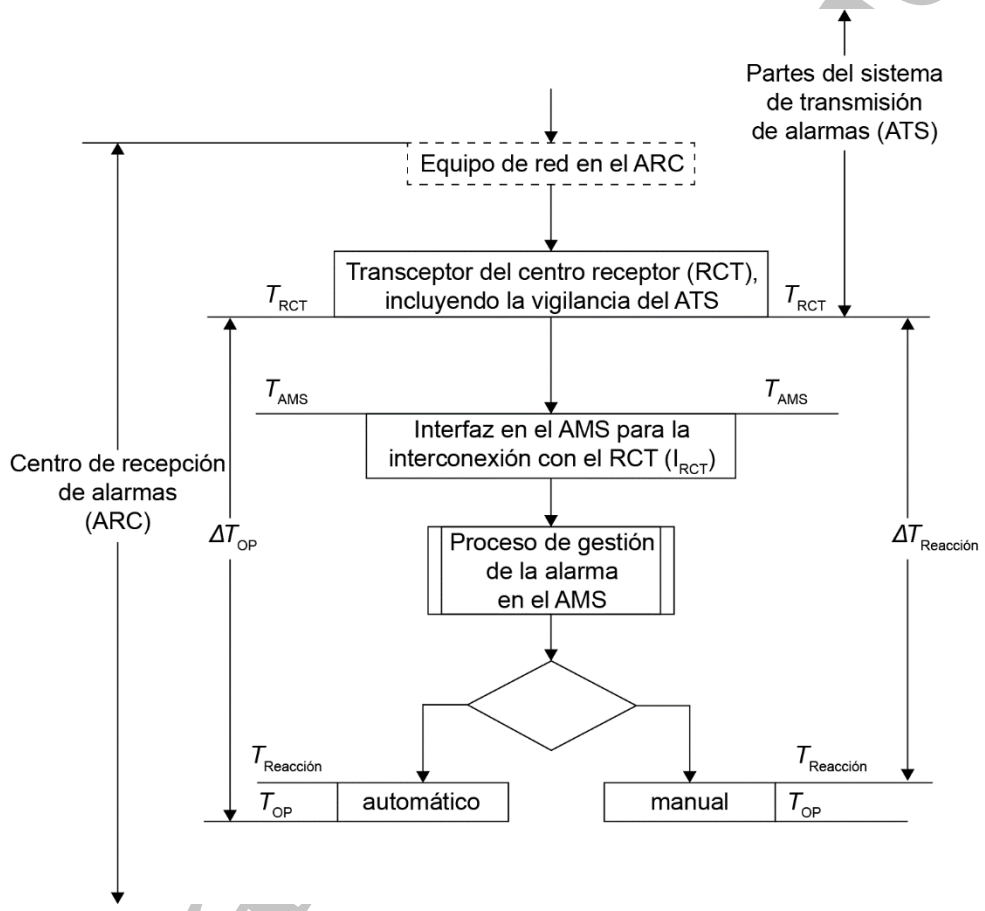
Cuando el generador de reserva se encuentre fuera de la estructura del centro de recepción de alarmas (ARC), el propio centro debe autorizar el acceso a dicha zona e incluir un sistema de videovigilancia cuyas imágenes se puedan ver desde el interior del centro.

8 Sistema de gestión de alarmas

8.1 Generalidades

Un sistema de gestión de alarmas (AMS) es un sistema que almacena, organiza, controla, gestiona y permite la recuperación de los datos de los clientes y que está conectado a un equipo receptor de alarmas para la notificación automática de mensajes para cada sistema de alarma. El propósito principal de un sistema de gestión de alarmas (AMS) es recibir y presentar información y mensajes de alarma. El anexo C describe una sistema de gestión de alarmas (AMS) típico.

La figura 2 muestra la secuencia de eventos que recaen bajo la responsabilidad del centro de recepción de alarmas (ARC) y que se aplican a cualquier mensaje de alarma generado por un sistema de alarma, como se detalla en el campo de aplicación de esta norma, una vez completado el procesamiento por parte del transceptor del centro de recepción. Si corresponde, esta figura se debe interpretar junto con la figura 1 de la Norma EN 50136-1:2012. Esta norma se aplica a un sistema de gestión de alarmas que gestiona los eventos desde T_{RCT} hasta $T_{Reacción}$.



Leyenda

T_{RCT} Tiempo del mensaje de salida del transceptor del centro de recepción (RCT)

T_{AMS} Tiempo de recepción de mensajes en el sistema de gestión de alarmas (AMS)

$T_{Reacción}$ Tiempo para proporcionar información al operador o para iniciar una acción automática

$\Delta T_{Reacción}$ Tiempo que transcurre entre el momento de disponibilidad del mensaje de alarma a la salida del transceptor del centro de recepción (RCT) y el comienzo de la gestión automática o manual de la alarma en el sistema de gestión de alarmas (AMS) ($\Delta T_{reacción} = T_{reacción} - T_{RCT}$)

T_{OP} Tiempo de la primera acción iniciada por el operador del centro de recepción de alarmas (ARC) o el sistema de gestión de alarmas (AMS) según el plan de acción acordado con el cliente

ΔT_{OP} Tiempo que transcurre entre el momento de disponibilidad del mensaje de alarma en la salida del transceptor del centro de recepción (RCT) y el momento de la primera acción iniciada por el operador del centro de recepción de alarmas (ARC) o el sistema de gestión de alarmas (AMS) ($\Delta T_{OP} = T_{OP} - T_{RCT}$)

Figura 2 – Secuencia de eventos

8.2 Sincronización temporal del equipo

Cualquier componente del equipo en el que se registre una referencia horaria con el fin de prestar servicio al centro de recepción de alarmas (ARC) se debe sincronizar con una fuente de tiempo UTC (tiempo universal coordinado). La sincronización se puede lograr a través del propio sistema de gestión de alarmas (AMS), del personal del centro de recepción de alarmas (ARC) o empleando una fuente interna o externa.

La sincronización se debe realizar al menos cada 24 h. El sistema de gestión de alarmas (AMS) debe tratar la falta de sincronización como un fallo cuando exceda las 24 h. También se deben tratar como un fallo aquellas situaciones en las que se produzca una diferencia específica de más de 5 s en la sincronización de la hora del sistema de gestión de alarmas (AMS) con respecto a la hora UTC.

En el caso de los componentes con una interfaz gráfica de usuario (GUI) para el procesamiento de alarmas, la hora local utilizada por el centro de recepción de alarmas (ARC) siempre debe estar disponible.

8.3 Grabación y registro de eventos

El centro de recepción de alarmas (ARC) debe mantener un registro automático de los siguientes eventos con fecha y hora:

- T_{RCT}, T_{AMS}, $T_{Reacción}$ y T_{OP};
- cualquier comunicación externa en la que se proporcione la identidad de la parte que se comunica (instalaciones vigiladas o línea telefónica desde la que llama), el tipo y el contenido del mensaje;
- cualquier acción del operador con detalles acerca de la acción realizada y la identidad del operador u operadores que la realizaron y completaron; incluidas la hora y fecha de finalización de la acción;
- cualquier acción automática adoptada por el propio sistema de gestión de alarmas (AMS) (véase el anexo C).

Todos los datos relacionados con la comunicación y las acciones deben conservarse de forma que se puedan recuperar durante un período mínimo de tres meses.

Para las alarmas sociales, véase la Norma EN 50134-7.

8.4 Almacenamiento de datos maestros

Se deben almacenar los datos maestros de cada sistema de alarma conectado al centro de recepción de alarmas (ARC) de forma que sean fácilmente recuperables en función de las necesidades de la gestión y de los operadores del centro. Los datos maestros se deben mantener actualizados en todo momento. Los cambios en los datos maestros se deben identificar con fecha y hora. Los datos maestros que se hayan modificado debido a un cambio contractual, a un cambio en la organización del cliente o que hayan quedado obsoletos a raíz de una cancelación o modificación del contrato se deben conservar durante un período mínimo de tres años.

Los datos maestros deben incluir:

- número de referencia único del sistema de alarma (AS);

- nombre, dirección y números de teléfono de las instalaciones vigiladas;
- las acciones que se deben adoptar para cada mensaje de alarma;
- datos de contacto de los respondedores (servicios de emergencia, titular de la llave);
- cualquier otro dato específico necesario para que el centro de recepción de alarmas (ARC) gestione los mensajes de alarma y lleve a cabo las acciones acordadas;
- definición de las alarmas de nivel prioritario y de los tiempos de respuesta correspondientes (si no coinciden con el rendimiento predeterminado que se especifica anteriormente).

9 Funcionamiento del centro de recepción de alarmas (ARC)

9.1 Procedimientos. Generalidades

9.1.1 Generalidades

Se deben establecer procedimientos habituales de funcionamiento (SOP), que deben ponerse a disposición de todo el personal según sea necesario en función de sus responsabilidades. Cada procedimiento habitual de funcionamiento (SOP) debe identificar a los responsables de su diseño, aplicación, ejecución, evaluación y mantenimiento. Cuando se requieran indicadores clave del rendimiento (KPI) para medir los niveles de ejecución y calidad de los procedimientos habituales de funcionamiento (SOP), se deben identificar junto con el método de medición. Se debe mantener en todo momento una visión general que documente la fecha válida de publicación de cada protocolo de funcionamiento habitual (SOP). Se deben documentar los procedimientos habituales de funcionamiento (SOP) para los siguientes propósitos:

9.1.2 Creación, modificación y cancelación de servicios o cuentas de clientes

El procedimiento debe incluir la forma en que se modifican y se archivan los datos maestros según lo descrito en los apartados 8.3 y 8.4.

9.1.3 Tratamiento de los mensajes

El procedimiento debe incluir el tratamiento de los mensajes procesados en el centro de recepción de alarmas (ARC) e incluir la recepción, el procesamiento y la(s) acción(es) del operador, desde el suministro de información al operador ($T_{\text{Reacción}}$) hasta la primera acción iniciada por el operador o el sistema de gestión de alarmas (AMS) (T_{OP}). Véase la figura 2.

9.1.4 Comunicación con los servicios de respuesta

Los procedimientos deben incluir cualquier información específica según lo acordado o requerido por los servicios de respuesta, como la policía, los bomberos, los guardias de seguridad y los titulares de las llaves.

9.1.5 Servicios individuales prestados por el centro de recepción de alarmas (ARC)

El procedimiento debe incluir cada uno de los servicios prestados por el centro de recepción de alarmas (ARC), incluyendo el rendimiento u otros indicadores clave del rendimiento (KPI).

9.1.6 Verificación de la alarma

Si se aplica un procedimiento de verificación de alarmas a la gestión de mensajes, dicho procedimiento debe describir cómo se verifican y gestionan los mensajes.

NOTA Algunos ejemplos de verificación de alarmas incluyen:

- Verificación secuencial: se trata de una alarma notificada que emana de dos o más fuentes independientes configuradas de tal manera que se considera una alarma auténtica. El procesamiento de la verificación secuencial puede llevarse a cabo dentro de las instalaciones vigiladas por el equipo de control y señalización o por el centro de recepción de alarmas (ARC).

- Verificación acústica: se trata una alarma notificada que ha sido verificada con información acústica en las instalaciones vigiladas, de tal manera que se considera una alarma auténtica.

- Verificación visual: se trata de una alarma notificada que ha sido verificada con una o varias imágenes de las instalaciones vigiladas, de tal manera que se considera una alarma auténtica.

- Verificación por parte del cliente/usuario: se trata de una alarma notificada que ha sido verificada por el cliente o el usuario. En este caso, el centro de recepción de alarmas (ARC) necesitará que se proporcione una verificación en base al método de identificación que se haya acordado.

9.1.7 Aumento inesperado de las señales de alarma

El procedimiento debe describir las medidas de contingencia adoptadas para hacer frente a aumentos inesperados de la actividad de alarma causados, por ejemplo, por el mal tiempo o por cortes en las comunicaciones.

9.1.8 Fallos en la vía de transmisión de alarmas

El procedimiento debe describir cómo se gestionan los fallos en la vía de transmisión de alarmas (ATP) e incluir indicadores del rendimiento.

9.1.9 Controles para mantener la calidad del servicio

El procedimiento debe incluir las medidas de control establecidas para evitar una respuesta deficiente por parte del centro de recepción de alarmas (ARC) hacia personas u objetos protegidos. Como parte de este procedimiento, se debería supervisar la ejecución (técnica/humana) de la respuesta según el plan de acción acordado.

9.1.10 Instalación, mantenimiento, protección, retirada y reutilización de los bienes bajo el control del centro de recepción de alarmas (ARC)

El procedimiento debe identificar a aquellas personas que estén autorizadas a aprobar y ejecutar la instalación, el mantenimiento, la retirada y la disposición/reutilización de los bienes. Para ello se deben tener en cuenta los riesgos específicos relacionados con los datos y los programas informáticos con licencia que puedan formar parte del conjunto de bienes. El procedimiento debe garantizar que los bienes sin supervisión dispongan de una protección adecuada.

9.1.11 Vigilancia y pruebas del equipo

Para asegurar el correcto funcionamiento del centro de recepción de alarmas (ARC), es necesario supervisar todo el equipo y someterlo a ensayo, así como registrar los resultados, con la siguiente frecuencia:

– Diaria

Se deben supervisar los transceptores del centro de recepción (RCT), el sistema de gestión de alarmas (AMS), el equipo de presentación, el equipo de comunicación y de red del centro de recepción de alarmas (ARC), así como todas las líneas de comunicación por voz, para asegurar su correcto funcionamiento.

– Mensual

Se deben supervisar y someter a ensayo todos los componentes del sistema de alimentación eléctrica, como se define en los apartados 7.1 y 7.2, y los propios sistemas de alarma del centro de recepción de alarmas (ARC) para garantizar su correcto funcionamiento.

– Anual

Se deben supervisar y someter a ensayo todos los componentes del sistema de alimentación eléctrica, como se define en los apartados 7.1 y 7.2, y los propios sistemas de alarma del centro de recepción de alarmas (ARC) apagando la fuente de alimentación primaria.

9.1.12 Procedimientos y notificación de fallos

Cualquier componente del equipo que esté involucrado en la recepción, visualización o transmisión ulterior de un mensaje de alarma, incluidas las fuentes de alimentación, deben disponer de una instalación y un procedimiento de reserva que pueda ponerse en funcionamiento de forma automática o por parte de un operador del centro de recepción de alarmas (ARC) en el plazo de 1 h desde el momento en que el operador conozca la existencia del fallo.

La reparación del equipo defectuoso debe incluir un plazo para iniciar el informe de los fallos, que no debe exceder los 15 min desde la detección del mismo. Se debe registrar cualquier condición de fallo de manera automática o manual en un registro de notificación de fallos.

La disponibilidad mensual del centro de recepción de alarmas (ARC) se debe expresar como el porcentaje de tiempo durante el cual las partes funcionales para la recepción de alarmas funcionan de conformidad con lo dispuesto en esta norma. Los componentes funcionales incluyen:

– todo el equipo involucrado en la recepción y el tratamiento de los mensajes de alarma, incluyendo, entre otros, el transceptor del centro de recepción (RCT), de acuerdo con la Norma EN 50136-3;

– el sistema de gestión de alarmas (AMS), incluyendo el hardware, el software y los componentes de red necesarios.

NOTA En los casos en los que los componentes funcionales estén por duplicado, proporcionando así redundancia para que el fallo de un componente individual no afecte a la recepción o visualización de las alarmas, el cálculo de la disponibilidad seguiría dando como resultado el 100%.

9.1.13 Gestión de la información

El procedimiento debe describir la manera en la que los datos se mantienen, organizan, modifican, gestionan y recuperan. El procedimiento habitual de funcionamiento (SOP) debe detallar la forma en la que los datos maestros se conectan con todo el equipo receptor de alarmas para la transmisión automática de todos los mensajes para cada sistema de alarma y para la conservación de los registros de las incidencias de funcionamiento relacionados con el cliente. Los procedimientos adicionales deben describir cómo se mantienen, protegen, conservan y eliminan los datos (la eliminación de los datos debe cumplir con los requisitos previstos por la Norma EN 15713). Se deben adoptar y mantener medidas para evitar la pérdida, destrucción, falsificación, el acceso no autorizado y la divulgación no autorizada de datos, ya sea mediante una interferencia involuntaria o malintencionada. Estas medidas deben tener en cuenta la legislación y los reglamentos aplicables, así como las obligaciones contractuales y los requisitos comerciales. Para los datos maestros de los clientes, se debe tener en cuenta el apartado 8.4.

Se debe asignar a cada sistema de alarmas (AS) conectado un registro individual, de referencia única, en el que se registren los detalles, junto con las instrucciones correspondientes. Asimismo, se debe asignar un registro histórico individual, que puede formar parte del registro anterior, en el que se registren todas las actividades relacionadas con los mensajes y las acciones del operador pertinentes.

9.1.14 Copia de seguridad de los datos

El procedimiento debe describir cómo se hacen las copias de seguridad de todos los datos del cliente y del sistema, cuya disponibilidad y fiabilidad ha de someterse a ensayo.

Cuando dos centros de recepción de alarmas (ARC) funcionen de manera conjunta para cumplir con lo dispuesto en el apartado 10.5.1, se debe poder acceder a los datos de los clientes desde ambos centros.

9.1.15 Confidencialidad y clasificación de la información

El procedimiento debe describir la manera en la que las personas que tengan acceso a los datos del centro de recepción de alarmas (ARC) garantizan la confidencialidad de la información.

Dicho procedimiento debe incluir:

- una política de escritorio limpio para documentos en papel y soportes de almacenamiento extraíbles y una política de pantalla limpia para las instalaciones de procesamiento de información;

- instrucciones de clasificación y etiquetado de la información en función de los requisitos legales y el valor, el grado de gravedad y la sensibilidad de los datos ante la divulgación o modificación no autorizada de los mismos.

9.1.16 Relaciones con proveedores esenciales

El procedimiento debe describir cómo interactúan los centros de recepción de alarmas (ARC) y el proveedor o proveedores esenciales. Se debe disponer de un contrato escrito individual para cada proveedor para los procedimientos específicos acordados.

El centro de recepción de alarmas (ARC) debe supervisar y examinar el desempeño de los proveedores esenciales con arreglo a los procedimientos acordados y realizar una evaluación en períodos que no excedan de un año.

9.1.17 Procedimientos administrativos

El procedimiento debe describir cómo se vinculan los procesos operativos del centro de recepción de alarmas (ARC) con los procesos administrativos, como los que se necesitan para las ventas, la gestión de los contratos de clientes y proveedores o la facturación para garantizar la coherencia de extremo a extremo.

9.1.18 Acceso físico

El procedimiento debe describir cómo se controla el acceso físico a y la salida del centro de recepción de alarmas (ARC). El procedimiento debe definir los métodos utilizados para identificar a las personas que soliciten acceso.

Para un centro de recepción de alarmas (ARC) de categoría I, el acceso físico se debe controlar mediante la acción de un operador dentro de la estructura del centro en el momento de acceso. Además, se debe mantener un registro de todos los visitantes que accedan a la estructura del centro de recepción de alarmas (ARC).

9.1.19 Acceso remoto

El procedimiento debe describir cómo se ha de controlar el acceso y la salida remotos de cualquier sistema dentro del centro de recepción de alarmas (ARC) y del equipo de procesamiento de recepción de datos (véase 5.8) mediante un procedimiento de inicio/cierre de sesión en el que se registren la hora y la fecha, las credenciales de la persona implicada y las acciones realizadas. Para conceder el acceso remoto, es necesario contar con autorización por parte del centro de recepción de alarmas (ARC). Véase el anexo B para más información relacionada con el acceso remoto al sistema.

9.1.20 Continuidad de las operaciones y emergencias

Se debe diseñar un procedimiento para la continuidad de las actividades y la recuperación en caso de desastre. El plan de contingencia debe incluir suficientes detalles para describir cómo se han de restablecer los servicios de supervisión. El centro de recepción de alarmas (ARC) debe revisar el plan cada seis meses.

El personal debe recibir formación acerca de los procedimientos operacionales y de emergencia para hacer frente a las incidencias disruptivas:

a) Los procedimientos de respuesta en caso de emergencia se deben acordar con los contratistas y los servicios de emergencia para permitir que se mantenga la función de supervisión del centro de recepción de alarmas (ARC) mientras se investiga el incidente de emergencia o mientras se mitigan o reparan los daños.

b) En el caso de que un centro de recepción de alarmas (ARC) quede totalmente fuera de servicio, se debe disponer de un procedimiento habitual de funcionamiento (SOP) de emergencia para hacer frente a esta situación (por ejemplo, transferencia de los servicios a otro centro, información a los clientes y socios).

9.1.21 Evacuación de emergencia y reingreso

El procedimiento debe describir los pasos a seguir para realizar una evacuación parcial o completa e incluir acciones para volver a acceder al centro o iniciar un proceso de recuperación tras una evacuación.

9.1.22 Entrada de emergencia

Se debe documentar el procedimiento de entrada de emergencia descrito en el apartado 5.7.3.

Todo el personal debe recibir formación y capacitación acerca de cómo actuar en un procedimiento de emergencia cada seis meses como mínimo. Estas actividades deben quedar registradas.

9.1.23 Indicadores clave del rendimiento

El procedimiento debe describir la forma en que se elaboran y se ponen a disposición las estadísticas de rendimiento para demostrar el cumplimiento de los servicios contratados y deben incluir la siguiente información:

a) Cada servicio prestado según el contrato del cliente.

b) Rendimiento de la gestión de los mensajes de alarma, véase el apartado 9.2.

c) Fallos en la vía de transmisión de alarmas (ATP).

9.2 Criterios de rendimiento – Gestión de mensajes

El equipo y los recursos para la gestión de alarmas deben ofrecer el siguiente rendimiento.

El tiempo ΔT_{OP} debe cumplir con los criterios de rendimiento acordados en el contrato con cada cliente, que como mínimo deben cubrir los siguientes valores:

- para atracos, incendios, sistemas fijos de lucha contra incendios, seguimiento de personas y para otras alarmas que se consideren de máxima prioridad según lo acordado: 30 s para el 80% de las alarmas recibidas y 60 s para el 98,5% de las alarmas recibidas;

- todas las demás condiciones de alarma: 90 s para el 80% de las alarmas recibidas y 180 s para el 98,5% de las alarmas recibidas.

Si el procedimiento de gestión de alarmas incluye un retraso en la gestión de las mismas, el período de retraso puede excluirse del cálculo del ΔT_{OP}. El procedimiento de gestión debe cumplir con el contrato del cliente.

Los criterios de funcionamiento de las alarmas sociales deben respetar las condiciones previstas en la Norma EN 50134-7.

Se debe lograr la conformidad con los criterios anteriores en un período de doce meses consecutivos.

10 Principios generales, liderazgo, gobernanza, gestión y personal

10.1 Generalidades

Este capítulo describe los instrumentos de gestión que se deben aplicar en el centro de recepción de alarmas (ARC). Estos instrumentos se deben tener en cuenta para definir los procedimientos de funcionamiento y diseñar la infraestructura técnica y los locales.

10.2 Gobernanza y estrategia

La dirección del centro de recepción de alarmas (ARC), por ejemplo, la persona o personas responsables de fijar los objetivos, preparar y tomar decisiones y ejecutarlas para alcanzar los objetivos del centro, debe garantizar la aplicación de un sistema de gestión. En particular debe:

- establecer la visión, fijar los objetivos, proporcionar dirección y gestionar los riesgos de su organización mediante la definición de estrategias escritas que tengan en cuenta las necesidades y expectativas de todas las partes interesadas pertinentes (como clientes, empleados, accionistas, socios comerciales, aseguradores, respondedores y autoridades públicas);

- poner en marcha y mantener medidas adecuadas para cumplir las condiciones previstas por esta norma;

- supervisar de manera continua el ambiente empresarial, así como el rendimiento de la organización;

- establecer una comunicación permanente con todas las partes interesadas para mantener un alto nivel de concienciación en relación con los servicios prestados de seguridad y protección.

NOTA Un sistema de gestión que siga los principios de la Norma EN ISO 9001 se considera adecuado para satisfacer este requisito.

10.3 Configuración jurídica y operativa

Los servicios de centro de recepción de alarmas (ARC) sólo los deben poder ofrecer, vender y ejecutar personas jurídicas que estén registradas legalmente en su lugar de actividad. Si los servicios del centro de recepción de alarmas (ARC) se ofrecen, venden o producen en lugares diferentes, este requisito se debe aplicar a cada uno de los lugares utilizados por el centro.

Los centros de recepción de alarmas (ARC) deben conservar los originales de todos los contratos activos con clientes, socios comerciales y proveedores. Los operadores del centro de recepción de alarmas (ARC) deben tener acceso a los procedimientos de funcionamiento oportunos. Para conservar los contratos con clientes que hayan expirado, se debe respetar la legislación local, aunque como mínimo se deberían conservar durante el tiempo especificado en el apartado 8.4.

10.4 Sistema de gestión

Dentro del sistema de gestión, los centros de recepción de alarmas deben contar con políticas y planes documentados y actualizados regularmente para los siguientes fines:

- **Gestión de riesgos y contingencias**, que abarca aspectos relacionados con la resistencia, la continuidad de las actividades y la recuperación ante un desastre con un análisis de riesgos exhaustivo, por ejemplo, según la serie de Normas ISO 31000. Debe incluir asimismo planes para el emplazamiento del centro de recepción de alarmas (ARC) y una descripción de los procedimientos del centro. Además, debe tener en cuenta las medidas previstas para gestionar las incidencias disruptivas y las medidas asociadas para la prevención, detección temprana y el remedio de dichas incidencias a nivel de gestión y a nivel técnico. En particular, debe incluir:

  - planificación del emplazamiento del centro de recepción de alarmas (ARC) y descripción de los procedimientos habituales de funcionamiento (SOP) del centro;

- seguridad de las TIC (tecnologías de la información y la comunicación) del centro de recepción de alarmas (ARC);

  NOTA La Norma ISO/IEC 27001 contiene los requisitos para la gestión de la seguridad de la información.

- asignación de prioridades para la preservación y/o restauración de actividades y servicios, incluidos los datos de contacto de los contratistas y proveedores de servicios capaces de llevar a cabo la restauración, descripción de los medios por los que se deben continuar o restaurar los servicios;
- gestión de los niveles de personal durante una incidencia disruptiva;
- comunicación con todas las partes interesadas durante y después de la interrupción;
- los informes y planes actuales de análisis de riesgos deben estar disponibles en cualquier momento por si es necesario llevar a cabo un examen de gestión o una auditoría.

- **Gestión de la información**, incluyendo los sistemas informáticos y la seguridad informática, de acuerdo con la Directiva europea en materia de protección de datos (95/46/CE) o similar.

- Gestión del rendimiento operativo, que abarca los siguientes aspectos:
  - métodos de listado y medición de los indicadores clave del rendimiento, que son esenciales para demostrar que los servicios vendidos funcionan con el rendimiento especificado;
  - métodos de listado y medición de los indicadores clave del rendimiento operativo, que son esenciales para la gestión diaria y la mejora continua del rendimiento del centro de recepción de alarmas (ARC).

- **Gestión de las quejas** de todas las partes interesadas, con miras a resolver cada una de las quejas individuales y a identificar los fallos sistemáticos que, además, requieran un ajuste de los procedimientos, políticas o directrices.

- **Gestión de la cartera de servicios** para la creación, gestión y eliminación gradual de los servicios prestados, incluida una lista de los servicios actualmente disponibles para nuevos contratos y una lista de los servicios adicionales que el centro de recepción de alarmas (ARC) presta a los clientes existentes.

- **Gestión de la dotación de personal** con directrices para investigar los antecedentes de seguridad y los antecedentes penales de todo el personal con acceso a los locales y procesos del centro de recepción de alarmas (ARC). Este proceso debe incluir descripciones de puestos y perfiles de calificación para todas las funciones, con planes de capacitación y perfiles de trayectoria profesional para los empleados, así como normas para dar por terminado el acceso a la información para los empleados que abandonen el centro de recepción de alarmas (ARC).

- **Gestión de clientes**, con el fin de garantizar que los datos del perfil proporcionados por el cliente y la información relativa al contrato y a las transacciones se mantengan actualizados. La responsabilidad de terceros debe quedar claramente excluida, en particular para los instaladores y los proveedores de servicios de telecomunicaciones.

- **Gestión de socios comerciales**, teniendo en cuenta los diversos casos comerciales aplicables y las relaciones contractuales/operativas con el centro de recepción de alarmas (ARC) (por ejemplo, instalador con supervisión de la venta al por mayor, supervisión de cuentas propias, proveedores del equipo, proveedores de servicios de telecomunicaciones, proveedores de servicios de vigilancia).

– Las **auditorías de cumplimiento** se deben llevar a cabo anualmente por parte de un organismo acreditado según la Norma EN ISO/IEC 17065 por cualquier signatario del Acuerdo Multilateral Europeo para la Acreditación (EA MLA) para la Norma EN 50518.

10.5 Dotación de personal

10.5.1 Generalidades

Debe haber un mínimo de dos operadores en el centro de recepción de alarmas (ARC) en todo momento, capaces de llevar a cabo todos los procedimientos de funcionamiento, a menos que el centro funcione en conjunto con otro centro de la misma categoría o de una superior y los métodos operativos aseguren el cumplimiento de los criterios de rendimiento que recoge el apartado 9.2.

10.5.2 Control de seguridad e investigación de antecedentes penales

Todos los empleados en puestos de trabajo relevantes deben someterse a un control de seguridad y a una investigación de antecedentes penales. Aparte de los visitantes, cualquier persona que acceda al centro de recepción de alarmas (ARC) debe pasar por un control de seguridad. Los visitantes deben estar acompañados por un empleado del centro de recepción de alarmas (ARC) en todo momento mientras estén dentro del mismo.

La verificación de seguridad debe comprender un período mínimo de cinco años hasta el comienzo del empleo pertinente en el centro de recepción de alarmas (ARC), o desde la fecha de finalización de los estudios a tiempo completo. Se debe llevar un registro de los progresos realizados para supervisar y registrar las medidas adoptadas y la información recibida durante el control de seguridad y la investigación de antecedentes penales. El control de seguridad se debe completar cuanto antes, al menos en un plazo de 12 semanas, salvo que un director/jefe del centro de recepción de alarmas (ARC) autorice una prórroga. En cualquier caso, el control no debe exceder las 16 semanas.

Si se contrata a un empleado antes de completar el control de seguridad o la investigación de antecedentes penales, se debe notificar a la persona interesada que la oferta de empleo está sujeta a un proceso satisfactorio de control de seguridad e investigación de antecedentes penales y que debería ser supervisado en todo momento mientras trabaje en el centro de recepción de alarmas (ARC).

Se debe contar con un procedimiento que describa cómo suspender los derechos de acceso.

10.5.3 Formación

La empresa se debe adherir a los procedimientos de formación para todos los empleados pertinentes, que deben abarcar las aptitudes teóricas y prácticas necesarias para cumplir con los requisitos de formación establecidos por la legislación o por el centro de recepción de alarmas (ARC).

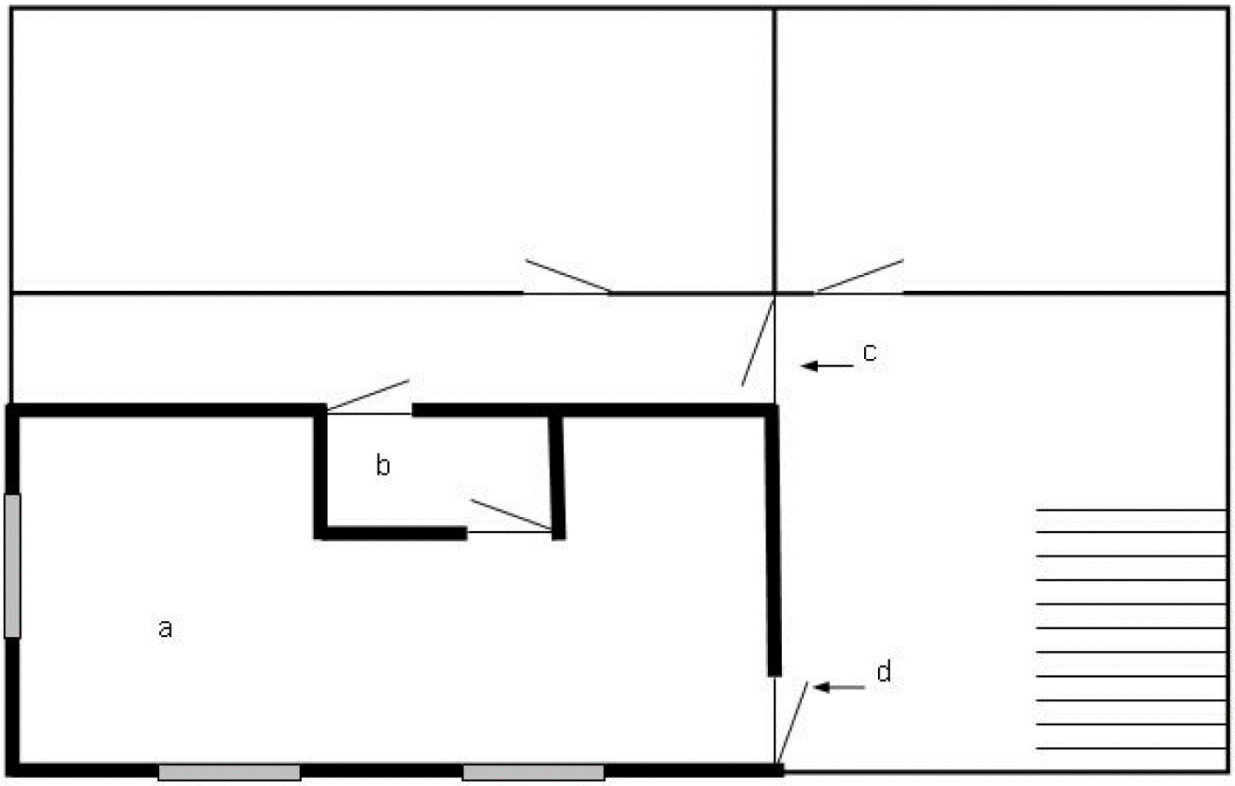
Debe establecerse un período de formación suficiente para garantizar que los empleados cuentan con las competencias mínimas para llevar a cabo las tareas específicas. Todos los operadores deben pasar por dicho período de formación antes de que se les permita gestionar las alarmas sin supervisión. Se debe proporcionar formación adicional acerca de temas específicos, como por ejemplo el nuevo equipo técnico o cambios en los procedimientos de funcionamiento.

La formación de los empleados se debe documentar y revisar cada año.

Anexo A (Informativo)

Disposición típica de un centro de recepción de alarmas (ARC) de categoría I

La figura A.1 muestra los elementos y la terminología utilizados en esta Norma Europea para describir un centro de recepción de alarmas (ARC). El diagrama que aparece a continuación no representa un dibujo de la construcción de un centro de recepción de alarmas (ARC).



Leyenda

a Centro de recepción de alarmas
b Vestíbulo de entrada
c Entrada a la parte del edificio
d Puerta de emergencia
Área acristalada en la estructura del centro de recepción de alarmas (ARC)
Muros de la estructura del centro de recepción de alarmas (ARC)

Figura A.1 – Disposición típica de un centro de recepción de alarmas (ARC) de categoría I

Anexo B (Informativo)

Consideraciones técnicas y de seguridad del acceso remoto a los datos del centro de recepción de alarmas (ARC)

B.1 Generalidades

Se recuerda a los operadores del centro de recepción de alarmas (ARC) de la existencia de otras normas relativas a la seguridad de los sistemas de gestión de la información, como por ejemplo la serie de Normas ISO/IEC 27000. De conformidad con lo dispuesto en el apartado 9.1.18, este anexo proporciona más información para facilitar el acceso a los datos del centro de recepción de alarmas (ARC).

B.2 Niveles de acceso

Aunque el acceso remoto a los datos del centro de recepción de alarmas (ARC) puede ser tan seguro como lo requiera el cliente, se deben emplear al menos dos niveles de seguridad.

a. Acceso remoto de nivel 1: el cliente debería conectarse al sistema operativo, que solo permite el acceso al programa de aplicación.

b. Acceso remoto de nivel 2: se requiere una clave de acceso diferente para acceder al nivel de aplicación.

Se puede conceder acceso al software de aplicación mediante un código de identificación de inicio de sesión junto con una clave de acceso de no menos de ocho caracteres. Tras 5 min de inactividad, se debería desconectar al cliente automáticamente del sistema y finalizar la conexión al nivel 1. Para volver a conectarse, se debería repetir todo el procedimiento de identificación.

B.3 Acceso al sistema

A fin de evitar el acceso no autorizado a los datos de las alarmas o que se produzca un impacto en el rendimiento de los sistemas utilizados para procesar los mensajes de alarma, los sistemas utilizados para facilitar el acceso remoto deberían estar separados física o lógicamente de los sistemas utilizados para procesar los mensajes de alarma.

Para evitar que se acceda al sistema de forma ilícita, el centro de recepción de alarmas (ARC) debería establecer procedimientos para desconectar al cliente durante al menos 1 h después de tres intentos fallidos de acceder al sistema.

B.4 Autorización para las instalaciones

B.4.1 Generalidades

Solo se debería permitir el acceso a los datos relativos a los contratos específicos de cada cliente con el centro de recepción de alarmas (ARC).

B.4.2 Modo lectura

Todos los datos relacionados con un contrato específico que esté cubierto por el uso de una contraseña determinada deberían estar disponibles para su visualización en modo lectura mediante acceso remoto, excepto en el caso de contraseñas, códigos de seguridad y números de teléfono de los servicios de emergencia.

B.4.3 Edición

El acceso a la función de edición solo debería estar disponible mediante una clave de acceso diferente a la del modo lectura, y el acceso debería suspenderse después de 5 min de inactividad. No se debería poder editar:

- el acuerdo de respuesta;
- el número de referencia único (URN) del servicio de emergencia pertinente;
- el historial de archivos;
- la suspensión del servicio.

B.4.4 Creación de un nuevo registro

La función para crear un nuevo registro debe ser distinta al modo de lectura o a la función de edición. La creación de un nuevo registro de clientes puede realizarse de manera remota, pero si se carga en línea, debe hacerse bajo el control del centro de recepción de alarmas (ARC).

B.4.5 Confirmación de los cambios realizados

Los operadores del centro de recepción de alarmas (ARC) deberían verificar en la medida de sus capacidades los cambios que se hayan editado. Para protegerse contra el riesgo de sufrir cambios no autorizados y mantener datos no válidos en el ordenador, se debería enviar una confirmación de los cambios a la persona/organización que tenga un contrato con el centro de recepción de alarmas (ARC). La confirmación se puede enviar en papel o por medios electrónicos (por ejemplo, por correo electrónico).

B.5 Ensayos de los sistemas

Las instalaciones empleadas para someter un sistema a ensayo no deberían estar disponibles en el nivel de acceso 1. Es importante que se haga una diferenciación entre ensayo y suspensión del servicio de supervisión. Por lo general, la suspensión del servicio recaería bajo la responsabilidad del centro de recepción de alarmas (ARC). Sólo se debería someter un sistema a ensayo de manera remota si se sabe que el sistema no está configurado.

Normalmente, los ensayos se realizan para diagnosticar fallos o como mantenimiento de rutina. Los ingenieros o clientes que quieran acceder al sistema deberían introducir tanto su código de acceso como el código de identificación del lugar. Los ensayos no deberían durar más de 4 h.

Los datos del centro de recepción de alarmas (ARC) deberían volver a su estado original tras 4 h. El cliente o el ingeniero que haya accedido al sistema tendría que conectarse de nuevo si se va a continuar con los ensayos.

B.6 Gestión de contraseñas

Se deben proporcionar medios para auditar, validar y/o eliminar nombres de usuario y contraseñas no utilizados, retirados o no autorizados.

Anexo C (Informativo)

Requisitos del sistema de gestión de alarmas

C.1 Estructura de un sistema de gestión de alarmas (AMS)

C.1.1 Generalidades

El sistema de gestión de alarmas (AMS) es un software que se ejecuta en uno o más ordenadores con almacenamiento físico de datos. Puede estar compuesto por uno o más módulos (componentes de software) (por ejemplo, módulos de interfaz para conectar transceptores del centro de recepción, módulos de comunicación, módulos de información, módulos de unión, etc.).

