Autoridad Nacional
para la protección de la información clasificada

- NS/03 -

Seguridad física

SEGURIDAD FÍSICA

ÍNDICE

NORMA NS/03

SEGURIDAD FÍSICA

1. INTRODUCCIÓN

La seguridad física es la condición que se alcanza en las instalaciones cuando se aplica un conjunto de medidas de protección eficaces para la prevención de posibles accesos a información clasificada por parte de personas no autorizadas, así como para proporcionar las evidencias necesarias cuando se produzca un acceso o un intento de acceso.

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.

Las instalaciones en las que se vaya a manejar o almacenar información clasificada deberán ser protegidas mediante las apropiadas medidas de seguridad física, teniendo en cuenta los siguientes factores:

- Grado de clasificación de la información.
- Tipo de información, en cuanto a su origen.
- Cantidad y formato de la información (papel, dispositivos informáticos, u otros).
- Necesidad de conocer del personal.
- Amenazas y vulnerabilidades.
- Medios de almacenamiento de la información.

Las medidas de seguridad física aplicables a cada caso serán concebidas para:

- Impedir la entrada por parte de intrusos, tanto si emplean métodos subrepticios como si utilizan otros que impliquen el uso de la fuerza.
- Disuadir, impedir o detectar acciones llevadas a cabo por personal desleal.
- Permitir la limitación del personal en su acceso a información clasificada de acuerdo con el principio de la necesidad de conocer.
- Detectar posibles brechas o violaciones de seguridad y ejercer las pertinentes acciones de corrección sobre éstas con la mayor brevedad posible.

Con carácter general, las instalaciones en que se adoptan medidas de protección y control reciben la denominación de zonas de seguridad.

Las medidas específicas de seguridad física incluidas en esta norma están orientadas principalmente hacia las 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. En cualquier caso, los conceptos de seguridad que se presentan en esta norma serán un objetivo deseable a alcanzar en toda ocasión.

2. CONCEPTO DE SEGURIDAD

2.1. Defensa en profundidad

La seguridad física se concibe según un concepto global, en el que las diferentes medidas de detección y retardo se complementan entre sí en los distintos niveles, de forma que, ante un intento de intrusión, el tiempo de detección sea el menor posible, lo que, indudablemente, debe reducir al mínimo el tiempo de reacción ante dicha intrusión.

Una vez detectado el intento de intrusión, las medidas de retardo deberán dificultar la acción del intruso el máximo tiempo posible, de forma que permitan la actuación de los elementos de reacción que neutralicen dicho intento de intrusión. De este modo, la neutralización de un intento de intrusión depende directamente de las medidas de detección, retardo y reacción, aplicadas a los locales a proteger. Si cualquiera de estas medidas falla, la intrusión tendrá éxito; de ahí la importancia de que éstas actúen en el momento oportuno y coordinadas entre sí.

Por todo ello, la seguridad se constituye según un esquema de **defensa en profundidad**, en diferentes entornos sucesivos, desde el perímetro exterior de la base, acuartelamiento, edificio o centro, hasta llegar al recinto final de la instalación.

Este esquema de defensa en profundidad establece tres niveles de protección:

- **Entorno global de seguridad**: Constituido por la zona exterior que rodea el local a proteger.
- **Entorno local de seguridad**: Constituido por el local donde se encuentra la información a proteger.
- **Entorno de seguridad electrónico**: relativa a la seguridad de emisiones, escuchas y equipos informáticos y de comunicaciones.

2.2. Entorno global de seguridad

Se refiere a los perímetros y zonas de seguridad exteriores que serán necesarios sobrepasar para llegar a la propia zona de acceso restringido, concepto que se define más adelante.

La protección física de locales y edificios requiere que exista, en la medida de lo posible, una cierta seguridad perimetral a su alrededor que suponga un primer obstáculo para cualquier amenaza de intrusión.

El entono global de seguridad incluirá todas las medidas de seguridad establecidas que es necesario atravesar para llegar al exterior de la propia zona de acceso restringido. Se compondrá de elementos de seguridad pasivos tales como elementos estructurales de protección (muros, verjas, vallas, bayonetas, alambradas), complementados con sistemas activos de protección perimetral (circuito cerrado de televisión, barreras de infrarrojos, barreras de microondas, volumétricos exteriores, cables sensores, iluminación de seguridad, etc.).

Estos sistemas de protección perimetral deberán contar, entre otras, con las siguientes características:

- Alta fiabilidad que garantice una alerta inmediata.
- Independientes de las condiciones meteorológicas.
- Capaz de discriminar entre la presencia humana y animales, fenómenos atmosféricos (viento, lluvia, etc.).
- Dotado de sistemas anti sabotaje.

La seguridad perimetral de sistemas activos y pasivos deberá reforzarse mediante la utilización de sistemas de control general de acceso e identificación y de guardias de seguridad, patrullas y fuerzas de reacción.

En este sentido, la eficacia de cualquier perímetro de seguridad dependerá en gran medida del nivel de seguridad de los puntos de acceso y del tipo de control de acceso que se establezca, entendiendo por control de acceso todo aquello que abarca la necesidad de un pase o sistema de reconocimiento personal, incluyendo los sistemas de control y el acompañamiento de visitas autorizadas.

2.3. Entorno local de seguridad

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 zona, en los propios paramentos y accesos, así como dentro de la misma, que impiden el acceso a la información clasificada allí manejada. Se compone de elementos de seguridad tales como elementos estructurales de protección (paramentos de fortaleza adecuada, puertas blindadas, cerraduras de seguridad, etc.), sistema de control de acceso, detectores de intrusión, cámaras CCTV, cajas y armarios de seguridad.

El local a proteger dispondrá de:

- Un perímetro definido de solidez suficiente.
- Un control de acceso al mismo.
- Mecanismos de detección de intrusiones, que se activan fuera de la jornada laboral, tales como circuito cerrado de televisión, volumétricos, sensores de intrusión, sensores sísmicos.
- Sistemas de alarma: alarmas sonoras, alarmas silenciosas, sistemas de alarma contra incendio.
- Sistemas de contención: puertas de seguridad, armarios de seguridad, cajas fuertes, cámaras acorazadas.

Será imprescindible la instalación de controles de acceso a los locales protegidos. Dicho control de acceso podrá ser ejercido por guardias de seguridad o por elementos electrónicos, no permitiéndose el acceso de visitantes a las zonas de acceso restringido sin el conocimiento y la autorización del responsable de seguridad. Dichos visitantes deberán estar permanentemente escoltados si existe la posibilidad de que tengan acceso a información clasificada, sin disponer de la habilitación personal de seguridad (HPS) o la necesidad de conocer.

No obstante, lo más razonable es que el acceso interior se limite a las zonas administrativas de protección, siempre bajo el control del responsable de seguridad. Los visitantes no accederán a una zona de acceso restringido a no ser que estén autorizados. El

responsable de seguridad deberá tomar las medidas adecuadas para evitar accesos no autorizados, accidentales o intencionados, a información clasificada.

Por lo que respecta a los armarios de seguridad y cajas fuertes, representan la última barrera en ese concepto de defensa en profundidad. Su capacidad para retardar el acceso de un posible intruso a la información clasificada deberá ser, en todo caso, inversamente proporcional a la capacidad de los demás sistemas aplicados. Así, si los sistemas perimetrales y de seguridad interior son numerosos y fiables no será preciso instalar armarios o cajas de excepcional resistencia, pudiendo optarse por algún modelo de menor nivel. Al contrario, si la seguridad perimetral e interior es escasa o de poca fiabilidad, será precisa la instalación de armarios o cajas fuertes de alto nivel para la protección de la información clasificada.

2.4. Entorno de seguridad electrónico

Los locales deberán estar protegidos frente a escuchas pasivas (filtración de información clasificada debido a comunicaciones poco seguras, escuchas realizadas directamente o a través de emisiones electromagnéticas no deliberadas) y frente a escuchas activas (filtración de información clasificada debido a micrófonos u otro tipo de dispositivos).

La protección frente a estos tipos de escuchas requiere la realización de inspecciones físicas y técnicas de seguridad de la estructura de los locales, mobiliario, accesorios, así como del equipo de oficina (incluidas las máquinas, fotocopiadoras y otros dispositivos), y las comunicaciones, quedando definidas como áreas técnicamente seguras, donde la entrada quedará controlada de manera especial.

En los dispositivos electrónicos (CPU, impresora, fotocopiadora, grabadora, teclado, pantalla, etc.) se incorporarán etiquetas de seguridad capaces de advertir una manipulación, y no podrán ingresar o abandonar el entorno local sin la correspondiente autorización del responsable de seguridad de la zona de acceso restringido.

Dentro del entorno local donde se hallen servidores, terminales, y equipos de cifra de los sistemas de información y comunicaciones que manejan información clasificada de grado "CONFIDENCIAL o equivalente" o superior, sus radiaciones electromagnéticas deberán ser controladas a través de un análisis TEMPEST.

3. ZONAS DE SEGURIDAD

3.1. Tipos

Una zona de seguridad es cualquier instalación con un perímetro definido dentro de la que existe un control y unas condiciones de protección específicas. Desde el punto de vista de la protección de la información clasificada se distinguen dos tipos:

- Zona de acceso restringido.
- Zona administrativa de protección.

3.2. Zona de acceso restringido (ZAR)

Son instalaciones donde se almacena o maneja información clasificada, normalmente

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. Estas instalaciones deberán ser oficial y formalmente acreditadas, y 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 dicha información, por lo que sólo puede acceder personal debidamente habilitado y autorizado. Este tipo de zona precisa:

   - Un perímetro claramente definido y protegido a través del cual se controlen todas las entradas y salidas.
   - Un sistema de control de entrada que admita exclusivamente a aquellas personas debidamente habilitadas y específicamente autorizadas para acceder a dicha área.
   - Que las personas que accedan a la zona sean informadas previamente del tipo y grado de clasificación de la información a la que da acceso la entrada.

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. Este tipo de zona precisa:

   - Un perímetro claramente definido y protegido a través del cual se controlen todas las entradas y salidas.
   - Un sistema de control de entrada que sólo permite el acceso sin escolta a aquellas personas con habilitación de seguridad y con autorización específica para acceder a la zona. A todas las demás personas se les proporcionará escolta o controles equivalentes a fin de evitar el acceso no autorizado a la información clasificada y la entrada, no controlada, a las zonas sujetas a inspección de seguridad técnica.

No existe una relación entre la configuración como clase I o II y el grado de protección que se aporta. La única diferencia entre ambas radica en las condiciones de accesibilidad a la información clasificada dentro de cada zona.

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

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

3.3. 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" inclusive, con las excepciones que se establecen en estas normas o de forma puntual.

Cuando sea necesario, se establecerá una zona administrativa de protección en torno a las zonas de acceso restringido clase I o clase II, o en las zonas que conducen a dichas zonas de seguridad.´

Estas instalaciones no precisan ser oficialmente acreditadas, pero sí serán declaradas y estarán perfectamente definidas y controladas como tales, especialmente para conocimiento de los usuarios de dichas instalaciones.

Tendrán las siguientes características:

- La puerta deberá tener un control de acceso que limite la entrada y salida, previa identificación positiva de la persona.
- Deberán contar con detectores de intrusión de perímetro u otros medios de vigilancia que permitan alertar de un intento de acceso no autorizado a la zona a través de cualquier punto.
- Contarán con mobiliario adecuado para guardar bajo llave la Información Clasificada de grado "DIFUSIÓN LIMITADA o equivalente".

En instalaciones no oficiales, como por ejemplo empresas contratistas, en que se vaya a almacenar información con grado de "DIFUSIÓN LIMITADA o equivalente", se exigirán medidas y procedimientos de protección adicionales para las zonas administrativas de protección que hayan de constituir.

Las organizaciones deberán designar un responsable de seguridad de zona administrativa de protección y difundir dicho nombramiento, dentro y fuera de la organización, según se precise. Dicho responsable deberá adquirir la formación adecuada a las responsabilidades que asume, especialmente en lo relativo a la protección de la información clasificada de grado "DIFUSIÓN LIMITADA o equivalente" que se maneje en dicha zona.

4. ACREDITACIÓN DE UNA ZONA DE ACCESO RESTRINGIDO

La Oficina Nacional o, por delegación expresa de la misma, otro organismo o entidad, autorizado, someterá a todo local, edificio, oficina, habitación u otro tipo de área en que se vaya a manejar o almacenar información clasificada hasta un determinado grado de clasificación, a un proceso de acreditación, por el que se declara su constitución como zona de acceso restringido.

La **acreditación** es el reconocimiento expreso, mediante certificado escrito (según modelo anexo I), 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 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.

Mediante dicha acreditación, la autoridad firmante ejercerá sus responsabilidades

respecto a la protección de la información clasificada y tomará conciencia del nivel de riesgo asumido.

La acreditación de una zona de acceso restringido exigirá la elaboración previa, por parte del responsable de seguridad de la zona de acceso restringido, de un **plan de protección**. Consta de tres documentos básicos:

- **Plan de acondicionamiento**: Su objeto es describir los sucesivos entornos de seguridad existentes, las características físicas y las medidas técnicas adoptadas, que permiten alcanzar un nivel de protección suficiente. No debe incluir, en ningún caso, procedimientos, normas o medidas organizativas, que sean objeto de los otros planes.

- **Plan de seguridad**: Su objeto es describir las medidas organizativas de seguridad, es decir, los procedimientos de control, gestión, trabajo, guarda, salvaguarda, etcétera, establecidos en el órgano, local o área de seguridad para, en conjunción con las medidas de seguridad física existentes (explicadas en el plan de acondicionamiento), permitir y garantizar la protección de la información clasificada y su adecuado manejo, en condiciones de trabajo habituales.

- **Plan de emergencia**: Su objeto es describir las medidas organizativas de seguridad a adoptar o seguir para mantener la protección de la información clasificada ante contingencias de tipo extraordinario que puedan afectar a la misma.

Estos documentos son de obligada confección como parte fundamental del expediente de acreditación de una zona de acceso restringido donde se vaya a manejar o almacenar información clasificada.

La finalidad principal de este plan es dar evidencia objetiva de que las medidas de seguridad implantadas, tanto de seguridad física, como de seguridad en el personal y de la información, junto con los procedimientos organizativos de seguridad, de obligado cumplimiento, constituyen un entorno de seguridad definido, estudiado y adaptado a la normativa vigente, que permite el manejo o almacenamiento seguro de la información clasificada.

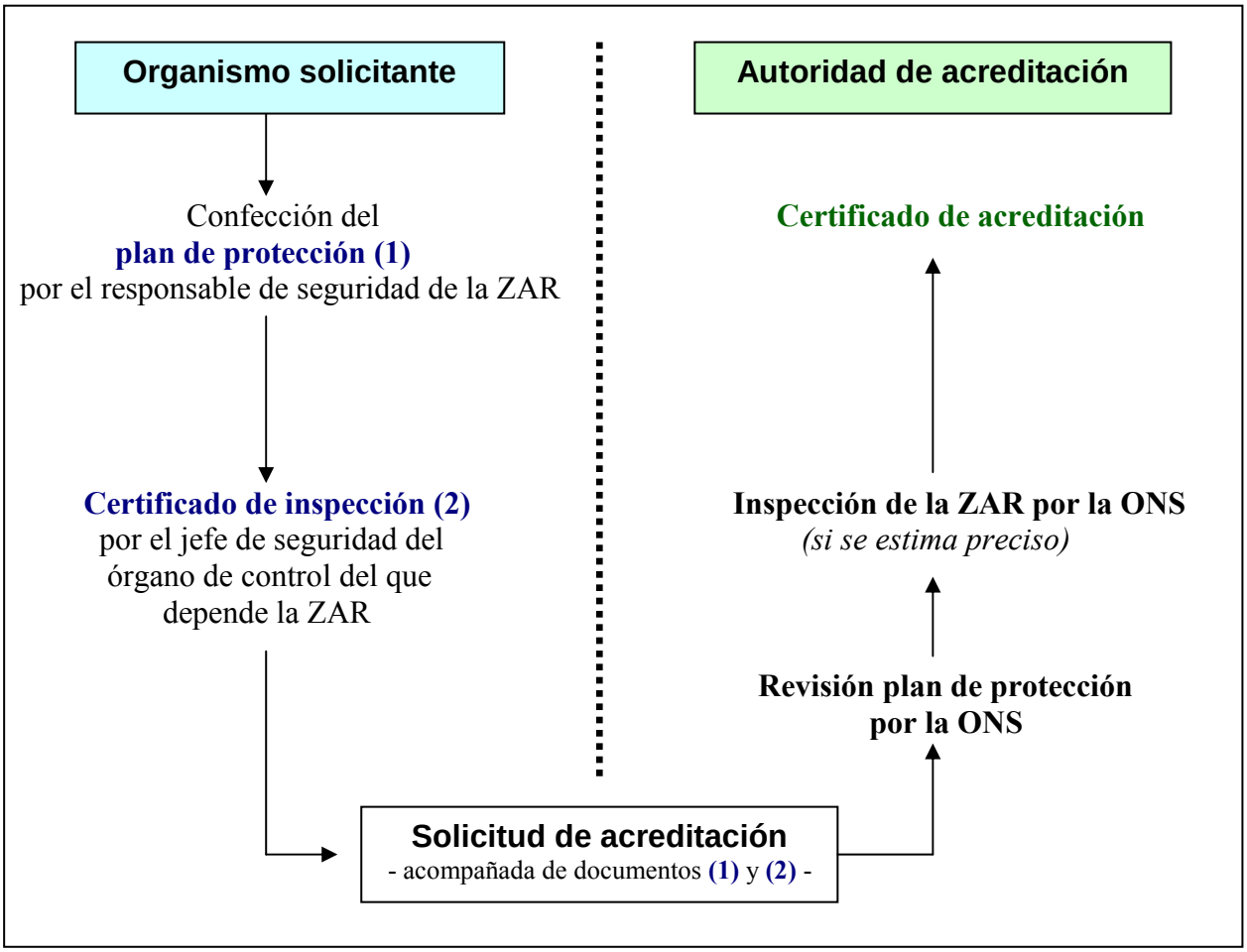
Son también objetivos de dicho plan:

- Constituir la guía de referencia a través de la cual los responsables de la seguridad y los usuarios, conozcan sus obligaciones en materia de protección.
- Constituir un documento básico en los relevos de responsabilidades de seguridad, al definir y asegurar el cumplimiento de unas mismas medidas de seguridad, con independencia del personal destinado en cada momento.
- Constituir la guía de referencia para las inspecciones tanto de apertura como de correcto desempeño.

El plan de protección deberá ser fiel reflejo de la situación real en materia de seguridad, por lo que deberá ser actualizado en función de los cambios que se vayan produciendo y que afecten a la misma. El certificado de acreditación sólo tendrá validez si el plan de protección en el que está basado se encuentra debidamente actualizado.

El responsable de seguridad de la zona de acceso restringido tiene el cometido de la confección del plan de protección, así como de su implantación y de asegurar su cumplimiento.

En el siguiente esquema se presenta el resumen de pasos a seguir para acreditar una zona de acceso restringido:



Previamente a la remisión del plan de protección para su aprobación, dentro del proceso de acreditación, se requerirá que la zona de acceso restringido sea inspeccionada por el jefe de seguridad de un órgano de control superior del que dependa funcionalmente en materia de seguridad, y que éste emita certificado de cumplimiento de la normativa de seguridad pertinente, según modelo del anexo II de este documento. Si esta inspección no resulta positiva, se adoptarán las medidas correctoras necesarias para solventarlas, requiriendo una inspección y certificación posteriores.

Al objeto de normalizar los procesos y facilitar su análisis y aprobación, se utilizarán los modelos de documentos editados por la Oficina Nacional.

El plan de protección, una vez cumplimentado, tendrá la clasificación de CONFIDENCIAL.

Se deberá solicitar la renovación de los certificados de acreditación en los tiempos máximos que se establecen a continuación, según el grado de clasificación establecido, o

cuando haya una modificación significativa de las condiciones de seguridad, para lo cual deberán remitir un nuevo plan de protección actualizado:

- SECRETO o equivalente: **3 años**
- RESERVADO o equivalente: **5 años**
- CONFIDENCIAL o equivalente: **10 años**

El certificado de acreditación de una ZAR mantiene su vigencia hasta que se cumpla la fecha de caducidad de la misma. **Si con antelación a la fecha de caducidad se hubiera recibido en la Oficina Nacional, y estuviera en trámite de concesión, la solicitud de renovación**, se admitirá un plazo máximo de seis (6) meses de prórroga de la validez del certificado, a contar desde la fecha de caducidad, con carácter automático y sin necesidad de solicitud al efecto.

5. COMETIDOS DEL JEFE DE SEGURIDAD DEL ÓRGANO DE CONTROL

El jefe de seguridad de un órgano de control que tenga bajo su responsabilidad una o varias zonas de acceso restringido, será responsable en cada una de ellas 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 el responsable de seguridad de la zona de acceso restringido, la responsabilidad será del jefe de seguridad del órgano de control superior.
- Supervisar el exacto cumplimiento de la normativa de protección de la información clasificada, y del plan de protección.
- Verificar que existe un responsable de seguridad de la zona de acceso restringido.
- Vigilar el correcto manejo de la información clasificada, especialmente en cuanto a custodia, control y acceso.

6. COMETIDOS DEL RESPONSABLE DE SEGURIDAD DE UNA ZONA DE ACCESO RESTRINGIDO

El responsable de seguridad de una zona de acceso restringido será responsable respecto a la misma de:

- Confeccionar el plan de protección.
- Establecimiento de un procedimiento de control de visitas.
- Realización de simulacros periódicos del plan de emergencia.
- Verificar que los sistemas de seguridad se mantienen de manera correcta, asegurando los niveles de seguridad necesarios.
- Confeccionar y mantener la lista de personal autorizado con acceso a la zona de acceso restringido, según el modelo del anexo III de este documento.
- Asegurar la firma, por parte del personal autorizado, de la declaración de lectura de la parte que les afecte del plan de protección de la zona de acceso restringido, según el modelo del anexo IV de este documento.

7. ANÁLISIS DE RIESGOS EN ZONAS DE SEGURIDAD

A la hora de enfrentarse con el problema de decidir las medidas específicas de seguridad física y de otra índole, necesarias para asegurar la protección de una instalación en la que se va a manejar o almacenar información clasificada, existen dos aproximaciones posibles. Una es la aplicación de estándares fijos de protección que permitan dar una seguridad adecuada en cualquier condición y situación, lo que constituye una solución que va a exigir mayores recursos iniciales, pero es más estable y permite mantener la seguridad de forma más automática.

Otra opción es la considerar los riesgos existentes, evaluando de la forma más aproximada posible las amenazas y vulnerabilidades que afectan o pueden afectar a dicha instalación en cada momento, mediante lo que se conoce como **análisis de riesgos**. Esta opción permite optimizar los recursos empleados, pero exige una mayor disciplina de seguridad, y mantener una gestión continua del riesgo existente, para adaptarse a las situaciones cambiantes sin merma de la protección en ningún momento.

El análisis de riesgos es, en este marco, el proceso por el que se identifican las amenazas y vulnerabilidades contra la seguridad de una instalación, se determina su magnitud y se descubren las áreas que necesitan medidas específicas de seguridad física o de otra índole. El análisis de riesgos sirve para identificar el riesgo existente y evaluar la actual seguridad de una instalación en relación con el manejo de información clasificada, para a continuación reunir la información necesaria para seleccionar las medidas de seguridad más eficaces.

El análisis de riesgos no es una tarea que se haga una única vez. Debe realizarse periódicamente, con objeto de que se mantenga actualizado frente a los cambios. La gestión del riesgo supone planificación, organización, dirección y control de recursos para garantizar que el riesgo permanece dentro de unos límites y un coste aceptables.

El proceso de análisis de riesgos es un ejercicio de recolección y valoración de datos que aborda dos cuestiones básicas: los activos que corren peligro, especialmente la información clasificada, y cuáles serían el impacto o las consecuencias si las vulnerabilidades identificadas fueran explotadas con éxito.

Una ventaja importante es que, a través del análisis de riesgos, se aumenta la concienciación en materia de seguridad, que debe estar presente en todos los niveles de la organización, desde el más alto nivel de gestión hasta el personal auxiliar y de operaciones. Asimismo, el resultado del proceso de gestión del riesgo puede facilitar detalles importantes a incluir en la documentación de seguridad requerida, en concreto en el plan de protección.

La presente norma no trata en detalle sobre procedimientos de análisis de riesgos, ni sobre los estándares de seguridad aplicables en cada situación. La Oficina Nacional desarrollará guías adicionales (orientaciones) para facilitar la aplicación de dichos conceptos.

En cualquier caso, en la mente de todo responsable de seguridad debe existir siempre una concepción del riesgo, y tratar de identificar en todo momento las amenazas presentes o posibles, y las vulnerabilidades de las que se pueda adolecer, de forma que el diseño de la protección a aplicar, volcado en el plan de protección, permita hacer frente a las mismas.

8. MEDIDAS ESPECÍFICAS DE SEGURIDAD FÍSICA

8.1. Generalidades

Se expone a continuación la enumeración y descripción, con un carácter general y sin entrar al detalle técnico, de las medidas específicas de seguridad física que se contemplan para la constitución de zonas de seguridad.

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 y volumen de la información a proteger.

En el documento "**Orientaciones para la constitución de zonas de acceso restringido"**, elaborado por la Oficina Nacional, se describen los estándares de medidas de seguridad para la protección de zonas donde de almacena o maneja información clasificada, aprobados por la Autoridad Nacional, a aplicar según el grado de clasificación y otras condiciones que sea preciso atender.

En otro documento denominado "**Orientaciones para el manejo de información clasificada con grado de DIFUSIÓN LIMITADA"**, elaborado igualmente por la Oficina Nacional, se incluirán las medidas de seguridad a aplicar en las zonas administrativas de protección en que se maneje o almacene información clasificada con grado de "DIFUSIÓN LIMITADA o equivalente".

8.2. Medidas estructurales

8.2.1. Perímetro de seguridad

Una cierre perimetral es una barrera física que identifica el área o zona que requiere protección. 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 instalados en la parte superior del mismo como: alambradas, sistemas de detección de intrusión, alumbrado de seguridad ó un circuito cerrado de televisión.

8.2.2. 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. 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.

8.2.3. 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.

Los dispositivos de cierre de las puertas que dan acceso a las zonas de acceso restringido serán accionados por cerraduras del grupo correspondiente a su grado de clasificación.

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 muelles telescópicos, que tiendan a mantener las puertas cerradas una vez franqueado el paso por las mismas.

8.2.4. 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.

8.2.5. Conductos

Los conductos de ventilación o cualquier otra apertura que pueda existir en los paramentos de una zona de acceso restringido, cuando sean de tamaño tal que supongan una vulnerabilidad de acceso no autorizado, deberán protegerse con barras de acero soldadas formando cuadro, sujetas firmemente con pernos a la estructura en el interior de la abertura.

8.2.6. Ventanas

Las ventanas existentes en la propia zona de acceso restringido, estarán provistas de un sistema de alarma contra apertura, rayado o rotura. Los cristales deberán ser opacos o translúcidos, de forma que se impida cualquier visión nítida desde el exterior.

Cuando los mismos muros del edificio constituyen en parte o por completo el perímetro de seguridad, todas las ventanas y conductos situados a menos de 5,5 metros por encima del nivel del suelo, en zonas no controladas, así como a igual distancia de los tejados, cornisas o bajantes de agua, deberán protegerse con barras de acero soldadas formando cuadro, sujetas firmemente con pernos a la estructura en el interior de la ventana o abertura.

8.3. 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).

8.4. Sistemas de detección de intrusión (conocidos por la sigla inglesa IDS)

Los IDS 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 respuesta ó fuerza de apoyo, que actúe en un tiempo razonable en caso de alarma.

8.5. Control de acceso

8.5.1. Generalidades

El control de acceso 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, electromecánico, mediante guardia o recepcionista.

Debe permitir la segregación de accesos en función de la necesidad de conocer.

8.5.2. Guardia de seguridad o recepcionista

Los guardias de seguridad deberán contar con una HPS 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.

8.5.3. Control de acceso automatizado

Un sistema de control de acceso automatizado deberá ser capaz de identificar al individuo que trata de entrar en la zona de seguridad, verificando su autorización para entrar en la misma. Permitirá asegurar que sólo el personal titular de una habilitación de seguridad apropiada y debidamente autorizado es admitido en una zona de acceso restringido.

Los sistemas de control de acceso automatizado se dividen en:

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

- 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 (conocido por la sigla inglesa 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.

8.6. Identificación de seguridad (pase)

Es necesario un sistema eficaz de identificación del personal, que facilite la circulación al personal autorizado para acceder a los distintos entornos de seguridad, 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.

8.7. 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.

8.8. 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.

8.9. 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.

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.

8.10. 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 o responsable de seguridad 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 veinticuatro (24) horas. En ningún caso dispondrán de los elementos que permitan la apertura de las cajas fuertes o de las cámaras acorazadas.

8.11. 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 convenientes 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.
- Auditoría: 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.

8.12. 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 trampillas acorazadas. Dado su alto grado de fortaleza y protección, se permite en estas cámaras acorazadas el almacenar información clasificada fuera de contenedores de seguridad.

8.13. Registros en 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 en entradas y salidas 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 a la entrada o salida de un determinado establecimiento o local.

8.14. Control de visitas

8.14.1. Generalidades

Toda zona de acceso restringido dispondrá de una lista de personal autorizado (anexo III), 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.

8.14.2. 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.

8.14.3. 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.

9. SEGURIDAD FÍSICA EN INSTALACIONES QUE ALBERGAN EQUIPOS DE INFORMACIÓN Y COMUNICACIONES

En instalaciones donde la información clasificada es visualizada, almacenada, procesada o transmitida utilizando sistemas de información y comunicaciones, o donde un potencial acceso a esa información sea posible, deberán establecerse los requerimientos necesarios para asegurar el cumplimiento de los objetivos de seguridad: confidencialidad, integridad y disponibilidad.

Las instalaciones en las que los sistemas de información y comunicaciones son

utilizados para visualizar, almacenar, procesar o transmitir información clasificada de grado "CONFIDENCIAL o equivalente" o superior, 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 Autoridad Nacional.

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 interrumpida. Las alertas asociadas con los controles medioambientales deberán ser permanentemente monitorizadas por el centro de control de alarmas.

Certificado de acreditación de locales

CERTIFICADO DE ACREDITACIÓN DE LOCALES

(NÚMERO DE CERTIFICADO: CAL-0191 – FECHA DE EXPIRACIÓN: 11.02.2015)

OFICINA NACIONAL DE SEGURIDAD
AREA DE SEGURIDAD DE LA INFRAESTRUCTURA Y DEL PERSONAL

SUBREGISTRO PRINCIPAL	SUBREGISTRO PRINCIPAL OTAN/UE/ESA DE ...
ORGANISMO / EMPRESA	
DIRECCIÓN COMPLETA	
DEPENDENCIA ACREDITADA	
RESPONSABLE	
JUSTIFICACIÓN	
ESCRITO REMISIÓN PLAN DE PROTECCIÓN	

CLASIFICACIÓN: ZONA DE ACCESO RESTRINGIDO CLASE I
GRADO Y TIPOS: RESERVADO / NATO SECRET / EU SECRET

CUALQUIER MODIFICACIÓN DEL LOCAL ACREDITADO DEBERÁ SER APROBADA POR LA OFICINA NACIONAL. EN CASO CONTRARIO ESTE CERTIFICADO NO SERÁ VÁLIDO.

Madrid, __ de _____ de 20___
EL JEFE DE AREA,

Formulario FPO-ASIP-01-06.02

Certificado de inspección y cumplimiento

CERTIFICADO DE INSPECCIÓN Y CUMPLIMIENTO QUE FORMULA EL JEFE DE SEGURIDAD DEL SUBREGISTRO PRINCIPAL ..... , RELATIVO A LA ZONA DE ACCESO RESTRINGIDO DE .....

CERTIFICO:

Que el Plan de Protección que se adjunta, así como las propias instalaciones y medios, de la Zona de Acceso Restringido de ..... , han sido todos ellos revisados e inspeccionados y se ha verificado que las medidas y procedimientos de seguridad implantados son suficientes y conformes con los requerimientos dictados por la Oficina Nacional, sobre la base de la normativa de seguridad en vigor.

En ....., a .. de .....de 20….

El Jefe de Seguridad

Fdo: .....

Lista de personal autorizado

LISTA DE PERSONAL AUTORIZADO CON ACCESO A LA ZONA DE ACCESO RESTRINGIDO

Identificación de la ZAR: _____

- .....
- .....
- .....
- .....
- .....
- .....
- .....
- .....
- .....
- .....
- .....
- .....
- .....

Declaración de lectura

DECLARACIÓN DE HABER LEÍDO EL PLAN DE PROTECCIÓN

Identificación de la ZAR: _____

Certifico haber leído y comprendido el Plan de Protección.

Usuario: _____

Nombre y empleo: _____

Despacho y extensión: _____

Fecha: _____

Firma:

Fecha de activación del acceso a ZAR: _____

Responsable de seguridad: _____

Despacho y extensión: _____

Firma: