OFICINA NACIONAL DE SEGURIDAD

OR-ASIP-01-02.04

ORIENTACIONES PARA LA CONSTITUCIÓN DE ZONAS DE ACCESO RESTRINGIDO

ÍNDICE

1. INTRODUCCIÓN

El presente documento de **Orientaciones para la constitución de Zonas de Acceso Restringido** se elabora como complemento de la norma NS/03, sobre Seguridad Física, de las Normas de la Autoridad Nacional para la protección de la información clasificada, y conforme se especifica en el apartado **8.1** de la misma.

En él se describen los estándares de medidas de seguridad para la protección de zonas donde se almacena o maneja información clasificada, aprobados por la Autoridad Nacional para la Protección de la Información Clasificada (ANPIC), a aplicar según el grado de clasificación y otras condiciones que sea preciso atender.

Los conceptos tratados en la norma NS/03 de seguridad física, que aquí no se desarrollan con el mismo nivel de detalle, deberán ser conocidos y tenidos en cuenta, previamente a la aplicación de lo indicado en estas orientaciones. Se han incluido algunos de dichos conceptos, para una mayor claridad expositiva, especialmente las medidas específicas de seguridad física.

La seguridad deberá ser concebida de forma global, mediante una combinación de medidas físicas complementarias que garanticen un grado de protección suficiente, coordinando su aplicación con el resto de medidas de seguridad: seguridad en el personal, seguridad de la información y seguridad en los sistemas de información y comunicaciones.

Estas orientaciones son de aplicación principalmente para instalaciones fijas o semipermanentes. En las instalaciones móviles, por motivos operacionales o de ejercicios, especialmente en el ámbito de Fuerzas Armadas, se presupone que las medidas de seguridad física adoptadas por el jefe de la unidad son las correctas, y son suficientes y acordes a la situación.

2. CONCEPTO DE DEFENSA EN PROFUNDIDAD

La seguridad se constituye según un esquema de defensa en profundidad, en diferentes entornos sucesivos. Se distinguen los siguientes entornos, definidos en la norma NS/03:

- **Entorno Global de Seguridad (EGS)**: El perímetro o perímetros de seguridad exteriores, que es necesario sobrepasar para llegar a la propia Zona de Acceso Restringido.

- **Entorno Local de Seguridad (ELS):** Viene referido a la seguridad inmediata e interior de la propia zona de acceso restringido, por lo que incluye las medidas instaladas en las zonas adyacentes a la misma, en los propios paramentos y accesos, así como en el interior de la propia instalación, impidiendo el acceso a la información clasificada allí manejada.

- **Entorno de Seguridad Electrónico (ESE):** Medidas implementadas para evitar fugas de información relacionadas con fenómenos TEMPEST, o establecidas contra escuchas activas o pasivas, o para impedir la manipulación de los equipos en que se maneja información clasificada.

3. ZONAS DE SEGURIDAD

3.1. Zonas de acceso restringido

Son instalaciones donde se almacena o maneja Información Clasificada de grado "CONFIDENCIAL o equivalente" o superior, por lo que deberán contar con las medidas y procedimientos de seguridad adecuados y suficientes, para asegurar la protección de la información clasificada en todo momento.

Deberán estar organizadas conforme a alguna de las siguientes configuraciones de trabajo:

a) **ÁREA CLASE I**: zona en la que se maneja y almacena información clasificada de tal forma que la entrada a la zona supone, a todos los efectos, el acceso a la información clasificada, por lo que sólo puede acceder personal debidamente habilitado y autorizado.

b) **ÁREA CLASE II**: zona en la que se maneja y almacena información clasificada de tal forma que pueda estar protegida del acceso de personas no autorizadas mediante controles establecidos internamente, por lo que se podrá admitir la entrada a personal visitante debidamente controlado.

Las organizaciones deberán designar un responsable de seguridad de zona de acceso restringido.

Una zona de acceso restringido siempre estará bajo el control de un órgano de control (servicio de protección de información clasificada, subregistro o punto de control).

3.2. Zona administrativa de protección

Son instalaciones con un perímetro claramente definido dentro del cual existe un control de las personas, material y vehículos. En estas zonas administrativas de protección sólo se manejará y almacenará información hasta el grado de "DIFUSIÓN LIMITADA o equivalente", con las excepciones que se establecen en las normas de la Autoridad Nacional o de forma puntual.

Estas zonas quedan fuera del ámbito de este documento, siendo tratadas en las orientaciones OR-ASIP-04-01, sobre manejo de información clasificada con grado de "DIFUSIÓN LIMITADA o equivalente"

4. ACREDITACIÓN DE UNA ZONA DE ACCESO RESTRINGIDO

La acreditación es el reconocimiento, mediante certificado escrito, de la capacidad de un determinado local, edificio, oficina, habitación u otra área para que en el mismo se pueda almacenar o manejar información clasificada, en unas condiciones establecidas, constituyéndose como zona de acceso restringido.

El certificado de acreditación de locales (CAL) correspondiente que se emite, es la autorización expresa que se otorga a la instalación, configurada como área clase I ó área clase

II, y que especifica los tipos (origen) y grado máximo de clasificación de la información clasificada que puede ser almacenada o manejada en la misma.

La acreditación de una zona de acceso restringido exigirá la elaboración previa, por parte del responsable de seguridad de la zona de acceso restringido, del **plan de protección**.

Dicho plan, en lo posible se deberá redactar conforme al modelo elaborado por la Oficina Nacional de Seguridad, órgano de trabajo de la Autoridad Nacional, en el documento de orientaciones **OR-ASIP-01-01** sobre el Plan de Protección de una ZAR, con sus tres documentos básicos:

- Informe de instalaciones.
- Procedimientos de seguridad.
- Plan de emergencia.

