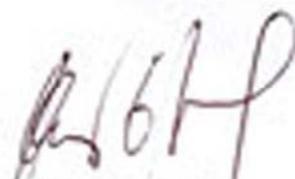




GUIA DE NORMAS IRAM APLICADAS A LA SEGURIDAD

IRAM 3860	Seguridad contra ilícitos	2
IRAM 3860-1	Seguridad contra ilícitos comercial	54
IRAM 4171-1	Sistemas de Alarmas Requisitos Generales	80
IRAM 4171-2	Requisitos Generales Código de Práctica	96
IRAM 4172	Detectores Infrarojos Pasivos	112
IRAM 4173-1	Sistemas de Transmisión RG	128
IRAM 4174	Centros de control a distancia	152
IRAM 4175	Planificación e Instalación de Alarmas	164
IRAM 4177	Instalación y Configuración para generar condiciones de confirmación de Alarma	206


Dirección de Certificación


Comité General de Certificación


Dirección General





INSTITUTO ARGENTINO
DE NORMALIZACIÓN
Y CERTIFICACIÓN

NORMA IRAM 3860

Diciembre 1994

ICS 13.310

*CNA MISC

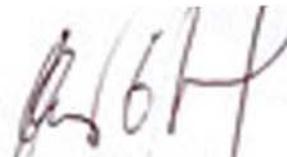
Certificado | sistemas de Gestión

GUÍA PARA LA SEGURIDAD CONTRA
ILÍCITOS EN INMUEBLES
DE USO PARTICULAR Y COMERCIAL



INSTITUTO ARGENTINO DE RACIONALIZACIÓN DE MATERIALES

* Corresponde a la Clase Nacional de Abastecimiento asignada por el Servicio Nacional de Catalogación dependiente del Ministerio de Defensa.


Dirección de Certificación


Comité General de Certificación


Dirección General



El estudio de esta norma ha estado a cargo de los organismos respectivos, integrados de la forma siguiente:

Comisión de Seguridad contra el delito

Integrante	Representa a:
Tco. E. Cabezas Liñayo	DIRECC. INT. EJERCITO ARG.
Ing. M. Camponovo	TELECOM
Dr. E. Carod	COLEGIO GRAD. CIENCIAS SEGURIDAD
Sr. S. Coelho	HIPERLOCK SRL
Dr. J. Cordero	UNIDAD CORONARIA MOVIL de QUILMES
Ing. C. Cruz	G y K S.A.
Tco. E. Ferreira Teixeira	TELEFONICA DE ARGENTINA
Ing. E. Florio	LA HOLANDO ARG.
Sr. H. Franza	VANGUARDIA S.A.
Tco. J. Gatti	GRACE ARG.
Sr. J. González	MUNICIPALIDAD DE QUILMES
Lic. M. Herrero	CNEA
Tco. H. Jerez	CAMARA DE ASEGURADORES
Ing. H. Lopez Cattáneo	ITSEMAP AUSTRAL
Sr. A. Maggio	A.A.S.PRI.
Lic. Miraglia Succi	COL. GRAD. CIENCIAS SEGURIDAD
Tco. C. Montanari	GENERAL INDUSTRIES ARG. S.A.
Ing. H. Mosquera	PLATEX
Sr. J. Nicosia	A.A.S.PRI.
Sr. A. Ortiz de Pinedo	INVITADO ESPECIAL
Arq. R. Pereyra	SOC. CENTRAL DE ARQUITECTOS
Crio (R) C. Reisz	A.A.S.PRI.
Ing. E. Ricucci Barrionuevo	CAI/UADI
Sra. R. Rozanski	ALERTALARMA
Lic. D. Saucedo	SEARCH
Lic. M. Soriano	COL. GRAD. CIENCIAS SEGURIDAD
Tco. J. Trejo	TELECOM
Ing. J. Cerutti	INSTITUTO IRAM
Ing. A. Paonessa	INSTITUTO IRAM

Comité General de Normas (C.G.N.)

Dr. V. Alderuccio	Ing. J. Kostic
Ing. J. V. Casella	Ing. J. Mangosio
Dr. E. Catalano	Ing. S. Mardyks
Dr. A. M. Cruz	Dr. E. Miró
Ing. D. Donegani	Dr. A. F. Otamendi
Ing. R. Fernández	Ing. T. A. Palacios
Lic. C. A. Grimaldi	Sr. F. R. Soldi
Dr. A. Grosso	Prof. M. P. Mestanza
Dr. R. L. Huste	

- En el estudio de esta norma se ha tenido en cuenta el antecedente siguiente:

BSI - **BRITISH STANDARDS INSTITUTION**
BS 8220: Part 2 - Security of buildings against crime. Offices and shops
(1987).

ÍNDICE TEMÁTICO

PRIMERA SECCIÓN - GENERALIDADES

- 1.1 Objeto y campo de aplicación
- 1.3 Definiciones
- 1.4 Oportunidades para robo, hurto e incendio provocado
- 1.5 Estrategia
- 1.6 Evaluación de las necesidades de seguridad con relación a los riesgos potenciales
- 1.7 Incendio-emergencias y otros riesgos en la seguridad

SEGUNDA SECCIÓN - ASPECTOS DE LA GESTIÓN DE LA SEGURIDAD

- 2.1 Generalidades
- 2.2 Pautas para mejorar la seguridad

TERCERA SECCIÓN - PROYECTO

- 3.1 Generalidades
- 3.2 Anteproyecto
- 3.3 Proyecto, características exteriores y estructurales
- 3.4 Diseño interior

LEONID LLONTOP CASTRO
Jefe de Seguridad Casa Matriz
Banco Ciudad Bs. As.

CUARTA SECCIÓN - VENTANAS

- 4.1 Generalidades
- 4.2 Riesgos por proteger
- 4.3 Conversión de ventanas de abrir en ventanas fijas
- 4.4 Directivas para el diseño de ventanas
- 4.5 Barrotes para ventanas
- 4.6 Rejas de ventanas y persianas
- 4.7 Cerraduras de ventanas y pestillos para ventanas de abrir
- 4.8 Ventilación

QUINTA SECCIÓN - PUERTAS EXTERIORES

- 5.1 Generalidades
- 5.2 Funciones de las puertas exteriores y control de accesos
- 5.3 Vulnerabilidad de las puertas a las embestidas
- 5.4 Construcción e instalación de puertas y marcos
- 5.5 Cerraduras y otros herrajes
- 5.6 Cierre y traba de las puertas exteriores
- 5.7 Incremento de la seguridad en puertas existentes
- 5.8 Llaves maestras

LEONID LLONTOP CASTRO
Jefe de Seguridad Casa Matriz
Banco Ciudad Bs. As.

SEXTA SECCIÓN - VIDRIOS Y VIDRIADOS DE PLANCHAS PLÁSTICAS

- 6.1 Generalidades
- 6.2 Comportamiento de diferentes tipos de vidrios
- 6.3 Selección del vidriado.
- 6.4 Áreas vidriadas que necesitan consideración especial
- 6.5 Vidriado.

**SÉPTIMA SECCIÓN - OTROS PUNTOS DE ACCESO, TECHOS, CERCOS,
PORTONES Y BARRERAS PARA EL TRÁNSITO**

- 7.1 Acceso a través del techo
- 7.2 Aberturas en techo
- 7.3 Cielorrasos y pisos suspendidos. Conductos para ventilación y otros servicios.
- 7.4 Puertas de sótanos
- 7.5 Conductos externos de desagüe
- 7.6 Cerco perimetral
- 7.7 Portones
- 7.8 Porterías
- 7.9 Barreras para el tránsito

LEONID LLONTOP CASTRO
Jefe de Seguridad Casa Matriz
Banco Ciudad Bs. As.

OCTAVA SECCIÓN - VIGILANCIA ELECTRÓNICA Y SISTEMAS DE ALARMA

- 8.1 Circuito cerrado de televisión
- 8.2 Sistemas de alarma contra intrusos

NOVENA SECCIÓN - AREAS Y ACTIVIDADES DE ALTO RIESGO

- 9.1 Manejo de dinero y oficinas con efectivo
- 9.2 Cámara de seguridad
- 9.3 Cajas fuertes
- 9.4 Robo de información

DÉCIMA SECCIÓN - ILUMINACIÓN

- 10.1 Generalidades
- 10.2 Necesidad de iluminación de seguridad
- 10.3 Estrategia
- 10.4 Pautas para el uso
- 10.5 Lámparas
- 10.6 Luminarias
- 10.7 Control
- 10.8 Instalación
- 10.9 Mantenimiento

LEONID LLONTOP CASTRO
Jefe de Seguridad Casa Matriz
Banco Ciudad Bs. As.

**GUÍA PARA LA SEGURIDAD CONTRA ILÍCITOS EN
INMUEBLES DE USO PARTICULAR Y COMERCIAL**

ICS 13.310
*CNA MISC

LEONID LLONTOP CASTRO
Jefe de Seguridad Casa Matriz
Banco Ciudad Bs. As.

PRIMERA SECCIÓN - GENERALIDADES

0 NORMAS PARA CONSULTA

- IRAM 3570 - Puertas contra incendio de madera y metálicas.
- IRAM 3730 - Sistema de señales luminosas y acústicas.
- IRAM 4171-1 - Sistema de alarmas. Exigencias generales.
- IRAM 4171-2 - Código de práctica de sistemas de alarma.
- IRAM 4172 - Sistemas de alarma. Detectores infrarrojos pasivos.
- IRAM 9509 - Maderas para carpintería.
- IRAM 9600 - Maderas aserradas preservadas.
- IRAM 9600-1 - Madera preservada contra agentes biológicos. Criterio para su compra.
- IRAM 9600-2 - Madera preservada contra agentes biológicos. Requisitos y métodos de ensayo.
- IRAM 10005-1 - Colores y señales fundamentales.
- IRAM 10005-2 - Aplicación de los colores de seguridad en señalizaciones particulares.
- IRAM 11505 - Carpintería de obra. Definiciones.
- IRAM 11506 - Ventanas de madera.
- IRAM 11507 - Ventanas y puertas exteriores.
- IRAM 11524 - Puertas metálicas para exteriores.
- IRAM 11530 - Ventanas metálicas para exteriores.
- IRAM 11543 - Cerramientos exteriores de aluminio.
- IRAM 12556 - Vidrios planos de seguridad.

LEONID LLONTOP CASTRO
Jefe de Seguridad Casa Matriz
Banco Ciudad Bs. As.

* Corresponde a la Clase Nacional de Abastecimiento asignada por el Servicio Nacional de Catalogación dependiente del Ministerio de Defensa.

IRAM 12595 - Vidrios de seguridad. Práctica recomendada de seguridad para vidrios susceptibles de impacto humano.

IRAM 12596 - Práctica recomendada para el empleo de vidrios de seguridad.

IRAM 91311 - Vidrios y sus productos. Definiciones.

LEONID LLONTOP CASTRO
Jefe de Seguridad Casa Matriz
Banco Ciudad Bs As

1 OBJETO Y CAMPO DE APLICACIÓN

1.1 Esta norma contiene medidas de seguridad físicas edilicias, empleando materiales y medios mecánicos, eléctricos, térmicos, acústicos y ópticos para aumentar la protección contra los ilícitos en inmuebles de uso particular y comercial. Las recomendaciones estratégicas para los arquitectos, ingenieros, constructores, diseñadores especializados, propietarios y ocupantes incluyen las condiciones necesarias y las restricciones para combatir robos y otros ilícitos (están tratados en esta sección).

La gestión y aspectos de diseño están considerados en las secciones 2 y 3. La sección 4 aconseja sobre medidas de seguridad en ventanas. Las puertas de entrada, puertas exteriores y el control de acceso están en la sección 5. El tema relacionado con las superficies vidriadas se trata en la sección 6.

Otros lugares potencialmente vulnerables que pueden ser aprovechados para entradas no autorizadas a los inmuebles se tratan en la sección 7. El uso de sistemas de alarma contra intrusos, circuitos cerrados de televisión y la iluminación de seguridad se describe en las secciones 8 a 10.

Las áreas y actividades de alto riesgo se tratan en la sección 9 que contiene información referente al manejo del dinero y a las cajas de efectivo, cámaras blindadas, cajas de caudales y al robo de información.

1.2 Debido a sus especiales necesidades de seguridad los bancos, las oficinas de correo y joyerías no están cubiertas por esta norma.

1.3 Definiciones

Además de los términos definidos en las normas IRAM 11535 y 11505 referentes a elementos de edificios, se agrega la definición siguiente.

salida final. Salida usada por la última persona para retirarse de un inmueble y por lo que requiere ser cerrada desde afuera.

Nota. La anterior definición no debe confundirse con el significado de la expresión cuando es usada con relación a los medios de escape en incendios. En este caso salida final es el punto terminal de una vía de escape hacia un espacio abierto más allá del cual las personas ya no están en peligro del alcance del fuego y pueden dispersarse con seguridad (ver Ley Nacional de Higiene y Seguridad en el Trabajo N° 19587 y Dto. 351/79).

1.4 Oportunidades para robo, hurto e incendio provocado

1.4.1 robo. Los delincuentes se interesan en los locales donde estiman que hay bienes valiosos que pueden ser rápidamente enajenados.

Robos en inmuebles comerciales. Pueden dividirse en dos grupos:

- a) locales de alto riesgo que atraen la atención de delincuentes que emprenden asaltos premeditados como por ejemplo robo a granel; robo de bienes de alto valor o robo de equipamiento o de información.
- b) robos de menor valor cometidos por oportunistas que aprovechan la vulnerabilidad de las medidas de seguridad.

Puntos de acceso. Las puertas exteriores, las ventanas accesibles, las áreas de almacenamiento, de recepción y de despacho que están fuera de la vista en la parte posterior de inmuebles comerciales son especialmente vulnerables. Las ventanas de planta baja y las ventanas accesibles desde balcones, pasillos y techos son más vulnerables que las ventanas de pisos superiores que están más allá del alcance normal. Las ventanas de abrir y puertas son usadas generalmente como puntos de ingreso. Los delincuentes procuran conseguir rápidamente el acceso con el mínimo de esfuerzo y ruido.

Algunos de los métodos usados por los delincuentes para entrar en los edificios son:

- a) a través de ventanas o puertas que han sido dejadas abiertas o sin cerradura;
- b) conseguir el acceso a los cerrojos de ventanas y pestillos de puertas rompiendo los paneles vidriados adyacentes;
- c) violentando puertas insuficientemente robustas para resistir embestidas;
- d) descerrajando cerraduras débiles;
- e) venciendo pestillos de resorte;
- f) levantando con palancas, puertas y ventanas previamente abiertas;
- g) a través de los techos.

LEONID LLONTOP CASTRO
Jefe de Seguridad Casa Matriz
Banco Ciudad Bs. As.

La reducida seguridad de las vidrieras puede también ser usada para conseguir el acceso o para destrozos, incursión y arrebatos.

Las áreas de garage y los recintos para estacionamiento de vehículos están frecuentemente sujetos a vandalismo y pueden dar oportunidades para ilícitos de o desde automóviles.

1.4.2 Hurto

Los delincuentes aprovechan la exhibición de mercaderías en comercios y frecuentemente utilizan el ocultamiento proporcionado por la multitud. Los bienes de gran valor, portátiles y de fácil enajenación pueden tener particular atractivo cuando las medidas de seguridad se descuidan. El hurto de las pertenencias del personal es más probable que ocurra cuando no se cuenta con los medios seguros para guardarlas.

1.4.3 Daño criminal por incendio

Muchos de los incendios son causados por delincuentes. Más frecuentemente son el resultado de actos deliberados. Lo que interesa para un delincuente es la facilidad de acceso y la disponibilidad de materiales con los cuales pueda iniciar el fuego.

La seguridad que evita el acceso a los edificios no elimina totalmente el riesgo de incendios intencionales.

El acceso al perímetro del inmueble puede permitir la iniciación de incendios mediante la introducción de fuentes de ignición a través de aberturas tales como ventanas rotas y buzones, mientras que también iniciados en el exterior, pueden penetrar en el edificio. Todos los inmuebles se encuentran potencialmente a riesgo de los incendiarios. Los bienes con mayores riesgos son los que están apartados, frecuentemente en locales no vigilados o con pequeña o ninguna seguridad física.

Los resquicios debajo de las puertas deben ser tan pequeños como sea necesario y cuando sea posible deben ser sellados. Los buzones deben estar provistos con receptáculos metálicos interiores.

Las sustancias peligrosas como líquidos inflamables y cilindros de gas, deben mantenerse en cantidad mínima necesaria en el caso de su exhibición en locales de ventas. Los almacenamientos mayores de tales materiales deben ser encerrados en depósitos especiales, particularmente fuera de las horas de trabajo (ver Decreto 351/79 Seguridad e Higiene en el Trabajo).

Un alto nivel de vigilancia en los inmuebles puede frustrar los atentados incendiarios o puede limitar su propagación con el consecuente daño.

El riesgo de un incendio externo ocasionado, por ejemplo, por desperdicios de combustibles y propagado al interior del edificio, debe ser tenido en cuenta.

1.4.4 Medidas de seguridad existentes

Una detallada apreciación de los inmuebles existentes, puede revelar que las medidas de seguridad física son adecuadas pero no son utilizadas o se las usa incorrectamente.

1.5 Estrategia

La estrategia global para combatir ilícitos en oficinas y locales de venta, debe resolver situaciones que rigen cuando los locales están abiertos y cuando están cerrados. La estrategia básica debe comprender:

- a) si bien las tendencias arquitectónicas actuales recurren en forma habitual a las superficies vidriadas y a los accesos múltiples, se recomienda limitar tanto como sea posible el número de puertas externas, ventanas accesibles y otros posibles puntos de acceso;
- b) asegurar cuando sea posible que los potenciales intrusos no puedan entrar inadvertidamente;
- c) proveer iluminación apropiada para dificultar que los intrusos actúen sin ser observados;
- d) proveer y mantener dispositivos adecuados de seguridad en puertas exteriores, en ventanas y otros posibles puntos de acceso;
- e) controlar los accesos a las oficinas y zonas de los locales no destinadas a ser utilizadas por los clientes en el horario comercial;
- f) proyectar la disposición interior para minimizar las pérdidas;
- g) estar alerta frente a hurto de los clientes y del personal;

- h) emplear personal de seguridad cuando sea conveniente;
- i) registrar y marcar mercaderías con la identificación de la empresa para ayudar a la policía en la recuperación de los artículos valiosos que puedan ser robados;
- j) reducir la posibilidad de la iniciación de incendios intencionales;
- k) privar de combustible disponible al potencial incendiario.

1.6 Evaluación de las necesidades de seguridad con relación a los riesgos potenciales.

El grado de seguridad necesaria para un inmueble en particular dependerá de su riesgo potencial. Para llegar a una evaluación es necesario considerar los siguientes aspectos:

- a) tipo de empresa;
- b) atractivo para los delincuentes profesionales u oportunista de mercadería, efectivo, y posiblemente documentos confidenciales guardados. Los artículos valiosos y portátiles y los que pueden ser fácilmente enajenados son particularmente atractivos;
- c) las potenciales vías para llevarse las mercaderías robadas, ellas pueden no ser las mismas que las posibles vías de entrada;
- d) facilidad de acceso desde calles, áreas descubiertas, techos adyacentes, pisos del edificio por arriba y por debajo de los locales de referencia, cuando están bajo ocupación separada y desde locales contiguos;
- e) grado de seguridad inherente a la construcción;
- f) vulnerabilidad relativa a las tendencias locales de ilícitos;
- g) vigilancia proporcionada por la actividad pública normal y la patrulla policial de rutina del área, o por la patrulla de seguridad del inmueble o sus alrededores.

1.7 Incendio-emergencias y otros riesgos en la seguridad

1.7.1 Una evaluación del riesgo para la seguridad se efectuará principalmente con la experiencia práctica para no alterar la ocupación funcional de los inmuebles. También se tendrá en cuenta la necesidad de asegurar que las disposiciones para la seguridad no interfieran en ninguna de las instalaciones o procedimientos relacionados con las precauciones contra incendios y otras emergencias, particularmente los medios de escape.

Tales instalaciones y procedimientos pueden ser requeridos por las reglamentaciones vigentes como las que se refieren a las precauciones contra incendios, la planificación urbana, reglamentos de construcción, etc.

Se requiere especial cuidado para asegurarse que no sean dañadas las instalaciones contra incendio en las playas de estacionamiento en subsuelos, áreas de servicio, playas de carga y las instalaciones para depósito de desperdicios.

Debe ser consultada la autoridad competente antes de efectuar alteraciones de la estructura o de la distribución de los inmuebles o de la disposición de las instalaciones. Con respecto a las precauciones contra incendio confiadas solamente a la experiencia práctica resultan habitualmente poco satisfactorias y es importante la consulta a expertos y a la autoridad competente.

1.7.2 Restricciones relacionadas con los incendios. Dentro de oficinas y locales de venta no es aceptable que las puertas que sirven como medio de escape en caso de incendio estén cerradas o trabadas de tal modo que los ocupantes necesiten usar llave para abrirlas. Cuando se evalúan medidas de seguridad es aconsejable considerar cerrojos que no requieran llaves cuando los locales estén ocupados.

Los pestillos y herrajes de seguridad pueden causar problemas cuando son usados en puertas resistentes al fuego porque cualquier dispositivo que requiera recortar alguna parte de la puerta puede reducir la resistencia al fuego a un grado inaceptable a los requisitos establecidos en la norma IRAM 3570.

Se debe tener en cuenta que las medidas de seguridad que restrinjan el acceso de los bomberos en el caso de incendio provocarán un mayor daño al inmueble y su contenido por la demora en el combate del fuego en la etapa más crítica.

SEGUNDA SECCIÓN - ASPECTOS DE LA GESTIÓN DE LA SEGURIDAD

2.1 Generalidades

La responsabilidad por la seguridad en inmuebles comerciales debe involucrar al máximo departamento gerencial de la empresa. Solamente a dicho nivel es posible abordar adecuadamente la magnitud y complejidad del problema y suministrar medidas para el virtual riesgo de cada empleado o visitante.

Con mucha frecuencia no hay una única y simple respuesta para los aspectos de la gestión de seguridad aunque casi invariablemente es posible determinar principios básicos con los cuales gerentes, supervisores y empleados deberán concordar.

Las medidas de seguridad serán afectadas durante las horas de trabajo por las partes del inmueble que deben estar abiertas para visitantes o compradores y aquellas partes donde se necesita limitar o regular el acceso.

2.2 Pautas para mejorar la seguridad

Los administradores deben capacitarse para apreciar si las disposiciones de seguridad existentes o propuestas son satisfactorias. Las acciones deben ser:

- a) evidentes y claras luego de la lectura de las distintas secciones de esta norma;
- b) las requeridas por la opinión de expertos y de otros ocupantes del mismo edificio o inmuebles adyacentes como puede ser, dotar en centros comerciales de un servicio de seguridad en el área.

TERCERA SECCIÓN - PROYECTO

LEONID LLONTOP CASTRO
Jefe de Seguridad Casa Matriz
Banco Ciudad Bs As

3.1 Generalidades

3.1.1 Aplicación de los principios de seguridad en la etapa de diseño

Es esencial que dichos principios se consideren en la etapa de proyecto porque las modificaciones posteriores en cualquier edificio para mejorar la seguridad no sólo resultan onerosas sino también pueden alterar la función primaria de los inmuebles. Un diseño claro y ordenado tanto en la parte exterior como en la interior de un terreno o edificio puede favorecer la vigilancia especialmente cuando se dispone de una buena iluminación natural y artificial.

3.1.2 Función del edificio

La apreciación de las amenazas a la seguridad debe ser contrapesada con las funciones del edificio.

3.1.3 Entorno

La ubicación específica y el ambiente circundante suministrarán detalles esenciales para el plan básico, que puede incluso cambiar los factores ambientales existentes tal como el caso de la habilitación de las instalaciones deportivas y la posible violencia urbana.

3.1.4 Perímetro de los inmuebles

Es importante una eficiente seguridad física en el perímetro exterior de los solares edificados empleando, cuanto sea posible, las ventajas físicas naturales. Debe considerarse la seguridad de puertas, ventanas y otras aberturas de servicio en el perímetro y áreas techadas de edificios. La seguridad física de entrada y salida y otras instalaciones dentro del inmueble estarán naturalmente influenciadas por la principal función de los locales, pero deben reflejar perfectamente y complementar el sistema de seguridad exterior.

3.1.5 Uso de materiales y equipamientos de seguridad comprobados

Los materiales y equipos de seguridad deben cumplimentar el plan básico proyectado.

3.1.6 Zonas riesgosas de los edificios

Las zonas de los edificios tales como cámaras blindadas, depósitos de bienes valiosos, oficinas de cajeros, departamento de computación y archivos de documentos requieren atención especial y deben estar dispuestos perfectamente dentro de la zona de protección tanto internas como externas. Estas áreas vulnerables pueden requerir materiales y equipos más sofisticados y esas especiales características deben estar integradas en el plan global de seguridad.

3.1.7 Factores para los diferentes tipos de inmuebles

No es posible dar factores de diseño a medida para cada clase de inmuebles, pero las pautas a controlar, detalladas en los párrafos 3.2; 3.3 y 3.4 dan una base sobre la cual se desarrollará el diseño de oficinas y locales de venta (incluyendo kioscos, locales de esquinas, en terrazas, semiseparados, separados, supermercados, grandes tiendas y locales que forman parte de centros comerciales).

3.2 Anteproyecto

Deberán considerarse:

- a) hasta qué punto la elección de la ubicación de los inmuebles puede ser predeterminada por otras consideraciones con el grado de influencia que pueden tener los factores de seguridad;
- b) el límite hasta el cual las medidas de seguridad serán influenciadas para un terreno propuesto, teniendo en cuenta;
 - 1) aislación de los inmuebles en zonas rurales;
 - 2) clases de ilícitos que pueden ocurrir si los inmuebles están en áreas urbanas;

LEONID LLONTOP CASTRO

Jefe de Seguridad Casa Matriz
Banco Ciudad Bs. As.

- 3) consideraciones especiales si los inmuebles estarán en zonas suburbanas;
- c) niveles de ilícitos zonales posibles o existentes tales como robo, hurtos, disturbios, vandalismo, las pintadas en muros y otros daños;
- d) proximidad a áreas de reuniones públicas, por ejemplo cancha de futbol, salas de baile, campos de deportes;
- e) el limite hasta el que puede influenciar en los problemas de seguridad el clima con sus factores estacionales tal como la afluencia de turistas;
- f) la posibilidad de lograr seguridad adicional con las características de la naturaleza como las suministradas por rios, arroyos, y accidentes del terreno;
- g) ventajas que pueden lograrse por la proximidad de establecimientos constantemente dotados con personal de seguridad como policías, bomberos y servicios médicos de emergencia o de perímetros de seguridad existentes en propiedades con altos muros o cercos;
- h) beneficios que pueden obtenerse de un eficiente alumbrado público;
- i) niveles de seguridad que los propietarios y ocupantes de otros edificios en el distrito emplean en su propiedad;
- j) factores de vigilancia tales como el alcance visual con que puede ser observada una propiedad desde otras fincas;

Para complementar las observaciones personales en estas cuestiones conviene recabar el asesoramiento de los expertos en seguridad. También en esta etapa se aconseja la consulta a instituciones como por ejemplo: LA COMISIÓN NACIONAL ASESORA PARA LA INTEGRACIÓN DE PERSONAS DISCAPACITADAS, para tener en cuenta en el diseño de accesos los aparatos y accesorios que ellas utilizan.

3.3 Proyecto, características exteriores y estructurales

EONID LLONTOP CASTRO
Jefe de Seguridad Casa Matriz
Banco Ciudad Bs. As.

3.3.1 Generalidades

El perímetro de todo tipo de inmueble debe ser seguro y resistente debiéndose brindar especial consideración al nivel de seguridad, destino y estructura de los edificios contiguos y de cualquier instalación compartida. Debe darse particular atención a la seguridad de entradas, salidas en muros y en techos expuestos.

3.3.2 Accesos - entradas

La ubicación y el tipo de entradas deberá equilibrarse con las comodidades de clientes y del personal y las necesidades para la seguridad. Una eficiente iluminación direccional, instalaciones de control, ya sean manuales, mecánicas o electrónicas bien mantenidas y líneas visuales sin obstáculos, favorecerán la seguridad.

3.3.3 Complejos comerciales

Para decidir el nivel de seguridad de un local dentro de un centro comercial debe considerarse si el complejo estará cerrado fuera de las horas de trabajo del local en cuestión, pues el edificio cerrado será más seguro y requerirá un nivel menor de vigilancia.

3.3.4 Instalación compartida

La seguridad de los inmuebles requiere tener en cuenta la vulnerabilidad de toda entrada o salida compartida. Donde sea apropiado se adoptarán medidas de seguridad mutuamente convenidas para servicios y caminos de uso común.

3.3.5 Caminos de tránsito interno

La buena iluminación, provisión de instalaciones de seguridad, señalización clara de caminos y otros carteles informativos mejorarán la supervisión del tránsito. Siempre que sea posible es ventajoso utilizar caminos separados para los vehículos de carga y los particulares.

3.3.6 Paradas de ómnibus y zonas de espera

Estas áreas, cerca de las paredes perimetrales o entradas y salidas pueden motivar requerimientos adicionales de seguridad.

3.3.7 Playas de estacionamiento

Las instalaciones de playas de estacionamiento son actualmente una parte esencial en la explotación de locales comerciales y oficinas. Cada tipo de playa de estacionamiento sea a nivel de terreno, subsuelo o en varias plantas presenta problemas particulares de seguridad, las que pueden ser minimizadas con buen control y supervisión de los accesos. Para oponerse al vandalismo debe haber una buena iluminación exterior, bien localizada y direccional, carteles con disposiciones y designación de áreas para vehículos sea con mercaderías, para mantenimiento y particulares. Donde sea apropiado deben ser asignadas franjas para ciclistas, peatones, tranvías, trolebus y otros medios de transporte.

La vigilancia puede ser mejorada con circuitos cerrados de televisión (ver sección octava). Se puede proporcionar mayor seguridad contratando a una compañía de taxis acreditada con servicio las 24 horas para que los automovilistas se desplacen de o desde la playa de estacionamiento mediante dicho servicio.

3.3.8 Recepción y despacho de mercadería

Estas áreas pueden ser especialmente vulnerables si no se proyectan teniendo en cuenta la seguridad.

LEONID LLONTOP CASTRO
Jefe de Seguridad Caso Meriz
Banco Ciudad Bs. As.

3.3.9 Instalaciones para servicio indispensables

Los proyectistas deben considerar la posibilidad del uso por personas no autorizadas de las instalaciones para servicios necesarios como: montacargas, puntos de recepción de combustibles, conductos de ventilación y aberturas para cintas transportadoras. Cuando sea posible se deben ocultar tales servicios o localizarlos en compartimientos cerrados.

Deben tomarse disposiciones para la seguridad en cañerías expuestas y servicios de emergencia, cables telefónicos, generadores, etc.

3.3.10 Construcción de edificios

Como premisa inicial de seguridad se deben ejecutar las construcciones con materiales con resistencia mecánica para soportar impactos, ataques y acciones vandálicas.

3.3.11 Aspectos básicos de diseño

Las plantas de edificación con líneas de edificación despejadas, sin obstáculos, tienen naturales ventajas para la seguridad. Innecesarios rebordes, parapetos, hendiduras, salientes pronunciadas y umbrales anchos, proporcionan medios para el acceso ilegal. Conviene que las tuberías externas sean empotradas o tapadas.

3.3.12 Techos

Un proyecto apropiado de los techos contribuye mucho para la seguridad, básicamente es necesario una construcción sólida con materiales resistentes. Se requieren cuidados especiales en las claraboyas y los accesos por ventanas de techos. Hay que considerar una iluminación exterior estratégica, una buena seguridad física de las vías de acceso a techos, incluido los contiguos, y a los espacios huecos de los cielorrasos. El tema de las vías de acceso a los techos se trata en Sección Séptima.

3.3.13 Ventanas accesibles

Hasta donde lo admitan otras consideraciones, el número de ventanas accesibles debe mantenerse en el mínimo, las cuestiones que deben ser consideradas para la seguridad, son:

- a) el tamaño y la forma;
- b) la selección del marco;
- c) el método de apertura;
- d) el tipo de cerradura y fallebas para ventanas de abrir;
- e) las ventajas que pueda obtenerse con el uso de ventanas fijas cuando otras consideraciones lo admitan;
- f) la seguridad adicional proporcionada por barrotes y rejas, especialmente en escaparates.

LEONID LLONTOP CASTRO
Jefe de Seguridad Casa Matriz
Banco Ciudad Bs. As.

Las ventanas se analizan en la Sección Cuarta.

3.3.14 Puertas exteriores

Son frecuentemente el foco de atención de los delincuentes. Los puntos que deben ser considerados, son:

- a) localización;
- b) mantenimiento del número de entradas y salidas en el mínimo;
- c) diseño y resistencia de puertas y marcos;
- d) selección de los paneles vidriados;
- e) tipo de madera, vidrio o metal;
- f) requerimientos obligatorios para las salidas contra incendio;
- g) tipo de puerta de salida final;

- h) refuerzo obtenible con revestimientos metálicos;
- i) restricciones en los cierre de las puertas de salida de emergencia.

Las puertas se analizan en Sección Quinta.

3.3.15 Vidrio y vidriado

Los factores que afectan a la seguridad, son:

- a) tipo;
- b) espesor;
- c) resistencia;
- d) fijación del bastidor;
- e) uso de doble vidriado.

LEONID LLONTOP CASTRO
Jefe de Seguridad Casa Matriz
Banco Ciudad Bs. As.

Estos temas se abordan en la Sección Sexta.

3.3.16 Cerraduras y otros herrajes de seguridad

Es esencial que las cerraduras sean seleccionadas de modo tal que desempeñen íntegramente su función oponiéndose al ingreso de los no autorizados.

3.4 Diseño interior

3.4.1 Áreas de recepción

Mientras hay razones comerciales para que las áreas de oficina y locales de venta sean irrestrictas y atractivas, es en esas zonas donde debe darse un claro mensaje a los clientes y visitantes acerca de que existe un sistema de seguridad, sin suministrar mayores precisiones sobre el mismo. Las mesas de recepción deben estar bien ubicadas para proporcionar la mejor visibilidad al personal.

Los accesos controlados pueden realizarse con puertas giratorias o barreras vaivén, que cumplan con las reglamentaciones vigentes. Las alarmas en la entrada que varían desde la simple activación de la puerta hasta los sofisticados monitoreos con circuitos cerrados de televisión, complementarán eficazmente los procedimientos de la seguridad. También son aconsejables los carteles con claras indicaciones acerca de las disposiciones de seguridad.

3.4.2 Área de exhibición

En esta zona se presenta frecuentemente un conflicto entre la seguridad y las consideraciones comerciales. Los proyectistas y diseñadores pueden colaborar en la reducción de los problemas de seguridad, proporcionando buena iluminación, claras líneas de visibilidad y evitando ocultamiento en esquinas.

Controlar la seguridad es esencial y puede variar entre simples espejos cruzados hasta protección general con circuitos cerrados de televisión.

Los medios apropiados de seguridad se suministrarán particularmente para las mercaderías más valiosas y equipamientos de oficinas con su documentación, ya sea con accesorios en las paredes y el techo o con gabinetes de seguridad.

3.4.3 Zona de mostradores, caja registradora y de cobranzas

El diseño deberá suministrar buen control del área de facturación y pago en los locales. Las disposiciones para la seguridad de cajas registradoras y de cobranza pueden realizarse con cajas de seguridad de piso y buzones con rampa. Cuando es necesario se puede proporcionar seguridad adicional con circuitos cerrados de televisión y sistemas de señalización de emergencia.

3.4.4 Oficinas para dinero y cámaras blindadas

La provisión de un área de seguridad interior para dinero en efectivo y otros valores puede ser una esencial necesidad. El diseño debe incluir consideraciones tales como:

- a) determinación del riesgo;
- b) decisión del sitio ideal dentro del edificio;
- c) uso de los materiales adecuados desde el punto de vista de la seguridad para la construcción de paredes, pisos y techos;
- d) resistencia al agua y al fuego;
- e) requerimientos para ventilación y salidas de emergencia;
- f) restringir aperturas innecesarias de puertas suministrando unidades de transferencia de dinero paredes o puertas y proveyendo comunicación con el exterior;
- g) buena visibilidad cruzada;
- h) provisión de circuitos cerrados de televisión y protección con alarma;
- i) protección de vestíbulo y salas de espera;
- j) puertas y cerraduras adecuadas al nivel de riesgo;
- k) cajas de seguridad con accesorios adecuados;
- l) armarios y vitrinas resistentes al fuego;
- m) armarios de seguridad;
- n) control de llaves de acceso;
- o) cumplimiento con normas operativas para ingreso-egreso (por ejemplo, haciendo entrar sólo una persona por vez bajo supervisión o también con dos puertas de apertura sucesiva y nunca simultánea separadas por un pasillo intermedio controlado).

LEONID LLONTOP CASTRO
Jefe de Seguridad Casa Matriz
Banco Ciudad Bs. As.

3.4.5 Depósitos internos para bienes y mercaderías valiosos

Si no se dispone de una sala segura y bien ventilada o de un depósito interior, hay que estudiar la construcción de un local con muros y techos con malla de acero y protegido con puerta y llave. Frecuentemente se usan trabas de metal o plástico como protección adicional de tales puertas además de buenos controles para el acceso y de la distribución de llaves.

3.4.6 Sala de personal

Excepto en pequeños locales y oficinas se debe proporcionar al personal un cuarto para su propio uso. Dicha sala deberá incluir instalaciones de roperos con llaves para guardar sus pertenencias personales. Debe haber un registro con la asignación de roperos y un sistema de control de llaves.

3.4.7 Equipamiento de otras áreas de servicio

El proyecto debe incluir aspectos de seguridad para prevenir robos y daños accidentales o intencionales al equipamiento tales como controles en cámaras frigoríficas o de generación de electricidad. Las zonas deben ser diseñadas para que puedan mantenerse libres y ordenadas asegurando una buena supervisión y reduciendo el riesgo de incendios.

3.4.8 Teléfonos

La provisión y la localización de las instalaciones telefónicas deben ser analizadas detalladamente en el plan de seguridad.

3.4.9 Sistemas de alarmas contra intrusos

El proyecto debe admitir la instalación de apropiados sistemas de alarmas contra intrusos cuando sean necesarios.

3.4.10 Alarmas contra incendio

Tiene relevancia por cuanto los incendios pueden ser causados con propósitos delictivos. La incorporación de detectores automáticos de incendios en los sistemas de alarma darán un aviso prematuro del incendio. Si la alarma es automáticamente transmitida al departamento de bomberos próximos. La pronta respuesta para la lucha contra el incendio reducirá el daño emergente.

3.4.11 Alarmas contra ataque al personal

Puede requerirse dichas instalaciones debiendo ser estratégicamente ubicadas para protección del personal que trabaja en lugares tales como oficinas de dinero, o zonas donde hay mercadería o bien valioso.

3.4.12 Emergencias

La distribución interior debe ser tal que puedan ser rápidamente puestos en marcha planes experimentados para emergencias tales como incendio, amenaza de bombas, robo y asalto.

Cuando emergencias diferentes exijan distintas acciones del personal, los medios para dar los apropiados avisos o instrucciones, deben ser inequívocos para evitar confusión (ver norma a estudiar IRAM 3730).

3.4.13 Sistemas para dirigirse al público

En grandes locales puede ser requerida la instalación de sistemas para dirigirse al público. Se utilizan principalmente para advertir rápidamente de una emergencia.

CUARTA SECCIÓN - VENTANAS

4.1 Generalidades

Esta sección se refiere particularmente a la seguridad de tres tipos de ventanas accesibles.

- a) ventanas de abrir;
- b) ventanas fijas;
- c) vidrieras.

LEONID LLONTOP CASTRO
Jefe de Seguridad Casa Matriz
Banco Ciudad Bs. As.

Se considera la seguridad con relación a la accesibilidad a cerraduras y fallebas y también el caso de las rotura de vidrieras para arrebatos.
Se dan directivas sobre:

- 1) naturaleza de los riesgos por proteger (ver 4.2);
- 2) conversión de ventanas de abrir en fijas (ver 4.3);
- 3) diseño de las ventanas (ver 4.4);
- 4) barrotes en las ventanas de abrir y fijas y su aplicación restringida en vidrieras (ver 4.5);
- 5) rejas y persianas para todo tipo de ventanas especialmente vidrieras (ver 4.6);
- 6) cerraduras y cierres para ventanas de abrir (ver 4.7);
- 7) ventilación (ver 4.8).

4.2 Riesgos por proteger

Los riesgos en las ventanas varían según el tipo, el uso y ubicación de los inmuebles y también por el valor de las mercaderías que están dentro de los mismos.

Se deben analizar dos tipos de riesgos en los inmuebles de venta:

- a) para la mercadería dentro del local con posibilidades de acceso a través de ventanas a nivel del terreno, particularmente en la parte posterior del edificio o donde hay acceso desde plataformas o techos a ventanas de pisos altos o también por el vidriado del techo;
- b) para la mercadería en vidrieras que puedan estar expuestas a roturas y robos relámpago.

Las oficinas pueden estar en edificios de poca altura hasta en elevadas torres, pero debido a los inmuebles contiguos, en algunos casos, el riesgo de robo es considerablemente mayor. Los edificios con aire acondicionado tienen la ventaja que todas las ventanas son fijas excepto unas pocas que deben ser abiertas en emergencias.

4.3 Conversión de ventanas de abrir en ventanas fijas

Las superficies de las ventanas de abrir son a veces mayores de las necesarias para proporcionar ventilación adecuada. En tales casos, algunas ventanas de abrir podrán ser convertidas en fijas, a menos que ellas sean necesarias por otras razones, como por ejemplo, ventilación para confort en verano, accesos o egresos de emergencia, extracción de humos o para su limpieza exterior.

El método normal para fijar ventanas de abrir por razones de seguridad, es usar tornillos atravesando el marco. Es aconsejable obtener asesoramiento especializado, antes de efectuarlo, para evitar afectar otros comportamientos de la ventana. Por ejemplo, la posición de los tornillos en las barreras térmicas de los marcos metálicos, puede ser crítica.

4.4 Directivas para el diseño de ventanas

4.4.1 Generalidades

Los materiales usados para marcos de ventanas son, generalmente madera, acero, aluminio, hormigón y plástico, algunas veces combinados. El grado de seguridad proporcionado por esos materiales, está directamente relacionado al diseño del sistema de vidriado y la resistencia de las secciones perfiladas de la estructura de la ventana. La resistencia proyectada de los perfiles para ventanas de abrir debe ser tal que los cierres para fijación puedan adaptarse firmemente. Las ventanas y sus bastidores auxiliares, deben ser sujetados a la estructura circundante. Debe evitarse el uso de bisagras exteriores o tornillos expuestos para fijación de pivotes y si son usados no deben ser demontables.

Para el diseño de ventanas relacionado con la seguridad del vidriado ver Sección Sexta.

4.4.2 Marcos de madera

La calidad de la madera en marcos y bastidores debe estar de acuerdo con la norma IRAM 9509. Otros factores que la seguridad debe tener en cuenta cuando se seleccionan las distintas especies de madera son, por ejemplo adaptabilidad para uso exterior o interior, la posible necesidad de tratar las maderas con preservantes (ver normas IRAM 9600, 9600-1 y 9600-2), y la idoneidad para utilizarla como alféizar de ventana o umbral de puerta (ver normas IRAM 11505, IRAM 11506 e IRAM 11507).

4.4.3 Ventanas metálicas

Deben responder a las normas IRAM 11505, IRAM 11507 e IRAM 11530.

4.4.4 Ventanas de aleaciones de aluminio

Deben cumplir con las normas IRAM 11507 e IRAM 11543.

4.4.5 Ventanas de plástico

Los problemas relacionados con el uso de plásticos son similares a los de otros materiales usados como estructura de ventanas en relación a la seguridad. Particularmente es importante la seguridad de las fijaciones de las secciones de los perfiles de plástico al muro adyacente.

4.4.6 Uso de vidriado de seguridad

Su necesidad surge para evitar el ingreso o robo como consecuencia de la rotura de vidrios sea en ventanas de abrir o nó. Cuando dicha prevención requiere el uso de vidrios de seguridad, los marcos deben ser de suficiente resistencia, fijados a la estructura adecuadamente y con rebajes de dimensiones apropiadas para el espesor del vidrio recomendado por el fabricante o el proveedor. Los vidrios de seguridad deben cumplir con las normas IRAM 12556, IRAM 12595 e IRAM 12596.

4.5 Barrotes para ventanas

4.5.1 Generalidades

Aunque las ventanas son consideradas como medio de escape solamente en circunstancias excepcionales, ello puede ser de importancia crítica si por cualquier razón las rutas de escape se tornan infranqueables. De ahí que los barrotes de seguridad que protegen ventanas de abrir presentan serios obstáculos para los medios de escape. Esto ha sido evidente en acontecimientos en los cuales se han producido muchas pérdidas de vidas cuando las personas quedaron atrapadas detrás de ventanas obstruidas y aún, en el mejor de los casos, los rescates fueron posibles solamente después de prolongadas maniobras para cortar los barrotes desde afuera.

Las autoridades competentes son concientes de dichos problemas potenciales y de acuerdo con las prácticas establecidas pueden exigir la remoción de los barrotes cuando sean perjudiciales para la seguridad personal de los ocupantes.

Las ventanas pueden también proveer convenientes medios de acceso en las operaciones para combatir incendios y en el contexto de la protección de la propiedad. Por lo expuesto se recomienda firmemente la consulta con las autoridades de bomberos antes de instalar barrotes en ventanas. También se recomienda hacer constar en los planos de aprobación la instalación de barrotes en las ventanas.

4.5.2 Recomendaciones básicas

Quando deba usarse barrotes en ventanas el mínimo nivel de seguridad exige que se cumpla con lo establecido en 4.5.3/4 y las recomendaciones siguientes:

- a) utilizar barras macizas de alto límite de fluencia o de acero comercial con diámetro nominal no menor que 16 mm o también con dicho lado de sección cuadrada, a distancia no mayor que 125 mm entre centros de barrotes;
- b) disposición de travesaños de planchuelas de acero de dimensiones nominales mínimas de 31,8 x 9,5 mm o sección equivalente a intervalos no mayores que 350 mm;
- c) suplementando la seguridad física con alarmas interiores contra intrusos que adviertan que se ha producido una intrusión.

4.5.3 Fijación a la estructura

4.5.3.1 Método 1. Cuando sea posible los barrotes deben empotrarse cada 500 mm en el interior de la mampostería circundante desplazados hacia adentro, a no menos que 50 mm desde el paramento exterior de la pared. Cada extremo de barra de anclaje debe empotrarse en el hormigón o en la mampostería como mínimo 75 mm. Cuando los barrotes tienen más de 600 mm deben colocarse travesaños que serán soldados en las intersecciones o fijados de otro modo no removible.

También los travesaños se empotran en la mampostería como mínimo 75 mm en cada extremo soldándose en las intersecciones con las barras perpendiculares (ver figs. 1 y 2).

BARROTES PARA VENTANAS

LEONID LLONTOP CASTRO
Jefe de Seguridad Casa Matriz
Banco Ciudad Bs. As.

- ① Barrote
- ② Travesaño
- ③ Barra perpendicular

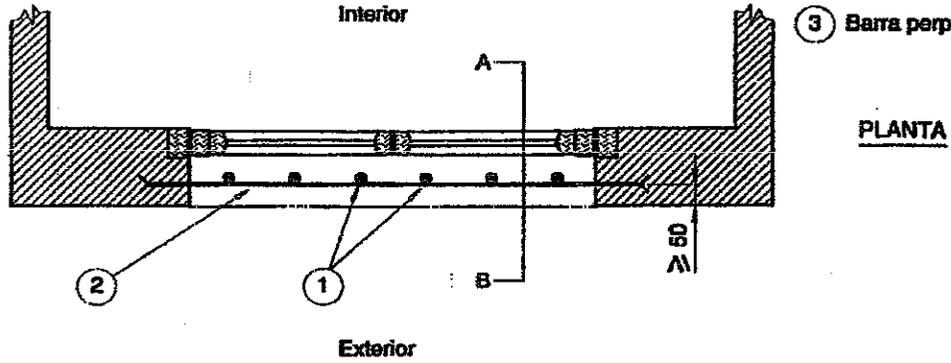
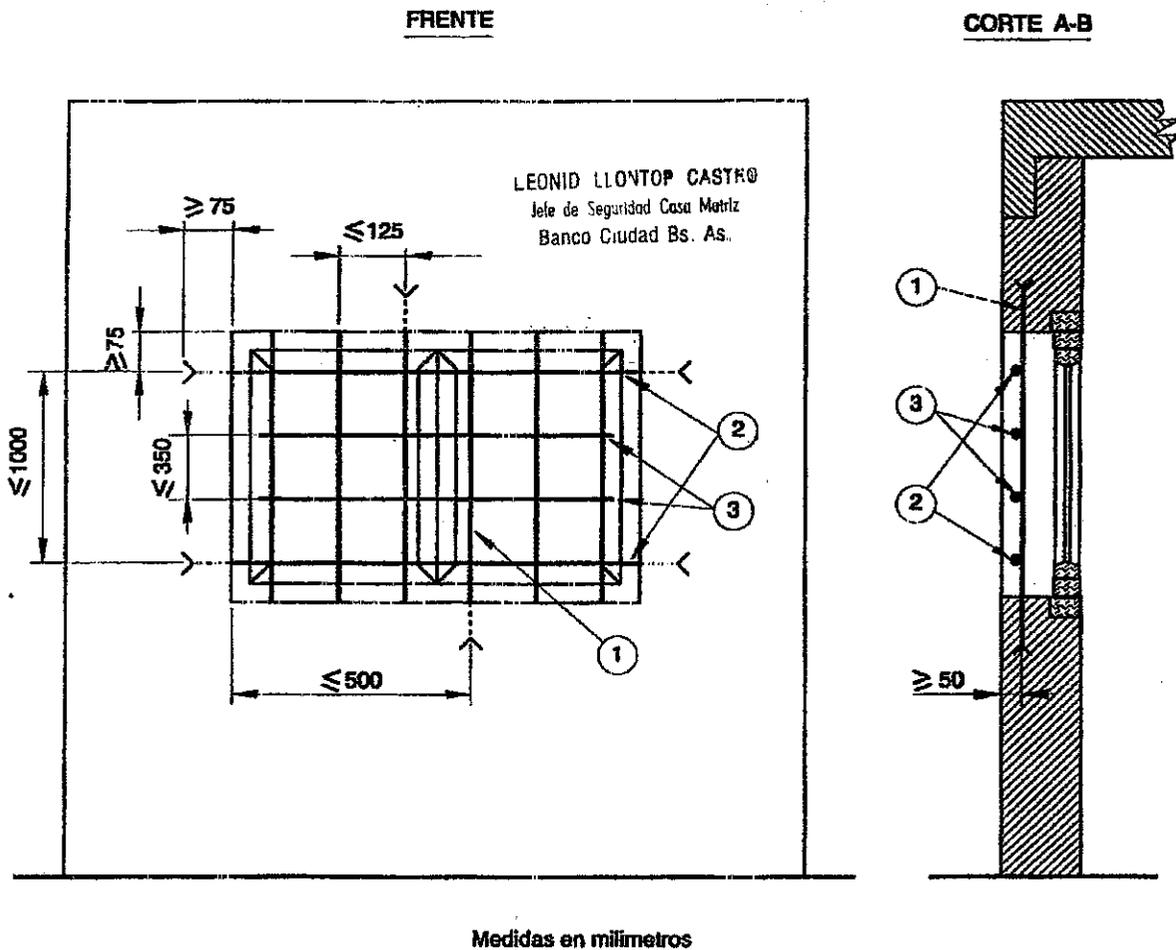


Figura 1 - Barrotes para ventanas



Medidas en milímetros

Las figuras sólo tienen carácter ilustrativo y no pretenden definir diseño

Figura 2

Las figuras sólo tienen carácter ilustrativo y no pretenden definir diseño.

4.5.3.2 Método 2. Cuando no sea posible empotrar los barrotes en la mampostería, los extremos separados de los travesaños en las zonas de anclaje se amuran a distancias no mayores que 1000 mm y como mínimo 75 mm (fig. 3). Los barrotes perpendiculares se deben soldar o asegurar por medios no desmontables en las intersecciones con los travesaños.

PIERSPECTIVA

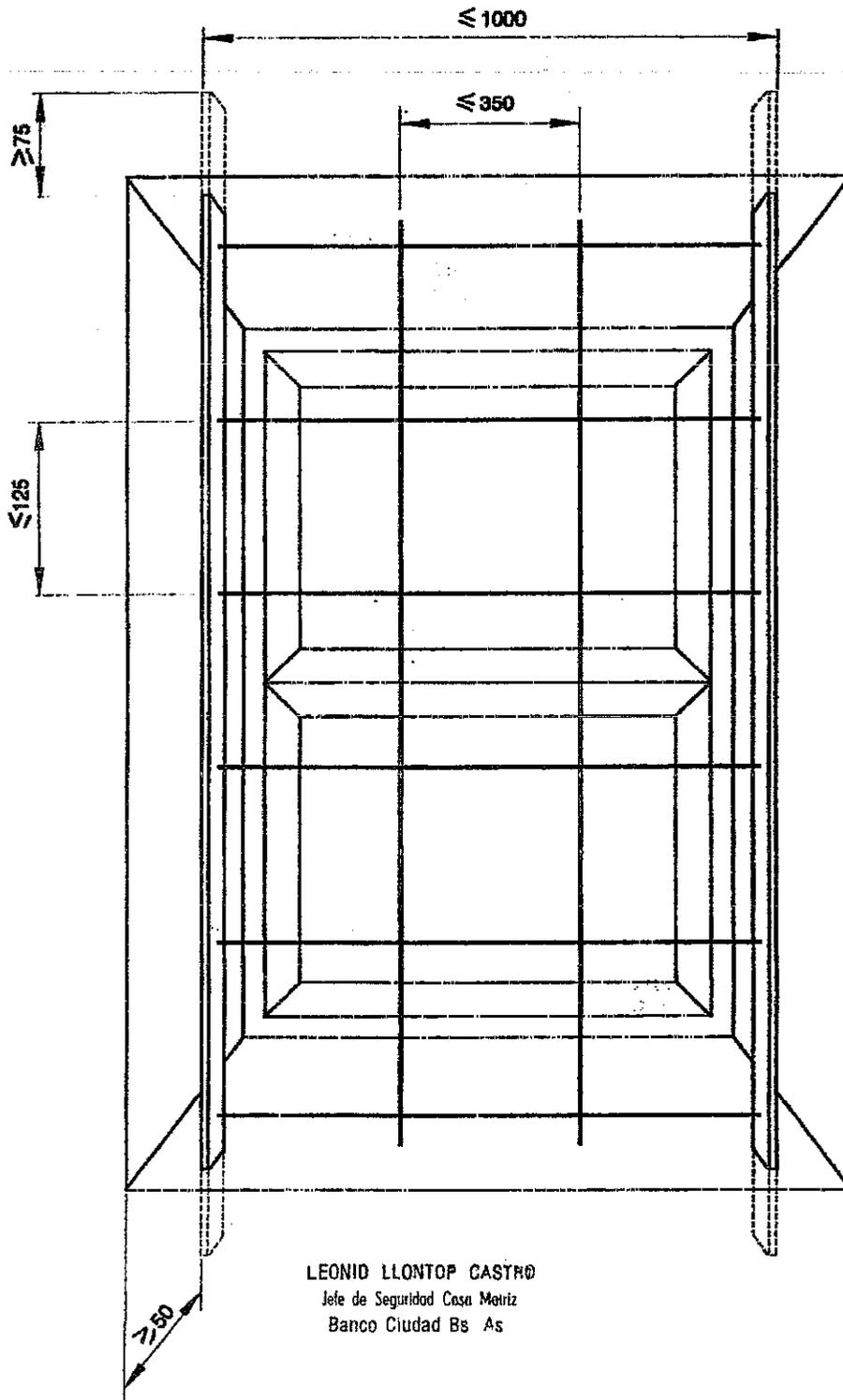


Figura 3

4.5.4 Fijación a ventanas con marcos de madera

Cuando no es factible empotrar en la mampostería las barras, deben ser soldadas en los extremos a un travesaño que es perforado en correspondencia de cada barra y se asegura al marco de madera con tirafondos ajustados con tuercas y arandelas. Las cabezas externas de los tirafondos deben ser embutidas bajo la superficie externa del marco y obturarse con relleno sellador. La resistencia de tal disposición depende también de la fijación del marco a la estructura.

4.5.5 Fijación de ventanas con marcos metálicos

Cuando no sea práctico empotrar las barras en la mampostería, habitualmente es posible fijar las barras a los marcos, pero debido a la variedad de tales marcos, es imposible sugerir un método uniforme de fijación. La fijación depende del material y resistencia del marco y de la sujeción del marco a la estructura.

4.5.6 Fijación a ventanas con marcos de plástico

Los barrotos de ventanas no se deben fijar en marcos de plástico aunque tengan refuerzos metálicos.

4.5.7 Vidriados en techos

Cuando se juzgue que hay riesgo para la seguridad, se evitará en lo posible la disposición de vidriados en los techos. Cuando deban ser instaladas claraboyas, iluminaciones cenitales, cúpulas vidriadas por donde los intrusos puedan acceder, en dichas superficies vidriadas deben adaptarse barrotos de seguridad de acuerdo con lo aconsejado en 4.5.3 y así obtener un razonable grado de seguridad. Los accesorios exteriores deben ser robustos, forrados con chapa de acero y fijados con tornillos o similares que no se puedan desmontar desde el exterior.

4.6 Rejas de ventanas y persianas

4.6.1 Rejas desmontables

Están supeditadas a que conformen con lo planificado. Las vidrieras pueden protegerse con rejas de diferentes tipos que incluyen las desmontables de metal desplegado y de malla soldada. El tipo de reja más adecuado dependerá de la naturaleza de los locales y del tipo y valor de las mercaderías en exhibición. Las barras tubulares son menos seguras que las sólidas pues pueden ser cortadas fácilmente. Las rejas deben ser empotradas internamente, cuando lo son exteriormente se debe tener cuidado de asegurar que no sean fácilmente desmontables.

Las dimensiones de la abertura de la reja dependen, en el caso de los locales de venta, del tipo de mercaderías expuestas.

La altura de la reja debe ser seleccionada teniendo en cuenta factores que incluyen: la altura de la vidriera, nivel del antepecho y otros medios que puedan ser usados como escalones para llegar hasta la reja.

En algunos locales puede ser necesario proveer una protección con rejas desmontables, hechas con metal desplegado o malla soldada con considerable espesor, fijado en un marco ajustado al tamaño de la ventana.

Tales rejas deben ser fijadas internamente por arandelas y tuercas mariposa sobre los extremos roscados de tirafondos fijados a través del marco o empotrados en la mampostería, con las cabezas de los tirafondos por debajo de la superficie vista y tapados con relleno.

Otros métodos de fijación comprenden el uso de candado con eslabones cerrados engrampados mediante los cuales la reja se ajusta, o por bisagras sobre uno de los lados de la reja y asegurados al borde de abrir con candado. La resistencia del marco es importante.

Las rejas más efectivas contra intrusos deben estar enmarcadas con planchuelas de acero que protejan los extremos de las mallas metálicas. No es aconsejable curvar o enlazar mallas pesadas de alambre tejido grueso para asegurarlas sin soldadura en los marcos (habitualmente son de varillas metálicas) ya que los extremos de la malla pueden ser abiertos y permitir el acceso por la ventana. Los extremos de las mallas deben ser soldados por puntos a los marcos de acero.

4.6.2 Rejas artísticas Frecuentemente están hechas de acero forjado y ofrecen un grado de seguridad además de ser decorativas. Sin embargo el diseño no debe crear apoyos para el pié que posibiliten su uso como peldaños de una escalera.

4.6.3 Persianas metálicas. Para la protección de vidrieras y arcadas o pórticos abiertos, en las áreas urbanas especialmente las céntricas, las persianas o cortinas de enrollar externas de acceso pueden considerarse apropiadas.

4.6.4 Persianas de madera. Las persianas de madera fijadas exteriormente no proporcionan un buen nivel de seguridad. La resistencia adicional se logra revistiendo con chapa metálica de espesor no menor que 1,5 mm. Con dicho espesor de chapa se incrementa el peso de la persiana en 12,5 kg/m². Las persianas deben ser aseguradas con una barra transversal y candado u otras trabas seguras.

4.7 Cerraduras de ventanas y pestillos para ventanas de abrir

4.7.1 Generalidades

Cuando el riesgo de la seguridad no es suficiente para justificar la instalación de barrotes, rejas o persianas, o cuando dichas protecciones son inapropiadas, la defensa contra la entrada por la rotura de vidrios para llegar a las manijas u otros herrajes de la ventana, se puede proporcionar instalando pestillos con traba de seguridad.

4.7.2 Especificaciones para ventanas nuevas o de reposición

Las ventanas de abrir para oficinas y locales de venta deben restringirse. Habitualmente las ventanas se hacen a medida y debe considerarse la necesidad de que funcionen con llave o herrajes multitraba. También cuando deben ser reemplazadas debe considerarse lo anterior y reducir la posibilidad de modificar marcos para recibir los accesorios adicionales de seguridad. La eficiencia de tales accesorios debe ser verificada por los proveedores de ventanas.

4.7.3 Cerraduras y pestillos para ventanas existentes

Antes de considerar la instalación de cierres de seguridad en ventanas de abrir, debe verificarse la necesidad de que estén abiertas, y en el caso que sea posible, para alguna de ellas, mantenerla permanentemente cerrada. Hay considerable variedad de mecanismos de cierre para ventanas. Ellos deben ser apropiados al tipo de ventana y la construcción del marco. Las cerraduras son generalmente colocadas en los marcos con tornillos comunes o autorroscantes. En todos los casos debe asegurarse que los extremos de los tornillos cuando se aprietan totalmente no toquen el vidrio.

4.7.4 Cerraduras con llaves comunes y especiales

Estas últimas presentan mayores dificultades que las comunes para destrabar las cerraduras cuando los intrusos rompen vidrios para lograr el acceso a la cerradura de la ventana.

4.7.5 Ventanas pivotantes y a balancin

Cuando las ventanas con bisagra tienen tornillos expuestos ellos deben ser reemplazados por tornillos no desmontables. Los pernos o pasadores exteriores en bisagras o pivotes se aseguran puliendo las cabezas expuestas.

4.7.6 Ventanas corredizas

El diseño de la ventana y sus herrajes deben ser tal en que no sea posible sacar las hojas desde el exterior cuando la ventana está cerrada.

4.7.7 Ventanas tipo celosía

Son ventanas para ventilación con hojas formadas por un bastidor y tablillas inclinadas. Se consideran de alto riesgo para la seguridad y no deben ser usadas en posiciones accesibles desde el exterior. En tal caso deben ser reemplazadas y si es necesario la ventilación que proporcionan debe sustituirse por otros medios. En caso contrario colocar barrotes o rejas de seguridad.

4.8 Ventilación

LEONID LLONTOP CASTRO

Jefe de Seguridad Casa Matriz

Banco Ciudad Bs. As.

4.8.1 Generalidades

Algunas ventanas tienen que proporcionar ventilación. En estos casos pueden colocarse barrotes y los dispositivos de ventilación en el vidrio o en el marco de la ventana. Deberán considerarse en ese caso las corrientes de aire y sus eventuales acciones indeseadas sobre detectores de movimiento del sistema de alarma. También se deben colocar herrajes que restrinjan la abertura de la ventana según el grado de seguridad requerida.

4.8.2 Dispositivos de ventilación

La ventilación puede suministrarse con dispositivos o por aire a presión. Los dispositivos pueden ser:

- a) aquellos que se adaptan en aberturas en paños vidriados;
- b) los ajustados en los bastidores metálicos o de madera de las hojas vidriadas.

Hay que tener en cuenta la seguridad en el diseño y la instalación de dispositivos como los extractores para evitar que las aberturas posibiliten el acceso a los herrajes de la ventana, por ejemplo introduciendo un trozo de alambre por las aberturas para ventilación.

4.8.3 Ventanas de abrir

Las ventanas que no están provistas con barrotes de seguridad y en las que no pueden adaptarse los dispositivos descriptos en 4.8.2 deben ser abiertas para proporcionar ventilación y cuando exista riesgo para la seguridad se deben instalar herrajes de cierre que restrinjan su abertura a un máximo ancho de 100 mm, pero que sin embargo puedan abrirse para su limpieza.

En el caso de ventanas a balancín o pivotantes, la restricción de la abertura puede lograrse con una barra que se traba interiormente en el plano del giro de la hoja.

QUINTA SECCIÓN - PUERTAS EXTERIORES

5.1 Generalidades

Las puertas exteriores deben localizarse a la vista del público y deben estar bien iluminadas para impedir intentos de ingresos ilícitos. Esto interesa particularmente en las puertas de salida final, las cuales no pueden ser abulnadas desde el interior.

5.2 Funciones de las puertas exteriores y control de accesos

5.2.1 Funciones exteriores

Estas puertas en locales de venta y oficinas, pueden desempeñar una o más funciones. El control de los accesos requerido por dichas puertas está regido por sus funciones y además por la naturaleza y tamaño de los locales. Las recomendaciones especiales relacionadas con las funciones particulares son tratadas como sigue:

- a) puertas de salida final para cerrar desde afuera por la última persona que abandona el local (ver 5.2.2);
- b) puertas de ingreso y salida para el personal (ver 5.2.3);
- c) puertas de ingreso y salida para visitantes de las oficinas (ver 5.2.4);
- d) puertas para la recepción y despacho de mercaderías (ver 5.2.5);
- e) puertas para otros servicios indispensables como entrega de combustibles, recolección de basura (ver 5.2.6);
- f) puertas de salida de emergencia (ver 5.2.7);
- g) puertas para ingreso de vehículos (ver 5.2.8).

Además hay recomendaciones referentes a puertas no vigiladas (ver 5.2.9) y puertas resistentes al fuego (ver 5.2.10).

Los proyectistas, los gerentes y administradores necesitan conocer claramente las funciones que debe desempeñar cada puerta y evitar su mal uso. Los cierres y los dispositivos de vigilancia para cada puerta deben ser proyectados de acuerdo con sus requisitos funcionales.

La capacitación del personal es de esencial importancia para mantener la seguridad de las puertas en todo momento apreciando sus funciones y los riesgos del mal uso.

5.2.2 Puertas de salida

Cuando están cerradas deben ser solamente reabiertas mediante el uso de llaves u otros dispositivos de cierre aprobados y deben ser localizadas en áreas bien iluminadas.

5.2.3 Puertas para ingreso y salida del personal

Algunos edificios para oficina y locales comerciales tienen puertas especiales para esa finalidad. En tal caso se debe proveer un acceso supervisado por un encargado o mediante el uso de circuitos cerrados de televisión u otro sistema de control de accesos.

En edificios donde la seguridad sea de gran importancia, ésta puede ser mejorada con sistemas de control de accesos de tecnologías varias. Los sistemas electrónicos estarán siempre complementados por dispositivos electromecánicos o cierres electromagnéticos a los cuales controlarán. Deberán agregarse cerrojos mecánicos para aumentar la seguridad física fuera de los horarios de trabajo.

5.2.4 Puertas para ingreso y salida para los visitantes de oficinas

Estas puertas deben:

- a) estar atendidas por un recepcionista o personal de seguridad debidamente capacitado;
- b) estar bajo continua vigilancia desde una oficina contigua;
- c) mantenerse cerrada debiendo solicitar el ingreso mediante un timbre u otra instalación apropiada como los sistemas de porteros eléctricos. Las puertas suelen tener instaladas mirillas de modo que los visitantes puedan ser reconocidos antes del ingreso.

5.2.5 Puertas para recepción y despacho de mercadería

Son áreas de suma importancia y se tendrá especial cuidado para el proyecto, su distribución interna y la elección de los procedimientos para minimizar los riesgos de sustracciones o daños de las mercaderías.

Las recomendaciones son:

- a) No se permitirá el estacionamiento de vehículos particulares cerca de las áreas de recepción.
- b) El proyecto debe evitar obstrucciones o huecos en donde puedan ocultarse mercaderías.
- c) El área debe estar adecuadamente iluminada (ver sección décima).
- d) Las áreas de recepción y despacho deben estar físicamente separadas.
- e) Las dársenas en las plataformas de carga de los galpones de despacho, deben construirse con las mismas dimensiones de los vehículos y sus acoplados. En sus bordes se colocan defensas de plástico o goma.
- f) Las puertas para el ingreso de peatones y para el acceso a la zona de recepción, deben estar separadas.
- g) La zona de carga no debe ser utilizada como atajo en la entrada y salida del personal.
- h) En las entradas y salidas de las zonas de carga se instalarán puertas y ventanas resistentes. Cuando el área no esté en funcionamiento, las puertas y persianas se mantendrán cerradas con los recaudos técnicos apropiados para evitar su vulneración.

- i) las puertas y/o persianas deben estar provistas de mirillas u otros sistemas de visualización.
- j) se deben realizar todos los esfuerzos para mantener el área ordenada. Las mercaderías descargadas se despejarán del área tan pronto como sea posible, antes de la entrega de nuevas mercaderías.
- k) Los espejos ubicados estratégicamente ayudarán a controlar lugares sin visibilidad.
- l) Las áreas de recepción serán de suficiente tamaño para que las mercaderías sean controladas antes de trasladarlas de la playa de carga a los locales de venta.
- m) Las zonas de recepción deben estar continuamente controladas en las horas del horario de entrega. Las persianas de las bahías de recepción deben mantenerse cerradas hasta que el conductor de un nuevo vehículo haya sido identificado en la puerta de ingreso.
- n) Cuando un área de recepción es adyacente a una pared lindera deben tomarse precauciones especiales de seguridad en las puertas y ventanas para evitar la sustracción de mercaderías.
- o) El circuito cerrado de televisión puede proveer seguridad adicional en el área de recepción de mercaderías.
- p) Deben tomarse disposiciones especiales en la recolección y almacenamiento de escombros y desperdicios para evitar la oportunidad de ocultar mercaderías o crear riesgos de incendio. Las mismas consideraciones se aplica para los pallet o tarimas para cargas y descargas y con los contenedores.
- q) Cualquier instalación de oficina en el área de recepción mercaderías, debe permitir buena visibilidad de la totalidad del área, además de ser segura en sí misma.
- r) Deberá disponerse de un lugar seguro para el archivo de documentos, registros y sellos.
- s) Se deben tomar precauciones con las mercaderías de gran valor colocándolas en un área de seguridad separada mientras esperan su traslado hacia el lugar definitivo dentro de la oficina o local de venta.
- t) Estarán atendidos por un recepcionista o personal de seguridad debidamente capacitado.

5.2.6 Puertas para otros servicios indispensables

Estas puertas tales como entrega de combustibles y recolección de basura, deberán supervisarse apropiadamente todo el tiempo que esten abiertas para llevar a cabo los servicios. La zona de recolección de basura estará separada de las áreas de recepción y despacho de mercaderías.

NORMA IRAM 3860: 1994

LEONID LLONTOP CASTRO
Jefe de Seguridad Casa Matriz
Banco Ciudad Bs. As.

5.2.7 Puertas de salida de emergencia

La señalización de las puertas proyectadas para uso como medio de escape en caso de incendio, se establece en la norma IRAM 10005-1 y 2. Conviene que ellas estén señalizadas siempre por carteles tales como SALIDA DE EMERGENCIA y deben ser reconocidas por todos los ocupantes del edificio.

Se recomienda el uso de un sistema de alarma que indique la apertura de estas puertas.

5.2.8 Puertas para entradas de vehículos

Las oficinas y los locales de venta suelen tener garajes como parte integral de los edificios. La entrada de vehículos deberá hacerse por puertas o portones controlados por un encargado o con dispositivos de seguridad.

En entradas sin vigilancia el personal autorizado a ingresar será provisto de llaves con dispositivos de destrabe o medios electrónicos de control de accesos.

Las puertas o portones deben ser de cierre y traba automática. Los vehículos de los visitantes, solamente serán autorizados cuando sea reconocida su autenticidad por el personal, mediante circuito cerrado de televisión u otros dispositivos de seguridad.

5.2.9 Puertas sin supervisión

Presentan los mayores riesgos para la seguridad. Estas puertas pueden servir a varios propósitos; frecuentemente sirven al personal como atajos para entrar o salir del edificio.

Se debe advertir al personal para que permanezcan cerradas una vez utilizadas. Deben ser de cierre y traba automática después de ser abiertas y no deben ser operables desde el exterior por personas no autorizadas.

Un sistema de alarma cuando las puertas han quedado semiabiertas, colaborará para evitar el ingreso de intrusos al alertar al personal de seguridad. Se recomienda que este sistema esté provisto de detectores de cerrojo que efectivamente sensen la penetración de los pernos y la reporten al personal de seguridad.

5.2.10 Puertas resistentes al fuego

Estas puertas estarán señalizadas mediante carteles con las palabras "Puerta Contra Incendio Mantener Cerrada" o con leyendas similares y cumplirán con la norma IRAM 3570. Cualquier tipo de dispositivo de seguridad instalado en una puerta contra incendios no debe disminuir su resistencia al fuego por debajo de la requerida. Los dispositivos montados superficialmente es poco probable que causen problemas importantes, a menos que los tornillos o pernos de fijación penetren profundamente en la estructura de la puerta.

Las fijaciones que atraviesan completamente la puerta no son aconsejables. Quitar una sección del marco de la puerta para insertar cualquier dispositivo, puede arriesgar su resistencia al fuego.

5.3 Vulnerabilidad de las puertas a las embestidas

Los intrusos, frecuentemente, aprovechan las debilidades de las puertas para lograr el acceso. Por lo tanto, es deseable que el número de puertas exteriores de los inmuebles, se mantenga en un mínimo. Las hojas y marcos de las puertas, como mínimo deben ser resistentes a las embestidas con los hombros y con las piernas.

Las debilidades que los intrusos pueden aprovechar, son:

- a) marcos y hojas de puertas débiles;
- b) fijación inadecuada a los marcos de la estructura circundante;
- c) cerradura, pestillos y pernos no proyectados para proporcionar resistencia contra las embestidas;
- d) bisagras débiles o en número insuficiente en puertas de abrir. Las puertas que abren hacia el exterior, son más vulnerables, porque los pasadores de las bisagras son accesibles para el asaltante.

5.4 Construcción e instalación de puertas y marcos

5.4.1 Generalidades

Las puertas exteriores deben construirse con materiales resistentes para hacer barreras apropiadas contra los intrusos.

5.4.2 Puertas y marcos de madera

5.4.2.1 Generalidades

Con respecto a la calidad de la madera, ver norma IRAM 9509 y para el tratamiento y la preservación las normas IRAM 9600 e IRAM 9601. Sobre requisitos de puertas exteriores ver la norma IRAM 11507.

5.4.2.2 Marcos

Los marcos deben tener como mínimo espesor en la parte rebajada 18 mm y deben tener superficie sección transversal para resistir y embutir la caja de la hembra del cerrojo. Las jambas de los marcos deben ser fijadas a cada lado a 450 mm entre centros en los vanos. También es recomendable fijaciones en el cabezal del marco. Los tipos de fijaciones no deben causar astillado ni perjudicar el anclaje con las variaciones climáticas y el transcurso del tiempo.

5.4.2.3 Hojas de puertas

Deben ser de 44 mm de espesor mínimo y construidas con madera maciza o de núcleo sólido. Los montantes del bastidor, para las hojas, deben tener 120 mm de ancho mínimo para permitir alojar cerraduras y otros cerrajes de seguridad. El máximo espesor de cerraduras embutidas es de 20 mm para hojas de 44 mm. En algunos casos, como refuerzo, se pueden colocar chapas empernadas desde el interior de la hoja.

5.4.3 Puertas y marcos metálicos

5.4.3.1 Requerimientos constructivos

Deben cumplirse con las normas IRAM 11507, IRAM 11524 e IRAM 11543. Los tableros y los travesaños de cerradura, deben ser de chapa de acero de espesor mínimo de 1,6 mm y deben tener fijaciones cubiertas. Las secciones de los marcos deben permitir el encaje de pestillos y trabas de seguridad. Por otra parte, deben rellenarse las secciones huecas de los marcos metálicos, junto a las obra circundante.

5.4.3.2 Bisagras

Los pasadores no deben ser removibles y las aletas deben ocultarse. Las aletas visibles deben ser remachadas o fijadas con tornillos de cabezas dentadas no reversibles.

5.4.3.3 Fijación de cerraduras

Cuando el espesor del material es insuficiente para el roscado, deben utilizarse dispositivos para la fijación de cerraduras que no deben ser removibles desde el exterior. Hay que limar las salientes de los pernos, para evitar el apalancamiento entre hembra y macho de las cerraduras.

5.5 Cerraduras y otros herrajes

LEONID LLONTOP CASTRO
Jefe de Seguridad Casa Matriz
Banco Ciudad Bs. As.

5.5.1 Generalidades

Siempre conviene consultar a cerrajeros y expertos en seguridad, sobre la eficiencia de los sistemas de cerradura existentes y nuevos. La variedad es muy grande, desde las cerraduras comunes hasta las de puntas múltiples. La tecnología en cerraduras está evolucionando continuamente. Cuando sea posible, las cerraduras deben ser operables con llave, tanto desde el interior como del exterior para que los asaltantes no puedan escapar fácilmente usando las puertas. Sin embargo, hay restricciones para ello, en puertas de salida de emergencia.

5.5.2 Candados y travesaños

Cuando no es importante la apariencia, la seguridad puede ser incrementada instalando travesaños de acero en todo el ancho asegurados con candado.

5.5.3 Buzones

Es preferible ubicarlos en las paredes, suficientemente alejados de puertas y ventanas. Cuando deben ser instalados en puertas, se posicionarán a más de 400 mm de la cerradura y con una caja interna o canasto de chapa metálica que dificultará el acceso a la cerradura.

5.5.4 Mirillas y cadenas limitadoras

Las mirillas son necesarias en ciertos locales para permitir el reconocimiento de los visitantes con las puertas cerradas. Si tienen un visor gran angular posibilitarán la completa visión de los clientes. Para ello, los espacios exteriores deben estar adecuadamente iluminados. Las cadenas limitadoras de puertas son una protección contra la entrada forzada cuando la puerta está sin llave.

5.6 Cierre y traba de las puertas exteriores

5.6.1 Generalidades

La eficiencia de los cierres de las puertas exteriores, no depende solamente del diseño sino de su correcta instalación por personal especializado.

5.6.2 Categorías de puertas

Considerando el cierre y la traba, las puertas pueden dividirse en tres categorías:

- a) Puertas de salida final que deben trabarse desde el exterior.
- b) Puertas de salida de emergencia, que no deben ser cerradas con llave cuando los locales a que sirven están ocupados.
- c) Otras puertas que deben ser aseguradas desde el interior de los locales.

El método de cierre y traba está influenciado por el funcionamiento y por los materiales de la puerta.

Los modos de funcionamiento, varían entre:

- 1) abisagradas con apertura hacia el interior o exterior de simple o doble hoja;
- 2) de vaivén con apertura hacia el interior o exterior y de doble acción, admitiendo empuje o tiro, también son simples o doble hoja;
- 3) corredizas de simple o doble hoja;
- 4) plegadizas y corredizas;
- 5) giratorias o rotativas;
- 6) de movimiento vertical ascendente.

LEONID LLONTOP CASTRO
Jefe de Seguridad Casa Matriz
Banco Ciudad Bs. As.

5.6.3 Puertas de salida final

La necesidad de que estas puertas estén trabadas desde afuera las hace más vulnerables que las que pueden ser aseguradas desde el interior de los locales. El tipo más seguro es el de simple hoja con apertura hacia adentro construida con madera sólida o chapas de acero ubicadas en una posición en la cual un intruso no pueda intentar forzarla sin ser observado.

5.6.4 Puertas de salida de emergencia

Cuando estas puertas en un edificio ocupado deben ser aseguradas contra la apertura desde el exterior, deben funcionar con un pestillo accionado desde el interior con una manija convencional.

5.6.5 Cortinas enrollables para puertas y portones

Es una protección adicional para vanos ubicados en la parte posterior de la fachada del edificio. Se instalan cortinas enrollables o portones tipo persiana que deben ser trabados.

Mientras los inmuebles están ocupados por público y personal dichas cortinas y portones enrollables deben estar trabados en su posición abierta.

5.7 Incremento de la seguridad en puertas existentes

5.7.1 Generalidades

Algunas puertas no son suficientemente robustas para alojar el embutido de cerraduras y otros accesorios de seguridad. Esto es frecuente en puertas metálicas y vidrieras donde la instalación de herrajes es dificultosa siendo necesario asesorarse con cerrajero experto.

5.7.2 Medidas para mejorar la seguridad

LEONID LLONTOP CASTRO
Jefe de Seguridad Casa Matriz
Banco Ciudad Bs. As.

Se deben considerar los medios siguientes:

- a) Mejorar la fijación del marco y la chapa hembra del cerrojo embutido en la mampostería.
- b) Instalar más bisagras según las características de la puerta.
- c) Aumentar el diámetro de los pernos de las bisagras externas.
- d) Reemplazar cerraduras existentes por otras más seguras.
- e) Agregar cerraduras adicional a resortes y pestillos accionados por llaves.
- f) Instalar alarmas contra intrusos.
- g) Verificar la efectividad de los herrajes contra entradas forzadas rompiendo paneles vidriados.
- h) Instalar rejas decorativas.
- i) Colocar refuerzos de acero en la partes adyacentes a las cerraduras embutidas.
- j) Revestir exteriormente la puerta con una chapa de acero de 1,6 mm de espesor. La chapa de revestimiento, debe ser empernada con tirafondos a través de la puerta a 150 mm entre centros o puede ser asegurada con tornillos trabables de cabeza endentada a 100 mm entre centros. El revestimiento de chapa debe ser plegado alrededor de los bordes de la puerta para reforzarla. Los tornillos de fijación deben quedar ocultos cuando la puerta está cerrada.

5.8 Llaves maestras

5.8.1 Generalidades

En lugar de disponer de llaves individuales para cada puerta se puede planificar las necesidades de un usuario en particular y entregarle una llave que permita el acceso a toda el área, donde el poseedor está autorizado a entrar. El usual llavero con la multiplicidad de llaves se evita.

5.8.2 Ventajas y desventajas

Las ventajas del sistema de llaves maestras son:

- a) se incrementa la utilidad del uso de cerraduras;
- b) la seguridad se aumenta como consecuencia de las ventajas para la guardia que patrulla la zona y la necesidad de distribuir menos llaves al personal del área.

Las desventajas:

- a) hay más llaves en circulación para una determinada puerta;
- b) el número de combinaciones de llaves es reducida;

En muchos edificios las ventajas pesan más que las desventajas, siempre que:

- 1) se planifique cuidadosamente el sistema de llaves maestras con la completa cooperación del fabricante, cerrajero competente y del usuario final;
- 2) se utilice el sistema para restringir la duplicación de llaves;
- 3) se adopte un eficiente sistema operacional de las llaves maestras. Con estos medios, la reducción en la seguridad, será mínima.

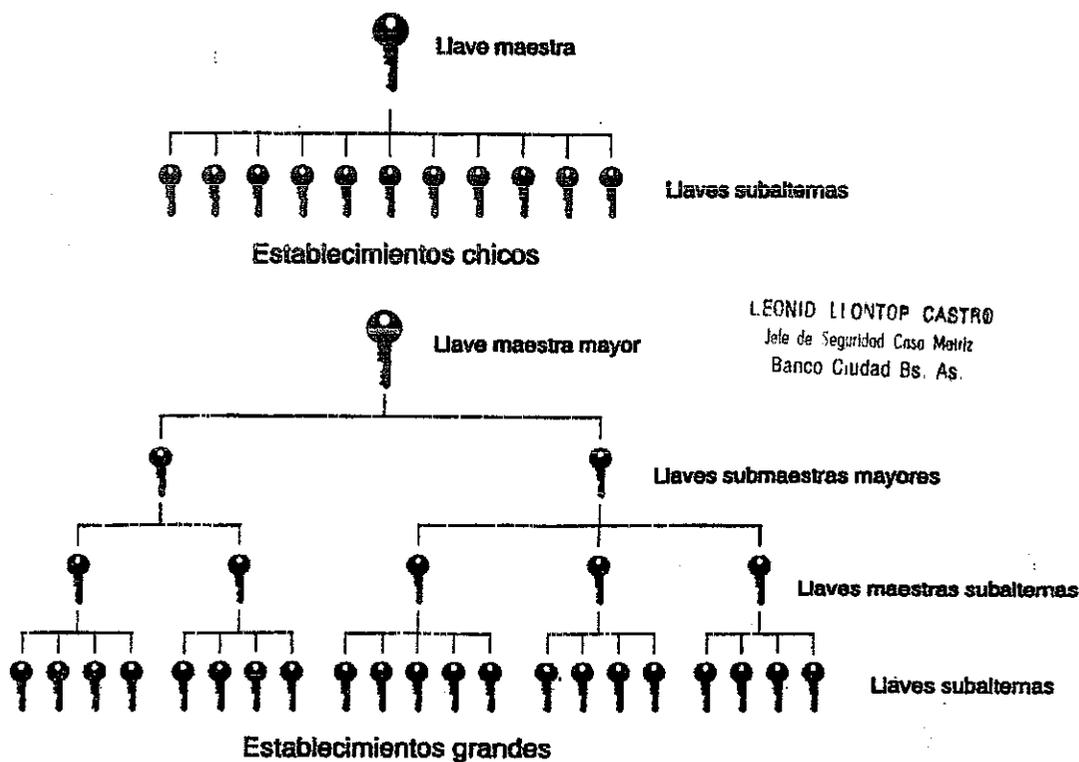


Figura 12a - Sistemas de llave maestra

SEXTA SECCIÓN - VIDRIOS Y VIDRIADOS DE PLANCHAS PLASTICAS

6.1 Generalidades

El compartimiento del vidriado bajo cualquier tipo de carga depende del tipo del vidrio, espesor, tamaño del paño y condiciones de apoyo. En lo referente a la seguridad, la principal consideración es la facilidad con la que el paño puede ser roto o removido proporcionando accesos a las cerraduras u otros herrajes de seguridad de puertas y ventanas o, inversamente el grado en que el paño actúa como barrera para la penetración.

6.2 Comportamiento de diferentes tipos de vidrios

Los diferentes tipos de vidrio, se tratan en la norma IRAM 91311 y los vidrios de seguridad en las normas IRAM 12556, IRAM 12595 e IRAM 12596.

6.2.1 Vidrio recocido.

Normalmente cuando es sometido a un impacto, con una energía que depende del tamaño y espesor del paño, se romperá con bordes afilados. La aplicación de una capa o película apropiada, incrementa la resistencia a la penetración en el vidrio recocido.

6.2.2 Vidrio armado.

La malla de acero, una vez roto el vidrio, puede ser cizallada con bajos niveles de impacto. El vidrio armado no es considerado una barrera para la seguridad.

6.2.3 Vidrio templado.

Su resistencia está relacionada con el espesor de la capa de compresión superficial producida durante el proceso de endurecimiento. Este vidrio, es resistente al impacto de objetos desafilados. Pero una vez fracturado no actúa como barrera.

6.2.4 Vidrio laminado.

Este vidrio compuesto puede ser resistente a un amplio rango de ataques y hasta utilizarse como antibalas. Si bien es posible fracturar una de las capas de vidrio, según el espesor y el tipo de intercapas de plástico, resulta extremadamente difícil penetrar en su totalidad el paño compuesto y se considera barrera.

6.2.5 Doble vidriado.

Puede ser formado por:

- a) dos o más paños de vidrio herméticamente sellados en su periferia. Presenta así dos o más paños para el intruso;
- b) ventanas dobles en el mismo vano. Los paños vidriados pueden ser contruidos con los tipos de vidrio mencionados en 6.2.2/4 suministrando similares impedimentos. Es necesario que la ventana secundaria interior sea segura contra ataques.

LEONID LLONTOP CASTRO
Jefe de Seguridad Casa Matiz
Banco Ciudad Bs. As.

6.2.6 Vidriado con chapas de material plástico

El comportamiento dependerá del tipo de polímero, espesor y condiciones de apoyo. Debe solicitarse asesoramiento al productor con respecto a la seguridad proporcionada.

6.3 Selección del vidriado

Hay que tener en cuenta el uso de los locales considerados, la atracción de la mercadería y el nivel de ataque previsto. Cuando se juzga necesario incrementar la seguridad, hay que recurrir al vidrio laminado compuesto con láminas plásticas. También puede decidirse utilizar otros dispositivos de seguridad como rejas o persianas.

6.4 Areas vidriadas que necesitan consideración especial

6.4.1 Vidrieras de locales

En muchos casos, se utiliza vidrio flotado grueso y el grado de seguridad puede ser incrementado.

- a) Con vidrio laminado.
- b) Incorporando una pantalla secundaria suspendida de vidrio templado o laminado. La pantalla debe ser suspendida aproximadamente 150 mm detrás del vidrio exterior y las cadenas de suspensión deben ser diseñadas y fijadas para permitir movimientos restringidos y absorber los impactos de objetos lanzados.

6.4.2 Vidrieras en fachadas o escaparates

Los vidrios en puertas y ventanas son las partes más vulnerables en una vidriera de fachada. El vidrio recocido de espesor mínimo 10 mm ofrece un razonable grado de resistencia, dependiendo del área del paño.

6.4.3 Paneles corredizos

La seguridad de estos paneles en vitrinas, kioscos, puede presentar problemas. Debe tenerse especial cuidado a los vidriados y la estructura del sistema deslizante y el tipo de herraje instalado.

6.4.4 Puertas vidriadas

La necesidad del uso de vidrios de seguridad puede reducirse si la rotura del panel no permite el acceso, ni al local ni a la cerradura de la puerta.

6.5 Vidriado

Los materiales descritos en 6.2 deben ser utilizados según la especificado en las normas IRAM 12595 y 12596. En todos los casos los vidrios deben ser fijados a la estructura de tal manera, que no puedan ser removidos desde el lado exterior.

Cuando se reemplaza la superficie vidriada para aumentar la seguridad, debe cuidarse de que el otro material posea como mínimo la resistencia al fuego requerida.

**SÉPTIMA SECCIÓN - OTROS PUNTOS DE ACCESO, TECHOS, CERCOS, PORTONES
Y BARRERAS PARA EL TRÁNSITO**

7.1 Acceso a través del techo

El acceso de delincuentes debe ser minimizado o impedido, con la inclusión de las medidas siguientes:

- a) restringiendo el acceso a la parte superior del techo, con barreras físicas;
- b) instalando metal desplegado o de malla soldada debajo de la cubierta del techo o dentro del espacio del techo;
- c) iluminación estratégica del área del techo;
- d) aplicación de pintura antitrepanadora.

LEONID LIONTOP CASTRO
Jefe de Seguridad Casa Matriz
Banco Ciudad Bs. As.

Todas estas medidas pueden ser complementadas por circuitos de alarma protegiendo los accesos al techo.

7.2 Aberturas en techo

En el caso que sean necesarias deben ser tratadas de la misma forma que las aberturas en las paredes de los locales.

Muchos edificios están provistos de sistemas automáticos de ventilación en techos. Están diseñados para liberar el calor, el humo y el fuego automáticamente en el caso de incendios reduciendo la propagación del fuego y mejorando las condiciones para el combate del incendio.

Las fijaciones externas deben ser robustas y cubrirse con chapas metálicas con tornillos de cabeza trabable. La estructura del techo para montar las fijaciones y aberturas en el techo, deben ser de construcción resistente. El método de fijación de rejillas de ventilación, debe impedir su remoción exterior.

7.3 Cielorrasos y pisos suspendidos. Conductos para ventilación y otros servicios.

Esta zona con espacios huecos, pueden ser utilizadas para intentos delictivos. Necesitan protecciones para prevenir el ingreso de intrusos; ya sea barreras físicas o instalando alarmas que detecten entradas en dichos espacios.

7.4 Puertas de sótanos

Deben ser de robusta construcción, sean macizas o enrejadas y sus mecanismos de cierre deben ser seguros y también soportarán su peso. Cuando el uso actual del local no justifique la existencia, se analizará el sellado permanente de la abertura.

7.5 Conductos externos de desagüe

Si bien es preferible que esos conductos estén empotrados en la obra, hay ocasiones donde no es posible y en tales casos la protección se logra colocando algunas formas físicas de obstrucción, como: clavos, alambres de púas y en cañerías ascendentes, la aplicación de pintura antitrepanante.

7.6 Cerco perimetral

Son medidas útiles para la seguridad. De acuerdo al tipo de protección requerida, puede ser:

- a) cerco de mampostería;
- b) cerco de placas y postes de hormigón armado;
- c) estacado con chapa de acero;
- d) cerco de alambre tejido con postes de hormigón o de acero.

LEONID LLONTOP CASTRO
Jefe de Seguridad Casa Matriz
Banco Ciudad Bs. As.

La iluminación estratégica agrega seguridad a los cercos. Cuando se requiera se incorporarán sistemas de alarma contra intrusos.

7.7 Portones

La altura, diseño y construcción debe corresponder a la del cerco adyacente. Las bisagras deben ser protegidas para evitar el levantamiento de las hojas del portón. El cerco y el portón con su diseño deben impedir que los intrusos los usen para escalar. Las cerraduras de los portones deben ser adecuadas a su características y pueden complementarse con candados.

7.8 Porterías

Cuando haya importante flujo de vehículos con mercaderías, pueden ser apropiadas casillas vigiladas para controles separados de los peatones, sean visitantes o personal.

7.9 Barreras para el tránsito

Restringen las extradas no autorizadas de vehículos o personas pueden ser:

- a) brazos pivotantes giratorios;
- b) planchas de elevación instalados a niveles del suelo;
- c) puertas giratorias;
- d) sistemas inteligentes de control accionados con tarjetas magnéticas.

Las puertas pueden ser controladas manual o automáticamente con controles localizados o remotos.

La instalación de barreras no deben dificultar el acceso para combatir incendios y servicios de emergencia. También en el proyecto de estas instalaciones se reitera la necesidad de considerar el acceso de personas discapacitadas y niños.

OCTAVA SECCIÓN - VIGILANCIA ELECTRÓNICA Y SISTEMAS DE ALARMA

8.1 Circuito cerrado de televisión

8.1.1 Generalidades

Debe ser considerado como complemento y no reemplazante de otras medidas de seguridad. Es de uso simple, silencioso y actúa como elemento disuasivo para intrusos, sin exponer al operador a los peligros potenciales.

8.1.2 Elección del sistema del circuito cerrado de televisión

Los factores que intervienen son:

LEONID LLONTOP CASTRO
Jefe de Seguridad Casa Matriz
Banco Ciudad Bs. As.

- a) necesidad de una clara imagen con buen contraste;
- b) confiabilidad del sistema;
- c) vigilancia requerida diurna, nocturna, interna, externa;
- d) tipo de riesgo a ser protegido y pérdidas potenciales;
- e) localización, distribución del edificio, iluminación y entorno vecinal.

8.1.3 Accesorios

La utilidad de las cámaras del sistema de C.C.T.V puede acrecentarse mediante varios accesorios

- a) elección de lentes: normal, gran angular, teleobjetivo y de gran luminosidad;
- b) accesorios para que la cámara pueda girar y moverse hacia arriba y abajo;
- c) sensores de alarma;
- d) contactos secuenciales, por la cual varias cámaras pueden ser vistas sobre el mismo monitor en rotación;
- e) registradores del tiempo transcurrido;
- f) luz infrarroja;
- g) : videograbadores especiales para registro de largos periodos.

8.1.4 Calidad de la imagen

Depende de la luz y de la sombra en el área observada. Ello varía en los diferentes momentos del día. La cámara puede tener lentes de ajuste automático en condiciones variables de iluminación de la escena.

8.1.5 Vigilancia continua de los monitores

Esto puede significar una tensión para el observador, a lo que hay que añadir que su atención puede ser alejada de la pantalla por otras obligaciones. Un detector de movimiento puede incorporarse para activar una alarma cuando aparece un movimiento sobre una pantalla previamente estática.

8.1.6. Transmisión de señales

Para transmitir desde una cámara a un monitor de TV, para distancias cortas (hasta 150 m) pueden utilizarse la vía coaxil y para distancias mayores, un núcleo de fibra óptica.

8.2 Sistemas de alarma contra intrusos

8.2.1 Generalidades

Las medidas de seguridad se mejoran con la detección electrónica de intrusos que usualmente se diseña para percibir la entrada a través de puertas y ventanas, detectando también el movimiento de personas dentro de ciertas áreas del edificio. Estos sistemas no sustituyen las otras medidas físicas de seguridad (ver norma IRAM en estudio 4171-1, IRAM 4171-2 e IRAM 4172).

8.2.2 Interferencia con el sistemas de alarma contra incendio

Cuando en el edificio hay un sistema de alarmas contra incendios se debe cuidar que la señal audible dada por el sistema de alarma contra intrusos no produzcan interferencias con las alarmas contra incendio y sean claramente distinguidas (ver norma IRAM 3730 en estudio).

NOVENA SECCIÓN - AREAS Y ACTIVIDADES DE ALTO RIESGO

9.1 Manejo de dinero y oficinas con efectivo

9.1.1 Generalidades

El manejo del dinero debe efectuarse en oficinas inaccesibles al público, o por lo menos ocultas a la vista. Deben ser equipadas con alarmas fácilmente accesibles. El personal debe ser instruido sobre los procedimientos establecidos en emergencias. Las actividades como contar el dinero en efectivo y el ensobrado de sueldos deben ser ejecutados lo más rápidamente posible y los puntos de acceso deben estar protegidos y vigilados. Mantener dinero en el edificio fuera de las horas de trabajo, debe ser restringido y si resultare necesario guardarlo en caja de seguridad.

9.1.2 Movimiento de dinero

Esta información debe ser dada solamente al personal directamente involucrado y esas disposiciones deben ser frecuentemente combinadas. Las rutas diarias para recolección y entrega de dinero deben ser decididas antes de cada viaje. Es aconsejable efectuar más de un depósito bancario diario para reducir el monto transportado. Cuando sea posible deben ser utilizadas compañías especializadas en el transporte del dinero.

9.2 Cámara de seguridad

9.2.1 Generalidades

Debe ser recabado el asesoramiento en la localización de este compartimiento, en la etapa de proyecto. En el caso de paredes medianeras hay que considerar si los locales adyacentes son fácilmente accesibles y si están desocupados. Las aberturas en los muros y las puertas posibilitan ataques con explosivos.

Deben tomarse cuidados especiales cuando estas cámaras se instalen en el perímetro del edificio, con el objeto de facilitar la transferencia de dinero para su transporte. Debe haber un control estricto en la utilización de llaves de acceso.

9.2.2 Construcción

Es un trabajo para expertos; durante el período de construcción se debe cuidar que personas no autorizadas tengan acceso para conocer los dispositivos de seguridad instalados. Las cámaras de alto grado de seguridad no tienen que tener otra abertura que las puertas, las salidas de emergencia, si se requieren deben ser de la misma resistencia que las puertas principales.

9.2.3 Cámaras de seguridad existentes

Es difícil modificar las estructuras existentes al nivel correspondiente a las necesidades actuales. Muchas cámaras están situadas en sótanos donde un asalto puede llevarse a cabo sin ser observado. Pueden lograrse refuerzos con el uso de bloques y otros premoldeados de hormigón y robustas puertas siempre que la pérdida de volumen del cuarto sea aceptable.

9.3 Cajas fuertes

LEONID LLONTOP CASTRO

Jefe de Seguridad Casa Matiz
Banco Ciudad Bs As.

9.3.1 Generalidades

Es importante que las combinaciones de las llaves y otros medios sean estrictamente controlados. Se sobreentiende que las cajas sean resistentes al fuego. Cuando los riesgos actuales a cubrir lo determinen deben reemplazarse las viejas cajas fuertes.

9.3.2 Localización en lugares despejados

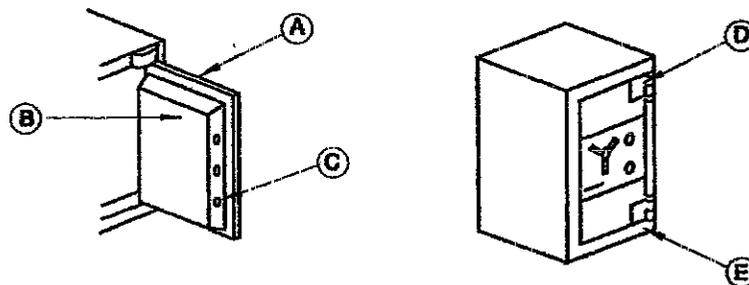
Cuando sea factible deben ubicarse las cajas de seguridad en posiciones visibles a las patrullas policiales, al personal de seguridad, serenos y si es posible al público. Son recomendados paneles vidriados y aberturas de observación en muros ciegos. Cuando no es posible visión directa pueden instalarse espejos para observar la caja y sus adyacencias. Las cajas deben ser colocadas junto a una sólida y ser abulonadas a una estructura resistente en el piso.

9.3.3 Cajas de seguridad bajo piso

Es esencial un buen ocultamiento que puede ser logrado con los usuales revestimientos de piso. Conviene localizarlas en la esquina del local para hacer más difícil el asalto. La instalación no debe disminuir la resistencia al fuego establecida por las reglamentaciones vigentes.

9.3.4 Cajas empotradas de pared

No proporcionan adecuada protección si se encuentran a la vista. Además debe cuidarse que no afecten la resistencia al fuego requerida de la pared.



LEONID LLONTOP CASTRO
Jefe de Seguridad Casa Matriz
Banco Ciudad Bs. As.

9.3.5 Protección de alarmas contra intrusos

En los locales donde un sistema de alarma esté instalado, o en estudio debe asegurarse que toda caja fuerte se ubique en el área protegida. Los detectores acústicos instalados en el ojo de la cerradura sirven para dar señales de vibraciones o sonidos producidos por intento de accesos forzados.

9.4 Robo de información

La información puede ser técnica o financiera, flujo de efectivo, correspondencia y registros de personal. El sistema de computación tienen gran riesgo pues contiene en su memoria datos accesibles en la pantalla o en su impresora.

Las medidas de seguridad son de tres clases:

- a) protección de software con escritura y lectura en clave;
- b) control del acceso al ámbito de la sala de computación usando por ejemplo tarjetas electrónicas u otros medios de seguridad;
- c) protección contra medios electrónicos escuchadores furtivos.

DÉCIMA SECCIÓN - ILUMINACIÓN

10.1 Generalidades

Uno de los objetivos de un delinciente es permanecer sin ser detectado. La protección de la oscuridad debe ser impedida con la iluminación de seguridad.

10.2 Necesidad de iluminación de seguridad

La provisión de una iluminación de seguridad amplía el alcance de la supervisión. La iluminación de seguridad puede ser un sistema destinado a desempeñar solamente una función, pero a menudo responde a un doble propósito. La instalación de iluminación de la exhibición de un local puede también utilizarse para seguridad. La iluminación proyectada puede ser decorativa y a su vez facilitar el trabajo exterior y tener un rol de seguridad. De este modo la seguridad puede resultar sin ningún costo adicional, implicando solamente los costos operativos adicionales en las horas de inactividad comercial.

10.3 Estrategia

LEONID LLONTOP CASTRO
Jefe de Seguridad Casa Matriz
Banco Ciudad Bs As

10.3.1 Generalidades

El objetivo básico de la iluminación de seguridad es el de evitar el encubrimiento de la oscuridad. Esto dependerá de varios factores relacionados con la distribución del inmueble a proteger y los procedimientos de supervisión adoptados.

Cuando la supervisión se efectúa con patrullas externas puede elegirse una iluminación externa o interna.

Cuando el edificio está separado, la iluminación alrededor del perímetro, dirigida hacia adentro, revelará a los intrusos ya sea directamente o por su silueta, dependiendo de qué lado se encuentran con respecto a la iluminación. La iluminación de áreas críticas que pueden ser vistas desde el exterior (vestibulos de entrada, corredores, escaleras y salones de ventas) permitirá la observación del movimiento de los intrusos en el interior.

Para los edificios con patrulla interna de seguridad hay diferencias fundamentales. La iluminación externa deberá dirigirse hacia afuera del edificio, de modo que los intrusos que se aproximan sean vistos rápidamente desde el interior. El encandilamiento es útil para dificultar la visión del intruso, pero debe tomarse en cuenta para que ello no se convierta en una molestia para el público o peligro para los conductores que pasar por el lugar. Cuando se usa una iluminación interna, ésta deberá planificarse de modo que la patrulla nunca tenga que entrar en un área oscura. Eso evitará el uso de linternas, que pueden revelar la presencia de la patrulla, dando tiempo a que los asaltantes se evadan.

No siempre la iluminación interna es apropiada para la seguridad. Con la estrategia básica se debe asegurar que todos los medios de ingreso y egreso estén iluminados. Puede resultar la necesidad de proveer una iluminación adicional para algún punto de acceso que pudiera poner en peligro la seguridad del perímetro.

10.3.2 Oficinas

El equipamiento de oficinas es frecuentemente de gran valor. La mayoría de las oficinas pequeñas a medianas confían en cerraduras, seguros y sistema de alarma para su protección. Se puede aumentar la efectividad agregando una iluminación de seguridad. Debe proporcionar una iluminación interna en los puntos importantes donde se pueda ver el movimiento desde el exterior (escaleras, corredores, vestíbulos, locales perimetrales). Los edificios más grandes pueden tener una patrulla de seguridad. El trayecto y los horarios de la patrulla deben ser irregulares. Una iluminación proyectada decorativa puede también desempeñar la función de seguridad.

10.3.3 Locales de venta

Los comentarios de 10.3.2 son también aplicables. Además se tomarán precauciones para que las playas de carga sean visibles para las patrullas y que las puertas y umbrales profundos no sean áreas sombreadas que permitan esconderse. La iluminación de escaparates y la iluminación interna vista a través de vanos puede usarse para la seguridad. Las lámparas de filamento, que se usan con fines de iluminación de mercaderías son de corta vida resultando preferibles las lámparas de descarga, de mayor duración.

En la decisión de utilizar lámparas de descarga siempre deberá evaluarse su proximidad y eventual interferencia a componentes de un sistema electrónico de seguridad.

10.4 Pautas para el uso

La iluminación de seguridad debe ser usada durante todas las horas de oscuridad, o por lo menos durante el tiempo en que el inmueble no es utilizado, en las horas sin luz natural. Utilizada continuamente desalienta a los asaltantes y facilita la tarea de los supervisores.

En algunos casos la iluminación continua puede no ser conveniente. En tales casos se puede activar con detectores de intrusos, el sistema de iluminación que se denomina de disparo deberá existir una protección adecuada contra falsas alarmas, ya sea involuntarias o urdidas.

En ningún caso se dejará el uso de la iluminación de seguridad al arbitrio de miembros no autorizados.

10.5 Lámparas

10.5.1 No existe una lámpara ideal de seguridad. Los factores que deben considerarse son:

- a) la velocidad con que se requiera la luz una vez accionado el interruptor;
- b) el costo de la energía consumida, en términos absolutos y con relación a los valores que se protegen;
- c) la vida de la lámpara se recuerda que hay aproximadamente 4000 horas de oscuridad por año;
- d) el color aparente y el rendimiento colorimétrico.

10.5.2 Rendimiento de la lámpara

La relación entre el flujo luminoso en lúmenes y la potencia consumida, en watios, es una consideración importante en la elección de la lámpara.

El rendimiento varía con la potencia consumida por la lámpara y el color aparente. Se debe consultar a los fabricantes para obtener datos de rendimiento de las diferentes lámparas.

10.5.3 Selección de la lámpara

En los artículos que siguen se dan las características de los principales tipos, ordenados según su rendimiento.

10.5.4 Lámparas de sodio de baja presión

Cuando se necesita la iluminación durante toda la noche y no importa el color, se pueden usar estas lámparas. Son de calentamiento lento, insumiendo algunos minutos, pero poseen rendimiento más alto, hasta 178 lm/W. Su vida útil alcanza 10000 horas, pero no es posible distinguir los colores debido a su luz monocromática amarillo oro. Suelen designarse SOX.

El tipo SOX es particularmente adecuado para sistemas perimetrales, donde la detección de intrusos es necesaria en distancias relativamente cortas (de hasta aproximadamente 20 m hacia afuera del perímetro). También puede usarse en la iluminación convencional de calles mediante faroles montados sobre postes o sobre ménsulas de pared. Con un dispositivo de control electrónico retoma instantáneamente la plena brillantez después de una corta interrupción de la alimentación (hasta cuatro minutos).

10.5.5 Lámparas de sodio de alta presión

Las lámparas de sodio de alta presión deben usarse cuando el color es importante, o cuando es necesaria la detección en distancias mayores que el alcance de las de baja presión (ver 10.5.4).

Las lámparas se producen en tres versiones designadas con SON para la lámpara normal, SONP para la lámpara de gran potencia y SONCONFORT para la versión del rendimiento mejorado de color. La envoltura de la lámpara puede ser tubular clara, elíptica difusa o, en un ámbito de potencia eléctrica restringida, con un reflector interno.

Las lámparas de sodio de alta presión tienen un rendimiento más bajo que el tipo SOX (SON hasta 120 lm/W), pero tienen una vida útil del orden de 20000 horas. El tiempo inicial de calentamiento es de pocos minutos. El rendimiento de color de lámparas SON es pobre, pero es adecuado para permitir distinguir entre numerosos colores. La versión SONCONFORT tiene una menor potencia en la emisión de luz utilizadas en luminarias para vía pública, el tipo SON alcanza distancias cortas de hasta 100 m.

Con arrancadores electrónicos esas lámparas se vuelven a encender en menos de un minuto después de una interrupción de la alimentación, pero no hasta la brillantez plena, siendo necesario un período adicional de calentamiento.

10.5.6 Lámparas fluorescentes

Son adecuadas para la iluminación interna de seguridad así como para la iluminación local externa, son sensibles a la temperatura. Tiempos muy fríos o muy calurosos pueden reducir significativamente el rendimiento lumínico.

Los tubos rectos (TL) o compactos (SL) tienen una vida útil de 5000 horas o de 7500 horas, dependiendo del tipo y la potencia eléctrica.

El tipo SL de reducida potencia, con rendimiento de hasta 60 lm/W, se utiliza ampliamente como reemplazante de las lámparas incandescentes en frontones y otras iluminaciones locales.

Las lámparas fluorescentes deben proporcionar luz inmediatamente después de encendidas, pero los tipos SL aumentan en brillantez a partir del primer minuto. Las lámparas TL poseen rendimiento de hasta 68 lm/W, dependiendo del color de la lámpara y del tipo de dispositivo de control. El reencendido es inmediato.

LEONID LLONTOP CASTRO
 Jefe de Seguridad Casa Matriz
 Banco Ciudad Bs. As.

10.5.7 Lámparas halogenadas

Las lámparas halogenadas son lámparas de mercurio con aditivos en la descarga para mejorar la restitución de color y la entrega de luz. Las lámparas claras, tubulares, se designan con HPT, mientras que las lámparas ovoidales se conocen como HP. La vida útil puede depender de las condiciones operativas y puede estar entre 6000 horas y 24000 horas, El rendimiento es de hasta 47 lm/W. Existen varios dispositivos de control del circuito, pero con los arrancadores electrónicos las características operativas son similares a las de las lámparas SON (ver 10.5.5).

10.5.8 Lámparas de mercurio con color corregido

Se usan raramente para fines de seguridad. Los revestimientos fluorescentes mejoran el rendimiento colorimétrico. Las del tipo HPL-N tienen rendimiento lumínico hasta 62Lm/W. Su vida útil es de 12.000 a 16.000h. Su reencendido es lento, después de la interrupción del suministro, insumen hasta 4 min en alcanzar el 80% del máximo flujo luminoso.

10.5.9 Lámparas halógenas de tungsteno

En uso principal de las lámparas halógenas de tungsteno (T3Q) es para los sistemas de iluminación eventual, en que las horas efectivas de los sistemas de operación están fijadas, o en puntos de verificación donde puede ser efectiva su alta luminosidad y buen rendimiento colorimétrico.

Generalmente las lámparas T3Q no se recomiendan para sistemas de iluminación de seguridad de grandes áreas o áreas perimetrales, debido al elevado consumo de energía.

Las lámparas de tungsteno proporcionan una iluminación plena instantánea, pero tienen un bajo rendimiento lumínico de hasta 24 lm/W y una corta vida útil (2000 horas).

10.5.10 Lámparas mezcladoras a vapor de mercurio

Se usan poco, insumen tiempo considerable para el encendido y reencendido. Reemplazan a las incandescentes con filamento de tungsteno. El tipo ML utiliza un filamento de tungsteno como reactancia y no requiere dispositivo adicional de control. Su vida útil es de alrededor de 6.000h. con un rendimiento de hasta 28 Lm/W

10.5.11 Lámparas con filamento de tungsteno

No se usan en gran escala con fines de seguridad por bajo rendimiento y vida útil. Existe una amplia gama: las normales, tipo NL y las reflectoras, tipo K. Su rendimiento es normalmente 14 Lm/W y su vida útil es de 1000h si bien algunos tipos alcanzan las 2000 h.

10.6 Luminarias

Las luminarias y accesorios debe ser robustos. La distribución luminosa de los artefactos varía entre una esfera difusa en un vano de puerta, hasta un angosto brazo abanicado usado en cercos perimetrales. El delincuente trata de lograr una zona de oscuridad para su asalto y por ello los artefactos deben resistir impactos y otros maltratos. Materiales como el policarbonato y aluminio fundido ofrecen altos niveles de protección, aunque aún el más robusto fallará con violencia extrema. Aparte de los artefactos difusores de la iluminación, los accesorios como mallas protectoras, los elementos de fijación como ménsulas y postes, deben también ser resistentes.

Las luminarias utilizadas en protección perimetral deberán estar protegidas contra vandalismo por ejemplo, con una malla metálica.

10.7 Control

Para que la iluminación de seguridad sea efectiva debe utilizarse en los horarios apropiados. Para instalaciones exteriores una simple célula fotoeléctrica que conecte el circuito cuando la luz diurna se desvanece y desconecta cuando reaparece la luz del día, es un control adecuado. Así también servirá automáticamente con las variaciones de duración del día por cambios estacionales y por diferentes condiciones climáticas, garantizando que la iluminación de seguridad estará disponible siempre que sea necesaria. También se dispone de interruptores horarios que se ajustan automáticamente a los cambios estacionales de la duración del día. También tienen un retén de resorte para continuar su ciclo programado cuando se produce una interrupción del suministro. Estos interruptores horarios pueden utilizarse para sistemas de iluminación interior que se requieran fuera del horario normal de trabajo, asegurándose que los fines de semana estén en servicio.

10.8 Instalación

La iluminación de seguridad es de poca utilidad ó se puede quedar inutilizada por el simple corte de un cable de alimentación. La mejor protección es colocar todo el cableado fuera del alcance de personas no autorizadas. Ello puede implicar enterrar el cable en una instalación perimetral y hacer desviaciones para los artefactos individuales a través de una ramal con fusible. Cuando a la iluminaria se le interpone un fusible, se protegerá al resto de la instalación. En tramos a la vista con cables comunes que se canalizan en caños de acero se disuade a intrusos. También puede disponerse que cualquier interferencia accione una señal de alarma; mientras el suministro público de electricidad sea adecuado no se requiere sistemas secundarios. En otros casos la energía eléctrica alternativa se puede proporcionar con una batería o con un generador auxiliar.

10.9 Mantenimiento

La limpieza de rutina y el cambio de lámparas de la instalación de iluminación de seguridad, no sólo es lógico económicamente, sino también indispensable para su correcto funcionamiento.

Cualquier lámpara o artefacto roto, así como cualquier otro daño en la instalación (cableado, postes, equipo auxiliar), deberá considerarse sospechoso. Puede ser accidental o el comienzo de un intento programado para crear áreas de oscuridad. Dos artefactos adyacentes con fallas en una instalación bien mantenida son particularmente sospechosos. Las patrullas de seguridad, o miembros responsables del personal deberán dar cuenta inmediatamente de cualquier falla, debiéndose tratar a las mismas con toda urgencia.

LEONID LIONTOP CASTRO
Jefe de Seguridad Casa Matriz
Banco Ciudad Bs. As

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100

0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99



INSTITUTO ARGENTINO
DE NORMALIZACIÓN
Y CERTIFICACIÓN

NORMA ARGENTINA

IRAM 3860-1*

Segunda edición
2011-04-15

Gestión para la prevención del delito Guía para la seguridad contra ilícitos

Parte 1 - Inmuebles de uso comercial

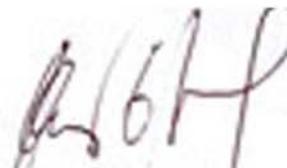
Crime prevention management
Safety guideline for security against illicit
Part 1 - Commercial use inmuebles

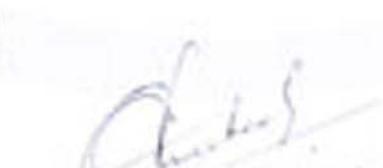
* Corresponde a la revisión parcial de la edición de diciembre de 1994, a la que esta Parte de la Segunda Edición, junto con la Parte 2 de esta norma, reemplaza.

LEONID ELONTOP CASTRO
Jefe de Seguridad Casa Metriz
Banco Ciudad Bs. As.



Referencia Numérica:
IRAM 3860-1:2011


Dirección de Certificación


Comité General de Certificación


Dirección General



Certificado sistemas de Gestión

IRAM 2011-04-15

No está permitida la reproducción de ninguna de las partes de esta publicación por cualquier medio, incluyendo fotocopiado y microfilmación, sin permiso escrito del IRAM.

LEONID LLONTOP CASTRO

Jefe de Seguridad Caso Matriz
Banco Ciudad Bs. As

LEONID LLONTOP CASTRO

Jefe de Seguridad
Banco Ciudad

Prefacio

El Instituto Argentino de Normalización y Certificación (IRAM) es una asociación civil sin fines de lucro cuyas finalidades específicas, en su carácter de Organismo Argentino de Normalización, son establecer normas técnicas, sin limitaciones en los ámbitos que abarquen, además de propender al conocimiento y la aplicación de la normalización como base de la calidad, promoviendo las actividades de certificación de productos y de sistemas de la calidad en las empresas para brindar seguridad al consumidor.

IRAM es el representante de la Argentina en la International Organization for Standardization (ISO), en la Comisión Panamericana de Normas Técnicas (COPANT) y en la Asociación MERCOSUR de Normalización (AMN).

Esta norma IRAM es el fruto del consenso técnico entre los diversos sectores involucrados, los que a través de sus representantes han intervenido en los Organismos de Estudio de Normas correspondientes.

Corresponde a la revisión parcial de la edición de diciembre de 1994, a la que esta Parte de la Segunda Edición, junto con la Parte 2 de esta norma, reemplaza.

Esta norma, bajo el título general Gestión para la prevención del delito. Guía para la seguridad contra ilícitos, se compone de las partes siguientes:

Parte 1 - Inmuebles de uso comercial.

Parte 2 - Inmuebles de uso particular.

LEONID LLONTOP CASTRO
Jefe de Seguridad Casa Matriz
Banco Ciudad Bs. As.

Índice

	Página
1 ALCANCE.....	5
2 DOCUMENTOS NORMATIVOS PARA CONSULTA.....	5
3 TÉRMINOS Y DEFINICIONES.....	6
4 PLANEAMIENTO Y DISEÑO.....	6
5 OPORTUNIDADES PARA EL DELITO.....	8
6 GESTIÓN DE LA SEGURIDAD.....	10
7 RECOMENDACIONES DE SEGURIDAD PARA COMERCIOS Y OFICINAS.....	11
8 PROTECCIÓN DE CAMINOS DE INGRESO, ACCESOS Y PERÍMETRO.....	13
9 PROTECCIÓN DE LA ENVOLVENTE DEL EDIFICIO.....	14
10 PROTECCIÓN DE ESPACIOS INTERNOS.....	17
11 SEGURIDAD DEL EDIFICIO FUERA DE HORAS DE TRABAJO NORMALES.....	19
Anexo A (Informativo) Clasificación de riesgos y niveles de amenazas.....	22
Anexo B (Informativo) Bibliografía.....	23
Anexo C (Informativo) Integrantes de los organismos de estudio.....	24

LEONID LLONTOP CASTRO
Jefe de Seguridad Casa Matriz
Banco Ciudad Bs. As.

Gestión para la prevención del delito

Guía para la seguridad contra ilícitos

Parte 1 - Inmuebles de uso comercial

LEONID LLONTOP CASTRO
 Jefe de Seguridad Casa Matriz
 Banco Ciudad Bs. As.

1 ALCANCE

Este documento brinda directrices y una estrategia recomendada para prevenir el robo, el hurto, los incendios intencionales y otros delitos que se cometen contra comercios y oficinas, nuevos y existentes.

En el anexo A se indican los niveles de seguridad recomendados para la protección de estos establecimientos, de acuerdo a su riesgo.

2 DOCUMENTOS NORMATIVOS PARA CONSULTA

Todo documento normativo que se menciona a continuación es indispensable para la aplicación de este documento.

Cuando en el listado se mencionan documentos normativos en los que se indica el año de publicación, esto significa que se debe aplicar dicha edición, en caso contrario, se debe aplicar la edición vigente, incluyendo todas sus modificaciones.

IRAM 3687 - Dispositivos antipánico para salidas de emergencia. Requisitos y métodos de ensayo.

IRAM 3840 - Gestión para la prevención del delito a través de la planificación urbana.

IRAM 4173-1 - Sistemas de alarma. Sistemas de transmisión. Parte 1: Requisitos generales.

IRAM 4173-2 - Sistemas de alarma. Sistemas de transmisión. Parte 2: Requisitos generales para los equipos utilizados.

IRAM 4175 - Sistemas de alarma de intrusión en inmuebles. Código de práctica para la planificación y la instalación.

IRAM 12841 - Vidrios de seguridad, antibala y antiintrusión.

EN 1143-1 - Unidades de almacenamiento de seguridad. Requisitos, clasificación y métodos de ensayo para resistencia al robo. Parte 1 - Cajas fuertes, cajeros automáticos, puertas y cámaras acorazadas.

EN 1303 - Herrajes para la edificación. Cilindros para cerraduras. Requisitos y métodos de ensayo.

EN 1906 - Herrajes para la edificación. Manillas y pomos de puertas. Requisitos y métodos de ensayo.

EN 10223-4 - Alambre de acero y productos de alambre para cerramientos. Parte 4 - Malla electrosoldada.

EN 10223-6 - Alambres de acero y productos de alambre para cerramientos. Parte 6 - Enrejado de simple torsión.

EN 10223-7 - Alambres de acero y productos de alambre para cerramientos. Parte 7 - Paneles de malla electrosoldada para cerramientos.

EN 12209 - Herrajes para edificación. Cerraduras y pestillos. Cerraduras, pestillos y cerraderos mecánicos. Requisitos y métodos de ensayo.

EN 12320 - Herrajes para la edificación. Candados y accesorios para candados. Requisitos y métodos de ensayo.

EN 13241-1 - Puertas industriales, comerciales, de garaje y portones. Norma de producto. Parte 1 - Productos sin características de resistencia al fuego o control de humos.

EN 13724 - Servicios postales. Aberturas de los casilleros o buzones domiciliarios y los bocacartas. Requisitos y métodos de ensayo.

EN 50131-1 - Sistemas de alarma. Sistemas de alarma de intrusión y atraco. Parte 1 - Requisitos del sistema.

EN 50132-7 - Sistemas de alarma. Sistemas de vigilancia CCTV para uso en aplicaciones de seguridad. Parte 7 - Guía de aplicación.

EN 50133-1 - Sistemas de alarma. Sistemas de control de accesos de uso en las aplicaciones de seguridad. Parte 1 - Requisitos de los sistemas.

UNE-ENV 1627 - Ventanas, puertas, persianas. Resistencia a la efracción. Requisitos y clasificación.

RENAR MA.02 - Materiales de resistencia balística para blindajes.

3 TÉRMINOS Y DEFINICIONES

Para los fines de la presente norma se aplica la definición siguiente:

resistencia al robo. Propiedad del conjunto de puerta, de ventana o cerrojo que le permite resistir tentativas de entrada forzada hacia un cuarto o un área protegida.

4 PLANEAMIENTO Y DISEÑO

LEONID LLONTOP CASTRO
Jefe de Seguridad Casa Matriz
Banco Ciudad Bs. As.

4.1 Generalidades

La seguridad del edificio se puede definir de una manera general como el uso de la disposición del sitio, de la estructura y de la forma de un edificio para proteger a los ocupantes y sus posesiones contra el delito. Los factores de diseño dominantes incluyen la disposición física, la ubicación de puertas y ventanas, el control de acceso y movimiento, y la vigilancia formal e informal. La integración de estos elementos de diseño arquitectónico en la etapa inicial, teniendo en cuenta su impacto sobre la seguridad, permite mejorar el control del delito y de la alteración del orden.

Para asegurarse que los factores de prevención del delito estén considerados en el diseño, se recomienda incluir en el equipo de proyecto

(ver 4.2) profesionales con experiencia apropiada en la prevención del delito.

4.2 Diseño para incluir la seguridad patrimonial y humana

Se recomienda que el equipo de diseño considere los diversos factores que pueden influir en la oportunidad de cometer delitos. Entre los más importantes están los siguientes:

- a) los inmuebles;
- b) la presencia de personas;
- c) la minimización del conflicto.

Es esencial que el diseño del espacio público sea tal, que la gente comience a considerarlo como propio y tome responsabilidad sobre el. Si puede lograrse esto, es menos probable que ocurra el delito y el comportamiento antisocial, sin que el público reaccione.

Uno de los factores más fuerte en la prevención del delito es el riesgo de ser visto e identificado. Por lo tanto, la presencia humana y la vigilancia natural son muy importantes. En lo posible, se recomienda el uso mixto de unidades ya que genera movimiento a lo largo del día. El mobiliario urbano debe diseñarse para permitir líneas de visión libres y para proporcionar vigilancia natural amplia. Por las mismas razones, se recomienda que los edificios den frente a un espacio público.

Se necesita considerar el miedo al delito, ya sea real o percibido, que el diseño ambiental lo refleje, evitando cualquier característica que pueda dar lugar a una situación de conflicto potencial. El diseño ambiental seguro e integrado animará al uso de los espacios, generando una sensación de seguridad.

LEONID LLONTOP CASTRO
Jefe de Seguridad Casa Matriz
Banco Ciudad Bs. As.

4.3 Análisis de riesgos

4.3.1 Generalidades

Cualquier estrategia de prevención del delito es esencialmente una estrategia de gestión de riesgos. Por lo tanto, antes de poder desarrollar una estrategia eficaz, es importante identificar y entender los factores de riesgo involucrados.

4.3.2 Factores locales

Al evaluar el nivel del riesgo es esencial dar prioridad a los factores locales realizando un diagnóstico. Esto puede implicar el realizar una encuesta de análisis sobre el delito en el vecindario inmediato, para identificar el tipo de delito que se reporta, dónde y cuándo ocurrieron incidentes y quiénes fueron las víctimas. Esto se puede lograr mediante un mapa espacial para identificar las concentraciones o los puntos críticos del delito.

También es importante tener en cuenta que los factores que pueden influir sobre la oportunidad para el delito, pueden no estar necesariamente en la cercanía inmediata. Por ejemplo, una ruta que conecta dos instalaciones atractivas pasando por un área comercial puede generar posibilidades de delinquir a determinadas personas o grupos. Aunque las instalaciones en sí pueden estar a una cierta distancia de los comercios u oficinas, la presencia de una cantidad relativamente grande de gente que usa la ruta puede influir en la posibilidad del delito.

Cuando el desarrollo está en un sitio nuevo, puede ser que no haya habido problemas previos de delito o no existen registros. En estos casos es importante considerar el desarrollo propuesto en términos de generación potencial del delito, es decir ¿qué delito o comportamiento antisocial se podría razonablemente anticipar?

En la IRAM 3840 se indican lineamientos sobre los métodos para determinar el riesgo del delito y los métodos destinados a reducir estos riesgos en barrios, centros de ciudad y sitios industriales (ver también el capítulo 5).

4.4 Imagen del vecindario

Las primeras impresiones de un potencial delincuente tienen la mayor influencia en su decisión de cometer o no un delito. Aunque los centros de compras o comerciales que parecen bien mantenidos pueden dar una impresión de prosperidad o bienestar económico, es también verdad que pueden dar una impresión igualmente fuerte que la gente que trabaja allí, está orgullosa del área y es más probable que esté comprometida con la seguridad.

Un desarrollo comercial que anima a los ocupantes a que trabajen juntos como una comunidad, para tomar una acción combinada para mejorar el ambiente contra los delincuentes potenciales, es probable que dé como resultado menos delitos y una mejora en la calidad de vida de los usuarios. Hay dos buenas maneras de alcanzar esto:

- a) definiendo el desarrollo para darle una identidad clara;
- b) asegurando la máxima vigilancia posible de una propiedad a otra propiedad. Los delincuentes potenciales no desean ser vistos. Siempre que sea posible también es recomendable intentar y obtener una mezcla de tipos de uso y de ocupantes. Esto puede dar lugar a una variación en los patrones de ocupación que permiten que más gente esté en cualquier área particular, ejerciendo una vigilancia informal.

4.5 Seguridad patrimonial

En la etapa del diseño del edificio se deben incorporar las premisas de seguridad. Al decidir la localización específica de un comercio o de una oficina es importante tomar en cuenta el presente y los progresos futuros previstos para el área.

Un diseño claro y despejado tanto para el exterior y el interior del edificio, puede ayudar a la vigilancia de seguridad, especialmente cuando está combinado con una buena iluminación natural y artificial.

4.6 El sitio

Se recomienda considerar lo siguiente:

- a) el grado de influencia de otros factores, por ejemplo, los requisitos del mercado y la seguridad, en la selección de la ubicación de las instalaciones;
- b) el grado en el cual las disposiciones de seguridad son influenciadas por una ubicación propuesta, considerando:
 - tipos de delito que pueden ocurrir en áreas de elevado delito, o donde los edi-

- ficios son generadores conocidos de delito, y
- los diversos tipos de delito, por ejemplo, en áreas marginales;
 - c) niveles existentes o potenciales de robo, hurto, incendios intencionales y daño criminal en el lugar;
 - d) proximidad a áreas de reunión pública, por ejemplo estadios de fútbol y otros deportes, patios de juego, parques de diversiones;
 - e) el grado de influencia sobre los problemas de seguridad debido a las características físicas y naturales tales como ríos, terrenos escarpados, con arroyos, el clima o factores estacionales tales como la afluencia de turistas;
 - f) las ventajas que se pueden obtener de la proximidad a las estaciones del policía, bomberos y de ambulancias o de los perímetros seguros existentes de instalaciones bien mantenidas con paredes o cercas altas;
 - g) la iluminación y cobertura proporcionadas por el alumbrado público existente;
 - h) niveles de seguridad que los dueños y los ocupantes de otros comercios y oficinas en el distrito aplican a sus instalaciones;
 - i) la vigilancia natural, es decir el grado de visibilidad de la propiedad desde otras instalaciones.

5 OPORTUNIDADES PARA EL DELITO

5.1 Generalidades

Es necesario analizar el tipo de delito que podría razonablemente esperarse que pueda ocurrir como resultado del nuevo desarrollo. Es esencial investigar el delito y el comportamiento antisocial existentes del lugar.

El objetivo primario es siempre tratar de prevenir que suceda el delito.

5.2 Tipos de delito que ocurren con más frecuencia

5.2.1 Generalidades

Los comercios y oficinas sufren delitos muy similares a las viviendas pero se diferencian en los horarios en que ocurre el delito. Por definición, los comercios y las oficinas son ocupados con más frecuencia durante el día mientras que la mayoría de las viviendas pueden estar desocupadas. Los ilícitos, tales como robo, ocurren generalmente durante los tiempos cuando las instalaciones están cerradas, más probable en la noche, pero el hurto y el robo en comercios (ver 5.2.2 a 5.2.3) ocurren durante el día. Las oficinas y los comercios deben, por lo tanto, tener diferentes tipos de protección contra diversos tipos de delitos en distintas horas del día.

También se recomienda recordar que las prácticas del trabajo están cambiando y tanto los comercios como las oficinas están teniendo períodos más largos de ocupación o permanecen abiertas más tiempo. Se recomienda que la evaluación del riesgo, por lo tanto, permita estas variaciones.

LEONID LLONTOP CASTRO
Jefe de Seguridad Casa Matriz
Banco Ciudad Bs. As.

5.2.2 Robo

El robo de comercios y oficinas ocurre principalmente cuando las instalaciones están desocupadas, y pueden dividirse en dos tipos:

- a) las instalaciones de alto riesgo son las que tienen la probabilidad de ser blanco de potenciales delincuentes profesionales organizados y determinados, que emprenden ataques premeditados, por ejemplo, robar en banda, robar mercancías de elevado valor o robar equipos, información o datos. Por ejemplo, se ingresa a un almacén de tabaco y se roba un camión cargado de cigarrillos;
- b) los ladrones oportunistas explotan debilidades en las medidas de seguridad y cometen robos de menor valor; éstos son más frecuentes que los ataques premeditados. Un ejemplo puede ser un robo en el que se rompe la vidriera de un comercio.

5.2.3 Hurto de las mercancías/robo en comercios

Las mercancías en exhibición en comercios son particularmente vulnerables al hurto. Se recomienda considerar cuidadosamente la orientación y la disposición interna tanto de comercios como de oficinas para reducir la oportunidad del hurto.

Se recomienda diseñar las áreas de recepción de la oficina para dar tanto una impresión de bienvenida a la gente de negocios y ser lo suficientemente formales para disuadir al ladrón oportunista. Se recomienda crear una disposición de los comercios que brinde al personal las máximas oportunidades para la vigilancia.

El hurto tal como el carterismo puede también ocurrir en áreas públicas. Esto se puede reducir mediante la disposición apropiada, tanto en el interior como en el exterior de las instalaciones. El hurto de pertenencias del personal de la oficina y del comercio es más probable que ocurran cuando no se proporcionan instalaciones para mantenerlas seguras. Se recomienda considerar cuidadosamente la seguridad en áreas de almacenamiento, áreas y zonas de entrega y áreas de estacionamiento.

5.2.4 Hurto de información y de datos

Se recomienda tomar medidas de seguridad especiales para reducir el riesgo del hurto de la información vital para la compañía.

El riesgo más grande es el hurto de los datos almacenados en sistemas informáticos; por lo tanto, se recomienda proporcionar protección para los servidores, computadoras y terminales.

Se recomienda tomar las medidas de seguridad siguientes para evitar el hurto de información o la corrupción de datos:

- a) dispositivos de traba de las computadoras, la protección del software mediante el uso de contraseñas, cortafuegos electrónicos, etc.;
- b) control del acceso al ambiente de los servidores, mediante por ejemplo, un sistema de restricción de entrada por tarjeta electrónica u otros medios apropiados;

- c) protección contra intromisiones electrónicas.

NOTA. Se está tornando cada vez más importante salvaguardar la información y los datos del hurto o de corrupción. Si bien una empresa puede sustituir las mercancías que se roban o se dañan, es a menudo mucho más perjudicial el perder información comercialmente confidencial, que puede cubrir todos los aspectos de la operación de la compañía.

5.2.5 Daños por incendio intencional

Se recomienda considerar las medidas de seguridad siguientes para disuadir a los incendiarios:

- a) proporcionar un perímetro seguro para disuadir a delincuentes potenciales;
- b) que la luz debajo de las puertas sea tan pequeña o sea sellada como sea posible;
- c) que los buzones cumplan los requisitos de la EN 13724, se ubiquen preferentemente fuera del edificio y, si están ubicados dentro del edificio, sean resistentes al fuego;
- d) que las compañías con operaciones sensibles utilicen escáner de correo;
- e) instalar sistemas automáticos de detección de incendio y de extinción, por ejemplo rociadores, con una instalación de transmisión automática de alarma, para proporcionar la alerta temprana de incendio a los bomberos;
- f) que las mercancías peligrosas tales como líquidos inflamables y cilindros de gas se guarden bajo llave en almacenes especiales, particularmente fuera de las horas de trabajo;
- g) que los elementos y desperdicios inflamables sin protección se almacenen fuera de los edificios para reducir el riesgo de propagación de un incendio.

NOTA. Todas las oficinas y comercios están potencialmente en riesgo de incendios intencionales. Las propiedades en mayor riesgo son a menudo las instalaciones aisladas o desatendidas o aquellas con poca o ninguna seguridad física.

5.2.6 Contaminación de producto

Cuando la amenaza de contaminación de producto es un riesgo serio, se recomienda tomar

precauciones rigurosas de seguridad. Se recomienda tener disponible un plan de emergencia completo de la compañía que se ocupe de las amenazas de contaminación de producto.

6 GESTIÓN DE LA SEGURIDAD

6.1 Generalidades

Se recomienda que la estrategia para prevenir el robo, hurto y los incendios intencionales en oficinas y comercios cubra las instalaciones tanto cuando están abiertas al público como cuando están cerradas. Se recomienda que todas las medidas preventivas técnicas y humanas a tomar contra el delito se analicen en los cuatro aspectos siguientes:

- a) disuasión del ataque;
- b) bloqueo del ataque;
- c) detección (dispositivos de alerta de que un ataque está en marcha);
- d) retraso del ataque.

Se recomienda que el resultado de este análisis se incorpore al plan global de seguridad. Es esencial que todas las unidades, ya sea un comercio, una oficina, un centro o un desarrollo comercial tengan un plan de seguridad que cubra todas las contingencias, se transmita y sea comprendido por todos los empleados.

LEONID LLONTOP CASTRO
 Jefe de Seguridad Casa Matriz
 Banco Ciudad Bs. As.

6.2 Análisis de riesgo

Para formular un plan de la seguridad primero es necesario realizar una profunda evaluación de riesgos. Para evaluar el grado de seguridad necesario para una oficina o un comercio particular se recomienda considerar los factores siguientes:

- a) tipo de actividad;
- b) atractivo para el delincuente potencial en términos de mercancías, efectivo o datos confidenciales;
- c) rutas de escape potenciales para huir con mercancías robadas. La ruta de escape

puede no ser la misma que la ruta de entrada;

- d) la facilidad de acceso desde la calle, áreas abiertas, azoteas adyacentes, niveles superiores e inferiores de las instalaciones en cuestión y de las colindantes;
- e) grado de seguridad inherente del establecimiento en lo referente a su construcción;
- f) la vulnerabilidad en relación con las tendencias de delitos locales;
- g) la vigilancia provista ya sea por la actividad pública normal, por patrullas rutinarias de la policía del área o por seguridad propia del establecimiento y de sus alrededores.

6.3 Vulnerabilidad del sitio y del edificio

Además de los criterios dados en 6.2, se recomienda que el análisis también incluya la consideración de los tres tipos siguientes de espacio alrededor del edificio. Cada tipo de espacio tiene condiciones especiales que requieren una evaluación antes de la incorporación en el plan global de seguridad:

- a) espacio periférico: terreno fuera del límite del perímetro del sitio;
- b) espacio perimétrico: área entre el límite del perímetro y la envolvente del edificio;
- c) espacio volumétrico: espacio incluido dentro del edificio.

6.4 Concepto de seguridad

En el diseño del edificio nuevo, se recomienda incorporar un plan de seguridad teniendo en cuenta el análisis del riesgo. Para un edificio existente, el análisis del riesgo se debe enfocar en los incidentes y la información pasados, presentes y proyectados. Además de las directrices de 6.2, se recomienda considerar los puntos siguientes:

- a) realizar una evaluación del riesgo en lo referente al valor de la propiedad y de los artículos que se deben proteger, incluyen-

- do los requisitos de seguridad contra incendio y los de la compañía de seguros;
- b) que el diseño del edificio y las medidas de seguridad empleadas aseguren tanto como sea posible que los intrusos potenciales no puedan lograr ingresar a las instalaciones sin ser vistos;
 - c) planificar la disposición interior de las oficinas y comercios para reducir al mínimo las pérdidas debidas al hurto;
 - d) supervisar el control de acceso y salida del personal, los conductores de vehículos de carga, los contratistas, personal de limpieza, mantenimiento y visitantes;
 - e) proporcionar y mantener barreras perimetrales y dispositivos de seguridad adecuados en puertas externas, ventanas y otros puntos posibles de entrada;
 - f) contar con personal de seguridad y cámaras de CCTV cuando sea apropiado;
 - g) contar con instalaciones para la protección de bienes de elevado valor, de información y de dinero en efectivo;
 - h) instalar líneas telefónicas y cables seguros para la transmisión de señales de alarmas;
 - i) que los vehículos se mantengan alejados de las áreas sensibles, pero bajo vigilancia para su propia seguridad;
 - j) tomar precauciones para el manejo de mercancías peligrosas;
 - k) instalar iluminación externa de seguridad;
 - m) proveer recintos externos de almacenaje.

7 RECOMENDACIONES DE SEGURIDAD PARA COMERCIOS Y OFICINAS

Identificación del grado de protección requerido

Para proteger los riesgos indicados en el anexo A, se recomienda aplicar los niveles mínimos de seguridad indicados en la tabla 1. Esto puede ser de aplicación en las instalaciones de oficina, donde también debe considerarse la amenaza de pérdida de información y de datos así como de equipos.

Las recomendaciones de esta norma pueden aplicarse tanto a los comercios como a las oficinas, según requisitos específicos.

LEONID LLONTOP CASTRO
 Jefe de Seguridad Casa Matriz
 Banco Ciudad Bs. As

Tabla 1 - Clase recomendada de resistencia del producto para lograr los niveles de protección especificados

Nivel de protección					
Equipo de construcción de comercios y oficinas	Grado 1	Grado 2	Grado 3	Grado 4	Grado 5
Puertas clase de resistencia de la UNE-ENV 1627	1-2	2-3	3-4	4-5	4-6
Ventanas clase de resistencia de la UNE-ENV 1627	1-2	1-3	3	3-4	4
Cortinas clase de resistencia de la UNE-ENV 1627	1	2	2-3	3-4	4-5
	Si la cortina ensayada se utiliza en conjunto con una ventana o una puerta antirrobo, se puede reducir la clase de resistencia				
Vidriados IRAM 12841	I	II	III	IV	V
Cilindros para cerraduras Clase de la EN 1303 Ver también la UNE-ENV 1627	4	4	5	5	5
Todos los cerramientos reforzados (rejillas de seguridad, paneles de policarbonato, acero o contrachapado)	No	No	Sí	Sí	Sí
	No	opcional	opcional	opcional	Sí
Sistema de control de accesos	La aplicación de sistemas de control de accesos dependerá de los niveles de protección requeridos junto con la vulnerabilidad de la ubicación.				
Control de tráfico barreras de colisión (bloques de calle, bolardos, barreras)	El uso de barreras de colisión depende de los accesos al edificio y acceso vehicular hacia el edificio.				
Vigilancia por CCTV EN 50132-7	opcional	opcional	opcional	Sí	Sí
	La aplicación de vigilancia por CCTV depende de la ubicación				
Sistemas de alarmas. Sistemas de intrusión Grado de la EN 50131-1	opcional 1	opcional 1	2	3	4
Caja fuerte EN 1143-1	Requerido cuando los valores exceden una cantidad específica				
Resistencia a las balas RENAR MA 02	La resistencia a las balas y a los explosivos depende de la naturaleza de las actividades (por ejemplo: orfebres, joyerías).				

Al decidir el nivel de seguridad de una unidad individual de venta al por menor dentro de un complejo de compras, se recomienda considerar si el complejo estará cerrado al público fuera del horario comercial. Un complejo cerrado al público fuera de este horario es más seguro y por lo tanto, necesita un nivel de seguridad interna menor que uno abierto al público en un horario extendido.

8 PROTECCIÓN DE CAMINOS DE INGRESO, ACCESOS Y PERÍMETRO

LEONID LLONTOP CASTRO

Jefe de Seguridad Casa Matriz
Banco Ciudad Bs. As

8.1 Generalidades

Un sitio específico puede o no tener las características siguientes.

8.2 Caminos de ingreso y entrada

Además de las recomendaciones de 6.3 en el tipo de espacio, se recomienda considerar lo siguiente:

- a) una clara señalización de direccionamiento;
- b) accesos abiertos y despejados;
- c) líneas de visión claras;
- d) iluminación apropiada.

Estas consideraciones se aplican por igual a los caminos de servicio, a las áreas de entrega y a los estacionamientos de vehículos. Se recomienda que el transporte público considere la localización, por ejemplo, de sus paradas.

8.3 Protección del espacio perimétrico del sitio

8.3.1 Cercas

Se recomienda instalar una cerca perimetral, cuando sea apropiado, para proporcionar una mejor protección del espacio periférico alrededor de un comercio o una oficina. La cerca perimetral puede ser uno de los tipos siguientes, dependiendo de la evaluación de riesgo:

- a) Cercas de simple torsión (ver EN 10223-6).

- b) Cercas de empalizada de acero (ver EN 10223-7).
- c) Cercas de metal desplegado.
- d) Cercas de malla soldada (ver EN 10223-4).
- e) Línea electrificada (en circunstancias excepcionales).

Es posible lograr una protección eficaz con medidas estéticamente más satisfactorias tales como los cercos vivos. En localizaciones de alto riesgo, la iluminación, CCTV y los sistemas de alarmas pueden reemplazar a las cercas.

8.3.2 Control de tránsito

Se recomienda utilizar barreras, cuando sea apropiado, para limitar el acceso no autorizado de vehículos al sitio o al edificio. Consisten en, por ejemplo:

- a) Barreras de brazo oscilante; (solamente un control de tránsito).
- b) Portones corredizos (control de peatones y de tránsito).
- c) Placas, escalones, bloques, balizas o reventadores de neumáticos, ascendentes. (contra el uso de vehículos como ariete).

Las barreras de tránsito se pueden controlar manual o automáticamente con instalaciones de mando local o remoto. Es esencial que la instalación de la barrera permita el acceso a los vehículos de emergencia.

8.3.3 Aberturas en cercas

Se recomienda que la altura, el diseño y la construcción de las aberturas tengan una protección similar a la de la cerca, que las bisagras se construyan de tal manera de evitar la extracción del portón y que sean protegidas, para evitar su uso como escalera o marco para trepar. Se recomienda que no sea posible pasar por debajo de la puerta y que la cerradura de la puerta se monte de forma segura y protegida como se indica en la EN 12209 y en la EN 1906.

8.3.4 Casilla de vigilancia

8.3.4.1 Generalidades

Cuando las instalaciones tienen una circulación importante de vehículos de carga, se recomienda instalar casillas de vigilancia con personal capacitado y el equipamiento apropiado. Se recomienda considerar puntos de acceso separados y controlados, para los peatones, el personal y los visitantes.

8.3.4.2 Ubicación y estructura

Debido a que la casilla de vigilancia es el primer punto de control de acceso a cualquier sitio o complejo, se recomienda que se ubique a una cierta distancia de los edificios principales, que forme parte integral de la cerca de seguridad perimetral para controlar el acceso al sitio y que sea de construcción sólida, capaz de soportar el impacto accidental o deliberado de vehículos.

Se recomienda que los portones y las barreras se abran solamente a las personas que se han anunciado e identificado y que los portones y las barreras sin supervisión se mantengan bloqueadas.

Se recomienda que la recepción incluya una sala de espera, un área de descanso para el personal, depósito y baño.

Se recomienda que las puertas de acceso sean bloqueables desde el interior, que sean de construcción resistente y no tengan ninguna manija externa. Se recomienda que los paneles de vidrio de las puertas sean de visión unidireccional.

8.3.4.3 Funciones básicas del personal de seguridad de la recepción

Las funciones de la recepción pueden incluir lo siguiente:

- a) Control de puertas y barreras.
- b) Supervisión de puertas.
- c) Control de movimientos de vehículos.

- d) Control e identificación de visitantes.
- e) Emisión de recuperación de pases para visitantes.
- f) Registro de tiempos de entrada y salida de vehículos y visitantes.
- g) Búsqueda de los vehículos, de los visitantes y del personal (si es una práctica aceptable).
- h) Escolta de visitantes.
- i) Control de entrega de mercancías contra registros.

9 PROTECCIÓN DE LA ENVOLVENTE DEL EDIFICIO

LEONID LLONTOP CASTRO

Jefe de Seguridad Casa Moritz
Banco Ciudad Bs. As.

9.1 Análisis de riesgos

Se recomienda que el análisis de riesgos del espacio perimetral (ver 6.3) alrededor de un comercio o de una oficina se enfoque en lo siguiente:

- a) Las aberturas, es decir, puertas y ventanas.
- b) Fachada y azotea.
- c) Playas privadas de estacionamiento.

9.2 Estructura del edificio

9.2.1 Generalidades

Se recomienda utilizar materiales resistentes al ataque o al daño manual, para lograr una seguridad inicial. Para evitar que delincuentes potenciales impacten un vehículo contra la estructura del edificio o que utilicen un vehículo para arrancar elementos de seguridad, pueden utilizarse rejas protectoras, bolardos, canchales de hormigón o elementos de defensa similares. Cuando se tenga en consideración las construcciones ligeras, por ejemplo, revestimientos de placas frágiles, un revestimiento reforzado, tal como una malla metálica soldada puede realzar la seguridad de la estructura del edificio.

9.2.2 Línea de edificación y fachada del edificio

Se recomienda utilizar una línea y fachada plana del edificio, sin salientes, tales como cornisas, parapetos, muescas y alfézares accesibles, que puede brindar medios que facilitan la entrada ilegal, para proporcionar una mayor protección del espacio perimetral (ver 6.3).

9.2.3 Instalaciones de servicios esenciales

Se recomienda que los diseñadores consideren la posibilidad de entradas no autorizadas a través del uso de las instalaciones para los servicios esenciales, por ejemplo, los ascensores de carga, los puntos de entrega de combustible o los conductos de ventilación.

Siempre que sea posible, se recomienda que tales servicios estén confinados y/o situados en compartimentos bloqueados. La manera más simple de comprometer la seguridad de un edificio es interferir con la fuente de energía. Los servicios son de gran importancia en la evaluación de riesgos.

9.3 Paisajismo

Cuando sea apropiado, se recomienda tener en cuenta la ubicación estratégica de mace-tas/canteros, bolardos, montículos o trincheras para disuadir a los intrusos de entrar usando un vehículo para embestir partes de la envolvente del edificio.

9.4 Puertas externas

LEONID LLONTOP CASTRO
Jefe de Seguridad Casa Matriz
Banco Ciudad Bs. As.

9.4.1 Generalidades

Se recomienda que las puertas externas se sitúen a la vista del público, que no estén ocultas y estén bien iluminadas para disuadir cualquier tentativa de entrada ilegal. Se necesita una consideración cuidadosa de las puertas de salida de emergencia o de incendio para evitar el abuso cuando el edificio está ocupado.

9.4.2 Puertas antirrobo

Se recomienda que las puertas externas antirrobo cumplan los requisitos de la UNE-ENV 1627.

9.4.3 Puertas de entrada y salida para el personal

Se recomienda que las puertas de entrada y salida para el personal estén aseguradas de tal manera que eviten el acceso no autorizado y que la entrada y la salida del personal se supervise, ya sea por un asistente en la puerta, o el uso de CCTV y de un sistema de control de accesos o ambos.

NOTA. En oficinas y comercios grandes, la seguridad puede mejorarse proveyendo al personal con tarjetas de control de identidad o de acceso. Sin embargo, los sistemas electrónicos de acceso no proporcionan normalmente un nivel físico aceptable de seguridad fuera de las horas de funcionamiento normales.

9.4.4 Puertas de entrada y salida para los visitantes

Se recomienda que las puertas para la admisión de visitantes sea alguna de las siguientes:

- Supervisada por una recepcionista o personal de seguridad.
- Bajo supervisión continua desde una oficina adyacente, ya sea directamente o por el uso de CCTV.
- Mantenida bloqueada, con admisión a solicitud mediante un botón u otro dispositivo adecuado, por ejemplo, un sistema de portero eléctrico.

Cuando sea apropiado, se recomienda que las puertas se equipen con visores de puerta u otros dispositivos de seguridad, de modo de poder examinar a los que llaman antes de su admisión y se evite que personas no autorizadas tengan acceso. Se recomienda que los visitantes no sean admitidos hasta tanto se haya establecido su identidad.

Se recomienda que para las puertas que conducen a áreas privadas o a las áreas para el uso exclusivo del personal, se utilicen algunas de las alternativas indicadas anteriormente.

9.4.5 Puertas de salida de emergencia

Se recomienda que los dispositivos antipánico de salida accionados por una barra horizontal de empuje cumplan los requisitos de la IRAM 3687.

9.4.6 Puertas para la admisión de vehículos

Se recomienda que las puertas y los portones de garajes comerciales, cumplan los requisitos de la EN 13241-1.

Se recomienda que la admisión de vehículos hacia áreas de entrega de riesgo elevado se realice a través de puertas o de portones en esclusa controlados, y el control ejecutado por un asistente o dispositivos de seguridad.

Se recomienda que los usuarios de vehículos visitantes sean admitidos solamente cuando se ha establecido su identidad y que las puertas sean de cierre y bloqueo automático y alternativo.

9.4.7 Puertas sin supervisión

Se recomienda tener especial cuidado que cualquier puerta que no pueda ser supervisada se considere como un riesgo inaceptable. Puede ser necesario tomar una acción correctiva en edificios existentes o el rediseño en edificios nuevos.

9.5 Candados y pasadores

Cuando no exista riesgo personal, la seguridad patrimonial se puede mejorar utilizando barras o pasadores de acero y candados. Se recomienda que los candados y sus accesorios cumplan los requisitos de la EN 12320. Se recomienda que la barra sea robusta y que se sujete con pernos a través de la puerta del lado interno, y sea al menos tan resistente como el candado. Se recomienda utilizar candados de traba oculta ya que ofrecen menores posibilidades de ataque.

Se recomienda que los tornillos y bulones de fijación con cabezas expuestas no puedan ser desatornillados del lado vulnerable; y que las roscas y los pernos de fijación estén del lado interno de la puerta. Se recomienda que sean del tipo de cabeza de giro único [resistente al vandalismo] o tener sus cabezas desfacetadas. Cuando se utilizan tuercas, se recomienda que las roscas expuestas de los bulones sean remachadas o soldadas.

9.6 Buzones

Se recomienda que los buzones cumplan los requisitos de la EN 13724 y se sitúen preferen-

temente en el exterior de la envolvente del edificio, lejos de puertas y de ventanas para evitar que los buzones se utilicen para tratar de forzar las cerraduras y tornillos de seguridad.

En el caso de instalarlo en una puerta, se recomienda no colocar la abertura de la correspondencia a menos de 400 mm de cualquier cerradura de puerta o ventana, a menos que haya un dispositivo de cierre auxiliar a más de 400 mm de la abertura.

Como alternativa, se recomienda colocar buzones detrás de la abertura de correspondencia, para dificultar a los intrusos el acceso a los accesorios de seguridad o robar correspondencia. Se recomienda que la acumulación de correspondencia detrás de una puerta no sea visible desde el exterior del edificio.

9.7 Ventanas

9.7.1 Ventanas antirrobo

Se recomienda que las ventanas antirrobo cumplan los requisitos de la UNE-ENV 1627.

9.7.2 Vidrieras/escaparates

Dependiendo del valor o de la portabilidad de la mercancía a proteger y del tipo de ataque previsto, el grado de seguridad de las vidrieras o escaparates se puede incrementar por medio de lo siguiente:

- a) vidriados de seguridad (vidrio laminado);
- b) incorporación de un vidriado de seguridad secundario, colocado detrás del vidriado existente.

Se recomienda que el vidriado de seguridad cumpla con los requisitos de la IRAM 12841.

9.8 Rejas y barras de ventana

Las rejas pueden proteger vidrieras o escaparates y pueden ser del tipo plegable (tijera), o de metal soldado, metal expandido o materiales macizos. El tipo más adecuado dependerá de la naturaleza de las instalaciones consideradas y del tipo y el valor de las mercancías en exhibición. Las barras tubulares son menos seguras

que las macizas pues pueden ser cortadas más fácilmente.

Se recomienda que las rejas se fijen internamente. Cuando se fijen externamente, se recomienda tener cuidado para asegurarse que están fijadas adecuadamente para evitar su fácil retiro.

En el caso de comercios, se recomienda seleccionar los tamaños de la abertura de las rejas según el tipo de mercancías exhibidas y seleccionar su altura considerando lo siguiente:

- a) altura de exhibición; LEONID LLONTOP CASTRO
Jefe de Seguridad Casa Matriz
Banco Ciudad Bs. As.
- b) nivel del alféizar externo;
- c) cualquier escalón o punto de apoyo en la entrada del comercio que se pueda utilizar para pasar sobre la reja.

En algunas instalaciones puede ser necesario proporcionar protección mediante rejas desprendibles hechas de metal expandido o malla soldada de espesor grande, fijadas a un marco adecuado al tamaño de la ventana. Se recomienda que dichas rejas se fijen internamente con pernos de seguridad fijados al marco y a la envolvente del edificio.

Se recomienda que las rejas se fijen a un marco de material adecuado para asegurar un anclaje resistente. Las rejas ornamentales hechas de hierro forjado u otros metales pueden ofrecer una medida de protección además de ser decorativas. Sin embargo, se recomienda diseñar las rejas de tal manera que no se creen puntos de apoyo para el pie, que las conviertan en un tipo de escalera.

9.9 Alarmas de ventanas

Para aumentar la seguridad, pueden utilizarse alarmas de ventanas, tales como el vidriado de seguridad con sensores internos, interruptores de contacto o dispositivos de vibración.

9.10 Persianas antirrobo

Se recomienda que las persianas antirrobo cumplan con los requisitos de la UNE-ENV 1627.

10 PROTECCIÓN DE ESPACIOS INTERNOS

10.1 Áreas accesibles a los clientes

10.1.1 Ventanillas, mostradores y cajas en comercios

Se recomienda que se diseñen de modo que sea posible el control de seguridad de las áreas de caja o pago de comercios. Se recomienda tomar medidas para la seguridad de las cajas y recaudaciones, mediante la provisión de cajas fuertes de piso, conductos para efectivo, y protectores de mostradores. Se puede proporcionar seguridad adicional, cuando sea necesario, mediante vigilancia por CCTV y un sistema de alarma. Los dispositivos antirrobo electrónicos pueden colocarse en las salidas en conjunción con el etiquetado (codificación) de los artículos.

10.1.2 Área de vidrieras

Se recomienda que el área de vidrieras tenga buena iluminación y se diseñe de modo que tengan líneas de visión claras evitando su interrupción con elementos ocasionales (por ejemplo: publicidad, ofertas, decoración u otros); y evitar las zonas ciegas u ocultas. Es esencial que se brinde vigilancia de seguridad mediante la instalación de espejos de dos vías simples o de un sistema amplio de CCTV.

Se recomienda que los gabinetes de seguridad de pared o de piso proporcionen un nivel de seguridad apropiado para las mercancías valiosas y los equipos de oficinas.

10.1.3 Área de recepción de la oficina

Se recomienda que el área de recepción en una oficina se sitúe adecuadamente para proporcionar la mejor visión para el personal. Las puertas giratorias o los molinetes pueden proporcionar un acceso controlado. Donde tales elementos forman parte de un camino de escape, se recomienda obtener de la autoridad competente la aprobación para su uso. Se recomienda que las alarmas de entrada, desde las accionadas por la simple activación de una puerta hasta la sofisticada supervisión por CCTV, se complementen con buenos procedimientos administrativos. Se

recomienda utilizar una buena iluminación y avisos claros de seguridad.

10.2 Áreas accesibles a los conductores de los vehículos de entrega

10.2.1 Áreas de entrega y despacho

Siempre que sea posible, se recomienda que las áreas de entrega y de despacho estén separadas unas de otras, y separadas de las entradas usadas por los clientes, el personal y los visitantes. Se recomienda que la iluminación sea óptima en todas las situaciones.

10.2.2 Dársenas de carga y descarga

Se recomienda que las dársenas de carga y descarga se construyan para adaptar la entrada a los tamaños de vehículos y de acoplados. Se recomienda que las áreas de recepción y de despacho sean del tamaño suficiente para permitir que las mercancías puedan ser comprobadas correctamente antes de ser movidas del área de descarga. También se recomienda que la seguridad sea complementada por el uso del CCTV.

NOTA. Se pueden colocar pantallas de caucho o de plástico para ajustar el ancho de las dársenas para evitar el acceso no autorizado

10.2.3 Oficinas de entrega y despacho

Se recomienda que las oficinas de entrega y despacho sean seguras y con buena visibilidad sobre la totalidad de las áreas de carga y descarga. Que el diseño sea tal que no haya zonas ciegas u ocultas, como cavidades, en las cuales se puedan ocultar o perder de vista las mercancías.

NOTA. Espejos estratégicamente colocados, la buena iluminación y el uso del CCTV pueden asistir a la supervisión de cualquier punto ciego.

10.3 Áreas accesibles al personal de mantenimiento

10.3.1 Equipo

Se recomienda que el diseño del edificio permita que el equipo y los servicios de planta, tales como interruptores importantes, gabinetes de congelador, y otros controles se instalen de manera tal que no puedan dañarse accidental ni deliberadamente.

10.3.2 Fuentes de energía

Todas las fuentes de energía deben ser consideradas muy cuidadosamente. Se recomienda que la energía entrante (cables y tuberías) esté contenida en forma segura y en áreas protegidas y que las subestaciones estén en áreas protegidas y seguras. Cuando sea apropiado, se recomienda tener disponibles generadores de reserva.

10.3.3 Teléfono

Se recomienda que los cables de teléfono estén en una canalización segura, en un área protegida, particularmente si conducen señales de alarma remotas.

Se recomienda que los teléfonos públicos y los teléfonos gratuitos de taxi se sitúen en posiciones donde los usuarios no tengan a la vista las cajas de efectivo o cajeros automáticos.

10.3.4 Alarmas y otras instalaciones

Se recomienda que los cables y otros componentes de las instalaciones de baja tensión estén en una canalización segura, en un área protegida.

10.4 Áreas accesibles a todo el personal

Sala para el personal

Excepto para las oficinas y comercios pequeños, se recomienda que se proporcione una habitación para el uso propio del personal, que incluya armarios con llave para sus pertenencias personales, con registros de la asignación de los armarios y un sistema para el control de las llaves.

10.5 Áreas de seguridad solamente accesibles a personal autorizado

10.5.1 Oficinas de manejo de dinero en efectivo

10.5.1.1 Generalidades

Se recomienda que el manejo de dinero en efectivo, cuando no sea en las cajas, solo tenga lugar en una oficina inaccesible al público y totalmente a cubierto de la vista del público. Idealmente, se recomienda que los lugares donde se maneja efectivo no estén aislados, sino que estén integrados en una estructura más grande

para una mayor seguridad. Asimismo, que estén equipados con medios fácilmente disponibles para activar una alarma; que existan procedimientos para el uso en emergencias y que se instruya al personal sobre el uso de dichos procedimientos de emergencia.

Se recomienda que los puntos de acceso se mantengan adecuadamente seguros hasta que el efectivo esté en una caja fuerte o asegurado y protegido; que el efectivo que se depositará en un banco siempre se proteja correctamente mientras esté pendiente la recolección; restringir a un mínimo el efectivo que se mantenga en las instalaciones fuera del horario de atención y se coloque en una caja fuerte que cumpla los requisitos de la EN 1143-1.

10.5.1.2 Movimiento del dinero en efectivo

Se recomienda que la información referente a los movimientos de efectivo esté reservada al personal que tiene relación inmediata con el movimiento. Se recomienda que se revisen todos los procedimientos. Es recomendable depositar efectivo más de una vez por día, dependiendo del nivel de ingresos. Cuando sea posible, se recomienda emplear compañías que se especializan en el retiro de efectivo. Si esto no es posible, se recomienda que se transporte en un vehículo con personal de custodia y que el efectivo esté en un contenedor adecuado con un sistema de supervisión.

Un sector vulnerable respecto a delitos contra transportadoras de caudales es la vía pública entre el vehículo y las instalaciones de los clientes. Se recomienda tener en cuenta la formación de un área segura y protegida para la transferencia del efectivo hacia y desde el vehículo.

10.5.2 Cajas fuertes

LEONID LLONTOP CASTRO
Jefe de Seguridad Casa Matriz
Banco Ciudad Bs. As

10.5.2.1 Generalidades

Se recomienda que las llaves de seguridad, las combinaciones de claves, y otros medios de acceso a las cajas fuertes se controlen estrictamente.

10.5.2.2 Localización de una caja fuerte no empotrada

Se recomienda que las cajas fuertes no empotradas se sitúen contra una pared interior de mampostería y que se sitúen en una posición

donde el personal de seguridad que patrulla pueda verlas. Cuando no es posible obtener una vista directa de una caja fuerte pueden utilizarse espejos o CCTV para ver la caja y su entorno.

NOTA: Cuando se instale un sistema de detección de intrusos (ver 11.3) es importante que cubra el área ocupada por la caja fuerte.

10.5.2.3 Caja fuerte oculta debajo del piso

Se recomienda que las cajas fuertes ocultas debajo del piso se sitúen idealmente en el rincón de un cuarto, para hacer más difícil el ataque y que la instalación se ajuste siempre a las instrucciones del fabricante.

10.5.3 Almacén interno para mercancías de elevado valor

Para almacenar mercancías de un valor más alto podría necesitarse un cuarto más seguro. En otros casos, puede ser suficiente una jaula de alambre protegida por una puerta bloqueable. Se recomienda utilizar precintos de metal o de plástico, controlar bien el acceso al almacén interno, entregar las llaves o el sistema de control de acceso a un número restringido de personas y tener en consideración la instalación de una alarma antirrobo.

10.5.4 Alarmas de pánico

Para la protección del personal que trabaja en lugares tales como oficinas, áreas de manejo de efectivo o donde se almacenan mercancías valiosas, puede ser necesario instalar alarmas de pánico estratégicamente localizadas, activadas mediante un botón que dé una indicación de alarma a otro personal y a la gerencia.

11 SEGURIDAD DEL EDIFICIO FUERA DE HORAS DE TRABAJO NORMALES

11.1 Sala de control

11.1.1 Generalidades

La EN 50133-1 brinda directrices sobre los requisitos de los sistemas de control de acceso para el uso en aplicaciones de seguridad en garitas, salas de control o estaciones centrales.

La IRAM 4173-1 y la IRAM 4173-2 brindan directrices sobre los requisitos de los sistemas de transmisión de la alarma.

11.1.2 Paneles de alarma de incendio y anti-intrusión

Se recomienda que los paneles de alarma de incendio y antiintrusión se localicen dentro de la sala de control y que exista espacio para las baterías de reserva. Además es conveniente que los paneles de señales de alarma y de estado remotas, por ejemplo: de calefacción, de ventilación y de aire acondicionado se sitúen también en la sala de control.

En este caso se recomienda que el personal de seguridad sea responsable en la evacuación de los ocupantes del edificio en caso de incendio o de otras emergencias.

11.1.3 Funciones adicionales realizadas por la sala de control

Pueden también ser parte de las funciones de la sala de control general las funciones siguientes:

- a) el sistema de recepción de público;
- b) la emisión y la codificación de las tarjetas de seguridad de pases;
- c) los paneles de alarma de ascensores;
- d) los registros de seguridad y los datos del personal;
- e) el control periódico de alarmas de áreas especiales, por ejemplo: las salas de computación climatizadas, los cuartos médicos o de servicios ambientales controlados por computadora;
- f) el depósito de los planos de ubicación de las salidas de emergencia y del equipo de lucha contra incendios;
- g) la custodia de llaves y del libro de registro de llaves;
- h) el equipo de primeros auxilios con materiales de salud y de seguridad.

11.1.4 Diseño de sala de control

Se recomienda que la sala de control brinde al personal un nivel apropiado de seguridad y con vidrio antibala donde se requiera. Se recomienda que las puertas de acceso siempre se bloqueen al exterior y, durante el período de presencia de personas, sólo puedan abrirse desde el interior. Se recomienda que la sala de control se construya de material resistente y que la puerta no tenga ninguna manija externa y que los paneles de cristal de la puerta sean de visión solamente unidireccional y antibala.

11.2 Vigilancia por CCTV

11.2.1 Generalidades

Se recomienda que los sistemas de vigilancia por CCTV para el uso en aplicaciones de seguridad cumplan los requisitos de la EN 50132-7.

NOTA. Es importante asegurarse que el uso de CCTV no está en conflicto con las reglamentaciones locales o nacionales.

11.2.2 Grabación de imágenes de CCTV

Se recomienda que el mantenimiento regular de las cámaras, de otros elementos del sistema de CCTV y del dispositivo y soporte de grabación, se realice de modo de asegurar que siempre se mantengan la calidad de la imagen final y de la memoria del acontecimiento.

Se recomienda considerar la generación de hora y de la fecha así como del número de la cámara en la etapa de diseño del sistema.

11.3 Sistemas de detección de intrusos

La instalación de un sistema de detección de intrusos diseñado para detectar automáticamente la entrada a través de puertas, ventanas, de la envolvente del edificio y de movimiento de personas dentro de las instalaciones realza las medidas de seguridad física. Las instalaciones pueden incluir los dispositivos de activación voluntaria con los cuales los ocupantes pueden accionar el sistema en caso de ataque personal o de una emergencia. Se recomienda que la detección no sea, sin embargo, considerada un sustituto de la seguridad física.

NOTA. La IRAM 4175 brinda directrices acerca de los requisitos de los sistemas de alarma para la detección de intrusos.

11.4 Iluminación

11.4.1 Iluminación externa

El objetivo básico de la iluminación de seguridad es eliminar el escondite que brinda la oscuridad.

Cuando la vigilancia de un edificio se realiza mediante patrullas externas puede existir la opción de iluminación externa o interna. Si las instalaciones son separadas, se recomienda considerar la iluminación alrededor del perímetro (dirigida hacia adentro), pues revelará a los intrusos directamente o por su silueta. Si el edificio está en un grupo de edificios linderos, la iluminación interna de las áreas críticas que pueden verse desde el exterior (por ejemplo, vestíbulos de entrada, pasillos, escaleras y descansos, oficinas y pisos de ventas) permiten que se vea el movimiento de intrusos.

Para los edificios con las patrullas internas de seguridad se recomienda que la iluminación externa se dirija en sentido opuesto al edificio para ver fácilmente desde el interior a los intrusos que se acercan. El resplandor de dicha iluminación es útil para dificultar al intruso saber si está siendo observado. Se recomienda tomar precauciones para asegurarse de que el resplandor no moleste y no represente un peligro a los peatones o a los conductores.

Es importante asegurarse de que todos los puntos posibles de entrada y salida estén iluminados. Esto puede significar el proveer iluminación adicional para los senderos de entrada y las ventanas en el nivel del sótano y de la planta baja y cualquier otra abertura de servicio que pueda comprometer la seguridad del perímetro del edificio.

11.4.2 Iluminación de oficinas

La iluminación de seguridad para las oficinas puede proporcionar protección adicional a las cerraduras y a los sistemas de alarma.

Se recomienda proveer iluminación interna en todos los puntos significativos donde el movimiento puede ser visto desde afuera, incluyen-

do escaleras, descansos, pasillos, cuartos del perímetro y vestíbulos de entrada.

11.4.3 Iluminación de comercios

Se recomienda que la iluminación del comercio cumpla las recomendaciones dadas para la iluminación de oficinas (ver 11.4.2). Además se sugiere tomar recaudos para asegurar que las dársenas de carga abiertas sean visibles a las patrullas o a las personas que pasan, y que los accesos y retiros de fachadas no generen áreas oscuras que ofrezcan escondite. La iluminación de la vidriera y la iluminación interior que se ven a través de los umbrales o de ventanas abiertas se pueden utilizar como iluminación de seguridad, pero se recomienda utilizar lámparas de descarga de larga vida antes que las lámparas de filamento de una vida más corta, de uso frecuente en vidrieras.

11.4.4 Instalación y control

Se recomienda que los cables y otros componentes de las instalaciones de iluminación de seguridad estén fuera de la vista y alcance de personal no autorizado, en una canalización segura, en un área protegida. Los cables también se pueden proteger por un sistema de alarma.

Para ser eficaz, se recomienda que la iluminación de seguridad esté funcionando en todo momento relevante. Para las instalaciones exteriores es más conveniente el uso de una célula fotoeléctrica simple, que encienda la luz cuando la luz del día se va desvaneciendo, y la apague cuando la luz del día vuelve. Esto asegura que la iluminación de seguridad esté disponible siempre que sea necesario. Los interruptores de tiempo también se pueden programar para el cambio en la duración del día y utilizarse para los sistemas de iluminación internos necesarios solamente fuera de las horas de oficina normales.

11.5 Niveles de seguridad recomendados

Los niveles de seguridad recomendados son los indicados en el anexo A.

Anexo A
(Informativo)

LEONID LLONTOP CASTRO
Jefe de Seguridad Casa Matriz
Banco Ciudad Bs. As.

Clasificación de riesgos y niveles de amenazas

Tabla A - Grados de seguridad recomendados para lograr los niveles especificados de protección

	Nivel de amenaza			
	1	2	3	4
Riesgo bajo	1	2	3	3
Riesgo medio	2	3	3	4
Riesgo alto	3	3	4	5
Riesgo muy alto	3	4	5	5

A.1 Nivel de amenaza. Percepción de la capacidad, motivación y nivel de habilidad del intruso. Se identifican cuatro niveles de amenaza.

A.1.1 Nivel de amenaza 1. Uno o más individuos poco habilidosos que tienen poco conocimiento de los sistemas de seguridad o de las medidas de protección, que atacan con una planificación pobre o no avanzada, generalmente a determinados bienes con medidas de seguridad escasas o no existentes. Generalmente la motivación es monetaria o vandálica.

A.1.2 Nivel de amenaza 2. Uno o más individuos semicapacitados, con algún conocimiento o habilidad para superar o comprometer medidas de seguridad de bajo nivel. Generalmente la motivación es el beneficio.

A.1.3 Nivel de amenaza 3. Un grupo de individuos capacitados, con una fuerte motivación, habilidad, conocimiento y fondos. Motivados por el beneficio, la atención pública o el corte de servicios.

A.1.4 Nivel de amenaza 4. Un grupo de individuos altamente capacitados con una fuerte motivación, un soporte tecnológico sustancial, conocimiento y fondos. Motivados por el beneficio, la atención pública, sabotaje o actos de guerra.

A.2 Clasificación de bienes (riesgo). Una categoría asignada que tiene la intención de unir las características principales de ese nivel de bienes y clasificar riesgo relativo; se pueden definir cuatro niveles de riesgo.

LEONID LLONTOP CASTRO
Jefe de Seguridad Casa Matriz
Banco Ciudad Bs. As.

A.2.1 Bajo. Pequeños negocios u oficinas con bienes moderados.

A.2.2 Medio. Edificios de oficinas, negocios minoristas, con alta afluencia de público con mercancías de valor apreciable.

A.2.3 Alto. Centros comerciales, negocios minoristas con alto valor de productos, o negocios mayoristas, o lugares de alto riesgo en los cuales se almacenan armas o narcóticos.

A.2.4 Muy alto riesgo. Oficinas de servicios y administración públicos y privados, e instalaciones que resultan atractivas para el nivel de amenaza 4.

Anexo B
(Informativo)

LEONID LLONTOP CASTRO
Jefe de Seguridad Casa Matriz
Banco Ciudad Bs As

Bibliografía

En el estudio de esta norma se han tenido en cuenta los antecedentes siguientes:

IRAM - INSTITUTO ARGENTINO DE NORMALIZACIÓN Y CERTIFICACIÓN

IRAM 3860:1994 - Guía para la seguridad contra ilícitos en inmuebles de uso particular y comercial.

IRAM 12841:1998 - Vidrios de seguridad, antibala y antiintrusión.

BSI - BRITISH STANDARDS INSTITUTION

DD CEN/TS 14383-4:2006 - Prevention of crime - Urban planning and design - Part 4: Shops and offices.

Anexo C
(Informativo)

Integrantes de los organismos de estudio

El estudio de esta norma ha estado a cargo de los organismos respectivos, integrados en la forma siguiente:

Comisión de Prevención del delito mediante el diseño ambiental

Integrante	Representa a
Arq. Gabriel ARTESE	TECNOLOGÍA EN CRISTALES S.A.
Lic. Mabel BELLANDI	PREVENTORES ONG
Arq. Diego CÁNOVAS	MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS
Arq. Carlos GARCÍA BASALO	MINISTERIO DE JUSTICIA Y DERECHOS HUMANOS
Sr. Leandro MOUMAJIAN	GLOBAL DOMAIN S. A.
Ing. Alberto SPARNOCCHIA	CITEFA / INST. DE INV. CIENT. Y TCAS. PARA LA DEFENSA (CITEDEF)
Arq. Marta ZENÓN	MUNICIPIO DE NEUQUÉN
Ing. Jorge CERUTTI	IRAM
Ing. Ángel M. PAONESSA	IRAM
Ing. Guillermo ZUCAL	IRAM
Ing. Juan M. LAVRIC	IRAM

LEONID LLONTOP CASTRO
Jefe de Seguridad Casa Matriz
Banco Ciudad Bs. As

Comité General de Normas (C.G.N.)

Integrante	Integrante
Dr. José M. CARACUEL	Ing. Samuel MARDYKS
Lic. Alberto CERINI	Lic. Héctor MUGICA
Ing. Ramiro FERNÁNDEZ	Ing. Tulio PALACIOS
Ing. Jorge KOSTIC	Tco. Ángel TESTORELLI
Ing. Jorge MANGOSIO	Ing. Raúl DELLA PORTA
Tco. Hugo D. MARCH	



INSTITUTO ARGENTINO
DE NORMALIZACIÓN
Y CERTIFICACIÓN

NORMA IRAM 4171-1

Diciembre 1993

ICS 13.320

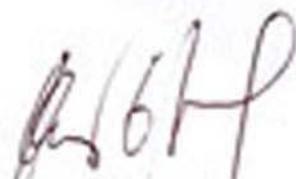
*CNA 6350

SISTEMAS DE ALARMA
Requisitos generales



INSTITUTO ARGENTINO DE RACIONALIZACIÓN DE MATERIALES

* **Corresponde a la Clase Nacional de Abastecimiento asignada por el Servicio Nacional de Catalogación dependiente del Ministerio de Defensa.**


Dirección de Certificación


Comité General de Certificación


Dirección General



Certificado | sistemas de Gestión

PREFACIO

- El estudio de esta norma estuvo a cargo del organismo respectivo, integrado de la forma siguiente:

Comisión de Sistemas de alarma

Integrante

Lic. M. Caliguiri
 Sr. J. M. Consoli
 Ing. C. Cruz
 Arq. E. Gonzalez
 Ing. H. Hamben
 Ing. R. Katz
 Ing. A. H. Martel
 Sr. C. Matinez
 Lic. C. Mecca
 Ing. R. Müller
 Ing. D. Petluik
 Ing. P. Ricci
 Ing. R. Mansour

Representa a:

POLICIA FEDERAL
 POLICIA FEDERAL
 G y K
 E.G. S.A.
 GENERAL INDUSTRIES
 G y K
 VALEO NEIMAN ARG.
 POLICIA FEDERAL
 SITEL GUARD S.A.
 ELECTRÓNICA SEARCH
 SITEL GUARD S.A.
 GENERAL INDUSTRIES
 INSTITUTO IRAM

Comité General de Normas (C.G.N.)

Dr. V. Alderuccio
 Ing. J. Arcioni
 Ing. J. V. Casella
 Dr. E. Catalano
 Ing. D. Donegani
 Lic. C. A. Grimaldi
 Dr. A. Grosso
 Ing. S. Ituarte
 Ing. J. Kostic

Ing. J. Mangosio
 Ing. S. Mardyks
 Ing. R. Martínez
 Dr. E. Miró
 Ing. N. O'Neill
 Dr. A. F. Otamendi
 Sr. F. R. Soldi
 Prof. M. P. Mestanza

- En el estudio de esta norma se ha tenido en cuenta el antecedente siguiente:

IEC - INTERNATIONAL ELECTROTECHNICAL COMMISSION
 IEC Standard 839-1-1 (1988-01) - Alarm Systems - Part 1: General requirements - Section 1: General.

LEONID LLONTOP CASTRO
 Jefe de Seguridad Caso Matriz
 Banco Ciudad Bs. As.



NORMA IRAM

4171-1

Diciembre 1993

SISTEMAS DE ALARMA

Requisitos generales

FE DE ERRATAS N° 1

Setiembre 1994

El subcomité de Sistemas de alarma en su sesión del 94-09-02 (Acta 3) salvó los errores de publicación siguientes:

Párrafo 4.3 Donde dice "4.3 compañía de alarma" debe leerse "4.3 compañía de alarmas".

Párrafo 4.26 Donde dice "para ser ocupada en caso de vigencia" debe leerse "pero no equipada para ser ocupada en caso de urgencia".

SISTEMAS DE ALARMA

Requisitos generales

ICS 13.320
*CNA 6350

INTRODUCCIÓN

Esta norma se corresponde con la publicación de la Comisión Electrotécnica Internacional IEC 839-1-1 (1º Edición 1988) - ALARM SYSTEMS- Part 1: General requirements - Section 1: General.

Con en fin de facilitar su aplicación sigue la misma estructura que el documento internacional, con diferencias de redacción y de forma consideradas necesarias para mantener una unidad de criterio con el conjunto de normas IRAM y lograr una mejor comprensión del texto.

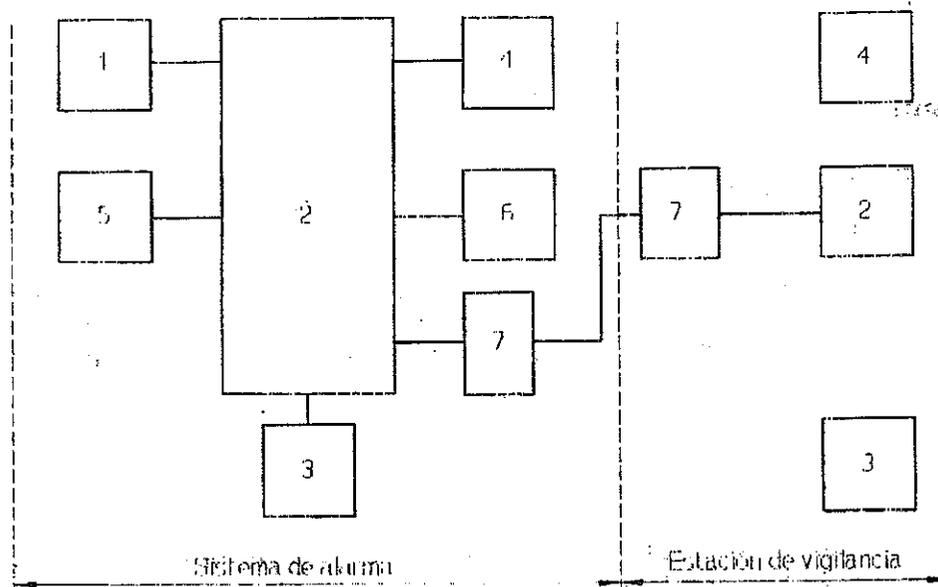
1 CAMPO DE APLICACIÓN

Esta norma define las exigencias generales relativas al diseño, a la instalación, al control después de la instalación, a la puesta en funcionamiento, al mantenimiento como también al registro (archivo) de los sistemas de alarma, manuales o automáticos, utilizados para la protección de las personas, de los bienes y del entorno.

Las exigencias particulares para ciertos tipos de sistemas de alarma se especifican en normas separadas, que deben utilizarse conjuntamente con esta norma, la que no es aplicable a las centrales de control a distancia.

La norma IRAM 4171-2 complementa a esta norma.

* Corresponde a la Clase Nacional de Abastecimiento asignada por el Servicio Nacional de Catalogación dependiente del Ministerio de Defensa.



- 1 - detector
- 2 - unidad central de alarma
- 3 - alimentación
- 4 - órganos de señalización visual y/o sonora
- 5 - dispositivo activado por la unidad central de alarma
- 6 - entradas programables
- 7 - interfase de señalización (modem)

Figura 1 - Elementos comunes de los diferentes sistemas de alarma

2 OBJETO

Asegurar que los sistemas de alarma brinden un nivel elevado de seguridad y de confiabilidad y una calidad de servicio óptima. Reducir las falsas alarmas y asegurar que los sistemas combinados sean compatibles entre ellos.

LEONID LLONTOP CASTRO
 Jefe de Seguridad Casa Matriz
 Banco Ciudad Bs. As

3 NORMAS PARA CONSULTA

Los documentos normativos siguientes contienen disposiciones, las cuales, mediante su cita en el texto, se transforman en disposiciones válidas para la presente norma IRAM. Las ediciones indicadas eran las vigentes en el momento de su publicación.

Todo documento es susceptible de ser revisado y las partes que realicen acuerdos basados en esta norma se deben esforzar para buscar la posibilidad de aplicar sus ediciones más recientes.

Los organismos internacionales de normalización y el IRAM, mantienen registros actualizados de sus normas.

IRAM 2444 - Clasificación de los grados de protección provistos por los encerramientos.

IRAM 4029 - Aparatos electrónicos para uso doméstico y similares. Condiciones generales de seguridad.

IRAM 2010 - Símbolos gráficos electrotécnicos.

IRAM-IAP-IEC 79 - Materiales eléctricos para atmósferas gaseosas explosivas.

IEC 364 - Instalaciones eléctricas en inmuebles.

IEC 617 - Símbolos gráficos para los diagramas.

IEC 839-1-2 - Sistemas de alarma. Primera parte: Exigencias generales. Segunda sección: Dispositivos de alimentación y características de funcionamiento.

IEC 839-1-3 - Sistemas de alarma. Primera parte: Exigencias generales. Tercera sección: Ensayos climáticos y mecánicos para los sistemas de alarma.

IEC 839-2-2 - Sistemas de alarma. Segunda parte: Exigencias para los sistemas de alarma de anti-intrusión. Segunda sección: Exigencias para los detectores. Generalidades.

LEONID LLONTOP CASTRO

Jefe de Seguridad Casa Motriz

Banco Ciudad Bs. As

4 DEFINICIONES

A los efectos de las normas para los sistemas de alarma, son de aplicación las definiciones siguientes:

4.1 **alarma.** Advertencia de la presencia de un peligro para la vida de las personas, para la preservación de los bienes o para el entorno.

4.2 **sistema de alarma.** Instalación eléctrica diseñada para detectar y señalar la presencia de una situación anormal, indicando la presencia de un peligro.

4.3 **compañía de alarma.** Organización que proporciona y/o instala y/o asegura el mantenimiento de los sistemas de alarma.

4.4 **usuario.** Persona u organización que utiliza los servicios de una sociedad de alarma para la provisión, la instalación y/o el mantenimiento de un sistema de alarma.

4.5 **recintos vigilados.** Parte de un edificio y/o de una zona donde puede detectarse un peligro mediante un sistema de alarma.

4.6 **autoridad responsable.** Autoridad designada, a la que incumbe la responsabilidad de tomar las medidas apropiadas, cuando se produce una alarma, en los recintos vigilados.

- 4.7 estado normal.** Estado de un sistema de alarma mientras está plenamente operativo y no está en cualquier otro estado definido.
- 4.8 estado de alarma.** Estado de un sistema de alarma, o de una parte del mismo, provocado por el disparo del sistema de alarma en presencia de un peligro.
- 4.9 estado de falla.** Estado del sistema de alarma que impide su funcionamiento en las condiciones previstas por las normas pertinentes.
- 4.10 estado de ensayo.** Estado de un sistema de alarma en el cual las funciones normales son modificadas con fines de ensayo.
- 4.11 estado fuera de servicio.** Estado creado deliberadamente para tornar inoperante una parte del sistema de alarma.
- 4.12 señal de alarma.** Señal generada por un sistema de alarma, cuando éste está en estado de alarma.
- 4.13 señal de falla.** Señal generada por un sistema de alarma, cuando éste está en estado de falla.
- 4.14 dispositivo de antidesarme (dispositivo "TAMPER").** Dispositivo diseñado para detectar la manipulación deliberada ó no en una parte de un sistema de alarma, ó en un elemento constitutivo del mismo.
- 4.15 detección de desarme.** Detección de la manipulación deliberada ó no en un sistema de alarma ó de un elemento constitutivo del mismo mediante la aplicación de uno ó varios dispositivos de antidesarme.
- 4.16 protección de antidesarme.** Aplicación de medios eléctricos y/ó mecánicos destinados a impedir la manipulación deliberada ó no con un sistema de alarma ó con un elemento constitutivo del mismo.
- 4.17 alarma antidesarme.** Alarma generada por el funcionamiento del dispositivo de antidesarme.
- 4.18 falsa alarma**
- 4.18.1 falsa alarma técnica.** Señal de alarma generada por error y provocada por: un mal funcionamiento, ó defecto de un elemento constitutivo del sistema de alarma.
- 4.18.2 falsa alarma de operación.** Señal de alarma generada por error y provocada por la maniobra accidental de un pulsador normal de alarma o por un error de un operador.
- 4.18.3 falsa alarma por factores externos.** Señal de alarma generada por error y provocada por interferencias electromagnéticas, factores ambientales, y/ó la respuesta de un dispositivo automático en condiciones distintas a las de la concepción original.
- 4.19 alimentación.** Parte de un sistema de alarma que provee la potencia para el funcionamiento de un sistema o de cualquier elemento constitutivo del mismo.
- 4.20 detector.** Dispositivo destinado a provocar el estado de alarma respondiendo a la captación de una situación anormal que indica la presencia de un peligro.
- 4.21 sensor.** Parte del detector que registra un cambio de estado, que puede indicar la presencia de un peligro.

- 4.22 **unidad central de alarma.** Equipo que procesa las señales de salida de uno o de varios detectores para determinar si el estado de alarma debe ser generado.
- 4.23 **estación de vigilancia.** Un emplazamiento situado a distancia de los locales supervisados, donde se recogen las informaciones concernientes al estado de uno o de varios sistemas de alarma, ya sea para la señalización (en el caso de una central de recepción de alarmas) o para la retransmisión (caso de una estación satelital o de un punto de centralización).
- 4.24 **central de control a distancia.** Centro ocupado en forma permanente por personas, al cual se envían las informaciones concernientes al estado de uno o de varios sistemas de alarma.
- 4.25 **estación satelital.** Central normalmente automática, pero equipada para ser ocupada en caso de urgencia, donde se recogen las informaciones concernientes al estado de un cierto número de sistemas de alarma para la retransmisión, directamente o por intermedio de otra estación satelital, hacia un centro de control a distancia.
- 4.26 **punto de centralización.** Central automática sin personal, para ser ocupada en caso de urgencia, donde se recogen las informaciones concernientes al estado de un cierto número de sistemas de alarma para su retransmisión, ya sea directamente o por intermedio de una estación satelital, hacia un centro de control a distancia.
- 4.27 **centro de supervisión.** Centro ocupado por personas, donde se vigila el estado de un sistema de transmisión de alarma.
- 4.28 **sistema mixto.** Sistema de alarma concebido para responder a más de un tipo de peligro.
- 4.29 **sistemas de transmisión de alarma.** Sistema que es utilizado para transferir informaciones concernientes al estado de uno o de varios sistemas de alarma entre lugares supervisados y uno o varios centros de control a distancia.
- 4.30 **comandos manuales.** Interruptores manuales, pulsadores de presión u otros dispositivos de comando que requieran accionamiento manual y tales que posean una influencia sobre el funcionamiento de la unidad central de alarma.
- 4.31 **protección física.** Protección de un elemento constitutivo del sistema de alarma contra un daño, o protección de personas ó bienes contra un peligro.

5 CONSIDERACIONES GENERALES

5.1 **OBJETIVOS DEL SISTEMA.** Un sistema de alarma debe responder a los criterios siguientes:

- a) una señal de alarma puede iniciarse en cualquier instante;
- b) deben reducirse los riesgos de falsas alarmas al mínimo;
- c) señalar las fallas;
- d) poder realizar ensayos sin interrupción significativa de su funcionamiento normal.

5.2 PLANEAMIENTO. Debe procederse a la búsqueda de informaciones teniendo en cuenta por una parte la evaluación de los tipos de riesgo a que pueden estar expuestos la zona protegida ó sus ocupantes, y, por otra parte la determinación de necesidades a cubrir por los diversos sistemas de alarma.

5.2.1 Especificación. Los requisitos para el sistema de alarma deben establecerse tan exactamente como sea posible, después de una consulta entre las partes interesadas (es decir entre el abonado, el ingeniero consultor, el instalador, la sociedad de vigilancia, las administraciones de telecomunicaciones, de policía local o los bomberos, el asegurador y todos los poderes públicos involucrados).

5.2.2 Conexión a distancia a una central de vigilancia. En el caso que se prevé la transmisión de señales de alarma hacia una central de vigilancia debe concertarse previamente entre las partes interesadas de manera de definir claramente la información a transmitir, así como las medidas a tomar ante la recepción de una señal de alarma, de una falla, de una señal de ensayo y de cualquier otra señal.

5.3 NIVELES DE RIESGO Y/O GRADOS DE URGENCIA. La relación existente entre el tipo de sistema de alarma y el nivel de riesgo involucrado está indicada en la norma IRAM 4 171-2*.

6 EXIGENCIAS

6.1 CONSIDERACIONES GENERALES. Un sistema de alarma se compone generalmente de tres partes: la que activa la señal, una parte a través de la cual se transmite la señal y por último la que recibe la señal. Además, en el sistema de alarma se incluyen una o más alimentaciones (fig.1).

Pueden integrarse sistemas de alarma en otros tipos de sistemas, en la medida en que ello sea conforme a las normas que rigen los sistemas de alarma, y que la función de cada uno de los sistemas de alarma no sea alterado por uno cualquiera de los otros sistemas, incluidos los sistemas de alarma.

6.1.1 El sistema debe ser diseñado de modo de proporcionar una indicación clara y no ambigua del origen de la señal de alarma.

Los sistemas de alarma deben diseñarse de modo de permitir el acceso fácil a los fines de mantenimiento y de servicio después de la venta en tanto que se restringirán en lo posible las posibilidades de acceso no autorizado a esos mismos sistemas de alarma.

6.1.2 Marcado. Se marcarán claramente y de manera permanente sobre los aparatos el nombre o el símbolo del fabricante, así como el número del modelo.

Cuando lo permita el diseño del dispositivo se marcará sobre él mismo en forma clara y permanente la información adicional siguiente:

- número de serie;
- fecha de fabricación (se admite el uso de códigos);
- características de la alimentación eléctrica (por ejemplo, tensión nominal, corriente nominal, frecuencia nominal).

* Hasta tanto termine el estudio de esta norma se consultará a la IEC 839-1-4.

Cuando el diseño del aparato no lo permite, los datos deben figurar en las especificaciones que acompañan el dispositivo o sobre su embalaje. Los bornes y los cables deben ser numerados, coloreados o identificados mediante otro medio.

El marcado debe ser durable y fácilmente legible. Para verificar las propiedades del marcado se realizará un examen visual luego de frotarlo con la mano durante 15 s con la ayuda de un paño impregnado con agua y a continuación, durante 15 s con un paño impregnado con nafta. El marcado debe permanecer fácilmente legible; las placas con el marcado no serán fácilmente removibles y no presentarán ningún signo de haber sido forzados.

6.1.3 Datos a suministrar con los dispositivos. El dispositivo se acompañará con instrucciones dando detalles sobre su instalación correcta si ello no aparece claramente sobre el aparato mismo.

Cualquier aparato que pueda ser dañado a consecuencia de la inversión de la polaridad de la entrada, ésto deberá estar claramente mencionado en las instrucciones que lo acompañan.

6.2 SISTEMAS COMPLETOS.

6.2.1 Cuando el sistema de alarma está instalado todos los circuitos de detección y de señalización utilizados para transmitir un estado de alarma, deben estar capacitados para detectar e indicar fallas, que no sean las que equivalen a un estado de alarma. Los diversos elementos constitutivos de un sistema de alarma deben satisfacer las exigencias de las normas pertinentes. Conviene vigilar que todos los elementos constitutivos del sistema sean compatibles entre sí y conformes a la especificación pertinente.

6.2.2 Condiciones ambientales. Los equipos utilizados en ambientes hostiles, tales como depósitos frigoríficos, talleres de metalizado o atmósferas corrosivas, deben responder a una especificación apropiada o, ante la falta de tal especificación, serán provistos de medidas particulares de protección, a los efectos de tener en cuenta los riesgos específicos.

Ante la posibilidad de que puedan existir riesgos de interferencias importantes provenientes de otros equipos o de fuentes externas, tales como rayos o transitorios en la alimentación, se tendrá un cuidado especial en el diseño y la instalación de los equipos de alarma con el fin de reducir los riesgos de señales interferentes que afecte el funcionamiento normal del sistema.

Para otros detalles, referirse a las normas específicas relativas a los equipos y a los ensayos mencionados en la publicación IEC 839-parte 1-Sección 3.

6.2.3 Seguridad. Los sistemas de alarma deben responder a las normas de seguridad que figuran en las normas IRAM 4029 e IEC 364. La construcción mecánica de cada una de las partes del sistema debe ser tal, que deberá reducir cualquier riesgo de daño originado por una inestabilidad mecánica del sistema, así como por aristas filosas en movimiento y saliencias.

El nivel de las señales en las áreas donde se permite el acceso a personas técnicamente incompetentes no deberá presentar ningún peligro.

En el caso en que se prevea instalar sistemas en zonas especiales, por ejemplo en atmósfera explosiva, deberá satisfacerse la publicación IEC 79.

6.2.4 Interferencias. El sistema no debe producir interferencia con otros sistemas o equipos (por ejemplo interferencia de radiofrecuencia). Los niveles de radiación no deben exceder los límites nacionales y/o internacionales.

6.3 COMPONENTES DE UN SISTEMA DE ALARMA. Las exigencias generales aplicables a los componentes de un sistema de alarma (por ejemplo las fuentes de alimentación y los detectores) están indicadas en la norma específica de cada componente de un sistema.

6.4 SISTEMAS DE TRANSMISIÓN. Los sistemas de transmisión deben diseñarse de manera de asegurar una transmisión confiable de la señal de alarma desde el transmisor hasta el receptor. El tiempo de transmisión debe ser compatible con, por una parte, la especificación general del sistema y, por otra parte, con las posibilidades de las líneas de transmisión. No obstante, en muchos casos la elección del sistema de transmisión puede depender de las reglamentaciones locales.

Si ocurre una falla en la línea de comunicación haciendo imposible la transmisión de una alarma, debe generarse en el centro de vigilancia una indicación de falla, mientras los medios de enlace lo permitan.

6.5 SISTEMAS MIXTOS.

6.5.1 Prioridad. En los sistemas mixtos debe darse prioridad a la transmisión de las alarmas y a las medidas que tienen por objeto preservar la vida de las personas.

6.5.2 Protección de los sistemas de alarma. En el caso en que los sistemas de alarma utilicen equipos, circuitos de control y de transmisión comunes para la detección o la señalización de más de algún tipo de peligro o de contingencia, se proveerá una protección para el sistema con la exigencia más severa de cada uno de los elementos constitutivos de los sistemas mixtos.

7 INSTALACIÓN

7.1 CONSIDERACIONES GENERALES. Para permanecer eficiente, el sistema de alarma instalado originariamente en un inmueble, puede cada tanto sufrir extensiones y/o modificaciones durante la vida útil del inmueble. Por lo tanto se tendrán cuidadosas consideraciones en la primera etapa, con las dimensiones y el emplazamiento de los conductos, cables, etc., de modo de permitir, en la medida de lo posible, extensiones y modificaciones ulteriores con un máximo de flexibilidad.

Son también de importancia la facilidad de mantenimiento, así como la protección adecuada del sistema contra los daños mecánicos y las manipulaciones no autorizadas revisten también importancia.

Al fijar el emplazamiento necesario para la unidad central de alarma y la alimentación es necesario asegurar el acceso a esos equipos con fines de mantenimiento y de servicio. La instalación de un sistema de alarma debe efectuarse de acuerdo con la Publicación IEC 364. El método de conexión a los conductos debe indicarse en las exigencias generales de la norma relativa a cada sistema individual de alarma.

8 PROCEDIMIENTO DE ENSAYO

8.1 PUESTA EN SERVICIO. Antes de transferir el sistema de alarma al usuario, los ensayos deben asegurar que el sistema funciona de manera satisfactoria y que se cumplen todas las exigencias. Si un sistema existente ha sido ampliado o modificado, se debe ensayar el sistema completo con el fin de asegurarse que el mismo funciona de manera satisfactoria y;

- a) que todos los equipos y conexiones funcionan correctamente y que responden a la especificación de la instalación;
- b) que cualquier conexión con la policía, los bomberos, o a la central de vigilancia funciona correctamente.

Una vez que los ensayos de puesta en servicio hayan sido efectuados con resultado satisfactorio, el instalador debe certificar que el sistema de alarma cumple con la especificación, o indicar en el certificado las desviaciones con respecto a la especificación que hayan sido aceptadas.

Puede convenirse que durante un período de tiempo la supervisión del sistema será efectuada por el instalador.

El instalador debe indicar al usuario los factores que pueden modificar el buen funcionamiento del sistema de alarma, los requisitos acerca de un mantenimiento de rutina, así como la necesidad de evitar maniobras o prácticas que pudieran generar falsas alarmas. Una vez terminado el control después de la instalación y la puesta en servicio del sistema, se hará una demostración práctica al usuario de los procedimientos de operación.

9 FUNCIONAMIENTO Y MANTENIMIENTO

9.1 CONSIDERACIONES GENERALES. El fabricante debe proporcionar al propietario y/o al usuario del sistema instrucciones de operación escritas y/o ilustradas.

9.2 SERVICE Y MANTENIMIENTO. El fabricante debe proporcionar recomendaciones relativas al mantenimiento y al service después de la venta.

9.3 FICHAS. Deben establecerse registros para los sistemas de alarma. Los tipos de fichas deben precisarse en el "código de práctica" (Norma IRAM 4171 Parte 2)* o en las normas relativas a los sistemas de alarma específicos.

* Hasta tanto se termine el estudio de esta norma se consultará la IEC 839-1-4.

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100

1



INSTITUTO ARGENTINO
DE NORMALIZACIÓN
Y CERTIFICACIÓN

NORMA IRAM 4171-2
IEC STANDARD 839-1-4
Junio 1994

ICS 13.320

*CNA 6350

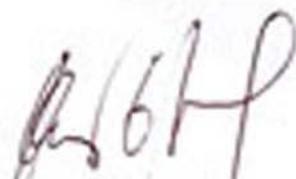
**SISTEMAS DE ALARMA
CÓDIGO DE PRÁCTICA**

Con relación a los requisitos generales



INSTITUTO ARGENTINO DE RACIONALIZACIÓN DE MATERIALES

* Corresponde a la Clase Nacional de Abastecimiento asignado por el Servicio Nacional de Catalogación del Ministerio de Defensa.


Dirección de Certificación


Comité General de Certificación


Dirección General



Certificado | sistemas de Gestión

Prefacio

El estudio de esta norma estuvo a cargo de los organismos respectivos, integrados de la forma siguiente:

Comisión de Alarmas

Integrante

Representa a:

Ing. H. Amden	GENERAL INDUSTRIES
Lic. M. Caligiuri	POLICIA FEDERAL ARGENTINA
Arq. E. Gonzalez	INVITADO ESPECIALIZADO
Ing. C. Cruz	G. Y K. S. A.
Ing. J.D. Méndez	SISTEMA ELECT. INTELIG.
Ing. E. Ricci	GENERAL INDUSTRIES
Ing. R. Mansour	INSTITUTO IRAM

COMITÉ GENERAL DE NORMAS

Dr. V. Alderuccio	Ing. S. Mardyks
Ing. J. Arcioni	Ing. R. Martínez
Ing. J.V. Casella	Dr. E. Miró
Dr. E. Caralano	Ing. N. O'Neill
Ing. D. Donegani	Dr. A.F. Otamendi
Lic. C.A. Grimaldi	Sr. F.R. Soldi
Dr. A. Grosso	Prof. M.P. Mestanza
Ing. S. Ituarte	
Ing. J. Kostic	
Ing. J. Mangosio	

Antecedentes

En el estudio de esta norma se ha tenido en cuenta el antecedente siguiente:

IEC - INTERNATIONAL ELECTROTECHNICAL COMMISSION
IEC Standard 839-1-4 - Alarm systems - Part 1: General requirements -
Section Four Code of practice

LEONID LLONTOP CASTRO

Jefe de Seguridad Casa Matriz
Banco Ciudad Bs. As

INDICE

	Página
Prefacio	2
Introducción	5
0 - Normas para consulta	5
1 - Objeto y campo de aplicación	5
2 - Definiciones	6
3 - Consideraciones generales	6
4 - Requisitos relativos al sistema	7
5 - Sistemas combinados	9
6 - Instalación	11
7 - Puesta de funcionamiento	12
8 - Medidas a tomarse en caso de alarma	13
9 - Mantenimiento	13
10 - Servicio de urgencia	14
11 - Archivos	14

0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99

100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200

SISTEMAS DE ALARMA**CÓDIGO DE PRÁCTICA****Con relación a los requisitos generales**

ICS 13.320

*CNA 6350

INTRODUCCIÓN

Esta norma es equivalente a la Publicación de la Comisión Electrotécnica Internacional IEC Standard 839-1-4 (1989) Alarm Systems Part 1: General requirements. Section 4 - Code of practice.

Con el fin de facilitar su aplicación sigue la misma estructura que el documento internacional, con matices de redacción y de forma derivados de su traducción al castellano considerados necesarios para mantener una unidad de criterio con el conjunto de normas IRAM y lograr una mejor comprensión del texto.

0 NORMAS PARA CONSULTA

Los documentos normativos siguientes contienen disposiciones, las cuales, mediante su cita en el texto, se transforman en disposiciones válidas para la presente norma IRAM. Las ediciones indicadas eran las vigentes en el momento de su publicación.

Todo documento es susceptible de ser revisado y las partes que realicen acuerdos basados en esta norma se deben esforzar para buscar la posibilidad de aplicar sus ediciones más recientes.

Los organismos internacionales de normalización y el IRAM, mantienen registros actualizados de sus normas.

IRAM 4171-1 (1993) - Sistemas de alarma. Exigencias generales. Generalidades

ISO 7731 (1986) - Señales de advertencia de peligro, audible para lugares de trabajo

IEC 849 (1989) - Sistemas electroacústicos para servicios de emergencia.

1 OBJETO Y CAMPO DE APLICACIÓN

La presente norma se aplica al diseño, a la instalación, al control después de la instalación, a la puesta en funcionamiento, al mantenimiento, a los ensayos como así también a los requisitos de los sistemas de alarma manuales y automáticos utilizados para la seguridad y la protección de las personas y de los bienes.

No es aplicable a los centros de vigilancia a distancia. Se utilizará conjuntamente con la norma para requisitos generales para sistemas de alarma IRAM 4171-1.

* Corresponde a la Clase Nacional de Abastecimiento asignado por el Servicio Nacional de Catalogación del Ministerio de Defensa.

2 DEFINICIONES

Para los fines de esta norma, las definiciones de la norma para los requisitos generales para sistemas de alarma (IRAM 4171-1) son aplicables conjuntamente con los siguientes:

2.1 niveles de riesgo. Grado de peligro que existe en el ambiente al cual están sometidos las personas y los bienes.

2.2 nivel de protección. Resultado de las medidas tomadas en el plano técnico y de organización para asegurar la protección y seguridad de las personas y de los bienes.

2.3 nivel de seguridad. Parte del nivel de riesgo cubierto por el nivel de protección.

3 CONSIDERACIONES GENERALES

3.1 Planificación

La norma que trata los requisitos generales para los sistemas de alarma indica que estos requisitos deben ser definidos mediante una consulta entre las partes interesadas. Sobre la base de esta consulta se prepararán los planos/especificaciones que indiquen:

- a) el detalle de la instalación del sistema de alarma propuesto;
- b) el sitio requerido para el equipo;
- c) las ranuras, los tubos, los conductos, los canales, etc. necesarios para el pasaje de los cables, y los accesorios necesarios para su adecuada separación;
- d) el suministro de energía.

3.2 Cronograma

Una lista típica de las operaciones a tenerse en cuenta, probable pero no necesariamente en el orden indicado, para preparar el cronograma es la siguiente:

- a) inspección del inmueble o examen de los planos y una evaluación del uso que se le da al inmueble;
- b) consideración de las medidas a tomarse en el caso de activación del sistema de alarma;
- c) concepción del sistema a los fines estimativos teniendo en cuenta los requisitos/recomendaciones de las partes interesadas;
- d) evaluación de los costos;
- e) consideración y cumplimiento de las especificaciones y de las notas;
- f) pedido del sistema;
- g) acuerdo sobre las medidas a tomarse en caso de activación del sistema;
- h) planificación detallada para la instalación;
- i) producción y entrega;

- j) instalación del sistema;
- k) puesta en servicio y ensayo del sistema por parte de la compañía de alarmas;
- l) entrega del sistema al usuario, conjuntamente con las instrucciones escritas concernientes al funcionamiento y al mantenimiento;
- m) conexión a la señalización a distancia especificada, si no fuera en el momento de la entrega.

Es conveniente incluir todas estas etapas en el cronograma utilizado para grandes trabajos de construcción. Para ciertas instalaciones importantes, los equipos de comando y de indicación se fabricarán especialmente y se enfatiza la importancia de pedir tal equipo especial.

En los inmuebles en construcción o reconstrucción puede ser necesaria una protección física temporaria para proteger el equipo contra los daños eventuales.

Es importante que la conexión final y la puesta en funcionamiento del sistema se hiciera en el momento acordado entre el usuario y el instalador.

3.3 Niveles de riesgo/grado de urgencia

El tipo de sistema elegido debe conferir a los bienes y a las personas expuestas a un riesgo, un nivel de protección compatible con la importancia del riesgo susceptible de producirse, así como con sus posibles consecuencias resultantes de la materialización del riesgo, de manera que el nivel de seguridad requerido esté asegurado.

Esto puede incidir en el tipo y en el número de dispositivos de alarma, en el modo de transmisión de la señal de alarma, en el dispositivo de autoprotección del sistema de alarma, así como en el sistema de recepción de las alarmas, etc., tal como se establece en la norma IRAM* correspondiente.

3.4 Reglamentaciones relativas al medio ambiente

El instalador, o el usuario deben asumir ciertas responsabilidades previstas por la legislación cuando se utiliza un sistema de alarma, por ejemplo cuando se utilizan detectores que contienen material radiactivo. En estos casos, las autoridades oficiales deben ser consultadas desde la etapa preliminar de la concepción del sistema.

4 REQUISITOS RELATIVOS AL SISTEMA

LEONID LLONTOP CASTRO
Jefe de Seguridad Casa Matriz
Banco Ciudad Bs. As.

4.1 Consideraciones generales

Las características de un sistema de alarma como así también su finalidad, deben ser objeto de un minucioso diseño.

Si, para obtener una indicación clara y no ambigua del origen de la alarma, se hace necesario dividir el sistema en zonas o circuitos, conviene que el diseño mismo del sistema permita tal división.

Cuando se diseña un sistema de alarma conviene que se dejen posibilidades para que el sistema pueda ser objeto de extensiones y/o modificaciones.

* En caso de no existir norma IRAM sobre el tema se consultará la IEC correspondiente.

El número de detectores a conectarse a cualquier circuito se decidirá de manera de identificar en forma práctica la naturaleza de la alarma y su origen. El sistema debe ser diseñado de manera tal que una alarma que se produzca en una parte del sistema no afecte otras partes del mismo.

Es preferible que las fallas técnicas estén indicadas separadamente en la central de alarma.

Se deben especificar ensayos de rutina para que se revelen las fallas no detectadas por los procedimientos de supervisión normales.

Los sistemas de alarma estarán diseñados de manera que el buen funcionamiento del sistema no puede ser perjudicado por personal no especializado que accione cualquier elemento de comando manual.

Se recomienda tomar las medidas necesarias que permitan efectuar el ensayo de los detectores individuales sin generar una alarma.

4.2 Condiciones del medio ambiente

El sistema estará diseñado de tal manera que satisfaga el comportamiento especificado en las condiciones ambientales a las cuales es susceptible de ser expuesto en los lugares protegidos, incluyendo el daño mecánico, el clima, la humedad, la corrosión, los aceites industriales así como el calor y la polución industrial.

Conviene tener en cuenta tanto las condiciones ambientales en el interior de los locales, como ser tratamientos industriales, sistemas de calefacción y de ventilación y los animales, como también las exteriores a los locales como ser condiciones atmosféricas extremas, actividades operacionales en locales próximos y el tránsito.

Ya que el sistema de alarma puede ser instalado tanto en el interior como en el exterior de los edificios en diversas condiciones en lo que concierne a la temperatura, a la humedad, a las condiciones climáticas y atmosféricas, a las posibilidades de daños mecánicos, etc. puede exigirse en la especificación del sistema una información completa referida a las condiciones ambientales.

4.3 Detectores

4.3.1 Dispositivos operados manualmente

El emplazamiento de los dispositivos será tal que limite el riesgo de operación accidental o bien de una operación mal intencionada y que aun así, sea de fácil acceso para el usuario.

Conviene que los diferentes métodos de operación de los dispositivos manuales en una instalación sean extremadamente restringidos.

4.3.2 Dispositivos de detección automática

Existen detectores de alarma que funcionan en una amplia gama de principios de operación. Ningún tipo de detector es adecuado para todas las aplicaciones, y la elección final depende de las circunstancias individuales. En algunos casos es preferible combinar diferentes tipos de detectores para proteger una zona en particular.

En cualquier sistema de alarma automático, el detector debe discriminar entre un riesgo de alarma real y el medio ambiente normal existente dentro del ámbito protegido. En el sistema de alarma debe emplear detectores que estén adaptados a las condiciones en las que se los va a utilizar y suministrar una señal de alarma rápida y confiable.

Los detectores conviene instalarlos de manera que suministren un área de cobertura de riesgo satisfactoria, que estén montados en forma segura sobre una estructura fija, libre de vibraciones y de choques y que se hallen ubicados en un lugar inaccesible a las personas no autorizadas. Toda regulación de su posicionamiento conviene en principio, que requiera la utilización de una herramienta. Conviene prestar atención a los riesgos de obstrucción del detector que pueden resultar debido a una modificación eventual de la disposición de la zona por proteger.

La sensibilidad del detector se recomienda elegirla de manera que proporcione el grado de protección necesario sin causar falsas alarmas debido a condiciones ambientales.

4.4 Equipo de control y de señalización

El equipo de control y de señalización puede comprender un equipo para la recepción, el control, el registro y la transmisión de señales provenientes de dispositivos de detección conectados a él y para la activación de sirenas y de dispositivos de señalización.

El sistema de alarma estará diseñado de manera que indique claramente el lugar de origen de la alarma.

Las alarmas y las fallas se indicarán separadamente.

4.5 Sistemas de transmisión

Es conveniente que los sistemas de alarma permitan la transmisión de señales de alarma a un centro de vigilancia a distancia (policía, etc.) así como el envío de una advertencia de falla.

Se recomienda que la vía de transmisión que parte de un local protegido sea subterránea u oculta. Si el sistema estuviera conectado en forma permanente al centro de vigilancia, conviene controlar en forma continua la vía de transmisión, de manera que, en caso de falla, la indicación de falla sea recibida en la central de recepción. Si la vía de transmisión no está controlada permanentemente para detectar fallas eventuales, entonces es conveniente especificar un programa de ensayos de rutina.

5 SISTEMAS COMBINADOS

LEONID LLONTOP CASTRO
Jefe de Seguridad Casa Matriz
Banco Ciudad Bs. As

5.1 Generalidades

Al planificar la instalación de un sistema de alarma en una construcción se recomienda tener en cuenta otros sistemas de alarma, eventualmente destinados para otros fines que pueden estar instalados o bien estar prevista su instalación en el mismo inmueble o en la misma propiedad. Es posible que las funciones de cualquiera de aquellos sistemas podrían combinarse ventajosamente con el sistema de alarma por instalarse, proporcionando de esta manera un servicio más completo.

Es importante asegurar que los sistemas múltiples, tanto en lo que concierne a su pre-planificación, su mantenimiento, su puesta en servicio y su funcionamiento sean compatibles los unos con los otros, sin reducir el nivel de rendimiento para los cuales son individualmente capaces y que no creen confusión entre sus modos diferentes de funcionar y de control o entre la diversidad de señales que generan.

Los sistemas de alarma frecuentemente son un elemento más en un proyecto destinado a la protección para los locales y a sus ocupantes, y algunas veces se utilizan conjuntamente con características de infraestructura, reglas de vigilancia humana, etc. para asegurar un nivel predeterminado de defensa contra contingencias adversas.

Otros aspectos por tener en cuenta al establecer este nivel predeterminado de defensa son: la probabilidad de una reacción correcta por parte de los ocupantes, su grado de vulnerabilidad y la del inmueble como un todo.

Al implementar un sistema de alarma en un inmueble deben prever los efectos de la puesta en funcionamiento ó de una falla en el sistema, sobre los dispositivos de defensa contra formas diferentes de riesgos ó peligros.

Por lo tanto es importante que las exigencias de confiabilidad impuestas a los sistemas de alarma por las normas de seguridad en general sean rigurosamente respetadas.

5.2 Prioridad de requisitos para sistemas de alarma

Si en algún caso, debido a los requisitos conflictuales inherentes a los diversos sistemas de alarma utilizados, se hace necesario tener que elegir entre la calidad del servicio o la confiabilidad, conviene dar prioridad a las consideraciones tendientes a preservar la vida de las personas.

El carácter inminente de peligro de vida de las personas debe ser el factor determinante donde la vida puede estar en juego por más de un tipo de peligro. El incendio es el siniestro susceptible de crear la pérdida más grande si no es detectado inmediatamente.

5.3 Comando de los sistemas de alarma

Conviene que el grado de influencia provisto por los elementos de comando manuales sobre la operación de activación de todo sistema de alarma individual se decida por una evaluación sobre la probabilidad del mal uso de dichos elementos de comando y las consecuencias resultantes. Los elementos de comando que permiten la activación de un sistema de alarma por comando manual deben estar concebidos de manera que sus funciones sean evidentes. La concepción de las centrales de alarma debe hacer imposible la activación del sistema de alarma, a menos que se utilicen en forma correcta los elementos de comando suministrados con ellas.

En caso de iniciarse procedimientos de emergencia, es esencial que las alarmas sonoras no interfieran o se superpongan a las utilizadas en éstos operativos de emergencia.

Todas las alarmas sonoras instaladas en los inmuebles estarán provistas con dispositivos que permitan silenciarlas.

5.4 Activación de la alarma

En el caso que se prevea que una alarma se active manualmente, los dispositivos de accionamiento manual destinados al mismo fin (prevenir un mismo peligro), se recomienda que funcionen de la misma manera y se identificarán en forma similar.

Si, en un mismo inmueble se prevé la posibilidad de activar la alarma en forma manual para más de un tipo de alarma, los dispositivos de comando destinados para diferentes fines (para prevenir diferentes peligros) serán claramente diferenciables unos de otros. Los sistemas de alarma pueden ser diseñados para dar una advertencia automática de una situación o hecho particular localizados en una zona determinada de un inmueble y éste puede contener varios de dichos sistemas. En tales casos, las señales de alarma conviene que sean transmitidas hacia centros específicos donde será comprendido su significado. Es posible que los dispositivos de detección automática previstos para diferentes fines (para detectar diferentes tipos de problemas) operen con principios de funcionamiento similares. Por lo tanto es posible que los sistemas de alarma que incorporen un sistema de conexión automática a un servicio de urgencia pueden hacer intervenir un servicio de urgencia inapropiado para hacer frente al evento que haya provocado la alarma.

Para evitar la intervención de un servicio de emergencia inadecuado, se tendrá en cuenta, desde la etapa de diseño, el posicionamiento de los dispositivos de detección y la elección de los principios de funcionamiento en que éstos operan.

5.5 Señales de alarma

Cuando se tienen que instalar sistemas de alarma para transmitir más de un tipo de peligro o evento, las señales de alarma para cada tipo de alarma conviene sean fácilmente identificables una de otra, a menos que la acción de intervención sea idéntica.

El funcionamiento de los dispositivos de señales de alarma sonoras no entorpecerá la comunicación que es esencial en un caso de urgencia y en particular no interferirá con la facilidad e inmediatez del pedido de ayuda formulado por teléfono o por cualquier otro medio.

NOTA: Las normas ISO 7731 e IEC 849 tratan las señales de evacuación.

5.6 Medidas a tomarse en caso de señales de alarma

Las medidas a tomarse en caso de alarma por parte de los ocupantes de un inmueble se definirán previamente mediante la estrecha colaboración con los organismos que tengan autoridad para aprobarlas y que sean competentes para determinar todos los factores a tenerse en cuenta cuando se decide cuál medida debe emprenderse en caso de alarma y qué señales sonoras y/o visibles se consideran apropiadas para ser previstas.

6 INSTALACIÓN

LEONID LLONTOP CASTRO

Jefe de Seguridad Casa Moritz

Banco Ciudad Bs As

6.1 Cableado

La selección y el material del conductor de conexión y su aislación serán tales que la tensión, aplicada a cualquier dispositivo o equipo, no sea menor que su tensión de funcionamiento mínima especificada, cuando se mida en las condiciones de consumo máximo.

6.2 Uniones

Las uniones del cableado de conexión serán eléctrica y mecánicamente efectivas y eléctricamente aisladas unas de otras. Las uniones entre conductores utilizarán un tablero con bornes recubiertos con un material aislante o bien estarán alojados en el interior de una caja de conexión.

Otros dispositivos de conexión (por ej.: fichas, conectores o empalmes, etc.) pueden utilizarse cuando corresponda, siempre que las conexiones de conductores hacia esos dispositivos sean eléctrica y mecánicamente efectivas y eléctricamente aislados unos de otros.

6.3 Conexiones flexibles

Las conexiones flexibles serán tales que el cableado y la aislación no sufrirán fatiga o esfuerzos en la aplicación particular.

6.4 Protección

Todo cableado conviene esté fijado adecuadamente por soportes y dispuesto o protegido de manera de evitar daños desde y hacia el medio ambiente en el cual se los utiliza. Se recomienda además proteger al cableado para dificultar daños accidentales o intencionales a los conductores.

6.5 Trabajos fuera del lugar de instalación

El equipo puede ser inspeccionado y ensayado en los talleres del fabricante, si se acordara de esta manera. El embalaje protegerá el equipo contra los daños que se puedan producir durante el transporte y el almacenarse y será etiquetado de tal manera que cada unidad pueda ser identificada. El equipo no se entregará antes de que se pueda efectuar la instalación, a menos que se haya dispuesto un lugar de almacenaje adecuado (incluyendo los aspectos de seguridad, que pueden ser de importancia).

6.6 Trabajos en el lugar de instalación

La instalación de los equipos de alarmas no se efectuará en la proximidad de fuentes de temperaturas extremas, como ser calefactores o acondicionadores de aire, si influyen en forma negativa sobre su funcionamiento. El trabajo por efectuarse en el lugar consiste en lo siguiente:

- a) instalación en un lugar que permita el mantenimiento;
- b) posicionamiento de la central de alarma, de las sirenas, de los dispositivos de señalización visual, de los detectores y de los dispositivos manuales de alarma;
- c) cableado y conexión;
- d) instalación del equipo;
- e) inspección, ensayo y control después de la instalación.

6.7 Extensiones y modificaciones

Si el trabajo por efectuarse consiste en una extensión de una instalación ya existente, conviene que se ensaye en forma completa el equipo existente para asegurar que funcionará satisfactoriamente con el equipo complementario y que las fuentes de alimentación tengan una capacidad suficiente para hacer frente a la carga adicional. Si el funcionamiento de los dispositivos de señalización sonora y/o la transmisión de señales de alarma se interrumpe cuando se conecta al equipo ya existente, conviene efectuar nuevos ensayos para asegurar el funcionamiento correcto de los dispositivos de señalización sonora y, si se autorizara, de los circuitos de transmisión de alarma.

7 PUESTA EN FUNCIONAMIENTO

Se recomienda que se entregue un certificado escrito después de verificar el funcionamiento del sistema en presencia del usuario y/o propietario. Una vez que se haya aceptado el certificado entregado por el instalador, el funcionamiento del sistema es responsabilidad del comprador.

El propietario o el ocupante de los locales debe designar una persona responsable para asegurar la supervisión del sistema. A esta persona se le debe dar suficiente autoridad como para que pueda asegurar la ejecución de todos los trabajos necesarios para mantener el sistema en buen estado de funcionamiento, el cumplimiento de las especificaciones prescriptas y el servicio de mantenimiento.

Los usuarios de la instalación deben ser instruidos para utilizar en forma correcta el sistema de alarma.

Se recomienda precisar los procedimientos a seguir en caso de alarma, de advertencia de falla o bien de puesta en servicio en forma parcial o total del sistema. Estos procedimientos serán autorizados por las autoridades competentes antes de su aplicación (ver capítulo 8).

Se establecerá contacto con aquellos responsables del mantenimiento del edificio y de su redecoración, etc., para asegurar que su trabajo no provoque fallas de funcionamiento en la instalación de alarma o bien interferencia de alguna otra manera con su funcionamiento.

Es conveniente que el usuario se asegure que el espacio disponible alrededor de cada detector quede libre y que todos los elementos de comando queden sin obstruir.

Si se producen modificaciones en el orden estructural o de ocupación, el usuario debe asegurarse que las modificaciones necesarias por efectuarse en el sistema de alarma hayan sido tenidas en cuenta previamente.

8 MEDIDAS A TOMARSE EN CASO DE ALARMA

Las medidas a tomarse se definirán en coordinación con los organismos que tengan experiencia o autoridad en estos asuntos y que sean competentes para determinar todos los factores por tenerse en cuenta cuando se decide la naturaleza de la acción por emprenderse en caso de alarma y qué sistemas de señalización son necesarias para apoyar dicha acción.

Los miembros apropiados del personal se recomienda sean instruídos en cómo activar correctamente una alarma y cómo actuar en caso de alarma. La eficacia de tal acción dependerá de las posibilidades de señalización del sistema de alarma y del tiempo que tarda en llegar el socorro al lugar, lo que se tendrá en cuenta en el momento de la planificación del sistema.

9 MANTENIMIENTO

El mantenimiento de rutina se efectuará a intervalos regulares conforme con los requisitos del sistema de alarma específico. Durante cada mantenimiento de rutina.

- a) verificar la instalación, los emplazamientos y el posicionamiento de todos los equipos y dispositivos comparando con el fichero;
- b) verificar el buen funcionamiento de todos los dispositivos de detección, incluyendo los elementos de comando manual;
- c) inspeccionar todas las conexiones flexibles comparando con los requisitos apropiados;
- d) verificar el buen funcionamiento y el buen estado de todas las fuentes de energía eléctrica normales y de reserva;
- e) verificar la central de alarma y efectuar el mantenimiento según el procedimiento indicado por la compañía que provee la alarma;
- f) verificar el buen funcionamiento de todo equipo de transmisión de alarma en coordinación con el organismo oficial o la central de vigilancia concerniente;

- g) verificar el buen funcionamiento de todos los dispositivos de señalización sonora;
- h) verificar que el sistema de alarma funcione en su totalidad.

10 SERVICIO DE URGENCIA

Cuando una compañía de alarmas suministra un servicio de urgencia, cada usuario debe estar al tanto de la dirección y el número de teléfono de la central de intervención. El servicio de urgencia estará disponible durante las horas en que funciona el sistema de alarma del usuario.

NOTA: Se recomienda que el servicio de urgencia esté situado y organizado de tal manera que, salvo en circunstancias anormales, el representante de la compañía de alarmas pueda llegar a los locales protegidos dentro de las 4 h de haber sido notificado de la falla.

Siempre que sea posible conviene informar al usuario del retardo aproximado para llegar al lugar cuando se notifica una falla.

11 ARCHIVOS

Se establecerá un sistema de fichas para cada sistema de alarma.

11.1 Ficha de los equipos

Se recomienda registrar el nombre y la dirección del usuario, el emplazamiento actual y el tipo de cada dispositivo de detección y de cualquier otro equipo. Conviene que se utilice un código o un sistema de abreviaturas a los fines del mantenimiento, asegurando la confidencialidad.

11.2 Historia

Para cada sistema de alarma conviene exista una ficha histórica, indicando la fecha de cada visita, las fallas constatadas y las medidas tomadas para remediarlas. Se incluirá una ficha de todas las alarmas conjuntamente con los detalles de la acción tomada en tal ocasión y, si fuera posible, la causa de dichas alarmas.

11.3 Ficha de mantenimiento

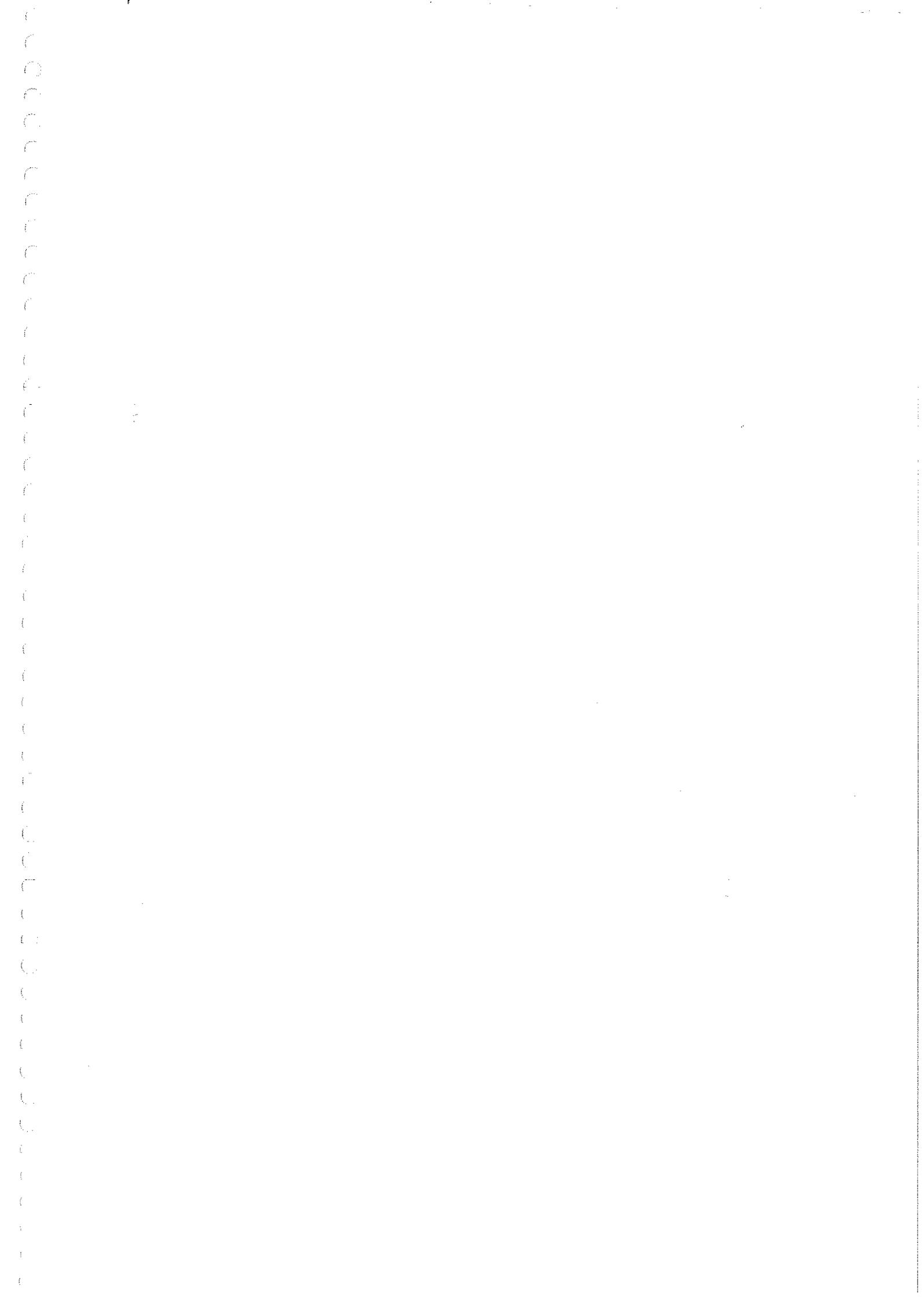
Conviene que haya una ficha separada de cada mantenimiento, que incluya fecha y las operaciones de verificación del capítulo 9 que no se pudieron efectuar en aquella visita, así como registrar la acción tomada para completar dicha operación, la fecha de su terminación.

11.4 Servicio de urgencia

Conviene registrar la fecha y la hora de la recepción de cada llamada de urgencia, conjuntamente con la fecha y la hora de terminación de la acción necesaria.

11.5 Registro de las desconexiones temporarias

Para cada sistema de alarma existirá una ficha que indique toda desconexión total o parcial del sistema de alarma, así como también los dispositivos de detección y todo equipo que en uno u otro momento no se encuentre en servicio. Se indicará la razón y la fecha de la desconexión. Para cada desconexión es conveniente requerir una autorización firmada del usuario o de sus representantes.





INSTITUTO ARGENTINO
DE NORMALIZACIÓN
Y CERTIFICACIÓN

NORMA IRAM 4172

Noviembre 1994

ICS 13.320

*CNA 6350

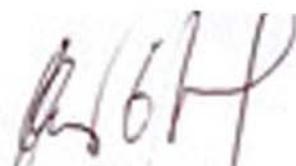
Certificado | sistemas de Gestión

**SISTEMAS DE ALARMA
DETECTORES INFRARROJOS PASIVOS
UTILIZADOS EN LOS EDIFICIOS**
Requisitos



INSTITUTO ARGENTINO DE RACIONALIZACIÓN DE MATERIALES

* Corresponde a la Clase Nacional de Abastecimiento asignada por el Servicio Nacional de Catalogación dependiente del Ministerio de Defensa.


Dirección de Certificación


Comité General de Certificación


Dirección General



PREFACIO

- El estudio de esta norma estuvo a cargo de los organismos respectivos, integrados de la forma siguiente:

Comisión de Alarmas

Integrante

Ing. C. Cruz
Arq. E. Gonzalez
Ing. A. Luongo
Sr. C. Martinez
Ing. D. Montes
Ing. E. Ricci
Sr. A. Trullen
Ing. R. Mansour

Representa a:

G y K S.A.
MIEMBRO PARTICULAR
TELECOM ARGENTINA
POLICIA FEDERAL ARG.
POLICIA FEDERAL ARG.
GENERAL INDUSTRIES
POLICIA FEDERAL ARG.
IRAM

Comité General de Normas (C.G.N.)

Dr. V. Alderuccio
Ing. J. Arcioni
Ing. J. V. Casella
Dr. E. Catalano
Ing. D. Donegani
Lic. C. A. Grimaldi
Dr. A. Grosso
Ing. S. Ituarte
Ing. J. Kostic

Ing. J. Mangosio
Ing. S. Mardyks
Ing. R. Martínez
Dr. E. Miró
Ing. N. O'Neill
Dr. A. F. Otamendi
Sr. F. R. Soldi
Prof. M. P. Mestanza

- En el estudio de esta norma se ha tenido en cuenta el antecedente siguiente:

IEC - INTERNATIONAL ELECTROTECHNICAL COMMISSION

IEC Standard 832-2-6 (1990-01) ALARM SYSTEMS - Requirements for intruder alarm systems
Section six - Passive infra-red detectors for use in buildings.

LEONID LLONTOP CASTRO
Jefe de Seguridad Casa Matriz
Banco Ciudad Bs. As.

INDICE

Párrafo	Página
1 Alcance	4
2 Normas para consulta	4
3 Definiciones	5
4 Consideraciones generales	5
5 Requisitos	6
6 Métodos de ensayo	8
Figuras	12

SISTEMAS DE ALARMA

DETECTORES INFRARROJOS PASIVOS UTILIZADOS

EN LOS EDIFICIOS

Requisitos

ICS 13.320

*CNA 6350

1 OBJETO Y CAMPO DE APLICACIÓN

La presente norma establece los requisitos específicos y los métodos de ensayo para los detectores infrarrojos pasivos utilizados en los sistemas de alarma antirrobo instalados en los edificios. Esta norma complementa los requisitos generales de los detectores utilizados en los sistemas de alarma antirrobo especificados en la norma IEC 839-2-2** y debe utilizarse conjuntamente con lo especificado en la norma IRAM 4171-1. El detector puede tener más de un sensor, pero todos ellos deben estar en la misma caja.

El objeto de la presente norma es especificar los requisitos para los detectores infrarrojos pasivos que aseguren su aptitud para funcionar satisfactoriamente y que minimización de las falsas alarmas.

2 NORMAS PARA CONSULTA

Los documentos normativos siguientes contienen disposiciones, las cuales, mediante su cita en el texto, se transforman en prescripciones válidas para la presente norma IRAM. Las ediciones indicadas eran las vigentes en el momento de su publicación. Todo documento es susceptible de ser revisado y las partes que realicen acuerdos basados en esta norma se deben esforzar para buscar la posibilidad de aplicar sus ediciones más recientes.

Los organismos internacionales de normalización y el IRAM, mantienen registros actualizados de sus normas.

IRAM 4171-Parte 1 (1993) SISTEMAS DE ALARMA - Exigencias generales. Generalidades.

IEC 809 - Lámparas para automóviles. Requisitos dimensionales, eléctricos y luminosos.

IEC 839-2-2 - Requisitos para sistemas de alarma contra intrusos. Requisitos para detectores. General.

* Corresponde a la Clase Nacional de Abastecimiento asignada por el Servicio Nacional de Catalogación dependiente del Ministerio de Defensa.

** Hasta tanto no exista una norma IRAM sobre el tema, se utilizará esta norma IEC.

3 DEFINICIONES

Para los fines de la presente norma, las siguientes definiciones son aplicables además de aquellas indicadas en los requisitos generales para los detectores utilizados en los sistemas de alarma antirobo (norma IEC 839-2-2*).

3.1 *detector infrarrojo pasivo*

Detector que genera un estado de alarma en respuesta a un cambio en el nivel de la variación infrarroja recibida, causada por personas que se desplazan en la zona de cobertura de detección.

3.2 *sectores sensibles*

Aquellos sectores del campo óptico del detector que detecta la radiación infrarroja.

3.3 *zona de cobertura de detección*

Zona en la cual un blanco de referencia que se desplaza a una distancia constante del detector provoca un estado de alarma.

3.4 *blanco de referencia*

Dispositivo con características de emisión infrarroja similares a los de una persona de talla media. Para los fines de la presente norma, dicho blanco toma la forma indicada en la figura 1.

3.5 *alcance de detección*

Los alcances de detección para las direcciones dadas se expresan por la distancia radial que separa al detector del límite exterior de la zona de cobertura de detección.

3.6 *blanco de referencia secundario.*

Dispositivo con características de emisión infrarrojas similares a las de un animal pequeño, como ser un roedor. Para los fines de la presente norma, dicho blanco toma la forma de un cilindro de 30 mm de diámetro y de 150 mm de largo.

4 CONSIDERACIONES GENERALES

El detector estará compuesto por uno o varios sensores y por un procesador. Cuando se agregan en forma opcional sensores adicionales, los ensayos prescritos en el párrafo 6 se deben efectuar sin estos sensores adicionales. Los detectores pueden tener medios incorporados para variar la dirección de los sectores sensibles. Estos medios deben estar en el interior de la caja del aparato. Los detectores también pueden estar equipados con medios que permitan la medición de la extensión de los sectores sensibles, pero si estos medios impiden que el detector satisfaga los requisitos de la presente norma, entonces se deberá efectuar la indicación correspondiente cada vez que estén en uso.

* Hasta tanto no exista una norma IRAM sobre el tema se utilizará esta norma IEC.

5 REQUISITOS

5.1 *Requisitos generales*

5.1.1 *Procesamiento de la señal*

El detector será capaz de detectar el movimiento lateral del blanco de referencia con respecto al detector dentro de la zona de cobertura a velocidades comprendidas entre los 0,3 m/s y los 3 m/s y provocará un estado de alarma antes que el desplazamiento unidireccional del blanco de referencia alcance los 3 m, estando dicho blanco a una distancia constante del detector.

5.1.2 *Restablecimiento después de un estado de alarma*

Después de un estado de alarma y después de la cesación del movimiento que los causó, el detector debe volver a su estado normal de no alarma dentro de los 10 s.

5.1.3 *Resistencia a los pequeños blancos*

La sensibilidad del detector debe ser tal que no se generará un estado de alarma cuando un blanco de referencia secundario se desplaza sobre el suelo cuando el detector está montado a la altura de fijación recomendada por el fabricante.

5.1.4 *Resistencia a las variaciones de la temperatura de fondo*

Las variaciones de la temperatura de fondo en la gama que se extiende desde los + 25°C a los + 40°C, a una velocidad de 1°C/min, no deben provocar un estado de alarma.

5.1.5 *Resistencia a la luz de los faros delanteros de los vehículos*

El detector no debe generar un estado de alarma como resultado de ser iluminado por el equivalente de una luz de un faro delantero de un vehículo iluminando a través de un vidrio cuando se lo ensaya según 6.2.5.

5.1.6 *Resistencia al aire turbulento*

Las turbulencias de aire por encima y por debajo de la temperatura ambiente alrededor del detector no debe provocar un estado de alarma cuando el detector se ensaya conforme a 6.2.6.

5.1.7 *Protección antidesarme*

El detector debe estar equipado con una protección antidesarme, que debe generar un estado de alarma cuando se abre la caja lo suficiente como para permitir el acceso a cualquier dispositivo de comando o a regulaciones de fijación mecánica.

5.1.8 Protección de los cables

Cuando un sensor se encuentra en una caja separada de la unidad central de alarmas, el cable de conexión se considerará que forma parte del detector. Debe ser supervisado eléctricamente de tal manera que, si la desconexión o el cortocircuito de uno o de varios conductores impide la recepción por el procesador de una información de alarma o del dispositivo antidesarme, el procesador propiamente dicho generará el estado de alarma dentro de los 10 s.

5.2 Reglas relativas al medio ambiente

No existen requisitos adicionales.

5.3 Seguridad

No existen requisitos adicionales.

5.4 Confiabilidad

No existen requisitos adicionales.

5.5 Interfase

No existen requisitos adicionales.

5.6 Construcción

No existen requisitos adicionales.

5.7 Indicador de movimiento

Si se instala un indicador de movimiento debe ser posible invalidar su indicación.

5.8 Especificaciones del fabricante

Además de la información que figura en los requisitos generales de la norma IEC 389-2-2*, el fabricante debe suministrar para cada detector lo siguiente:

- a) la geometría de los sectores sensibles por esquema;
- b) la zona de cobertura de detección (esto se puede incorporar en el mismo esquema que a)), para cada regulación de sensibilidad y el número de pulsos, cuando existen estas regulaciones; si la sensibilidad es variable continuamente, entonces la zona de cobertura se debe dar para las sensibilidades máximas y mínimas;
- c) la altura de fijación o gama de las alturas de fijación;
- d) la regulación óptima de la óptica.

* Hasta tanto no exista una norma IRAM sobre el tema se utilizará esta norma IEC.

5.9 Opciones

No existen requisitos adicionales.

6 MÉTODOS DE ENSAYO

6.1 Condiciones de ensayo

La experiencia ha demostrado la dificultad de obtener resultados de ensayo repetibles y reproducibles utilizando un blanco humano. Por lo tanto se propone como alternativa el siguiente método de ensayo que utiliza un blanco simulado. El método no se ha demostrado todavía en la práctica, por ello puede estar sujeto a modificación en el futuro.

Para la realización de los ensayos funcionales, debe montarse el detector a la altura recomendada por el fabricante y conforme a sus instrucciones. Los dispositivos ópticos se deben regular a su funcionamiento óptimo tal como lo indica el fabricante.

Cuando se da una gama de alturas de fijación, los ensayos se deben efectuar en las posiciones superior e inferior.

Cuando se proveen comandos de conteo de pulsos o comandos de sensibilidad, los ensayos se deben efectuar con dichos comandos en sus posiciones superiores e inferiores.

El blanco de referencia se debe montar con su eje principal vertical y su borde inferior a no más de 100 mm del suelo. Su temperatura debe estar distribuída en forma uniforme, con una variación total de la temperatura promedio de no más de 0,2°C sobre su superficie.

El fondo que se encuentra en el campo de visión del detector debe tener la misma emisividad que el blanco de referencia y su temperatura debe estar comprendida entre los 20°C y los 25°C, y debe permanecer constante durante toda la duración de los ensayos. Su temperatura debe estar distribuída en forma uniforme, con una variación total de no más de 0,5°C sobre su superficie.

La temperatura promedio del blanco de referencia debe ser de 4°C \pm 0,25°C por encima de la temperatura promedio del fondo.

Los ensayos se pueden realizar ya sea mediante la fijación del detector y desplazando el blanco de referencia o bien mediante la fijación del blanco de referencia y haciendo girar el detector. En ambos casos, la distancia radial no debe variar en más del \pm 5 %.

6.2 Ensayos funcionales

6.2.1 Cobertura de detección

6.2.1.1 El blanco de referencia se debe situar a la distancia de detección máxima para la cual se instaló y reguló el detector.

Se debe mover el blanco de referencia o bien se debe girar el detector para obtener el efecto de un movimiento unidireccional a una distancia constante entre el blanco de referencia y el detector. El movimiento debe crear el equivalente de una velocidad lateral de 0,3 m/s.

El estado de alarma se debe generar dentro de un desplazamiento equivalente de 3 m.

6.2.1.2 El ensayo de 6.2.1.1 se debe repetir a una velocidad lateral equivalente de 3 m/s.

6.2.1.3 Los ensayos de 6.2.1.1 y 6.2.1.2 se deben repetir con el blanco de referencia situado en el límite inferior de la zona de cobertura de detección para el cual el detector ha sido instalado y regulado.

6.2.1.4 El ensayo de 6.2.1.2 se debe repetir con el blanco de referencia situado en tres posiciones elegidas al azar dentro de la zona de cobertura de detección.

6.2.2 Reestablecimiento después de un estado de alarma

Se efectúa el ensayo de 6.2.1.1 y se anota la distancia equivalente que se recorre para generar un estado de alarma. El blanco de referencia se debe volver a su posición inicial.

Luego se hace desplazar una persona o un objeto distinto al blanco de referencia, suficiente para provocar un estado de alarma, después de lo cual se detiene el desplazamiento. Después de 10 s adicionales se repite el ensayo de 6.2.1.1 y la distancia equivalente para generar un estado de alarma no debe variar en más del 10 % en relación a la distancia lograda durante la primera parte de este ensayo.

6.2.3 Resistencia a los blancos pequeños

Para este ensayo son aplicables las condiciones de ensayo de 6.1, con la excepción de que el blanco a utilizarse debe ser el blanco de referencia secundario. El blanco se debe montar a no más de 100 mm del suelo con su eje más grande tangencial al detector y paralelo con relación al suelo. La posición del blanco se elige en función de la geometría de los sectores sensibles a fin de obtener un efecto máximo. El blanco de referencia se debe desplazar o bien se debe girar el detector a fin de obtener el efecto del movimiento lateral del blanco de referencia secundario con respecto al detector. El movimiento debe crear el equivalente de una velocidad de 1,0 m/s.

No se debe generar ningún estado de alarma.

L.EONID LIONTOP CASTRO
Jefe de Seguridad Caso Moriz
Banco Ciudad Bs. As

6.2.4 Resistencia a los cambios de la temperatura de fondo

El detector se debe regular para ver un fondo donde la temperatura debe ser de aproximadamente 25°C, distribuida en forma uniforme, con una variación total de no más de 0,5°C sobre su superficie. La temperatura del detector debe permanecer constante durante todo el ensayo.

La temperatura de fondo se debe aumentar a una velocidad de 1°C/min hasta que alcanza los 40°C. No se debe desencadenar ningún estado de alarma.

Este ensayo se puede simular aumentando la temperatura de fondo en un solo sector sensible. La simulación debe ser tal que el cambio en el flujo radiante en la apertura del detector debe ser el mismo que en el ensayo integral.

6.2.5 Resistencia a la luz de los faros delanteros de los vehículos

La disposición del ensayo se indica esquemáticamente en la figura 2.

El detector se debe montar en el centro de una superficie vertical en una caja oscura. El costado de la caja opuesto al detector debe estar compuesto por dos láminas de vidrio limpias, cada una de 500 mm de lado y 4 mm de espesor, separadas por no menos de 10 mm. El dispositivo de fijación de los vidrios debe permitir el pasaje de aire entre ellos.

El conjunto de iluminación debe comprender una lámpara halógena H4 de 60 W, conforme a la IEC 809, ubicada en un reflector sin lente. La lámpara debe haber funcionado al menos durante 10 h pero durante no más de 100 h. El conjunto de la lámpara se debe colocar en una zona sensible de la parte del patrón que forma el ángulo más pequeño con relación a la horizontal. Debe estar a una distancia de al menos 3 m del detector y se debe ubicar de tal manera como para producir un flujo constante de $6\ 500\text{ lx} \pm 10\%$ en la cubierta del sensor.

La lámpara debe estar alimentada con 13,5 V de corriente continua y se debe encender durante 2 s y luego se apaga durante 2 s. Este ciclo completo se debe repetir cinco veces.

No se debe producir ningún estado de alarma como consecuencia de este ensayo.

6.2.6 Resistencia a las turbulencias

El detector se debe montar a una altura adecuada un fondo uniforme y todos los comandos se deben regular para obtener la sensibilidad máxima.

Un calefactor ventilador de 1 000 W con una sección de salida de 55 mm x 180 mm se coloca a 1 m debajo y a 1 m delante del detector y se posiciona de manera que el flujo de aire sea dirigido hacia el detector a un ángulo de 12° con relación a la horizontal, hacia el detector. El flujo de aire del calefactor debe ser de $2,2\text{ m/s} \pm 0,2\text{ m/s}$ y el flujo de aire en la cara del detector debe ser de $0,7\text{ m/s} \pm 0,1\text{ m/s}$.

El calefactor se debe hacer funcionar durante un período de 5 min.

No se debe desencadenar ningún estado de alarma.

6.3 Ensayos relativos al medio ambiente

El detector debe someterse a los ensayos relativos al medio ambiente especificados en la IEC 839-2-2*. Para los ensayos siguientes, el detector debe regularse para la sensibilidad máxima:

- "picos eléctricos"; (sobretensiones transitorias);
- descargas electrostáticas;
- campos electromagnéticos.

Para los otros ensayos relativos al medio ambiente se puede utilizar una regulación cualquiera dentro de la gama del detector, pero dicha regulación no se debe modificar durante el ensayo.

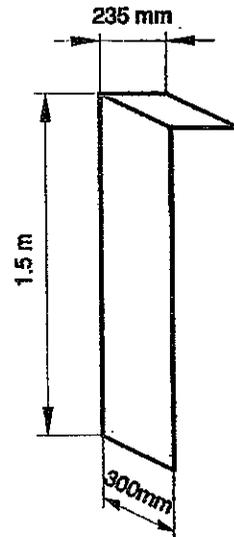
Durante cada ensayo relativos al medio ambiente, el detector debe ser operacional, pero la apertura se puede tapar para evitar una falsa operación debida a las variaciones de fondo.

No se debe generar ningún estado de alarma durante cualquiera de los ensayos relativos al medio ambiente.

Antes y después de cada ensayo relativo al medio ambiente, se deben efectuar los ensayos de 6.2.1.1 y 6.2.1.2. Para cada ensayo la distancia recorrida para generar un estado de alarma no debe variar en más del 10 % de la distancia inicial. Los ensayos se pueden simular con la condición de que se pueda demostrar que la simulación da los mismos resultados que la modalidad de ensayo descripta, calibrada a la temperatura del ambiente.

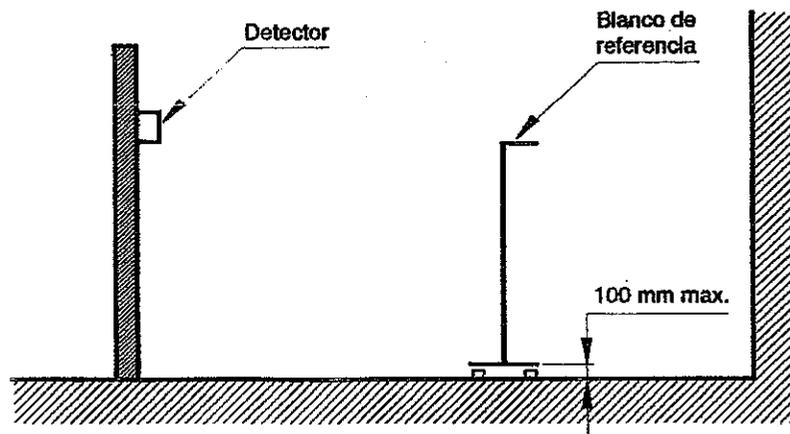
Después de los ensayos de calor seco y de frío, se deben efectuar los ensayos anteriormente mencionados mientras el detector todavía se encuentra a temperatura de ensayo.

* Hasta tanto no exista una norma IRAM sobre el tema se utilizará esta norma IEC.



LEONID LIONTOP CASTRO
Jefe de Seguridad Casa Matriz
Banco Ciudad Bs As

a) blanco de referencia



b) montaje de ensayo

Figura 1 - Blanco de referencia (3.4)

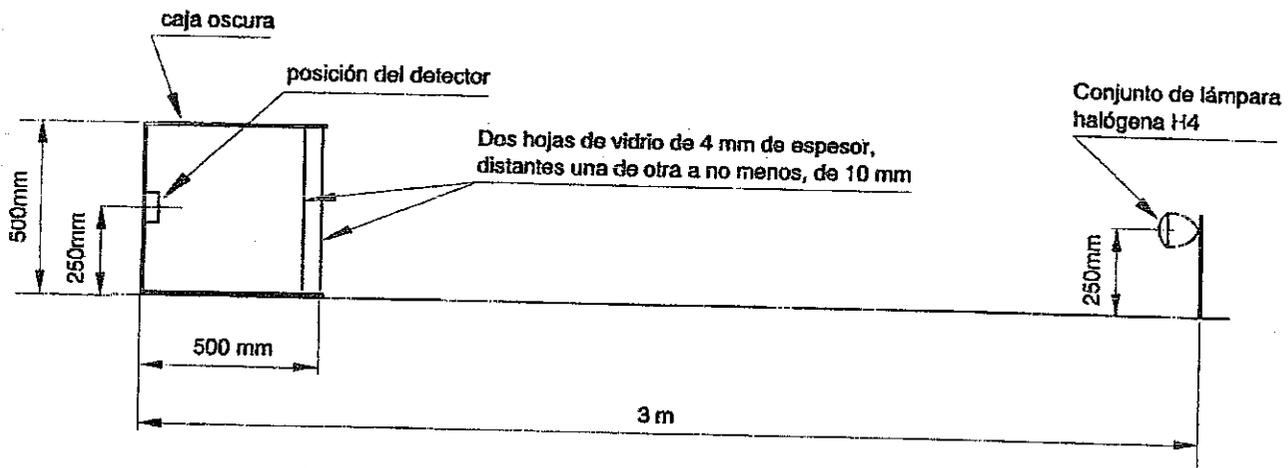


Figura 2 - Equipo para el ensayo de 6.2.5: Resistencia a la luz de los faros delanteros de los vehículos

LEONID LLONTOP CASTRO
Jefe de Seguridad Caso Matriz
Banco Ciudad Bs As

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100



INSTITUTO ARGENTINO
DE NORMALIZACIÓN
Y CERTIFICACIÓN

NORMA IRAM 4173-1

Agosto 1997

(IEC 839-5-1)

ICS 13.320;13.310

*CNA 6350

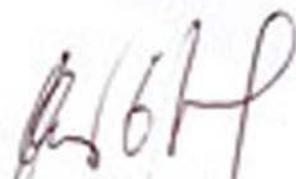
Certificado | sistemas de Gestión

SISTEMAS DE ALARMA
SISTEMAS DE TRANSMISIÓN
Sección 1 – Requisitos generales



INSTITUTO ARGENTINO DE NORMALIZACIÓN

* Corresponde al la Clasificación Nacional de Abastecimiento asignado por el Servicio Nacional de Catalogación del Ministerio de Defensa.


Dirección de Certificación


Comité General de Certificación


Dirección General



NORMA IRAM 4173-1: 1997

- El estudio de esta norma estuvo a cargo de los organismos respectivos, integrados de la forma siguiente:

Subcomité de Sistemas de alarma

Integrante

Ing. A. Amdem
Ing. C. Cruz
Ing. L. Ginesta
Arq. E. Gonzalez
Sr. M. Hirsch
Ing. A. Luongo
Ing. R. Katz
Sgto. C. Martínez
Ing. H. Mazza
Ing. P. Ricci
Ing. J. Roson
Sgto. A. Trullen
Lic. M. Soriano

Ing. R. Mansour

Representa a:

GENERAL INDUSTRIES S.A.
G & K S.A.
GUARD
INVITADO ESPECIALISTA
POLICIA BONAERENSE
TELECOM ARG.
G & K S.A.
POLICÍA FEDERAL
INTI
GENERAL INDUSTRIES S.A.
E.Y.S.E.
POLICÍA FEDERAL
COLEGIO DE GRADUADOS EN
CIENCIAS DE SEGURIDAD
IRAM

Comité General de Normas (C.G.N.)

Ing. J. Arcioni
Ing. S. Ituarte
Ing. S. Mardyks

Ing. R. Martínez
Ing. N. O'Neill
Ing. R. Barbosa

LEONID LLONTOP CASTRO
Jefe de Seguridad Casa Matriz
Banco Ciudad Bs. As

PREFACIO

El Instituto Argentino de Normalización (IRAM) es una asociación civil sin fines de lucro cuyas finalidades específicas, en su carácter de Organismo Argentino de Normalización, son establecer normas técnicas, sin limitaciones en los ámbitos que abarquen, además de propender al conocimiento y la aplicación de la normalización como base de la calidad, promoviendo las actividades de certificación de productos y de sistemas de la calidad en las empresas para brindar seguridad al consumidor.

IRAM es el representante de la Argentina en la International Organization for Standardization (ISO), en la Comisión Panamericana de Normas Técnicas (COPANT) y en el Comité MERCOSUR de Normalización (CMN).

Esta norma IRAM es el fruto del consenso técnico entre los diversos sectores involucrados, los que a través de sus representantes han intervenido en los Organismos de Estudio de Normas correspondientes.

LEONID LLONTOP CASTRO
Jefe de Seguridad Casa Matriz
Banco Ciudad Bs. As.

ÍNDICE	Página
INTRODUCCIÓN.....	5
1 OBJETO Y CAMPO DE APLICACIÓN	5
2 NORMAS PARA CONSULTA.....	6
3 DEFINICIONES.....	6
4 CONSIDERACIONES GENERALES.....	7
5 REQUISITOS.....	8
6 MÉTODOS DE ENSAYO.....	14
Figura 1 - Sistema de transmisión de alarma.....	19
Figura 2 - Configuración con un centro de control a distancia.....	19
Figura 3 - Configuración con dos centros de control a distancia.....	20
ANEXO A -	21

SISTEMAS DE ALARMA

SISTEMAS DE TRANSMISIÓN

SECCIÓN 1 - REQUISITOS GENERALES

ICS 113.320;13.310
*CNA 6350

INTRODUCCIÓN

Esta norma es equivalente a la norma de la Comisión Electrotécnica Internacional IEC 839-5-1 (1991-04): Sistemas de alarma. Parte 5: Requisitos para los sistemas de transmisión Sección 1: Requisitos Generales para los sistemas de transmisión. Con el fin de facilitar su aplicación sigue la misma estructura que el documento internacional y las diferencias con dicho documento se reducen a cambios de redacción y de forma considerados necesarios para mantener una unidad de criterio con el conjunto de las normas IRAM y lograr una mejor comprensión del texto.

NOTA: Los agregados están señalados con una línea recta en el margen izquierdo.

1 OBJETO Y CAMPO DE APLICACIÓN

La presente serie de normas IRAM 4173 especifica los requisitos generales relativos a las características de funcionamiento, de confiabilidad y de seguridad de los sistemas de transmisión de alarma.

Cubre los requisitos generales relativos a las conexiones que aseguran la señalización entre un sistema de alarma y una estación de vigilancia.

Se pueden encontrar requisitos adicionales relativos a los sistemas de transmisión de alarma específicos en normas separadas que forman parte de la serie IRAM 4173**. Este no excluye el uso de algún otro sistema de transmisión no cubierto por una de estas normas específicas, siempre que satisfaga estos requisitos generales.

Esta norma no especifica el método de presentación de la información y la instalación del equipo.

* Corresponde a la Clasificación Nacional de Abastecimiento asignado por el Servicio Nacional de Catalogación del Ministerio de Defensa.

** Hasta tanto se complete esta serie de normas IRAM se consultará en caso necesario la serie de normas IEC 839-5 restantes.

2 NORMAS PARA CONSULTA

Los documentos normativos siguientes contienen disposiciones, las cuales, mediante su cita en el texto, se transforman en prescripciones válidas para la presente norma IRAM. Las ediciones indicadas eran las vigentes en el momento de su publicación. Todo documento es susceptible de ser revisado y las partes que realicen acuerdos basados en esta norma se deben esforzar para buscar la posibilidad de aplicar sus ediciones más recientes.

Los organismos internacionales de normalización y el IRAM, mantienen registros actualizados de sus normas

IRAM 4173-2* - Sistemas de alarma. Sistemas de transmisión. Parte 2: Requisitos generales para los equipos utilizados.

3 DEFINICIONES

3.1 compañía de alarmas. Organización que proporciona y/o asegura el mantenimiento de los sistemas de alarma.

3.2 estado de alarma. Estado de un sistema de alarma o de una parte de aquél, que resulta de la reacción del sistema o de una parte de aquél, en presencia de un riesgo.

3.3 sistema de alarma. Instalación eléctrica diseñada para detectar y señalar la presencia de una situación anormal y generar una señal de alarma que indica la presencia de un peligro.

3.4 sistema de transmisión de alarma. Equipo y red que permite transferir las informaciones relativas al estado de uno o de varios sistemas de alarma a uno o varios centros de control a distancia.

NOTA: Los sistemas de transmisión de alarma no comprenden las conexiones locales directas, por ejemplo las interconexiones entre partes de un sistema de alarma que no requieren una interfaz para transformar las informaciones del sistema de alarma en una forma adecuada para la transmisión.

3.5 función antidesarme. Función que detecta acciones y/o manipulaciones en un elemento constitutivo de un sistema de alarma.

3.6 estación central. Ver central de control a distancia.

3.7 encriptado. Codificación, traducción u otra modificación de la información en la cual el modo en que la información es modificada varía con el tiempo de forma pseudo-aleatoria.

3.8 estación de vigilancia. Emplazamiento a distancia de los locales supervisados, donde se recoge la información correspondiente al estado de uno o varios sistemas de alarma ya sea para los fines de señalización (es decir un centro de control a distancia) o para los fines de retransmisión (es decir una estación satelital o un punto de centralización).

* Hasta tanto se termine el estudio de esta norma se consultará la IEC 839-5-2.

3.8.1 centro de control a distancia (estación central). Central a distancia que tiene personal a disposición en forma permanente, a la cual se comunican las informaciones relativas al estado de uno o varios sistemas de alarma.

3.8.2 centro de supervisión. Central a distancia que tiene personal a disposición, donde se supervisa el estado de un sistema de transmisión de alarma.

NOTA: El centro de supervisión puede ser una central distinta o bien puede formar parte del centro de control a distancia.

3.8.3 estación satelital. Estación de vigilancia, habitualmente sin personal presente, pero donde pueden acudir en caso de urgencia. Allí se recogen las informaciones relativas al estado de un cierto número de sistemas de alarma a los fines de su retransmisión, ya sea en forma directa o vía otra central satelital, a una central de recepción de alarma.

3.8.4 punto de centralización. Estación de vigilancia sin personal, sin posibilidad de recibirlo en caso de urgencia, donde las informaciones relativas al estado de un cierto número de sistemas de alarma se recogen para su retransmisión, ya sea en forma directa o por intermedio de una estación satelital, a una central de recepción de alarma.

3.9 "Scrambling". Codificación, traducción u otra modificación de la información, en la cual el modo de modificar las informaciones está determinado por una clave aleatoria, pero sin variación en el tiempo.

4 CONSIDERACIONES GENERALES

4.1 Normas aplicables

En caso de utilización de redes públicas se aplican las recomendaciones correspondientes (UIT-T, UIT-R, etc.). Cuando fuera conveniente también se debería hacer referencia al modelo de arquitectura en capas "Interconexión de Sistemas Abiertos" (OSI) de la ISO.

4.2 Configuración del sistema

La configuración lógica de un sistema de transmisión de alarma está representada en la figura 1.

Dependiendo de los niveles de confiabilidad requerida y de las características de funcionamiento de las centrales de recepción de alarma son posibles distintas configuraciones del sistema, por ejemplo:

- configuración de un centro de control a distancia (ver figura 2);
- configuración con dos centros de control a distancia, donde el puesto principal funciona y el puesto secundario está inactivo o en reserva (ver figura 3).

Otras configuraciones del sistema que satisfacen los requisitos de la presente sección son admisibles.

La elección del tipo de sistema de transmisión de alarma utilizado para un sistema de alarma debe depender del nivel de confiabilidad y/o seguridad exigidos. Conviene hacer referencia a las otras normas individuales que describen diferentes tipos de sistemas de transmisión de alarma.

Para asegurar una mejor confiabilidad de la transmisión se puede utilizar más de una vía de transmisión entre un sistema de alarma y uno o varios centros de controles a distancia.

Para asegurar la redundancia de la transmisión se puede conectar un sistema de alarma a una estación de vigilancia por medio de varios tipos de transmisión, por ejemplo: vías de transmisión reservadas y comunicadores digitales que utilizan la red telefónica pública conmutada.

4.3 Características de la transmisión

La transmisión del estado de sistema de alarma debe ser:

- a) continua, o
- b) periódica y/o
- c) por requerimiento (cada vez que cambie el estado).

Si la transmisión no es continua, el comando de la transmisión depende:

- a) del sistema de alarma y/o
- b) del centro de control a distancia, o
- c) del sistema de transmisión.

5 REQUISITOS

El sistema de transmisión de alarma debe asegurar la comunicación entre uno o varios sistemas de alarma y uno o varios centros de control a distancia.

5.1 Sistemas de transmisión de alarmas con múltiples sistemas de alarma

El sistema de transmisión de alarma debe ser diseñado de tal manera que el agregado, la modificación o la supresión de abonados no influya en las señales de otros abonados.

Las comunicaciones entre un sistema de alarma y un centro de control a distancia deben cumplir con los requisitos de la categoría apropiada dadas en la tabla 1 aún en presencia de cualquier otra señal transmitida por el mismo sistema de transmisión de alarma.

Para los sistemas de supervisión automática, las señales y los estados anormales que impiden la operación correcta del sistema de transmisión de alarma darán como resultado una señal de falla.

Las comunicaciones entre un sistema de alarma y un centro de control a distancia deben continuar cumpliendo con los requisitos de la categoría apropiada dada en la tabla 1, aún cuando las señales de alarma o falla sean emitidas por hasta el 1 % del total de los transmisores conectados a ese sistema, generando cada uno de ellos una señal de ese tipo por minuto

Si se supera esta tasa de transmisión se debe indicar en la especificación del sistema el grado de disminución del rendimiento del sistema de transmisión de alarmas. La disminución debe evolucionar en forma gradual (por ej. los tiempos de transmisión pueden aumentar lentamente) hasta una tasa equivalente a una señal por minuto desde cada uno de los transmisores hasta llegar al 10 % del total de los transmisores conectados a ese sistema, y debe responder de nuevo a los requisitos de la presente norma dentro de los 5 min posteriores al retorno a una tasa total de transmisión del 1 % del total de los transmisores como se indicó anteriormente.

NOTA: Así, un sistema con 1000 transmisores conectados debe continuar respondiendo a los requisitos de esta norma, si las alarmas se suceden en razón de 10/min

5.2 Sistemas de transmisión de alarmas compartidos con sistemas distintos de los de sistemas de alarma

Los sistemas de transmisión compartidos con sistemas distintos de los sistemas de alarma deben estar diseñados de tal manera que el funcionamiento y el mantenimiento de dichos servicios no eviten que el sistema de transmisión de alarma cumpla con los requisitos de la presente norma.

NOTA: Lo arriba mencionado es aplicable en el caso de una red conmutada después de que se establece la conexión.

5.3 Funcionamiento

5.3.1 Generalidades

El sistema de transmisión de alarma debe transmitir las informaciones relativas al estado del sistema de alarma al centro de control a distancia apropiado.

5.3.2 Retardo de la transmisión

El retardo de la transmisión no debe ser superior a los valores especificados en la tabla 1 para la clase apropiada. El retardo se debe medir a partir del momento en que el sistema de alarma cambia el estado hasta que se señala el nuevo estado al centro de control a distancia, excluyendo todo retardo externo al sistema de transmisión de alarma. Los retardos internos del sistema de alarma y los de la estación de vigilancia no se encuentran comprendidos en este concepto (ver también párrafo 6.3).

Tabla 1

Clases	D0	D1	D2	D3	D4
	s				
Media aritmética de todas las transmisiones	-	120	60	20	10
95 percentil mayor para todas las transmisiones	240	240	80	30	15
Retardo máximo admisible	-	480	120	50	20

5.3.3 Supervisión de la interconexión con el sistema de alarma

En el caso que el sistema de alarma esté separado del sistema de transmisión de alarma, cuando exista una falla en la interconexión entre ambos, se debe transmitir una señal de alarma o de falla al centro de control a distancia. El retardo de emisión de dicha señal debe satisfacer los valores especificados en la tabla 1 para la clase apropiada

5.3.4 Supervisión del sistema de transmisión de alarma

Para los sistemas con supervisión automática, el retardo entre el momento en que aparece una falla en el sistema de transmisión de alarma y el momento en que se señala dicha falla en el centro de control a distancia y/o el centro de supervisión no debe ser superior al valor especificado en la tabla 2 para la clase apropiada.

Tabla 2

Clase	T1	T2	T3	T4	T5
Retardo máximo	32 días	25 h	65 min	90 s	20 s

Las fallas de corta duración del sistema de transmisión de alarma no necesitan ser señalizadas siempre que se sigan cumpliendo con los requisitos de 5.3.2

5.3.5 Disponibilidad del sistema de transmisión de alarma

La disponibilidad del sistema de transmisión de alarma es el porcentaje de tiempo durante el cual el sistema se encuentra disponible para transmitir sin alteración, el estado de todo sistema de alarma al servicio conectado a él, al centro de control a distancia y dentro del retardo de transmisión especificado y, cuando correspondiere, para transmitir un mensaje (por ej.: un acuse de recibo) de un centro de control a distancia a un sistema de alarma.

Cuando existen varias interfaces al sistema de transmisión de alarma, ya sea en el sistema de alarma o bien en el centro de control a distancia predefinido, el sistema de transmisión de alarma se debe considerar apto para funcionar en caso de la existencia de una falla que afecta a una o varias de tales interfases, a condición de que:

- a) al menos exista una vía de transmisión entre una interface en el sistema de alarma y una interface en el centro de control a distancia y que además
- b) los mensajes sean normalmente emitidos en todas aquellas interfaces, o bien
- c) que los mensajes sean normalmente emitidos y recibidos en una interface primaria en cada extremo, pero que en caso de falla, el sistema cambie automáticamente a una interface secundaria.

5.3.6 Defectos del sistema de transmisión de alarma

A los fines de calcular la disponibilidad del sistema se deben considerar sólo las siguientes condiciones:

- a) Todos los defectos en el sistema de transmisión de alarma que eviten que una alarma sea transmitida de cualquier sistema de alarma en servicio a su centro de control a distancia destinatario, aún cuando la alarma se desvíe satisfactoriamente a un centro de control a distancia alternativo en un lugar diferente.

NOTA: Las entradas ocupadas en la estación de recepción no constituyen defectos del sistema de transmisión.

- b) Todos los defectos que alteran la transmisión de una alarma, de manera que alguna o toda la información transmitida se pierde, excepto cuando la información puede ser recuperada por retransmisión automática de la alarma de manera que se la recibe dentro del retardo máximo especificado en la tabla 1.

- c) Todos los defectos que retardan un mensaje de manera que su retardo de transmisión total supera el retardo máximo admisible especificado en la tabla 1.

- d) No disponibilidad debido al mantenimiento, a menos que se prevean instalaciones alternativas.

El sistema de transmisión de alarma se debe considerar como no disponible mientras exista una de las condiciones arriba descriptas.

LEONID LLONTOP CASTRO
Jefe de Seguridad Casa Matriz
Banco Ciudad Bs. As

5.3.7 Duración de los defectos

El tiempo durante el cual el sistema de transmisión de alarma debe considerarse como no disponible debe ser el retardo entre el último momento en que el sistema se conoció como disponible (es decir sin defectos) y el momento en que se detecta y se repara un defecto y se ensaya el sistema. Para cada defecto, el tiempo de no disponibilidad mínima debe ser de 15 min. Los defectos causados por intentos deliberados para deteriorar el sistema no se deben incluir, siempre que se los detecte y señale dentro del valor especificado en la tabla 2 para la clase apropiada y que sean reparados dentro de las 12 h.

5.3.8 Disponibilidad

La disponibilidad de un sistema de transmisión de alarma no debe ser inferior a los valores especificados en la tabla 3 para la clase correspondiente.

Tabla 3

Clase	A1	A2	A3	A4	A5
	%				
Disponibilidad anual de todo el sistema	97	99,3	99,5	99,8	99,99
Disponibilidad durante un mes	75	91	95	98,5	99,95

La disponibilidad de una parte del sistema de transmisión de alarma que afecta a 16 o menos sistemas de alarma puede ser aquella del nivel de disponibilidad inmediatamente inferior, siempre que la disponibilidad de las otras partes satisfaga la clase correspondiente.

NOTA: Las clases de la tabla 3 se corresponden aproximadamente a lo siguiente, pero no exclusivamente a los ejemplos que se citan.

A1 - Uno o varios defectos, cuya duración promedio, tal como se define en 5.3.7, es inferior a 11 días anuales por usuario (3 % de 365 días) pero es superior a los 7 días por usuario (25 % de 30 días) durante el mes. Por ejemplo, dos defectos durante el año, cada uno toma 5 días para identificarse y repararse.

Los 11 días anuales por abonado corresponden a una indisponibilidad anual del 3% de 365 días (100 - 97 (A1))

Los 7 días mensuales por abonado corresponden a una indisponibilidad mensual del 25 % de 30 días (100 - 75 (A1)).

LEONID LLONTOP CASTRO
 Jefe de Seguridad Casa Matriz
 Banco Ciudad Bs. As.

NORMA IRAM 4173-1: 1997

El mismo razonamiento vale para los ejemplos de las clases A2, A3, A4 y A5

A2 - Uno o varios defectos, cuya duración promedio es inferior a 2,5 días por usuario (0.7 % de 365 días) En los equipamientos del sistema de transmisión de alarma comunes a 16 usuarios o menos se pueden admitir 11 días por usuario, siempre que se mantenga el valor total inferior.

Por ejemplo, en un sistema en que se alimentan 7 grupos de usuarios por el mismo circuito principal, un defecto que dura 1 día en el circuito principal acompañado por defectos que duran 3 días en dos grupos, se encontraría dentro de los valores admitidos para esta clase.

A3 - Uno o varios defectos, cuya duración promedio es inferior a las 44 h por usuario (0,5 % x 365 x 24 hs) En los equipamientos del sistema de transmisión de alarma comunes a 16 usuarios o menos se pueden admitir 2,5 días por usuario, (A2).

Esta exigencia se cumple en un sistema en el cual los defectos son identificados y reparados al final del siguiente día de trabajo.

A4 - Uno o varios defectos, cuya duración promedio es inferior a las 17 h por usuario (0,2 % x 365 x 24 hs). En los equipamientos del sistema de transmisión de alarma comunes a 16 usuarios o menos se pueden admitir 44 h por usuario.

A5 - Uno o varios defectos, cuya duración promedio es inferior a 1 h por usuario (0,01 % 365 x 24 hs). En los equipamientos del sistema de transmisión de alarma comunes a 16 usuarios o menos se pueden admitir 17 h por usuario.

Es probable que los sistemas capaces de satisfacer los requisitos de las clases A4 ó A5 necesiten un alto grado de duplicación de los equipamientos comunes del sistema.

5.4 Seguridad de la señalización

El sistema de transmisión de alarma proporcionará los dispositivos para evitar o detectar las tentativas deliberadas de interferencia de la transmisión de una señal de alarma por interrupción o sustitución, en una de las siguientes maneras:

- S1 - Ningún dispositivo.
- S2 - Dispositivos para verificar y señalar la disponibilidad del sistema de transmisión de alarma conforme con 5.3.3 y 5.3.4.

Esto debe incluir la necesidad de supervisar los equipamientos redundantes eventuales del sistema, donde el defecto no influye inmediatamente sobre la disponibilidad del sistema.

- S3- Dispositivos del tipo S2, pero con "scrambling" de la señal en el circuito de transmisión de alarma. El sistema debe tener un mínimo de 250 claves únicas.

- S4 - Dispositivos del tipo S2, pero con encriptado de la señal en el circuito de transmisión de alarma. El algoritmo de encriptado debe ser tal que para los sistemas de transmisión de alarma sincrónicos, el patrón de datos de todo conjunto de 100 bits consecutivos no debe repetirse en forma idéntica en 10 000.000 de bits consecutivos, o para los sistemas asincrónicos, el patrón de datos de todo conjunto de 100 bytes consecutivos no se debe repetir en 1.000.000 de bytes consecutivos.

5.5 Equipamiento en las propiedades supervisadas

5.5.1 Contenedor del equipo

El equipo de transmisión de alarma se puede alojar ya sea en el mismo contenedor que el equipo de control del sistema de alarma asociado o bien en un contenedor separado.

Si no se aloja dentro del equipo de control, entonces el contenedor del equipo de transmisión de alarma debe tener un grado de resistencia al maltrato al menos igual a aquél especificado para el contenedor del equipo de control y a aquél especificado en la IEC 839-5-2. La conexión entre el sistema de alarma y el equipo de transmisión de alarma debe estar protegida contra el deterioro y las señales de interferencia.

5.5.2 Alimentación eléctrica

Si el equipo de transmisión de alarma exige una alimentación eléctrica local separada, deberá tener una capacidad de reserva al menos igual a aquella especificada para el sistema de alarma asociado.

5.5.3 Interface y/o equipo de adaptación de protocolo

Si un equipo de adaptación de protocolo y/o de interface es necesario y si dicho equipo se encuentra alojado en forma separada, el contenedor deberá estar protegido de la misma forma que el equipo de sistema de alarma.

6 MÉTODOS DE ENSAYO

6.1 Generalidades

Cuando una red de transmisión sirve como tronco común de un sistema de transmisión de alarma utilizado por varios sistemas de alarma, el ensayo se debe efectuar después de la conformación inicial de la red y después de todo mejoramiento importante. Dicha verificación debe asegurar que la supervisión sea efectiva en todas las partes de la red y que los mensajes de alarma o de defecto sean generados y transmitidos satisfactoriamente en el caso de la detección de un defecto.

El ensayo de un sistema de transmisión de alarma debe comprender diferentes aspectos enumerados a continuación:

- a) La verificación para asegurar que una señal de alarma de entrada presentada correctamente sea aceptada por el sistema de transmisión de alarma.

NOTA: El ensayo de la interface del sistema de alarma está descrito en la IEC 4173-2*

- b) La verificación de que el funcionamiento básico del sistema responde a los requisitos de la presente norma y a toda norma que se relacione con esta. Esto debe incluir el ensayo para establecer que las alarmas se transmitan a través del sistema al destino deseado y la verificación del sistema de supervisión.
- c) Verificación del retardo de la transmisión de alarma.
- d) Las verificaciones comunes o rutinarias necesarias para establecer o para confirmar la disponibilidad del sistema.

La verificación debe asegurar que para la configuración del sistema y el número de sistemas de alarma potencialmente previstos para ser conectados, el sistema de transmisión de alarma debe ser capaz de satisfacer los requisitos de 5.1. Esto debe efectuarse ya sea por:

- a) la verificación del sistema de recepción, ó
- b) la verificación y el examen del equipo en el momento del ensayo conforme con la IRAM 4173-2*, ó
- c) el análisis del equipo y su configuración, ó
- d) una combinación de estos tres puntos.

6.2 Grupo de sistemas de transmisión de alarma

En lo concerniente a los ensayos, un grupo de sistemas de transmisión de alarma puede conectar todos los sistemas de transmisión de alarma de un tipo con una única estación de vigilancia

Cuando los sistemas de transmisión de alarma están geográficamente repartidos en grupos distintos y cuando dichos grupos se comunican con equipos de recepción diferentes en el interior de la estación de vigilancia o bien pueden ser identificados separadamente de alguna otra manera, cada grupo puede ser ensayado en forma separada. Cuando se utiliza esta posibilidad, el ensayo se debe efectuar en cada uno de los grupos identificados.

* Hasta tanto, termine el estudio de esta norma se consultará la IEC 839-5-2

6.3 Verificación del retardo de la transmisión

Cuando todo nuevo sistema de alarma está conformado de acuerdo al sistema de transmisión de alarma, la transmisión correcta de todos los mensajes de alarma a su destino previsto debe ser verificado, incluyendo cuando correspondiere, la transmisión de mensajes de alarma o de falla asociados con la supervisión del sistema.

El tiempo que se tarda en transmitir una alarma debe medirse y debe encontrarse dentro de la clase correspondiente de la tabla 1.

En el caso de los sistemas que proveen una señalización del nivel de seguridad S2 o superior (ver 5.4), el tiempo que se tarda en transmitir una condición de alarma o de falla resultante de una puesta en cortocircuito de la línea de transmisión que viene de las propiedades supervisadas, debe medirse y debe encontrarse dentro de la clase apropiada de la tabla 2.

Los ensayos de rutina, que incluyen verificación de las secuencias necesarias para los mensajes de alarma y falla, deben repetirse al menos una vez por año para cada sistema de alarma conectado o bien a intervalos de servicio periódicos del sistema de alarma, si éste último período es más largo.

Cuando el sistema de transmisión de alarma es capaz de transmitir diferentes mensajes con prioridades y secuencias distintas, los ensayos se deben efectuar para cada grupo en forma separada. En tales casos los resultados de los ensayos en cada grupo constitutivo deben ser constatados.

Cuando la tasa de transmisión de alarmas a través del sistema varía con el tiempo en forma previsible o cuando el uso del sistema de transmisión de alarma por otros servicios que utilizan el mismo equipo varía con el tiempo (por ej.: sistemas que utilizan la red telefónica pública conmutada), la distribución de las duraciones de los ensayos debe reflejar la distribución de las duraciones durante el día o la semana en que se transmiten las alarmas reales.

Los resultados de los ensayos en cada sistema de transmisión de alarma se deben analizar en varios períodos sucesivos de tres meses.

6.4 Disponibilidad

6.4.1 Registros

La compañía de alarmas responsable del sistema de transmisión de alarma debe tener registros de todas las fallas y de todos los ensayos efectuados en el sistema

La compañía de alarmas debe tener registros de todas las fallas del sistema, incluyendo aquellos en que no hubo perturbación del servicio debido a la redundancia del sistema.

Estos registros deben estar a disposición para ser inspeccionados por representantes de organismos nacionales de control o bien por alguna organización de aprobación independiente (por ej.: una compañía de seguros) cuando se lo requiera. Debe ser posible encontrar cada falla del sistema en los documentos compilados que deben satisfacer esta norma como así también debe ser posible remontarse hasta las cifras documentadas de cada falla o ensayo individuales.

Los registros deben contener para cada falla:

- a) la hora y la fecha en que la falla fue identificada;
- b) el último instante y la fecha durante la cual se puede informar con certeza que la falla dejó de existir (no es necesario en los sistemas supervisados en forma permanente);
- c) la duración de la perturbación del servicio;
- d) el número de usuarios cuyo servicio fuera afectado por la falla y;
- e) las precisiones sobre la falla.

6.4.2 Análisis

Los registros de todos los ensayos efectuados en un sistema de transmisión de alarma deben utilizarse para determinar la disponibilidad del sistema. Los ensayos complementarios (por ej.: el desarrollo secuencial de la transmisión correcta de una señal de alarma) se deben efectuar para verificar que los ensayos provienen de una muestra representativa de sistemas de alarma y que contienen datos de alarma o bien que son de un tipo de alarma que es representativa de las alarmas en su conjunto. También puede ser necesario efectuar ensayos suplementarios para identificar el número de sistemas de alarmas afectados por una falla y para aumentar la disponibilidad probada del sistema (por ej.: aumentando la frecuencia de los ensayos de rutina).

En cada caso en que el sistema no está disponible (ver 5.3.6 y 5.3.7) el tiempo de indisponibilidad se debe calcular de la siguiente manera:

Duración de la falla = duración del defecto en minutos x número de sistemas de alarma conectados, afectados por dicha falla

NORMA IRAM 4173-1: 1997

Para cada mes, la disponibilidad del sistema se debe calcular de la siguiente forma:

$$\text{Disponibilidad mensual} = 1 - \frac{\text{suma de duraciones de las fallas}}{43800 * \text{número de sistemas de alarma conectados}}$$

* (minutos x mes promediados en el año)

Por suma de duraciones de las fallas debe entenderse la totalidad de las fallas corregidas durante un mes. El número de sistemas de alarma conectados debe ser aquel de la medianoche del último día del mes

La disponibilidad del sistema, según 5.3.8, debe ser la media aritmética promedio de las disponibilidades mensuales durante 12 meses sucesivos.

Cuando un sistema se amplía la disponibilidad de la nueva zona puede ser ignorada no más allá de un mes a partir de la fecha de la ampliación.

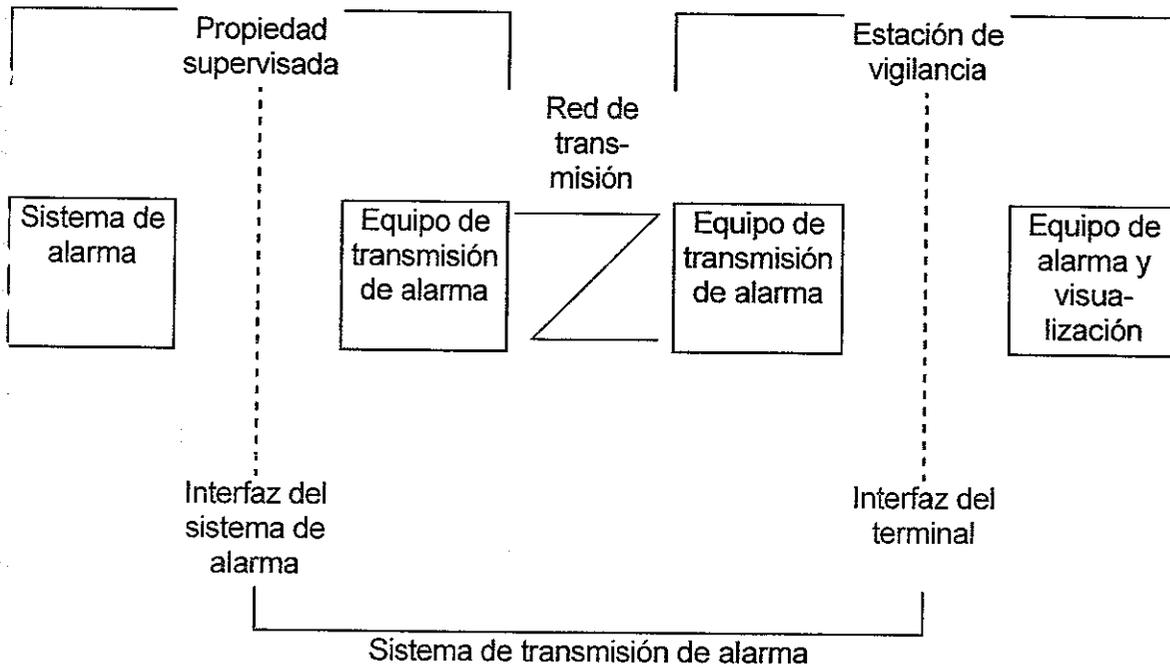


Figura 1 - Sistema de transmisión de alarma

LEONID LLONTOP CASTRO
Jefe de Seguridad Casa Metriz
Banco Ciudad Bs. As

**Configuración
con un centro de control
a distancia**

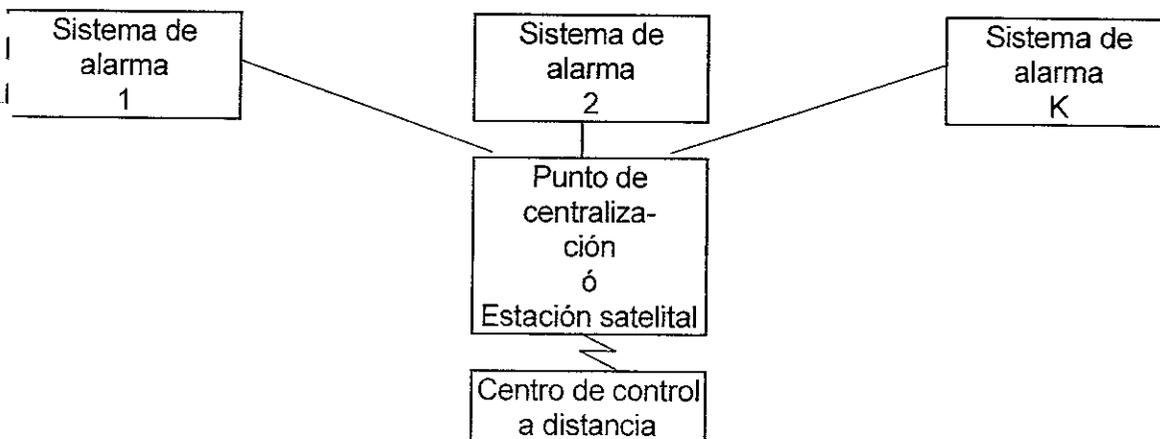


Figura 2 - Configuración con un centro de control a distancia

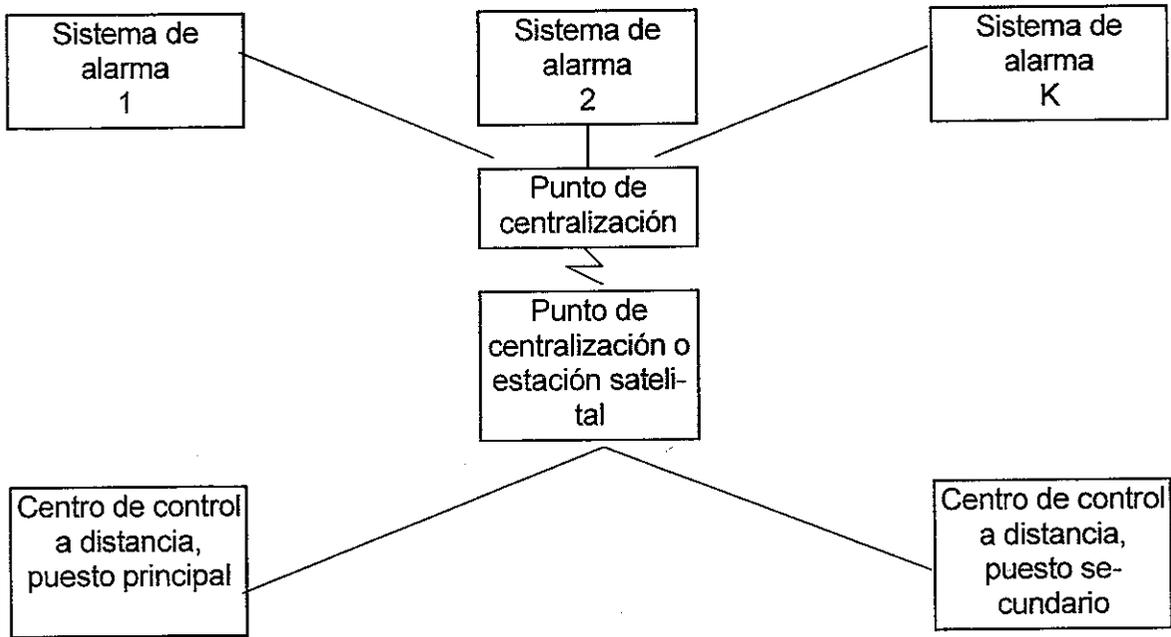


Figura 3 - Configuración con dos centros de control a distancia

RONID MONTOP CASTRO
Ingeniero en Electricidad Casa Matriz
Buenos Aires Ciudad Bs. As

**ANEXO A
(Informativo)**

BIBLIOGRAFÍA

- En el estudio de esta norma se ha tenido en cuenta el antecedente siguiente:

IEC – INTERNATIONAL ELECTROTECHNICAL COMMISSION

IEC 839-5-1 (1991-04) - Alarm systems - Part 5: Requirements for alarm transmission systems - Section 1: General requirements for systems

LEONID LLONTOP CASTRO
Jefe de Seguridad Caso Matriz
Banco Ciudad Bs. As.







INSTITUTO ARGENTINO
DE NORMALIZACIÓN
Y CERTIFICACIÓN

IRAM
4174

Primera edición
1999-10-08

Certificado | sistemas de Gestión

Sistemas de alarma

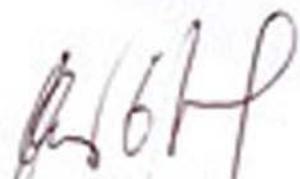
Centros de Control a Distancia

Requisitos mínimos

Alarm systems - Remote Control Centers - Minimum Requirements



Referencia Numérica:
IRAM 4174:1999


Dirección de Certificación


Comité General de Certificación


Dirección General



IRAM 1999

No está permitida la reproducción de ninguna de las partes de esta publicación por cualquier medio, incluyendo fotocopiado y microfilmación, sin permiso escrito del IRAM.

LEONID LLONTOP CASTRO
Jefe de Seguridad Casa Matriz
Banco Ciudad Bs. As.

Prefacio

El Instituto Argentino de Normalización (IRAM) es una asociación civil sin fines de lucro cuyas finalidades específicas, en su carácter de Organismo Argentino de Normalización, son establecer normas técnicas, sin limitaciones en los ámbitos que abarquen, además de propender al conocimiento y la aplicación de la normalización como base de la calidad, promoviendo las actividades de certificación de productos y de sistemas de la calidad en las empresas para brindar seguridad al consumidor.

IRAM es el representante de la Argentina en la International Organization for Standardization (ISO), en la Comisión Panamericana de Normas Técnicas (COPANT) y en el Comité MERCOSUR de Normalización (CMN).

Esta norma IRAM es el fruto del consenso técnico entre los diversos sectores involucrados, los que a través de sus representantes han intervenido en los Organismos de Estudio de Normas correspondientes.

LEONID LLONTOP CASTRO

Jefe de Seguridad Casa Metritz
Banco Ciudad Bs. As.

Índice

	Página
1 OBJETO Y CAMPO DE APLICACIÓN	5
2 NORMAS PARA CONSULTA.....	5
3 DEFINICIONES.....	5
3.1 ESTACIÓN DE VIGILANCIA.....	5
3.2 CENTRO DE CONTROL A DISTANCIA (ESTACIÓN CENTRAL).....	5
3.3 CENTRO DE SUPERVISIÓN.....	5
4 REQUISITOS.....	6
4.1 REFERENTES AL LOCAL DE SUPERVISIÓN.....	6
4.2 REFERENTE A LOS OPERADORES.....	6
4.3 REFERENTE AL EQUIPAMIENTO.....	6
4.4 REQUISITOS ADICIONALES DE CARÁCTER GENERAL.....	7
Anexo A (Informativo).....	8

LEONID LLONTOP CASTRO
Jefe de Seguridad Casa Matriz
Banco Ciudad Bs. As.

Sistemas de alarma

Centros de Control a Distancia

Requisitos mínimos

1 OBJETO Y CAMPO DE APLICACIÓN

El objeto de esta norma es especificar los requisitos mínimos que debe cumplir un centro de control a distancia, tal como se define en esta norma, que recibe las señales transmitidas por un sistema de alarma de acuerdo a lo especificado en las normas IRAM 4173-1 y 4173-2. Estos requisitos comprenden aspectos referentes al local donde se emplace, a los operadores, al equipamiento y, requisitos de carácter general. Pueden incluirse otras características adicionales, siempre que la eficacia y la confiabilidad del centro de control a distancia no resulten afectadas desfavorablemente.

2 NORMAS PARA CONSULTA

Las siguientes normas contienen disposiciones, las cuales mediante su cita en este texto, se transforman en disposiciones válidas para esta Norma IRAM. En el momento de la publicación, las ediciones indicadas estaban en vigencia. Todas las normas están sujetas a revisión y las partes que realicen acuerdos basados en esta norma se deben esforzar en buscar la posibilidad de aplicar las ediciones más recientes de las normas indicadas a continuación.

IRAM-AADL J 2027:1990 – Alumbrado de emergencia en interiores de establecimientos.

IRAM 3517-1:1985 – Matafuegos manuales y sobre ruedas. Elección, instalación y uso.

IRAM 3652:1992 – Protección contra incendios. Prescripciones generales para centros de procesamiento de datos.

IRAM 4173-1:1997 – Sistemas de alarma. Sistemas de transmisión. Sección 1 - Requisitos generales.

IRAM 4173-2:1998 - Sistemas de alarma. Sistemas de transmisión. Sección 2 - Requisitos generales para los equipos utilizados.

3 DEFINICIONES

Dentro del marco de esta norma son de aplicación las definiciones siguientes:

3.1 estación de vigilancia

Recinto distante de los locales supervisados, donde se recoge la información correspondiente al estado de uno o varios sistemas de alarma ya sea para los fines de señalización (es decir un centro de control a distancia) o para los fines de retransmisión (es decir una estación satelital o un punto de centralización).

3.2 centro de control a distancia (estación central)

Estación de vigilancia que tiene personal a disposición en forma permanente, a la cual se comunican las informaciones relativas al estado de uno o varios sistemas de alarma.

3.3 centro de supervisión

Central a distancia que tiene personal a disposición donde se supervisa el estado de un sistema de transmisión de alarma.

NOTA: El centro de supervisión puede ser una central distinta o bien puede formar parte del centro de control a distancia

4 REQUISITOS

4.1 Referentes al local de supervisión

- a) Deberá existir un recinto específico dedicado exclusivamente a la supervisión, control y administración de las señales provenientes de los sistemas de alarma. Éste no deberá ser un lugar de paso a sectores asignados a otras actividades. Deberán atravesarse como mínimo dos puertas, antes de ingresar al recinto específico desde el exterior, palier o áreas comunes del edificio,
- b) Las aberturas hacia el exterior del recinto (si las hubiere), deberán contar con algún tipo de protección contra el vandalismo y deberá evitarse la observación directa de dicho recinto desde el exterior.
- c) Deberá cumplir con los reglamentos técnicos vigentes que correspondan.
- d) En lo que respecta a la protección contra incendio, además de las disposiciones legales vigentes se deberá cumplir con las normas IRAM 3652/92 y la norma IRAM 3517-Parte1.
- e) Deberá tener alumbrado de emergencia de acuerdo con la norma IRAM-AADL J 2027.
- f) Tendrá algún sistema de protección física y/o electrónica y/o mecánica a los efectos de evitar y/o demorar una posible intrusión al local y permitir al operador dar aviso a la autoridad competente.
- g) Deberá contar con instalaciones de baño y cocina adecuadas para el personal de acuerdo con las leyes de higiene y seguridad en el trabajo.

4.2 Referente a los operadores

- a) El personal afectado a las tareas específicas de supervisión administración y control de las señales de alarma deberá tener una capacitación adecuada a su función.

- b) Habrá como mínimo dos operadores por turno, durante las 24 horas.
- c) El personal del centro de control a distancia no deberá tener antecedentes penales por causas relacionadas con conductas incompatibles con su función en este centro, debiendo el empleador mantener una copia del certificado expedido por el Registro Nacional de Estadística y Reincidencia Criminal, salvo que se contrate personal de organizaciones que ya cumplan con este requisito.
- d) El empleador deberá mantener registros de análisis psicotécnicos y ambientales del personal, salvo que se contrate personal de organizaciones que ya cumplan este requisito.

4.3 Referente al equipamiento

Todo el equipamiento debe tener la redundancia necesaria que asegure la continuidad de la prestación del servicio en el sistema. Debe poder verificarse el funcionamiento correcto y adecuado del equipamiento destinado a la supervisión, control y administración de las señales provenientes de los sistemas de alarma.

4.3.1 Sistema telefónico

Si se utiliza un sistema telefónico para recibir y cursar señales de alarma, deberá cumplirse con los requisitos siguientes:

- a) Deberá tener como mínimo 2 (dos) líneas telefónicas exclusivas, para la recepción de las señales provenientes de los sistemas de alarma.
- b) Deberá tener sistemas de recepción adecuados, tales como receptores digitales de eventos, de manera que exista una correspondencia inequívoca entre las señales transmitidas y las señales recibidas. Deberán poder atenderse dos (2) líneas simultáneamente, como mínimo.
- c) No se aceptará como equipamiento de recepción de abonado aquellos sistemas

que no cuenten con una confirmación y reconocimiento inequívoco del abonado.

- d) Como equipamiento complementario deberá utilizarse computadora y software de gestión de supervisión de alarmas y eventos, que permita llevar un adecuado registro informático y/o impreso de dichos eventos. Este equipamiento podrá compararse con otros sistemas de recepción de señales provenientes de los sistemas de alarma

4.3.2 Sistema radioeléctrico

Si se utiliza un sistema radioeléctrico para recibir y cursar señales de alarma, deberá cumplirse con los requisitos siguientes:

- a) El equipamiento deberá estar homologado por la Comisión Nacional de Comunicaciones (frecuencia y equipamiento autorizados).
- b) El equipamiento radioeléctrico que se utilice para la supervisión de los locales vigilados, será de uso exclusivo para esta función, no permitiéndose la utilización de este equipamiento para la transmisión de voz y/u otro tipo de servicio.
- c) El equipamiento deberá tener medios para detectar faltas y/o fallas en la comunicación.
- d) Deberá tener sistemas de recepción adecuados de manera que exista una correspondencia inequívoca entre las señales transmitidas y las señales recibidas.
- e) Como equipamiento complementario deberá utilizarse computadora y software de gestión de supervisión de alarmas y eventos, que permita llevar un adecuado registro informático y/o impreso de dichos eventos. Este equipamiento podrá com-

partirse con otros sistemas de recepción de señales provenientes de los sistemas de alarma.

4.3.3 En el caso que el equipamiento sea capaz de recibir imágenes u otros servicios de vigilancia a distancia (audio, telecomando, etc.) deberán proveerse líneas o canales adicionales de manera que no se degrade el sistema.

4.4 Requisitos adicionales de carácter general

- a) Con la finalidad exclusiva de permitir la comunicación de eventos a la autoridad competente, deberá tener dos (2) vías de comunicación alternativas y diferentes (teléfono, celular, radio, etc.)
 - b) Deberá tener una o más fuentes de energía ininterrumpida (UPS) que posibilite 20 minutos de operación continua, de la totalidad de los equipos afectados al centro de control a distancia, ante cortes de energía.
 - c) Deberá contarse además con un generador de energía eléctrica de servicio continuo, y/o sistema alternativo que garantice un servicio de energía ininterrumpido.
- NOTA:** Si se utiliza un generador de energía eléctrica, se deberá contar con combustible de reserva para 12 horas de operación, almacenado en un ambiente distinto al del generador y del recinto de la central de supervisión.
- d) Deberá existir en el recinto algún equipo de abonado similar al de los usualmente supervisados conectado a una línea telefónica ajena al sistema de recepción, y tal que permita realizar una prueba real de recepción de alarmas por medio del equipamiento preparado a tal efecto.

LEONID LLONTOP CASTRO
 Jefe de Seguridad Caso Matriz
 Banco Ciudad Bs. As.

Anexo A (Informativo)

El estudio de esta norma estuvo a cargo de los organismos respectivos, integrados de la forma siguiente:

Subcomité de Sistemas de alarma

Integrante

Ing. Horacio AMDEN
Tco. Fabián BONGIOVANNI
Sr. Néstor CEBALLOS
Ing. Carlos CRUZ
Tco. Ruben CHANUAR
Sr. Diego GARCÍA
Ing. Luis GINESTA
Arq. Eduardo GONZALEZ
Sr. Marcelo HIRSCH
Ing. Ricardo KATZ
Ing. Antonio LUONGO
Sr. Claudio MARTINEZ
Ing. Modesto MIGUEZ
Ing. Carlos REISZ
Ing. Pablo RICCI
Ing. José ROSON
Sgto. Alberto TRULLEN
Ing. Rita MANSOUR

Representa a:

GENERAL INDUSTRIES S.A.
READY-ALARM . Concepto 2000
POL. FED ARGENTINA-DIV ALARMAS
MINISTERIO DEL INTERIOR
LOGOTEC S.A.
CENTRAL DE MONITOREO
TACTICAL TRAINING
INVITADO ESPECIALISTA
POLICÍA BONAERENSE
CEMARA
TELECOM ARG.
POLICÍA FEDERAL
AASPRI
AASPRI
GENERAL INDUSTRIES S.A.
E.Y.S.E.
POLICÍA FEDERAL
IRAM

Comité General de Normas (C.G.N.)

Integrante

Ing. Juan C. ARCIONI
Ing. Severiano ITUARTE
Ing. Samuel MARDYKS
Ing. Norberto O'NEILL
Dr. Mario PECORELLI
Ing. Rodolfo BARBOSA

LEONID LLONTOP CASTRO
Jefe de Seguridad Casa Matriz
Banco Ciudad Bs. As

IRAM 4174:1999

ICS 13.320
* CNA 6350

LEONID LLONTOP CASTRO
Jefe de Seguridad Caso Meriz
Banco Ciudad Bs. As.

* Corresponde a la Clasificación Nacional de Abastecimiento asignada por el Servicio Nacional de Catalogación del Ministerio de Defensa.



INSTITUTO ARGENTINO
DE NORMALIZACIÓN
Y CERTIFICACIÓN



INSTITUTO ARGENTINO
DE NORMALIZACIÓN
Y CERTIFICACIÓN

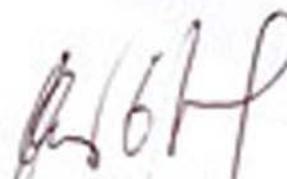
ESQUEMA 2

DE NORMA IRAM 4175

Sistemas de alarma de intrusión en inmuebles

Código de práctica para la planificación y la instalación

Intruder alarm systems in building
Code of practice for planning and installation


Dirección de Certificación


Comité General de Certificación


Dirección General



**LAS OBSERVACIONES DEBEN
ENVIARSE CON EL FORMULARIO DE LA
ETAPA DE
DISCUSIÓN PÚBLICA**

LEONID LLONTOP CASTRO
Jefe de Seguridad Casa Matriz
Banco Ciudad Bs As.

DOCUMENTO EN ESTUDIO

Prefacio

El Instituto Argentino de Normalización y Certificación (IRAM) es una asociación civil sin fines de lucro cuyas finalidades específicas, en su carácter de Organismo Argentino de Normalización, son establecer normas técnicas, sin limitaciones en los ámbitos que abarquen, además de propender al conocimiento y la aplicación de la normalización como base de la calidad, promoviendo las actividades de certificación de productos y de sistemas de la calidad en las empresas para brindar seguridad al consumidor.

IRAM es el representante de la Argentina en la International Organization for Standardization (ISO), en la Comisión Panamericana de Normas Técnicas (COPANT) y en la Asociación MERCOSUR de Normalización (AMN).

Esta norma IRAM es el fruto del consenso técnico entre los diversos sectores involucrados, los que a través de sus representantes han intervenido en los Organismos de Estudio de Normas correspondientes.

LEONID LLONTOP CASTRO
Jefe de Seguridad Caso Matriz
Banco Ciudad Bs. As.

Índice

	Página
0. INTRODUCCIÓN.....	5
1. OBJETO Y CAMPO DE APLICACIÓN.....	5
2. DOCUMENTOS NORMATIVOS PARA CONSULTA.....	5
3. DEFINICIONES.....	6
3.1 Activado (en servicio) [1].....	6
3.2 Alarma.....	6
3.3 Centro de control a distancia (estación central).....	6
3.4 Condición de alarma.....	6
3.5 Desactivado (fuera de servicio).....	6
3.6 Empresa o compañía de alarma.....	6
3.7 Falsa alarma.....	7
3.7.1 Falsa alarma técnica.....	7
3.7.2 Falsa alarma de operación.....	7
3.7.3 Falsa alarma por factores externos.....	7
3.8 Sistema de alarma.....	7
3.9 Sistema de alarma de intrusión.....	7
3.10 Unidad central de alarma.....	7
3.10.1 Unidad de procesamiento.....	7
3.10.2 Panel de señalización y control.....	7
3.11 Usuario.....	8
3.12 Zona de detección.....	8
4. PLANIFICACIÓN.....	8
4.1 Consulta.....	8
4.1.1 Generalidades.....	8
4.1.2 Planificación y especificaciones.....	8
4.2 Cronograma.....	9
4.2.1 Preparación.....	9
4.2.2 Camino crítico.....	10
4.2.3 Operación parcial.....	10
4.3 Relevamiento.....	10
4.3.1 Inspección del sitio a ser protegido y sus contenidos.....	10
4.3.2 Factores ambientales, mecánicos y otros.....	11
4.3.3 Ubicación de la unidad central de alarmas.....	13
4.3.4 Tipo y ubicación de los sensores y detectores.....	13
4.3.5 Horarios de activación y desactivación.....	13
4.4 Diseño del sistema.....	13
4.4.1 Funciones y operación.....	13
4.4.2 Condiciones generales del sistema.....	13
4.4.3 Rutas de Entrada y Salida.....	14
4.4.4 Zonas supervisadas.....	15
4.4.5 Zonas protegidas las 24 h ("Zona 24hs").....	15
4.4.6 Instalación eléctrica relacionada con el sistema de alarma. Diagramación del Cableado.....	15
4.4.7 Consideraciones para Interconexiones inalámbricas.....	15
5. INSTALACIÓN.....	16
5.1 Generalidades.....	16
5.1.1 Responsabilidades y funciones del instalador.....	16
5.1.2 Equipamiento.....	16
5.1.3 Cableado del Sistema.....	16
5.1.4 Interconexiones inalámbricas.....	18
5.1.5 Supervisión de la instalación.....	18
5.2 Detectores.....	18
5.2.1 Generalidades.....	18
5.2.2 Sensores de apertura.....	19
5.2.3 Detectores de vibraciones.....	19

5.2.4	Detectores de rotura de vidrio	20
5.2.5	Alfombras detectoras de presión	21
5.2.6	Barreras infrarrojas	22
5.2.7	Detectores de Movimiento	23
5.2.7.1	Generalidades	23
5.2.7.2	Detectores de efecto Doppler ultrasónico	23
5.2.7.3	Detectores Doppler de microondas	24
5.2.7.4	Detectores infrarrojos pasivos	25
5.2.7.5	Dispositivos de tecnologías múltiples	25
5.2.8	Dispositivos de activación deliberada	26
5.2.9	Cableado continuo	27
5.2.10	Dispositivo para Alambre tenso	27
5.3	Unidad central de alarma	27
5.3.1	Generalidades	27
5.3.2	Indicadores	28
5.3.3	Activación y desactivación	28
5.4	Dispositivos de Advertencia	28
5.4.1	Alarmas audibles	28
5.4.1.1	Alarmas audibles externas	29
5.4.1.2	Alarmas audibles internas	29
5.4.2	Sistema de transmisión de alarmas - Dispositivos de señalización remota	29
5.5	Cableado de interconexión	30
5.5.1	Selección y ubicación	30
5.5.2	Puesta a tierra e interferencia eléctrica	31
5.6	Suministro de alimentación	31
5.6.1	Equipo de alimentación	31
5.6.2	Tipos de equipos de alimentación	31
5.6.2.1	Alimentación de red y de batería recargable de reserva	31
5.6.2.2	Alimentación sólo con batería recargable	32
5.6.3	Conexiones a las baterías y a las fuentes de alimentación	32
5.6.4	Ubicación y alojamiento	32
5.6.5	Desempeño	33
5.7	Verificación y entrega del sistema instalado	33
5.7.1	Generalidades	33
5.7.2	Verificaciones	33
5.7.3	Verificaciones operacionales	34
5.7.3.1	Generalidades	34
5.7.3.2	Detectores y detección de desarme ("tamper detection")	35
5.7.3.3	Suministros de energía	35
5.7.3.4	Dispositivos de advertencia y señalización	35
5.7.4	Entrega	35
Anexo A	37
Bibliografía	37
Anexo B	38
Integrantes del organismo de estudio	38

Sistema de alarma de intrusión en inmuebles

Código de práctica para la planificación y la instalación

0. INTRODUCCIÓN

El objeto de esta norma es el de maximizar la efectividad de los sistemas de alarma, en lo que respecta a la detección y señalización de intrusiones no deseadas y/o no autorizadas en inmuebles, y minimizar la ocurrencia de falsas alarmas.

Aún cuando la planificación o diseño de un sistema de alarma sea minuciosamente realizado, ningún sistema puede garantizar totalmente la detección de intrusos. El propósito de un sistema de alarma es el de conferir a los bienes y a las personas en riesgo, un nivel de seguridad, balanceado con el grado de determinación y pericia del intruso, por medio de un planeamiento cuidadoso. Al hacer esta evaluación, todas las circunstancias físicas del riesgo deben contemplarse, pero el grado de seguridad adoptado tiene que ser consistente con un sistema en todo sentido práctico y confiable, y que no se transforme en una carga para las personas en general o la policía.

Aún más, ningún sistema de alarma, correctamente diseñado e instalado, es completamente confiable o a prueba de sabotaje. La operación exitosa de un sistema de alarma, requiere también la colaboración activa del usuario, en llevar a cabo los procedimientos necesarios en forma cuidadosa, adecuada y regular.

La utilidad de todo el sistema puede verse comprometida por la falta de cuidado o inadecuada atención de la rutina de mantenimiento preventivo y correctivo. Este cuidado es extensivo a la seguridad de claves y de información relacionada con el sistema, su instalación y operación.

LEONID LLONTOP CASTRO
Jefe de Seguridad Casa Matriz
Banco Ciudad Bs. As.

1. OBJETO Y CAMPO DE APLICACIÓN

Esta norma tiene por objeto dar las recomendaciones para la planificación, el diseño y la instalación de sistemas de alarmas de intrusión automáticas o de accionamiento voluntario, en inmuebles.

Esta norma no excluye ninguna otra norma aplicable o recomendación para casos específicos.

2. DOCUMENTOS NORMATIVOS PARA CONSULTA

Los documentos normativos que se indican a continuación son indispensables para la aplicación de este documento.

Para los documentos normativos en los que se indica el año de publicación, se aplican las ediciones citadas.

Para los documentos normativos en los que no se indica el año de publicación, se aplican las ediciones vigentes, incluyendo todas sus modificaciones.

IRAM 2281-3 - Puesta a tierra de sistemas eléctricos. Instalaciones industriales y domiciliarias (inmuebles) y redes de baja tensión. Código de práctica.

IRAM 2281-5 - Código de práctica para puesta a tierra de sistemas eléctricos. Puesta a tierra de sistemas de telecomunicaciones (telefonía, telemedición y equipos de procesamiento de datos).

IRAM 4171-1 - Sistemas de alarma. Primera Parte. Generalidades.

IRAM 4171-2 - Sistemas de alarma. Requisitos generales. Código de práctica.

IRAM 4172 - Sistemas de alarma. Detectores infrarrojos pasivos utilizados en los edificios. Requisitos.

IRAM 4254 - Sistemas de alarma. Detectores de intrusión. Requisitos generales.

IRAM-IEC 1241 - Materiales eléctricos para uso en presencia de polvos combustibles (serie de normas).

IRAM-IAP-IEC 79 - Materiales eléctricos para atmósferas gaseosas explosivas (serie de normas).

AEA - Reglamentación para la ejecución de instalaciones eléctricas en inmuebles.

3. DEFINICIONES

Para los fines de la presente norma se aplican las definiciones siguientes:

3.1 Activado (en servicio) [1]

Estado de un sistema de alarma de intrusión o parte de éste en el que se hace posible la notificación de una condición de alarma.

3.2 Alarma

Advertencia de la presencia de un riesgo para la vida, la preservación de los bienes o del ambiente

3.3 Centro de control a distancia (estación central)

Estación de vigilancia que tiene personal a disposición en forma permanente, a la cual se comunican las informaciones relativas al estado de uno o varios sistemas de alarma.

3.4 Condición de alarma

Condición del sistema de alarma o parte de éste como respuesta del sistema ante la presencia de un riesgo.

3.5 Desactivado (fuera de servicio)

Estado de un sistema de alarma de intrusión en el que no es posible que se notifique una condición de alarma.

3.6 Empresa o compañía de alarma

LEONID LLONTOP CASTRO
Jefe de Seguridad Casa Matriz
Banco Ciudad Bs. As.

Organización que proporciona, instala y/o provee el mantenimiento de los sistemas de alarma.

3.7 Falsa alarma

Condición de alarma no generada por una intrusión o intento de intrusión en las instalaciones supervisadas.

3.7.1 Falsa alarma técnica

Señal de alarma generada por error y provocada por un mal funcionamiento o defecto de algún elemento constitutivo del sistema de alarma.

3.7.2 Falsa alarma de operación

Señal de alarma generada por error y provocada por algún error en la operación del sistema de alarma, por ejemplo: la maniobra accidental de un pulsador, errores de operación en el panel de señalización y control, o por un error de un operador o usuario.

3.7.3 Falsa alarma por factores externos

Señal de alarma generada por error y provocada por ejemplo por interferencias electromagnéticas, factores ambientales, y /ó la respuesta de un dispositivo automático en condiciones distintas a las de la concepción original.

3.8 Sistema de alarma

Instalación eléctrica diseñada para detectar y señalar la presencia de una situación anormal, indicando la existencia de un riesgo.

3.9 Sistema de alarma de intrusión

Sistema de alarma diseñado para detectar y señalar la presencia, entrada o intento de entrada de un intruso en las instalaciones supervisadas.

3.10 Unidad central de alarma

Equipo que procesa las señales de salida de uno o de varios detectores para determinar si el estado de alarma debe ser generado.

La unidad central de alarma comprende una unidad de procesamiento y uno o más paneles de señalización y control.

3.10.1 Unidad de procesamiento

Parte de la unidad central de alarma que procesa las señales.

3.10.2 Panel de señalización y control

Parte de la unidad central de alarma donde se visualiza el estado del sistema y desde donde se lo opera.

3.11 Usuario

Persona autorizada a utilizar el sistema de alarma o persona u organización que contrata a una empresa de alarmas.

3.12 Zona de detección

Cada una de las secciones de la unidad central de alarma con distintas condiciones de uso que permiten conectar detectores para la protección de las distintas áreas.

4. PLANIFICACIÓN

4.1 Consulta

LEONID LLONTOP CASTRO
Jefe de Seguridad Casa Matriz
Banco Ciudad Bs. As.

4.1.1 Generalidades

Los requisitos para un sistema de alarmas en inmuebles deben acordarse lo más detalladamente posible entre las partes interesadas como ser: usuarios, arquitectos, consultores, empresas de alarmas, organizaciones que provean servicios de control a distancia, la policía local, aseguradores, compañías de telecomunicaciones y las autoridades públicas concernientes. Cuando se provean medios para la transmisión de las señales de alarma hacia un centro de control a distancia, estación de policía o algún otro organismo de seguridad, debe haber una consulta o acuerdo previo entre las partes interesadas.

4.1.2 Planificación y especificaciones

Sobre las bases de la consulta, se deben elaborar las especificaciones y si es necesario planos.

Éstos deben contener:

- a) Detalles del sistema de alarmas propuesto.
- b) Detalles de la alimentación eléctrica necesaria.
- c) Espacio requerido para el equipamiento.
- d) Canalizaciones requeridas para el cableado, de ser aplicable.

Los sistemas deben consistir en: uno o más detectores y/o uno o más sensores con procesadores asociados; una o más unidades centrales de alarmas; uno o más dispositivos de prevención y/o equipamiento de señalización; equipamiento de fuentes de energía necesario; y cuando sea apropiado una fuente de alimentación independiente.

La distribución del cableado debe ser acordada, si correspondiera, con los responsables de otros servicios para permitir la realización de las canalizaciones necesarias, previamente a la iniciación de las obras en el inmueble. La necesidad de la separación física del cableado destinado al sistema de alarmas debe tomarse en cuenta en esta etapa.

NOTA. Tomar en cuenta la "Reglamentación para la Ejecución de Instalaciones Eléctricas en Inmuebles" de la Asociación Electrotécnica Argentina y reglamentaciones vigentes referentes a instalaciones radioeléctricas.

Cuando se usan interconexiones inalámbricas, se deben considerar los factores siguientes:

- a) Emplazamiento de las antenas para asegurarse una comunicación fiable con otros componentes del sistema.
- b) Posibilidad de que otros equipos de RF interfieran con el equipo de interconexión del sistema de alarma de intrusión.
- c) Proximidad de grandes objetos metálicos a la antena del equipo.

NOTA. Tener en cuenta las reglamentaciones locales vigentes aplicables.

4.2 Cronograma

LEONID LLONTOP CASTRO
Jefe de Seguridad Casa Matriz
Banco Ciudad Bs. As.

4.2.1 Preparación

Para preparar un cronograma, puede tomarse en consideración la siguiente lista de pasos, no necesariamente en el orden indicado:

- a) Relevamiento del predio, local o edificio y estudio de sus planos y el destino y utilización del inmueble.
- b) Diseño inicial del sistema, teniendo en cuenta los requisitos y las recomendaciones (si las hubiere) de todas las partes interesadas.
- c) De ser necesario, verificar la disponibilidad de vínculos de comunicaciones, contactándose con los proveedores u organismos de regulación.
- d) Estimación de costos.
- e) Elevar a la consideración del cliente el diseño propuesto y su cotización.
- f) De ser necesario, ajustar los detalles del diseño luego de una revisión conjunta con el cliente.
- g) Emitir las órdenes de compra por los componentes del sistema.
- h) Planificar detalladamente la instalación.
- i) Aprovisionamiento y/o producción y entrega.
- j) Instalación del sistema
- k) Ensayo y verificación funcional del sistema.
- l) Analizar y convenir las acciones a llevar a cabo en el caso de un evento que active el sistema.

- m) Entrega del sistema al cliente y capacitación acerca de los procedimientos de operación del sistema.
- n) Conexión de alguna señalización accesoria remota que haya sido previamente acordada y que no se haya podido instalar hasta el momento de la entrega.
- o) De ser necesario notificar a las autoridades competentes según reglamentaciones vigentes.

4.2.2 Camino crítico

En instalaciones grandes o especiales será de práctica normal para todas las etapas dadas en 4.2.1 incluirlas en un diagrama de camino crítico. En algunas instalaciones se debe tener en cuenta la necesidad de abastecimiento de equipamiento especial. En edificios en construcción o reconstrucción, el cableado o la interconexión inalámbrica de los sistemas de alarma deben llevarse a cabo en tiempo y etapas de construcción y decoración acordadas con el contratista principal u otros contratistas. La instalación del equipamiento del sistema de alarmas debe coordinarse cuidadosamente con las tareas de otros gremios u oficios para minimizar las posibilidades de daño causado por trabajos de decoración, humedad, polvo, etc. Puede ser necesaria la utilización de una protección provisoria para el equipamiento.

4.2.3 Operación parcial

La conexión final y la puesta en marcha del sistema deben realizarse en el momento acordado entre el cliente y la empresa de alarmas. Sin embargo, puede existir un período de operación parcial, ya sea durante la ocupación parcial del edificio o para proveer de seguridad durante la construcción. Dicha operación es un tema de acuerdo entre las partes interesadas y debe revisarse regularmente.

NOTA. Durante cualquier período de operación parcial del sistema de alarma, el cliente debe ser informado para que tome en cuenta los necesarios desplazamientos de los trabajadores durante la obra

4.3 Relevamiento

LEONID LLONTOP CASTRO
Jefe de Seguridad Casa Matriz
Banco Ciudad Bs. As.

4.3.1 Inspección del sitio a ser protegido y sus contenidos

El sitio a ser protegido y sus contenidos deben ser inspeccionados de forma tal de poder determinar los requisitos particulares del diseño de un sistema de alarma que garantice una adecuada capacidad de detección y de aviso o señalización. Los aspectos enunciados a continuación, se deben considerar en forma conjunta con todos aquellos requisitos legales de cumplimiento obligatorio y, si son aplicables, los de las aseguradoras u otros cualquiera fuere su naturaleza.

- a) Con respecto al Sitio
 - 1) Su construcción y disposición.
 - 2) Características de ocupación.
 - 3) Características de no ocupación.
 - 4) Responsables autorizados para asignarles códigos o llaves.
 - 5) Entorno.

- 6) Ubicación.
 - 7) Edificios o sitios vecinos y su ocupación.
 - 8) Disposición o distribución de sus ocupantes.
 - 9) Posibilidades de acceso al sitio a proteger.
 - 10) Naturaleza de la seguridad ya existente.
 - 11) Puertas y ventanas.
 - 12) Intrusiones previas.
 - 13) Normas y regulaciones de salubridad, incendio y seguridad aplicables.
 - 14) Contaminación o polución por ruidos, o interferencias electromagnéticas.
- b) Con respecto a los Contenidos o Bienes
- 1) Tipo y naturaleza.
 - 2) Valor.
 - 3) Dimensiones físicas (tamaño y peso).
 - 4) Seguro.
 - 5) Pérdidas o sustracciones previas.
 - 6) Estimación del valor de una única pérdida.
 - 7) Facilidad de retiro del lugar.
 - 8) Facilidad de reducción posterior.
 - 9) Disponibilidad de reemplazos.
 - 10) Efectos de la pérdida.
 - 11) Distribución física de los contenidos o bienes dentro del sitio.

4.3.2 Factores ambientales, mecánicos y otros

Los factores ambientales existentes y también los potenciales del sitio a ser protegido deben ser considerados en el momento de efectuar la planificación del sistema a ser instalado. Deben tomarse en cuenta las protecciones contra daño mecánico, clima, humedad, corrosión, aceites y otros agentes adversos propios de una atmósfera industrial y otros factores que puedan existir y que deban ser considerados y sólo se los podrá conocer luego de una minuciosa inspección del sitio y/o de la realización de preguntas a sus ocupantes o responsables.

Si bien es imposible definir tales riesgos, se los puede agrupar en dos grandes grupos:

- a) Aquellos presentes dentro del área a ser protegida o en las adyacencias inmediatas que están bajo el control del cliente, como por ejemplo:
 - 1) Cañerías de agua.

- 2) Ventiladores y piezas anexas a éstos.
 - 3) Señalizaciones o carteles suspendidos.
 - 4) Aire acondicionado.
 - 5) Montacargas o ascensores.
 - 6) Iluminación fluorescente.
 - 7) Timbre de aparatos telefónicos.
 - 8) Sistemas de calefacción.
 - 9) Roedores, pájaros, etc...
 - 10) Ruidos extraños.
 - 11) Corrientes de aire provenientes de puertas y ventanas con cierrres defectuosos.
 - 12) Interferencias electromagnéticas.
- b) Aquellos que están más allá del control del cliente y que podrían afectar o comprometer la estabilidad del funcionamiento del sistema de alarma, como por ejemplo:
- 1) Los efectos del tránsito vehicular, ferroviario o aéreo.
 - 2) La construcción de túneles por debajo de las fundaciones o cimientos.
 - 3) Sitios ocupados parcialmente por terceros.
 - 4) Sitios contiguos que al ser ocupados afecten a la propiedad protegida.
 - 5) Condiciones ambientales extremas.
 - 6) Construcciones o edificaciones prefabricadas o livianas.
 - 7) Interferencia por radiofrecuencias.
 - 8) Transitorios en la alimentación eléctrica de red.

Además, es conveniente inspeccionar el sitio detalladamente en la búsqueda de otros factores que requieran una consideración especial, tales como:

- 1) Sectores que requieran mantener una atmósfera de aire libre de impurezas.
- 2) La presencia de sustancias inflamables o explosivas tales como gases, polvos, vapores o líquidos volátiles.
- 3) El acceso al sitio protegido en caso de una emergencia.
- 4) La posibilidad de que se produzcan activaciones o accionamientos no deseados por ejemplo por personas que circunstancialmente pasen por el lugar.
- 5) Cualquier sospecha de que vayan a existir cambios en las necesidades de seguridad en un futuro cercano.
- 6) Cualquier característica poco común del sitio sus contenidos o su funcionamiento por ejemplo problemas con la red eléctrica

- 7) Cualquier restricción particular propia de los materiales con que está construido el sitio a ser protegido como así también cualquier norma de incendio de características especiales que sea de aplicación.

4.3.3 Ubicación de la unidad central de alarmas

La unidad de procesamiento de la unidad central de alarmas debe ubicarse en un sitio tal que no sea visible desde el exterior del sitio protegido. También debe existir suficiente espacio libre como para que un técnico de mantenimiento pueda acceder y trabajar sobre el equipamiento. Se debe tener particular cuidado en no invadir con el equipamiento zonas que sean de paso frecuente y que puedan dar lugar a lastimaduras o accidentes.

La extensión de la seguridad a la unidad central de alarmas en sí es importante y puede llegar a ser necesario un gabinete protegido por el mismo sistema de alarma para alojar al equipamiento y para aumentar la dificultad del acceso no autorizado a la unidad de procesamiento.

Es recomendable, a fin de darle mayor seguridad al sistema, que la unidad central de alarmas disponga de un panel de control y señalización remota. En este caso, el usuario dispondrá de un fácil acceso para la operación y visualización del estado del sistema.

Cuando se esté determinando la mejor ubicación para la unidad central de alarmas, se debe tener en consideración el o los caminos de acceso o de entrada y salida.

4.3.4 Tipo y ubicación de los sensores y detectores

Los sensores o detectores que no sean de accionamiento voluntario (pulsadores manuales), estarán diseñados para sensar o detectar a una o más personas alterando o moviéndose a través del área protegida o perturben dicha área. Es importante asegurarse durante la inspección previa que los sensores o detectores no se accionen por cualquier otra perturbación que no se desee detectar cuando el sistema esté activado.

4.3.5 Horarios de activación y desactivación

Si se utiliza el servicio de un centro de control a distancia y a fin de que se puedan verificar los horarios de activación y desactivación del sistema, es necesario determinar los horarios o los períodos en los cuales los procedimientos de activación y desactivación se podrán llevar a cabo, estableciéndose horarios y días de la semana, tolerancias admitidas y previsiones especiales para los días feriados. La activación o desactivación del sistema en horarios irregulares impedirá utilizar todas las funciones de supervisión que una central de control a distancia puede ofrecer. Cuando se revise este tema se deben tener en cuenta los ingresos y egresos de personal de limpieza, maestranza y de mantenimiento al sitio protegido.

4.4 Diseño del sistema

LEONID LLONTOP CASTRO
Jefe de Seguridad Casa Matriz
Banco Ciudad Bs As.

4.4.1 Funciones y operación

A continuación del relevamiento inicial y antes del comienzo de la instalación se debe realizar un diseño detallado del funcionamiento y operación del sistema. Cada elemento de la instalación debe ser adecuado y compatible con la especificación de protección o cobertura acordada. Esto puede requerir la consulta a un especialista experimentado y un cuidadoso análisis de los temas mencionados en 4.4.2 y 4.4.5.

4.4.2 Condiciones generales del sistema

El sistema cumplirá con los requisitos de las IRAM 4171-1, IRAM 4171-2 e IRAM 4172.

Además el sistema será tal que cumpla las condiciones siguientes:

- a) Cualquier circuito o zona que provoque el accionamiento inicial del sistema y/o que genere un reporte o transmisión, debe poder ser identificado aún cuando el sistema sea desactivado.
- b) Los pulsadores manuales, si son utilizados, tendrán algún dispositivo que permita la identificación inequívoca de su accionamiento.
- c) El sistema tendrá una cantidad racional de detectores por zona de detección en función del mantenimiento, localización, identificación de fallas, características físicas y eléctricas del equipo. Esta cantidad no debe ser superior a diez (10) detectores por zona, si se utilizan detectores con capacidad de identificación individual. Si se incluyen en esta cantidad máxima, detectores sin capacidad de identificación individual, se limitará a cinco (5) el número máximo de éste tipo de detectores por zona.
- d) No se utilizarán en una misma zona detectores con distintas tecnologías de detección que puedan provocar la anulación o enmascaramiento de eventos (Ej.: sensores magnéticos que queden autorretenidos y no permitan el restablecimiento de la zona impidiendo el envío de una señal de alarma posterior que pudo haber sido generada por un sensor de reposición automática como el infrarrojo).

4.4.3 Rutas de Entrada y Salida

La(s) ruta(s) o recorrido(s) de entrada y de salida son normalmente, pero no necesariamente, la(s) misma(s). Son utilizadas para proveer un trayecto por el cual, durante el transcurso del procedimiento de desactivación o de activación, la persona autorizada para activar o desactivar el sistema, pueda moverse entre el punto de ingreso y la unidad central de alarmas, y entre la unidad central de alarmas y el punto de salida.

El inicio del procedimiento de activación total o parcial del sistema debe ser realizado por medio del panel de señalización y control.

Si alguna zona de detección no se encuentra en el estado correcto al intentar la activación del sistema, el sistema debe permanecer desactivado hasta tanto el dispositivo o zona de detección se encuentre en estado correcto. Si se decide inhabilitar dicha zona, a sabiendas de que se está disminuyendo el nivel de seguridad acordada, el usuario debe dar aviso al servicio técnico pertinente.

Debe mantenerse una señalización interna audible, durante el tiempo de salida e inhibirse la operación de cualquier equipamiento de señalización local o remota durante ese lapso.

El procedimiento de activación o desactivación se debe realizar mediante alguna de las siguientes modalidades o bien una combinación de ellas:

- a) Operación de un teclado instalado en el interior de la propiedad protegida, que contemple una entrada/salida temporizada

NOTA. Es aconsejable la existencia de una señal sonora y/o visual que advierta acerca de la finalización del tiempo prefijado para la temporización.

- b) Operación de una cerradura de contacto de seguridad instalada en la puerta de entrada/salida o cercana a ella.
- c) Operación de un comando remoto (por ejemplo transmisor de radio frecuencia, telefónico, etc).

NOTA. Puede considerarse a la modalidad a) como la opción más segura.

Los períodos de tiempo permitidos para las entradas o salidas temporizadas deben ser acordados al momento del relevamiento, y deben ser puestos como propuestas en la especificación. La decisión final debe tomarse cuando el sistema sea entregado al usuario.

El periodo de tiempo que haya sido acordado después de una prueba real debe registrarse (ver 5.7.4)

4.4.4 Zonas supervisadas

Todas las zonas deben tener una forma de detectar falla(s) o sabotaje (por ejemplo con la utilización de una resistencia de final de línea conectada al final de la línea o método equivalente).

4.4.5 Zonas protegidas las 24 h ("Zona 24hs")

A los efectos de lograr un temprano diagnóstico y corrección de fallas, el sistema debe ser tal que cuando esté desactivado, supervisará continuamente cualquier zona de detección de 24hs. Las condiciones de falla deben ser señalizadas en forma visible y audible en el panel de señalización y control, el que debe identificar al circuito en condición de falla. La señalización debe mantenerse hasta que la condición de falla haya sido corregida.

Es aceptable poder cancelar solo la señalización audible, siempre que el sistema o parte de él no pueda activarse en esas condiciones.

4.4.6 Instalación eléctrica relacionada con el sistema de alarma. Diagramación del Cableado

En instalaciones de gran tamaño o especiales, es importante que durante el relevamiento y antes de comenzar la instalación, se planifique y defina la diagramación de la instalación eléctrica relacionada con el sistema de alarma. Si los cables pueden ser sometidos a daño accidental, deben ser protegidos mecánicamente. En ambientes tales como las viviendas, oficinas, salas de exposiciones, debe planificarse el cableado oculto (o bajo cañerías) donde sea posible. El cableado a la vista entre la unidad central de alarmas, los dispositivos de aviso audible, el panel de control y señalización y las fuentes de alimentación asociadas (si existen), debe ser protegido mecánicamente a los efectos de proporcionarle mayor seguridad. Debe prestarse especial atención a la carga en los cables de alimentación y las caídas de tensión en largos recorridos, a fin de asegurar que se mantendrán en el sistema los valores adecuados de tensión de operación.

En todos los casos debe cumplirse con lo establecido en la "Reglamentación para la ejecución de instalaciones eléctricas en inmuebles" de la Asociación Electrotécnica Argentina, como así también cualquier otra reglamentación legal aplicable vigente, y la IRAM 2281-3: Puesta a tierra de sistemas eléctricos. Instalaciones industriales y domiciliarias (inmuebles) y redes de baja tensión. Código de práctica.

Si la instalación eléctrica relacionada con el sistema de alarma recorre áreas con atmósferas explosivas deben considerarse las normas aplicables de la serie de normas IRAM-IAP-IEC 79 e IRAM-IEC 1241.

4.4.7 Consideraciones para Interconexiones inalámbricas

En los casos en los que se seleccionen interconexiones inalámbricas, se debe prestar una consideración cuidadosa a la influencia de las transmisiones intencionadas o no intencionadas

que usen la misma frecuencia y/o medios de modulación de señal que los del sistema de alarmas. Las transmisiones de este tipo pueden dar lugar a que en el sistema de alarmas se generen condiciones de manipulación o de falla o que impidan que las interconexiones funcionen correctamente.

5. INSTALACIÓN

LEONID LLONTOP CASTRO
Jefe de Seguridad Casa Matriz
Banco Ciudad Bs. As.

5.1 Generalidades

5.1.1 Responsabilidades y funciones del instalador

El o los responsables de la instalación deben contar con las especificaciones completas a fin de asegurar que:

- a) Todo el equipamiento y otros materiales estén disponibles para completar la instalación.
- b) Sea conocida la ubicación de todo el equipamiento y que las unidades sean apropiadas para instalarse en los lugares especificados.
- c) Los detectores de movimiento sean ubicados en las posiciones y ángulos (altitudes) adecuados.

No debe realizarse ninguna modificación a la especificación que no haya sido previamente acordada.

5.1.2 Equipamiento

Todo el equipamiento, antes de ser enviado al lugar de la instalación, debe ser inspeccionado y probado a fin de asegurar la correcta operación de las unidades antes de su instalación. Debe utilizarse un embalaje y almacenamiento adecuados en el vehículo de transporte a fin de reducir el riesgo de daño al equipamiento delicado en tránsito. Deben considerarse y tomar las previsiones del caso a fin de almacenar adecuadamente el equipamiento una vez recibido en el lugar, previo a su instalación.

5.1.3 Cableado del Sistema

Antes de comenzar la instalación, se debe pasar un tiempo inspeccionando el edificio en atención al recorrido del cableado propuesto y a cualquier problema potencial que pudiera surgir, como ser daños ambientales o mecánicos.

En instalaciones de alto riesgo deben utilizarse cajas de conexión con detección de sabotajes a discreción del instalador y el asegurador.

Todos los cables deben identificarse en los extremos, a fin de facilitar un rápido rastreo en caso de fallas de interconexión. Se dejarán suficientes puntos de prueba, dentro de las cajas de conexión, a fin de identificar fallas eficientemente.

NOTA. El corte de la aislación de los cables como práctica para realizar pruebas está reñida con las reglas del arte de la correcta práctica de la ingeniería eléctrica.

Durante las instalaciones se deben contemplar los siguientes puntos importantes:

- a) El cableado de interconexión del sistema de alarmas, sea este a la vista o dentro de canalización, no debe pasar a través del hueco de ascensores.
- b) El cableado de interconexión no debe pasar por canalizaciones que contengan el cableado de la alimentación principal de red, a menos que el cableado de interconexión esté adecuadamente blindado y puesto a tierra o con separaciones metálicas puestas a tierra, o esté separado de alguna manera del cableado de la alimentación principal de red por ejemplo en otra canalización, o esté aislado al nivel de la tensión más alta presente en el del cableado de la alimentación principal de red.
- c) Las instalaciones que presentan problemas ambientales pueden requerir precauciones especiales, por ejemplo, revestimientos, corazas, etc., cuando se deba considerar la acción corrosiva de los ácidos.
- d) El alma de los cables que estén unidos en una caja de empalme debe mantener la misma codificación de color.
- e) Se debe seguir lo establecido en la "Reglamentación para la ejecución de instalaciones eléctricas en inmuebles" de la Asociación Electrotécnica Argentina o reglamentaciones legales vigentes.

El cableado de interconexión debe estar adecuadamente sustentado: pueden considerarse como fijaciones adecuadas las siguientes:

- 1) Conductos: Cuando se utilicen conductos metálicos, deben fijarse en cada extremo protecciones o conectores adecuados cuando sea conveniente, para evitar daños en el cable.
- 2) Canalizaciones de PVC o de metal: Cuando se utilicen canalizaciones de PVC o de metal para transportar el cable, la canalización debe terminar tan cerca como sea posible de la unidad que se está conectando.
- 3) Grampas aisladas.
- 4) Clips y sujetadores de cables.
- 5) Catenarias aéreas: Cuando se utilice este método, la catenaria debe estar sujeta en condiciones seguras al edificio.
- 6) Adhesivos: El uso de adhesivos adecuados se permite cuando se fijan a superficies tales como vidrio o mármol.

Se debe tener cuidado cuando se fijan cables sobre madera para evitar daños. Cuando se utilice una pistola engrampadora, se debe tener cuidado para asegurar que la aislación del cable no sea dañada por la grampa.

Las uniones o conexión entre cables retorcidos deben estar soldados, para evitar que se oxiden con el aire, creando uniones de alta resistencia y potenciales falsas alarmas.

5.1.4 Interconexiones inalámbricas

Cuando se utilizan interconexiones inalámbricas, se deben considerar los factores siguientes:

- a) Emplazamiento de las antenas para asegurarse una comunicación fiable con otros componentes del sistema.
- b) Posibilidad de que otros equipos de RF interfieran con el equipo de interconexión del sistema de alarmas.
- c) Proximidad de grandes objetos metálicos a la antena del equipo.

5.1.5 Supervisión de la instalación

El nivel de supervisión durante la instalación depende del tamaño y la complejidad del sistema que se instale, de la cantidad y el nivel de los técnicos involucrados y la vinculación requerida con otros oficios.

Debe verificarse que el equipamiento que está siendo instalado y su instalación cumplan con las especificaciones acordadas.

5.2 Detectores

LEONID LLONTOP CASTRO
Jefe de Seguridad Casa Matriz
Banco Ciudad Bs. As

5.2.1 Generalidades

Es importante que se seleccionen, empleen e instalen dispositivos de detección apropiados. Cuando existan instrucciones y especificaciones del fabricante, deben ser consultadas antes de proceder a la selección y la instalación.

Los detectores instalados en el exterior de la propiedad protegida deben ser fabricados conforme a la específica aplicación y deben ser resistentes a, o estar adecuadamente protegidos de, las condiciones ambientales externas y deben ser instalados de forma tal que no puedan generarse condiciones de alarma ante un acceso autorizado o normal a la propiedad, por la degradación de las condiciones atmosféricas locales, tales como vientos fuertes o bruma, o por aves, animales pequeños, etc.

Un detector debe ser fijado de manera tal que sean posibles las pruebas eléctricas y las operaciones de ajuste sin mover al dispositivo de su fijación. No debe ser posible ajustar un detector sin activar un dispositivo antisabotaje.

Debe prestarse especial atención a los requisitos establecidos por el fabricante para los detectores de múltiple tecnología.

A continuación se dan algunos ejemplos de los aspectos mencionados en este apartado, a tener en cuenta para la instalación de los detectores:

- a) Objetos en movimiento dentro del alcance de un detector.
- b) Animales dentro del alcance del detector cuando se activa el sistema de alarma.
- c) Selección correcta del equipo en función del ambiente.
- d) Instalación de acuerdo con la especificación del fabricante.
- e) Selección de detectores con requisitos de cobertura adecuados para la identificación individual de los detectores electrónicos en caso de activación.
- f) Disposición de instalaciones de ensayo para verificar el funcionamiento de los detectores.
- g) Posicionamiento para desalentar la inhabilitación o manipulación.

5.2.2 Sensores de apertura

Un sensor de apertura es un detector asociado a una parte móvil, como una puerta o una ventana, que genera una condición de alarma cuando se abre. Hay dos clases de sensores de apertura en uso corriente: el microinterruptor ("microswitch"), que se activa mecánicamente y el interruptor de lengüeta ("reed switch"), que se activa magnéticamente. Se puede usar otro tipo de interruptores o sensores de apertura. Un sensor de apertura debe operar de manera tal que se genere una condición de alarma cuando se abre la parte móvil en funcionamiento normal antes de que se produzca una separación libre máxima de 100 mm de ancho.

Los sensores de apertura pueden estar montados en superficies o embutidos, pero debe utilizarse un sensor de apertura oculto, siempre que sea posible. Cualquiera sea el tipo utilizado, el dispositivo y sus conexiones no deben ser accesibles desde el lado menos seguro de la parte móvil. Al ser instalado, no debe resultar posible determinar visualmente la conexión del cableado del dispositivo.

Deben tomarse precauciones para protegerlos de la manipulación desde el lado menos seguro de la parte móvil. Existen sensores de apertura que proporcionan una seguridad adicional contra determinados métodos de manipulación.

Los sensores de apertura deben usarse solamente cuando la parte móvil en cuestión es capaz de mantenerse firmemente en la posición requerida por medios mecánicos y los marcos deben estar firmemente fijados a la estructura circundante.

Cuando la puerta o ventana que se debe proteger tenga más de una parte móvil, cada parte móvil debe estar protegida en la misma manera que una parte móvil única.

Se debe tener cuidado en la aplicación de los interruptores de lengüeta magnéticos a aceros o puertas laminadas en acero para asegurar que el metal no afecte negativamente el campo del magneto asociado.

Cuando las partes móviles se encuentran cerradas y puedan tener alguna oscilación, ningún movimiento permitido por los dispositivos de seguridad mecánicos podrá dar lugar a una condición de alarma.

LEONID LLONTOP CASTRO
 Jefe de Seguridad Casa Matriz
 Banco Ciudad Bs. As

5.2.3 Detectores de vibraciones

Un detector de vibraciones es un dispositivo que genera una condición de alarma en respuesta a la vibración resultante de un ataque físico sobre la estructura a la que está adosado. Estos detectores detectan vibraciones estructurales de sus soportes y deben estar adosados en forma segura y/o agregados mecánicamente a la estructura que protegen. Su uso

debe estar restringido a los materiales que tienen buena transmisión mecánica, por ejemplo, ladrillo, hormigón, metal. No se debe instalar un detector de vibración a ninguna puerta que esté sujeta a un uso intenso que pueda causar un daño mecánico al dispositivo, a la conexión y/o generar falsas alarmas.

Las vibraciones del ambiente, tanto internas como externas, se deben evaluar antes de la instalación y se debe tener cuidado de ajustar el detector a la sensibilidad adecuada. Los ambientes expuestos a vibraciones intensas, por ejemplo, debidas a procesos industriales en instalaciones vecinas o rutas adyacentes o tráfico sobre rieles, pueden ser inadecuados para esta forma de protección. Particularmente, la aplicación directa en techos, ascensores, ventanas, puertas accesibles, superficies o uniones que puedan expandirse o contraerse cuando se exponen a la luz solar o al cambio de temperatura, podrían ser una fuente de falsas alarmas.

Las irregularidades tales como grietas, vigas, pilares y la interfaz entre distintos modos de construcción pueden interferir con la transmisión de la vibración. A fin de mejorar la eficiencia de la instalación en la reacción a un ataque a un determinado punto sobre una estructura sujeta a propiedades de transmisión irregulares, los detectores deben ser alojados en cajas de metal interconectadas mediante conductos metálicos. Las cajas deben estar firmemente fijadas a la estructura y las cajas y los conductos deben estar acoplados mediante una conexión conductora de vibraciones. Asimismo, el conducto debe estar adosado a la estructura a intervalos regulares, por ejemplo, 1 m.

El detector será capaz de discriminar entre las señales características de las condiciones ambientales normales y aquellas características de un ataque a la instalación protegida y de señalar una condición de alarma a la unidad central de alarmas. En el caso de utilizar un tipo de detector constituido por un procesador y varios sensores, el procesador puede recibir entradas desde uno o más sensores de vibración, hasta un máximo de 10 sensores, y cada procesador con su sensor asociado constituye un detector. Para obtener tanto una uniformidad de la sensibilidad como una discriminación confiable, puede ser necesario utilizar una cierta cantidad de procesadores separados con regulaciones de sensibilidad para las distintas estructuras a proteger. La regulación para un detector de vibración ajustable debe registrarse en el registro del sistema, en forma gráfica si fuera necesario.

El procesador puede estar incorporado a la unidad central de alarmas, puede estar construido dentro de una unidad individual incorporando también un sensor o puede estar ubicado en forma separada. Las unidades individuales que contienen un sensor y un procesador y que tienen un medio de ajustar la respuesta al ataque, requieren una regulación individual durante la instalación; ello es para compensar las características diferentes de las superficies protegidas. En cada caso, cada procesador debe tener una indicación del ajuste de sensibilidad de cada condición de alarma o de una condición de alarma simulada producida para ensayos de mantenimiento.

LEONID LLONTOP CASTRO
Jefe de Seguridad Casa Matriz
Banco Ciudad Bs. As.

5.2.4 Detectores de rotura de vidrio

Un detector de rotura de vidrio es un dispositivo que genera una condición de alarma en respuesta a un ataque físico sobre el vidrio.

Hay dos tipos de dispositivos en uso, el que se adosa a la superficie del vidrio y el que está separado de la superficie del vidrio (usualmente denominado "ambiental").

Algunos detectores pueden generar una condición de alarma cuando se encuentran expuestos a una de las condiciones siguientes:

- a) Vibración ambiental.
- b) Movimiento del vidrio con daños existentes, por ejemplo, grietas o astillado.
- c) Impacto o abrasión que no resulte en un daño real

- d) Fuentes de ruidos tales como frenos de vehículos, aspiradoras mecánicas, timbres, aviones, etc.

Dichos dispositivos no deben emplearse donde pudieran existir esas condiciones.

Es esencial que se sigan las especificaciones del fabricante respecto de la ubicación, el montaje y el suministro de energía, dado que la capacidad del dispositivo para desempeñarse correctamente en la totalidad del área prevista para ser protegida depende muy probablemente de su estricta observación. El desempeño del dispositivo puede variar entre vidrios de distinta fabricación o especificaciones. Se debe observar que estos detectores están generalmente diseñados para proteger solamente de ataques al vidrio y que el desplazamiento de una parte móvil, por ejemplo, la abertura de la ventana de una vitrina, no será detectada.

El área a la cual se aplicará el dispositivo adosado al vidrio debe ser limpiada en su totalidad, utilizando un agente limpiador adecuado, generalmente alcoholes metílicos. Se debe tener cuidado en asegurar que el agente no constituya un peligro para la salud y la seguridad en el ambiente. Se debe dejar secar el agente limpiador y luego se debe pulir el área con un paño seco, libre de pelusas. El dispositivo debe mantenerse en el lugar mediante un adhesivo rígido; no se recomiendan los dispositivos autoadhesivos. La conexión al dispositivo debe fijarse firmemente.

Cuando se utiliza un dispositivo que va separado del vidrio ("ambiental"), es fundamental no colocar nada entre un dispositivo separado y el vidrio, dado que estos dispositivos están generalmente diseñados para funcionar solamente con un sendero acústico libre de obstrucciones entre ellos y el vidrio. La introducción de materiales absorbente de sonidos en el ambiente o la aplicación de una película solar en el vidrio también alteran el comportamiento del detector.

El detector será capaz de discriminar entre las señales características de las condiciones ambientales normales y aquellas características de un ataque al vidrio y de señalar una condición de alarma a la unidad central de alarmas. En el caso de utilizar un tipo de detector constituido por un procesador y varios sensores, el procesador puede recibir entradas desde uno o más sensores de vibración, hasta un máximo de 10 sensores, y cada procesador con su sensor asociado constituye un detector. Un procesador puede estar incorporado a la unidad central de alarmas, puede estar construido dentro de una única unidad incorporando también un sensor o puede estar ubicado en forma separada. En cada caso, cada procesador debe tener una indicación del ajuste de sensibilidad de cualquier condición de alarma o de una condición de alarma simulada producida para ensayos de mantenimiento.

5.2.5 Alfombras detectoras de presión

Una alfombra detectora de presión es un dispositivo que tiene la estructura de una alfombra y que genera una condición de alarma cuando recibe el peso de una persona.

Las alfombras detectoras de presión se fabrican según diferentes especificaciones y se debe tener cuidado en la selección para asegurar que la durabilidad y la confiabilidad son las requeridas para la ubicación prevista.

La empresa de alarmas, alertará al usuario de prestar atención de no colocar objetos sobre la alfombra detectora de presión en todo momento.

Las alfombras detectoras de presión deben estar estratégicamente ubicadas donde:

- a) El nivel esperado de tránsito de personas no sea tal que produzca un desgaste excesivo.
- b) La ubicación no esté sujeta a condiciones de humedad o inundaciones.

c) La superficie sea firme, regular, lisa y limpia.

La alfombra detectora de presión debe estar asegurada a la superficie para evitar que se mueva de la posición en la que fue instalada y debe estar cubierta por un material que proporcione una protección adecuada contra daños accidentales, desgaste y roturas. En el momento de la instalación puede no ser posible distinguir el contorno de la alfombra detectora de presión. Si la cubierta es tal que en el transcurso del tiempo el perfil puede verse claramente, el valor de la seguridad del detector se reduce considerablemente.

5.2.6 Barreras infrarrojas

Un detector de interrupción de haz infrarrojo activo es un dispositivo que genera una condición de alarma cuando se interrumpe completamente un haz de radiación infrarroja entre un transmisor y un receptor, en contenedores separados. El detector sólo proporciona una protección en la línea de la visual entre el transmisor y el receptor y los intrusos que pasan por encima o por debajo del rayo no son detectados. Si se desea una detección lineal mejorada, se pueden instalar haces adicionales, uno encima del otro, cuidando que los emisores de cada segmento no incidan sobre los receptores de los otros. La protección es más eficaz cuando las unidades están ocultas o camufladas. Los detectores de este tipo deben utilizarse solamente dentro de lo especificado por el fabricante, con la frecuencia del haz fuera de la parte visible del espectro.

El transmisor y el receptor deben estar adosados a superficies rígidas, por ejemplo, ladrillos, bloques, hormigón y acero estructural, de manera tal de asegurar una alineación correcta. No se aconseja el uso de espejos para redirigir el haz, ya que proyectar el haz a través de material vidriado afecta la intensidad y la dirección del haz. Se debe establecer la alineación correcta durante la instalación y la rutina de mantenimiento con un atenuador o instrumento adecuado.

Deben tomarse precauciones respecto de las aplicaciones en áreas tales como corredores o pasillos, donde la radiación multivía reflejada podría entregar suficiente radiación al receptor para evitar una condición de alarma, aún donde el haz directo está completamente obstruido.

Las unidades de transmisores y receptores deben estar cuidadosamente ubicadas para asegurar que la luz solar u otras fuentes extrañas de luz intensa, por ejemplo, luces de faros de vehículos, no incidan sobre la cara de las unidades. Se debe prestar especial atención al ángulo de cambio del sol en el transcurso del año, y se debe añadir algún tipo de protección contra fuentes externas de luz al equipo si se anticipan o experimentan problemas de luz solar.

La distancia entre las unidades transmisoras y receptoras no debe exceder la recomendada por el fabricante y se debe considerar debidamente la visibilidad defectuosa, tal como la causada por la humedad elevada, las partículas de polvo, etc. En tales casos, será necesario utilizar el detector a menos de la separación máxima recomendada por el fabricante.

Cuando sea necesario, por ejemplo cuando transiten camiones o carros, el equipo debe ser provisto de una protección física adecuada para reducir el riesgo de daños y/o desalineación. En instalaciones de múltiples haces, se debe tener cuidado al ubicar los haces para asegurar que un receptor reaccione solamente ante el transmisor previsto.

Cuando se desee conectar dos detectores en un circuito eléctricamente paralelo, dada la presencia de riesgos de falsa alarma producidos por animales o pájaros, para que se genere la condición de alarma ambos haces deben estar simultáneamente interrumpidos y cada haz debe reajustarse desde una condición activada antes de que la condición de alarma se genere. Los ejes de los haces no deben estar separados en más de 500 mm.

Son también de utilización frecuente para instalaciones externas, barreras con haces múltiples.

5.2.7 Detectores de Movimiento

5.2.7.1 Generalidades

A los fines de este código de práctica, los detectores de efecto Doppler ultrasónicos, de microondas y los detectores infrarrojo pasivos se consideran en conjunto con el nombre de detectores de movimiento. Los detectores de efecto Doppler ultrasónicos y de microondas montados en paredes, son más sensibles a los movimientos radiales con respecto al detector, y los detectores de infrarrojo pasivos son más sensibles a movimientos transversales a sus radios de cobertura. Este apartado da recomendaciones comunes a los tres tipos de detectores y los apartados 5.2.7.2 a 5.2.7.4 dan recomendaciones específicas para cada tipo.

El patrón de protección de este tipo de detector está afectado por la manera en que los objetos están dispuestos o se mueven.

Cuando se instala un detector de movimiento, se debe prestar particular atención a las instrucciones del fabricante respecto a la ubicación, el montaje y el suministro de energía.

El detector debe estar asegurado y fijado a una superficie sólida y libre de vibraciones en una posición tal que su obstrucción no sea posible. Se debe tener cuidado en asegurar que dentro del campo de visión inmediato no haya objetos que puedan moverse o sobre los cuales puedan moverse pájaros o insectos durante el período de activación, a menos que pueda verificarse que cualquier movimiento de este tipo no generará una condición de alarma.

Ejemplos de fenómenos que pueden causar falsas alarmas con los detectores de movimiento son los movimientos continuos o intermitentes tales como aquellos asociados con máquinas automáticas, péndulos de relojes, animales, incluyendo peceras, aspas de ventiladores, láminas de tejados inseguras, persianas o cortinas y carteles o lámparas colgantes que puedan ser movidas por ráfagas de aire o calentadores. Asimismo, se deben considerar los posibles efectos del asentamiento de objetos apilados, y los movimientos de persianas, puertas, etc.

Debe existir un indicador de detección que pueda ser deshabilitado y cuya indicación será una representación del estado de detección.

Si la sensibilidad del detector es ajustable, debe ajustarse al mínimo nivel acorde a la cobertura requerida.

Cuando, debido a la presencia de riesgos de falsas alarmas, se desee conectar dos detectores en un circuito eléctricamente paralelo, ambos detectores deben estar en condición de alarma en forma simultánea, para que se pueda generar la condición de alarma.

5.2.7.2 Detectores de efecto Doppler ultrasónico

Un detector de efecto Doppler ultrasónico es un dispositivo que genera una condición de alarma en respuesta al efecto Doppler producido en la reflexión de ondas ultrasónicas provenientes de un objeto en movimiento. La mayoría de los detectores de efecto Doppler ultrasónico funcionan a una frecuencia de entre 19 kHz y 40 kHz; las frecuencias superiores a 19 kHz se consideran inaudibles para el oído humano y se definen como ultrasónicas.

Las ondas ultrasónicas no penetran la mayoría de los tipos de estructuras, puertas o ventanas, pero se reflejan dependiendo de la absorción acústica de una habitación y su contenido. Un transmisor irradia ondas ultrasónicas que llenan el área o volumen donde se requiere detección, y la radiación reflejada por las paredes, el cielo raso, el piso y los objetos que se encuentran en el área, es recibida y analizada por un procesador. Si la frecuencia reflejada es la misma que la del transmisor, no debe producirse una alarma. Cuando hay un movimiento en la habitación o su contenido que produce un cambio de frecuencia, debe generarse una condición de alarma.

Se debe tener cuidado al seleccionar y ubicar un detector de efecto Doppler ultrasónico. Las ondas irradiadas pueden ser reflejadas por los objetos sólidos, por lo tanto es importante asegurar que el mobiliario y otras disposiciones no impidan que el detector cubra el área requerida. La forma y la longitud del patrón de protección están determinadas por el tipo del detector utilizado. El detector de efecto Doppler ultrasónico estándar emitirá un patrón de señal oval, pero los deflectores y la estructura de una habitación, sus revestimientos y contenido pueden modificar el patrón. Los detectores de efecto Doppler ultrasónico pueden estar montados en una pared o el cielo raso y se deben seguir las instrucciones del fabricante respecto de la altura de montaje desde el nivel del suelo para asegurar la máxima eficacia.

Se debe tener cuidado al ubicar varios detectores para asegurar que no se interfieran entre sí; las recomendaciones del fabricante son lo más importante en este respecto. En instalaciones de varios detectores, el detector de efecto Doppler ultrasónico puede recibir no solamente la radiación reflejada de su propio transmisor, sino también la radiación de los otros detectores que se encuentran en el área.

El ruido ultrasónico creado por otras fuentes puede afectar a los detectores y en este caso podría limitarse la cantidad de detectores a una menor que la recomendada por el fabricante.

Una fuente de sonido dentro del rango audible, como la campanilla de un teléfono, puede tener un contenido ultrasónico que puede causar el mal funcionamiento de esta clase de detector. Antes de instalar un detector de efecto Doppler ultrasónico, deben realizarse ensayos para asegurar que no hay un nivel inaceptable de ruido ultrasónico causado por el siseo de tubos de vapor, pérdidas de tubos de aire, campanillas de teléfonos, etc.

El desempeño de un detector de efecto Doppler ultrasónico puede ser afectado también por el movimiento de aire causado por sistemas de aire forzados, ráfagas producidas por movimientos de puertas y ventanas y corrientes de aire termales provenientes de otras fuentes de calor. La radiación ultrasónica es afectada por cambios en la humedad y se debe tener cuidado de asegurar que la gama prevista de humedad relativa no pueda afectar negativamente el desempeño del detector.

LEONID LLONTOP CASTRO
Jefe de Seguridad Casa Matriz
Banco Ciudad Bs. As

5.2.7.3 Detectores Doppler de microondas

Un detector Doppler de microondas es un dispositivo que genera una condición de alarma en respuesta al efecto Doppler producido por la reflexión de ondas de radio provenientes de un objeto en movimiento. El metal, el hormigón y las paredes de ladrillo macizo de 30 cm de ancho constituyen una pantalla efectiva para las frecuencias de banda X y superiores, pero puede haber una penetración considerable a través de bloques de cemento o de hormigón alveolar, paredes de ladrillos simples, materiales vidriados, puertas de madera y techados no metálicos. El movimiento de líquido en tubos de plásticos, asbesto u otro material no metálico, puede crear problemas.

Un detector Doppler de microondas no debe ser dirigido hacia el perímetro que no sea una pantalla de microondas eficaz, excepto cuando las condiciones del área a proteger no lo permitan.

Un detector Doppler de microondas no debe ser dirigido hacia superficies altamente reflectantes, como metal, espejos o botellas de líquidos, si esto pudiera hacer que la radiación se reflejara a través de materiales vidriados o de construcción permeable que recojan movimientos fuera del perímetro, o si el detector pudiera ser afectado por reflejos generando falsas alarmas.

Los detectores deben estar diseñados y/o ubicados de modo tal que eviten la interferencia indebida de lámparas fluorescentes, y deben ser sometidos a ensayos de interferencias causadas por las lámparas al ser encendidas o apagadas o por las lámparas que permanecen encendidas.

La interferencia, que puede activar el dispositivo de detección, puede ser generada por fuentes tales como señales de radio, chispas eléctricas y conductores aéreos de alta tensión.

Deben realizarse mediciones previas de las condiciones de ruido ambiental en el entorno. El nivel de la señal de ruido ambiental no debe exceder de 20 dB del nivel del umbral de detección del dispositivo detector, a menos que el detector tenga dispositivos de procesamiento diseñados para proporcionar el desempeño equivalente con una relación de señal-ruido más baja

Si se instalan dos o más detectores de microondas para cubrir un área extensa, es importante asegurar que no se interfieran entre sí.

Si el dispositivo cuenta con una regulación o un ajuste, éste debe regularse al mínimo posible para evitar falsas alarmas.

LEONID LLONTOP CASTRO
Jefe de Seguridad Caso Matriz
Banco Ciudad Bs. As

5.2.7.4 Detectores infrarrojos pasivos

Un detector infrarrojo pasivo es un dispositivo que genera una condición de alarma en respuesta a cambios significativos en el nivel de la energía infrarroja irradiada por objetos que se encuentran dentro de su campo visual. Existe una amplia variedad de detectores infrarrojos pasivos que ofrecen distintos patrones de cobertura, como ángulo amplio, cortina, o de largo alcance. Se debe tener cuidado al seleccionar y ubicar un dispositivo, dado que pueden generar falsas alarmas o situaciones de no detección si no se consideran debidamente los límites ambientales.

Los detectores infrarrojos pasivos funcionan al detectar un cambio de temperatura dentro de su patrón de detección. Se debe seleccionar el detector de manera que tenga una especificación de temperatura apropiada al ambiente en que funcionan. Se deben seguir las recomendaciones del fabricante sobre la altura de instalación, y los detectores deben ser ubicados de modo que la dirección prevista del movimiento de un intruso sea en ángulo recto respecto a los haces de detección. No debe haber objetos que puedan cambiar la temperatura durante el período de protección, por ejemplo, lámparas eléctricas, calentadores, máquinas de café, radiadores, congeladores, etc., dentro de la zona de cobertura.

Los detectores infrarrojos pasivos no deben estar instalados donde puedan ser influidos por corrientes de aire, soplos de aire caliente o luz solar directa, y no deben apuntar a las ventanas o puertas.

NOTA. Si bien un detector no detectará movimientos a través de vidrios, el sol puede producir un efecto de calentamiento, lo que puede provocar que el dispositivo no funcione apropiadamente.

Los detectores infrarrojos pasivos deben ser sometidos al "ensayo de caminata" para identificar todas las zonas de detección y asegurar que se logra la cobertura deseada.

Se puede utilizar una cantidad cualquiera de detectores infrarrojos pasivos en una misma habitación o un mismo edificio sin riesgo de interferencia entre sí.

El indicador luminoso de prueba ("led") solo estará habilitado durante el ensayo de caminata.

5.2.7.5 Dispositivos de tecnologías múltiples

Los detectores de tecnologías múltiples pueden incluir dos o más tecnologías de detección (ejemplo: infrarrojos pasivos y microondas) La utilización de este tipo de dispositivos tiende a disminuir las falsas alarmas, siempre que las diferentes tecnologías de detección se utilicen en forma simultánea.

Como son susceptibles a diferentes influencias, se debe prestar consideración a cualquiera que podría afectar a las características de funcionamiento del detector en su conjunto. A continuación se incluyen ejemplos de otros aspectos a considerar:

- a) Todos los factores que corresponden a cada tecnología individual.
- b) Instalaciones de ensayo independientes para cada tecnología.
- c) Consideración de los patrones de detección de ambas tecnologías o de todas ellas para asegurarse de que se logra un patrón de detección común.

5.2.8 Dispositivos de activación deliberada

Un dispositivo de activación deliberada es un dispositivo que permite al usuario crear deliberadamente una condición de alarma en el caso de una emergencia.

NOTA. No se excluyen otros tipos de dispositivos, siempre que cumplan con estas recomendaciones y que su uso sea acordado entre el usuario y la empresa de alarmas.

Los dispositivos de activación deliberada deben ubicarse de manera que permiten su operación sin necesidad de movimientos obvios, pero en una posición tal que se evite su activación accidental. Cuando sea posible, la parte operativa del dispositivo de activación deliberada debe estar bajo nivel con respecto de la superficie de su gabinete.

Se debe tener cuidado al seleccionar y ubicar estos dispositivos para evitar la posible confusión entre el dispositivo y los interruptores cercanos o adyacentes utilizados para otros propósitos.

LEONID LLONTOP CASTRO

Jefe de Seguridad Casa Matriz

Banco Ciudad Bs. As.

NOTAS:

- La empresa de alarmas debe asegurar que todos los usuarios potenciales conozcan la ubicación de los dispositivos de activación deliberada y que se realicen revisiones regulares para confirmar que los dispositivos están ubicados en la posición más conveniente.
- Si un dispositivo de activación deliberada ya no fuera necesario, debe ser retirado del lugar. Antes de que el área que posee un dispositivo de activación deliberada sea reorganizada, se debe desconectar el dispositivo para prevenir falsas alarmas.

Los cables de conexión añadidos a objetos móviles deben tener la flexibilidad suficiente como para prevenir daños durante la limpieza, etc.

Los dispositivos de activación deliberada no deben estar ubicados en áreas utilizadas por el público general, y cuando estén instalados en dependencias residenciales deben estar ubicados lejos del alcance de los niños.

Si un sistema incluye una cierta cantidad de dispositivos de activación deliberada, debe tenerse en cuenta la división del sistema en zonas para permitir la fácil identificación del lugar de procedencia de la señal de alarma y la localización de fallas. Esto es particularmente importante para instalaciones en ambientes de múltiples pisos u oficinas, donde puede ser necesario que la persona que se encuentra en el centro de control a distancia indique a la autoridad competente la zona en la cual se ha activado un dispositivo.

Se deben proporcionar los medios para permitir los ensayos individuales de los dispositivos de activación deliberada sin activar los dispositivos de aviso a la autoridad competente.

Todo dispositivo de activación deliberada debe indicar en forma inequívoca cual fue el dispositivo accionado

En la etapa de diseño del sistema, la empresa de alarmas debe asesorar al usuario que existe la opción de activar un dispositivo de aviso audible en el lugar y/o utilizar solamente señalización remota silenciosa a la autoridad competente local o a una estación central.

Cuando un dispositivo de activación deliberada genera una condición de alarma que debe ser señalizada a una estación receptora, la señal debe ser reconocible como proveniente de un dispositivo de activación deliberada.

5.2.9 Cableado continuo

El cableado continuo es un método de detección que produce una condición de alarma cuando se modifican o alteran las condiciones de continuidad o instalación.

Se consideran los aspectos siguientes:

- a) Configuración del cableado para detectar el método de intrusión anticipada. Ejemplo: un acceso de mano por hueco o acceso total.
- b) Asegurar la unión y el diseño para impedir la retirada del cable de detección sin activación. Ejemplo: el uso de bucles de anclaje.
- c) Instalación sólo sobre una superficie adecuada que no pueda dañar al cableado.
- d) Emplazamiento del cableado de detección sólo dentro de las instalaciones supervisadas.
- e) Consideración de las condiciones ambientales.
- f) Protección contra daños accidentales. Ejemplo: cables blindados contra daños físicos.
- g) Configuración para detectar una rotura o cortocircuito.
- h) Supervisión continua para la detección precoz de fallas.
- i) Unión a superficies de una manera que evite el estiramiento.

5.2.10 Dispositivo para Alambre tenso

Este dispositivo de detección genera una condición de alarma cuando se modifican o alteran las condiciones físicas (tensión mecánica) de un alambre tenso.

Se consideran los aspectos siguientes:

- a) Cambios de temperatura y humedad.
- b) Instalación dentro de las instalaciones supervisadas;
- c) Configuración para detectar el método de intrusión anticipada.

5.3 Unidad central de alarma

LEONID LLONTOP CASTRO
Jefe de Seguridad Casa Matriz
Banco Ciudad Bs As

5.3.1 Generalidades

Este equipo procesa las señales de salida de uno o de varios detectores para determinar si el estado de alarma debe ser generado. La unidad central de alarma debe proporcionar también los medios para permitir el ensayo del sistema de alarma.

La unidad central de alarma comprende un panel principal y dispositivos relacionados con la operación de este panel, denominados de ahora en más "dispositivos de operación" (por Ej.: teclado, cerraduras codificadas de conmutación, lectores de tarjetas de control de acceso, control remoto codificado, etc.)

Es conveniente que el panel principal esté accesible y oculto, mientras que los dispositivos de operación estén separados del panel, accesibles y visibles al operador y que contengan elementos de señalización.

Los dispositivos de operación de la unidad central de alarma deben proveer métodos seguros para el comando del panel central como ser: la operación de un teclado, una llave de conmutación, la combinación de estos dos u otro método de similar seguridad.

La unidad central de alarma estará montada sobre una superficie fija, libre de vibraciones con tornillos de una longitud y un diámetro acordes con el peso y el uso. La entrada de los cables y los conductores de alimentación a la red deben cumplir con lo establecido en la Reglamentación para Instalaciones Eléctricas en Inmuebles.

Es importante también tener en cuenta los aspectos relevados según 4.3.

5.3.2 Indicadores

En el caso de una unidad central de alarma con dispositivos de operación separados del panel principal, los indicadores estarán en los dispositivos de operación.

La indicación de que la unidad está efectivamente alimentada por la red de alimentación principal o no debe ser claramente visible en el panel de señalización y control.

La unidad central de alarma debe indicar, en forma visual y auditiva, el estado eléctrico de las zonas de detección en el momento de la activación.

En una condición de alarma, la unidad central de alarma debe indicar, en el momento de completar el procedimiento de desactivación, el detector o la zona de los detectores responsables de la condición de alarma.

No debería ser posible retirar esa indicación hasta que el sistema de alarma haya sido desactivado y activado nuevamente por la persona autorizada (ver 5.4.3), especialmente en casos de señalización remota a centros de control a distancia.

5.3.3 Activación y desactivación

No debería ser posible realizar el procedimiento de activación si una zona de detección se encuentra en condiciones de falla o detección, a menos que esa zona estuviera anulada.

La posibilidad de activar el sistema con alguna zona en circuito abierto ("activación forzada" o "armado forzado") debe restringirse a casos excepcionales y no permanentes.

Es conveniente que no se genere una condición de alarma durante los procesos de activación y desactivación (tiempos de entrada y salida). Ello no se contrapone con el uso de "zonas 24 h" que no están involucrados en el procedimiento normal de activación.

Debe existir una indicación, auditiva y visual, que evidencie que la activación o el desactivado se ha completado satisfactoriamente.

5.4 Dispositivos de Advertencia

5.4.1 Alarmas audibles

LEONID LLONTOP CASTRO
Jefe de Seguridad Casa Matriz
Banco Ciudad Bs As

El sistema de alarma debe contar por lo menos con un dispositivo de advertencia

Se recomienda la utilización de un dispositivo de advertencia interno y otro externo. En caso de utilizar sólo uno, este debe ser el interno.

Es recomendable que los dispositivos de advertencia audibles, cuando haya más de uno, no estén conectados en la misma alimentación ya que en caso de sabotaje de alguno de ellos, podrían quedar todos inutilizados.

LEONID LLONTOP CASTRÓ
Jefe de Seguridad Casa Matriz
Banco Ciudad Bs. As.

5.4.1.1 Alarmas audibles externas

Cuando sea aplicable, el dispositivo de advertencia audible externo se ubicará preferentemente en un lugar fuera del alcance normal y en una posición que implique riesgos mínimos de daños accidentales o intencionales a los dispositivos o las conexiones, con razonable acceso para el mantenimiento y de manera de proporcionar una respuesta eficaz. El cable de conexión de las alarmas auditivas debe estar protegido para asegurar que no se produzcan daños mecánicos accidentales o intencionales.

Se debe fijar firmemente una alarma audible externa a la estructura del edificio y los métodos aceptables típicos para ello son los siguientes:

- a) Para una pared de ladrillos: un mínimo de tres tornillos de acero N° 10 que penetren el ladrillo (no el mortero, la mezcla de cemento o el revoque) al menos 40 mm y atornillados en huecos adecuados.
- b) Para recubrimientos delgados y metal o revestidos en madera: tornillos que penetren el material con una placa posterior.

El alojamiento debe ofrecer la mayor resistencia al uso de cuerdas, cadenas, ganchos o cables, etc., adosados con el fin de retirarlo de sus cimientos. Ninguna interferencia eléctrica generada por un dispositivo de advertencia audible debe afectar a otras partes del sistema ni contravenir los reglamentos respecto de radio interferencia.

En cada caso, referirse a las reglamentaciones legales vigentes aplicables a cada jurisdicción referidas al nivel de ruido y al tiempo de emisión de las alarmas externas audibles permitidos.

NOTA. Se sugieren tiempos de sonoridad de las alarmas externas de 2 a 4 minutos en zonas urbanizadas

El dispositivo de advertencia audible debe contar siempre con una detección de sabotaje

5.4.1.2 Alarmas audibles internas

Es conveniente que un dispositivo de alarma audible interna esté ubicado de modo que dé el máximo efecto dentro de las zonas protegidas. Siempre que sea necesario, el cable conectado al dispositivo debe estar protegido contra los daños mecánicos.

El dispositivo se debe montar en su posición con tornillos de dimensiones adecuadas para evitar que se afloje en funcionamiento normal.

El dispositivo de advertencia audible interno instalado en un lugar de acceso al público debe contar con una detección de sabotaje.

5.4.2 Sistema de transmisión de alarmas - Dispositivos de señalización remota

La señalización puede lograrse mediante equipos de discado automático, comunicadores digitales, y/o sistemas inalámbricos y equipos de comunicación mediante líneas físicas directas o una combinación de los citados medios.

Es conveniente que los equipos estén ubicados dentro del área protegida. Cuando este equipo está separado de la unidad central de alarmas, es conveniente que su contenedor esté firmemente asegurado a la estructura del edificio.

El sistema de comunicación debe estar supervisado y en caso de interrupción (ej.: corte de línea telefónica terrestre) o sabotaje, se debe generar una señalización al menos en el panel de control y señalización y opcionalmente producirse una conmutación automática a otro medio de comunicación para enviar la información a quien corresponda.

En el caso de utilizarse comunicadores digitales, el par telefónico debe estar conectado de forma tal que la unidad de procesamiento tenga prioridad de uso del servicio telefónico.

5.5 Cableado de interconexión

LEONID LLONTOP CASTRO
Jefe de Seguridad Casa Matriz
Banco Ciudad Bs As.

5.5.1 Selección y ubicación

Todos los cableados de interconexión, empalmes e interconexiones flexibles deben cumplir los requisitos de la "Reglamentación para la Ejecución de Instalaciones Eléctricas en Inmuebles" de la Asociación Electrotécnica Argentina.

Se debe tener cuidado en asegurar que todos los conductores estén dimensionados para la corriente y la tensión requeridas y que tengan una resistencia suficientemente baja para asegurar que la caída de tensión no resulte en una tensión inferior a la especificada por el fabricante para cada dispositivo.

Se debe tener cuidado de que los cables se instalen tan lejos como sea posible de la influencia de otros cables, especialmente cuando estos últimos están a altas tensiones o conducen altas corrientes. Si es probable cualquier interferencia eléctrica, incluida la de radio, es conveniente que los cables estén protegidos mediante blindaje o pantalla, o que se tomen otras medidas para reducir los efectos de dicha interferencia (ver 5.5.2).

Es conveniente que el cableado de interconexión esté dispuesto de manera que no pueda ser alcanzado o manipulado por ninguna persona fuera del área protegida sin la operación de un detector y la subsiguiente generación de una condición de alarma.

Es conveniente que los cables se instalen de manera que exista el mínimo riesgo de un daño físico. Cuando un cable esté instalado bajo recubrimientos de pisos (alfombra, piso flexible, etc.) es conveniente que esté paralelo y adyacente a las paredes y no atraviese habitaciones ni aberturas, a menos que se utilice correctamente una franja umbral de alfombra para proteger el cable. Si existe riesgo de daños físicos, es conveniente proteger el cable mediante ductos, canalizaciones, y en caso que éstos fueran de un material conductor debe tenerse especial cuidado en su puesta a tierra, por razones de seguridad, y que ésta conexión a tierra se realice en un único punto, a fin de evitar interferencias eléctricas. En determinadas circunstancias puede ser necesario usar material no conductor, o aislar los ductos, las canalizaciones o los conductos de las partes circundantes del edificio. Ésta aislación puede lograrse utilizando abrazaderas no conductoras o aislantes.

5.5.2 Puesta a tierra e interferencia eléctrica

La puesta a tierra de un sistema de alarma es esencial para asegurar la operación correcta del sistema. Debe cumplir con los requisitos de la IRAM 2281-5: "Código de práctica para puesta a tierra de sistemas eléctricos. Puesta a tierra de sistemas de telecomunicaciones (telefonía, telemedición y equipos de procesamiento de datos)".

Existen generalmente dos razones para la puesta a tierra: la primera es la de prevenir lesiones a seres vivos o daños en el caso que cualquier parte conductora del sistema quede bajo tensión, y en segundo lugar, eliminar la interferencia eléctrica.

A los propósitos de la seguridad, normalmente es suficiente asegurar que todos los equipos conectados a la red de alimentación estén conectados a la tierra principal.

La interferencia eléctrica, provocada por una o más de las siguientes causas puede crear falsas alarmas:

- a) Fuga de corriente de red de alimentación al circuito de muy baja tensión.
- b) Inducción.
- c) Radiofrecuencia.
- d) Descargas eléctricas atmosféricas.

Éstas pueden generalmente solucionarse mediante:

- 1) Colocación de filtros a la entrada de la alimentación de la red.
- 2) Separación de los cables de baja tensión de los de alta tensión.
- 3) Blindaje de los cables.

Actualmente no hay un método completamente eficaz para la protección contra descargas eléctricas atmosféricas

Cuando la longitud del blindaje sea eléctricamente continua, la puesta a tierra debe hacerse en un único punto.

5.6 Suministro de alimentación

LEONID LLONTOP CASTRO
Jefe de seguridad Casa Matriz
Banco Ciudad Bs. As

5.6.1 Equipo de alimentación

Estos requisitos se aplican a todos los equipos de alimentación (incluyendo aquellos montados como parte integral de cualquier unidad central de alarmas o detector) con la excepción de fuentes para alarmas externas audibles o equipos de discado automático y comunicadores digitales.

El equipo de alimentación debe cumplir con 5.6.2.1, 5.6.2.2 ó 5.6.2.3, según corresponda.

5.6.2 Tipos de equipos de alimentación

Las baterías que se utilicen, deben ser selladas o tales que no produzcan emanaciones que puedan afectar al medio ambiente o a los seres vivos.

5.6.2.1 Alimentación de red y de batería recargable de reserva

La alimentación será la de red conectada en forma permanente, no a través de una ficha y tomacorrientes, sino a través de un fusible o protección termomagnética adecuada.

Cualquier derivación del suministro de red destinada al sistema de alarmas, debe utilizarse únicamente para el uso del sistema de alarma.

Una batería recargable de reserva, con suficiente capacidad para 8 h de operación normal del sistema de alarma sin recargarse, complementará el equipo de alimentación del sistema.

La energía suministrada será suficiente para abastecer al sistema de alarma en estado normal (no disparado) y simultáneamente recargar la batería a la capacidad requerida dentro de las 24 h.

La batería de reserva entrará automáticamente en uso cuando la tensión de red caiga por debajo del nivel requerido para asegurar que la tensión de salida sea suficiente como para operar el sistema de alarma. El sistema tomará alimentación de la red nuevamente y la batería de reserva se recargará automáticamente, cuando la tensión de red se haya restablecido a su valor nominal.

Se marcará sobre la batería la fecha de su instalación.

En determinados casos, estos requisitos pueden ser considerados insuficientes en términos de la capacidad o las velocidades de recarga; en tales casos es conveniente proveer capacidad adicional.

NOTA. Se pueden hallar ejemplos de la necesidad de requerir una capacidad extra en las baterías de reserva cuando sea necesario realizar tareas de reparación o mantenimiento edilicio de partes del edificio no protegidas durante períodos de tiempo prolongados requiriéndose para ello carga extra de la batería.

5.6.2.2 Alimentación sólo con batería recargable

La batería recargable tendrá capacidad suficiente como para abastecer al sistema de alarma en operación normal, incluyendo 4 h en condición de alarma, para el período máximo esperado antes de la recarga.

Se marcará sobre la batería la fecha de su instalación.

5.6.3 Conexiones a las baterías y a las fuentes de alimentación

Las conexiones a la batería deben realizarse por medios compatibles con el diseño de las terminales de la batería, los cables de conexión y de la tensión y corriente utilizados.

Cuando se utilicen terminales atornillados se debe tener cuidado que estén suficientemente ajustados para asegurar conexiones buenas y resistentes a la corrosión, sin dañar ninguna parte de la batería o del cable. Los equipos de alimentación no deben normalmente encontrarse expuestos a condiciones corrosivas, pero si esto fuera inevitable, se deben tomar medidas para proteger las conexiones contra el ambiente corrosivo.

LEONID LLONTOP CASTRO
Jefe de Seguridad Casa Matriz
Banco Ciudad Bs. As.

5.6.4 Ubicación y alojamiento

El equipo de alimentación estará integrado en la unidad central de alarmas o en un contenedor separado ubicado dentro del local protegido. Esto no se aplica a equipos de alimentación utilizados únicamente para sensores, detectores o procesadores o sus circuitos. Las pilas utilizadas como fuentes para sensores, detectores o circuitos procesadores estarán alojadas en portapilas adecuados.

Las interconexiones entre la unidad central de alarmas y sus fuentes de alimentación separadas, deben protegerse mecánicamente.

Se recomienda que el equipo de alimentación esté ubicado en una posición que permita el fácil acceso para el mantenimiento, no sea estéticamente desagradable y no interfiera con la decoración. Es conveniente que esté situado de manera que no haya interferencia alguna con ninguna parte de los equipos vecinos.

Es conveniente considerar tanto los distintos métodos que pueden ser necesarios para la recarga de distintos tipos de baterías como el hecho de que el uso de un método equivocado puede dañar seriamente a la batería. Por lo tanto, los medios de carga de una batería deben cumplir con las instrucciones del fabricante.

5.6.5 Desempeño

La tensión suministrada por la fuente de alimentación debe ser:

- a) 12 Vc.c., ó
- b) Cuando la utilización de 12 Vc.c. sea impracticable, otra tensión menor o igual a 50 V. El desempeño de cualquier equipo de alimentación que utilice el suministro de la red, cumplirá con 5.6.2.1 bajo cualquier combinación de las condiciones siguientes:

- **Tensión de red:** $\pm 10\%$ del valor de alimentación nominal
- **Cambios instantáneos en la tensión de red:** Desde el valor de alimentación nominal más 10% a cero, y de cero al valor de la alimentación nominal más 10%
- **Frecuencia de red:** $\pm 4\%$ del valor de alimentación nominal
- **Temperatura ambiente:** -10°C a $+ 40^{\circ} \text{C}$

5.7 Verificación y entrega del sistema instalado

LEONID LIONTOP CASTRO
Jefe de Seguridad Casa Matriz
Banco Ciudad Bs As

5.7.1 Generalidades

En grandes instalaciones, es conveniente realizar inspecciones a intervalos regulares durante la instalación del sistema. La verificación y las inspecciones finales deben ser realizadas por el personal de la empresa de alarmas. Cuando sea posible, debe tratarse de personas distintas de las empleadas en la instalación.

5.7.2 Verificaciones

A todo el cableado de la instalación (continuo o interconectado) se le debe verificar su continuidad y las lecturas obtenidas de cada circuito deben ser registradas, in situ, en alguna planilla o cuaderno del sistema. La continuidad se verificará utilizando un instrumento adecuado ("tester", multímetro) con un valor de impedancia de entrada de por lo menos 20 k Ω por volt u otro equipo de ensayo adecuado.

La verificación de la aislación entre cada conductor y la tierra deben realizarse utilizando un medidor de aislación u otro equipo de ensayo adecuado. La resistencia de la aislación debe ser mayor que 1 M Ω .

Previamente a la realización de la verificación del cableado de la instalación, es esencial asegurar que no hay ningún equipo agregado al cableado, dado que los diodos, transistores,

4

circuitos integrados, etc., pueden ser dañados por el equipo de ensayo de aislación de alta tensión.

Las cajas de empalme utilizadas para empalmar los cables de interconexión deben ser inspeccionadas para asegurar que:

- a) La unión del cableado haya sido realizada mediante un método apropiado.
- b) Se mantengan los códigos de color en los cables de alimentación.
- c) Las tapas que sellan las cajas de empalme estén asegurados mediante la cantidad y el tamaño adecuados de tornillos.

Todo empalme que haya que realizar necesariamente fuera de las cajas de empalme (normalmente asociada con el cableado continuo) debe ser examinado para asegurar que los conductores estén apropiadamente retorcidos y soldados, y completamente encapsulados con material aislante.

La puesta a tierra de las fuentes de alimentación y los transformadores y/o rectificadores debe ser verificada de acuerdo con lo establecido en la "Reglamentación para la Ejecución de Instalaciones Eléctricas en Inmuebles" de la Asociación Electrotécnica Argentina. También debe verificarse que dicha puesta a tierra esté identificada con los colores verde y amarillo.

Se debe verificar la puesta a tierra de los dispositivos que la requieran, tales como comunicadores telefónicos, etc.

Se debe verificar las baterías para asegurar que:

- 1) Estén dispuestas de manera de facilitar el mantenimiento y no estén en posiciones poco adecuadas, por ejemplo, debajo de falsos cielorrasos, y que se cumpla con los requisitos de salud y seguridad para evitar daños a personas que se encuentren en las cercanías;
- 2) Estén completamente cargadas y en caso de ser recargables, que su capacidad de recarga sea satisfactoria.

Debe verificarse el desempeño de las baterías recargables con la alimentación de red desconectada, para asegurar que las cargas normales y las cargas en estado de alarma sean suficientes. Se debe verificar que la capacidad de la batería sea la adecuada de acuerdo a lo establecido en 5.6.2.1, 5.6.2.2 ó 5.6.2.3.

El equipo de carga debe ser verificado para asegurar que dará la salida requerida especificada por el fabricante de las baterías.

Todos los fusibles deben ser verificados para asegurar que sus especificaciones sean las adecuadas en todas las alimentaciones del sistema, incluyendo aquellas que alimentan a los dispositivos de detección. Se consultaran también las recomendaciones del fabricante.

La alimentación de red a cada unidad de alimentación en el sistema, se verificará para asegurar que se cumple con lo establecido en 5.6.2.1.

5.7.3 Verificaciones operacionales

EQNID LLONTOP CASTRO
Jefe de Seguridad Caso Matriz
Banco Ciudad Bs. As

5.7.3.1 Generalidades

Se verificarán todas las partes de un sistema que estén relacionadas con la operación correcta del sistema. Las verificaciones operacionales de un sistema deben incluir las verificaciones apropiadas para el sistema indicadas en 5.7.2. Es importante que el usuario esté

presente cuando se realizan las verificaciones operacionales. Igualmente, es importante que todos los usuarios finales potenciales del sistema se hallen también presentes.

5.7.3.2 Detectores y detección de desarme ("tamper detection")

Se verificará el correcto funcionamiento de cada detector del sistema para la correcta operación de acuerdo con los requisitos correspondientes de las IRAM 4254 y/o, IRAM 4172 según corresponda, y las recomendaciones del fabricante. Se operará cuando el sistema se encuentra activado.

Se verificará la correcta operación e indicación de la detección de desarme.

Se verificarán operativamente el correcto funcionamiento de todos los detectores instalados en el sistema con excepción de los que se destruyen cuando se produce la detección.

5.7.3.3 Suministros de energía

La alimentación de la red suministrada al sistema debe ser verificada para asegurar que proviene de un suministro permanentemente conectado y debe verificarse que las baterías estén completamente cargadas en el momento de la entrega.

Se verificará la salida de la tensión de la fuente de alimentación para asegurar que está dentro de la gama requerida y se registrará dicho valor.

Se medirá la tensión de operación en todos los dispositivos que requieren alimentación. Se debe asegurar que las tensiones de operación en esos dispositivos estén dentro de las especificaciones del fabricante y que los valores obtenidos sean registrados.

La corriente provista a los detectores de movimiento tales como Dopplers microondas, detectores de Doppler infrarrojos y ultrasónicos en una condición de activación, sin alarma, será medida y registrada.

Se desconectará la alimentación de red y se medirá la corriente y la tensión suministrada por las baterías de reserva cuando el sistema está activado y junto con la tensión de vacío de la batería, se calcula y registra la resistencia de las baterías. Con la alimentación de red desconectada, se activa el sistema durante un período adecuado y se verifica entonces la operación correcta del sistema completo.

LEONID LLONTOP CASTRO
Jefe de Seguridad Casa Matriz
Banco Ciudad Bs. As

5.7.3.4 Dispositivos de advertencia y señalización

Se verificará la audibilidad de los indicadores audibles y los dispositivos de advertencia en todas las áreas donde se requiere que sean oídos. Los dispositivos de advertencia audibles producirán por lo menos dos frecuencias fundamentales dentro de la banda de 300 Hz a 3 kHz.

La operación de las alarmas sonoras autoalimentadas debe ser ensayada para asegurar que suenen correctamente cuando se corta la alimentación.

Se verificará que toda función de retardo de alarma sonora funcione correctamente y se registrará el tiempo de demora.

Cuando un sistema tiene un equipo de señalización remoto, se debe generar una condición de alarma con el sistema activado, para asegurar que sea señalizada y recibida una llamada de alarma en su lugar de destino, por ejemplo, la estación central o la estación de policía.

5.7.4 Entrega

Con el sistema se debe entregar instrucciones de operación escritas, configuración del sistema que detalle las ubicaciones y tipos de equipos indicando las áreas de cobertura, y un formulario de registro de eventos.

El formulario de registro de eventos del sistema debe estar en un formato adecuado para registrar por ejemplo detalles de alarmas, falsas u otras, visitas y trabajos realizados por el personal de mantenimiento y cualquier alteración del sistema.

Durante la entrega del sistema, se debe explicar verbalmente y demostrar físicamente cada etapa de las instrucciones escritas a todos y a cada uno de los usuarios u operadores potenciales del sistema.

Es importante hacer una demostración de todas las eventualidades que puedan tener lugar durante los procedimientos de activación y desactivación. Estas eventualidades pueden incluir: efectos de la alteración de las rutas de entrada y salida, y el exceso en los tiempos permitidos con sistemas que usan entradas y salidas temporizadas. En caso de que se provea un sistema de alarmas con claves personalizadas la instrucción y la carga de la clave será realizada individualmente junto con el usuario. Al terminar de instruir al usuario sobre el uso correcto y el funcionamiento del sistema, el representante de la empresa de alarmas responsable en la entrega, debe obtener un recibo firmado de que las claves del sistema han sido cargadas y una firma que avale que las instrucciones han sido recibidas y comprendidas y que el sistema funciona. La fecha de entrega y toda información adicional a partir de la entrega del sistema debe ser registrado en el formulario de registro de eventos del sistema.

Finalmente, el representante de la empresa de alarmas debe informar al usuario cuáles son las responsabilidades de éste último con respecto de la gestión del sistema instalado.

A este fin se recomienda que se tengan en consideración los puntos siguientes:

- a) Que el sistema de alarma sea operado únicamente por personas que han sido debidamente instruidas para su uso y restringir su número a un mínimo posible.
- b) Informar a la empresa de alarmas sobre los usuarios autorizados y de cualquier cambio al respecto, si es aplicable.
- c) Cerrar y asegurar cuidadosamente todas las puertas y ventanas.
- d) No permitir que haya objetos en movimiento en el alcance de los detectores de movimiento.
- e) Cuidar que los procedimientos de entrada y salida acordados sean seguidos sin desviaciones.
- f) Informar a la empresa de alarmas de cualquier cambio en el edificio y los contenidos que puedan afectar al sistema de alarma, si es aplicable.
- g) No activar el sistema de alarma después de una posible falsa alarma, a menos que el defecto haya sido determinado y rectificado.
- h) Realizar tareas periódicas de mantenimiento y la verificación del correcto funcionamiento por una empresa de mantenimiento. La periodicidad estará de acuerdo con el grado de seguridad requerido y los dispositivos utilizados.
- i) Registrar todos los eventos y visitas de mantenimiento en el formulario de registro de eventos.
- j) Si el sistema es un sistema supervisado por un centro de control a distancia, notificar a dicho centro de cualquier cambio pueda incidir en las condiciones de funcionamiento del sistema.

- k) Verificar la identidad del técnico enviado por el Centro de Control a Distancia para autorizar su actuación.

Anexo A

(Informativo)

Bibliografía

En el estudio de este Esquema se han tenido en cuenta los antecedentes siguientes:

BSI - BRITISH STANDARDS INSTITUTION
British Standard 4737:1988 (Modifications 1:1992 and 2:1999) - Section 4.1: Intruder alarm Systems in buildings. Section 4.1 Code of practice for planning and installation.

- Los datos aportados por los miembros del Subcomité.

LEONID LLONTOP CASTRO
Jefe de Seguridad Caso Matriz
Banco Ciudad Bs. As.

Anexo B

(Informativo)

Integrantes del organismo de estudio

El estudio de este Esquema ha estado a cargo del organismo respectivo, integrado en la forma siguiente:

Subcomité de Sistemas de alarma

Integrante:	Representa a:
Sra. Alejandra BAUER	CEC EDUCACIÓN AL CONSUMIDOR)
Ing. Gabriel BENHABIB	GENERAL INDUSTRIES ARGENTINA S.A.
Sr. Marcelo BENVENISTE	MARCODINA S.A.
Sr. Héctor BLANCO	AASPRI
Sr. Roberto CALEGIURE	AASPRI, ALARMAS INTEGRADAS S.A.
Sr. Walter COSTA	CEMARA
Sr. Ricardo GARABELLO	SISTEMAS ELECTRÓNICOS APLICADOS
Sr. Gabriel FERNÁNDEZ	AASPRI
Arq. Eduardo GONZALEZ	SÁF
Sr. Alberto GUTIERREZ	AASPRI
Lic. Sergio GWIRC	INTI-CITEI
Ing. Ricardo KATZ	PRIORIDAD 1
Sr. Ricardo MARQUEZ	DIALER ALARMAS S.A., CASEL
Sr. Fernando MARTÍN	KOMPUSUR S.A.
Subcrio Miguel MARZANO	POLICÍA FEDERAL ARGENTINA
Ing. Modesto MIGUEZ	AASPRI, CEMARA, CENTRAL DE MONITOREO S.A.
Pcipal. Alberto OBREGÓN	POLICÍA FEDERAL ARGENTINA
Subcrio Norberto PLAQUIN	POLICÍA FEDERAL ARGENTINA
Prof. Carlos REISZ	AASPRI, CEMARA, REIZ S.A.
Ing. José ROSON	E.Y.S.E. S.A.
Ing. Sergio SUTIN	MINIST. DE SEG. POLICIA PROV. BS.AS.
Sr. Daniel VELLA	KOMPUSUR S.A.
Ing. Rita MANSOUR	IRAM

LEONID LLONTOP CASTRO
Jefe de Seguridad Casa Matriz
Banco Ciudad Bs. As.

TRÁMITE

El estudio de esta norma se inició en la reunión del 1998/10/06 (Acta 6-1998), 1998/11/03

(Acta 7-1998), 1999/06/01 (Acta 2-1999), 1999/08/03 (Acta 3-1999), 1999/11/02 (Acta 4-1999), 2000/04/04 (Acta 1-2000), 2000/05/025 (Acta 2-2000), 2000/06/06 (Acta 3-2000), 2000/09/05

(Acta 4-2000), 2000/10/03 (Acta 5-2000), 2000/11/07 (Acta 6-2000), 2001/04/10 (Acta 1-2001), 2001/05/08 (Acta 2-2001), 2001/06/06 (Acta 3-2001), 2001/08/07 (Acta 4-2001), 2001/09/04

(Acta 5-2001), 2001/10/02 (Acta 6-2001), 2001/11/06 (Acta 7-2001), 2002/04/09 (Acta 1-2002), 2002/05/07 (Acta 2-2002), 2002/06/04 (Acta 3-2002), 2002/08/06 (Acta 4-2002), 2002/09/03

(Acta 5-2002), 2002/10/01 (Acta 6-2002), 2002/11/05 (Acta 7-2002), 2003/04/08 (Acta 1-2003), 2003/05/13 (Acta 2-2003), prosiguiendo en las del 2003/06/11 (Acta 3-2003), 2003/08/05

(Acta 4-2003), 2003/09/02 (Acta 5-2003), 2003/10/07 (Acta 6-2003), 2003/11/04 (Acta 7-2003), 2004/04/13 (Acta 1-2004), 2004/05/04 (Acta 2-2004), 2004/06/01 (Acta 3-2004), 2004/08/03

(Acta 4-2004), 2004/09/07 (Acta 5-2004), 2004/10/05 (Acta 6-2004), 2004/11/02 (Acta 7-2004), 2004/12/01 (Acta 8-2004), en la última de las cuales se aprobó como Esquema 1, disponiéndose su envío a Discusión Pública por un lapso de 45 días.

Vuelta de Discusión Pública, se considera en las reuniones del 2006/05/02(Acta 2- 2006), 2006/06/06(Acta 3-2006), 2006/07/05(Acta 5-2006) y 2006/08/22(Acta 6-2006), en la última de las cuales se aprobó como Esquema 2, disponiéndose su envío a Discusión Pública por el término de 30 días.



**INSTITUTO ARGENTINO
DE NORMALIZACIÓN
Y CERTIFICACIÓN**

Asimismo, en el estudio de este Esquema se han considerado los aspectos siguientes:

Aspectos	¿SE HAN INCORPORADO? Sí / No / No corresponde	Comentarios
Ambientales	No	
Salud	No corresponde	
Seguridad	Sí	

APROBADO SU ENVÍO A DISCUSIÓN PÚBLICA POR EL SUBCOMITÉ DE SISTEMAS DE ALARMA EN SU SESIÓN DEL 22 DE AGOSTO DE 2006 (Acta 6-2006)

FIRMADO
Ing. Rita Mansour
Coordinadora del Subcomité

LEONID LLONTOP CASTRO
Jefe de Seguridad Casa Matriz
Banco Ciudad Bs. As.

FIRMADO
Ing. Modesto Miguez
Secretario de Subcomité

FIRMADO
Ing. Osvaldo Petroni
Vº Bº Gerente Eléctrica Electrónica

[1] En la jerga se utiliza el término "armado".

LEONID LIONTOP CASTRO
Jefe de Seguridad Casa Matriz
Banco Ciudad Bs. As





INSTITUTO ARGENTINO
DE NORMALIZACIÓN
Y CERTIFICACIÓN

IRAM
4177

Primera edición
2012-12-14

Certificado | sistemas de Gestión

Sistemas de alarma

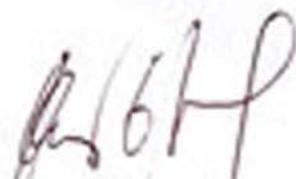
Instalación y configuración de sistemas de alarma diseñados para generar condiciones de confirmación de alarma

Código de práctica

Alarm systems
Installation and configuration of intruder alarm systems designed to generate confirmed alarm conditions
Code of practice



Referencia Numérica:
IRAM 4177:2012


Dirección de Certificación


Comité General de Certificación


Dirección General



IRAM 2012-12-14

No está permitida la reproducción de ninguna de las partes de esta publicación por cualquier medio incluyendo fotocopiado y microfilmación, sin permiso escrito del IRAM.

LEONID LLONTOP CASTRO
Jefe de Seguridad Casa Matriz
Banco Ciudad Bs. As.

Prefacio

El Instituto Argentino de Normalización y Certificación (IRAM) es una asociación civil sin fines de lucro cuyas finalidades específicas, en su carácter de Organismo Argentino de Normalización, son establecer normas técnicas, sin limitaciones en los ámbitos que abarquen, además de propender al conocimiento y la aplicación de la normalización como base de la calidad, promoviendo las actividades de certificación de productos y de sistemas de la calidad en las empresas para brindar seguridad al consumidor.

IRAM es el representante de Argentina en la International Organization for Standardization (ISO), en la Comisión Panamericana de Normas Técnicas (COPANT) y en la Asociación MERCOSUR de Normalización (AMN).

Esta norma es el fruto del consenso técnico entre los diversos sectores involucrados, los que a través de sus representantes han intervenido en los Organismos de Estudio de Normas correspondientes.

LEONID LLONTOP CASTRO
Jefe de Seguridad Caso Matriz
Banco Ciudad Bs. As.

Índice

	Página
1 OBJETO Y CAMPO DE APLICACIÓN.....	5
2 DOCUMENTOS NORMATIVOS PARA CONSULTA	5
3 DEFINICIONES	5
4 DISEÑO PRIMARIO Y CONSIDERACIONES DE CONFIGURACIÓN.....	8
5 DISEÑO, INSTALACIÓN Y CONFIGURACIÓN DE SISTEMAS DE ALARMAS DE INTRUSIÓN QUE INCORPORAN TECNOLOGÍA DE CONFIRMACIÓN DE ALARMA	10
6 OTROS MEDIOS PARA MINIMIZAR <u>ALARMAS NO DESEADAS</u>	15
7 <u>MANEJO DE INFORMACIÓN DE SEÑALES EN LOS CENTROS RECEPTORES DE ALARMAS</u>	16
Anexo A (Normativo) Recomendaciones adicionales para diseño, instalación y configuración	20
Anexo B (Informativo) Ejemplo de los procedimientos de manejo de señales de alarmas en el centro receptor de alarmas (CRA) para señales de alarmas asociadas con la falla de las señales de transmisión.....	24
Anexo C (Informativo) Procedimientos en el centro receptor de alarmas para el manejo de dos señales de falla de transmisión	25
Anexo D (Informativo) Requisitos operacionales para un sistema de alarmas de intrusión equipado con tecnología de confirmación secuencial	26
Anexo E (Informativo) Procedimientos del centro receptor de alarmas para sistemas de alarma capaces de proveer confirmación	27
Anexo F (Informativo) Información recomendada a ser incluida en la propuesta de diseño del sistema y en los documentos adjuntos	30
Anexo G (Informativo) Bibliografía.....	32
Anexo H (Informativo) Integrantes de los organismos de estudio.....	33

LEONID LLONTOP CASTRO
 Jefe de Seguridad Casa Matriz
 Banco Ciudad Bs. As.

Sistemas de alarma

Instalación y configuración de sistemas de alarma diseñados para generar condiciones de confirmación de alarma

Código de práctica

1 OBJETO Y CAMPO DE APLICACIÓN

Esta norma da recomendaciones para el diseño, instalación y configuración de un sistema de alarmas anti intrusión que incorpora tecnología de confirmación de alarmas, con sistemas de señalización que reportan a un centro de control a distancia o centro receptor de alarmas y que requiera respuesta de la autoridad de seguridad pública.

Esta norma incluye recomendaciones destinadas a minimizar la posibilidad de alarmas no deseadas (o falsas alarmas) y se recomienda su uso en conjunto con las demás normas aplicables a sistemas de alarma.

Las alarmas de asalto (ya sean sistemas de alarmas de asalto independientes o integrados a un sistema de alarma de intrusión) están fuera del alcance de esta norma.

NOTA 1. Esto no significa que los dispositivos de asalto no puedan formar parte de un sistema de alarma que incorpora tecnología de confirmación de alarmas.

2 DOCUMENTOS NORMATIVOS PARA CONSULTA

Todo documento normativo que se menciona a continuación es indispensable para la aplicación de este documento.

Cuando en el listado se mencionan documentos normativos en los que se indica el año de publicación, significa que se debe aplicar dicha edición. En caso contrario, se debe aplicar la edición vigente, incluyendo todas sus modificaciones.

IRAM 4175 - Sistema de alarma de intrusión en inmuebles. Código de práctica para la planificación y la instalación.

IRAM 4176 - Sistemas de alarma contra la intrusión y el asalto. Requisitos generales de desempeño considerando grados de seguridad y clases ambientales.*

BS 8473 - Management of false alarms.**

IEC 62642-1 - Alarm systems-Intrusion and hold up systems. Part 1: System requirements.

3 DEFINICIONES

Para los fines de la presente norma se aplican las definiciones siguientes.

Son aplicables además, según sea necesario, las definiciones de las IRAM 4175 e IRAM 4176*.

En toda la norma los términos definidos en este capítulo, se resaltan con subrayado.

3.1 filtrado de alarma (autorizado por el abonado)

Procedimiento por el cual se analizan previamente en un centro receptor de alarmas, las condiciones de señalización de un evento de alarma y se revisan sus estados, con el propósito de cancelar aquellas condiciones autorizadas por el abonado.

* En estudio. Hasta tanto finalice su estudio, se debe consultar la IEC 62642-1

** Hasta tanto no se realice el estudio de la norma IRAM correspondiente, se empleará la norma BS citada

3.2 llamada para verificación

Comunicación desde un centro de recepción de alarmas hacia la/las parte/s apropiada/s, cuando una condición de alarma ha ocurrido en un local supervisado, o para proveer información suplementaria concerniente de alguna condición de alarma anteriormente reportada.

3.3 centro receptor de alarmas (o centro de recepción de alarmas) (CRA)

Centro atendido de forma continua por personas en el que se reciben los datos relacionados con el estado de uno o más sistemas de alarmas.

3.4 señal de alarma

Señal que, habiendo sido recibida o recibida y procesada en un centro de recepción de alarmas, se identifica la señalización como una condición de alarma.

3.5 equipo auxiliar de control (EAC)

Equipo empleado para fines de control suplementario.

3.6 documento de la instalación definitiva (o documento de final de obra)

Documento en el que se registra el detalle de la instalación definitiva del sistema de alarmas.

3.7 confirmación por audio (o confirmada por audio)

Denominación en un centro de recepción de alarmas que surge de la interpretación de información de audio transmitida desde locales supervisados y la determinación de una alta probabilidad de que una intrusión real o un intento de intrusión real haya ocurrido.

3.8 dispositivo captador de audio (DCA)

Instrumento conversor de ondas sonoras a variaciones de energía eléctrica para la consecuente reconversión a ondas sonoras (ejemplo: micrófono).

3.9 dispositivo de supervisión de audio (DSA)

Instrumento que se activa por sonidos por encima de un umbral específico.

NOTA. Típicamente este tipo de dispositivo tiene un micrófono incorporado.

3.10 tiempo de confirmación

Tiempo permitido para la ocurrencia de una alarma secuencialmente confirmada luego de producida una alarma no confirmada.

3.11 equipo de control y de señalización (ECS)

Equipo destinado a recibir, procesar, controlar, indicar e iniciar la transmisión de la información.

3.12 abonado

Persona u organización que compra el sistema de alarma y/o otros servicios de una compañía de alarmas o de un centro de recepción de alarmas.

3.13 detector de doble tecnología

Dispositivo de detección que emplea dos tecnologías de sensado diferentes supervisadas por un procesador común con una salida de alarma única.

3.14 reporte de formato detallado

Notificación hacia un sistema de transmisión de alarmas generada por partes específicas de un sistema de alarma generalmente desde un circuito, una zona o un área.

3.15 alarma no deseada (o falsa alarma)

Condición de alarma que no resulte de:

- a) Intrusión o tentativa de intrusión a un local supervisado, a un equipo de alarma, o a la línea que lleva la señal de alarmas;
- b) tentativa de daño o daño a un local supervisado, a un equipo de alarma, o a la línea que lleva la señal de alarmas;
- c) acciones de los servicios de emergencia en ejercicio de sus deberes;
- d) una llamada proveniente de un sistema de alarma de asalto realizada con intenciones legítimas o bien intencionadas. (estrés, coacción, etc.).

NOTA. La activación de los detectores sin daño aparente o por la entrada a los locales supervisados, u otros hechos diferentes a los anteriormente descritos, se considera una alarma no deseada (falsa alarma) a menos que se pruebe lo contrario.

LEONID LLONTOP CASTRO

Jefe de Seguridad Casa Matriz
Banco Ciudad Bs. As.

3.16 falsa alerta

Condición de alarma señalizada, que es considerada por el centro receptor de alarma como cancelada, habiendo sido tal cancelación autorizada por el abonado.

3.17 puerta final de salida

Puerta designada para la salida de los locales supervisados.

3.18 dispositivo de captura de imagen

Dispositivo que convierte una imagen óptica en una señal eléctrica.

NOTA. Una cámara es un ejemplo de dispositivo de captura de imagen.

3.19 puerta inicial de entrada

Puerta designada para la entrada a los locales supervisados.

3.20 escuchar

Acción en un centro receptor de alarmas, de escuchar audio ya sea directo o almacenado, recibido desde los locales supervisados.

3.21 audio en vivo

Información de naturaleza audible, que está ocurriendo en tiempo real.

3.22 señal de operación incorrecta

Señal que es identificable en el centro de recepción de alarmas que indica que el sistema de alarmas se ha operado incorrectamente y por lo tanto que la condición de alarma señalizada es para ser cancelada y considerada como una alerta falsa.

NOTA. La designación de un tipo particular de señal como señal de operación incorrecta es por lo tanto un asunto de acuerdo entre la compañía de alarma y el centro de recepción de alarmas, con la anuencia del abonado.

3.23 notificación

Envío de una condición de alarma, falla o sabotaje a los dispositivos de advertencia y/o a los sistemas de transmisión de alarmas.

3.24 equipo auxiliar de control portátil (EPAC)

Dispositivo portátil utilizado para armar y/o desarmar un sistema de alarmas.

3.25 lector del equipo auxiliar de control portátil (lector del EPAC)

Equipamiento fijo, que permite desarmar un sistema de alarmas utilizando un equipo auxiliar de control portátil y que puede estar incorporado dentro del equipo de control y de señalización, o el equipo auxiliar de control, o puede ser un ítem separado o un subsistema que provea la funcionalidad requerida.

3.26 centro remoto

Emplazamiento de ubicación remota con respecto a los locales supervisados, en el cual se recibe la información concerniente con el estado de uno o más sistemas de alarma, para reportar o transmitir.

3.27 restablecer

Procedimiento de cancelación de una alarma, de una protección contra la manipulación, falla u otra condición de retorno del sistema de alarma a una condición previa.

3.28 secuencialmente confirmada (o confirmación secuencial)

Condición emanada de uno o más detectores independientes, que están configurados de manera tal que exista una alta probabilidad de que haya ocurrido una intrusión genuina o un intento de intrusión.

3.29 cerradura de conmutación

Cerradura de puerta que incorpora un dispositivo de conmutación dentro del alojamiento de la cerradura.

3.30 señalización de una condición de alarma

Estado del equipamiento de supervisión en un centro de recepción de alarmas remoto, que indica una condición de alarma.

NOTA. Esto no excluye a otras señales (ejemplo: desarmado, armado, mal funcionamiento, falla) recibidas en un centro de recepción de alarmas.

3.31 audio almacenado

Grabaciones en formato audible realizadas en emplazamientos supervisados, antes durante, y después del momento de una condición de alarma.

3.32 locales supervisados (o local supervisado)

Parte de un edificio y/o área en la cual una intrusión, un intento de intrusión, o el disparo de un dispositivo de asalto pueden ser detectados por un sistema de alarma o sistema de alarma de asalto y de intrusión.

3.33 propuesta de diseño de sistema

Documento de especificación para una propuesta de sistema de alarma, listando el equipamiento y los componentes a suministrar, detallando la localización propuesta y conteniendo una indicación general de su cobertura o propósito.

3.34 detección de manipulación indebida o de sabotaje (detección de "tamper")

Detección de una acción indebida deliberada a un sistema de alarma o alguna de sus partes.

3.35 señal de falla de transmisión

Indicación de falla durante el trayecto de la señal de alarma.

3.36 alarmas no confirmadas

Señal que no ha sido designada como alarma confirmada por audio, visualmente confirmada o secuencialmente confirmada.

3.37 usuario

Persona autorizada para operar un sistema de alarma.

3.38 dispositivo de supervisión de video (DVS)

Dispositivo que se activa por perturbaciones de imagen respecto de un patrón específico.

NOTA. Típicamente un dispositivo de supervisión de video estaría incorporado en un dispositivo de captura de imagen.

3.39 visualmente confirmado/a (o de confirmación visual)

Designación en un centro de recepción de alarmas que surge de la interpretación de la información visual transmitida de los locales supervisados y determinando que existe una alta probabilidad que una intrusión genuina o un intento genuino de intrusión ha ocurrido.

3.40 armado (o activado/ o activación*)

Estado del sistema de alarma o parte de éste en el cual una condición de alarma de intrusión puede ser notificada.

3.41 desarmado (o desactivado/o desactivación*)

Estado de un sistema de alarma de intrusión en el que no es posible que se notifique una condición de alarma.

3.42 condición de falla

Condición del sistema de alarma que impide el funcionamiento normal del sistema de alarma de intrusión o de partes de éste.

3.43 condición de alarma

Condición de un sistema de alarma, o parte de éste, que resulta de la respuesta del sistema ante la presencia de un peligro.

3.44 condición de alarma de asalto(o alarma de asalto)

Condición de un sistema de alarma, o parte de éste, que resulta de la respuesta del sistema al accionamiento de un dispositivo de asalto.

3.45 dispositivo de asalto (o pulsador de pánico)

Dispositivo que cuando es disparado (o pulsado, que cuando es accionado), provoca la generación de una señal de alarma de asalto o de un mensaje.

4 DISEÑO PRIMARIO Y CONSIDERACIONES DE CONFIGURACIÓN

4.1 Objetivos de diseño

Se recomienda que los sistemas de alarma se diseñen, instalen y configuren para:

- a) proveer prestaciones efectivas de confirmación;
- b) minimizar la probabilidad de alarmas no deseadas.

LEONID LLONTOP CASTRO
Jefe de Seguridad Casa Matriz
Banco Ciudad Bs. As.

* Denominación utilizada para este término en la IRAM 4175.

Se recomienda que los sistemas de alarma que incorporan tecnología de confirmación de alarmas, se diseñen, instalen y configuren de acuerdo con el capítulo 5 y el anexo A. La provisión de una tecnología de confirmación ayuda a la minimización de las alarmas no deseadas.

En el capítulo 6 se dan otras recomendaciones para minimizar las probabilidades de alarmas no deseadas (por ejemplo procedimientos para desarmado).

4.2 Tecnología de confirmación de alarmas

La tecnología de confirmación de alarmas apunta a proveer una alta confianza en que una señal de alarma ha sido causada por una intrusión genuina o un intento genuino de intrusión.

Existen tres formas de tecnología de confirmación de alarmas para uso con sistemas de alarma de intrusión instalados en locales, consideradas en esta norma:

- a) tecnología de confirmación por audio (ver 5.2);
- b) tecnología de confirmación visual (visualmente confirmada, ver 5.3);
- c) tecnología de confirmación secuencial (secuencialmente confirmada, ver 5.4).

Se recomienda que todos los sistemas de alarma de intrusión incorporen tecnología de confirmación secuencial.

Los sistemas de alarma de intrusión pueden incorporar las otras dos tecnologías, de acuerdo a:

- necesidades y expectativas del abonado;
- las condiciones ambientales de los locales supervisados.

4.3 Señales de falla de transmisión

Hay dos circunstancias en las que, en un sistema de alarmas de intrusión instalado en conformidad con esta norma, puede haber una alta probabilidad de certeza de que exista una intrusión genuina o un intento de intrusión genuino.

- a) Si un centro de recepción de alarmas recibe una señal de falla de transmisión seguida por una señal de alarma, o viceversa, proveniente del mismo local vigilado durante el armado simple en un período de hasta un máximo de 96 h.
- b) Si dos señales de falla de transmisión existen al mismo tiempo del mismo local supervisado, una desde cada uno de los dos medios de transmisión de diferentes tecnologías (ejemplo: cable y radio) durante el armado simple en un período de hasta un máximo de 96 h.

La conexión a dos medios de transmisión es opcional y por acuerdo con el abonado.

Cuando se proponga el diseño de un sistema de transmisión de alarmas con la señalización de un único medio de transmisión, se recomienda incluir una advertencia en negrita, como la siguiente, en la propuesta de diseño del sistema a continuación de la descripción del método de señalización:

IMPORTANTE

Prestar atención a que si hay una falla en el único medio de transmisión, ésta no debe ser notificada a la autoridad de seguridad pública. Mientras la falla persista, no podrán transmitirse las alarmas subsecuentes al centro de recepción de alarmas y notificarlas a la autoridad de seguridad pública.

NOTA. La conexión a dos medios de transmisión no iguala o constituye, a equiparar el sistema de alarmas con la tecnología de confirmación de alarmas.

Es recomendable que cuando las fallas de transmisión deban ser notificadas, la compañía de alarmas debe informar al abonado por escrito, en el momento del acuerdo de supervisión entre la compañía de alarma y el abonado, los procedimientos a realizar por el centro receptor de alarmas al detectar una señal de falla de transmisión o señales de falla de transmisión.

En el anexo B se da un ejemplo de procedimientos que manejan los centros receptores de alarmas para señales de alarmas asociadas con señales de falla de transmisión.

En el anexo C se da un ejemplo de procedimientos de centro receptor de alarmas para manejar dos señales de falla de transmisión.

5 DISEÑO, INSTALACIÓN Y CONFIGURACIÓN DE SISTEMAS DE ALARMAS DE INTRUSIÓN QUE INCORPORAN TECNOLOGÍA DE CONFIRMACIÓN DE ALARMA

5.1 Generalidades

5.1.1 Proceso de diseño

El diseño y la configuración del sistema de alarmas de intrusión que incorpora la tecnología de confirmación de alarma deben tener en cuenta las necesidades y expectativas del abonado y la respuesta deseada a las alarmas. Es recomendable que el proceso de diseño considere todo el local supervisado.

NOTA 1. Es materia del diseño del sistema, cubrir las necesidades y las expectativas del abonado, en cuanto a si la tecnología de confirmación de alarmas es aplicada a cada área del local supervisado, o sólo a alguna/s área/s.

Se recomienda considerar el uso del reporte de formato detallado.

NOTA 2. El reporte de formato detallado puede ser de utilidad en el suministro de información adicional sobre la intrusión, aportando además información sobre:

- a) la ubicación de detectores que se han activado;
- b) activaciones múltiples de detectores;
- c) la identificación de detectores perimetrales que se han activado.

Se recomienda que los detectores instalados fuera del área que se quiere proteger no contribuyan a la generación de alarmas audiblemente, visualmente o secuencialmente confirmadas.

NOTA 3. Los sistemas de CCTV supervisados remotamente y activados por detector pueden incorporar detectores instalados fuera del local supervisado. Las activaciones de tales detectores son consideradas como causa suficiente para solicitar la intervención de la autoridad de seguridad pública si hay evidencia certera en las imágenes de las condiciones requeridas para una respuesta de emergencia y/o de una actividad criminal real.

5.1.2 Provisión de una instalación de confirmación eficaz

Según las necesidades y las expectativas del abonado, se recomienda emplear alguna de las opciones siguientes:

- a) Instalación de confirmación eficaz en todas partes del local supervisado.

Se recomienda que el sistema de alarmas de intrusión sea diseñado y configurado de manera que cuando un intruso entre en cualquier parte del local supervisado, que no sea un medio designado como entrada:

- 1) el sistema de alarmas de intrusión sea capaz de proveer confirmación de actividad en todas partes del local supervisado;
- 2) haya una expectativa razonable de que el sistema de alarmas de intrusión proporcione tal confirmación (a condición de que el intruso haya ganado el acceso por un medio/ruta destinado a ser supervisado por el sistema de alarma).

- b) Instalación de confirmación eficaz en partes especificadas del local supervisado.

Se recomienda que el sistema de alarmas de intrusión sea diseñado y configurado de tal modo que cuando un intruso entra en partes especificadas del local supervisado:

- 1) el sistema de alarmas de intrusión sea capaz de proveer confirmación de actividad en las partes especificadas del local supervisado;
- 2) haya una expectativa razonable de que el sistema de alarmas de intrusión proporcione tal confirmación (a condición de que el intruso haya ganado el acceso por un medio/ruta destinado a ser supervisado mediante el sistema de alarma).

Se recomienda que la propuesta de diseño del sistema y el documento adjunto (ver anexo F, identifiquen las partes especificadas del local supervisado, que tengan o no, realmente instalación de confirmación eficaz.

Cuando no sea posible decir que todas las condiciones de alarma que provienen de un sistema de alarmas de intrusión dado resultan en una alarma confirmada, se enfatiza que la designación como confirmada se haga caso por caso para cada condición de alarma.

NOTA Generalmente, es aconsejable usar la frase *sistema de alarmas de intrusión que incorpora la tecnología de confirmación de alarma o sistema de alarmas de intrusión capaz de generar alarmas confirmadas*, y no *sistemas confirmados* porque tal sistema de alarmas de intrusión podría generar a veces sólo alarmas no confirmadas.

5.1.3 Notificación de condición de alarma y otra información

Se recomienda que la notificación de condiciones de alarma cumpla con la IRAM 4176*, para permitir el funcionamiento eficaz de sistemas de alarmas de intrusión que incorpora la tecnología de confirmación de alarma, sin embargo, es necesario para información adicional o adjunta que sea transmitida al centro receptor de alarmas.

Es recomendable llegar a un acuerdo entre la compañía de alarma y el abonado (quién debe ser aconsejado para que consulte con sus aseguradores, si es aplicable) en:

- la cantidad de información adicional o adjunta transmitida del local supervisado a un centro receptor de alarmas;
- las circunstancias en las cuales la información es transmitida;
- cualquier tiempo de demora intencional en el local antes de la transmisión de la información adicional o adjunta.

5.1.4 Ubicación del equipo de control y de señalización y del equipo de notificación

Se recomienda que el equipo de control y de señalización y el equipo de notificación se localicen y supervisen de manera de minimizar el riesgo de vandalismo o sabotaje.

5.1.5 Recomendaciones adicionales

Recomendaciones adicionales para:

* En estudio. Hasta tanto finalice su estudio, se debe consultar la IEC 62642-1.

- la tecnología de confirmación por audio, ver 5.2;
- la tecnología de confirmación visual, ver 5.3;
- la tecnología de confirmación secuencial, ver 5.4.

5.2 Diseño y configuración de confirmación por audio de sistema de alarmas de intrusión

5.2.1 Generalidades

Se recomienda que:

- la propuesta de diseño del sistema y las especificaciones técnicas adjuntas establezcan claramente el alcance, el grado y la cobertura de la instalación de confirmación por audio, incluyendo aquellas áreas dentro del local supervisado que están en el alcance y la proximidad esperadas de los dispositivos captadores de audio;
- el dispositivo captador de audio esté ubicado de modo de evitar cualquier fuente de ruido que pueda interferir con la escucha de audio por el operador del centro receptor de alarmas;
- el personal a cargo del servicio se contacte con el usuario o el abonado antes de comenzar cualquier procedimiento de mantenimiento que habilite a escuchar el audio en forma local o remota;
- la tecnología de confirmación por audio utilizada pueda ser la confirmación por audio de la detección de una intrusión (ver 5.2.2), la confirmación por audio de la activación del dispositivo de supervisión de audio (ver 5.2.3) o una combinación de los dos métodos;
- el sistema de alarmas de intrusión equipado con la confirmación por audio de detección de intrusión también se configure para generar alarmas secuencialmente confirmadas.

5.2.2 Confirmación por audio de detección de intrusión

Cuando un detector en un sistema de alarmas de intrusión que incorpore la tecnología de confirmación por audio es activado provocando

una condición de alarma, se debe transmitir el audio del local supervisado al centro receptor de alarmas para su interpretación.

En las partes del local supervisado que cuenten con confirmación por audio, todos los detectores, equipo de control y de señalización y el equipo de notificación deben situarse dentro del alcance esperado de un dispositivo captador de audio.

Se recomienda que el área de cobertura de un dispositivo captador de audio sea mayor que el área de cobertura de cualquier detector(es) que lo acompañe.

Se deben tomar los recaudos necesarios para asegurar que cualquier parte del local supervisado que pudiera estar ocupada cuando el sistema de alarmas de intrusión esté armado parcialmente, esté configurado de tal modo que sea posible aislar tanto detectores como los dispositivos captadores de audio que cubren el área o el grupo desarmado.

En áreas múltiples o sistemas de grupo (particiones), sólo los dispositivos captadores de audio en el área de activación o grupo deben ser capaces de proporcionar el audio.

Cuando la confirmación por audio de la detección de intrusión esté instalada, debe haber:

- a) almacenamiento de audio de no menos de 10 s inmediatamente antes de una condición de alarma, que es almacenado en el local supervisado listo para la transmisión al centro receptor de alarmas;
- b) almacenamiento de audio inmediatamente después de una condición de alarma, el cual es almacenado en el local supervisado listo para la transmisión al centro receptor de alarmas:
 - 1) en el caso donde el enlace de audio entre el local supervisado y el centro receptor de alarmas es iniciado por el centro receptor de alarmas (es decir discado revertido), no menos de 15 s de audio almacenado,
 - 2) en el caso donde el enlace de audio entre el local supervisado y el centro receptor de alarmas es iniciado auto-

máticamente por el equipo en el local supervisado (es decir discado automático), el audio almacenado debe ser de una duración no menor que el tiempo tomado para establecer el enlace de audio bajo condiciones de funcionamiento normales;

- c) instalaciones apropiadas en el centro receptor de alarmas para recibir audio en vivo.

A menos que una condición de alarma haya sido recibida en el centro receptor de alarmas, los únicos otros medios disponibles de escucha al local supervisado, deben ser aquellos accesibles a través de las funciones habilitadas al personal de servicio en el equipo de control y de señalización del local supervisado.

5.2.3 Confirmación por audio de activación del dispositivo de supervisión de audio

Cuando los sonidos activan un dispositivo de supervisión de audio en un sistema de alarmas de intrusión que incorpora la tecnología de confirmación por audio, el audio debe ser transmitido del local supervisado al centro receptor de alarmas para su interpretación.

Si es aplicable, la propuesta de diseño del sistema y la documentación adjunta deben establecer claramente el alcance, el grado y la cobertura de la instalación del dispositivo de supervisión de audio, incluso en aquellas áreas que están dentro del local supervisado que puedan estar dentro del rango esperado y en la proximidad de los dispositivos de supervisión de audio (ver también el anexo F).

En partes del local supervisado con la confirmación por audio, todos los detectores, el equipo de control y de señalización y el equipo de notificación deben situarse dentro del rango esperado de un dispositivo de supervisión de audio y de su dispositivo captador de audio acompañante.

Cuando los dispositivos de supervisión de audio están instalados debe haber:

- a) almacenamiento de audio de no menos de 1 s inmediatamente antes de una activación del dispositivo de supervisión de audio, que es almacenado en el local su-

pervisado listo para la transmisión al centro receptor de alarmas;

- b) almacenamiento de audio inmediatamente después de la activación de un dispositivo de supervisión de audio, el cual es almacenado en el local supervisado listo para la transmisión al centro receptor de alarmas:
- 1) en caso de que el enlace de audio entre el local supervisado y el centro receptor de alarmas sea iniciado por el centro receptor de alarmas (por ejemplo: discado revertido), audio almacenado por 15 s o más,
 - 2) en caso de que el enlace de audio entre el local supervisado y el centro receptor de alarmas sea iniciado automáticamente por el equipo en el local supervisado (es decir discado automático), el audio almacenado debe ser de una duración no menor que el tiempo tomado para establecer el enlace de audio bajo condiciones de funcionamiento normales;
- c) instalaciones apropiadas en el centro receptor de alarmas para recibir audio en vivo.

A menos que un dispositivo de supervisión de audio se haya disparado, los únicos otros medios disponibles de escucha al local supervisado, deben ser aquellos accesibles a través de las funciones habilitadas al personal de servicio en el equipo de control y de señalización del local supervisado.

5.3 Diseño y configuración de confirmación visual de sistemas de alarmas de intrusión

5.3.1 Generalidades

La propuesta de diseño de sistema y la documentación adjunta deben declarar claramente el alcance, extensión y la cobertura de la instalación de confirmación visual, incluso aquellas áreas dentro del local supervisado que están dentro del campo de visión de los dispositivos de captura de imagen.

Los dispositivos de captura de imagen deben ser situados para evitar que fuentes de luz interfieran con la interpretación del operador en el centro receptor de alarmas y el campo de visión debe

iluminarse de modo tal que en el centro receptor de alarmas se reciba una imagen clara.

Cuando se realiza una instalación de confirmación visual, el o los dispositivos de captura de imagen deben ver toda el área de cobertura de cualquier detector que lo acompañe.

Después de una condición de alarma, debe haber un mínimo de tres imágenes transmitidas al centro receptor de alarmas, una imagen en el momento de la condición de alarma o la activación del dispositivo de supervisión de video, y dos imágenes más dentro de los 5 s posteriores a la condición de alarma o la activación del dispositivo de supervisión de video.

El personal de servicio debe acordar con el usuario o el abonado antes de comenzar cualquier procedimiento de mantenimiento que permita visualizar las imágenes.

La tecnología de confirmación visual utilizada puede ser la confirmación visual de la detección de intruso (ver 5.3.2), confirmación visual de la activación del dispositivo de supervisión de video (ver 5.3.3) o una combinación de los dos métodos.

El sistema de alarmas de intrusión equipado con la confirmación visual de detección de intruso también debe configurarse para generar alarmas secuencialmente confirmadas.

5.3.2 Confirmación visual de detección de intruso

Cuando un detector es activado en un sistema de alarmas de intrusión incorporando la tecnología de confirmación visual causando una condición de alarma, las imágenes deberán ser transmitidas del local supervisado al centro receptor de alarmas para su interpretación.

5.3.3 Confirmación visual de activación del dispositivo de supervisión de video

Cuando las perturbaciones disparan un dispositivo de supervisión de video en un sistema de alarmas de intrusión que incorpora tecnología de confirmación visual, las imágenes deben ser transmitidas del local supervisado al centro receptor de alarmas para su interpretación.

5.4 Diseño y configuración de los sistemas de alarmas de intrusión con confirmación secuencial

5.4.1 Criterios para condiciones de alarmas secuencialmente confirmadas

Para que una condición de alarma sea considerada como secuencialmente confirmada deben darse las condiciones siguientes:

- a) el sistema de alarmas de intrusión debe ser configurado de modo que al menos dos condiciones de alarma separadas sean reportadas, cada una originada en un detector independiente dentro del tiempo de confirmación;
- b) los dos detectores deben ser de:
 - 1) tecnologías diferentes que permitan tener áreas que se superponen en la cobertura, o
 - 2) la misma tecnología simple y no tener áreas que se superpongan en la cobertura.

Para ser considerado como independiente cada detector debe reportar condiciones de alarmas por separado al equipo de control y de señalización, además, la señal de entrada de un detector no debe influir en la salida de otro detector.

El tiempo de confirmación debe ser no menos de 30 minutos y no más de 60 minutos.

La figura D.1 ilustra un ejemplo de los requisitos operacionales para un sistema de alarmas de intrusión equipado con la tecnología de confirmación secuencial.

5.4.2 Configuraciones de detectores de movimiento con áreas de cobertura superpuestas que pueden ofrecer una condición de alarma secuencialmente confirmada

Dos detectores de movimiento de doble tecnología independientes que incorporan las mismas dos tecnologías, pueden ser considerados como detectores de tecnologías diferentes de acuerdo con 5.4.1b) 1).

De acuerdo con 5.4.1b) 1) dos detectores de tecnologías diferentes con las áreas de cober-

tura superpuestas son capaces de causar una alarma secuencialmente confirmada. Sin embargo, cuando los dos detectores son de movimiento, al menos uno debe ser un detector de movimiento de doble tecnología.

Los detectores de movimiento individuales deben ubicarse de manera tal de minimizar la posibilidad de alarmas no deseadas. También debe considerarse cuidadosamente la localización de cualquier área superpuesta de la cobertura de detectores de movimiento para reducir al mínimo la posibilidad de alarma no deseada. Por lo tanto, los detectores de movimiento deben ser localizados a alguna distancia entre ellos, generalmente una distancia mínima entre los gabinetes de los detectores de 2.5 m.

Cuando los detectores de movimiento están configurados para el propósito de proveer alarmas que podrían ser señalizadas como secuencialmente confirmadas, es importante hacer regularmente una prueba de caminata.

5.4.3 Configuraciones de detectores de movimiento sin área de cobertura superpuesta que puede ofrecer una condición de alarma secuencialmente confirmada

Donde no hay ninguna área de cobertura superpuesta, se debe tener cuidado de ubicar los detectores de movimiento de manera de minimizar la posibilidad de que alarmas secuencialmente confirmadas terminen siendo alarmas no deseadas, por ejemplo, debido a factores ambientales que influyan en los detectores de movimiento, cumpliendo con lo establecido en 4.3.4, 5.2 y 5.7.3.2 de la IRAM 4175.

Cuando los detectores de movimiento están configurados para el propósito de proveer alarmas que podrían ser señalizadas como secuencialmente confirmadas, es importante hacer regularmente la prueba de caminata.

5.4.4 Configuraciones que no proveen una condición de alarma secuencialmente confirmada

Dos detectores de movimiento de tecnología simple que tienen áreas de cobertura superpuestas no se considera como que ofrecen una

condición de alarma secuencialmente confirmada (ver 5.4.1 y 5.4.2).

Además, las configuraciones siguientes no son consideradas como que ofrecen una condición de alarma secuencialmente confirmada:

- a) una configuración de doble disparo;
- b) un sólo detector de doble tecnología;
- c) dos (o más) detectores de vibración con sus áreas de cobertura superpuestas;
- d) dos (o más) detectores de rotura de cristal con sus áreas de cobertura superpuestas;
- e) dos (o más) detectores de rotura de cristal por cinta de metal instalados en el mismo paño de cristal;
- f) dos (o más) detectores de apertura (contactos de puerta) fijados en la misma puerta o ventana;
- g) dos (o más) dispositivos de supervisión de audio;
- h) dos (o más) dispositivos de supervisión de video;
- i) dos (o más) detectores que responden a un cambio de presión atmosférica.

5.4.5 Propuesta del diseño del sistema y documentación adjunta

La propuesta de diseño del sistema y la documentación adjunta debe especificar y explicar los parámetros operacionales de las características secuenciales del sistema de alarma, incluyendo lo siguiente:

- a) debe estar claramente establecido si hay combinaciones de detectores, que, cuando más de uno de estos reporta una condición de alarma no se genere un mensaje de alarma confirmada;
- b) debe estar claramente establecido el tiempo de confirmación (debe ser no menos de 30 minutos y no más de 60 minutos).

6 OTROS MEDIOS PARA MINIMIZAR ALARMAS NO DESEADAS

6.1 Generalidades

La probabilidad de alarmas no deseadas debe ser minimizada de acuerdo con 6.2, 6.3, 6.4 y con la BS 8473*.

6.2 Filtrado de alarma

6.2.1 Generalidades

La intención de aplicar filtrado de alarmas es ayudar a minimizar la probabilidad de alarmas no deseadas. El filtrado también puede ayudar a evitar algunas llamadas innecesarias a usuarios y/o personas con acceso autorizado.

Las recomendaciones para la aplicación del filtrado de alarmas por parte de centros receptores de alarmas se indican en el capítulo 7.

6.2.2 Medios para facilitar el filtrado de llamadas por alarmas no deseadas

Todo sistema de alarmas de intrusión debe:

- a) tener los medios para indicar al centro receptor de alarmas si el sistema de alarmas de intrusión está armado o desarmado, o
- b) ser capaz de generar una señal secundaria identificable, en el centro receptor de alarmas, como una señal de operación incorrecta.

Siempre que exista la posibilidad de que una señal de alarma esté siendo transmitida al centro receptor de alarmas, deben proveerse los medios para implementar al menos una de estas opciones.

6.3 Medios para minimizar las alarmas no deseadas en el armado

El equipo de control y de señalización o el equipo auxiliar de control, debe estar instalado cerca de la puerta final de salida y debe existir en ésta, necesariamente, un sensor de apertura, el cual

* Hasta tanto no se realice el estudio de la norma IRAM correspondiente, se empleará la norma BS citada

podrá establecer el modo de armado total o parcial conforme esté configurado el sistema y se haya abierto o no esta última puerta luego del armado.

Debe considerarse suministrar indicaciones, como mínimo auditivas o visuales, internas suplementarias previo al armado (de modo que las personas dentro de un local supervisado sean informadas que el sistema de alarmas de intrusión está pronto a ser armado) y el suministro adicional del equipo auxiliar de control (de modo que si el sistema de alarmas de intrusión es armado haya medios disponibles localmente dentro del lugar supervisado para desarmar el sistema de alarmas de intrusión).

6.4 Medios para minimizar las alarmas no deseadas en el desarmado

Los medios de desarmado pueden minimizar la probabilidad de alarmas no deseadas. El método recomendado es asegurar que las alarmas confirmadas no ocurran momentos después del desbloqueo o apertura de la puerta inicial de entrada.

El medio determinado para el desarmado de un sistema de alarmas de intrusión debe ser adecuadamente descrito en la propuesta de diseño del sistema y el documento adjunto, proporcionado por la compañía de alarma al abonado.

En todas las opciones de desarmado, cuando el procedimiento de desarmado ha sido satisfactoriamente completado, debe haber una indicación audible o visual que permita saber que el sistema de alarmas de intrusión está desarmado. La indicación debe ser de tiempo limitado, informando al usuario que el sistema de alarmas de intrusión ha sido desarmado.

Se recomienda considerar la posibilidad de suministrar, dentro de la ruta de entrada, un medio de comunicación de voz con el centro receptor de alarmas.

La ubicación del equipo auxiliar de control debe ser fácilmente accesible para su operación. Bajo una operación normal, una persona no autorizada debe ser impedida de observar el código de desarmado.

El equipo auxiliar de control montado externamente debe ser provisto de detección de sabotaje ("Tamper"). La aplicación de fuerza física a un equipo auxiliar de control montado en exterior no debe ser capaz de iniciar un cambio en el estado (armado-desarmado) del sistema de alarmas de intrusión.

7 MANEJO DE INFORMACIÓN DE SEÑALES EN LOS CENTROS RECEPTORES DE ALARMAS

7.1 Manejo de información de señales provenientes de sistemas de alarmas de intrusión capaces de proporcionar confirmación por audio

7.1.1 Escucha

Sólo debe ser posible escuchar un local supervisado desde una posición remota únicamente después de la recepción de una condición de alarma. Una vez que el centro receptor de alarmas ha escuchado y luego se desconectó, a no ser que se convenga otra cosa con el abonado, no debe ser posible para el centro receptor de alarmas poder escuchar otra vez hasta que una condición de alarma adicional, o una activación de un dispositivo de supervisión de audio adicional, sean recibidas en el centro receptor de alarmas.

Cuando el centro receptor de alarmas entra en contacto con el local supervisado, debe haber una indicación audible o visual en el centro receptor de alarmas que verifica la identidad del local supervisado. Esta identificación puede ser generada desde el equipo localizado en el local supervisado.

En caso de confirmación por audio de la detección de intruso, los periodos de escucha deben ser de un mínimo de 60 s e incluir todos los audios almacenados, si el audio en vivo no proporciona sonidos consecuentes con la intrusión o intento de intrusión en el local supervisado.

NOTA. Este periodo de escucha intenta no demorar la acción del centro receptor de alarmas cuando hay evidencia positiva de intrusión o tentativa de intrusión.

Si, a consecuencia de la escucha en el local supervisado, el centro receptor de alarmas decide no designar la condición de alarma como confirmada por audio, entonces las acciones tomadas por el centro receptor de alarmas deben ser realizadas según lo convenido con el abonado. Dentro de estas acciones, para este caso, no deben incluir ponerse en contacto con la autoridad de seguridad pública y, si la tecnología lo permite, la activación de los dispositivos de advertencia (WD) en el local supervisado.

Todas las señales de audio recibidas en el centro receptor de alarmas deben ser registradas en el centro receptor de alarmas con la hora y fecha, conservados durante al menos 3 meses y ser capaces de ser reproducidos nuevamente.

Ver en el anexo E un ejemplo de procedimientos para manejo de señales en el centro receptor de alarmas, para sistemas de alarma capaces de proveer confirmación por audio.

7.1.2 Señales de alarma confirmada por audio

Tan pronto como el centro receptor de alarmas llega a la conclusión, según procedimientos acordados, de que los sonidos que emanan del local supervisado son tales que ellos son consistentes con una intrusión o intento de intrusión en el local supervisado, la señal de alarma debe considerarse como que es confirmada por audio.

7.2 Manejo de información de señales provenientes de sistemas de alarmas de intrusión capaces de proporcionar confirmación visual

7.2.1 Visualización

Sólo debe ser posible ver imágenes de un local supervisado en una posición remota después de la recepción de una condición de alarma o la activación de un dispositivo de supervisión de video. Una vez que el centro receptor de alarmas ha visto imágenes y se desconectó, a no ser que se convenga otra cosa con el abonado, no debe ser posible para el centro receptor de alarmas ver imágenes otra vez hasta que una condición de alarma adicional, o una activación dispositivo de supervisión de video adicional, sean recibidas en el centro receptor de alarmas.

Cuando el centro receptor de alarmas entra en contacto con el local supervisado, debe haber una indicación audible o visual en el centro receptor de alarmas que verifica la identidad del local supervisado. Esta identificación debe ser generada desde el equipo localizado en el local supervisado.

El centro receptor de alarmas debe ver todas las imágenes recibidas a consecuencia de una condición de alarma hasta el punto donde la alarma es considerada como visualmente confirmada.

El centro receptor de alarmas debe ver todas las imágenes recibidas a consecuencia de una activación de un dispositivo de supervisión de video hasta el punto donde la activación dispositivo de supervisión de video es tratada como visualmente confirmada.

Si a consecuencia de la inspección de imágenes del local supervisado, el centro receptor de alarmas decide no designar la condición de alarma, como visualmente confirmada, o no tratar la activación dispositivo de supervisión de video como visualmente confirmada, entonces las acciones tomadas por el centro receptor de alarmas deben efectuarse según lo convenido con el abonado. Dentro de estas acciones, para este caso, no deben incluir ponerse en contacto con la autoridad de seguridad pública y, si la tecnología lo permite, la activación de los dispositivos de advertencia (WD) en el local supervisado.

Todas las imágenes recibidas en el centro receptor de alarmas deben ser registradas con la hora y la fecha y guardadas durante al menos 3 meses y ser capaz de ser impresas o mostradas.

Ver en el anexo E un ejemplo de los procedimientos de manejo de alarmas en el centro receptor de alarmas (para sistemas de alarmas capaces de proporcionar confirmación visual).

7.2.2 Señales de alarma visualmente confirmadas

Tan pronto como el centro receptor de alarmas decide que las imágenes que emanan de los locales supervisados corresponden según procedimientos acordados, a una intrusión o intento de intrusión al local supervisado, la señal de alarma debe ser considerada como señal de alarma visualmente confirmada.

Si las imágenes son no concluyentes en cuanto a intrusión o intento de intrusión en el local supervisado, la señal de alarma no debe ser considerada como que es una señal de alarma visualmente confirmada y el centro receptor de alarmas debe esperar la ocurrencia de una alarma secuencialmente confirmada.

7.3 Designación de señales de alarma de sistemas de alarmas de intrusión capaces de proporcionar una confirmación secuencial

Una condición de alarma del primer detector activado debe iniciar la transmisión de una alarma no confirmada al centro receptor de alarmas, por ejemplo Formato Fast "código 3", SIA "BA" o Contact ID "130".

Si un detector independiente se activa posteriormente dentro del tiempo de confirmación entonces una señal de alarma inequívoca secuencialmente confirmada debe ser presentada al operador del centro receptor de alarmas, por ejemplo Formato Fast "código 7", SIA "BV" o Contact ID "139". Si un detector (por ejemplo: independientemente reportando) separado no se activa dentro del tiempo de confirmación entonces el tiempo de confirmación debe reiniciarse automáticamente (ver A.3).

NOTA 1. La transmisión de señales de alarma desde los locales supervisados al centro receptor de alarmas, pueden por ejemplo ocurrir como resultado de iniciaciones separadas del equipo de notificación o como resultado de una iniciación única seguida de una comunicación serial de datos.

NOTA 2. La presentación de una señal de alarma secuencialmente confirmada no ambigua al operador del centro receptor de alarmas significa que el procesamiento de la señal fue hecho por el equipo de control y de señalización o por el equipamiento en el centro receptor de alarmas y no por el operador del centro receptor de alarmas.

Un ejemplo de los procedimientos de manejo de alarma en un centro receptor de alarmas para sistemas de alarma capaces de proporcionar confirmación secuencial se da en el anexo E.

7.4 Filtrado de alarmas

7.4.1 Aplicación de filtrado de alarmas

El centro receptor de alarmas debe aplicar el filtrado de alarma de acuerdo con 7.4.3 a todas las alarmas no confirmadas que no han sido prece-

didadas por una señal de falta de transmisión del mismo local supervisado durante el mismo período de armado hasta un máximo de 96 h.

No es necesario continuar con el filtrado de alarma de alarmas no confirmadas si el centro receptor de alarmas recibe una señal de falta de transmisión del mismo local supervisado durante el mismo período de armado hasta un máximo de 96 h después de que la alarma ha sido recibida.

7.4.2 Autorización de cancelación

La cancelación de una condición de alarma señalizada debe ser individualmente aprobada por el abonado, caso por caso de acuerdo con una rutina definida de filtrado de alarma, por lo cual el usuario o el sistema de alarmas de intrusión se comunican con el centro receptor de alarmas (usando palabras de código convenientes o números) afirmando que el sistema de alarmas de intrusión ha sido operado incorrectamente y que la alarma debe ser eliminada.

NOTA 1. La comunicación por la cual el usuario o el sistema de alarma de intrusión causa una señal de operación incorrecta a ser enviada al centro receptor de alarmas, afirmando que el sistema de alarma de intrusión ha sido operado incorrectamente y por lo tanto que la señalización de la condición de alarma debe ser eliminada luego de filtrada, es un ejemplo de cancelación individual autorizada por el abonado.

NOTA 2. La comunicación por la cual el usuario o el sistema de alarma de intrusión causa una señal de desarmado para ser enviada al centro receptor de alarmas, afirmando que el sistema de alarmas de intrusión ha sido desarmado y por lo tanto que la condición de alarma señalizada es para cancelar, es un ejemplo de cancelación individualmente autorizada por el abonado.

NOTA 3. Esto no imposibilita al centro receptor de alarmas que, aunque el abonado le otorgue una autorización general o específica por un acuerdo escrito previo, que centro receptor de alarmas pueda designar a algunas señales de alarma como inválidas.

7.4.3 Método de filtrado de alarma

Las alarmas no confirmadas pueden tener una demora intencional de hasta 120 s, que es el máximo retardo de filtrado de alarma recomendable, antes de realizar una llamada para verificación. Esta es una oportunidad para que una señal de alarma sea designada como que es una alarma no deseada y por lo tanto cancelada.

lada como parte de la rutina de filtrado de alarma. Si durante el retardo de filtrado de alarma, el centro receptor de alarmas recibe una señal que es identificable como:

- a) señal de operación incorrecta (ver el 3.22); o
- b) indicación de que el sistema de alarma ha sido desarmado;

entonces el centro receptor de alarmas, en ausencia de cualquier indicación contraria, debe designar la condición de alarma señalizada como que es una alarma no deseada y considerar la condición de alarma señalizada como cancelada.

NOTA. Ejemplos de indicaciones contrarias son las evidencias audibles o visuales de una intrusión genuina o un intento genuino de intrusión.

Si una alarma secuencialmente confirmada es recibida durante la demora de filtrado de alarma, entonces la llamada para verificación debe ser retrasada hasta el final de la demora de filtrado de la alarma, como una oportunidad para que la alarma secuencialmente confirmada sea designada como una alarma no deseada, o el retardo puede no ser completado si se cumplen las cuatro condiciones siguientes:

- 1) el centro receptor de alarmas ha consentido de antemano con el abonado en proporcionar la supervisión de armado y desarmado;
- 2) la alarma secuencialmente confirmada es recibida por lo menos 30 minutos después del último tiempo acordado para el armado;
- 3) la alarma secuencialmente confirmada es recibida por lo menos 30 minutos antes del tiempo más temprano que se acordó para el desarmado;
- 4) el centro receptor de alarmas tiene evidencias separadas que indican que el sistema de alarmas de intrusión en el local supervisado está en la condición de armado y ha estado en la condición de armado por al menos 15 minutos.

Cuando un centro receptor de alarmas lleva a cabo la supervisión del armado y desarmado de un sistema de alarmas de intrusión, la auto-

ridad de seguridad pública no debe ser llamada para responder con relación a la desviación del usuario de las listas de tiempo concordadas para armado y desarmado. El centro receptor de alarmas debe ponerse en contacto con el abonado u otro usuario/tenedor de llaves según lo convenido con el abonado.

NOTA 2. Es un asunto entre las partes, cuando los usuarios responsables (o tenedores de llaves) deben ser llamados o no en el evento de una falsa alerta.

La compañía de alarma puede indicar por escrito al abonado, que si una señal de operación incorrecta o una señal de desarmado es recibida por el centro receptor de alarmas, dentro del tiempo de demora de filtrado de alarma especificado, entonces el centro receptor de alarmas debe cancelar la alarma y considerar la alarma como una falsa alerta.

NOTA 3. Durante el filtrado de alarma el centro receptor de alarmas y el usuario responsable o tenedor de llaves pueden contactarse telefónicamente identificándose adecuadamente por medio de contraseñas, para designar la condición de alarma como una alerta falsa y por consiguiente determinar la cancelación. Tal práctica puede ser considerada como opcional (ejemplo: adicional al descrito en 7.4.3) o por acuerdo contractual.

En circunstancias adversas e imprevistas (por ejemplo, condiciones meteorológicas severas o apagones amplios) que afecten la supervisión de alarmas en un centro receptor de alarmas, el procesamiento de alarmas por el centro receptor de alarmas puede verse de vez en cuando retrasado, hasta en el 1,5% de señales recibidas. Es permisible en estas circunstancias que las alarmas sean mantenidas en la demora del filtrado de alarma por un tiempo más largo que 120 s y para que la alarma sea anulada, si una señal de operación incorrecta o una señal de desarmado son recibidas durante el tiempo ampliado de demora del filtrado de alarma, proveyendo que tales extensiones de demora de filtrado de alarma son minimizadas. Debe haber una indicación en el centro receptor de alarmas, disponible al supervisor de centro receptor de alarmas, del número de alarmas mantenidas en espera en la demora de filtrado para facilitar la optimización del recurso humano (operadores) y ponerse en contacto con el personal de reserva (suplentes).

LEONID LLONTOP CASTRO
Jefe de Seguridad Casa Matriz
Banco Ciudad Bs. As

Anexo A (Normativo)

Recomendaciones adicionales para diseño, instalación y configuración

Recomendaciones adicionales para diseño, instalación y configuración de sistema de alarmas de intrusión que incorporen tecnología de confirmación de alarmas.

A.1 Equipo auxiliar de control portátil utilizado para armado y desarmado

A.1.1 Generalidades

El equipo auxiliar de control portátil utilizado para el armado y desarmado del sistema de alarmas de intrusión debe:

- a) requerir una sola acción manual para el desarmado;
- b) ofrecer un grado de seguridad mayor o igual que 1 000 000 de combinaciones diferentes;
- c) emplear un código rotativo en aquellas circunstancias en que un usuario pueda completar el procedimiento de desarmado desde una posición de más de 1 m de distancia del receptor;
- d) no incluir en el equipo auxiliar de control portátil el dispositivo de asalto o el de emergencia médica, ni aún en canales independientes.

Las recomendaciones para la tecnología de radio empleada por el equipo auxiliar de control portátil están dadas en A.1.2. Sin embargo, otras tecnologías pueden ser usadas (por ejemplo, infrarrojo, etiquetas de proximidad, tarjetas de control de acceso y otros dispositivos de acción simple).

Debe haber una indicación adecuada que proporcione el reconocimiento de que la operación de armado o el desarmado hayan sido completados con éxito.

Si se produce una condición de baja tensión de batería, el equipo auxiliar de control portátil autoalimentado debe reportar la condición al equipo de control y de señalización (si es aplicable vía el equipo auxiliar de control), cada vez que el equipo auxiliar de control portátil sea usado para el desarmado. Mientras la condición de baja tensión de batería existiese, este informe debe ser hecho en cada acontecimiento de desarmado para un mínimo de 25 acontecimientos, durante un período que no exceda de 1 mes. Cada vez que se reporta batería baja, debe haber una indicación de batería baja en el equipo donde la finalización del procedimiento de desarmado es llevado a cabo (equipo de control y de señalización o equipo auxiliar de control) y el sistema de alarmas de intrusión no debe armarse hasta que la indicación de batería baja haya sido reconocida manualmente en el equipo de control y de señalización o equipo auxiliar de control. Los informes de batería baja y la admisión manual deben ser registrados en el equipo de control y de señalización e identificar a los usuarios relevantes.

Los receptores deben ser alojados en el equipo de control y de señalización o en un alojamiento separado (que puede ser el alojamiento del equipo auxiliar de control) cumpliendo las exigencias para ubicación, alojamiento y suministro de energía aplicable al equipo de control y de señalización.

La interconexión entre el receptor y el equipo de control y de señalización debe ser eléctricamente y mecánicamente protegida.

LEONID LLONTOP CASTRO
Jefe de Seguridad Casa Matriz
Banco Ciudad Bs. As

A.1.2 Equipo auxiliar de control portátil inalámbrico

Debe ser minimizada la posibilidad de alarmas no deseadas, debido a un mal funcionamiento técnico o a un diseño pobre de los equipos.

Deben proporcionarse técnicas de verificación para asegurar la integridad de la señal para minimizar la posibilidad de alarmas no deseadas en presencia de ruido impulsivo por interferencia y transitorios.

Los componentes no deben ser adversamente afectados por interferencia de radiofrecuencia o eléctrica en el ambiente, incluso aquellos que puedan instalarse o que puedan ser instalados en un futuro cercano.

La posibilidad de no operación debido a interferencia mutua debe ser minimizada y el sistema de transmisión utilizado debe minimizar los efectos de la interferencia mutua mediante el uso de receptores de banda angosta y técnicas de verificación y codificación.

El elemento de recepción, por ejemplo la antena o el transductor deben protegerse contra daño mecánico.

Debe tenerse especial cuidado en el montaje de la antena del receptor para asegurar una recepción satisfactoria de señales y para minimizar la recepción accidental o deliberada de señales interferentes. La conexión entre una antena y un receptor debe ser protegida contra el daño casual.

A.2 Detección de manipulación indebida o de sabotaje

Se recomienda que el dispositivo de supervisión de audio, dispositivo captador de audio, dispositivo de supervisión de videos y los dispositivos de captura de imágenes, y el circuito de interconexiones para estos dispositivos estén provistos de detección de manipulación indebida o de sabotaje o de acuerdo con normas aplicables.

La detección de pérdida de video puede ser utilizada como un medio para proveer detección de manipulación indebida o de sabotaje.

A.3 Reinicio del tiempo de confirmación del sistema de alarmas de intrusión

A.3.1 Sistema de alarmas de intrusión que incorpora solo tecnología de confirmación secuencial

Si luego del armado de un sistema de alarmas de intrusión diseñado con tecnología de confirmación secuencial, se produjera una activación de un detector de dicho sistema, esta acción debe considerarse como una alarma no confirmada y como consecuencia debe comenzar el tiempo de confirmación.

Si durante el tiempo de confirmación, no se activa un segundo detector independiente (ver 5.4.1) y el tiempo de confirmación expira, el sistema de alarmas de intrusión debe volver a su condición inicial de modo que si otra vez un detector se activa, se genera una nueva alarma no confirmada y el tiempo de confirmación comienza nuevamente.

NOTA. Si se desarma el sistema de alarma de intrusión antes de que expire el tiempo de confirmación, cesa todo proceso de confirmación.

En el caso en que un detector(es) permanezca(n) en la condición de alarma al vencimiento del tiempo de confirmación, al no enviar el equipo de control y de señalización una señal de restitución, el centro receptor de alarmas debe informar al usuario responsable que el detector(es) en el sistema de alarmas ha(n) sido inhibido(s).

Para sistemas en los que en el desarmado la puerta inicial de entrada es inhibida debido a estar abierta en el momento del reinicio del tiempo de confirmación del sistema de alarma de intrusión, se recomienda que el tiempo de entrada comience por otros medios. El sistema de alarma de intrusión debe ser configurado tal que la notificación de cualquier alarma e iniciación del tiempo de confirmación sea retrasado hasta la finalización del tiempo de entrada total. Si una alarma ocurre como consecuencia de la finalización del tiempo de entrada total, la condición de alarma debe notificarse como una alarma no confirmada.

El proceso de reinicio del tiempo de confirmación no debe eliminar una condición de alarma, de modo que cuando el sistema de alarma de intrusión es desarmado debe haber una indicación en el equipo de control y de señalización de que una condición de alarma ha ocurrido y que se requiere una restauración (ver A.4).

Si el primer detector en activarse durante el período de armado se activa otra vez dentro del tiempo de confirmación, el tiempo de confirmación puede ser reanudado en el momento que ocurra la segunda activación, y de ser consensuado entre todas las partes involucradas (usuario, compañía de alarmas, etc.) se reiniciará el tiempo de confirmación para cada activación futura de este detector. Esto podría ser posible utilizando el reporte de formato detallado (3.14). Cada activación del primer detector debe generar una alarma no confirmada.

El número de eventos registrados de cualquier origen debe ser limitado a tres durante cualquier período de confirmación, por lo tanto el número de eventos registrados de cualquier origen simple puede exceder de tres durante cualquier período de armado.

A.3.2 Sistema de alarmas de intrusión que incorpora tecnología de confirmación secuencial y una u otra tecnología de confirmación por audio y/o visual

Para sistemas de alarma de intrusión que incorporan tecnología de confirmación secuencial y una u otra tecnología de confirmación por audio y/o visual, las recomendaciones dadas en A.3.1 deben aplicarse respecto de la tecnología de confirmación secuencial.

Las señales de alarmas recibidas por el centro receptor alarmas del sistema de alarma de intrusión que incorpora la tecnología de confirmación por audio y/o visual, deben ser alarmas no confirmadas hasta que sean designadas por el centro receptor de alarmas como audiblemente o visualmente confirmadas.

Si una alarma no confirmada no es designada como confirmada por el centro receptor de alarmas, el sistema de alarma de intrusión debe ser capaz de seguir notificando alarmas al centro receptor de alarmas, de detectores que se han activado así como de detectores que no se han activado previamente.

Si el centro receptor de alarmas no designa la alarma no confirmada como confirmada por audio o visualmente confirmada, el centro receptor de alarmas debe esperar normalmente a ver si una alarma secuencialmente confirmada se presenta dentro del tiempo de confirmación. El operador del centro de recepción de alarmas puede sin embargo restablecer el sistema de alarma de intrusión antes del vencimiento del tiempo de confirmación, siempre que la tecnología lo permita y haya acuerdo escrito específico con el abonado.

Si el centro receptor de alarmas no toma la decisión de considerar la activación del dispositivo de supervisión de audio como confirmada por audio o la activación del dispositivo de supervisión de video como visualmente confirmada, el centro receptor de alarmas debe esperar normalmente a ver si una alarma secuencialmente confirmada se presenta dentro del tiempo de confirmación. El operador del centro receptor de alarmas puede sin embargo, restablecer el sistema de alarma de intrusión antes

del vencimiento del tiempo de confirmación, siempre que la tecnología lo permita y haya acuerdo escrito específico con el abonado.

El centro receptor de alarmas puede aislar detectores que dan alarmas reiteradas, por ejemplo debido a una falla, si hay acuerdo escrito específico con el abonado. El centro receptor de alarmas debe comunicar cada caso de aislamiento de detector al tenedor de llaves autorizado cuanto antes.

El centro receptor de alarmas puede aislar dispositivos de supervisión de audio o dispositivos de supervisión de video en ocasión de alarmas reiteradas, por ejemplo debido a una falla, si hay un acuerdo escrito específico con el abonado. El centro receptor de alarmas debe comunicar cada caso de aislamiento de dispositivos de supervisión de audio o de dispositivos de supervisión de video al tenedor de llaves autorizado cuanto antes.

A.4 Restablecimiento luego de una condición de alarma

Luego de una alarma no confirmada se recomienda restablecer nuevamente el sistema de alarma, salvo que se haya verificado un mal funcionamiento o falla que deba ser corregida.

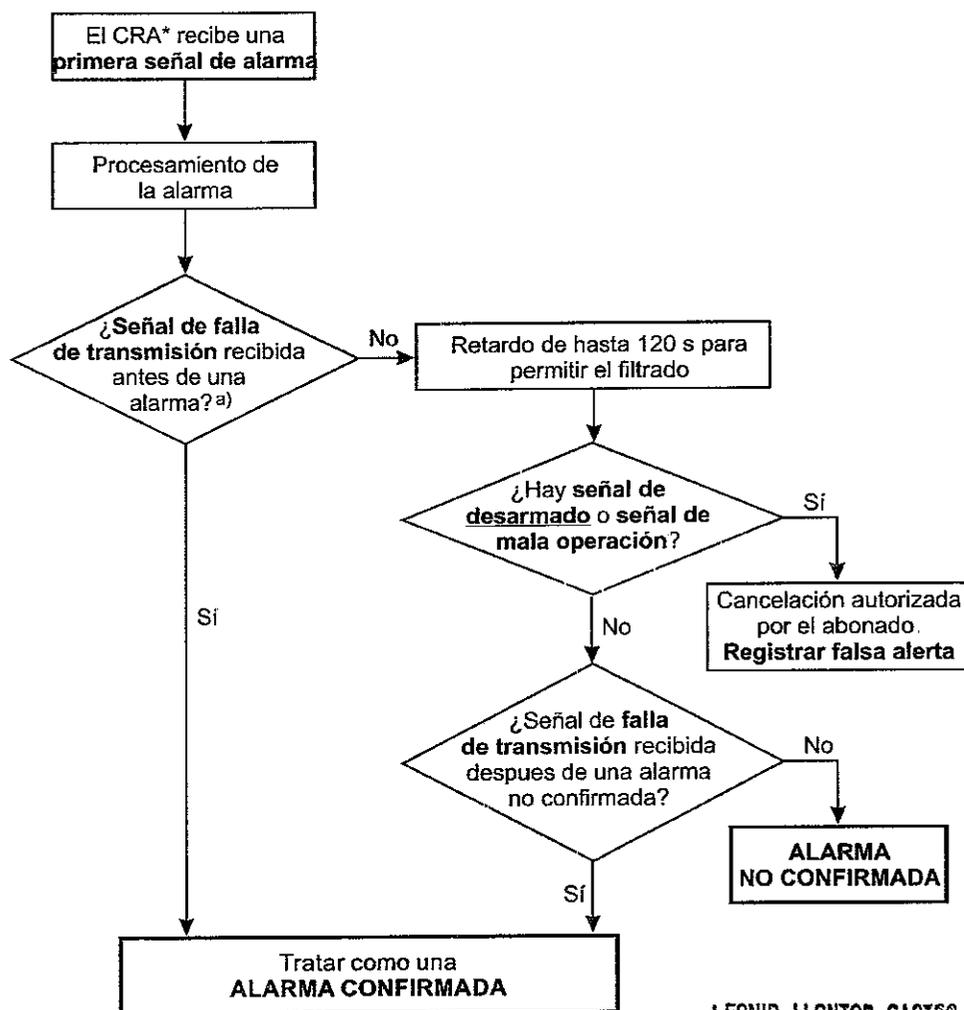
LEONID LLONTOP CASTRO
Jefe de Seguridad
Banco Ciudad S.A.

Anexo B
(Informativo)

Ejemplo de los procedimientos de manejo de señales de alarmas en el centro receptor de alarmas (CRA) para señales de alarmas asociadas con la falla de las señales de transmisión

En la figura B.1 se da un ejemplo de un procedimiento de manejo de señales de alarmas en el centro receptor de alarmas asociado con señales de falla de transmisión.

NOTA. Esta figura no ilustra el proceso total de confirmación de alarma.



LEONID LLONTOP CASTRO
Jefe de Seguridad Casa Matriz
Banco Ciudad Bs As

* CRA: centro receptor de alarmas

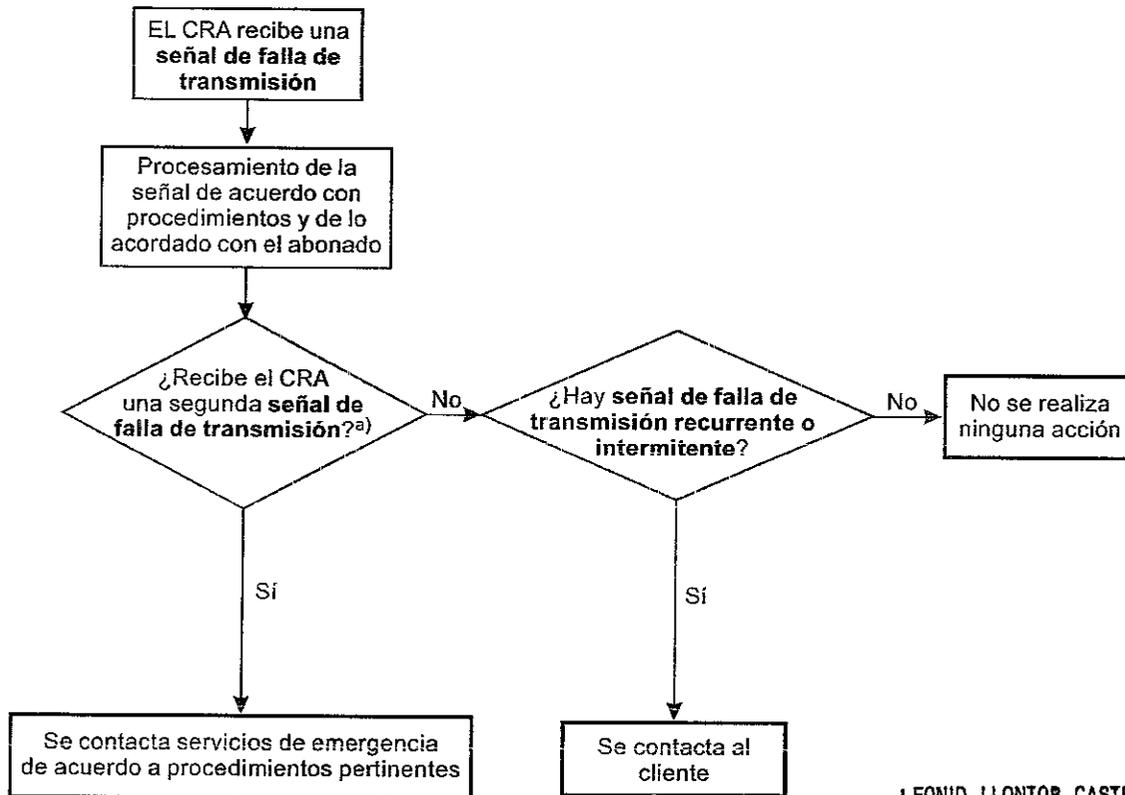
a) Señal de falla de transmisión recibida desde el mismo local supervisado durante un periodo simple de armado de un máximo de 96 h

Figura B.1 - Ejemplo de procedimiento de manejo de señales de alarmas asociadas con señales de fallas de transmisión

Anexo C
(Informativo)

Procedimientos en el centro receptor de alarmas para el manejo de dos señales de falla de transmisión

En la figura C.1 se da un ejemplo de los procedimientos de manejo del centro receptor de alarmas de dos señales de falla de transmisión provenientes de vínculos de transmisión diferentes.



LEONID LLONTOP CASTRO
Jefe de Seguridad Casa Matriz
Banco Ciudad Bs As

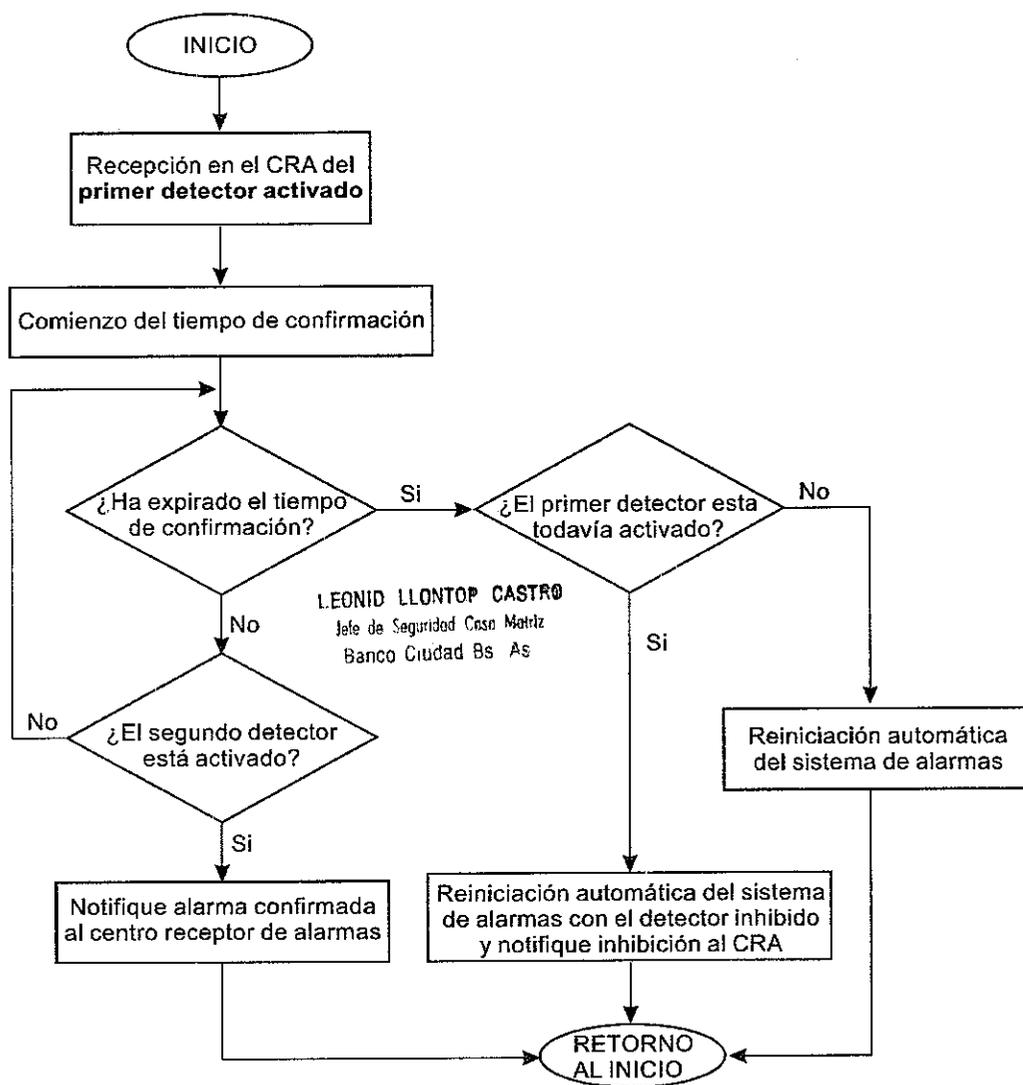
a) Corresponde a una segunda señal de falla de transmisión recibida del mismo local supervisado, a través de vías de transmisión de diferente tecnología durante un periodo simple de armado de hasta un máximo de 96 h.

Figura C.1 - Ejemplo de un procedimiento en el centro receptor de alarmas del manejo de dos señales de falla de transmisión

Anexo D (Informativo)

Requisitos operacionales para un sistema de alarmas de intrusión equipado con tecnología de confirmación secuencial

La figura D.1 muestra un ejemplo de los requisitos operacionales para un sistema de alarmas de intrusión equipado con tecnología de confirmación secuencial.



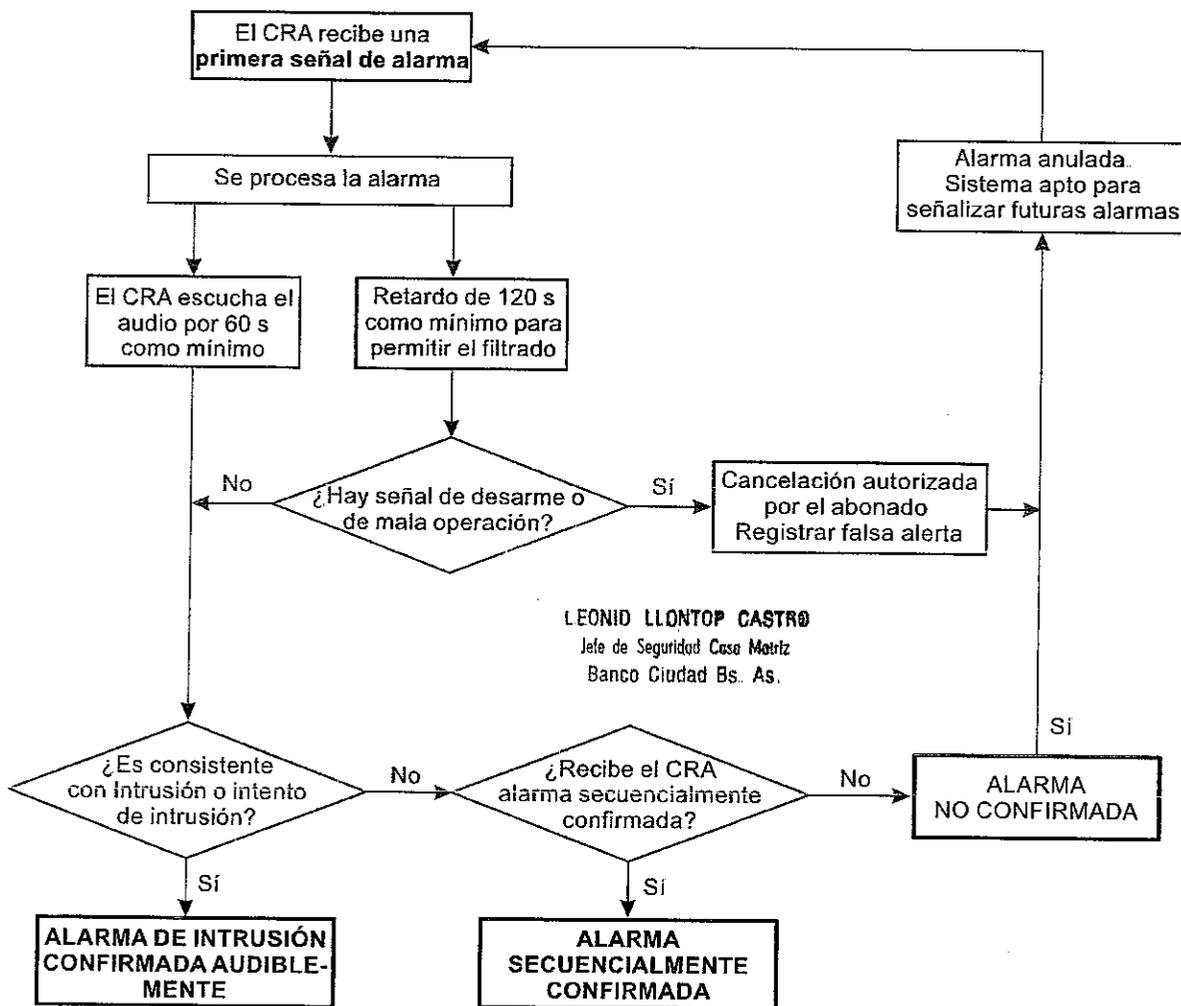
NOTA. La Indicación audible interna es opcional. Dispositivos de advertencia audibles operan en algunas etapas. No se aplica retardos en la operación de los dispositivos de advertencia audibles si ellos operan cuando ocurre una alarma no confirmada. Un retardo en la operación de los dispositivos de advertencia audibles puede aplicarse si ellos solo operan cuando ocurra una alarma confirmada

Figura D.1 - Ejemplo de requisitos operacionales para un sistema de alarmas de intrusión equipado con tecnología de confirmación secuencial

Anexo E (Informativo)

Procedimientos del centro receptor de alarmas para sistemas de alarma capaces de proveer confirmación

En las figuras E.1, E.2 y E.3 se dan ejemplos de manejo de los procedimientos en el centro receptor de alarmas para sistemas de alarma capaces de proveer confirmación.



NOTA. En la actualidad estos sistemas están siendo poco utilizados.

Figura E.1 - Ejemplo de procedimientos de manejo de alarmas para sistemas de alarma por confirmación por audio

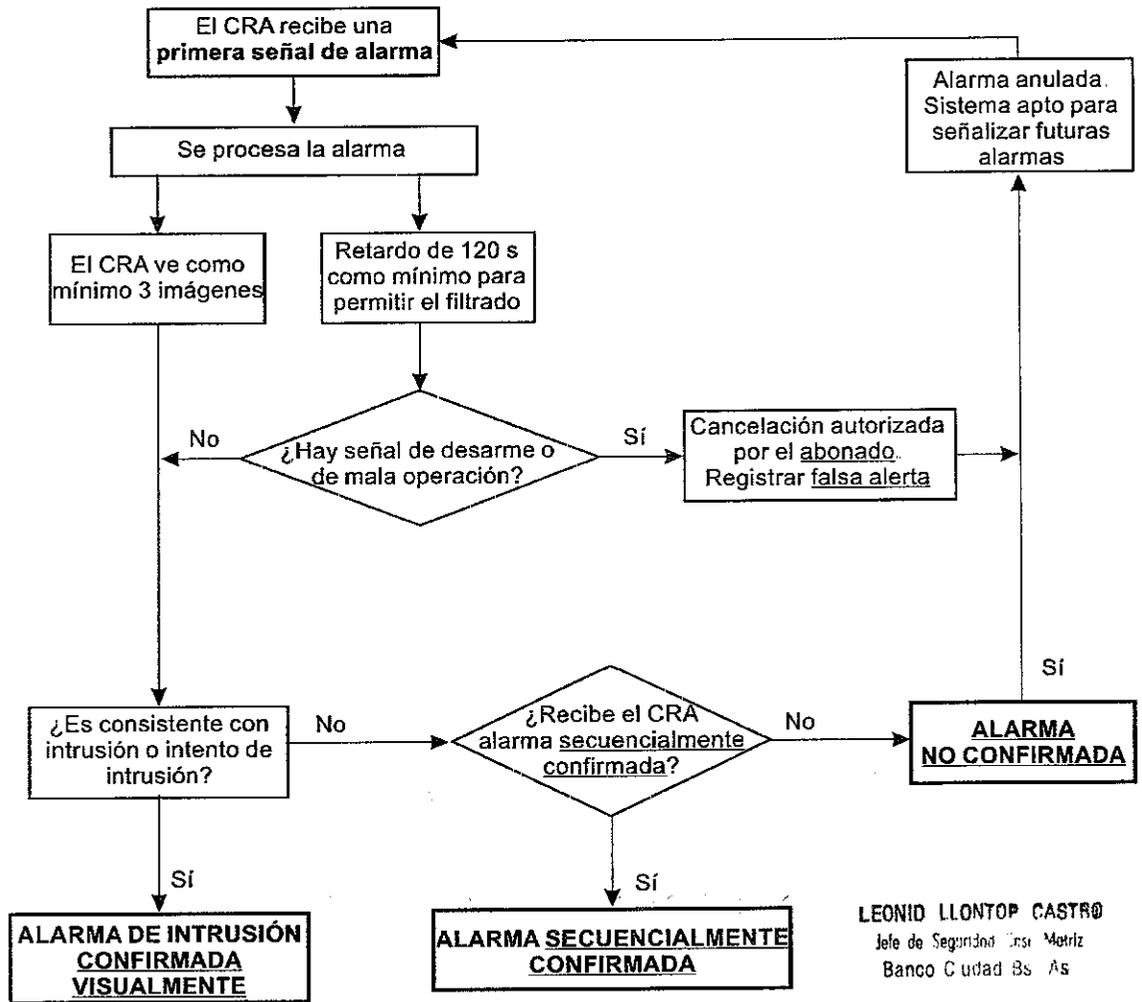


Figura E.2 - Ejemplo de procedimientos de manejo de alarmas para sistemas de alarma con confirmación por video

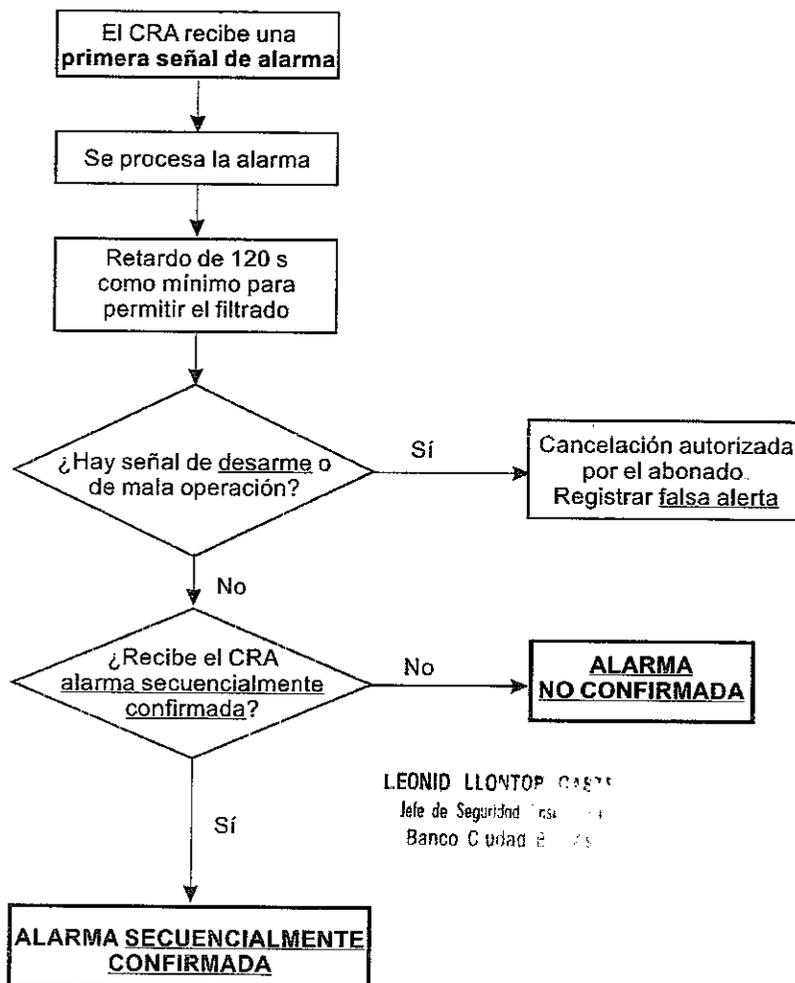


Figura E.3 - Ejemplo de procedimientos de manejo de alarmas para sistemas de alarma con confirmación secuencial

Anexo F (Informativo)

Información recomendada a ser incluida en la propuesta de diseño del sistema y en los documentos adjuntos

F.1 Propuesta de diseño del sistema

Se recomienda incluir la información siguiente en la propuesta de diseño de sistema:

- a) cuando se proponga un medio único de transmisión para el sistema de alarmas de intrusión (ver 4.3), se recomienda incluir una advertencia, en negrita, como sigue:

“IMPORTANTE

Prestar atención a que si hay una falla en el único medio de transmisión, ésta no será notificada la autoridad de seguridad pública. Mientras la falla persista, no podrán transmitirse las alarmas subsecuentes al centro de recepción de alarmas y notificarlas a la autoridad de seguridad pública.”;

- b) las partes especificadas del local supervisado que tengan o no una efectiva confirmación de alarmas (ver 5.1.2);
- c) el alcance, extensión y cobertura de cualquier instalación de confirmación por audio (ver 5.2.1) incluso aquellas áreas del local supervisado que están dentro del rango y proximidad esperado del dispositivo captador de audio;
- d) el alcance, extensión y cobertura de cualquier dispositivo de supervisión de audio (ver 5.2.3) incluyendo aquellas áreas dentro del local supervisado que están dentro del rango y proximidad esperada del dispositivo de supervisión de audio;
- e) el alcance, extensión y cobertura de cualquier dispositivo de confirmación visual (ver 5.3.1), incluyendo aquellas áreas dentro del local supervisado que están dentro del campo de visión de los dispositivos de visualización de imágenes;
- f) especificar y explicar los parámetros operacionales de las características secuenciales del sistema de alarma (ver 5.4.5), incluyendo lo siguiente:
- 1) establecer claramente que si hay combinación de detectores, cuando más de uno de ellos reporta una condición de alarma, no producen un mensaje de alarma confirmada,
 - 2) establecer claramente el tiempo de confirmación (debe ser no menos de 30 minutos y no más de 60 minutos.);
- g) una descripción de la opción de desarmado seleccionada para el sistema de alarmas de intrusión (ver 6.4.);
- h) si se utiliza desarmado automático por tiempo, detallar cuando el sistema de alarmas de intrusión ha sido desarmado y como queda la seguridad del local hasta que los usuarios lleguen.

F.2 Documento adjunto

Lo siguiente es información que se recomienda incluir en el documento adjunto:

- a) cuando se proponga para el sistema de alarmas de intrusión (ver 4.3) un medio único de señalización, se recomienda incluir la siguiente advertencia en negrita:

“IMPORTANTE

Prestar atención a que una falla o un compromiso en la señalización de un medio único de transmisión, no puede ser enviado a la autoridad de seguridad pública. Mientras la falla persista, no pueden señalizarse alarmas subsecuentes al centro de recepción de alarmas y enviarlas a la autoridad de seguridad pública.”;

- b) las partes especificadas del local supervisado que tienen o no tienen la instalación de confirmación eficaz (ver 5.1.2);
- c) el alcance, extensión y cobertura de cualquier instalación de confirmación por audio (ver 5.2.1), incluso aquellas áreas del local supervisado que están dentro del rango y proximidad esperado del dispositivo captador de audio;
- d) el alcance, extensión y cobertura de cualquier dispositivo de supervisión de audio (ver 5.2.3) incluyendo aquellas áreas dentro del local supervisado que están dentro del rango y proximidad esperada del dispositivo de supervisión de audio;
- e) el alcance, extensión y cobertura de cualquier dispositivo de confirmación visual (ver 5.3.1), incluyendo aquellas áreas dentro del local supervisado que están dentro del campo de visión de los dispositivos de visualización de imágenes;
- f) especificar y explicar los parámetros operacionales de las características secuenciales del sistema de alarma (ver 5.4.5), incluyendo lo siguiente:
- 1) establecer claramente si hay combinación de detectores que, cuando más de uno de ellos reporta una condición de alarma, no producen un mensaje de alarma confirmada,
 - 2) establecer claramente el tiempo de confirmación (debe ser no menos de 30 minutos y no más de 60 minutos);
- g) una descripción de la opción de desarmado seleccionada para el sistema de alarmas de intrusión (ver 6.4);
- h) si se utiliza desarmado automático por tiempo, detallar cuando el sistema de alarmas de intrusión ha sido desarmado y como queda la seguridad del local hasta que los usuarios lleguen.

LEONID LLONTOP CASTRO
Jefe de Seguridad Casa Moritz
Banco Ciudad Bs. As.

Anexo G
(Informativo)

Bibliografía

En el estudio de este proyecto se ha tenido en cuenta el antecedente siguiente:

BSI - BRITISH STANDARDS INSTITUTION

BS DD 243:2004 - Installation and configuration of intruder alarm systems designed to generate confirmed alarm conditions-Code of practice.

Anexo H (Informativo)

Integrantes de los organismos de estudio

El estudio de esta norma ha estado a cargo de los organismos respectivos, integrados en la forma siguiente:

Subcomité de Sistemas de alarmas

Integrante	Representa a:
Ing. Gabriel BENHABIB	GENERAL INDUSTRIES ARG. S.A. / PROSEGUR
Ing. Héctor BLANCO	TECNOLOGÍA DE ARGENTINA S.A. ASOCIACIÓN ARGENTINA DE SEGURIDAD PRIVADA (AASPRI) / FACULTAD DE CIENCIAS DE LA SEGURIDAD I.U.P.F.A.
Sr. Héctor BUCIARDI	H.B. SEGURIDAD Y CUSTODIA S.R.L.
Sr. Carlos CASTRO	SEGURIDAD PRIVADA INTEGRAL
Sr. Pablo CORONEL	POLICÍA DE LA PROVINCIA DE BUENOS AIRES
Lic. Walter COSTA	CEMARA-SESYTEL SRL
Ing. Jorge DI BLASI	POLICÍA METROPOLITANA
Sr. Julio FUMAGALU	CEMARA
Sr. Ricardo GARABELLO	SISTEMAS ELECTRÓNICOS APLICADOS S.R.L.
Arq. Eduardo GONZÁLEZ	SAF/ ARQUIDOMO
Sr. Ricardo GONZALEZ	CEMARA
Sr. Alberto GUTIERREZ	ASOCIACIÓN ARGENTINA DE SEGURIDAD PRIVADA (AASPRI)
Sr. Martín HANONO	PYRONIX LTD.
Lic. Gustavo HASPERVE	POLICÍA DE LA PROVINCIA DE BUENOS AIRES
Ing. Ricardo KATZ	CEMARA
Sr. Ricardo MARQUEZ	CÁMARA ARGENTINA DE LA SEG. ELECTRÓNICA
Coronel Pablo MARTÍN	POLICÍA DE LA PROVINCIA DE BUENOS AIRES
Ing. Modesto MIGUEZ	CENTRAL DE MONITOREO S.A.
Ppal. Alberto OBREGÓN	POLICÍA FEDERAL ARGENTINA. DIV. ALARMAS
Sr. Sandro ORTIZ	POLICÍA METROPOLITANA
Ing. Luciano OTERO	POLICÍA METROPOLITANA
Subcrio. Norberto PLAQUIN	POLICÍA FEDERAL ARGENTINA
Ing. Mario REBORI	POLICÍA DE LA PROVINCIA DE BUENOS AIRES. CENTRO DESPACHO EMERGENCIAS 911. LANÚS
Prof. Carlos REISZ	C.F. REISZ Y ASOCIADOS / ASOCIACIÓN ARGENTINA DE SEGURIDAD PRIVADA (AASPRI) / MARCODINA S.A.
Capitán Manuel RIVAS	POLICÍA DE LA PROVINCIA DE BUENOS AIRES. CENTRO DESPACHO EMERGENCIAS 911. LANÚS
Ing. Mario SALATINO	POLICÍA METROPOLITANA
Ing. Sergio SUTIN	MINISTERIO DE SEGURIDAD POLICÍA PROV. BS. AS
Ing. Fernando SOLARI	CEMARA-NIKRO S.A.
Ing. Adolfo BERGANZA	IRAM
Ing. Rita MANSOUR	IRAM

LEONID LLONTOP CASTRO
Jefe de Seguridad Casa Matriz
Banco Ciudad Bs As

Comité General de Normas (C.G.N.)

Integrante

Ing. Juan C. ARCIONI
Ing. Roberto BARNEDA
Ing. Samuel MARDYKS
Dr. Mario PECORELLI
Ing. Raúl DELLA PORTA

IRAM 4177:2012

ICS 13.310
* CNA 6350

LEONID LLONTOP CASTRO
Jefe de Seguridad Casa Matriz
Banco Ciudad Bs. As

* Corresponde a la Clasificación Nacional de Abastecimiento asignada por el Servicio Nacional de Catalogación del Ministerio de Defensa.

IRAM 3860-1:2011

ICS 13.310; 91.040.20
* CNA 00.00

LEONID LLONTOP CASTRO
Jefe de Seguridad Casa Matriz
Banco Ciudad Bs. As.

* Corresponde a la Clasificación Nacional de Abastecimiento asignada por el Servicio Nacional de Catalogación del Ministerio de Defensa