ANEXO I

Relación de Normas UNE o UNE-EN que resultan de aplicación en los sistemas de alarma

Tipo	Número	Año	Denominación
UNE-EN.	50130-4/A1.	1998	Sistemas de alarma. Parte 4: Compatibilidad electromagnética Norma de familia de producto: Requisitos de inmunidad para componentes de sistemas de detección de incendios, intrusión y alarma social.
UNE-EN.	50130-4.	1997	Sistemas de alarma. Parte 4: Compatibilidad electromagnética. Norma de familia de producto: Requisitos de inmunidad para componentes de sistemas de detección de incendios, intrusión y alarma social.
UNE-EN.	50130-4.	1997/A2 2005	Sistemas de alarma. Parte 4: Compatibilidad electromagnética. Norma de familia de producto: Requisitos de inmunidad para componentes de sistemas de detección de incendios, intrusión y alarma social.
UNE-EN.	50130-5.	2000	Sistemas de alarma. Parte 5: Métodos de ensayo ambiental.
UNE-EN.	50131-1.	2008	Sistemas de alarma. Sistemas de alarma contra intrusión y atraco. Parte 1: Requisitos del sistema
UNE-EN.	50131-1.	2008/A1:2010	Sistemas de alarma. Sistemas de alarma contra intrusión y atraco. Parte 1: Requisitos del sistema.
UNE-EN.	50131-2-2.	2008	Sistemas de alarma. Sistemas de alarma de intrusión y atraco. Parte 2-2: Detectores de intrusión. Detectores de infrarrojos pasivos.
UNE-EN.	50131-2-3.	2009	Sistemas de alarma. Sistemas de alarma de intrusión y atraco. Parte 2-3: Requisitos para detectores de microondas.
UNE-EN.	50131-2-4.	2008	Sistemas de alarma. Sistemas de alarma de intrusión y atraco. Parte 2-4: Requisitos para detectores combinados de infrarrojos pasivos y microondas.
UNE-EN.	50131-2-5.	2009	Sistemas de alarma. Sistemas de alarma de intrusión y atraco. Parte 2-5: Requisitos para detectores combinados de infrarrojos pasivos y ultrasónicos.
UNE-EN.	50131-2-6.	2009	Sistemas de alarma. Sistemas de alarma de intrusión y atraco. Parte 2-6: Contactos de apertura (magnéticos).
UNE-EN.	50131-3.	2010	Sistemas de alarma. Sistemas de alarma de intrusión y atraco. Parte 3: Equipo de control y señalización.
UNE-EN.	50131-4.	2010	Sistemas de alarma. Sistemas de alarma de intrusión y atraco. Parte 4: Dispositivos de advertencia.
UNE-EN.	50131-5-3.	2005	Sistemas de alarma. Sistemas de alarma de intrusión. Parte 5-3: Requisitos para los equipos de interconexión que usan técnicas de radiofrecuencia.
UNE-EN.	50131-5-3.	2005/A1:2008	Sistemas de alarma. Sistemas de alarma de intrusión. Parte 5-3: Requisitos para los equipos de interconexión que usan técnicas de radiofrecuencia.
UNE-EN.	50131-6.	1999	Sistemas de alarma. Sistemas de alarma de intrusión. Parte 6: Fuentes de alimentación.
UNE-EN.	50131-6.	2008	Sistemas de alarma. Sistemas de alarma de intrusión y atraco. Parte 6: Fuentes de alimentación.
UNE-EN.	50131-8.	2009	Sistemas de alarma. Sistemas de alarma de intrusión y atraco. Parte 8: Sistemas/dispositivos de niebla de seguridad.
UNE-CLC/TS.	50131-2-2.	2005 V2	Sistemas de alarma. Sistemas de alarma de intrusión. Parte 2-2: Requisitos para los detectores de infrarrojos pasivos.
UNE-CLC/TS.	50131-2-3.	2005 V2	Sistemas de alarma. Sistemas de alarma de intrusión. Parte 2-3: Requisitos para detectores de microondas.
UNE-CLC/TS.	50131-2-4.	2005 V2	Sistemas de alarma. Sistemas de alarma de intrusión. Parte 2-4: Requisitos para los detectores combinados de infrarrojos pasivos y de microondas.
UNE-CLC/TS.	50131-2-5.	2005 V2	Sistemas de alarma. Sistemas de alarma de intrusión. Parte 2-5: Requisitos para los detectores combinados de infrarrojos pasivos y ultrasónicos.
UNE-CLC/TS.	50131-2-6.	2005 V2	Sistemas de alarma. Sistemas de alarma de intrusión. Parte 2-6: Requisitos para contactos de apertura (magnéticos).
UNE-CLC/TS.	50131-3.	2005 V2	Sistemas de alarma. Sistemas de alarma de intrusión. Parte 3: Equipo de control y señalización.

cve: BOE-A-2011-3170

Tipo	Número	Año	Denominación
UNE-CLC/TS.	50131-7.	2005 V2	Sistemas de alarma. Sistemas de alarma de intrusión. Parte 7. Guía de aplicación
UNE-EN.	50132-1.	2010	Sistemas de alarma. Sistemas de vigilancia CCTV para uso en aplicaciones de seguridad. Parte 1: Requisitos del sistema.
UNE-EN.	50132-2-1.	1998	Sistemas de alarma. Sistemas de vigilancia CCTV para uso en aplicaciones de seguridad. Parte 2-1: Cámaras en blanco y negro.
UNE-EN.	50132-4-1.	2002	Sistemas de alarma. Sistemas de vigilancia CCTV para uso en aplicaciones de seguridad. Parte 4-1: Monitores en blanco y negro.
UNE-EN.	50132-5.	2002	Sistemas de alarma. Sistemas de vigilancia CCTV para uso en aplicaciones de seguridad. Parte 5: Transmisión de vídeo.
UNE-EN.	50132-7 CORR.	2004	Sistemas de alarma - Sistemas de vigilancia CCTV para uso en aplicaciones de seguridad. Parte 7: Guía de aplicación.
UNE-EN.	50132-7.	1997	Sistemas de alarma. Sistemas de vigilancia CCTV para uso en aplicaciones de seguridad. Parte 7: Guía de aplicación.
UNE-EN.	50133-1 CORR.	1998	Sistemas de alarma. Sistemas de control de accesos de uso en las aplicaciones de seguridad. Parte 1: Requisitos de los sistemas.
UNE-EN.	50133-1/A1.	2004	Sistemas de alarma. Sistemas de control de accesos de uso en las aplicaciones de seguridad. Parte 1: Requisitos de los sistemas.
UNE-EN.	50133-1.	1998	Sistemas de alarma. Sistemas de control de accesos de uso en las aplicaciones de seguridad. Parte 1: Requisitos de los sistemas.
UNE-EN.	50133-2-1.	2001	Sistemas de alarma. Sistemas de control de accesos de uso en las aplicaciones de seguridad. Parte 2-1: Requisitos generales de los componentes.
UNE-EN.	50133-7.	2000	Sistemas de alarma. Sistemas de control de accesos de uso en las aplicaciones de seguridad. Parte 7: Guía de aplicación.
UNE-CLC/TS.	50134-7.	2005	Sistemas de alarma. Sistemas de alarma social. Parte 7: Guía de aplicación.
UNE-EN.	50134-1.	2003	Sistemas de alarma. Sistemas de alarma social. Parte 1: Requisitos del sistema.
UNE-EN.	50134-2.	2000	Sistemas de alarma. Sistemas de alarma social. Parte 2: Dispositivos de activación.
UNE-EN.	50134-3.	2002	Sistemas de alarma. Sistemas de alarma social. Parte 3: Unidad local y controlador.
UNE-EN.	50134-5.	2005	Sistemas de alarma. Sistemas de alarma social. Parte 5: Interconexiones y comunicaciones.
UNE-EN.	50136-1-1/A1.	2002	Sistemas de alarma. Sistemas y equipos de transmisión de alarma. Parte 1-1: Requisitos generales para sistemas de transmisión de alarma.
UNE-EN.	50136-1-1.	1999	Sistemas de alarma. Sistemas y equipos de transmisión de alarma. Parte 1-1: Requisitos generales para sistemas de transmisión de alarma.
UNE-EN.	50136-1-1.	1999/A2:2009	Sistemas de alarma. Sistemas y equipos de transmisión de alarma. Parte 1-1: Requisitos generales para sistemas de transmisión de alarma.
UNE-EN.	50136-1-2.	2000	Sistemas de alarma. Sistemas y equipos de transmisión de alarma. Parte 1-2: Requisitos para los sistemas que hacen uso de vías de alarma dedicadas.
UNE-EN.	50136-1-3.	1998	Sistemas de alarma. Sistemas y equipos de transmisión de alarma. Parte 1-3: Requisitos para sistemas con transmisores digitales que hacen uso de la red telefónica pública autoconmutada.
UNE-EN.	50136-1-4.	1998	Sistemas de alarma. Sistemas y equipos de transmisión de alarma. Parte 1-4: Requisitos para los sistemas con trasmisores de voz que hacen uso de la red telefónica pública conmutada.
UNE-EN.	50136-1-5.	2009	Sistemas de alarma. Sistemas y equipos de transmisión de alarmas. Parte 1-5: Requisitos para la red de conmutación de paquetes.
UNE-EN.	50136-2-1/A1.	2002	Sistemas de alarma. Sistemas y equipos de transmisión de alarma. Parte 2-1: Requisitos generales para los equipos de transmisión de alarma.
UNE-EN.	50136-2-1.	1998	Sistemas de alarma. Sistemas y equipos de transmisión de alarma. Parte 2-1: Requisitos generales para los equipos de transmisión de alarma.
UNE-EN.	50136-2-2.	1998	Sistemas de alarma. Sistemas y equipos de transmisión de alarma. Parte 2-2: Requisitos generales para los equipos usados en sistemas que hacen uso de vías dedicadas de alarma.

cve: BOE-A-2011-3170

Tipo	Número	Año	Denominación
UNE-EN.	50136-2-3.	1998	Sistemas de alarma. Sistemas y equipos de transmisión de alarma. Parte 2-3: Requisitos para los equipos usados en sistemas con transmisores digitales que hacen uso de la red telefónica pública conmutada.
UNE-EN.	50136-2-4.	1998	Sistemas de alarma. Sistemas y equipos de transmisión de alarma. Parte 2-4: Requisitos para los equipos usados en sistemas con transmisores de voz que hacen uso de la red telefónica pública conmutada.
UNE-CLC/TS.	50136-4.	2005 V2	Sistemas de alarma. Sistemas y equipos de transmisión de alarma. Parte 4: Equipos anunciadores usados en centrales receptoras de alarma.
UNE-CLC/TS.	50136-7.	2005 V2	Sistemas de alarma. Sistemas y equipos de transmisión de alarma. Parte 7: Guía de aplicación.
UNE CLC/TS.	50398.	2005 V2	Sistemas de alarma. Sistemas de alarma combinados e integrados.

ANEXO II

Mantenimiento presencial anual de sistemas electrónicos de seguridad

Equipos	Acciones	Periodicidad (*)
Objetivo	Efectuar un completo test del estado y de la funcionalidad de un sistema. Se deberá preparar por parte de la empresa mantenedora un impreso estándar en la que reflejar, además del tipo de CIE (marca, modelo, etc.) y del resto de elementos utilizados, los resultados de las pruebas efectuadas con el fin de evitar el posible olvido de alguna de ellas. Sirva esta guía para su confección. Una copia de ese impreso deberá ser entregada al usuario, debidamente firmada por el técnico, al finalizar las pruebas.	Anual
Situación de pruebas	Antes de iniciar el proceso de mantenimiento de un sistema, el técnico, identificándose debidamente, informará a la CRA, que situará el sistema en estado de pruebas, registrando las señales recibidas de forma automática, pero sin cursar su trámite. Deberá obtenerse inicialmente el registro de incidencias del sistema de modo que, si su capacidad lo permite, reproduzca los últimos 15 días. Al final del test se obtendrá otro registro de incidencias del periodo de pruebas para comprobar que todas han sido llevadas a cabo correctamente. Igualmente, al final del test se comprobará con la CRA si todas las señales de alarma generadas han alcanzado su destino.	Anual
Alimentación del sistema	Las comprobaciones han de efectuarse sobre la fuente de alimentación (PS) de la propia CIE y también sobre otras posibles fuentes de alimentación auxiliares que el sistema emplee de forma tanto centralizada como distribuida, siendo necesario abrir las cajas de los equipos implicados. Verificar: Posibles anomalías de alimentación mediante el registro de incidencias de la CIE. Suministro de c.a. Toma de tierra. Tensión de la c.c. de las salidas auxiliares: Aprox. 13,8 V +/- 5%. Id. retirando la c.a. (sólo batería): Aprox. 12 V +/- 5%. Tensión de carga de la batería: Aprox. 13,8 V +/- 5%. Antigüedad de la batería (sustituir si más de 6 años). Provocar un fallo red de c.a. y, tras reponerla al cabo de aprox. 1 min., Provocar también un fallo de batería de la misma duración y reponerla igualmente. Comprobar su señalización local en el(los) teclado(s) y las transmisiones de alarma y reposiciones a la CRA (cotejar con CRA al final del test y/o observar el registro final de incidencias). Nota: La notificación del fallo de red de c.a. puede tener asignado un retardo y no aparecer en ese tiempo. Comprobarlo consultando la programación de la central (CIE).	Anual

cve: BOE-A-2011-3170

Equipos	Acciones	Periodicidad (*)
CIE o Central	Igualmente, con la caja abierta, comprobar: Estado y funcionamiento del tamper (grados 2 y 3) y del posible antidespegue (grado 3). Elementos de cierre de la caja del equipo (tornillos, bisagras, cerradura, etc.). Aspecto general del interior (conexiones de clemas, timbrado de cables, etc.).	Anual
ACE(s) o teclado(s)	Investigación de posibles problemas de funcionamiento (preguntando a los usuarios). Comprobar el display, las teclas, los indicadores luminosos y el zumbador. Ver el estado del tamper (grados 2 y 3) y el antidespegue.(grado 3)	
Detectores y actuadores manuales	Comprobar la cobertura de detectores y el funcionamiento de los elementos que exigen una activación manual. Comprobar que los posibles cambios en la distribución del mobiliario, objetos almacenados, carteles colgantes, etc. no afecten a la cobertura de los detectores de movimiento. Situar el sistema en el modo «test de andado» (walk test). Comprobar, mediante el zumbador del teclado y la posible ayuda de un colaborador, si el entorno vigilado es de grandes dimensiones, la correcta activación de todos y cada uno de los elementos existentes que puedan examinarse mediante este medio (volumétricos, contactos magnéticos, pulsadores de atraco, etc.). Comprobar el resto de elementos mediante el procedimiento más adecuado: Sísmicos: Herramienta específica del Sistema o percusión. Vibración: Percusión. Rotura de cristal: Herramienta específica de test.–Etc. Situando el sistema en estado normal (desarmado), comprobar aleatoriamente la activación del tamper de algunos detectores (grados 2 y 3) y la transmisión de esta incidencia a la CRA. Enmascarar los detectores volumétricos de este tipo (grado 3) y comprobar su reacción y la transmisión de esta incidencia a la CRA. Verificar la activación de los elementos comprobados mediante el registro de incidencias del sistema.	Anual
Operativa habitual	Armar el sistema (debería llevarlo a cabo uno de los usuarios habituales con su código). Si éste está distribuido en particiones, se deberán realizar una por una. Comprobar la duración del tiempo de salida. Generar una alarma de robo. Comprobar la activación de la(s) posible(s) sirena(s). Verificar la correcta actuación del sistema de seguridad sobre un posible videograbador digital, tanto con alarmas en armado (robo) como en desarmado (atraco).	Anual
Comunicaciones	Las pruebas a efectuar variarán en función del n.º de vías, 1 ó 2, de las que disponga el sistema. Si se emplean 2 vías, ambas deben estar mutuamente supervisadas. Transmisor RTB, IP, GPRS/GSM o cualquier otra vía de utilizada. Provocar una o más alarmas y comprobar, con los medios disponibles (indicadores luminosos, escucha de la línea, etc.), el correcto curso de la llamada a CRA. Observar si el tiempo de transmisión es correcto (alrededor de 20 seg.) En caso de que sea un transmisor RTB o GSM, o de forma prácticamente instantánea en caso de comunicaciones IP o GPRS), o si, por el contrario, se producen demoras, reintentos, etc. Descolgado de llamadas entrantes. Con el sistema en reposo, comprobar su correcta respuesta ante una llamada entrante efectuada desde cualquier teléfono, de acuerdo con el método seleccionado (n.º fijo de ring o modo contestador). Verificar que, de estar la línea compartida (fax, etc.), nada obstaculiza su respuesta. Esta prueba es fundamental para comprobar que un acceso bidireccional desde la CRA será posible. Solicitar al operador de la CRA un acceso bidireccional y comprobar que no existen problemas que dificulten esta comunicación.	Anual

cve: BOE-A-2011-3170

Equipos	Acciones	Periodicidad (*)
Comunicaciones	Doble vía de comunicación: Provocar una o más alarmas y comprobar, con los medios disponibles (indicadores luminosos, escucha de la línea, etc.), el correcto curso de la llamada a CRA por la vía de comunicación primaria. Observar si el tiempo de transmisión es correcto (alrededor de 20 seg. En caso de que sea un transmisor RTB o GSM, o de forma prácticamente instantánea en caso de comunicaciones IP o GPRS) o si, por el contrario, se producen demoras, reintentos, etc. Desconectar la línea de comunicación primaria del sistema. Comprobar que, al cabo de un cierto tiempo (alrededor de 1 min.), su fallo es transmitido por la vía de comunicación alternativa. Reconectar RTB y retirar la antena del GSM. Si esto basta para provocar un fallo de cobertura (dependerá de la zona), comprobar que éste es transmitido por RTB. Si la segunda vía de comunicación es la línea IP, hay que tener en cuenta que un simple fallo IP no debe ser transmitido por la vía principal. Desconectar de nuevo la vía de comunicación principal y provocar algunas alarmas. Comprobar que son debidamente transmitidas por La vía alternativa. Al finalizar, reconectar la línea principal. Solicitar al operador de la CRA un acceso bidireccional por la vía principal(y, si es posible, también por la vía secundaria) y comprobar que no existen problemas que dificulten esta comunicación.	Anual
Contacto bidireccional	Solicitar al operador de la CRA que acceda al sistema por las distintas vías habilitadas (IP, RTB y/o posible GSM/GPRS) y compruebe la correcta calidad de establecimiento de la comunicación, el mantenimiento de ésta y la capacidad de actuación sobre el sistema, ejecutando alguna función (anulación/restauración de zonas, armado/desarmado, etc.).	Anual
Registro final	Obtener un nuevo registro de incidencias del periodo de pruebas y comprobar que todo ha sido debidamente grabado.	Anual

(*) El incremento de esta frecuencia estará en función de que el sistema permita la revisión bidireccional, desde la central de alarmas, de todos los elementos que lo componen, conforme al artículo 43.2 del Reglamento de Seguridad Privada y de factores tales como la climatología, la contaminación ambiental y acústica y otros de análoga naturaleza que permitan detectar cualquier anomalía del sistema o de alguno de sus elementos.

ANEXO III

Mantenimiento presencial trimestral, con posible alternativa automatizada (autotest) y bidireccional

Equipos	Acciones	Periodicidad (*)
Objetivos	Alimentación del sistema (red de c.a. y batería(s). Detección (funcionamiento de todos los volumétricos, sísmicos, etc.). En caso de que sea mantenimiento bidireccional, se solicitará la colaboración del usuario final para realizar esta comprobación en los detectores en los que no sea posible su prueba remota. Activación manual de alarmas (pulsadores y otros elementos activadores de atraco). En caso de que sea mantenimiento bidireccional, se solicitará la colaboración del usuario final. Prueba de posible sirena. Transmisión de incidencias a CRA por todas las vías habilitadas para ello (IP, RTB, etc.). Atención al usuario sobre posibles dificultades o problemas de utilización.	Trimestral
Funciones automáticas de test	Test periódicos automáticos: Las comunicaciones con la CRA deberán ser comprobadas periódicamente. La CRA deberá detectar los posibles fallos al generarse una «omisión» debida a la ausencia de recepción de un determinado número de señales consecutivas. Esta función ha de estar presente de forma independiente para todas las vías de comunicación, de acuerdo con los periodos marcados por la normativa en función del grado y del tipo de vía, principal o secundaria. Se habrá de comprobar en el registro de eventos del panel que las señales de test se han enviado correctamente de acuerdo a lo anteriormente indicado.	Trimestral

cve: BOE-A-2011-3170

Equipos	Acciones	Periodicidad (*)
Funciones automáticas de test	Batería: La batería se comprobará también de forma automática y, en caso de fallo, éste será transmitido a la CRA. Red de c.a: La red de c.a. estará también supervisada. Cualquier fallo deberá ser comunicado a la CRA, con un posible retardo. Un corte accidental del suministro eléctrico de poca duración no debe tener incidencia sobre el sistema. Registro de incidencias: Deberá ser obtenido bidireccionalmente, permitiendo analizar posibles fallos.	Trimestral
Funciones avanzadas de autotest	Sísmicos: Los sísmicos pueden ser comprobados de forma periódica y automática y, de producirse un fallo, éste será comunicado a la CRA. Para ello, cada sísmico debe poseer una cerámica de test en su interior o en sus inmediaciones que generará una vibración de corta duración al ser activada mediante una salida del CIE. Esta vibración generará una señal de alarma que será ignorada como tal por la central, sin embargo, si esta señal de alarma no se produjera, su omisión sí sería interpretada como fallo. Detectores y contactos Los detectores de movimiento y los contactos magnéticos montados sobre puertas y ventanas practicadas habitualmente se activan cuando el sistema se encuentra desarmado. Sus señales de alarma llegan a la central pero son ignoradas en estas circunstancias, no obstante, pueden emplearse para determinar un posible fallo de uno de estos elementos. Si es posible asignar de forma individual o colectiva a estos detectores un periodo de tiempo en el que, al menos, han de activarse una vez estando desarmado el sistema, podemos emplear esta función para detectar un posible fallo. Si un detector o contacto no se activa ninguna vez en el periodo establecido, puede interpretarse este hecho como un fallo del elemento.	Trimestral
Alternativa automatizada y bidireccional	Si un sistema dispone de las funciones vistas en los párrafos anteriores, podrán establecerse estos medios como alternativa a los mantenimientos presenciales, siempre y cuando sean activados, comprobados y certificados por la empresa instaladora durante su implantación. Para validar este método se comprobará, mensualmente como mínimo, que la comunicación bidireccional no plantea ninguna dificultad por las distintas vías establecidas. Igualmente se solicitará por teléfono, una vez cada 3 meses, la colaboración del usuario para la activación de los elementos de aviso de atraco y la activación de la volumetría de la instalación.	Trimestral

(*) En ningún caso podrán transcurrir más de cuatro meses entre dos revisiones sucesivas, conforme al artículo 43.1 del Reglamento de Seguridad Privada.

cve: BOE-A-2011-3170