El jefe de seguridad del órgano de control (servicio de protección de información clasificada, subregistro o punto de control) bajo cuyo control esté la zona de acceso restringido, será responsable de verificar y declarar que el plan de protección es completo, correcto y está adecuadamente implantado. Cuando el propio jefe de seguridad sea a su vez responsable de seguridad de la zona de acceso restringido, la responsabilidad será del jefe de seguridad del órgano de control superior.

5. MEDIDAS ESPECÍFICAS DE SEGURIDAD FÍSICA

5.1. Medidas Estructurales

5.1.1. Perímetro de Seguridad

Una cierre perimetral es una barrera física que identifica el área que requiere protección o recinto de seguridad. El nivel de protección ofrecido por un cierre dependerá de su altura, construcción, material utilizado y las características empleadas para incrementar su efectividad, así como los elementos adicionales instalados en el mismo, como: alambradas, sistemas de detección de intrusión, alumbrado de seguridad ó un circuito cerrado de televisión.

Los cierres deberán ser rectilíneos, de forma que permita una vigilancia visual sin obstáculos, sin huecos o discontinuidades y anclados a tierra. Como mínimo deberán contar con 2,15 metros de altura, dejando una zona despejada de 25 metros alrededor de los mismos, cuando sea factible.

Los propios muros de los edificios, cuando reúnan las características necesarias de fortaleza y protección, podrán constituir, parcial o totalmente, el perímetro de seguridad, siempre que formen parte del entorno global de seguridad, pero **no del entorno local de seguridad**. En este último caso no puede hablarse de perímetro de seguridad.

En edificios de varias plantas, los muros exteriores de las plantas inferiores pueden tener la consideración de perímetro de seguridad, siempre que cumplan los criterios indicados arriba. Los conductos y ventanas deben cumplir los requisitos que se indican posteriormente en los apartados **5.1.6** y **5.1.7**, en función de su altura o distancia a posibles puntos de acceso ilegal.

5.1.2. Paramentos horizontales y verticales

Los muros, suelos y techos de una zona de acceso restringido serán de construcción permanente y estarán unidos los unos con los otros. La construcción debe evidenciar de manera visible la imposibilidad de un acceso no autorizado.

Se deberán proteger convenientemente los espacios que dan acceso a falsos suelos y techos.

La construcción debe estar realizada de tal manera que provea evidencia visual inmediata de cualquier intento de penetración no autorizado. En este sentido es conveniente que los paramentos sea visitables exteriormente, para verificar su estado en las rondas de seguridad que se realicen, especialmente si no hay otros medios electrónicos de detección o visualización de intentos de intrusión.

5.1.3. Puertas

Las puertas que dan acceso a zonas de acceso restringido estarán compuestas de madera maciza, metal u otro material sólido. Su superficie no presentará huellas de golpes o raspaduras con el objeto de que sea posible detectar un intento de penetración.

Las bisagras y sus correspondientes pivotes se montarán hacia el interior, o bien se soldarán o fijarán con abrazaderas para impedir que la puerta pueda ser arrancada. Los marcos y las fijaciones deberán ser tan sólidos como la misma puerta.

Las puertas deberán cerrarse cuando no estén en uso y controlarse cuando se estén utilizando. Se instalarán dispositivos automáticos de cierre de puertas, como por ejemplo cierra-puertas o muelles telescópicos, que tiendan a mantener las puertas cerradas una vez franqueado el paso por las mismas.

5.1.4. Puertas de emergencia

Se deberá controlar el uso de las puertas de emergencia en las zonas de acceso restringido, limitando el acceso y salida por las mismas exclusivamente a los casos de emergencia o ensayo. Siempre que sea posible, se utilizarán puertas del tipo anti pánico, de composición y fortaleza equivalente a las puertas habituales de acceso a la zona. Para abandonar el recinto, los usuarios deberán presionar en la barra anti pánico retrayendo el pestillo para la apertura de la puerta.

Se instalarán dispositivos magnéticos que permitan detectar una inapropiada apertura de las puertas, estos sistemas deberán dotarse de sistemas anti sabotaje.

5.1.5. Cerraduras

Las cerraduras deberán ser de alta seguridad con, al menos, 5 puntos de cierre al frente.

En el caso de las puertas a las que no se accede frecuentemente, una cerradura mecánica de llave multipunto es la solución más económica y menos propensa a los problemas técnicos.

Las cerraduras electrónicas o electromagnéticas son utilizadas asociadas a los sistemas de control de acceso. La selección de la cerradura dependerá de la configuración y modelo de la puerta. Se presentan en distintos modelos y estilos: eléctricas, electromagnéticas o de pernos.

Los términos **"*Fail Safe*"** (normalmente abierto) y **"*Fail Secure*"** (normalmente cerrado) son frecuentemente utilizados en aplicaciones de seguridad para definir la manera en la que las cerraduras y los dispositivos de señal trabajan cuando se asocian con sistemas de control de acceso y sistemas de alarma.

Una cerradura "*Fail Safe*" es aquella que se abre cuando no existe corriente, por tanto, requiere electricidad para mantenerse cerrada. Si la electricidad está desconectada, estará constantemente en modo abierto, por lo que sería posible el acceso en entrada y salida, sin ningún medio de cierre.

Una cerradura "*Fail Secure*" se refiere a una cerradura que permanece bloqueada hasta que se le aplica corriente para desbloquear la misma. Permitirá la salida sin restricción al empujar o accionar el mecanismo del picaporte. Por tanto, si la electricidad falla, la cerradura no limitará la salida, aunque sí impedirá el acceso en entrada.

5.1.6. Conductos

Todos los conductos de ventilación deberán protegerse con barras de acero soldadas formando cuadro, sujetas firmemente con pernos a la estructura en el interior de la abertura. Las barras tendrán 25 mm de espesor y estarán espaciadas 150 mm de centro a centro, apoyándose en unas pletinas horizontales de 45 x 6 mm, espaciadas 200 mm de centro a centro.

5.1.7. Ventanas

Cuando los mismos muros de un edificio constituyen, en parte o por completo, el perímetro de seguridad, todas las ventanas y conductos situados en zonas sin vigilancia permanente y a menos de 5,5 metros por encima del nivel del suelo, o a igual distancia de tejados o cornisas accesibles, deberán protegerse con una **reja de seguridad**, constituida por barras de acero soldadas formando cuadro, sujetas firmemente con pernos a la estructura en el interior de la ventana o abertura. Las barras tendrán 25mm de espesor y estarán espaciadas 150 mm de centro a centro, apoyándose en unas pletinas horizontales de 45 x 6 mm, espaciadas 200 mm de centro a centro.

Las ventanas existentes en los paramentos de una zona de acceso restringido estarán provistas de un sistema de alarma contra apertura, rayado o rotura, salvo que dispongan de reja de seguridad. Los cristales deberán ser opacos o translúcidos, de forma que se impida cualquier visión nítida desde el exterior. En caso de ubicarse en zonas sin vigilancia permanente y a alturas o distancias inferiores a las indicadas anteriormente para ventanas en muros del perímetro de seguridad, o en el caso de no disponer de sistemas de alarma adicionales, deberán protegerse con rejas de seguridad.

5.2. Iluminación de Seguridad

Los sistemas de alumbrado ofrecen un alto grado de disuasión a un potencial intruso, además de proporcionar la iluminación necesaria para una efectiva vigilancia, ya sea directamente por los guardias o indirectamente mediante un circuito cerrado de televisión (CCTV).

5.3. Sistemas de Detección de Intrusión (IDS)

Los sistemas de detección de intrusión se constituyen de acuerdo con el principio de "defensa en profundidad". Pueden ser utilizados en perímetros de seguridad para aumentar el nivel de seguridad ofrecido por un cerramiento o en las propias zonas de acceso restringido. Pueden ser instalados como sistemas encubiertos o de manera manifiesta como elemento disuasorio.

Estos sistemas son propensos a las falsas alarmas por lo que normalmente sólo son utilizados junto con sistemas de verificación de alarmas, como CCTV.

En habitaciones o edificios en los que la guardia de seguridad o personal de servicio esté permanentemente presente, se podrá prescindir de IDS. Para ser efectivos, los IDS deberán coexistir con una fuerza de repuesta ó fuerza de apoyo, que actúe en un tiempo razonable en caso de alarma.

5.4. Control de Acceso

5.4.1. Generalidades

El procedimiento de control de acceso deberá ser el mismo para todos los individuos, creando de este modo, una cultura de respeto y adhesión a este proceso y su práctica. Puede aplicarse a un lugar, a un edificio o varios edificios de un lugar, o bien a zonas o salas dentro de un edificio.

El control podrá ser electrónico, o mediante guardia o recepcionista.

5.4.2. Guardia de seguridad o recepcionista

Los guardias de seguridad deberán contar con una habilitación personal de seguridad del grado apropiado. Si pertenecen a una empresa de servicios de seguridad, la empresa deberá contar con una habilitación de seguridad de empresa (HSEM) vigente.

5.4.3. Control de Acceso Automatizado

Un sistema de control de acceso automatizado deberá ser capaz de identificar al individuo que trata de entrar en el recinto o zona de seguridad, verificando su autorización para entrar en el mismo. Los sistemas de identificación de seguridad deberán asociarse a los sistemas de control de acceso automatizado incrementando su uso y efectividad.

Un sistema de pase o tarjeta de seguridad permitirá asegurar que sólo el personal titular de una habilitación de seguridad apropiada y debidamente autorizado es admitido en el recinto o zona de seguridad.

Los sistemas de control de acceso automatizado se dividen en:

- Sistemas de credencial material
    - Llaves: mecánica, eléctrica, electrónica, magnética, mixta.

- Tarjetas: con código de circuito eléctrico, con banda magnética, mecánica, holográfica, con código magnético, con código capacitivo, con código óptico, con código electrónico, mixtas.
- Emisores: de radiofrecuencia, de infrarrojos, de ultrasonidos.

– Sistemas de credencial de conocimiento y personal.

- Credencial de conocimiento: teclado digital, cerradura de combinación, escritura.
- Credencial personal: huella digital, voz, geometría de la mano, rasgos faciales, iris de ojos, etc.

Los sistemas de control de acceso deben incluir también dispositivos en los que se mantengan registros de las entradas y salidas del personal, tanto en horario de trabajo como, especialmente, fuera de dicho horario.

El sistema más común de doble tecnología es la tarjeta o pase de seguridad, que se acompaña de un número de identificación personal (PIN). El PIN deberá ser introducido en el sistema por cada individuo utilizando un teclado numérico. El PIN deberá consistir en cuatro o más dígitos, seleccionados aleatoriamente, sin conocimiento o asociación lógica con el individuo. El PIN deberá ser cambiado cuando exista cualquier duda sobre una violación o riesgo del mismo.

Según el grado de clasificación, se implementarán sistemas avanzados de control de acceso tipo "*Antipassback*" que obligue a los usuarios a salir antes de poder entrar y viceversa, de esta forma se evita el abuso en la utilización de los sistemas de credencial para entrar más de un individuo con un mismo dispositivo de acceso.

5.5. Identificación de seguridad (pases)

El sistema de pases constituye un sistema eficaz de identificación del personal, que facilita las entradas al personal autorizado para acceder a los distintos entornos de seguridad, y permite practicar diferenciaciones entre los usuarios e impedir accesos no autorizados.

Los pases deberán colocarse de manera bien visible dentro de los entornos de seguridad, con el fin de que el titular pueda ser reconocido e identificado. Deberán ocultarse cuando se abandone el entorno global de seguridad.

Cada pase deberá reunir las siguientes características:

- Llevar impreso un número de serie.
- Portar indicaciones sucintas que permitan la identificación del titular del mismo, específicamente: firma y fotografía.
- No mencionar, ni el nombre de la organización a la que permite el acceso, ni la habilitación de seguridad del titular.
- Fecha de vencimiento.

Los pases expedidos deberán figurar en un registro. Con el fin de practicar una identificación suplementaria entre las personas que han accedido a los distintos entornos de seguridad se deben utilizar códigos de colores o símbolos diferentes que permita distinguir, por ejemplo, entre visitantes y trabajadores permanentes.

Los pases deberán renovarse periódicamente. Las pérdidas de pases deberán comunicarse inmediatamente a un responsable de seguridad de la organización.

5.6. Guardias de seguridad

El empleo de guardias adecuadamente habilitados, entrenados y supervisados proporciona un elemento valioso de disuasión frente a aquellas personas que puedan planear una intrusión encubierta.

Las obligaciones de los guardias y la necesidad y frecuencia de las patrullas se decidirán teniendo en cuenta el nivel de riesgo y cualesquiera otros sistemas o equipos de seguridad que pudieran estar en el lugar. Por otra parte, a los guardias se les proporcionarán directrices adecuadas por escrito para asegurarse de que las tareas que les han sido específicamente asignadas se llevan a cabo de acuerdo con las necesidades.

Los guardias habrán de contar con un medio de comunicación con su centro de control de alarmas.

Cuando se recurra a los guardias para garantizar la integridad de las zonas de seguridad y de la información clasificada, éstos habrán de ser adecuadamente habilitados, entrenados y supervisados.

Es preciso contar con una fuerza de respuesta que proporcione un mínimo de dos personas a cualquier punto en el que se produzca un problema de seguridad, sin debilitar la protección local de otra parte. Se comprobará la respuesta de la guardia ante las alarmas o las señales de emergencia y se garantizará que dicha respuesta se produce dentro de un plazo que se considere adecuado para impedir el acceso de un intruso a la información clasificada que se protege.

Los inmuebles, urbanizaciones, polígonos o cualquier tipo de infraestructura que no disponga de un servicio de vigilancia propio en el entorno de sus instalaciones contratará un servicio de vigilancia externo contratado, como mínimo, en horario fuera de la jornada laboral.

5.7. Circuito Cerrado de Televisión (CCTV)

El CCTV representa una valiosa ayuda para los guardias de seguridad a la hora de verificar incidentes y alarmas en lugares o perímetros extensos. Sin embargo, la eficacia de este sistema dependerá de la selección de un equipo adecuado, de su instalación y de la supervisión que se ejerza desde el centro de control de alarmas.

5.8. Cajas fuertes, armarios blindados y contenedores de seguridad.

Se utilizan para almacenar en su interior la información clasificada de grado “CONFIDENCIAL o equivalente” o superior, cuando no está en uso. En determinadas condiciones, también para grado “DIFUSIÓN LIMITADA o equivalente” podrá requerirse su almacenamiento en estos contenedores por la Autoridad Nacional.

Se deberá mantener un control de los nombres de las personas que conocen las combinaciones o están en posesión de las llaves de cajas fuertes, armarios blindados y contenedores de seguridad.

Las cajas fuertes, armarios blindados, y otros contenedores de seguridad autorizados por la Autoridad Nacional, se deberán mantener cerrados cuando no estén bajo la supervisión de una persona autorizada.

No se almacenarán en los mismos valores distintos a la propia información clasificada que puedan actuar como un reclamo de intentos de intrusión (joyas, dinero, armas, etc.).

Las combinaciones y llaves deberán ser almacenadas de acuerdo con el mayor grado de clasificación del material o información almacenada en ese contenedor.

5.9. Combinaciones

Sólo tendrán conocimiento de los códigos del sistema de acceso a las zonas de acceso restringido, de las claves de control de la central de alarmas, así como de las combinaciones de los lugares de custodia de las materias clasificadas, el jefe de seguridad del órgano de control y las personas que él designe, que serán las mínimas imprescindibles

Las claves de combinación para la apertura de las cajas fuertes o cámaras acorazadas, y los códigos de control de la central de alarmas no deben conservarse en claro, debiendo ser modificados obligatoriamente en los siguientes casos:

- Al recibirse los contenedores de seguridad e instalarse la central de alarmas, modificando las claves y códigos que traen de fábrica.
- Cada seis (6) meses.
- Cuando se produzca un cambio en las personas que hayan tenido acceso a las mismas.
- Cuando personas no autorizadas hayan podido tener acceso a las mismas, incluido el personal de las empresas mantenedoras.

Se llevará un libro de registro de los cambios realizados.

Deberá ocultarse la identificación del fabricante, modelo, año de construcción u otros datos que puedan facilitar un conocimiento de las características de las cajas fuertes o cámaras acorazadas.

Para posibilitar el acceso a los guardias de seguridad en caso de emergencia, el jefe o responsable de seguridad les habrá entregado un sobre debidamente cerrado y precintado, con los elementos necesarios para dicho acceso. En caso de utilización de código de entrada, deberá ser cambiado ineludiblemente por el jefe o responsable de seguridad o persona autorizada, en un plazo máximo de 24 horas. En ningún caso dispondrán de los elementos que permitan la apertura de las cajas fuertes o de las cámaras acorazadas.

5.10. Control de Llaves

Para establecer una efectiva política de control de llaves es preciso realizar un exhaustivo examen e inventario de todas y cada una de las llaves de todas las cerraduras de la instalación.

Ante cualquier duda de existencia de llaves no controladas, será necesario cambiar el bombín de todas las cerraduras del emplazamiento que sean afectadas.

A continuación se indican una serie de medios y pautas que deben ser utilizadas para obtener y mantener un efectivo control de llaves:

- Armario de llaves: un armario de seguridad que permita asegurar cada llave individualmente, programable para entregar las llaves solo a usuarios autorizados y durante un lapso de tiempo determinado. Deberá contar con alarma, tanto para los distintos componentes del armario contenedor, como para las llaves.
- Registro de llaves: se procederá al registro administrativo de las llaves. En el mismo se indicará el número de serie y marca de la misma, así como la cerradura a la que pertenece.
- Llaves ciegas: Las llaves utilizadas para la generación de réplicas deberán marcarse convenientemente, asegurando que ningún empleado puede generar sus propios duplicados. Las llaves originales serán depositadas en contenedores dedicados y protegidos, accesibles sólo por personal autorizado, cuando no estén en uso. Los originales sólo serán distribuidos, bajo firma de un recibo, a las personas autorizadas para la realización de réplicas y por un tiempo limitado. Las llaves dañadas en el proceso de replicado deberán ser devueltas a efectos de su contabilidad.
- Inventario: se realizarán inventarios periódicos, personales, de las copias y de las llaves originales.
- Auditoria: además de los inventarios, se deberán realizar auditorías sin previo aviso de los registros y procedimientos de control de llaves. Durante el transcurso de estas auditorías se realizará un inventario de todas las llaves.
- Informe diario: se deberá confeccionar un informe diario indicando los empleados que han abandonado o van a abandonar la zona de seguridad. A partir de este informe se iniciarán las acciones pertinentes para recuperar las llaves e identificaciones de seguridad.

Las llaves de armarios, cajas de seguridad y cámaras acorazadas que almacenen información clasificada, así como las llaves de puertas, alarmas y sistemas de seguridad, no abandonarán el entorno global de seguridad establecido. Las llaves y claves serán depositadas en contenedores dedicados y protegidos, accesibles sólo por personal autorizado, cuando no estén en uso.

Las llaves de las cajas fuertes y de las cámaras acorazadas deberán guardarse de forma segura, en distinto lugar de donde se custodien las claves de combinación para la apertura de las mismas.

5.11. Cámara acorazada

Se entiende por cámara acorazada un local conformado por paramentos de gran fortaleza (acorazados), que delimita un recinto o espacio a proteger, accesible a través de una o varias aberturas, cubiertas por puertas y trampones acorazados. Dado su alto grado de fortaleza y protección, se permite en estas cámaras acorazadas el almacenar información clasificada fuera de contenedores de seguridad.

5.12. Registros de entradas y salidas

Se realizarán registros aleatorios a la entrada y a la salida, concebidos para que actúen como elemento de disuasión para la introducción no autorizada de material o para la retirada no autorizada de información clasificada de una zona o de un edificio.

Los registros de entrada y salida podrán convertirse en condición para la entrada a un lugar o edificio.

Se colocará un aviso en el que se indique que se pueden realizar registros de entrada y de salida aleatorios.

5.13. Control de visitas

5.13.1. Generalidades

Toda zona de acceso restringido dispondrá de una lista de personal autorizado, donde figurarán las personas que están permanentemente autorizadas a acceder a dicha zona.

Cuando otra persona distinta, que no figura en la citada lista, ha de acceder a la zona, tendrá la consideración de **visita**. Existirá un libro de registro de visitas, en formato papel o electrónico, donde se controlen todas las visitas recibidas y los detalles relevantes de las mismas.

La nacionalidad del visitante, su habilitación de seguridad, la necesidad de conocer y el tipo de local, determinan que a un visitante se le permita acceder con o sin escolta a un establecimiento clasificado, sin perjuicio de lo establecido con carácter general respecto a personal que ha de acceder a zonas de acceso restringido configuradas como área clase I o área clase II.

En los siguientes apartados se describe el tipo de control a llevar sobre los visitantes a estas zonas.

5.13.2. Visitas con escolta

Los visitantes que necesiten escolta dentro de una zona, irán acompañados en todo momento. Si necesitan visitar departamentos diferentes o a miembros diferentes del personal, pasarán oficialmente de un escolta al siguiente junto con la documentación que les acompañe. Puede exigirse llevar un pase que identifique a estas personas como visitantes.

La escolta podrá ser realizada específicamente por guardias de seguridad, especialmente cuando las condiciones de seguridad así lo aconsejen por ser mayor el riesgo que supone la visita.

En condiciones de menor riesgo, la escolta podrá ser realizada por el propio personal con acceso autorizado en la zona. En dicho caso, quien realice la escolta deberá ser consciente de que está desarrollando dicho cometido y de la responsabilidad que asume.

5.13.3. Visitas sin escolta

Los visitantes a los que se les permita la estancia sin escolta en una zona, por ser personal controlado, con necesidad de conocer y la oportuna habilitación de seguridad, deberán llevar

un pase permanentemente visible que les identifique como visitantes. El sistema de pases para las visitas sólo será eficaz si a todo el personal habitual se le exige igualmente que lleve pase.

5.13.4. Personal de mantenimiento y limpieza

Al personal de mantenimiento de instalaciones y limpieza le estará prohibido acceder sin escolta en las zonas de acceso restringido.

6. EQUIPAMIENTO DE SEGURIDAD

En este apartado se describen las medidas específicas de seguridad física que, con carácter normalizado, constituyen el equipamiento de seguridad de una zona de acceso restringido, en función del grado de clasificación de la información que vaya a ser manejada o almacenada en la misma. Las condiciones particulares de cada instalación y su emplazamiento podrán obligar a reforzar determinadas medidas, o impedirán la existencia de otras. No obstante, los diferentes entornos deben constituir un todo armónico que asegure una protección adecuada a la naturaleza, volumen de la información a proteger, y al nivel de riesgo existente.

El equipamiento de seguridad que se indica en cada caso, deberá regirse conforme a los criterios indicados en el apartado **5** de este documento para cada medida específica de seguridad física.

6.1. Grado "CONFIDENCIAL o equivalente"

6.1.1. Entorno global de seguridad (EGS)

No existen requerimientos especiales para el entorno global de seguridad, aunque se valorará su presencia.

6.1.2. Entorno local de seguridad (ELS)

La información clasificada con grado de "CONFIDENCIAL o equivalente" deberá ser almacenada dentro de una zona de acceso restringido configurada como área clase I o área clase II, con las siguientes medidas de protección:

- Las paredes, techo y suelo, deberán ofrecer el mismo nivel de resistencia, siendo las paredes de ladrillo macizo, como mínimo de medio pie. Las paredes irán desde el verdadero suelo hasta el verdadero techo.
- Los conductos existentes en los paramentos de la zona de acceso restringido estarán protegidos conforme a las medidas de seguridad establecidas en el apartado **5.1.6** de este documento.
- Las ventanas existentes en los paramentos de la zona de acceso restringido estarán provistas de las medidas de seguridad que se establecen en el apartado **5.1.7** de este documento.
- La puerta de acceso a la zona de acceso restringido será blindada para interior de grado 4 según norma europea UNE-EN-1627, de características RF-30 según las normas UNE-EN-13501, provista de una cerradura mecánica de alta seguridad con al menos 5 puntos de cierre al frente, cuyo mecanismo será obligatoriamente accionado cuando no

haya nadie presente en la misma. También dispondrá de un dispositivo que obligue a la puerta a permanecer cerrada cuando no se esté franqueando.

- Deberá disponer de un sistema electrónico de control de acceso de doble tecnología: material (tarjeta, llave, etc.) y conocimiento o personal (PIN, biométrico, etc.), debidamente homologado, que limite, identifique y registre dichos accesos a la zona de acceso restringido, configurado en modo "*Fail Secure*".
- Los sistemas de control de acceso deberán incluir dispositivos en los que se mantengan registros de las entradas y salidas del personal, tanto en horario de trabajo como, especialmente, fuera de dicho horario. Estos registros se deben conservar durante un tiempo no inferior a un año.
- La zona de acceso restringido dispondrá de detectores de presencia y/o de movimiento (IDS) como mínimo de doble tecnología, conectados al centro de control de alarmas, que estarán instalados en función de la superficie y configuración, de manera que se cubra la zona en su totalidad, salvo que la instalación esté ocupada por personal presente las 24 horas al día. Estos sistemas dispondrán de dispositivos anti sabotaje.
- En el interior de la zona de acceso restringido se instalará una caja fuerte de al menos nivel III, conforme a la norma UNE-EN 1143, y cerradura clase B, homologada conforme a la norma UNE-EN-1300, o equivalentes en vigor, donde se custodiarán obligatoriamente las materias clasificadas durante los períodos de tiempo en que no se estén manejando. En instalaciones oficiales de la Administración se podrá autorizar un armario blindado, siempre que exista un nivel de seguridad en el entorno global de seguridad que impida de forma fehaciente el acceso y permanencia de personal no controlado en las inmediaciones de la zona de acceso restringido, especialmente fuera de horario de trabajo.

6.2. Grado "RESERVADO o equivalente"

6.2.1. Entorno Global de Seguridad (EGS)

- Deberá existir un perímetro de seguridad bien definido, constituido por cierres perimetrales físicos, preferiblemente rectilíneos, de un mínimo de 2,15 metros de alto. Se completarán con Sistemas de Detección de Intrusión Perimetral (PIDS) para aumentar el nivel de seguridad ofrecido por los mismos. Las alarmas procedentes de los detectores de intrusión perimetrales, deberán gestionarse desde un centro de control de alarmas con capacidad para alertar al servicio de seguridad de manera inmediata.
- El conjunto se completará con un sistema de CCTV capaz de trabajar en el espectro visible e infrarrojo (este último, si fuera necesario).
- El perímetro de seguridad dispondrá de, al menos, un punto de acceso donde se identifiquen usuarios y vehículos, facilitando distintivos o pases a las posibles visitas que permitan, durante su permanencia en el recinto, acreditar su condición de visitantes ante el servicio de seguridad y demás usuarios del mencionado recinto.
- Se dispondrá de un servicio de seguridad "in situ" que reaccione ante cualquier intento de acceso no autorizado. Cuando el servicio de seguridad esté integrado por personal de una empresa de seguridad privada, dicha empresa contará con una HSEM, con al menos el grado de "CONFIDENCIAL o equivalente", si bien el personal que pudiese acceder a zonas de mayor clasificación deberá disponer de habilitación personal de seguridad de grado correspondiente al grado de clasificación de la documentación almacenada en ésta.

6.2.2. Entorno local de seguridad (ELS)

La información clasificada con grado de "RESERVADO o equivalente" deberá ser almacenada dentro de una zona de acceso restringido configurada como área clase I o área clase II, con las siguientes medidas de protección:

- Las paredes, techo y suelo, deberán ofrecer el mismo nivel de resistencia, siendo las paredes de ladrillo macizo, como mínimo de medio pie. Las paredes irán desde el verdadero suelo hasta el verdadero techo.
- Los conductos existentes en los paramentos de la zona de acceso restringido estarán protegidos conforme a las medidas de seguridad establecidas en el apartado **5.1.6** de este documento.
- Las ventanas existentes en los paramentos de la Zona de Acceso Restringido estarán provistas de las medidas de seguridad que se establecen en el apartado **5.1.7** de este documento.
- En las inmediaciones de las zonas de acceso restringido se contará con un sistema CCTV de manera que puedan avistarse movimientos, especialmente en la puerta de acceso.
- La zona de acceso restringido dispondrá de detectores de presencia y/o de movimiento (IDS) como mínimo de doble tecnología, conectados al centro de control de alarmas, que estarán instalados en función de la superficie y configuración, de manera que se cubra la zona en su totalidad, salvo que la instalación este ocupada por personal presente las 24 horas al día. Estos sistemas dispondrán de dispositivos antisabotaje.
- La puerta de acceso a la zona de acceso restringido será blindada para interior de grado 4 según norma europea UNE-EN-1627, de características RF-60 según las normas UNE-EN-13501 y deberá disponer de una cerradura mecánica de alta seguridad con al menos 5 puntos de cierre al frente, cuyo mecanismo será obligatoriamente accionado cuando no haya nadie presente en la misma. También dispondrá de un dispositivo que obligue a la puerta a permanecer cerrada cuando no se esté franqueando. Se instalará un dispositivo que detecte la apertura de la misma.
- Deberá disponer de un sistema electrónico de control de acceso de doble tecnología: material (tarjeta, llave, etc.) y conocimiento o personal (PIN, biométrico, etc.), debidamente homologado, que limite, identifique y registre dichos accesos a la zona de acceso restringido, configurado en modo "*Fail Secure*".
- Los sistemas de control de acceso deberán incluir dispositivos en los que se mantengan registros de las entradas y salidas del personal, tanto en horario de trabajo como, especialmente, fuera de dicho horario. Estos registros se deben conservar durante un tiempo no inferior a un año.
- En el interior de la zona de acceso restringido se instalará una caja fuerte de al menos nivel IV (en instalaciones oficiales de la Administración se podrá autorizar el nivel III), conforme la norma UNE-EN-1143, y equipada con dos cerraduras clase B según norma UNE-EN-1300 o equivalentes en vigor. Al menos una de las cerraduras deberá disponer de combinación electrónica.

Todos los medios activos de seguridad procedentes de las zonas de acceso restringido (IDS, sensores sísmicos, CCTV) deberán estar conectados al centro de control de alarmas, con capacidad para alertar al servicio de seguridad en un plazo establecido.

En caso de no existir EGS, o de no proporcionar una protección adecuada, el ELS deberá establecerse conforme a los criterios correspondientes a grado de "SECRETO o equivalente".

6.2.3. Entorno de seguridad electrónico (ESE)

- En los servidores, terminales y equipos de cifra se instalarán sistemas contra la manipulación de los equipos, es decir, etiquetas de seguridad.
- Se establecerán medidas para evitar fugas de información relacionadas con fenómenos TEMPEST, o establecidas contra escuchas activas o pasivas.
- Se prohibirá la entrada en el recinto de equipos electrónicos no controlados.

6.3. Grado "SECRETO o equivalente"

6.3.1. Entorno global de seguridad (EGS)

- Deberá existir un perímetro de seguridad bien definido, constituido por cierres perimetrales físicos, preferiblemente rectilíneos, de un mínimo de 2,15 metros de alto. Se completarán con PIDS para aumentar el nivel de seguridad ofrecido por los mismos. Las alarmas procedentes de los detectores de intrusión perimetrales, deberán gestionarse desde un centro de control de alarmas con capacidad para alertar al servicio de seguridad de manera inmediata.
- Se instalará un sistema de iluminación de protección que mejore la eficiencia del servicio de seguridad y se constituya en elemento disuasorio.
- El conjunto se completará con un sistema de CCTV capaz de trabajar en el espectro visible e infrarrojo.
- El perímetro de seguridad dispondrá de, al menos, un punto de acceso donde se identifiquen usuarios y vehículos, facilitando distintivos a las posibles visitas que permitan, durante su permanencia en el recinto, acreditar su condición de visitantes ante el servicio de seguridad y demás usuarios del mencionado recinto.
- Se dispondrá de un servicio de seguridad "in situ" que reaccione ante cualquier intento de acceso no autorizado. Cuando el servicio de seguridad esté integrado por personal de una empresa de seguridad privada, dicha empresa contará con una HSEM, con al menos el grado de "CONFIDENCIAL o equivalente", si bien el personal que pudiese acceder a zonas de mayor clasificación deberá disponer de habilitación personal de seguridad de grado correspondiente al grado de clasificación de la documentación almacenada en ésta.

6.3.2. Entorno local de seguridad (ELS)

La información clasificada con grado de "SECRETO o equivalente" deberá ser almacenada dentro de una zona de acceso restringido configurada como área clase I o área clase II, con las siguientes medidas de protección:

- Las paredes, techo y suelo, deberán ofrecer el mismo nivel de resistencia, siendo las paredes de ladrillo macizo, como mínimo de medio pie. Las paredes irán desde el verdadero suelo hasta el verdadero techo.
- Los conductos existentes en los paramentos de la zona de acceso restringido estarán protegidos conforme a las medidas de seguridad establecidas en el apartado **5.1.6** de este documento.

- Las ventanas existentes en los paramentos de la zona de acceso restringido estarán provistas de las medidas de seguridad que se establecen en el apartado **5.1.7** de este documento.
- Cuando la zona de acceso restringido sea limítrofe con el exterior o con áreas no controladas, se instalarán sensores sísmicos que transmitan una señal de alarma al producirse un intento de intrusión. Estos sistemas dispondrán de dispositivos anti sabotaje.
- En las inmediaciones de las zonas de acceso restringido se contará con un sistema CCTV de manera que puedan avistarse movimientos, especialmente en la puerta de acceso.
- La zona de acceso restringido dispondrá de detectores de presencia y/o de movimiento (IDS) como mínimo de doble tecnología, conectados al centro de control de alarmas, que estarán instalados en función de la superficie y configuración, de manera que se cubra la zona en su totalidad, salvo que la instalación este ocupada por personal presente las 24 horas al día. Estos sistemas dispondrán de dispositivos anti sabotaje.
- La puerta de acceso a la zona de acceso restringido será blindada para interior de grado 4 según norma europea UNE-EN-1627, de características RF-60 según las normas UNE-EN-13501 y deberá disponer de una cerradura mecánica de alta seguridad con al menos 5 puntos de cierre al frente, cuyo mecanismo será obligatoriamente accionado cuando no haya nadie presente en la misma. También dispondrá de un dispositivo que obligue a la puerta a permanecer cerrada cuando no se esté franqueando. Se instalará un dispositivo que detecte la apertura de la misma.
- Deberá disponer de un sistema electrónico de control de acceso de doble tecnología: material (tarjeta, llave, etc.) y conocimiento o personal (PIN, biométrico, etc.), debidamente homologado, que limite, identifique y registre dichos accesos a la zona de acceso restringido, configurado en modo "*Fail Secure*".
- Los sistemas de control de acceso deberán incluir dispositivos en los que se mantengan registros de las entradas y salidas del personal, tanto en horario de trabajo como, especialmente, fuera de dicho horario. Estos registros se deben conservar durante un tiempo no inferior a un año.
- El sistema de control de accesos impedirá la entrada de cualquier persona no identificada y registrada a la salida, sistema "*antipassback*".
- En el interior de la zona de acceso restringido se instalará una caja fuerte de al menos nivel VI (en instalaciones oficiales de la Administración se podrá autorizar el Nivel IV), conforme la norma UNE-EN-1143, y equipada con dos cerraduras clase C según norma UNE-EN-1300 o equivalentes en vigor. Al menos una de las cerraduras deberá disponer de combinación electrónica.

Todos los medios activos de seguridad procedentes de las zonas de acceso restringido (IDS, sensores sísmicos, CCTV) deberán estar conectados al centro de control de alarmas con capacidad para alertar al servicio de seguridad de manera inmediata.

6.3.3. Entorno de seguridad electrónico (ESE)

- En los servidores, terminales y equipos de cifra se instalarán sistemas contra la manipulación de los equipos, es decir, etiquetas de seguridad.
- Se establecerán medidas para evitar fugas de información relacionadas con fenómenos TEMPEST, o establecidas contra escuchas activas o pasivas.
- Se prohibirá la entrada en el recinto de equipos electrónicos no controlados.

7. SEGURIDAD FÍSICA PARA LOS SISTEMAS DE INFORMACIÓN Y COMUNICACIONES (CIS)

En instalaciones donde la información clasificada es almacenada o manejada utilizando sistemas de información y comunicaciones (CIS), deberán establecerse los requerimientos necesarios para asegurar el cumplimiento de los objetivos de seguridad: confidencialidad, integridad y disponibilidad.

Si en dichos CIS se va a manejar información clasificada de grado "CONFIDENCIAL o equivalente" o superior, las instalaciones deberán ser acreditadas como zonas de acceso restringido, configuradas como área clase I o área clase II, según el procedimiento de explotación de la información clasificada que se siga en dicha zona.

Cuando la información manejada sea de grado "DIFUSIÓN LIMITADA o equivalente", las instalaciones deberán constituirse como zonas administrativas de protección.

Las instalaciones que alojan servidores o equipos críticos de red, de comunicaciones o de cifra, que almacenan, procesan o transmiten información clasificada, podrán necesitar ser acreditadas obligatoriamente como área clase I, conforme a los criterios que se indican en la norma NS/05 de la ANPIC.

Con relación a los objetivos de disponibilidad e integridad, una combinación de controles medioambientales deberá ser instalada en estas zonas: equipos de detección de incendios, equipos de detección de temperatura y humedad, sensores de agua y sistemas de alimentación ininterrumpida. Las alertas asociadas con los controles medioambientales deberán ser permanentemente monitorizadas por el centro de control de alarmas.

En cualquier caso, la presencia de uno o más CIS en una ZAR va a afectar de forma significativa a los requerimientos de protección de esa instalación, obligando a la adopción de medidas de seguridad complementarias a las que ya puedan estar reflejadas en el propio plan de protección de la ZAR. En consecuencia, es objetivo final a alcanzar el que la coexistencia del plan de protección de la ZAR junto con los procedimientos operativos de seguridad (POS) del CIS, constituya una condición necesaria y suficiente para garantizar la protección de la información manejada.

En unos casos esto obligará a hacer cambios en el propio plan de protección y en otros bastará con incluir en los POS del CIS las medidas complementarias a adoptar. Dependerá de las condiciones y procedimientos de explotación del CIS. No es lo mismo, por ejemplo, que la información clasificada que reside en los discos duros o soportes extraíbles esté cifrada con una herramienta aprobada para el grado de clasificación de la información, o que esté en claro; las medidas de protección a adoptar y reflejar en la normativa serán muy diferentes.

La casuística puede ser muy variada, por lo que el análisis de riesgos que se realice será determinante para alcanzar una solución válida (riesgo residual aceptable). Lo importante es que las normativas de seguridad del sistema y de la instalación, reflejen de forma explícita las medidas de seguridad y procedimientos de trabajo, y que estos sean suficientes para el objetivo de seguridad perseguido.

Los usuarios de los CIS manejados en la ZAR deberán conocer y firmar tanto el plan de protección de la ZAR como los POS del sistema.