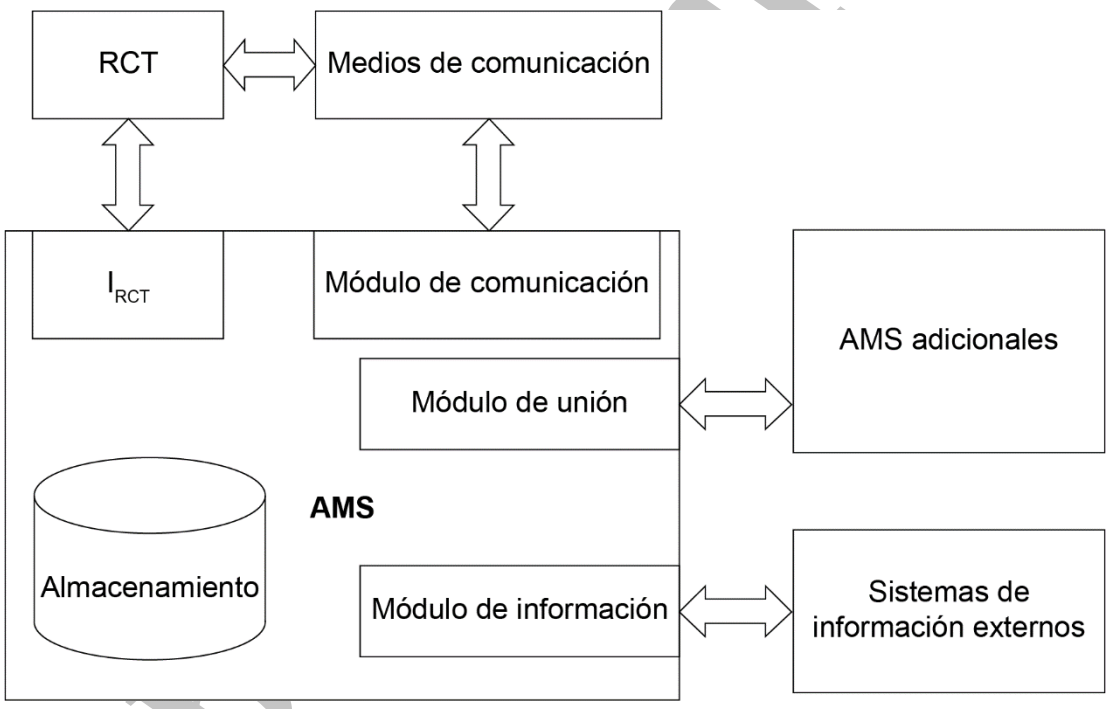


Figura C.1 – Sistema de gestión de alarmas (AMS)

Si el sistema de gestión de alarmas (AMS) incluye otras funciones distintas de las necesarias para recibir y presentar la información y los mensajes de alarma, estas no deberían influir en la recepción y presentación de la información y los mensajes de alarma.

Si el sistema de gestión de alarmas (AMS) se va a utilizar como parte de un sistema de alarma social, entonces debería cumplir con la Norma EN 50134-1.

NOTA Se ha hecho referencia a esta norma para incluir los requisitos específicos de los sistemas de alarma social que difieren de otros tipos de sistemas de alarma, principalmente debido a la necesidad de un sistema de comunicación oral bidireccional.

C.1.2 Interfaz para la interconexión con el transceptor del centro de recepción (I_{RCT})

Para establecer una comunicación con los transceptores de instalaciones vigiladas (SPT), los transceptores del centro de recepción (RCT) deberían cumplir con los requisitos de la Norma EN 50136-3.

Se pueden conectar varios transceptores del centro de recepción (RCT) de diferentes fabricantes a un sistema de gestión de alarmas (AMS) a través de un módulo de interfaz (I_{RCT}).

El sistema de gestión de alarmas (AMS) puede formar parte de un conjunto con uno o varios transceptores del centro de recepción (RCT) o funcionar como un dispositivo o sistema independiente. En cualquiera de los dos casos se deberían aplicar los requisitos de la presente norma.

C.1.3 Interconexión con otros sistemas de gestión de alarmas (AMS) (módulo de unión)

El módulo de unión de un sistema de gestión de alarmas (AMS) se utiliza para conectarlo con otros sistemas de gestión de alarmas (AMS) instalados en el mismo centro de recepción de alarmas (ARC) o en otros centros distintos. La(s) vía(s) de comunicación entre dos o más conjuntos de sistemas de gestión de alarmas (AMS) debe(n) tener al menos el mismo nivel de seguridad y rendimiento (véase 8.1) que el sistema de transmisión de alarma más exigente que esté conectado a cualquiera de los sistemas de gestión de alarmas (AMS).

C.1.4 Módulo de comunicación

Esta interfaz se utiliza para conectar dispositivos de comunicación externos (por ejemplo, correo electrónico, fax, impresoras, teléfonos, etc.). Se debería documentar y someter a ensayo la interoperabilidad del módulo de comunicación y de los dispositivos de comunicación.

C.1.5 Módulo de información

Este módulo se utiliza para conectarse con sistemas de información externos que proporcionan información para el proceso de gestión de alarmas, por ejemplo, información de tráfico o información meteorológica.

C.1.6 Interfaz de usuario

La interfaz para los operadores del centro de recepción de alarmas (ARC) debería ser parte del sistema de gestión de alarmas (AMS). También es posible conectar el sistema de gestión de alarmas (AMS) a través del módulo de unión a otro sistema con una interfaz de usuario para los operadores del centro de recepción de alarmas (ARC).

C.2 Fallos

C.2.1 Generalidades

El sistema de gestión de alarmas (AMS) debería supervisar su correcto funcionamiento, así como el funcionamiento de los componentes de hardware y software (por ejemplo, software de perro guardián).

C.2.2 Detección de fallos

Se deberían detectar los siguientes fallos:

- mal funcionamiento o fallo de partes del software de gestión de alarmas;
- introducción manual de datos no válidos;
- recepción de datos, que no pueden ser interpretados o procesados correctamente por el sistema de gestión de alarmas (AMS).

C.2.3 Prevención de fallos en la introducción manual de datos

Se debe evitar la introducción manual de datos incorrectos o no válidos mediante un examen sustantivo. Esto se aplica a los campos de entrada en los que la verificación sea lógicamente factible.

C.2.4 Presentación de la información de fallos

Se debería presentar la información relativa a los fallos en un plazo de 10 s a partir de la aparición de los mismos, a menos que se especifique lo contrario.

C.3 Mensaje

C.3.1 Acuse de recibo del mensaje

El sistema de gestión de alarmas (AMS) debería acusar recibo de todos los mensajes una vez que estos se hayan protegido (por ejemplo, en una cola de mensajes protegida o en el registro). Los mensajes deberían protegerse antes de poder ser procesados. El fabricante debería especificar en su documentación el tiempo relativo al acuse de recibo del mensaje.

C.3.2 Mensajes de alarma

Cuando no se estén procesando otros mensajes de alarma, se deberían presentar los nuevos mensajes de alarma en un plazo de 5 s tras su acuse de recibo para esperar la aceptación del mensaje. Se debería emitir una indicación de alerta al operador del centro de recepción de alarmas (ARC) (por ejemplo, acústica y/o visual) al mismo tiempo que la presentación.

NOTA Si una indicación de alerta está activa, puede reiniciarse por cada nuevo mensaje confirmado que se presente.

C.3.3 Mensajes de fallos

Se deberían seguir las indicaciones del apartado C.3.2 relativo a los mensajes de alarma para procesar los mensajes de aviso de fallos.

C.3.4 Mensajes previstos

No es necesario presentar los mensajes previstos que haya recibido el sistema de gestión de alarmas (AMS) dentro de los plazos acordados previamente, siempre que tras el acuse de recibo el sistema de gestión de alarmas (AMS) lleve a cabo el procesamiento de forma automática.

Si el sistema de gestión de alarmas (AMS) no recibe ni acusa recibo de los mensajes previstos dentro de los plazos acordados previamente, el sistema debería generar un mensaje y procesarlo de acuerdo con el apartado C.3.2.

El sistema de gestión de alarmas (AMS) debería permitir que se presenten los mensajes previstos a petición.

C.3.5 Otros mensajes recibidos

Si el sistema de gestión de alarmas (AMS) es capaz de recibir mensajes distintos de los descritos en los apartados C.3.2, C.3.3 y C.3.4, se deberían procesar y presentar a petición.

C.3.6 Cola de mensajes

El sistema de gestión de alarmas (AMS) debería incluir una cola de mensajes.

Los mensajes deberían recuperarse de la cola de mensajes por orden de llegada, excepto cuando el sistema de gestión de alarmas (AMS) incluya medios para priorizar las entradas. Cuando se incluyan medios para priorizar las entradas, los mensajes deberían recuperarse según lo dispuesto en el apartado C.3.7.

Se debería emitir una notificación cuando haya uno o más mensajes en la cola de mensajes. El sistema de gestión de alarmas (AMS) debería indicar la existencia de múltiples mensajes en la cola de mensajes en un plazo de 5 s tras acusar recibo. Esta notificación no debería interferir con la presentación de los mensajes que se estén gestionando en ese momento o que se encuentren en la cola de mensajes en espera de aceptación.

La notificación del cambio de estado de la cola de mensajes, que resulta de la presentación y la posterior aceptación de un mensaje, debería realizarse en un plazo de 5 s a partir de la aceptación del mensaje.

El sistema de gestión de alarmas (AMS) debería tener la posibilidad de presentar, bajo demanda, los mensajes procedentes de un único sistema de alarma. Los mensajes provenientes de un único sistema de alarma deberían presentarse por orden de llegada.

El fabricante debería especificar en su documentación la capacidad de la cola de mensajes.

Se debería emitir una alerta cuando la cola de mensajes alcance el 90% de su capacidad.

Si la cola de mensajes está llena, el sistema de gestión de alarmas (AMS) ya no debería acusar recibo de los mensajes entrantes.

C.3.7 Prioridades de entrada

Si el sistema de gestión de alarmas (AMS) incluye una función para establecer prioridades de entrada, los mensajes deberían recuperarse de acuerdo con los niveles de prioridad. El fabricante debería especificar en su documentación el método que se debe emplear para definir las prioridades de entrada (por ejemplo, tipo de alarmas, grado, etc.).

Si hay varios mensajes con la misma prioridad en la cola, se deberían recuperar por orden de llegada.

C.3.8 Indicación de alerta

Se debería proporcionar una indicación de alerta dentro del sistema de gestión de alarmas (AMS) que se active cuando se presenten los mensajes. La indicación de alerta debería activarse en un plazo de 5 s tras el acuse de recibo de un mensaje o la generación de información local.

Por lo general, la indicación de alerta debería suspenderse cuando se acepte el mensaje.

También debería proporcionarse un medio para suspender la indicación de alerta que resulte del acuse de recibo de mensajes que no sean de alarma o de la generación de información local. Este medio debería limitarse al nivel de acceso 2.

Se puede proporcionar un medio para habilitar y deshabilitar la activación de la indicación de alerta cuando se reciban los mensajes. Esta función debería desactivarse automáticamente cuando la cola no contenga mensajes de alarma. El acceso a esta función debería limitarse al nivel de acceso 3.

C.3.9 Aceptación del mensaje

Debería proporcionarse un medio que permita la aceptación del mensaje. La aceptación de un mensaje (que se presenta) debería suspender la indicación de alerta. La aceptación de mensajes debería eliminar el mensaje aceptado de la cola de mensajes y permitir la presentación del siguiente mensaje en la cola de mensajes (si lo hay).

Se debería proporcionar un medio para medir el período de tiempo que transcurre entre el acuse de recibo del mensaje y su aceptación.

Una vez superado dicho período se debería generar una indicación de alerta.

Si el sistema de gestión de alarmas (AMS) incluye un mecanismo para establecer prioridades de entrada, se debería contar con un medio para supervisar el período de tiempo transcurrido entre el acuse de recibo del mensaje y la aceptación del mismo para cada prioridad de entrada. Si se puede seleccionar el medio para establecer el período de tiempo permitido entre el acuse de recibo del mensaje y la aceptación del mismo, se debería limitar al nivel de acceso 3.

C.4 Información a presentar

C.4.1 Información a presentar en relación con los mensajes

El sistema de gestión de alarmas (AMS) debería presentar la información relacionada con los mensajes recibidos necesaria para iniciar una acción apropiada por parte del operador del centro de recepción de alarmas (ARC). La información debería presentarse antes de la aceptación del mensaje y debe estar disponible a petición.

El sistema de gestión de alarmas (AMS) debería ser capaz de proporcionar la siguiente información:

- la identidad del sistema de alarma de origen; al menos la dirección de los locales protegidos;
- el tipo de mensaje (por ejemplo, incendio, intrusión);
- el contenido del mensaje tal y como se especifica en la documentación del fabricante (por ejemplo, alarma, fallo, fecha y hora de activación y desactivación);

- la fecha y la hora en que el mensaje fue recibido por el sistema de gestión de alarmas (AMS) (redondeadas al segundo más cercano);
- la fecha y la hora en que el mensaje fue enviado por el transceptor de las instalaciones protegidas (SPT) (en segundos);
- el nivel de prioridad de los mensajes, si procede, de acuerdo con el apartado C.3.7.

NOTA 1 El tipo de mensaje se puede incluir en el contenido del mensaje.

NOTA 2 Se puede presentar otra información siempre y cuando no se altere la presentación de la información relativa a los mensajes o a la información sobre fallos.

El cliente y el centro de recepción de alarmas (ARC) deberían acordar el contenido y la estructura de la información presentada.

C.4.2 Información a presentar en relación con la información de fallos recibida de los sistemas de alarma

Se debe presentar la siguiente información mínima en un mensaje de información de fallos:

- la identidad del sistema de alarma de origen; al menos la dirección de los locales protegidos;
- el tipo de fallo (por ejemplo, un fallo en la alimentación eléctrica);
- la incidencia del fallo (por ejemplo, la fuente de alimentación principal);
- la fecha y hora de la incidencia del fallo de origen.

C.4.3 Fallo de los medios de presentación de la información

En caso de que se produzca un fallo total de los medios de presentación de la información, el sistema de gestión de alarmas (AMS) debería dejar de acusar recibo de los mensajes entrantes. Se debería generar una condición de fallo y activar una indicación de alerta.

C.5 Registro

C.5.1 Generalidades

El flujo de información del sistema de gestión de alarmas (AMS) incluye la creación y mantenimiento de datos maestros, la gestión de eventos y la transmisión de alarmas a otros sistemas de gestión de alarmas (AMS) a través del módulo de unión, si está disponible.

Se puede elegir entre un procesamiento automático por parte del sistema de gestión de alarmas (AMS) y un procesamiento por parte del operador. También se puede pasar de un procesamiento automático a uno manual y viceversa. No se debería perder o corromper la información al procesar las incidencias.

Para lograr una visión unificada del flujo de información, el sistema de gestión de alarmas (AMS) debería ser capaz de generar registros fijos normalizados. Los registros se deben dividir en registro de datos maestros (registro M), registros de datos de incidencias (registro E) y, si están disponibles, registros del módulo de unión (registros J).

Los datos registrados se deberían proteger contra el borrado accidental o intencional y contra la sobrescritura. Los datos históricos deberían estar disponibles a petición.

Los datos a partir de los cuales se generan los registros deberían modificarse utilizando únicamente las funciones que proporciona el sistema de gestión de alarmas (AMS). Se deberían poder rastrear las modificaciones ulteriores que se hagan a dichos datos.

NOTA Cambiar los datos incluye añadir, modificar o eliminar información.

C.5.2 Marcas de tiempo para el registro

El sistema de gestión de alarmas (AMS) debería generar la marca de tiempo requerida (redondeada al segundo más cercano) y estar preparado para cualquier evaluación.

La marca de tiempo de las entradas del registro debería reflejar la fecha en que se ha completado cada una de las operaciones registradas. Las marcas de tiempo deberían ajustarse al Tiempo Universal Coordinado (UTC) con una precisión de resolución de al menos un segundo.

Un sistema de gestión de alarmas (AMS) que incluya una interfaz del transceptor del centro de recepción (I_{RCT}) debería registrar la marca de tiempo del transceptor (T_{RCT}) y el tiempo de reacción ($T_{Reacción}$) y estar preparado para cualquier evaluación.

Para las incidencias que no se hayan desencadenado por una entrada de mensaje en la interfaz del transceptor del centro de recepción (I_{RCT}), se debe tratar el momento de generación del incidente como T_{RCT}. En este caso, la fecha de inicio del procesamiento por parte del sistema de gestión de alarmas (AMS) o del trabajo por parte del operador del centro de recepción de alarmas (ARC) se debe tratar como $T_{Reacción}$.

C.5.3 Registro de datos maestros (registro M1)

El registro M1 debe incluir los datos intercambiados con los subsistemas, objetos y procesos. Se deberían registrar todas las entradas y cambios de tal forma que se pueda ver el tiempo y la entidad del cambio (operador o automático). El estado de los datos maestros debería reconstruirse por cada momento dado dentro del período preservado.

C.5.4 Registros de incidencias

C.5.4.1 Registro de incidencias E1

Los registros de incidencias deberían utilizarse para el registro de los datos entrantes a través de la interfaz para I_{RCT}. También pueden utilizarse para datos provenientes de otras interfaces y módulos.

En el caso del registro E1, los datos en bruto entrantes se registran con el número de registro E1-ID y con la marca de tiempo del sistema de gestión de alarmas (AMS). La marca de tiempo se corresponde con T_{RCT}.

C.5.4.2 Registro de incidencias E2

El registro de incidencias E2 representa los datos en bruto en el formato específico del sistema de gestión de alarmas (AMS) con el número de registro E2-ID, incluida la relación con el número o números de registro E1-ID y la marca de tiempo del sistema de gestión de alarmas (AMS) ($T_{\text{Registro E2}}$).

Se pueden resumir varios registros E1 en un solo registro E2 o generar varios registros E2 a partir de un registro E1.

C.5.4.3 Registro de eventos E3

El registro de eventos E3 es el resultado de la fusión del registro E2, incluyendo los identificadores únicos de objetos y los identificadores de las incidencias asociadas de los datos maestros o la función de identificación de la incidencia interna. El registro también incluye el número de registro E3-ID y la marca de tiempo del sistema de gestión de alarmas (AMS) ($T_{\text{Registro E3}}$).

Se pueden resumir varios registros E2 en un único registro E3 o generar varios registros E3 a partir de un registro E2.

Se debe incluir en el registro E3 toda la información del registro E2 aunque no se pueda hacer referencia a un objeto o a un objeto-incidencia, ya sea por falta de datos maestros o porque estos sean incorrectos.

Dicho registro de incidencias también debería incluir las incidencias internas que provengan del sistema de gestión de alarmas (AMS) (por ejemplo, una incidencia debida a la falta de mensajes de rutina) o incidentes generados por el operador del centro de recepción de alarmas (ARC).

C.5.4.4 Registro de eventos E4

El registro de eventos E4 representa el resultado de la acción y reacción del sistema de gestión de alarmas (AMS) y/o el operador del centro de recepción de alarmas (ARC) como parte del tratamiento de la información del registro E3. El registro también incluye el número de registro E4-ID y la marca de tiempo del sistema de gestión de alarmas (AMS) ($T_{\text{Registro E4}}$).

Se pueden resumir varios registros E3 en un único registro E4 o generar varios registros E4 a partir de un registro E3.

C.5.4.5 Fallo del registro

En caso de que se produzca un fallo en el registro, se debería generar una indicación de alerta en un plazo de 5 s tras la presentación de la información por parte del transceptor del centro de recepción al sistema de gestión de alarmas (AMS), en la que se avise de que no se ha podido registrar un mensaje por un fallo del registro.

C.5.5 Niveles de acceso

El sistema de gestión de alarmas (AMS) debería estar dotado de medios para restringir el acceso a sus funciones.

El fabricante debería especificar los medios proporcionados para restringir el acceso y especificar las funciones a las que se puede acceder en cada nivel de acceso (por ejemplo, llaves físicas o contraseñas lógicas).

El acceso a las funciones del sistema de gestión de alarmas (AMS) debería dividirse en un mínimo de cuatro niveles, como se especifica a continuación:

- nivel de acceso 1: no se requiere autorización;
- nivel de acceso 2: se permite el funcionamiento del sistema de gestión de alarmas (AMS) (por ejemplo, la aceptación de mensajes);
- nivel de acceso 3: se habilita el acceso para la configuración o la modificación de la configuración del sistema de gestión de alarmas (AMS) (por ejemplo, desactivando la indicación de alerta o estableciendo prioridades de entrada);
- nivel de acceso 4: se permite el acceso y modificación del hardware o software del sistema de gestión de alarmas (AMS) (por ejemplo, modificaciones realizadas por el fabricante).

Se debería impedir el acceso al nivel 4 hasta que se haya permitido el acceso al nivel 3. Cada nivel de acceso puede dividirse en varios subniveles; cualquiera de esos subniveles de acceso debería estar descrito en la documentación del fabricante.

El funcionamiento del sistema de gestión de alarmas (AMS) debería requerir que cada usuario se conecte al nivel de acceso apropiado y se desconecte cuando termine la operación.

Se debería registrar la conexión y desconexión de los usuarios y los cambios que se hayan hecho a las contraseñas (si procede).

Se debería proporcionar un medio para identificar a los usuarios y sus correspondientes niveles de acceso en el nivel de acceso 3.

También se deberían proporcionar herramientas para editar a los usuarios y sus niveles de acceso y modificar las contraseñas.

La modificación de las contraseñas debería limitarse a los usuarios de esas contraseñas o al nivel de acceso 4.

C.5.6 Acceso a la base de datos

Se debería poder modificar la base de datos tanto a nivel local como de manera remota en el nivel de acceso 3. Los transceptores del centro de recepción (RCT) utilizados para la comunicación con los transceptores de instalaciones vigiladas (SPT) no deberían utilizarse para el acceso remoto a la base de datos.

C.5.7 Acceso al sistema de gestión de alarmas

El acceso a las funciones de aceptación de mensajes y presentación de información se debería limitar al nivel de acceso 2.

C.5.8 Acceso a los datos de configuración del sistema de gestión de alarmas

Si el sistema de gestión de alarmas (AMS) incluye datos de configuración, el acceso a los datos se debería autorizar a través de los niveles de acceso apropiados.

Se deberían proporcionar herramientas para ver y modificar los datos de configuración del sistema.

La visualización de los datos de configuración debería requerir el acceso al nivel 2.

La modificación de los datos de configuración debería requerir el acceso al nivel 3.

Se debería registrar cualquier modificación que se haga en la configuración (por ejemplo, introducir o cambiar contraseñas).

C.5.9 Acceso a los datos del registro

Se debería proporcionar un medio para acceder a los datos del registro. Solo se debe poder acceder a los datos del registro, con el fin de hacer una copia de seguridad de los datos para su almacenamiento a largo plazo, en el nivel de acceso 3.

C.6 Vigilancia de la interconexión con el transceptor del centro de recepción

El sistema de gestión de alarmas (AMS) debería supervisar la interconexión con los transceptores del centro de recepción. Los medios de supervisión proporcionados y el tipo de fallo que se quiera detectar deberían estar descritos en la documentación del fabricante (por ejemplo, cortocircuito o circuito abierto, interrupción de la comunicación, etc.). Como mínimo, se debería reconocer y detectar la interrupción física de la interconexión.

Si se produce un fallo de interconexión, se debe generar y presentar la información relativa a dicho fallo en un plazo de 10 s. La indicación de alerta debería funcionar en un plazo de 10 s.

No se debe acusar recibo de los mensajes cuando se produzca un fallo en la interconexión entre el sistema de gestión de alarmas (AMS) y el transceptor del centro receptor (RCT).

Bibliografía

[1] CEN/TR 14383-8, *Prevention of crime. Urban planning and building design. Part 8: Protection of buildings and sites against criminal attacks with vehicles.*

[2] EN 81-28, *Safety rules for the construction and installation of lifts. Lifts for the transport of persons and goods. Part 28: Remote alarm on passenger and goods passenger lifts.*

[3] EN 1154, *Building hardware. Controlled door closing devices. Requirements and test methods.*

[4] EN 50131 (todas las partes), *Alarm systems. Intrusion and hold-up systems.*

[5] EN 50132 (todas las partes), *Alarm systems. CCTV surveillance systems for use in security applications.*

[6] EN 50133 (todas las partes), *Alarm systems. Access control systems for use in security applications.*

[7] EN 50134 (todas las partes), *Alarm systems. Social alarm systems.*

[8] EN 50136 (todas las partes), *Alarm systems. Alarm transmission systems and equipment.*

[9] EN 61000-4-2, *Electromagnetic compatibility (EMC). Part 4-2: Testing and measurement techniques. Electrostatic discharge immunity test.*

[10] ISO/IEC 27000 series, *Information technology. Security techniques.*

[11] ISO/IEC 27001, *Information technology. Security techniques. Information security management systems. Requirements.*

[12] EN ISO 9001, *Quality management systems. Requirements (ISO 9001).*

[13] ISO-EN 11064 (todas las partes), *Ergonomic design of control centres.*

[14] Directive 95/46/EC, The protection on individuals with regard to the processing of personal data and on the free movement of such data.

[15] EN 15602, *Security service providers. Terminology.*

[16] CLC/TS 50131-7:2010, *Alarm systems. Intrusion and hold-up systems. Part 7: Application guidelines.*

[17] ISO 31000 (series), *Risk management.*

[18] EN-IEC 62820 (todas las partes), *Alarm systems. Building intercom systems.*

[19] EN ISO/IEC 17065, *Conformity assessment. Requirements for bodies certifying products, processes and services (ISO/IEC 17065).*

Para información relacionada con el desarrollo de las normas contacte con:

Asociación Española de Normalización
Génova, 6
28004 MADRID-España
Tel.: 915 294 900
info@une.org
www.une.org

Para información relacionada con la venta y distribución de las normas contacte con:

AENOR INTERNACIONAL S.A.U.
Tel.: 914 326 000
normas@aenor.com
www.aenor.com

UNE NormalizaciónEspañola organismo de normalización español en: