AUTORIDAD DELEGADA PARA LA SEGURIDAD
DE LA INFORMACIÓN CLASIFICADA

NORMAS DE LA AUTORIDAD NACIONAL PARA LA PROTECCIÓN DE LA INFORMACIÓN CLASIFICADA

MINISTERIO DE DEFENSA

Autoridad Delegada para la
Seguridad de la Información Clasificada

Normas de la Autoridad Nacional para la Protección de la Información Clasificada

MINISTERIO DE DEFENSA

CATÁLOGO GENERAL DE PUBLICACIONES OFICIALES
http://publicacionesoficiales.boe.es/

Edita:

MINISTERIO DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

https://publicaciones.defensa.gob.es/

NIPO: 083-19-041-6 (edición papel)
NIPO: 083-19-040-0 (edición en línea)

Depósito Legal: M-37291-2018
Cuarta edición
Maqueta e imprime: Ministerio de Defensa

En esta edición se ha utilizado papel 100 % libre de cloro procedente de bosques gestionados de forma sostenible.

En la sociedad actual, la información es un valor y su tratamiento no debe ser ajeno a la eficaz labor de la Administración del Estado. Exige el acceso a una enorme variedad de fuentes de información e impone la transparencia como una exigencia al trabajo de cada día.

Esa exigencia incuestionable de transparencia viene constitucionalmente delimitada por la existencia de determinados tipos de información que deben gozar de protección especial. Y este es el caso de la información clasificada, que afecta a la seguridad nacional.

Dicho reconocimiento constitucional implica que, la protección de la información relacionada con la defensa y la seguridad nacional, se convierta en un elemento indispensable para la salvaguarda de los intereses fundamentales de España y de los españoles.

La protección se dirige no sólo a la información asociada a operaciones militares, policiales o de inteligencia, que permite al Gobierno tomar las decisiones adecuadas, sino también aquella información asociada a actividades diplomáticas, científicas, económicas o industriales, que contribuye de manera fundamental y decisiva al desarrollo y progreso de España.

El enorme incremento de las actividades de ciberespionaje y el crecimiento exponencial del número de ciberataques sufridos en todas las actividades de nuestra sociedad, basados en el uso de nuevas tecnologías, convierten la necesidad de proteger nuestra información estratégica, en una exigencia clave para la estabilidad y seguridad nacionales.

La importancia que tiene la protección de la información clasificada viene recogida, además, en la propia Ley de Secretos Oficiales y en la Estrategia de Seguridad Nacional, donde se reconoce que la información clasificada es un objetivo fundamental para los servicios de inteligencia hostiles, para grupos terroristas que tienen por objetivo la amenaza a nuestra seguridad y la desestabilización de nuestro sistema democrático, y para otros países con intereses económicos o comerciales en competencia con los de nuestra industria.

Otro factor importante, de la protección de la información clasificada, lo constituye el de su tratamiento dentro del ámbito empresarial. La necesidad de preservar las garantías de protección de la información en el desarrollo de aquellos contratos o proyectos en los que se produce o maneja información clasificada, implica para las empresas la obligación de prestar una especial atención a cumplir con una serie de requisitos y obligaciones de seguridad. Requisitos que, por su importancia y especificidad, se plasman en una norma específica dedicada a la seguridad de la información clasificada en el ámbito industrial.

Todo lo anterior también es de aplicación en el marco de las relaciones exteriores donde la globalización impone como exigencia el intercambio de información clasificada. Sin embargo, ningún país se muestra proclive a ceder su información si no cuenta con las garantías suficientes de que dicha información va a ser convenientemente protegida, por lo que el receptor debe contar con una base legislativa suficiente que garantice a los interlocutores internacionales una seguridad válida para su propia información.

Con la presente edición actualizada de las «*Normas de la Autoridad Nacional de Seguridad para la protección de la información clasificada*» se pretende dar adecuada respuesta a los retos señalados en los párrafos anteriores, proporcionando la herramienta adecuada para proteger la información clasificada de forma eficaz, siendo ésta la herramienta sobre la que se ha volcado todo el conocimiento adquirido por la Oficina Nacional de Seguridad, a lo largo de sus ya más de treinta años de experiencia, tanto en el ámbito nacional como en el internacional.

Madrid, a 4 de octubre de 2018

La Autoridad Delegada para la
Seguridad de la Información Clasificada

Fdo: Félix Sanz Roldan
Secretario de Estado Director del CNI

Índice

NORMA NS/00

LA PROTECCIÓN DE LA INFORMACIÓN CLASIFICADA EN ESPAÑA

1. LEGISLACIÓN APLICABLE

La **Constitución española** en su artículo 105 b) establece el principio general de publicidad de los actos de la Administración, de la forma siguiente: «*La Ley regulará el acceso de los ciudadanos a los archivos y registros administrativos, salvo en lo que afecte a la seguridad y defensa del Estado, la averiguación de los delitos y la intimidad de las personas*».

Por su parte, la **Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno**, en su artículo 12, establece que «*Todas las personas tienen derecho a acceder a la información pública, en los términos previstos en el artículo 105 b) de la Constitución Española, desarrollados por esta Ley.*», declarando, en su artículo 14 las limitaciones a ese principio general de acceso, entre las cuales se encuentran la seguridad nacional, la defensa y la seguridad pública. Así mismo, en la disposición adicional primera, apartado 2, dispone que «*Se regirán **por su normativa específica**, y por esta Ley con carácter supletorio, aquellas materias que tengan previsto un régimen jurídico específico de acceso a la información.*»

Todo ello significa que, la información clasificada, cuyo acceso queda limitado por Ley, deberá regirse por su propia normativa que, actualmente y a mayor nivel, está constituida por la **Ley 9/1968, modificada por la Ley 48/78, sobre Secretos Oficiales**, y su **Decreto de desarrollo 242/1969**.

La **Ley 24/2011**, de 1 de agosto, de **contratos del sector público en los ámbitos de la defensa y de la seguridad**, exige, en su disposición adicional quinta, que las empresas que vayan a acceder a información clasificada con motivo de la

contratación en estos ámbitos, han de regirse por las disposiciones que dicte la «*Autoridad Nacional para la Seguridad de la Información Clasificada*».

La **Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia**, en su artículo 4, encomienda a este organismo la función de «*Velar por el cumplimiento de la normativa relativa a la protección de la información clasificada*». A dicho fin, y motivado por el amplio espectro de obligaciones a las que ha de darse cumplimiento, se promulgan las Normas de la Autoridad Nacional para la Protección de la Información Clasificada, que se constituyen como normativa básica para la protección de la información clasificada, con independencia de su origen y clasificación, en la seguridad de que con su cumplimiento se satisfacen todas las exigencias de protección existentes.

Estas **Normas de la Autoridad Nacional para la Protección de la Información Clasificada** constituyen el desarrollo normativo con el que se regula el manejo de la información clasificada en España y se da respuesta a las obligaciones contraídas en el ámbito internacional por nuestro país con otros estados u organizaciones internacionales, que más adelante se desarrollan.

2. CONCEPTO DE INFORMACIÓN CLASIFICADA

Por información clasificada se entenderá cualquier información o material respecto del cual se decida que requiere protección contra su divulgación no autorizada y a la que se ha asignado una clasificación de seguridad.

En este sentido hay que tener en cuenta que cuando hablamos de información no nos estamos refiriendo sólo a documentos en papel, sino también a cualquier material (armamento, piezas industriales…) o a aquella información contenida en sistemas de información y comunicaciones.

Aunque la Ley de Secretos Oficiales en su decreto de desarrollo impone la denominación de «materias clasificadas», por motivos de unificación y adaptación a la práctica internacional actual, a lo largo del texto se utilizará la denominación de «información clasificada» en lugar de «materia clasificada».

En función de su origen, distinguimos entre información clasificada nacional (la que ha sido generada por los organismos del Estado y clasificada por los órganos con competencias para ello), e información clasificada internacional (la que ha sido generada por los organismos u organizaciones internacionales de los que España es país miembro, o por otros países con los que España ha concluido un acuerdo para la protección de información clasificada).

3. TRATAMIENTO DE LOS DISTINTOS TIPOS DE INFORMACIÓN

Debido a la existencia de distintos tipos de información según su origen, podrán existir dos estructuras de protección diferenciadas en cuanto a su dependencia funcional: una para información clasificada nacional y otra para la internacional.

Siempre que ello sea posible, cuando un ministerio, organismo o entidad deba almacenar o manejar distintos tipos de información clasificada, se intentará, por economía de recursos y de una forma práctica, que la responsabilidad de ambas estructuras recaiga en las mismas unidades y personas, dado que los mecanismos y sistemas de protección son equivalentes.

Cuando hablamos de estructura de protección nos referimos, no sólo a un sistema de registro y control documental, sino a un sistema completo de protección que incluye medios materiales o físicos, humanos y organizativos.

Además, mediante la elaboración de una normativa de protección unificada, la aplicación de unos criterios adecuados de selección del personal, la asignación de unos recursos adecuados para su ejecución y la firme voluntad de cumplimiento basada en la concienciación, a todos los niveles, sobre la necesidad de proteger, conseguiremos un nivel de protección óptimo de la información clasificada.

Por decisión del jefe o responsable de un determinado ministerio, organismo o entidad, y al amparo de lo señalado en la **Ley 9/1968, modificada por la Ley 48/78, sobre Secretos Oficiales**, y su **Decreto de desarrollo 242/1969**, se constituyen los servicios de protección de información clasificada (SPIC), como las estructuras encargadas de garantizar la adecuada protección de la información clasificada a cargo de su ministerio, organismo o entidad.

Cada SPIC estará bajo el mando de un **jefe de seguridad del servicio de protección**, que será responsable del cumplimiento de todos los cometidos, ante el jefe del organismo o entidad al que presta servicio, y que dependerá funcionalmente de la Autoridad Nacional para la Protección de la Información Clasificada en el ámbito de competencias de esta última, a través de la Oficina Nacional de Seguridad.

Bajo la dependencia funcional del SPIC se establecerán los órganos de control que se consideren necesarios para la adecuada protección de la información clasificada a cargo del ministerio, organismo o entidad.

En el marco legislativo actual, la diferencia fundamental entre las dos estructuras (nacional e internacional) para la protección de la información clasificada con-

siste en su dependencia funcional. Es decir, debido a la especial configuración establecida por la Ley de Secretos Oficiales, los **servicios de protección de información clasificada nacional** dependerán **orgánica y funcionalmente** del Ministro o del jefe superior del organismo o entidad correspondiente, y, sin embargo, los **servicios de protección de información clasificada internacional** dependen orgánicamente del Ministro o del jefe superior del organismo o entidad correspondiente **y funcionalmente** de la Autoridad Nacional para la Protección de la Información Clasificada (ANPIC) nombrada especialmente al efecto por el Gobierno de España.

Las particularidades correspondientes a las dependencias de estos Servicios de Protección en el ámbito industrial están señaladas en la Norma específica sobre Seguridad Industrial.

4. INFORMACIÓN CLASIFICADA NACIONAL

La Ley de Secretos Oficiales y su Decreto de desarrollo prevén la existencia en los departamentos ministeriales de los **servicios de protección de información clasificada**, como unidades centrales o dependencias afectas a los ministros respectivos para la protección de la información clasificada. Entre los cometidos que se asigna a estas unidades está el de elaborar las condiciones de seguridad específicas del ministerio y constituir los procedimientos adecuados.

En consecuencia, la Ley impone que en todo organismo o entidad, el jefe sea el responsable de la adecuada protección de la información clasificada, tanto en su custodia como en su manejo. Para asegurar el cumplimiento de sus cometidos en este aspecto, deberá disponer de los medios y recursos adecuados, es decir, de una estructura funcional y orgánica responsable de la ejecución de dicha protección.

Por su parte, la labor de tutela sobre la protección de la información clasificada que la anteriormente citada Ley 11/2002 confiere al CNI, obliga a establecer unos parámetros de referencia comunes a todo el ámbito nacional, aplicables a las condiciones de seguridad y procedimientos para la protección de la información clasificada. Dichos parámetros comunes deberán ser recogidos en las políticas individuales de cada uno de los departamentos ministeriales, de forma que estas sean uniformes y mutuamente compatibles tanto en el ámbito nacional como en el internacional.

Las presentes Normas de la Autoridad Nacional para la Protección de la Información Clasificada, promulgadas por el Secretario de Estado Director del Centro

Nacional de Inteligencia, pretenden cubrir dichos aspectos. Si a ello se une el valor añadido de que estos parámetros de referencia se adaptan a los estándares internacionales, con el uso de estas Normas se habrá conseguido un beneficio en cuanto a economía de medios, personal y procedimientos, que redundará en una mayor eficacia y eficiencia de estos servicios de protección, y en cuanto a interoperabilidad en todos los ámbitos.

5. INFORMACIÓN CLASIFICADA INTERNACIONAL

5.1. Organizaciones internacionales

La pertenencia de España a organizaciones internacionales como la Organización del Tratado del Atlántico Norte (OTAN), la Unión Europea (UE) o la Agencia Espacial Europea (ESA)[1] obliga a la asunción de las políticas y acuerdos de seguridad de cada una de ellas, mediante la ratificación por España de tratados internacionales sobre seguridad de la información.

Estas políticas obligan a que en cada país miembro exista una autoridad nacional de seguridad (ANS), como figura responsable de garantizar el cumplimiento de la normativa de seguridad derivada de las citadas políticas y acuerdos.

En España, mediante Acuerdo de Consejo de Ministros de 21 de mayo de 2012, basado en los precedentes acuerdos de Consejo de Ministros de 1982, 2002 y 2005, se designa Autoridad Nacional de Seguridad para la protección de la información clasificada originada por la OTAN, la UE y la ESA a los Ministros de la Presidencia, de Defensa y de Asuntos Exteriores y de Cooperación, de forma conjunta, quienes por Acuerdo de Consejo de Ministros, delegan dicha función en el Secretario de Estado Director del Centro Nacional de Inteligencia.

Con la finalidad de implementar dichas políticas y acuerdos de seguridad, surge la necesidad de establecer una estructura que garantice la adecuada protección de la información clasificada que estas organizaciones internacionales confían a España, y que permita que la información sea gestionada y manejada de forma segura. La estructura se basa en la existencia de una serie de **servicios de protección de información clasificada internacional**, con idénticas misiones y cometidos que los servicios de protección para la información clasificada nacional. Estos servicios de protección **dependerán funcionalmente** de la ANPIC.

[1] Se utiliza la sigla en inglés (ESA, de «*European Space Agency*»)

Siempre que ha sido posible, se ha procurado que esta estructura se integre con la de protección a nivel nacional, aunque pueden existir casos en los que haya estructuras independientes.

Por iguales criterios prácticos de unificación, se ha adoptado la denominación de Autoridad Nacional para la Protección de la Información Clasificada (ANPIC), en la esfera nacional referida al Secretario de Estado Director del CNI, como ejecutor de la misión asignada en la Ley 11/2002. Por lo que, a lo largo de las Normas, se utilizará la expresión ANPIC.

5.2. Acuerdos para la protección de la información clasificada

Un acuerdo para la protección de la información clasificada es un tratado internacional ratificado por el Parlamento, firmado entre dos o más países, por medio del cual se dan garantías mutuas sobre la protección de la información clasificada que, sobre la base de dicho acuerdo, se intercambie o ceda entre las partes firmantes, obligándose estas a cumplir exactamente lo establecido en su articulado.

El Gobierno ha venido facultando al Secretario de Estado Director del CNI para negociar con otros estados, en nombre del Reino de España, los acuerdos para la protección de la información clasificada.

Estos acuerdos se negocian sobre la base de las presentes Normas y en ellos se define la existencia de una figura responsable de la aplicación de lo establecido en aquellos. Esta responsabilidad se hace recaer, en el caso de España, en la ANPIC.

Los acuerdos se constituyen en tratados internacionales de obligado cumplimiento interno al entrar a formar parte de la legislación española, y son fuente de obligaciones internacionales por cuanto España se compromete a custodiar la información clasificada recibida conforme a los términos establecidos.

En España, la protección de la información clasificada perteneciente a otros países se efectuará a través de los **servicios de protección de información clasificada internacional.** No obstante, cuando así se estime oportuno y con autorización expresa de la ANPIC, estas competencias podrán ser asumidas por los servicios de protección de la información clasificada nacional.

6. GRADOS DE PROTECCIÓN DE LA INFORMACIÓN CLASIFICADA

La información se clasifica en distintos grados en función del daño que su difusión pueda ocasionar a la seguridad nacional.

Con la finalidad de que los distintos tipos de información clasificada puedan tener un tratamiento equiparable según su grado de clasificación, se ha de establecer un sistema de equivalencias con las clasificaciones existentes a nivel internacional. Dichas equivalencias se determinan en los acuerdos de seguridad, tanto de las organizaciones internacionales (equivalencia entre las clasificaciones de seguridad de la organización y de cada uno de los estados miembros), como de los países con los que España ha firmado un acuerdo para la protección de la información clasificada (equivalencia entre las clasificaciones de seguridad de cada uno de los estados firmantes del acuerdo).

En España existen las materias clasificadas (denominación adoptada por la Ley de Secretos Oficiales), que son SECRETO y RESERVADO, y materias de reserva interna, que son CONFIDENCIAL y DIFUSIÓN LIMITADA.

Por todo ello, y para distinguir, en los casos que sea necesario, entre los distintos requisitos de manejo de la información nacional y de la internacional, a lo largo de las Normas se hablará de:

- Información clasificada de grado SECRETO, RESERVADO, CONFIDENCIAL y DIFUSIÓN LIMITADA, en referencia exclusivamente a información nacional.
- Información «SECRETO o equivalente», «RESERVADO o equivalente», «CONFIDENCIAL o equivalente» y «DIFUSIÓN LIMITADA o equivalente» para referirse a información clasificada tanto nacional como internacional que merece un mismo grado de protección.
- Información «equivalente a SECRETO», «equivalente a RESERVADO», «equivalente a CONFIDENCIAL» y «equivalente a DIFUSIÓN LIMITADA», cuando se excluya a la información clasificada nacional española.

7. NORMAS DE LA AUTORIDAD

Las presentes Normas de la ANPIC pretenden dar respuesta a todas las necesidades de protección de la información clasificada en todos los ámbitos, estructurándose, en seis normas diferentes pero complementarias:

- La protección de la información clasificada en España (NS/00), mediante la que se exponen los principios básicos sobre la información clasificada y su forma de protegerla en España.
- Estructura nacional de protección de la información clasificada (NS/01), mediante la que se establecen los requisitos orgánicos y funcionales necesarios para que en un organismo o entidad se maneje información clasificada.

- Seguridad en el personal (NS/02), mediante la que se exponen todos los requerimientos para el acceso a la información clasificada y, especialmente las vicisitudes referidas a la Habilitación Personal de Seguridad (HPS).
- Seguridad física (NS/03), mediante la que se establecen las medidas requeridas en las zonas donde se maneje información clasificada, de forma que se controlen los accesos autorizados a dicha información y se impidan los no autorizados.
- Seguridad de la información (NS/04), mediante la que se establece la forma en la que se ha de manejar la información clasificada.
- Seguridad en los sistemas de información y comunicaciones (NS/05), mediante la que se establecen los requisitos que debe reunir un sistema de información y comunicaciones para poder manejar en él información clasificada.
- Seguridad industrial (NS/06), mediante la que se especifican los especiales requerimientos, en el ámbito industrial, para el manejo de la información clasificada como consecuencia del desarrollo de contratos, proyectos o programas clasificados.

NORMA NS/01

ESTRUCTURA NACIONAL DE PROTECCIÓN DE LA INFORMACIÓN CLASIFICADA

1. ÁMBITO DE APLICACIÓN

Las Normas de la Autoridad Nacional para la Protección de la Información Clasificada son de aplicación a las Administraciones Públicas, las Fuerzas Armadas, los organismos públicos vinculados o dependientes de los anteriores, y las entidades públicas o privadas que manejen o tengan acceso a información clasificada nacional, o a la perteneciente a organismos u organizaciones internacionales de las que el Reino de España forma parte en virtud de un tratado, o a la de otro país, que haya sido entregada a España al amparo de un tratado para la protección de la información clasificada.

2. ESTRUCTURA NACIONAL DE PROTECCIÓN

2.1. Constitución

La estructura nacional de protección de la información clasificada es el conjunto de todos los órganos y servicios que se ocupan de la protección de la información clasificada manejada en España, sea nacional o internacional.

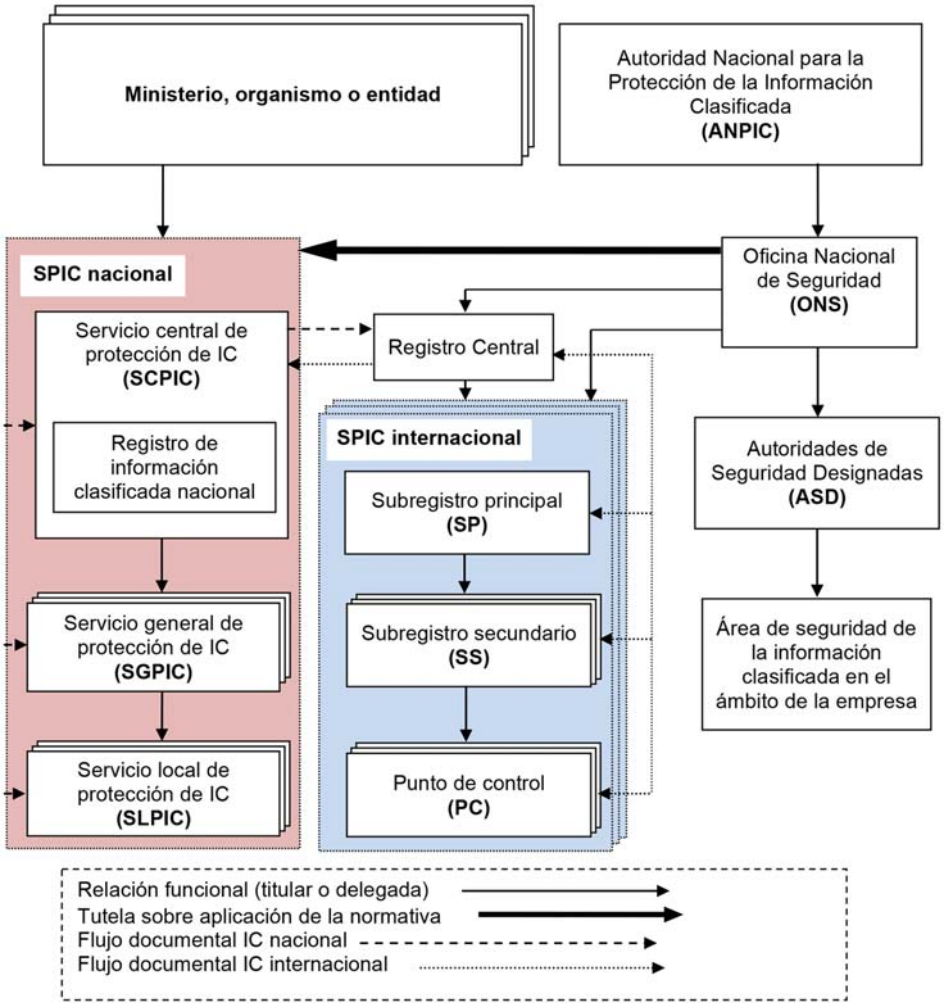
Forman parte de la estructura nacional de protección de la información clasificada:

- La Autoridad Nacional para la Protección de la Información Clasificada (ANPIC).
- La Oficina Nacional de Seguridad (ONS).
- El Registro Central.

- Los servicios de protección de información clasificada (SPIC), con sus órganos de control subordinados e instalaciones separadas constituidas como zonas de acceso restringido (ZAR) dependientes.
- Las Autoridades de Seguridad Designadas (ASD)

Esta estructura está organizada, dentro de cada tipo de información (nacional o internacional), de forma piramidal, basada en los órganos de control (ver diagrama a continuación).

Podrán constituirse ZAR en que se maneje información clasificada sin que tengan que ser un órgano de control. No obstante, estas ZAR dependerán siempre de un órgano de control y contarán con un responsable de seguridad.



2.2. Autoridad Nacional para la Protección de la Información Clasificada (ANPIC)

En virtud de lo señalado en la Ley 11/2002 y Acuerdos de Consejo de Ministros por los que se designa a la Autoridad nacional de Seguridad y su Autoridad delegada, la ANPIC es la figura responsable en España de la protección de la información clasificada, recayendo esta responsabilidad en el Secretario de Estado Director del Centro Nacional de Inteligencia (SEDCNI).

Con carácter general tiene asignadas las siguientes funciones:

a) Velar por el cumplimiento de la legislación y normativa de desarrollo relativa a la protección de la información clasificada.
b) Elaborar y aprobar las normas de desarrollo para la protección de la información clasificada.
c) Valorar la idoneidad de las personas que deban tener acceso a la información clasificada y emitir el correspondiente certificado en forma de Habilitación Personal de Seguridad (HPS).
d) Autorizar el establecimiento o disolución de los servicios de protección de información clasificada internacionales y el de los nacionales bajo su responsabilidad funcional directa, así como de los órganos de control que los componen.
e) Valorar la idoneidad de las entidades privadas que deban tener acceso a información clasificada, en función de un programa, contrato o actividad clasificada, emitiendo el correspondiente certificado en forma de Habilitación de Seguridad de Empresa (HSEM) y de Establecimiento (HSES).
f) Certificar ante los países u organismos nacionales o internacionales, cuando así lo soliciten, la idoneidad para acceder o manejar información clasificada de organismos, entidades públicas o privadas y personas.
g) Garantizar que se realizan las correspondientes inspecciones periódicas sobre las medidas de seguridad para la protección de la información clasificada.
h) Aprobar los planes de protección.
i) Relacionarse, en nombre del Gobierno de España, con las autoridades competentes de las organizaciones internacionales y de otros países, para los temas relacionados con la protección de la información clasificada.
j) Designar los representantes españoles en los comités y grupos de trabajo de las organizaciones internacionales encargados de la protección de la información clasificada.
k) Negociar los Acuerdos para el intercambio de información clasificada con otros países u organizaciones internacionales.
l) Autorizar los sistemas CIS que deban manejar información clasificada.

En el ámbito específico de la seguridad industrial, la ANPIC podrá nombrar autoridades de seguridad designadas (ASD) las cuales se encargarán de la imple-

mentación correcta de la política de seguridad industrial. Normalmente, el ámbito de competencia de una ASD será el ministerial. Estas ASD estarán bajo la dependencia funcional de la ANPIC y responderán ante ella de sus actuaciones. En ausencia de ASD, esta función será realizada por la propia ANPIC. Esta figura se trata específicamente en el **apartado 2.5** de esta norma.

2.3. Oficina Nacional de Seguridad (ONS)

La Oficina Nacional de Seguridad (ONS) es el órgano de trabajo de la ANPIC y, asume las siguientes funciones:

a) Ejecutar los cometidos y decisiones de la ANPIC
b) Dirigir, controlar y supervisar la actuación de los servicios de protección de información clasificada (SPIC).
c) Inspeccionar los SPIC, e indicar las medidas de seguridad preventivas y correctivas que deban ser adoptadas.
d) Promocionar, orientar y supervisar el cumplimiento de la normativa relativa a la protección de la información clasificada en cualquier ámbito.
e) Participar en representación de España en los Comités de Seguridad de los diferentes organismos y organizaciones internacionales.
f) Elaborar las normas de desarrollo para la protección de la información clasificada.
g) Difundir la normativa y procedimientos de seguridad, y exigir el cumplimiento de las obligaciones derivadas de los tratados para la protección de la información clasificada suscritos por España.

2.4. Registro Central

Es el órgano, encuadrado orgánicamente en la ONS, responsable de velar por que dentro de la estructura nacional de protección de la información clasificada internacional se lleve a cabo de forma correcta la recepción, registro, archivo, distribución y remisión de la información.

El Registro Central tiene las siguientes funciones:

a) Llevar a cabo la recepción, registro, control, archivo, distribución y remisión de la documentación clasificada de ámbito internacional entregada a España, que se reciba a través, o con el concurso, de dicho Registro Central.
b) Realizar el registro, seguimiento y control exhaustivo de los documentos de grado «equivalente a SECRETO» que entren en la estructura nacional

de protección de la información clasificada, con independencia del canal por el que se cursen. Dará las instrucciones precisas, y establecerá los procedimientos, para que cualquier órgano de control destinatario que reciba este tipo de documentación lo comunique formalmente, con la mayor brevedad, por los conductos funcionales reglamentarios, conociendo su localización exacta en todo momento.

c) Realizar el inventario anual de los documentos de grado «equivalente a SECRETO» presentes en el sistema de registro en España, para su remisión a las oficinas de seguridad de las organizaciones internacionales originadoras y propietarias, en las fechas y con los criterios que rijan para cada caso.

d) Estar informado de cualquier comprometimiento o infracción de seguridad detectados en la recepción, registro, archivo, distribución y remisión de la documentación clasificada de grado «equivalente a CONFIDENCIAL» o superior, o con limitaciones especiales, ocurrido en un órgano de control.

e) Controlar los datos de contacto y las relaciones de firmas reconocidas de los subregistros principales, así como de aquellos servicios centrales de protección de información clasificada con los que se relaciona.

f) Mantener al día la relación de registros extranjeros con los que se mantenga intercambio documental, así como los datos de contacto y firmas reconocidas de sus responsables.

g) Planificar y ejecutar la transmisión por medios tecnológicos y el transporte de documentos clasificados que entren o salgan de la estructura nacional a través del Registro Central.

h) Dirigir la actividad de los correos oficiales españoles que realizan estos transportes.

i) Emitir, distribuir y controlar los certificados de correo, necesarios para autorizar los transportes de información clasificada por los servicios de protección de IC internacional.

j) Mantener contacto frecuente con los SPIC para asesorar y supervisar el correcto tratamiento de la información clasificada.

k) Proponer las medidas que considere adecuadas para corregir posibles vulnerabilidades en materia de protección.

l) Participar en las inspecciones ordinarias y extraordinarias a los servicios de protección de IC internacional.

2.5. Servicios de protección de información clasificada

2.5.1. Generalidades

En todo ministerio, organismo o entidad, el jefe es responsable de la adecuada protección de la información clasificada, tanto en su custodia como en su manejo.

Para asegurar el cumplimiento de sus cometidos en este aspecto, deberá disponer de los medios y recursos adecuados, es decir, de una estructura funcional y orgánica responsable de la ejecución de dicha protección.

Esta estructura, considerada al más alto nivel de la organización, recibe el nombre de **servicio de protección de información clasificada (SPIC)**, que estará bajo el mando de un jefe de seguridad del servicio de protección. Podrá existir un SPIC para información clasificada nacional y otro para internacional, aunque, como se indicó en la norma NS/00, se intentará que la responsabilidad de ambas estructuras recaiga en las mismas unidades y personas.

Cuando en un ministerio, organismo o entidad se constituya un único servicio de protección de información clasificada que aglutine el servicio de protección de información clasificada nacional y el servicio de protección de información clasificada internacional, el jefe de seguridad recibirá la denominación de **director de seguridad del servicio de protección (DSSP)**.

Bajo dependencia orgánica o funcional del director o jefe de seguridad del servicio de protección se constituye una estructura completa de protección de la información clasificada, basada en lo que se denominan órganos de control, que se extienden hasta los últimos escalones del ministerio, organismo o entidad en que se maneja la información clasificada.

Los órganos de control son las unidades básicas, estructuradas jerárquicamente, que componen los SPIC y se ocupan del manejo, custodia y protección de la información clasificada. Según el origen de la información podrán ser órganos de control nacionales o internacionales. Cada órgano de control estará bajo el mando de un jefe de seguridad, que contará siempre con un suplente.

Por tanto, un SPIC es el conjunto jerárquico de todos los órganos de control (nacionales o internacionales, o ambos) existentes en un ministerio, organismo o entidad.

Los órganos de control son responsables de todos los aspectos relacionados con la seguridad de la información, es decir, tanto de su manejo y custodia (recepción, registro, almacenaje, distribución, etc.), como de la seguridad física, seguridad en el personal, seguridad en los sistemas de información y comunicaciones, etc.

El funcionamiento de estos órganos de control se basa en:

– Un personal con dedicación preferente a esta tarea, específicamente formado para sus funciones de seguridad, y con autoridad suficiente para cumplir con sus cometidos. El **jefe de seguridad del órgano de control**

es el máximo responsable del cumplimiento de las normas de seguridad y figura clave del sistema.
- Unos medios e instalaciones de seguridad específicamente adaptados y aprobados para la custodia, control y manejo de la información clasificada, constituidos como **zona de acceso restringido (ZAR)**.
- Una exacta ejecución de la normativa de seguridad por la que se rigen, especialmente la relativa a la protección, registro, custodia, manejo y distribución de la información clasificada.
- El cumplimiento de unos procedimientos operativos expresados en un **plan de protección** elaborado al efecto.

Según el tipo de información clasificada que manejan y el nivel jerárquico funcional en que se encuadran, los órganos de control adoptarán la denominación de:

ÓRGANOS DE CONTROL	
INFORMACIÓN CLASIFICADA NACIONAL	**INFORMACIÓN CLASIFICADA INTERNACIONAL**
Servicio central de protección de información clasificada **(SCPIC)**	Subregistro principal **(SP)**
Servicio general de protección de información clasificada **(SGPIC)**	Subregistro secundario **(SS)**
Servicio local de protección de información clasificada **(SLPIC)**	Punto de control **(PC)**
Cuenta de cifra	Cuenta de cifra

Como ya se ha indicado anteriormente, las funciones de un órgano de control internacional son compatibles con las de un órgano de control nacional, por lo que, siempre que sea posible, se intentará unificar ambas funciones dentro de la misma estructura y bajo el mismo responsable. Solo cuando no sea posible llevar a cabo dicha unificación, se mantendrán separados, bajo un mismo o distinto responsable.

En el ámbito de la **seguridad industrial**, las empresas contratistas que participen en actividades, contratos o proyectos clasificados deberán constituir un servicio de protección de información clasificada, que asumirá **todas las responsabilidades de protección de información clasificada**, según se regula en la norma NS/06 sobre «Seguridad Industrial» de la ANPIC.

2.5.2. Órganos de control nacionales

Son las unidades responsables de aplicar las medidas necesarias para lograr un adecuado manejo y protección de la información clasificada de origen nacional.

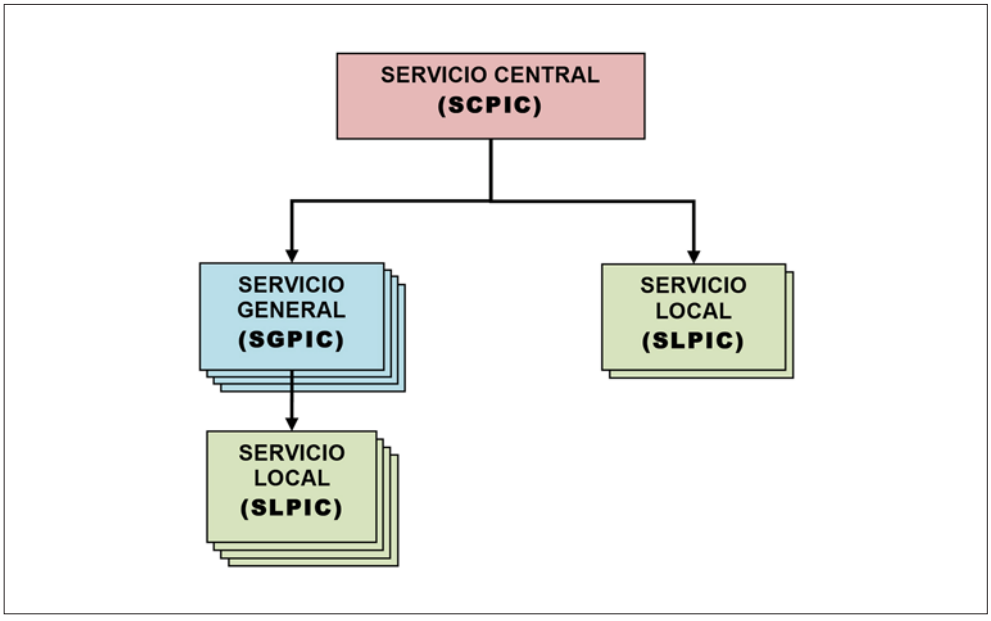
En función de su ubicación funcional dentro del organigrama de la organización podrán ser servicios **centrales, generales o locales** de protección. Además de los anteriores, tendrán consideración de órganos de control, a todos los efectos, las cuentas de cifra.

Todos los departamentos ministeriales y organismos públicos independientes, de la Administración, que precisen manejar información clasificada nacional, deberán contar, con un **servicio central de protección de información clasificada (SCPIC)**, que se constituye como órgano de trabajo del jefe de seguridad del SPIC nacional.

El jefe de seguridad del servicio de protección de información clasificada nacional podrá ejercer como jefe de seguridad del SCPIC, cuando así se estime conveniente. En otro caso se nombrará un jefe de seguridad específico. Igualmente se nombrará un suplente.

Cuando la complejidad orgánica y modo de trabajo de algún departamento ministerial, organismo o entidad así lo aconseje, se podrán constituir uno o varios **servicios generales (SGPIC) y locales (SLPIC)** de protección, subordinados funcionalmente al servicio central de protección.

A modo de ejemplo, podrán adoptar una estructura similar a la del siguiente gráfico, que podrá ampliarse en función de las necesidades del organismo:



Según se indicó en la norma NS/00, toda esta estructura nacional constituida en cada ministerio, organismo o entidad, depende orgánica y funcionalmente del Ministro o jefe responsable.

Registros superiores de información clasificada nacional

Todo servicio central de protección de información clasificada nacional deberá constituirse en registro superior de información clasificada nacional del ministerio u organismo al que pertenezca, y como tal tendrá las siguientes funciones:

a) Establecer un sistema de registro, control, archivo y distribución de la documentación clasificada que le permita, en todo momento, conocer la existencia y localización de toda la documentación de clasificación de grado RESERVADO o superior en su ministerio u organismo.
b) Distribuir y cursar la información clasificada que entre o salga del sistema de registro, a través suyo o con su concurso.
c) Realizar el registro, seguimiento y control exhaustivo de todos los documentos de grado SECRETO que se encuentren en el sistema de registro de su ministerio u organismo debiendo conocer su localización exacta en todo momento.
d) Efectuar el seguimiento de cualquier comprometimiento o infracción de seguridad detectados en la recepción, registro, archivo, distribución y remisión de la documentación clasificada de grado CONFIDENCIAL o superior, o con limitaciones especiales, ocurrido en un órgano de control subordinado.
e) Planificar y ejecutar la transmisión y el transporte de documentos clasificados que entren o salgan a través suyo.
f) Proponer las medidas que considere adecuadas para corregir posibles vulnerabilidades en materia de protección de la información.
g) Participar en las inspecciones ordinarias y extraordinarias a los órganos de control nacionales de él dependientes.

2.5.3. Órganos de control internacionales

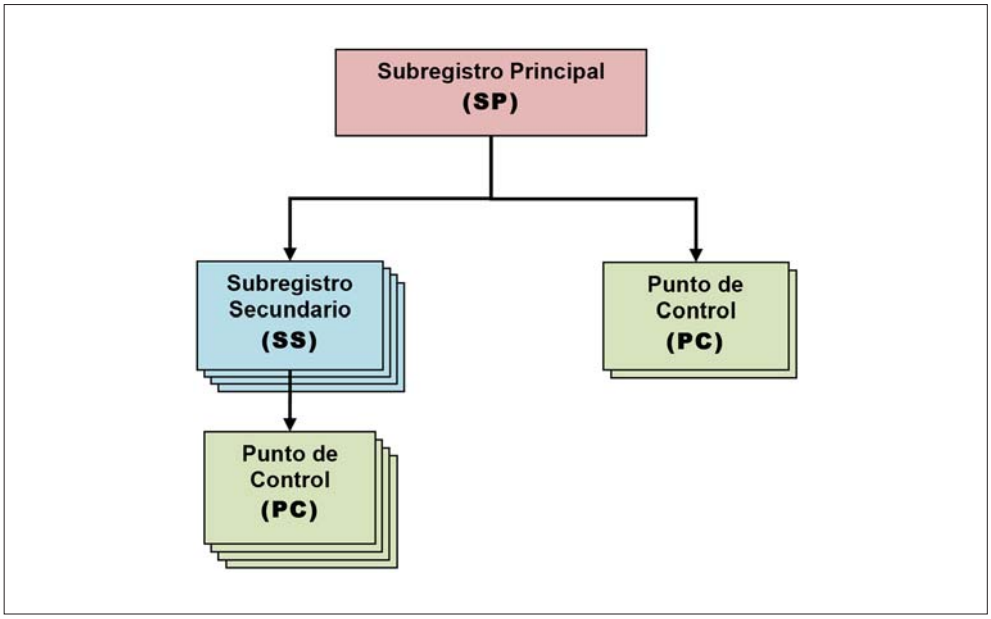
Son las unidades responsables de aplicar las medidas necesarias para lograr un adecuado manejo y protección de la información clasificada que proceda de organismos internacionales u otros estados. En función de su ubicación dentro del organigrama de la organización podrán ser subregistros principales, subregistros secundarios y puntos de control. Además de los anteriores, tendrán consideración de órganos de control, a todos los efectos, las cuentas de cifra.

Todos los departamentos ministeriales, organismos públicos independientes, el Cuartel General del EMAD, y los Cuarteles Generales de los Ejércitos, deberán constituir un subregistro principal, que se constituye como órgano de trabajo del jefe de seguridad del SPIC internacional.

El jefe de seguridad del servicio de protección de información clasificada internacional podrá ejercer como jefe de seguridad del subregistro principal, cuando así se estime conveniente. En otro caso se nombrará un jefe de seguridad específico. Igualmente se nombrará un suplente.

Cuando la complejidad orgánica y modo de trabajo de algún departamento ministerial u organismo así lo aconseje, se podrán constituir uno o varios subregistros secundarios y puntos de control, subordinados jerárquica y funcionalmente al subregistro principal.

A modo de ejemplo, podrán adoptar una estructura similar a la del siguiente gráfico, que podrá ampliarse en función de las necesidades del organismo:



Según se indicó en la norma NS/00, toda esta estructura internacional constituida en cada ministerio, organismo o entidad, depende orgánicamente del Ministro o jefe responsable, y funcionalmente de la ANPIC (a través de la ONS).

2.5.4. Estructura de los servicios de protección de información clasificada

Los órganos de control que componen un servicio de protección de información clasificada, atendiendo al nivel orgánico en que se encuentren enmarcados dentro de sus organismos, podrán ser:

A) Servicio central de protección de información clasificada / Subregistro principal

Es el órgano de control de nivel superior, que actúa como órgano de trabajo del jefe de seguridad del SPIC.

Aunque orgánicamente se pueden encuadrar en la estructura más conveniente, funcionalmente deben dar servicio al más alto nivel de cada departamento ministerial, Fuerzas Armadas, u otros organismos, o de sus órganos principales subordinados (Subsecretarías, Secretarías de Estado, Ejércitos, etc.), según aconseje la estructura orgánica y de funcionamiento de cada organismo o entidad en que se decida su constitución.

Será responsable de:

a) Ejecutar los cometidos que marca la normativa de seguridad y las decisiones del jefe de seguridad del SPIC.
b) Dirigir, controlar y supervisar la actuación de los órganos de control subordinados.
c) Inspeccionar el cumplimiento de la normativa relativa a la protección de la información clasificada.
d) Inspeccionar los órganos de control subordinados e indicar las medidas de seguridad preventivas y correctivas que deban ser adoptadas.
e) Establecer un sistema de recepción, registro, control, archivo, distribución y remisión de la información clasificada manejada en su organismo, que permita, en todo momento, conocer dónde se encuentra la documentación de grado «CONFIDENCIAL o equivalente» o superior.
f) Gestionar las aperturas, cierres o modificaciones de los órganos de control, cuentas de cifra y zonas de acceso restringido y las autorizaciones de sistemas de información y comunicaciones correspondientes al organismo o entidad al que sirven.
g) Centralizar la tramitación de los expedientes de solicitud de habilitación personal de seguridad correspondientes a sus organismos dependientes, y apoyar en las investigaciones cuando así les sea requerido por la ONS.
h) Centralizar la tramitación de los expedientes de acreditación de los sistemas CIS que vayan a manejar información clasificada dentro de su ámbito de actuación.

i) Tramitar las solicitudes de visitas clasificadas («Request for Visit» -RFV- en terminología internacional) y comunicaciones de asistencia a reuniones internacionales clasificadas, así como los planes de transporte de material clasificado de sus organismos dependientes, cuando no sea responsabilidad de un órgano específico.

B) Subregistro principal exterior

Son los órganos de control situados en las representaciones nacionales ante organizaciones internacionales, encargados de la recepción y entrega de la información clasificada procedente o dirigida a dichas organizaciones.

Su función es fundamental porque constituyen el punto de intercambio documental «in situ» entre España y la organización internacional ante quien ejercen su representación. Asimismo, son responsables de velar por el cumplimiento de la normativa de seguridad de la ANPIC por todo el personal de sus delegaciones y de dar soporte al resto de personal que, en representación de España, asiste o participa en actividades de dichas organizaciones internacionales.

Especialmente crítico es el apoyo al flujo documental de la información clasificada que los delegados reciben por su participación en los diferentes comités y grupos de trabajo, a los que, cuando así se requiera, deben facilitar su recogida y transmisión por canales seguros, evitándose que los delegados viajen de forma irregular con información clasificada.

Se relacionan directamente con la ONS en aquellas materias de su competencia.

C) Servicios generales de protección / Subregistros secundarios

Son los órganos de control con dependencia funcional directa de un servicio central de protección de IC / subregistro principal, de los que a su vez pueden depender otros órganos de control subordinados funcionalmente. Están encargados de asegurar la difusión, control y protección de la información clasificada a sus órganos de control subordinados, y a aquellos organismos a los que sirven.

D) Servicios locales de protección / Puntos de control

Constituyen las unidades elementales del sistema de protección. Dependen de un servicio central o general de protección o de un subregistro, principal o secundario, a través del cual realizan normalmente todas las operaciones de recepción y envío de documentación clasificada, estando encargados de asegurar la difusión,

control y protección de la información clasificada en aquellos organismos a los que sirven.

En caso de necesitarlo se podrán constituir puntos de control secundarios, dependientes jerárquicamente de puntos de control, con los mismos requisitos y funcionalidades.

E) Cuentas de cifra

Cuando un organismo tenga necesidad de manejar material de cifra (equipos criptográficos, claves, etc.), se constituirá una **cuenta de cifra** al efecto, que tendrá también la consideración de órgano de control, y deberá cumplir con todos los requisitos de seguridad y procedimientos señalados para éstos.

2.5.5. Dependencia, apertura y cierre de servicios de protección y órganos de control

Los servicios de protección de información clasificada nacional, así como sus órganos de control subordinados, dependen orgánica y funcionalmente del ministerio, organismo o entidad que los ha constituido, por lo que los nombramientos de los jefes y suplentes y las aperturas y cierres de cada órgano, quedan bajo su responsabilidad.

Los servicios de protección de información clasificada internacional, así como sus órganos de control subordinados, dependen orgánicamente del respectivo ministerio, organismo o entidad que los ha constituido, y funcionalmente, a través de los órganos de control superiores y del jefe del servicio de protección de información clasificada internacional, de la ANPIC. Por ello, los nombramientos de los jefes y suplentes y las aperturas y cierres de cada órgano, serán siempre a propuesta del correspondiente ministerio, organismo o entidad, pero habrán de ser aprobados por la ANPIC o la ONS, según se especifica posteriormente.

Necesidades de seguridad, temporales, de ubicación física, de dotación de personal, de carácter técnico o circunstanciales, pueden aconsejar que un determinado órgano de control, dentro de una determinada estructura orgánica, dependa funcionalmente de un servicio de protección de otro organismo o entidad, o que se haga responsable de personas u organismos ajenos a la estructura orgánica del organismo o entidad al que sirve.

En su ámbito de responsabilidad, la ANPIC decidirá, en cada caso y a propuesta de los interesados, la dependencia funcional más adecuada.

Corresponde a la **ANPIC autorizar la apertura de todos** los subregistros principales y órganos de control de ellos dependientes que componen el servicio de protección de información clasificada de un organismo o entidad.

Para la constitución inicial (si no existiera previamente) de un servicio de protección de información clasificada internacional en un organismo o entidad, el **jefe orgánico o responsable,** de dicho organismo o entidad **remitirá a la ANPIC** la propuesta de nombramiento de un jefe de seguridad del servicio de protección y la propuesta de apertura de un subregistro principal. El expediente completo incluirá lo siguiente:

a) Identificación de la autoridad superior del organismo o entidad, con la que haya de relacionarse la ANPIC.
b) Dependencia y encuadramiento orgánico del subregistro principal dentro del organismo o entidad.
c) Organismo, organismos o entidades a los que servirá.
d) Plan de protección del local elegido como zona de acceso restringido (configurado como área clase I o II) para la instalación del subregistro principal, compuesto por:

- Informe de Instalaciones. Su objeto es describir los sucesivos entornos de seguridad existentes, las características físicas y las medidas técnicas adoptadas, que permiten alcanzar un grado de protección suficiente. No debe incluir, en ningún caso, procedimientos, normas o medidas organizativas, que son objeto de los otros documentos.
- Procedimientos 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 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 afectarla.

e) Propuesta de nombramiento de jefe de seguridad del servicio de protección y del jefe de seguridad del subregistro principal (podrán ser la misma persona).

Para la apertura de los subregistros secundarios, puntos de control y cuentas de cifra dependientes del subregistro principal, se remitirá a la ONS un informe

análogo, a través del jefe de seguridad del servicio de protección, que propone su apertura.

Las propuestas de modificaciones en los órganos de control que afecten al plan de protección, se comunicarán puntualmente a la ONS, quien será responsable de su aprobación.

El **cierre de un órgano de control**, de los indicados anteriormente, deberá ser **aprobado por la ANPIC**. Para proceder al cierre de un órgano de control, el jefe de seguridad del servicio de protección remitirá propuesta de cierre a la ONS, quien establecerá, en su caso, los procedimientos adecuados.

Antes de producirse el cierre de un órgano de control, toda la información clasificada que tuviera bajo su custodia, así como los libros de registro, actas de destrucción y resto de documentación relevante, deberán ser formalmente entregados al órgano superior del que dependía funcionalmente.

El cambio de ubicación de subregistros principales y órganos de control de ellos dependientes, a nuevas instalaciones no precisa que se solicite su cierre y nueva apertura, salvo que vaya a dar servicio a un organismo o entidad distinto al que solicitó su constitución inicialmente, o pase a depender funcionalmente de un órgano de control superior distinto.

El cambio de ubicación del órgano de control precisa de la aprobación previa por la ONS, por lo que se remitirá solicitud al efecto.

No se hará el cambio en tanto no se hayan acreditado las nuevas instalaciones, con un nuevo plan de protección.

Cuando un subregistro principal o un órgano de control dependiente, aunque no cambie de ubicación, vaya a dar servicio a un organismo o entidad distinto al que solicitó su constitución inicialmente, o pase a depender funcionalmente de un órgano de control superior distinto, se deberá proceder a su cierre y posterior apertura, con las formalidades y requisitos indicados en las presentes normas.

Se tendrá especial cuidado en el control y registro de la información clasificada, al producirse un cambio de responsabilidades que va a afectar no sólo a dicho órgano de control y al organismo o entidad al que sirve, sino también a los órganos de control superiores de los que dependa funcionalmente en cada momento y al nuevo organismo o entidad al que dará servicio.

2.5.6. Instalaciones separadas constituidas como zonas de acceso restringido (ZAR) dependientes

Las instalaciones o locales en que se maneje información clasificada de grado «CONFIDENCIAL o equivalente» o superior, o que alberguen en sus instalaciones sistemas de información y comunicaciones que manejen información clasificada de dicho grado, deberán cumplir unos requisitos específicos, tanto de seguridad como de apertura, modificación, cierre y control.

En todos los casos dependerán, a efectos de protección de la información clasificada, de un órgano de control y estarán constituidos como zonas de acceso restringido (ZAR).

Las especificaciones sobre los requisitos que deben tener estas instalaciones se especifican en la NS/03.

2.6. Autoridad de Seguridad Designada (ASD) y área de seguridad de la información clasificada en el ámbito industrial

Cuando en un ministerio se desarrollen actividades, contratos o programas clasificados, que impliquen la participación de empresas privadas o públicas, se deberá establecer un área de seguridad de la información clasificada en el ámbito industrial, que dependerá funcionalmente de la ASD, en el caso de que haya sido nombrada.

Esta autoridad será responsable de que en el propio ministerio y en las empresas, se adopten las medidas necesarias para asegurar la protección de la información clasificada que se maneje e intercambie al amparo de dichas actividades, contratos o programas clasificados.

Dichas medidas deberán ser acordes a lo estipulado en las normas de la ANPIC, y especialmente las específicas de seguridad industrial definidas en la norma NS/06, en la que se definen los cometidos, estructuras y procedimientos específicos aplicables al ámbito de la seguridad industrial.

3. ESTRUCTURA DE SEGURIDAD EN LOS SISTEMAS DE INFORMACIÓN Y COMUNICACIONES

Se deberá establecer, obligatoriamente, una **estructura de seguridad de las tecnologías de información y telecomunicaciones (STIC) de la organización** en cada ministerio, organismo o entidad del más alto nivel de la Administra-

ción (departamentos ministeriales, Fuerzas Armadas, etc.), dado que, cada vez en mayor volumen, la información se almacena, distribuye y custodia en sistemas de información y comunicaciones (CIS),.

Esta estructura será responsable de que se adopten las medidas STIC necesarias para garantizar la protección de la información clasificada que se maneje e intercambie en CIS, debiendo cumplir en todo momento lo estipulado en las normas de la ANPIC, especialmente en la norma NS/05. Estará dotada del personal, formación y recursos necesarios, y actuará siempre en coordinación y bajo la supervisión de la estructura de protección de la información clasificada de la organización.

Las funciones asignadas a esta estructura STIC serán las de dirección, control, ejecución, inspección y seguimiento de todos los procesos de acreditación de sistemas que se realicen en la organización a la que sirve, asegurando que los sistemas que se presentan para su acreditación cumplen con todos los requisitos marcados por la Autoridad de Acreditación de Seguridad (AAS) y la normativa aplicable.

En la norma NS/05, se definen los cometidos, estructuras y procedimientos específicos y aplicables al ámbito de la seguridad en los sistemas de información y comunicaciones.

En aquellas organizaciones en las que se maneje material de cifra, se establecerá una estructura responsable del control de material de cifra, con cometidos específicos en el control, custodia y uso de los equipos y documentación de cifra, y del material de claves. Sus funciones y cometidos se rigen por normativa específica, complementaria a estas normas, desarrollada por las autoridades de cifra.

4. JEFE DE SEGURIDAD DEL ÓRGANO DE CONTROL

4.1. Dependencia, nombramiento y cese

Lo indicado en este **apartado 4.1** aplica especialmente a los servicios de protección de información clasificada que tengan una dependencia funcional de la ANPIC, es decir, aquellos del ámbito de la información clasificada internacional, aunque no se excluye al resto de que puedan aplicarlo de forma análoga.

El jefe de seguridad de un órgano de control es la persona que, propuesta por el jefe o responsable del organismo o entidad al que da servicio dicho órgano, y una vez aprobado su nombramiento, responde de la correcta aplicación de las normas para la protección de la información clasificada en el organismo o entidad.

El jefe de seguridad deberá contar con un **suplente**, que asuma sus funciones en ausencia del primero. Es responsabilidad del jefe de seguridad titular la formación en sus labores específicas de seguridad del suplente.

En todo servicio de protección de información clasificada existirá la figura del **jefe de seguridad del servicio de protección (JSSP)**, que será el responsable principal, del cumplimiento de todos los cometidos, ante el jefe o responsable del organismo o entidad al que presta servicio, y que dependerá funcionalmente de la ANPIC en el ámbito de las competencias de esta última, a través de su relación directa con la ONS.

El **jefe o responsable** del organismo o entidad que tiene constituido un servicio de protección de información clasificada con dependencia funcional de la ANPIC, **remitirá a dicha ANPIC** la propuesta de nombramiento de jefe de seguridad del servicio de protección, para su aprobación por ésta, cada vez que se produzca un cambio del titular. Previamente a su aceptación por la ANPIC será instruido en los cometidos específicos de su cargo por el personal de la ONS. La ANPIC podrá denegar la propuesta mediante escrito motivado dirigido a la autoridad que lo propuso.

Cuando el jefe de seguridad del servicio de protección vaya a ejercer también como jefe de seguridad de subregistro principal, se hará constar en la propuesta de nombramiento dirigida a la ANPIC.

El cese como jefe de seguridad o suplente del servicio de protección o de un órgano de control, no precisa de aprobación por parte de la ANPIC o de la ONS, sino que se producirá por decisión adoptada al efecto dentro de su canal jerárquico superior, o con ocasión del nombramiento de un nuevo titular. En cualquier caso, se comunicará a la ONS de forma inmediata.

En los subregistros principales, por la especial responsabilidad del puesto, el suplente estará integrado **obligatoriamente** dentro de la estructura del órgano de control.

Cuando el puesto como jefe de seguridad del subregistro principal coincida, a su vez, con el de jefe de seguridad del servicio de protección, su suplente ejercerá también la suplencia en ambos puestos.

El jefe de seguridad del servicio de protección de información clasificada **remitirá a la ONS** las propuestas de jefes de seguridad del subregistro principal (salvo cuando sea él mismo), subregistros secundarios y puntos de control dependientes, así como de los suplentes, para su aprobación por dicha Oficina. Respecto a

las cuentas de cifra sólo se remitirá la propuesta de jefe y suplente para la apertura inicial, no siendo preciso para los sucesivos relevos en tanto no se cierre el órgano.

La ONS, en nombre de la ANPIC, podrá denegar la propuesta mediante escrito motivado dirigido al proponente.

Los jefes de seguridad titulares de órganos de control, hasta punto de control incluido, realizarán **un curso de formación específico**, para adquirir los conocimientos que les ayuden a ejercer sus funciones como tales. La forma y contenidos de estos cursos serán establecidos por la ONS, con el apoyo de los subregistros principales para su impartición.

4.2. Empleos o niveles requeridos

Para que las normas de seguridad sean eficaces es necesario que los jefes de seguridad tengan una dependencia en línea jerárquica directa del jefe o responsable del organismo o entidad al que den servicio, cuenten con su respaldo activo y tengan acceso personal y directo al resto de la dirección, con objeto de facilitar el cumplimiento de su misión.

El nivel personal o empleo del propuesto para cada una de las figuras que componen el organigrama de mando de la estructura de protección de la información clasificada, debe ser acorde a las responsabilidades que asume, de forma que les permita ejecutarla con la autoridad y representatividad necesarias.

En el siguiente cuadro se marcan los empleos o niveles mínimos exigibles para el ejercicio de las funciones asignadas en función del tipo de órgano de control:

SERVICIO u ÓRGANO	JEFE DE SEGURIDAD	SUPLENTE
Director o Jefe del SPIC	A1-30 o 29 / General o Coronel	N/P
SP o SCPIC	A1-29 o 28 / Coronel o Tcol	Comandante / A1-27 o 26
SS o SGPIC	A1-28 o 27 / Tcol o Cte	Capitán / A1-26
PC o SLPIC	A1-27 o 26 / Cte o Cap	Oficial / A1 o A2-24
Cuenta de cifra	A1 o A2 / Oficial o Suboficial	N/P

Cuando la entidad del organismo al que sirven es pequeña, y no permite o no aconseja adoptar estos niveles o empleos, se justificará adecuadamente en el momento de solicitar la aprobación del nombramiento del jefe de seguridad o suplente.

4.3. Relevo de responsabilidades

Cuando se produzca un relevo o cese de jefe de seguridad en un servicio de protección de IC se deberá elaborar un acta de relevo, que será firmada por el saliente y el entrante, con el visto bueno del jefe o responsable del organismo o entidad al que sirve, o de un superior jerárquico dependiente de dicho jefe. Esta acta hará mención como mínimo a la conformidad en la entrega, recuento y control de:

- Estructura de protección dependiente (órganos de control subordinados).
- Hojas de registro de firma de los órganos de control superior y subordinados.
- Información clasificada controlada a cargo.
- Llaves y combinaciones de seguridad.
- Libros de registro.
- Listado de sistemas de información y comunicaciones acreditados bajo control.
- Listados de personal autorizado en el servicio de protección.
- Documentación de seguridad (plan de protección, procedimientos operativos de seguridad de los sistemas de información y comunicaciones, certificados de locales, manuales técnicos y de mantenimiento de los sistemas de seguridad).
- Registro de habilitaciones personales de seguridad (HPS) del personal a cargo.
- Expedientes de solicitud de HPS.
- Listado de control COSMIC/TOP SECRET/SECRETO (si es aplicable).
- Programa de inspecciones a órganos de control subordinados.
- Cualquier otro detalle que se considere necesario.

4.4. Criterios de actuación

La normativa de seguridad para proteger la información clasificada deberá desarrollarse y complementarse con **normas internas de obligado cumplimiento** dentro de cada organismo o entidad. Su ejecución exige el concurso de personal especializado dedicado a la seguridad de manera preferente.

El jefe de seguridad del servicio de protección centralizará la ejecución de todos los aspectos de protección de la información clasificada, manteniendo un enlace frecuente con los órganos de control que de él dependen, y también con la ONS.

El jefe de seguridad de cualquier órgano de control mantendrá un **enlace frecuente** con los jefes de seguridad de los órganos de control subordinados. Asimismo, mantendrá este enlace con el jefe de seguridad del órgano de control del que dependa.

La ONS y los jefes de seguridad de los servicios de protección de información clasificada funcionalmente dependientes mantendrán **reuniones periódicas** con la finalidad de aclarar dudas, actualizar y modificar las normas y los procedimientos, y resolver los problemas que pudiera plantear la aplicación de las normas. La iniciativa para plantear estas reuniones podrá partir de la propia ONS o a petición de alguno de los servicios de protección.

4.5. Misiones del jefe de seguridad

Los jefes de seguridad de servicio de protección u órgano de control tienen, con carácter general, las siguientes **misiones**:

a) Velar por la correcta protección de la información clasificada en su ámbito de responsabilidad.
b) Controlar la aplicación de todos los aspectos de la normativa de seguridad, en lo que concierne a la protección de la información clasificada.
c) Proponer y aplicar las medidas específicas de seguridad propias dentro de su organismo o entidad, relacionadas con la información clasificada.
d) Estimular, mediante los correspondientes programas de formación, de divulgación y de reciclaje, la sensibilidad en materia de seguridad del personal relacionado con la información clasificada.

De estas misiones se derivan una serie de cometidos concretos, y son los siguientes:

Cometidos generales:

– Redactar unas normas de seguridad, basadas en las difundidas por la ANPIC, que se adapten a las circunstancias particulares de su organismo o entidad.
– Difundir las normas de seguridad y supervisar su cumplimiento.
– Asesorar a sus superiores en todo aquello relativo a la protección de la información clasificada.

- Informar, por los canales reglamentarios, a la ONS, con la debida reserva y discreción, sobre las infracciones y vulnerabilidades que se detecten.
- Tener previstos los canales de relación dentro del organismo o entidad con la ONS u órgano de control superior, que permitan dar parte inmediato de las infracciones que puedan comprometer la seguridad de la información clasificada.
- Elaborar y mantener actualizado el plan de protección.
- Impulsar, inspeccionar y certificar la correcta elaboración e implantación de los planes de protección de las zonas de acceso restringido (configuradas como áreas clase I o II) de él dependientes.
- Organizar la seguridad de reuniones en las que se vaya a manejar información clasificada de grado superior o igual a «CONFIDENCIAL o equivalente».
- Preparar y ejecutar los programas de inspecciones a órganos subordinados.

Cometidos relativos a la seguridad en el personal

- Prever, gestionar y tramitar con la debida antelación las solicitudes de concesión y renovación de las HPS, y asesorar al jefe o responsable del organismo o entidad sobre la idoneidad de la persona a habilitar, a efectos de seguridad.
- Cumplimentar los apartados de su responsabilidad en los formularios de solicitud de HPS que le corresponda tramitar.
- Supervisar que los expedientes de solicitud de HPS se cursan correctos y completos.
- Instruir al personal de su organismo o entidad en el conocimiento de la normativa de seguridad, especialmente sus obligaciones en cuanto a la protección de la información clasificada, antes de producirse el primer acceso, y efectuar reciclajes de formación periódicos, como mínimo con carácter anual.
- Instruir al personal en el cumplimiento de los requisitos y obligaciones relativas a actividades en las que vaya a participar, donde se maneje información clasificada (visitas, reuniones, etc.).
- Proponer y elevar para su aprobación, los nombramientos de los jefes de seguridad y suplentes de los órganos de control dependientes.
- Mantener actualizado el registro de HPS y, en el caso de los subregistros principales, tener la custodia de ellas y ocuparse de remitirlas, en caso de ser necesario, a los nuevos organismos o entidades de los que pasen a depender los titulares de las habilitaciones, con conocimiento de la ONS.
- Promover la comunicación, por parte de los jefes de seguridad de los órganos de control subordinados, de aquellos aspectos en los interesados que pudieran constituir un riesgo para la seguridad de la información clasificada.

– Informar oportunamente al jefe o responsable del organismo o entidad, al escalón superior del servicio de protección y a la ONS, en su caso, de cualquier circunstancia en el personal que pudiera constituir un riesgo para la seguridad de la información clasificada.

Cometidos relativos a la seguridad de la información

– Establecer los planes de difusión, de transporte y de destrucción de información clasificada, especialmente en casos de emergencia.
– Asesorar al jefe de su organismo o entidad sobre la asignación, o propuesta de asignación, de grados de clasificación a la información clasificada que se origine.
– Mantener actualizado el registro de información clasificada.
– Inspeccionar periódicamente los registros y archivos de información clasificada, así como los procedimientos de contabilidad, registro, archivo y protección.
– Efectuar el seguimiento y tener acceso a los documentos clasificados objeto de uso y consulta por parte de los usuarios, para verificar el cumplimiento de las medidas de seguridad.
– Autorizar, registrar, numerar y controlar las copias, traducciones y extractos de los documentos clasificados, hasta el grado máximo que tenga autorizado.
– Autorizar y certificar la destrucción de los documentos clasificados previamente decidida por los principales usuarios, hasta el grado máximo que tenga autorizado.
– Inspeccionar periódicamente las operaciones y los métodos de destrucción.
– Comprobar que el transporte de la documentación y material clasificado se lleva a cabo con las debidas garantías de seguridad.
– Informar al Registro Central y órgano de control superior, según corresponda, de las altas y bajas de información clasificada que se produzcan, conforme a los criterios marcados por la ANPIC.

Cometidos relativos a la seguridad física

– Establecer los sistemas de control de acceso del personal a las zonas de acceso restringido (ZAR), que son locales o zonas específicas de seguridad en los que, con autorización expresa, se custodia o maneja habitualmente información clasificada.
– Comprobar y aprobar, si procede, las condiciones de seguridad de los despachos y cajas fuertes de aquellos usuarios que, por su función y con carácter excepcional y temporal, necesiten disponer de documentación clasificada y se les ha autorizado expresamente a ello.

- Comprobar las condiciones de seguridad físicas de las instalaciones (incluyendo cuentas de cifra y locales que alberguen sistemas de información y comunicaciones que manejen información clasificada, que serán, todas ellas, zonas de acceso restringido), muebles de seguridad, cajas fuertes, sistemas informáticos, etc., en los que se custodie o archive información clasificada.
- Inspeccionar con la debida antelación las salas y despachos en los que, de forma habitual o esporádica, se celebren reuniones de trabajo en las que se maneje información clasificada y adoptar las medidas necesarias para garantizar el grado de protección adecuado.
- Realizar controles aleatorios esporádicos para detectar posibles fallos en los sistemas de seguridad establecidos y evitar así futuras vulnerabilidades.

Cometidos relativos a la seguridad en los sistemas de información y comunicaciones

- Verificar que los sistemas de información y comunicaciones en que se almacena, procesa o transmite información clasificada estén correctamente acreditados y ubicados en zonas de acceso restringido (ZAR) aprobadas, en los casos que sea preceptivo.
- Establecer la obligada dependencia funcional, relativa a protección de la información clasificada, del responsable de seguridad de la ZAR respecto a un servicio de protección, especialmente para asegurar el correcto archivo, difusión y registro de la documentación clasificada.
- Inspeccionar periódicamente la correcta implantación y adecuación de las medidas de seguridad en el personal, física y de la información en las ZAR donde se ubiquen sistemas.
- Supervisar los procedimientos de contabilidad, registro, archivo y protección de información clasificada, en especial las copias de seguridad («back-up»), que se custodian en la propia ZAR del sistema.

5. CONTROL E INSPECCIONES

Corresponde a la ANPIC, como autoridad responsable de velar por el cumplimiento de la normativa de protección de la información clasificada, el control y la supervisión de la estructura de protección de la información clasificada. La ONS establecerá un plan de inspecciones anual, a los servicios de protección de información clasificada, de tal forma que, en dos años, se hayan inspeccionado la totalidad de los existentes.

El Registro Central, en su ámbito de competencia, y con independencia de los inventarios y comprobaciones que tenga previsto realizar, deberá hacer un inven-

tario anual de la documentación de grado «equivalente a SECRETO», que remitirá a las oficinas de seguridad de las organizaciones internacionales que corresponda. A fin de cotejar dicha información, todos los subregistros principales remitirán al Registro Central relación de todos los documentos de grado «equivalente a SECRETO» a su cargo antes del 31 de enero de cada año. Caso de no tener a su cargo ningún documento de dicho grado, también deberán comunicar dicha situación.

Los JSSP efectuarán una inspección completa sobre todos los órganos de control a su cargo que custodien información de grado «CONFIDENCIAL o equivalente» o superior, al menos una vez cada **veinticuatro (24) meses**. Esta función podrá ser delegada en los JSSP de los órganos de control de inferior nivel de ellos dependientes.

Se informará por escrito a la ONS de cualquier comprometimiento de la información clasificada o incidencia relevante que se detecte durante dichas inspecciones, con independencia de cumplir con cuanto se establece al efecto de los comprometimientos en el **apartado 11** de la norma NS/04.

Los JSSP de los servicios centrales de protección / subregistros principales, remitirán a la ONS:

1) Antes del día 1 de octubre de cada año:

   – Los programas anuales de las inspecciones que tengan planificado hacer a sus órganos de control subordinados durante el siguiente año.
   – La relación actualizada de firmas autorizadas del subregistro principal.

2) Con un mes de antelación a recibir la inspección bienal de la ONS:

   – La relación detallada y actualizada de los órganos de control subordinados, hasta punto de control incluido, con indicación de jefe de seguridad y suplente de cada uno, ZAR donde se ubican y sistemas de información y comunicaciones acreditados instalados en sus locales.
   – Registro informático actualizado de la información imputable, de grado «equivalente a RESERVADO», custodiada o a cargo en toda su estructura de protección dependiente, de la que es responsable.

NORMA NS/02

SEGURIDAD EN EL PERSONAL. HABILITACIÓN DE SEGURIDAD DEL PERSONAL

1. INTRODUCCIÓN

La protección de la información clasificada y su seguridad recaen, en último extremo, en las personas que la manejan, gestionan, transportan, o simplemente acceden a ella de forma accidental.

La seguridad en el personal es la condición que se alcanza cuando se aplican un conjunto de medidas eficaces y procedimientos establecidos, para reducir a un grado mínimo aceptable el riesgo de comprometimiento de la información clasificada por causa debida exclusivamente al personal que accede a ella, ya sea de forma voluntaria, involuntaria, autorizada o sin autorización.

La normativa de seguridad en el personal regula el procedimiento de habilitación de las personas, establece las directrices a las que éstas se deberán someter para manejar información clasificada, así como los criterios de autorización de acceso.

Los responsables de la custodia y correcto manejo de la información clasificada velaran porque todas las personas de su respectivo organismo o entidad, que necesiten acceder a información clasificada, asuman y cumplan sus obligaciones al respecto.

2. CONCEPTOS PREVIOS

2.1. Habilitación personal de seguridad

La habilitación personal de seguridad (HPS) es la resolución positiva de la ANPIC por la que, en nombre del Gobierno del Reino de España, reconoce formalmente

la capacidad e idoneidad de una persona para tener acceso a información clasificada en el ámbito y grado autorizado, al haber superado el proceso de investigación de seguridad y haber sido concienciado en el compromiso de reserva que adquiere y en las responsabilidades que se derivan de su incumplimiento, resolución que se materializa en un documento firmado por la ANPIC.

La concesión de la HPS se realiza en virtud de la ausencia de riesgos no asumibles o de vulnerabilidades manifiestas en el momento de la investigación. La HPS conllevará un grado de confianza sobre la lealtad, veracidad y fiabilidad de las personas a las que se conceda.

La HPS no es un derecho del interesado, sino un reconocimiento de las condiciones de seguridad presentes en una persona y su entorno. Supone, por tanto, la expresión explícita de la confianza del Estado en dicho individuo para su acceso a información clasificada.

Deberán disponer de HPS todas aquellas personas que manejen información clasificada de grado «CONFIDENCIAL o equivalente» o superior, los encargados de su custodia y traslado y, en general, cualquiera que pudiera contar con la posibilidad razonable de tener acceso a ella.

2.2. Necesidad de conocer

La «necesidad de conocer» es la determinación de que una persona requiere el acceso a información para desempeñar servicios, tareas o cometidos oficiales. Ninguna persona podrá tener acceso a información clasificada exclusivamente por razón de su cargo o posición, o por estar en posesión de una HPS, sin la preceptiva necesidad de conocer.

Por consiguiente, ocupar un cargo o disponer de una HPS no justifica, en sí mismo, el acceso a información clasificada.

2.3. Concienciación de seguridad

La concienciación de seguridad implica el conocimiento, por todo usuario de información clasificada, de las obligaciones y conceptos básicos, del deber de reserva que se adquiere y de las responsabilidades penales y disciplinarias que les son de aplicación en caso de incumplimiento.

Dicho «deber de reserva» se conserva para siempre, con independencia de que el interesado haya finalizado su necesidad de acceso a información clasificada.

La concienciación de seguridad se encuadra dentro del proceso de solicitud de la HPS y es **requisito previo para la concesión**.

2.4. Instrucción de seguridad

La instrucción de seguridad proporciona el conocimiento detallado que precisa todo usuario de información clasificada para su correcto manejo. Es obligatoria y complementaria a la concienciación de seguridad, definida anteriormente. Deberá impartirse antes de que se produzca el primer acceso a la información clasificada y repetirse de forma periódica.

3. CONDICIONES PARA EL ACCESO A LA INFORMACIÓN CLASIFICADA

3.1. Requisitos de acceso

Una persona sólo podrá ser autorizada a acceder a la información clasificada de grado «CONFIDENCIAL o equivalente» o superior, cuando se cumplan conjuntamente los siguientes requisitos:

- Le ha sido concedida una habilitación personal de seguridad adecuada.
- Se ha verificado su «necesidad de conocer».
- Ha recibido la instrucción de seguridad preceptiva.

Para el acceso a información clasificada con grado de clasificación de «DIFUSIÓN LÍMITADA o equivalente» no es necesario que se disponga de HPS, aunque sí se deberán cumplir los requisitos de la necesidad de conocer y de haber recibido la instrucción sobre las responsabilidades de seguridad.

3.2. Acceso en el ámbito de la seguridad industrial

El ámbito de la **seguridad industrial** hace referencia al personal que trabaja para empresas con habilitación de seguridad de empresa (HSEM) y que deba trabajar con información clasificada.

Dada su sensibilidad y especiales características, en este ámbito se emplearán criterios más restrictivos de autorización de acceso. Aparte de la posesión de HPS, de la necesidad de conocer y de la instrucción preceptiva de seguridad, se requerirá, además, disponer de:

- **El certificado de habilitación personal de seguridad** asociado a la empresa con HSEM para la que trabaja, emitido por el **área de seguridad de**

la información clasificada en el ámbito industrial, o por la Autoridad de Seguridad Designada (ASD) en su caso, o, en su defecto, por la ONS. Este certificado podrá tener el mismo formato que el definido en el **apartado 5.4.8.2.** para el caso general, o ser uno colectivo para varios interesados. En cualquier caso, ha de incluir una indicación expresa de la empresa para la que se emite y, cuando se estime necesario, de los contratos, programas o actividades clasificados a los que está autorizado el titular, o titulares, detalles que se incluirán en el apartado relativo a **«objeto del certificado»** del modelo propuesto en el apartado citado.

– **La autorización de acceso,** documento por el que el órgano de contratación, oficina de programa, o el organismo o ente responsable de una actividad clasificada, autoriza el acceso a personal de una empresa, en posesión de una HPS, a la información clasificada especificada.

3.3. Responsabilidades

La responsabilidad de justificar la necesidad de acceso a información clasificada y de solicitar la correspondiente HPS, recae en el organismo o entidad en el que va a trabajar esa persona. Para ello contará con personal responsable en materia de protección de la información clasificada, principalmente el jefe de seguridad del órgano de control establecido al efecto.

La responsabilidad de tramitar a la ANPIC española, una solicitud de HPS para un ciudadano español que trabaje en el ámbito de alguna organización internacional, será asumida por las oficinas de seguridad de estas.

Asimismo, la responsabilidad de la tramitación de una solicitud de HPS o de información de seguridad, relativa a un ciudadano español que trabaje para un país con acuerdo para la protección de información clasificada firmado con España, podrá ser asumida por las autoridades nacionales de seguridad de dichos países, haciendo uso de los formularios de solicitud españoles.

4. TIPO, GRADO Y ESPECIALIDAD DE LA HPS

4.1. Generalidades

Dentro del concepto de HPS, se entenderá por:

– **GRADO**: la máxima clasificación de la información clasificada a la que se le habilita el acceso, si es necesario. Por ejemplo RESERVADO.

- **TIPO**: es el ámbito de origen al que pertenece la información, es decir, la organización o nación propietaria de la información clasificada a la que puede tener acceso, si es necesario. Por ejemplo: OTAN, UE, NACIONAL.
- **ESPECIALIDAD**: Determinadas informaciones pertenecen a ámbitos más concretos que exigen una especial preparación del futuro usuario y un control más exhaustivo. Son ejemplo de especialidad: ATOMAL, CRYPTO o BOHEMIA.

4.2. Clasificación de tipo y grado

4.2.1. Información nacional o derivada de acuerdos para la protección de información clasificada

El grado de la HPS determina la máxima clasificación de la información a la que el titular tendrá acceso. Por tanto, se solicitarán los grados de HPS de acuerdo con los grados de información clasificada a la que se requiere acceder.

La denominación de los grados de HPS, de mayor a menor, son los siguientes:

- **SECRETO (S)**
- **RESERVADO (R)**
- **CONFIDENCIAL (C)**

La habilitación para acceso a información clasificada de otros países, en función de los acuerdos para la protección de información clasificada firmados entre estados, se basará en la HPS NACIONAL. Esto no es de aplicación para la información de organizaciones internacionales con políticas de seguridad específicas (OTAN, UE, ESA).

La información clasificada elaborada por organizaciones internacionales, por los países miembro o por organismos vinculados a éstas, se protegerá de acuerdo a los grados de clasificación de seguridad propios, manteniendo los idiomas y formatos oficiales.

4.2.2. Información de la OTAN

La denominación de los grados de HPS para información clasificada OTAN estará basada en la versión en inglés de las clasificaciones usadas por dicha organización:

- **COSMIC TOP SECRET (CTS)**
- **NATO SECRET (NS)**
- **NATO CONFIDENTIAL (NC)**

4.2.3. Información de la Unión Europea

La denominación de los grados de HPS para información clasificada UE estará basada en la versión en inglés de las clasificaciones usadas por la Unión Europea:

- **EU TOP SECRET (EU-TS)**
- **EU SECRET (EU-S)**
- **EU CONFIDENTIAL (EU-C)**

4.2.4. Información de la Agencia Espacial Europea

La denominación de los grados de HPS para habilitar acceso a información clasificada ESA, son los siguientes:

- **ESA TOP SECRET (ESA TS)**
- **ESA SECRET (ESA S)**
- **ESA CONFIDENTIAL (ESA C)**

4.2.5. Información de otras organizaciones internacionales o multinacionales

El tipo de HPS que se exigirá para acceder a información clasificada se determinará en función de la organización internacional o multinacional de que se trate y de la información clasificada que se maneje, teniendo como referencia los cuatro tipos mencionados anteriormente.

Actualmente son de aplicación los siguientes:

ORGANIZACIÓN	TIPO DE HPS
EUROPEAN CORPS	Unión Europea y OTAN
EUROGENDFOR	Unión Europea
OCCAR	Nacional
Programas LOI	Nacional
Programas de otros países con acuerdo de protección con España	Nacional

4.2.6. Especificación de tipo y grado

Todos estos grados se han de tipificar en las HPS, listados de concesión y certificados de HPS que se soliciten y concedan. Con independencia del ámbito, existe una

equivalencia entre todos ellos a efectos de las medidas de protección aplicables. Es decir, son equivalentes y tendrán un tratamiento igual en el proceso, los grados:

- **CTS / EU-TS / ESA TS / S**
- **NS / EU-S / ESA S / R**
- **NC / EU-C / ESA C / C**

Se utilizarán las expresiones «SECRETO o equivalente», «RESERVADO o equivalente», y «CONFIDENCIAL o equivalente», para referirse a grados de distintos tipos pero equivalentes.

4.3. Especialidades

4.3.1. Concepto

En determinados ámbitos de información clasificada, de mayor sensibilidad, es necesario recibir una formación específica y una autorización explícita, antes de poder manejar dicha información. Esta autorización recibe el nombre de especialidad y formará parte de la HPS cuando se precise.

4.3.2. Ámbito de la OTAN

En el ámbito **OTAN** existen las siguientes especialidades:

- **ATOMAL**: Capacita a sus titulares a acceder a información relativa a los activos nucleares a disposición de la Alianza.
- **CRYPTO**: Capacita a sus titulares el acceso al conocimiento y manejo de la documentación y claves utilizadas en los equipos y sistemas criptográficos y de comunicaciones de la OTAN.
- **BOHEMIA**: Capacita a su titular para asistir a reuniones sobre inteligencia de señales, guerra electrónica y para la utilización de medios de comunicaciones para la obtención de información, y garantiza que es consciente de la confidencialidad del asunto y que posee los conocimientos técnicos necesarios.

4.3.3. Ámbito de la Unión Europea

En el ámbito **UE** existen las siguientes especialidades:

- **CRYPTO**: Capacita a sus titulares el acceso al conocimiento y manejo de la documentación y claves utilizadas en los equipos y sistemas criptográficos y de comunicaciones de la UE.

4.3.4. Ámbito de la Agencia Espacial Europea

En el ámbito **ESA** existen las siguientes especialidades:

- **CRYPTO**: Capacita a sus titulares el acceso al conocimiento y manejo de la documentación y claves utilizadas en los equipos y sistemas criptográficos y de comunicaciones de la ESA.

4.3.5. Ámbito nacional

En el ámbito **NACIONAL**, existen las especialidades:

- **CRIPTO**: Capacita a sus titulares el acceso al conocimiento y manejo de la documentación y claves utilizadas en los equipos y sistemas criptográficos y de comunicaciones nacionales, o, al amparo de un acuerdo de seguridad válido que así lo contemple, de otra nación.
- **SIGINT**: Con la misma función que la especialidad BOHEMIA, pero en el ámbito nacional.

5. PROCEDIMIENTO DE HABILITACIÓN DE SEGURIDAD DEL PERSONAL

5.1. Generalidades

El proceso de tramitación de una solicitud de HPS se basa en una investigación sobre las condiciones de seguridad del interesado y de su entorno, es decir, en la realización de un análisis de los riesgos presentes.

El interesado conoce, y autoriza, que va a ser sometido a un proceso de investigación sobre su persona y su entorno. La investigación será más exhaustiva en función del grado de información clasificada al que se necesite acceder. Para ello el interesado debe aportar al expediente de solicitud los datos iniciales para su realización. Durante el transcurso de la investigación se le podrán solicitar los datos adicionales que se estimen necesarios para determinar el riesgo.

Durante la vigencia de la HPS el interesado estará sometido a un proceso de evaluación continua de las condiciones de seguridad, por lo que la investigación podrá retomarse en cualquier momento.

Los datos aportados por el interesado tienen carácter de declaración de seguridad y están exentos de ciertas tutelas previstas en las leyes que regulan la relación

electrónica del ciudadano con la Administración y la protección de datos de carácter personal. En concreto, dada su especial relevancia, se indican:

- Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos. No será de aplicación lo que se establece en artículo 6, párrafo 2, apartado b, con respecto a datos que hayan sido aportados en anteriores declaraciones y con el mismo objeto de obtener una HPS.
- Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. Los ficheros que contienen los datos aportados en los expedientes de solicitud no están sujetos al régimen de protección de los datos de carácter personal que se establece en dicha ley, al estar éstos sometidos a la normativa sobre protección de materias clasificadas, supuesto que se contempla en el artículo 2, párrafo 2, apartado b, de dicha ley.

Estar en posesión de una HPS de un tipo concreto no garantiza, directa y necesariamente, la concesión de acceso a otros diferentes, siendo precisa para ello una nueva solicitud.

5.2. Competencias de los responsables

La ANPIC es la responsable de tomar la decisión respecto a la idoneidad de los ciudadanos que requieran tener una HPS. La concesión o denegación de HPS, y su suspensión o retirada, son competencia exclusiva de la ANPIC.

La ONS, como órgano de trabajo de la ANPIC, es responsable de la gestión y control de los procesos para la determinación de dicha idoneidad. Las solicitudes de HPS serán tramitadas a través de los órganos de control u oficinas de seguridad responsables en los organismos o entidades a las que pertenezcan los interesados.

La ONS podrá solicitar de dichos organismos o entidades cuanta información adicional precise relativa a la solicitud.

Los organismos, unidades y empresas dispondrán de los medios necesarios para gestionar el proceso de solicitud de HPS de su personal. La tramitación de las solicitudes de HPS se realizará por el canal funcional o jerárquico de responsabilidad que sea pertinente y que estará previamente definido.

Es responsabilidad de las autoridades, mandos o responsables, determinar y catalogar aquellos puestos de trabajo de sus respectivos organismos, unidades o empresas, en los que se debe estar en posesión de la oportuna HPS.

Las autoridades y órganos que determinan la necesidad, e inician la tramitación o la gestionan a la ONS, de cada solicitud de HPS, junto con sus respectivos servicios de protección de información clasificada, serán responsables de:

- Verificar que la solicitud corresponde a una persona que ocupa un puesto que precisa HPS.
- Determinar y aprobar, caso por caso, la necesidad y pertinencia de su tramitación.
- Tramitar exclusivamente las solicitudes de aquellos interesados de acreditada confianza.
- La correcta elaboración y tramitación del expediente, en la parte de su competencia.
- La instrucción y concienciación de seguridad del interesado de la solicitud.
- En los casos en que se tengan competencias de investigación autorizadas, gestionar su realización.
- Certificar los pasos del proceso que sean de su competencia.
- Garantizar que las personas que manejan o custodian información clasificada tengan concedida la HPS antes de asumir sus obligaciones.

En determinados casos podrá ser necesario solicitar HPS para personas que no pertenecen al organismo, unidad o empresa en cuyo beneficio y bajo cuya responsabilidad van a trabajar (por ejemplo, asesores de la Administración, personal no empleado del contratista, o personal agregado de otros organismos). En este caso, dicho organismo, unidad o empresa, podrá tramitar la correspondiente solicitud, como si de personal propio se tratara, aunque indicando su especial situación de dependencia.

En el caso particular de personal laboral de empresas o autónomos, contratado para prestar servicio de asesoramiento, las condiciones que han de darse son:

- El interesado está contratado específicamente para prestar el servicio designado y no podrá ser sustituido a criterio de la empresa.
- El interesado va a acceder a la información clasificada exclusivamente en las instalaciones del órgano para el que trabaja.
- El interesado no podrá compartir la información clasificada de la que tenga conocimiento con la empresa de la que procede.

Si estas condiciones no se pudieran cumplir, la actividad debería englobarse en los supuestos previstos en la norma NS/06.

Es importante conocer las diferencias y los matices entre una y otra situación, al objeto de hacer un uso correcto de esta facilidad y no como una forma de eludir

el cumplimiento de las obligaciones que contraen las empresas que quieran participar en contratos, programas o actividades, clasificados, con la Administración.

El uso de este procedimiento particular no eximirá a las empresas del cumplimiento de las obligaciones que contraen con la Administración por el hecho de participar en contratos, programas o actividades clasificados.

5.3. Derechos y obligaciones de los interesados

Los interesados, adquieren la obligación de aportar los datos solicitados, de forma veraz y cuanta información adicional se les requiera. Asimismo, deberán comunicar los cambios significativos en su situación personal desde el momento de la concesión de la HPS.

El incumplimiento de cualquiera de estos requisitos podrá ser motivo de denegación o retirada de la HPS.

Por otra parte, los procesos de investigación de seguridad estarán de acuerdo con la legislación nacional y dentro de las prerrogativas que la misma concede a la ANPIC. En todo caso, habrán de ser conformes a cualquier otra legislación nacional de mayor rango que afecte a la protección de los derechos de los individuos.

Los datos aportados por los interesados en el proceso de tramitación se custodiarán con la debida protección a lo largo de todo el trámite de solicitud.

Los interesados no podrán tramitar directamente solicitudes de HPS a la ANPIC, por ser precisa la existencia de un organismo, unidad o empresa garante de la solicitud.

5.4. Procedimiento de habilitación de seguridad del personal

5.4.1. Generalidades

El proceso de habilitación de seguridad del personal se desarrolla en los siguientes pasos:

- Determinación del personal para el que se debe solicitar una HPS.
- Elaboración del expediente de solicitud.
- Realización de investigaciones de seguridad autorizadas y su certificación.
- Tramitación del expediente de solicitud.

– Análisis e investigación de expedientes en la ONS.
– Concesión o denegación de la HPS. Certificaciones.

Forman también parte del proceso:

– Retirada de la HPS.
– Renovación de la HPS.
– Ampliación de la HPS.
– Suspensión de la HPS.

La gestión del proceso de solicitud de una HPS será similar tanto si se trata de una solicitud inicial, como de una renovación o ampliación de una previa existente. Únicamente en el caso de la ampliación se puede eximir al órgano solicitante o al interesado de algunos trámites o formularios, según se indica más adelante.

5.4.2. Condiciones de elegibilidad para solicitar una HPS

Por criterios de elegibilidad se entienden el conjunto de condiciones o requisitos básicos que una persona, salvo excepción expresamente autorizada por la ANPIC, debe cumplir previamente para optar a una HPS.

Solo se asignará a puestos que precisen que su titular posea HPS, al personal que cumpla los requisitos de elegibilidad necesarios o que ya esté en posesión de la HPS del grado y tipo adecuados.

Los requisitos de elegibilidad son:

a) Tener edad superior a los 18 años.
b) Tener plena capacidad legal.
c) Cumplir con alguno de los siguientes requisitos relativos a la nacionalidad y grado de compromiso con España:

– Ser español y haber ostentado la nacionalidad española durante el siguiente tiempo mínimo, **inmediato al de solicitud de la HPS**:

• **tres (3) años**, para HPS de grado «CONFIDENCIAL o equivalente»,
• **cinco (5) años**, para HPS de grado «RESERVADO o equivalente», y
• **diez (10) años**, para HPS de grado «SECRETO o equivalente».

Tratándose de casos de doble nacionalidad, en los que una de las nacionalidades del interesado no coincida con alguna de las señaladas

posteriormente, la solicitud de HPS será objeto de un análisis caso por caso por parte de la ONS, al objeto de evitar que se dé un posible conflicto de lealtades.

– Ser nacional de un estado miembro de alguna de las organizaciones internacionales a las que España pertenece. En este caso, se tramitará la solicitud de HPS a su país de origen, utilizando sus formularios y procedimientos.

  En el ámbito de seguridad industrial si el interesado acredita al menos 5 años de residencia continuada en España, la ANPIC podrá conceder la HPS, conforme a sus procedimientos (establecidos en esta norma).

– Ser nacional de un país con los que España tenga firmado un acuerdo para la protección de la información clasificada. Para la tramitación de la HPS se procederá caso por caso en función de lo establecido en el acuerdo.

El personal de procedencia extranjera que no cumpla los anteriores requisitos de elegibilidad no podrá, por tanto, ser asignado a ningún puesto que implique la necesidad de estar en posesión de una HPS.

Las autoridades, mandos o responsables, sólo tramitarán aquellas solicitudes de HPS en las que el interesado cumpla los requisitos de elegibilidad.

Si se estimara imprescindible tramitar una solicitud en la que no se cumpla alguno de estos requisitos se remitirá un informe adjunto de motivaciones con la solicitud. El criterio de admisión a trámite en la ONS será restrictivo, elevando a la ANPIC la solicitud, con las motivaciones y hechos que concurren, para una decisión final sobre la denegación o concesión.

Las solicitudes correspondientes a personas que no cumplan los requisitos de elegibilidad serán devueltas al organismo o entidad solicitante.

5.4.3. Elaboración del expediente de solicitud

El expediente inicial de solicitud de HPS consta de una serie de formularios básicos, publicados para su uso en la página «web» de la ONS, en la dirección URL:

http://www.cni.es/es/ons/documentacion/formularios

Los formularios actualmente vigentes son:

– **Solicitud de habilitación personal de seguridad**. En este formulario, el órgano solicitante identifica los datos fundamentales del interesado

y expresa lo que se solicita, junto con una justificación detallada de la necesidad. Asimismo, el jefe o responsable de quien depende el interesado, con el nivel de responsabilidad y la competencia adecuados, certificará la necesidad y la pertinencia de la solicitud, y autorizará su tramitación. Incluye una declaración por la que el jefe de seguridad avala con su firma que el interesado ha sido concienciado en la protección de la información clasificada y, en su caso, instruido en las especialidades pertinentes.

– **Declaración personal de seguridad**. Formulario que deberá rellenar exclusivamente el interesado, quien certificará con su firma la veracidad de los datos aportados. Aparte de los datos que se aportan, el interesado declara y firma que comprende perfectamente sus obligaciones especiales y permanentes en lo que se refiere a la protección de la información clasificada. Asimismo, reconoce las responsabilidades penales y disciplinarias por la divulgación no autorizada de esta clase de informaciones**.** Del mismo modo, autoriza el uso de los datos aportados, o de aquellos que sea necesario recabar posteriormente, para la investigación de seguridad.

Para los expedientes de solicitud de ampliación de una HPS, si no ha habido cambios en los datos de la declaración personal de seguridad, no será necesaria la remisión completa de dicho formulario[1]. En cualquier caso, **será obligatoria** la remisión del **apartado 7 de dicho formulario, que contiene la declaración personal del interesado**.

Se encuentra disponible en la página «web» de la ONS un documento adicional de Orientaciones con instrucciones específicas para la cumplimentación y tramitación de las solicitudes de HPS.

En el caso de interesados que hayan adquirido cualquiera de las nacionalidades mencionadas en el **apartado 5.4.2., párrafo 2, letra c)**, se deberá incluir, adjunta a la solicitud:

– Copia compulsada del **acta de nacionalización** u otro documento oficial que lo avale, donde deberá figurar la fecha en que se adquiere la nueva nacionalidad.

[1] Dado que ha habido un cambio de formularios y los datos aportados con el antiguo difieren de los requeridos actualmente, si la solicitud anterior fue tramitada con los formularios CPS y CIS antiguos, **en este caso se deberá remitir obligatoriamente el DPS completo**.

5.4.4. Elaboración del expediente de solicitud en el ámbito de la seguridad industrial

En el ámbito de la **seguridad industrial**, los expedientes de solicitud de HPS del personal perteneciente a empresas contratistas, además de la documentación indicada en el apartado anterior, deberán incluir el siguiente formulario, disponible en la página «web» de la ONS:

– **Propuesta de Personal**. En este formulario, el contratista especifica el perfil laboral del interesado y los contratos clasificados en los que se prevé su participación. Incluye el visto bueno del inspector de seguridad industrial, que avala con su firma el proceso de solicitud, desde el punto de vista de la seguridad industrial.

En la citada norma NS/06 se amplían detalles sobre este procedimiento específico.

5.4.5. Tramitación del expediente de solicitud

5.4.5.1. Proceso secuencial de trámite

El proceso secuencial de trámite es el siguiente:

– El órgano solicitante, tras determinar la necesidad de solicitar una HPS para el interesado, rellena el formulario de solicitud de HPS, dando exacto cumplimiento a cuanto en él se requiere.
– El órgano de control u oficina de seguridad, responsable de su tramitación, imparte, o verifica, la ejecución de la concienciación en seguridad del interesado.
– El interesado, a requerimiento y asesorado por el personal del órgano de seguridad de la información clasificada de su organismo o entidad, rellena la declaración personal de seguridad.
– El expediente, al que se irá adjuntando la documentación adicional que se precise, se remite a través de la estructura nacional de protección de la información clasificada, para que finalmente llegue a la ONS. Cada escalón jerárquico por el que circule es responsable de que los expedientes estén **completa y correctamente cumplimentados**.
– El organismo responsable de la remisión del expediente a la ONS, certificará con el sello oficial y firma, estampados en la Solicitud de HPS, que todo el proceso se ha efectuado conforme a la normativa y que la documentación que se entrega está revisada y completa.

La fecha de entrada del expediente de solicitud en la ONS no podrá ser posterior a seis (6) meses de la fecha de firma de la declaración personal de seguridad por el interesado, al objeto de asegurar la vigencia de los datos aportados.

Una norma particular de la Autoridad SIGINT de España, establecerá las peculiaridades de tratamiento para la concesión de HPS con especialidad BOHEMIA o SIGINT, que requiere una instrucción especial y su tramitación a través de canales específicos.

5.4.5.2. Clasificación de la documentación aportada

El expediente inicial de solicitud tendrá un tratamiento de reserva especial, no permitiendo su acceso a personal ajeno al proceso, tanto durante su tramitación como durante su almacenamiento y custodia. No obstante, el expediente no tendrá consideración de información clasificada.

5.4.5.3. Personal español en el extranjero

Los oficiales de seguridad de los órganos de protección de la información clasificada de cada país u organismo que determine la necesidad de HPS, serán quienes deban responsabilizarse de la concienciación en seguridad y de la acreditación de la necesidad de conocer de los interesados.

Los responsables de las oficinas de seguridad de los mandos, agencias u organismos, así como las autoridades nacionales de seguridad (ANS) de otros países, tramitarán a la ANPIC los expedientes de solicitud, conforme a los modelos y criterios españoles.

Los casos más comunes son:

- **Personal español destinado en organismos militares o civiles de la OTAN**. Tramitan las solicitudes las oficinas de seguridad de los mandos y agencias, o la propia Oficina de Seguridad de OTAN (NOS).
- **Personal español destinado en el Consejo de la Unión Europea, en la Comisión Europea, en el Servicio Europeo de Acción Exterior, o en agencias dependientes**. Tramitan las solicitudes principalmente a través de la Oficina de Seguridad de la Secretaría General del Consejo y del Departamento de Seguridad de la Comisión, o directamente desde las Agencias. Dado que estos órganos normalmente son los que otorgan su propia autorización de acceso, España emite un certificado dictaminando la idoneidad o no idoneidad del interesado para un grado específico.

- **Personal español destinado en el Parlamento Europeo**. Tramitan las solicitudes a través del Departamento de Seguridad del Parlamento Europeo.
- **Personal español en organismos y empresas de otros países**. La ANS del país en cuestión, tramitará las solicitudes directamente a la ANPIC española.
- **Personal en otras organizaciones internacionales o en programas de carácter militar o civil, como EUROCUERPO, OCCAR, etc.** Tramitan las solicitudes las oficinas de seguridad respectivas.

Se habilitarán procedimientos específicos para aquellos otros casos que, a juicio de la ONS, así lo requieran.

5.4.5.4. Necesidad de órgano garante

Como norma general, será precisa la existencia de un organismo, departamento o empresa que actúe como garante y patrocinador del interesado y que tramite la solicitud. Dicho garante deberá contar con una estructura y medios de seguridad adecuados y oficialmente acreditados, definidos por los siguientes requisitos:

- **Organismos y departamentos de la Administración**: habrán de tener establecido un órgano de control, aprobado por la ANPIC.
- **Empresas**: deberán tener concedida una HSEM.
- **Organismos internacionales**: deberán tener establecida una oficina de seguridad.

5.4.6. Realización de investigaciones de seguridad autorizadas y su certificación

Aquellos organismos que tienen capacidad de investigación para determinar las condiciones de seguridad de los interesados, están autorizados para realizar las investigaciones del personal propio. Este es el caso de los tres Ejércitos, las Fuerzas y Cuerpos de Seguridad Estado y del CNI. No están incluidas por tanto, las investigaciones del personal perteneciente a los Cuerpos Comunes de los Ejércitos.

Si se estima preciso, la ONS podrá realizar una investigación de seguridad complementaria a la ya realizada por el organismo con competencias de investigación de seguridad. En este sentido, las solicitudes de HPS de grado «SECRETO o equivalente» serán sometidas a investigaciones adicionales específicas. Para solicitudes de grado de clasificación inferior, la ONS decidirá, para cada caso, si se precisa o no el realizar investigaciones adicionales.

Los Cuarteles Generales de los tres Ejércitos, la Guardia Civil, la Policía Nacional y el CNI establecerán su normativa particular por la que se ha de regir el proceso

de investigación de seguridad. Las investigaciones se basarán en los datos disponibles del interesado en las bases de datos, expedientes de su organismo o entidad de procedencia, en las investigaciones internas y en las entrevistas que se puedan realizar.

El resultado de la investigación de seguridad realizada por estos organismos sobre cada interesado se reflejará en un **certificado de investigación de seguridad autorizada**, que será remitido a la ONS dentro del expediente de solicitud de habilitación de cada interesado.

Tendrán capacidad de firma de estos certificados, para el personal de su ámbito de competencia:

- Los Segundos Jefes de los Estados Mayores del Ejército de Tierra, Armada y Ejército del Aire,
- El Director Adjunto Operativo de la Guardia Civil,
- El Director Adjunto Operativo del Cuerpo Nacional de Policía, y
- El Secretario General del Centro Nacional de Inteligencia.

La firma de estos certificados podrá ser delegada, por el titular, en quien éste estime oportuno, debiendo previamente informar de dicha delegación a la ANPIC, identificando a la persona o cargo en quien delega, quien firmará siempre «Por orden» del titular.

Existirá un único modelo de certificado, vigente en cada momento, que se utilizará tanto si se ha determinado la existencia de circunstancias relevantes para la protección de la información clasificada, como si no. El certificado no reflejará en ningún caso los hechos concretos observados en las investigaciones realizadas, limitándose únicamente a la indicación de su existencia.

Las modificaciones que se realicen en el modelo de certificado serán debidamente comunicadas a los organismos afectados.

Se podrá emitir un certificado colectivo sobre varios interesados siempre que en ninguno de ellos se hayan apreciado circunstancias relevantes para la seguridad. En caso contrario, el certificado deberá ser individual.

En caso de que se emita un certificado colectivo, en el expediente de cada interesado se incluirá una copia compulsada del certificado original.

Los datos concretos de las investigaciones, que sean relevantes, se harán llegar a la ONS por los conductos autorizados a tal fin, mediante informe adicional.

Los certificados de investigación de seguridad autorizada, así como los informes asociados, no serán, en ningún caso, directamente vinculantes para la ANPIC, quien en virtud de su competencia exclusiva en la concesión, denegación y retirada de HPS, podrá conceder o denegar una HPS aún en contra de los resultados relevantes de aquéllos.

En nombre de la ANPIC, la ONS podrá reclamar información de investigación guardada u otra adicional, en cualquier momento, para proceder a nuevas investigaciones y a las comprobaciones de seguridad que sean precisas, incluso después de terminar la vigencia de la HPS.

Los datos y resultados de las investigaciones, se conservarán al menos hasta que transcurra **un (1) año** desde que haya caducado la HPS objeto de las investigaciones.

En el caso del personal militar de los Cuerpos Comunes, la investigación de seguridad la realizará la ONS.

5.4.7. Análisis e investigación de expedientes en la ONS.

5.4.7.1. Análisis

Los expedientes de solicitud de HPS una vez han tenido entrada en la ONS son revisados para determinar que están completos y conformes a la normativa. En caso contrario, se devolverán al órgano tramitador para su revisión.

Los expedientes que sean admitidos seguirán el proceso de tramitación.

5.4.7.2. Condiciones de la investigación

Es preceptivo que la concesión de una HPS por la ANPIC esté basada en una investigación de seguridad sobre el interesado y su entorno. Los criterios de valoración de idoneidad se establecen en el **apartado 6** de esta norma.

La investigación previa del interesado y su entorno debe abarcar un periodo de tiempo mínimo, inmediato al de solicitud de la HPS, sobre el cual realizar los chequeos de seguridad, periodo que vendrá marcado por el grado de HPS que se solicita. Estos periodos de tiempo mínimo son:

– Cinco (5) últimos años, o desde que cumplió los 18 años hasta la fecha (el que sea inferior), para HPS solicitada de grado «CONFIDENCIAL o equivalente»,

– Diez (10) últimos años, o desde que cumplió los 18 años hasta la fecha (el que sea inferior), para HPS solicitada de grado «RESERVADO o equivalente» y superior.

Las condiciones de residencia del interesado y de su cónyuge o cohabitante, deben permitir efectuar una investigación de seguridad adecuada. Por lo tanto, todas aquellas solicitudes en las que por motivos de residencia no se puedan realizar las investigaciones preceptivas para los tiempos mínimos establecidos, podrán ser objeto de devolución.

Si el interesado, o persona de su entorno, ha residido durante el periodo objeto del chequeo en otros países, se podrán solicitar investigaciones de seguridad a las autoridades competentes de los países afectados, relativas al periodo de tiempo de dicha residencia. En estos casos es necesaria la existencia de un acuerdo para la protección de información clasificada o una reglamentación de seguridad ratificada por el Reino de España que avale el proceso de investigación realizado.

De manera excepcional, y estudiando la conveniencia caso por caso, podrán establecerse convenios de colaboración en materia de investigación con países no incluidos en los casos del apartado anterior.

Para aquellos países u organizaciones en los que estos acuerdos o reglamentación no existen, se considerarán los períodos de tiempo de residencia en estas condiciones como no efectivos para la investigación de seguridad. No se solicitarán investigaciones a estos países u organizaciones, en estas condiciones.

Durante los periodos que se deben chequear, el tiempo no efectivo, para el interesado, no deberá superar el cincuenta por ciento del tiempo total. Si lo supera, se considerará como motivo justificado de devolución de la solicitud.

5.4.8. Concesión de la HPS. Certificaciones.

5.4.8.1. Concesión

Una vez finalizadas las investigaciones de seguridad, y siendo favorables los informes, se formalizará la concesión de la HPS. La HPS se extiende, inicialmente, por un periodo de validez de cinco años, salvo que se conceda con carácter restringido en el tiempo, caso que se considera más adelante, en este mismo apartado.

La HPS definirá explícitamente los términos exactos del acceso a que se habilita, es decir, grado, tipos y especialidades para los que se expide, así como las fechas de concesión y de caducidad.

El acto de concesión de la HPS por la ANPIC tendrá plena validez con la firma de los listados de concesión de HPS, que le son presentados por la ONS para su aprobación.

La comunicación de la concesión a los órganos solicitantes, cuando éstos sean los servicios de protección de información clasificada, podrá realizarse mediante documento expreso para cada HPS, firmado por la ANPIC, conforme al modelo del anexo I, o comunicarse globalmente mediante un certificado de listado de concesión de HPS. En determinadas condiciones, y para efectos concretos, la comunicación se realizará mediante una certificación individualizada de dicha concesión firmada por un responsable autorizado de la ONS, conforme al modelo del anexo II.

Las HPS concedidas y los certificados de listados de concesión de HPS de un determinado organismo o entidad, serán custodiados o en el subregistro principal o en el servicio central de protección de información clasificada (si no existe subregistro principal), bajo la responsabilidad directa de su Jefe de Seguridad, manteniendo un registro actualizado único y completo de habilitaciones concedidas. La pérdida o extravío de una HPS o de un certificado de listado de concesión de HPS, tendrá la consideración de comprometimiento de la seguridad y será motivo de informe a la ONS, que emitirá en caso necesario un duplicado.

Cuando el titular de una HPS cambie de destino o de puesto de trabajo, si implica un cambio de dependencia a un subregistro principal distinto (o servicio central de protección, en su caso), el titular de la HPS deberá comunicarlo para que su HPS sea remitida al nuevo, **con conocimiento de la ONS**. Si en el nuevo destino no precisa acceder a información clasificada, la HPS se devolverá a la ONS.

Se procurará que el tiempo necesario para la **concesión de una HPS** no exceda de **seis meses** desde su admisión a trámite por la ONS. Este plazo quedará interrumpido cuando se soliciten investigaciones a organismos ajenos a la ONS, o cuando haya de realizarse una investigación en mayor profundidad.

Cuando en algún expediente se aprecien circunstancias de seguridad que así lo aconsejen, o cuando por la justificación de la necesidad de conocer se determine que el acceso a información clasificada vaya a ser limitado en el tiempo, se podrá proceder a una **concesión restringida** de la HPS. La restricción en la concesión podrá afectar al grado solicitado, al periodo de validez o a ambos aspectos.

Como norma general, el grado concedido a una persona se tratará que sea único, con independencia de los tipos a los que tenga acceso, dado que la investigación de seguridad siempre se realizará para el grado más elevado solicitado. No obstante, cuando resulte innecesario disponer de la HPS de grado máximo a nivel nacional o internacional, se podrán solicitar grados distintos. En estos casos, la vigencia de ambas habilitaciones vendrá determinada por la caducidad de la HPS de mayor grado.

Es responsabilidad del organismo, unidad o empresa que custodia la información, el no permitir a ningún usuario el acceso a información clasificada de grado superior al que precisa conforme a su necesidad de conocer, con independencia del grado que tenga concedido. En caso necesario, con la finalidad de evitar posibles comprometimientos, los órganos de control emitirán certificaciones de HPS del grado requerido, aunque éste sea inferior al grado concedido que ostenta el titular de la HPS.

5.4.8.2. Emisión de certificados de HPS

En virtud de la existencia de la HPS concedida por la ANPIC, los subregistros principales (o servicios centrales de protección, es su caso) podrán emitir Certificados de HPS, usando un modelo propio basado en el del anexo II. Este certificado será para **uso exclusivo dentro de España**, a efectos de comunicación a órganos de control subordinados o de certificaciones a personas.

La capacidad de determinados subregistros principales para poder emitir, con carácter general, certificaciones válidas internacionalmente, requerirá autorización formal previa de la ONS y estará sujeta a las condiciones de ejecución y limitaciones que, mediante escrito oficial, se determinen.

Estos certificados, cuando sean con validez internacional autorizada, deberán ir siempre firmados por el jefe de seguridad del subregistro principal, o su suplente, caso de ausencia del primero.

Los Certificados de HPS siempre incluirán el **propósito** o fin para el que se expide y el **periodo de validez** para el que se emite. Estarán numerados y se llevará un registro de los emitidos. El periodo de validez no podrá exceder a la fecha de caducidad de la HPS sobre la que se certifica, salvo en los certificados emitidos durante el proceso de renovación de la HPS y que se contempla más adelante.

Cuando se emitan directamente a personas, su periodo de validez nunca superará el año, siendo recomendable, en cualquier caso, el que se extiendan sólo para el plazo de duración de la actividad para la cual se emiten.

Cuando se emitan para órganos de control subordinados, se tendrá en cuenta que, en caso de retirada o modificación de la HPS en la que se basan, los certificados perderán su razón de ser, por lo que deberán ser retirados y destruidos por quien los emitió.

5.4.9. Denegación de la HPS

En los casos en los que el resultado de la investigación determine la existencia de riesgos no asumibles para la seguridad de la información clasificada, en el interesado o en su entorno, la ANPIC no concederá la HPS.

Los factores de riesgo para la seguridad de la información clasificada se recogen en los criterios de valoración establecidos en el apartado 6 de esta norma.

La existencia de riesgos no asumibles se fundamentará en una resolución de denegación firmada por la ANPIC.

La denegación de la HPS se basará no solo en la existencia de circunstancias evidentes y concretas que permitan determinar un riesgo evidente de compromemetimiento de la información clasificada en caso de su concesión (delitos, conductas, etc.), sino que también se tendrá en cuenta la existencia de indicios de vulnerabilidades o de amenazas que afectan, o que pueden afectar, al interesado o a su entorno, incluso por la posible acción de un tercero.

Será motivo suficiente de denegación o retirada el que se falsee cualquiera de los datos que se requieren en el expediente de solicitud, o el que estos no se aporten en su totalidad en el plazo establecido.

La denegación se comunicará al órgano solicitante mediante oficio, incluyendo la resolución de denegación para su entrega al interesado.

El órgano solicitante será responsable de entregar la resolución y de remitir el acuse de recibo firmado por el interesado a la ONS.

La denegación, con carácter general, tendrá el efecto adicional de inhabilitar al interesado para que se le pueda solicitar una nueva HPS durante los 5 años siguientes, independientemente del grado de la HPS denegada. El periodo de inhabilitación contará a partir de la fecha de firma del acuse de recibo.

Este plazo podrá extinguirse, mediante resolución al efecto, cuando quede suficientemente demostrado y avalado que las causas que motivaron la denegación han desaparecido y no tienen efecto alguno que desaconseje una concesión.

Para poder acogerse a esta exención será preciso que el organismo, o entidad al que pertenece el interesado solicite previamente de la ONS su revisión, debiendo aportar para ello las pruebas y datos necesarios que puedan modificar el análisis de riesgo previamente realizado. No se tramitarán en ningún caso expedientes de solicitud de interesados inhabilitados sin tener la autorización previa de la ONS para proceder.

5.4.10. Retirada de la HPS

La ANPIC podrá proceder a la retirada de una HPS si considera que existen motivos en el interesado o en su entorno que lo justifican.

En caso de retirada, se aplicará la misma restricción de tiempo, y la misma excepción, que se señala en el **apartado 5.4.9,** relativo a la denegación, a contar a partir de la fecha de firma del acuse de recibo de la resolución de retirada.

5.4.11. Apelación

Las resoluciones adoptadas estarán sujetas al régimen jurídico establecido en la Ley del Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común.

5.4.12. Renovación de la HPS

La HPS se extiende, inicialmente, por un periodo de validez de **cinco años**, salvo concesión restringida en el tiempo. Si al terminar este período se mantiene la necesidad de seguir disponiendo de la HPS, se solicitará su renovación a la ANPIC con antelación suficiente, para lo que se seguirán los mismos trámites y se usarán los mismos formularios que si se tratara de una solicitud inicial.

Se considerará periodo de renovación cuando reste menos de un año para la caducidad de la HPS.

Cada renovación exige una nueva investigación de seguridad del titular de la HPS, sobre la base de la declaración personal de seguridad, que deberá ser rellenada de nuevo por el interesado con datos actualizados, y que formará parte del expediente de solicitud.

La renovación se puede realizar para el mismo grado, tipos y especialidades de la que caduca, o bien, para otros diferentes, manteniendo en todos los casos el carácter de renovación.

El expediente de solicitud de renovación tendrá el mismo contenido y tratamiento que una solicitud inicial, con la única salvedad de que el plazo de validez de la HPS que se conceda puede ser diferente. El periodo de validez de la HPS renovada, con carácter general, será de **cinco años** en el caso de las habilitaciones de grado «SECRETO o equivalente» y de **diez años** en el caso de las habilitaciones de grado RESERVADO y CONFIDENCIAL, o equivalentes. En todo caso será también aplicable para las renovaciones la posibilidad de realizar una concesión restringida.

La HPS con especialidad ATOMAL o con especialidad BOHEMIA / SIGINT, se renovará siempre por **cinco años**, con independencia del grado de clasificación. Para la especialidad CRIPTO / CRYPTO no es de aplicación esta restricción.

Si se solicita renovación de la HPS una vez transcurrida la fecha de caducidad de la anterior, será considerado como una solicitud inicial, por lo que se concederá únicamente por **cinco años**. A dichos efectos se tendrá en cuenta la fecha de entrada de la solicitud en la ONS.

Una HPS mantiene su vigencia hasta que se cumpla su fecha de caducidad. **Si con antelación a la fecha de caducidad se hubiera recibido en la ONS, y estuviera en trámite de concesión, la solicitud de renovación**, se admitirá un plazo máximo de seis meses de prórroga de la validez de la HPS, a contar desde la fecha de caducidad, con carácter automático y sin necesidad de solicitud al efecto. En estas condiciones, y sin sobrepasar el plazo indicado, los órganos autorizados podrán emitir certificados de HPS válidos.

5.4.13. Ampliación de la HPS

La HPS se emite con un determinado grado de clasificación y para uno o varios tipos de información (OTAN, UE, ESA, nacional) a los que se precisa y se habilita para acceder.

En caso de ser necesario, se puede solicitar una ampliación de HPS, bien del grado de clasificación como del tipo o especialidad de información clasificada al que se autoriza a acceder. La ampliación se solicitará a la ANPIC por la línea de tramitación habitual, concediéndose, en su caso, con la misma fecha de caducidad que la HPS original que se amplía, salvo que el nuevo grado implique un período

de vigencia menor (como ocurre para grado «SECRETO o equivalente», o para determinadas especialidades).

El expediente de solicitud de ampliación de HPS básicamente consta de la solicitud de habilitación personal de seguridad, rellena de la misma forma que para una solicitud inicial. Cuando se tramite un expediente de solicitud como ampliación, si no ha habido cambios en los datos de la declaración personal de seguridad, no será necesaria la remisión de dicho formulario completo. En cualquier caso, **siempre será obligatoria la remisión, como mínimo, del apartado 7 del formulario**, donde se contiene la declaración personal del interesado.

No se podrá solicitar ampliación en caso de que quede menos de un año para la caducidad de la HPS sobre la que se amplía. En este caso se solicitará directamente como una renovación.

La solicitud de ampliación siempre incluirá en el formulario de solicitud todos los tipos, especialidades y grados que el interesado requiere. Es decir, no se solicitará solo lo que se amplía, sino también lo que se mantiene, de forma que los accesos que no se incluyan en la nueva solicitud de ampliación se suprimirán de la nueva HPS del interesado que se emita. En todos los casos, la anterior HPS quedará automáticamente cancelada al emitirse la nueva, debiendo ser devuelta a la ONS.

5.4.14. Asignación provisional de grado superior

En aquellos casos en que haya diferentes titulares de HPS que opten a una misma vacante que requiere una HPS de grado superior a la que ostentan, se autoriza a que el jefe de seguridad del servicio de protección pueda solicitar a la ANPIC una certificación de HPS del grado requerido para dicha vacante para el titular al que le sea concedida.

El jefe de seguridad del servicio de protección, responsable último de la tramitación del expediente a la ONS, deberá solicitar expresamente y de forma motivada, la aplicación de este procedimiento, por oficio dirigido a esta.

Este procedimiento de certificación de HPS tiene carácter excepcional y para su solicitud deberán concurrir las siguientes circunstancias:

a) La vacante ha sido asignada de forma oficial al interesado.
b) El interesado debe ser ya titular de una HPS del grado inmediatamente inferior al solicitado.
c) Quedan excluidas las especialidades de este proceso (Cripto, Atomal, etc.).

d) Se hayan iniciado las acciones pertinentes para proceder a la ampliación de grado, o se inician en ese mismo momento.

Una vez autorizado, la ONS emitirá un **certificado de HPS con una validez de seis (6) meses**, plazo en el que deberán resolverse los trámites para la concesión definitiva.

En virtud de este certificado, el jefe de seguridad del órgano de control correspondiente podrá emitir las certificaciones precisas para la incorporación del interesado a su nuevo destino.

5.4.15. Suspensión de la HPS

Una HPS estará en estado de suspensión cuando, sin haber llegado a su fecha de caducidad, deja de tener vigencia para el interesado.

En determinados casos, si se tuviese conocimiento de la existencia de aspectos que puedan afectar a la seguridad de la información clasificada, la ANPIC podrá proceder, en cualquier momento, a la suspensión de una HPS en vigor. Simultáneamente, la ONS llevará a cabo una investigación de la que se derivará la retirada o la confirmación de la HPS afectada.

Durante el periodo de suspensión, **a todos los efectos el usuario carece de habilitación personal de seguridad**, lo que deberá ser comunicado al órgano responsable de la custodia de la HPS, a los organismos que dispongan de certificaciones en vigor sobre esta HPS y al propio usuario.

El tiempo de suspensión no tendrá efecto alguno sobre la fecha de caducidad de la HPS.

6. CRITERIOS DE VALORACIÓN DE IDONEIDAD DE LAS PERSONAS

La investigación de seguridad de un interesado supone un **análisis de riesgos** realizado sobre la persona y su entorno, donde el objetivo es identificar y valorar las **vulnerabilidades** que presenta y las **amenazas** a las que pueda estar sometido, con la finalidad de determinar que el grado de riesgo que se asume al habilitarlo resulta aceptable para el Reino de España.

A continuación se enumeran los principales aspectos (amenazas y vulnerabilidades) que se tienen en consideración durante el análisis de riesgo para la determi-

nación del grado de lealtad, honradez y fiabilidad de una persona en el manejo de información clasificada.

Los criterios de valoración que se citan, también serán de aplicación para las personas más cercanas del entorno del interesado y se tendrán en cuenta a la hora de considerar su idoneidad.

En este sentido, se harán las investigaciones necesarias para determinar si una persona, su cónyuge o pareja, familiares cercanos (hasta primer y segundo grado por consanguinidad o afinidad), o personas vinculadas cercanas, se encuentran tipificados dentro de alguna de las siguientes situaciones de riesgo, o existen indicios razonables de que puedan estarlo:

a) La participación, conspiración, ayuda o inducción a la comisión de actos de sabotaje, espionaje, terrorismo, traición o sedición,
b) La colaboración o relación, de forma interesada o inconsciente, con un servicio de inteligencia o gobierno extranjero que pueda constituir una amenaza para la seguridad de España, de la OTAN, de la Unión Europea o de sus Estados Miembros o de otros aliados del Reino de España. Quedan excluidas las relaciones autorizadas de carácter oficial.
c) La asociación, adscripción, afinidad ideológica, amistad o complicidad con organizaciones, grupos o personas que utilicen medios violentos o ilícitos para subvertir el orden constitucional de España o de sus aliados.
d) La pertenencia o afinidad del interesado a asociaciones, grupos o fundaciones, cualesquiera que sea su forma jurídica, que pudiera suponer un conflicto de lealtades con la protección de la información clasificada.
e) La falta de acatamiento a la Constitución y al ordenamiento jurídico de España o de la Unión Europea.
f) La asociación, adscripción, afinidad, amistad o complicidad con organizaciones, grupos o personas, cuyas actividades impidan a otros el ejercicio de sus libertades y derechos constitucionales.
g) La falta de colaboración o el intento de engaño en la investigación de seguridad.
h) Falsear, ocultar, mentir, o no aportar la información o los datos requeridos, durante el proceso de tramitación de la solicitud de HPS o durante la vigencia de la misma.
i) La existencia de deudas con la Administración tributaria o la seguridad social de España o de otros Estados Miembros de la Unión Europea, derivadas de engaño o fraude.
j) La detección de indicios de actividades delictivas, independientemente de que deriven o no en responsabilidades penales.
k) La existencia de dificultades financieras graves.

l) La existencia de ingresos patrimoniales injustificados.
ll) El consumo reiterado de drogas ilegales o el consumo abusivo de drogas lícitas.
m) El abuso en el consumo de bebidas alcohólicas.
n) Cualquier adicción, dependencia o conducta, pasada o actual, reiterada e incontrolada, que pueda afectar de forma significativa a las normas de convivencia o suponer una vulnerabilidad personal por chantaje o presión.
o) La falta de discreción relativa a su vida privada o laboral que pueda derivar en una vulnerabilidad personal.
p) La falta de fiabilidad.
q) La falta de honradez.
r) La falta de lealtad.
s) Haber infringido reiteradamente las normas de seguridad establecidas o haber causado un daño grave a la organización por su incumplimiento.
t) El acceso no autorizado a sistemas informáticos o de telecomunicaciones, tanto en su vida profesional como en la privada, vulnerando las medidas de seguridad y la normativa de utilización de estos.
u) La realización de actividades reiteradas en beneficio propio, en perjuicio grave de terceros
v) La existencia de informes laborales que evidencien conductas conflictivas o acciones reivindicativas llevadas a cabo por medios ilegales.
w) La existencia de informes médicos que evidencien que el interesado padece una psicopatología con afectación al juicio de realidad o a la responsabilidad de sus actos.
x) La existencia de evidencias de grado inasumible de estulticia que pueda derivar en una vulnerabilidad personal.
y) La existencia de cualesquiera aspectos que pudieran ser utilizados como medio de coacción para obtener información.
z) Cualquier otra circunstancia que específicamente no esté contemplada en los criterios anteriores y que pueda suponer una vulnerabilidad.

7. CONCIENCIACIÓN E INSTRUCCIÓN DE SEGURIDAD DEL PERSONAL

7.1. Fases

La formación en materia de seguridad para los usuarios de información clasificada contempla dos fases, ambas necesarias y obligatorias:

– Concienciación de seguridad.
– Instrucción de seguridad.

7.2. Fase de concienciación de seguridad

Esta fase se encuadra dentro del proceso de solicitud de la HPS y es **requisito previo para su concesión**.

Todos los interesados para los que se solicita HPS deberán declarar por escrito, como requisito previo para su concesión, que entienden plenamente los siguientes conceptos:

- Las implicaciones que tiene el deber de reserva respecto a la información clasificada a la que accederán.
- Las consecuencias que las leyes contemplan en el caso de que la información clasificada llegue a manos no autorizadas, ya sea de forma intencionada o por negligencia, por incumplimiento de la normativa para su manejo.

La evidencia de la impartición de esta concienciación previa se plasma en dos documentos complementarios:

- La declaración de concienciación de seguridad del formulario de solicitud de HPS, firmada por el jefe de seguridad del organismo solicitante, como responsable de que se ha impartido la concienciación.
- La declaración personal del interesado (apartado 7 del formulario de declaración personal de seguridad), firmada por el propio interesado.

Para determinadas solicitudes de HPS de personal que ocupe puestos de relevancia en las organizaciones, la ONS podrá llevar a cabo la concienciación de seguridad como requisito necesario para la concesión de la HPS solicitada.

7.3. Fase de instrucción de seguridad

7.3.1. Concepto

Esta fase se encuadra como **requisito previo para el acceso** efectivo a la información clasificada.

La instrucción de seguridad se define como aquellas consignas y conocimientos que deben ser impartidos a cada individuo para mantenerle informado de las amenazas contra la seguridad, hacerle consciente de sus vulnerabilidades y concienciarle de sus responsabilidades para prevenir unas y otras. La instrucción en seguridad es un proceso continuo que no permite que el sujeto se estanque en sus conocimientos y que asegura que es consciente, en todo momento, de sus

responsabilidades. El sujeto debe saber qué es lo que puede hacer dentro de su organización y lo que no puede hacer, en relación con el manejo de la información clasificada.

El propósito de la instrucción de seguridad es sensibilizar al individuo sobre la necesidad de la seguridad, de la interiorización de los procedimientos para llevarla a efecto y de la asunción de sus responsabilidades personales. Consecuentemente el interesado, de forma consciente, adoptará las necesarias precauciones de seguridad como parte normal de sus cometidos.

Todas las personas autorizadas a acceder a información clasificada, o que tengan que manejarla, serán alertadas, al menos una vez al año, sobre los peligros que entrañan para la seguridad las conversaciones indiscretas con personas que no tengan necesidad de conocer, su relación con los medios de comunicación y la amenaza que representan las actividades de los servicios de inteligencia extranjeros. Las personas serán advertidas de su obligación de notificar inmediatamente, a las autoridades de seguridad pertinentes, cualquier aproximación o maniobra que consideren sospechosa o fuera de lo corriente.

En función del puesto ocupado y la correspondiente necesidad de conocer, la instrucción de seguridad podrá variar de unas personas a otras. Habrá en cada organización un plan de instrucción general, para todo el personal que pueda acceder a información clasificada, y otros planes particulares, para los casos concretos:

- Instrucción de seguridad en cada especialidad que se necesite poseer: CRIPTO, ATOMAL o SIGINT.
- Instrucción de seguridad sobre el plan de protección de cada zona de acceso restringido en que se precise trabajar.
- Instrucción de seguridad sobre la documentación de seguridad (especialmente el procedimiento operativo de seguridad – POS) de cada sistema de información y comunicaciones que se deba manejar.
- Instrucción de seguridad para jefes de seguridad de órganos de control.

7.3.2. Ámbito de aplicación y registro

Debe quedar evidencia objetiva escrita, en forma de certificado de instrucción o libro de registro, de que la instrucción de seguridad previa al acceso a información clasificada ha sido impartida por una persona cualificada. El responsable del órgano de control del que dependa la persona instruida o que provea el acceso, deberá mantener dichos registros permanentemente actualizados y disponibles para su inspección, debiendo conservarlos diez (10) años.

7.3.3. Responsabilidad de los jefes de seguridad en la instrucción

La instrucción de seguridad habrá de ser impartida por personal especializado en cuestiones de seguridad o bajo la supervisión de éste, orientada en todo momento por la ONS, especialmente mediante el uso del material didáctico elaborado por esta.

Los jefes de seguridad de los órganos de control son los responsables de que la formación se imparta y de guardar evidencia objetiva de que se ha llevado a efecto, así como de las instrucciones periódicas de recuerdo.

La instrucción de seguridad de los jefes de seguridad de los servicios de protección y subregistros principales (o servicios centrales de protección, en algunos casos), en el ámbito de competencias de la ANPIC, será realizada directamente por parte de la ONS, para asegurar el mejor desempeño de sus funciones.

Los jefes de seguridad instruidos por la ONS, serán a su vez responsables directos de impartir la instrucción de seguridad a sus suplentes en el cargo, así como a los jefes de seguridad de los órganos de control directamente subordinados, y estos a su vez de los subordinados, hasta llegar al último escalón.

La ONS podrá impartir los cursos de formación a los jefes de seguridad de cualquier órgano de control, pudiendo convocar cursos de formación colectivos, con carácter de obligada asistencia.

8. ACCESOS ESPECIALES A INFORMACIÓN CLASIFICADA

8.1. Acceso a información clasificada de grado «SECRETO o equivalente»

El acceso a información clasificada de grado «SECRETO o equivalente», será objeto de un control especial. Las personas que tengan «necesidad de conocer» esta clase de informaciones serán designadas por el mando o responsable de su organismo o entidad. Sus nombres se anotarán en la correspondiente lista de control, que habrá de crearse y mantenerse en los órganos de control de custodia de los documentos, denominándose:

- Para información nacional: Lista de Control SECRETO.
- Para información OTAN: Lista de Control COSMIC.
- Para información UE: Lista de Control TS-UE.

Cuando una persona cese en aquel puesto cuyas funciones requerían el acceso a información SECRETO, COSMIC TOP SECRET, o EU TOP SECRET, su nombre

se borrará de la lista de control correspondiente y se le instruirá de nuevo sobre su responsabilidad permanente en lo que concierne a la salvaguarda de la información a la que tuvo acceso.

El interesado deberá firmar un certificado, según formato en vigor (publicado en la página «web» de la ONS), por el que reconoce que es plenamente consciente de esta responsabilidad.

Los jefes de seguridad de los órganos de control responsables del acceso, garantizarán con su firma y sello en cada certificado, que el interesado ha recibido la instrucción correspondiente. Conservarán los registros firmados durante diez años.

8.2. Acceso a información clasificada de contenido CRIPTO, SIGINT Y ATOMAL

Los jefes de seguridad de los órganos de control garantizarán que aquellas personas para las que se solicita una autorización especial CRIPTO/CRYPTO, BOHEMIA/SIGINT, o ATOMAL, han sido instruidas convenientemente en dicha materia.

8.3. Guardias de seguridad

Los guardias de seguridad empleados en el transporte de información clasificada de grado «CONFIDENCIAL o equivalente» o superior, deberán contar con HPS del grado requerido de acuerdo con el grado de clasificación de la información que vayan a transportar.

Los guardias de seguridad que por razón de su trabajo puedan tener acceso a información clasificada, deberán contar con HPS del grado apropiado.

Cuando los guardias de seguridad pertenezcan a una empresa de servicios de seguridad, ésta deberá tener HSEM del grado apropiado.

8.4. Personal de mantenimiento y limpieza.

Sólo en casos particulares y siempre que se trate de personal fijo, se podrá solicitar HPS para personas que presten servicios de mantenimiento o limpieza de instalaciones. En concreto, será necesario cuando dichos trabajos se realicen en una zona de acceso restringido configurada como área clase I, en la que no es posible ocultar toda la información clasificada o puede producirse con cierta probabilidad un acceso fortuito a la misma.

En estos casos, el propio órgano de control del que depende la zona de acceso restringido, será el responsable de iniciar y tramitar el expediente de habilitación de seguridad de dicho personal. La empresa de servicios a la que pertenezca el personal no precisará disponer de una HSEM.

Al personal de mantenimiento de instalaciones y limpieza le será prohibida la entrada sin escolta en las zonas de acceso restringido, aun cuando cuente con HPS. Esta escolta no necesariamente tendrá que prestarse por personal específico de seguridad, sino que podrá ser personal de la organización autorizado para acceder a dicha zona quien les acompañe. Durante su permanencia en la zona, las informaciones clasificadas estarán protegidas de la observación y de la escucha pasiva o activa, no quedando nunca sin control el personal ajeno mientras se encuentre dentro de la zona.

9. ORGANIZACIÓN Y ASISTENCIA A ACTIVIDADES CLASIFICADAS

9.1. Asistencia a actividades clasificadas en el extranjero.

La asistencia a actividades en que se trate o maneje información clasificada de nivel «CONFIDENCIAL o equivalente» o superior, lleva asociado el requisito de que todos los asistentes estén en posesión de la correspondiente HPS.

Por ello, el acceso en el extranjero a determinados Cuarteles Generales, mandos, sedes, instalaciones, fábricas, etc., tanto en el ámbito de una organización internacional, como en cualquier país con el que exista un acuerdo para la protección de información clasificada que regule esta materia, y donde se celebren reuniones, cursos, seminarios, comités, grupos de trabajo o simplemente visitas, puede requerir de una HPS.

Con objeto de que la llegada de los representantes españoles sea conocida por los servicios de seguridad y, en su caso, tengan preparados los correspondientes pases de acceso, la ONS, en nombre de la ANPIC, comunicará a estos servicios, con la suficiente antelación, por los cauces y con las formalidades reglamentarios, la identidad de los desplazados, su grado de HPS, la identificación de la actividad en la que van a participar, las fechas de comienzo y finalización y el lugar concreto donde se desarrolle.

Para ello remitirá una certificación de HPS de las personas que se desplazan, que podrá adoptar un formato específico en función del ámbito y destino, como por ejemplo «*Certificate for Assistance*» (certificado de asistencia) a actividades oficiales, o «*Request for Visit*» (RFV) en el ámbito industrial, o cualquier otro que pudiera estar reglamentado en la actualidad o en el futuro.

A estos efectos, y con carácter general, los jefes de seguridad de los servicios de protección de los que dependan los organismos o empresas que vayan a enviar representantes a una reunión, comité, curso, visita, etc., deberán comunicárselo a la ONS con un mínimo de diez (10) días hábiles de antelación a la fecha de inicio de la actividad. En determinado ámbito o contexto, en normativa específica, podrá establecerse un plazo de tiempo mayor.

En ciertos casos, para ámbitos, destinos y condiciones expresamente indicados por escrito, la ONS, en nombre de la ANPIC, podrá autorizar de oficio a determinados jefes de seguridad de servicio de protección a remitir directamente estas certificaciones, incluyendo normalmente como destinatario de información a la ONS, a efectos de control del proceso.

Análogamente, en el ámbito de la seguridad industrial, la ONS podrá delegar, en determinadas áreas de seguridad de la información clasificada en el ámbito industrial, todas o parte de estas competencias.

Cuando no se conozca con precisión el procedimiento para el envío de la certificación de HPS requerida, será aconsejable que los interesados lleven consigo un certificado de HPS, emitido al efecto con los criterios establecidos en el **apartado 5.4.8.2**, que acredite su titularidad como habilitado.

9.2. Organización de actividades clasificadas en ESPAÑA

La organización en España de cualquier actividad internacional, incluidas visitas, en la que se maneje información clasificada de organizaciones internacionales u otros países con acuerdo de seguridad, con independencia de su grado de clasificación, requiere su comunicación previa a la ONS, u otro órgano en que pueda haber delegado, adjuntando la lista de participantes, al objeto de conocer su celebración y controlar las certificaciones de HPS que se reciban.

Es responsabilidad de quien organiza la actividad el solicitar de los asistentes la comunicación de su grado de HPS y vigencia. Con carácter general esta comunicación, para personal extranjero, se tramitará, con al menos diez (10) días hábiles de antelación, a través de la ANS de su país de origen, a la ANPIC, o por otro cauce que específicamente esté establecido y autorizado por las Autoridades Nacionales concernidas.

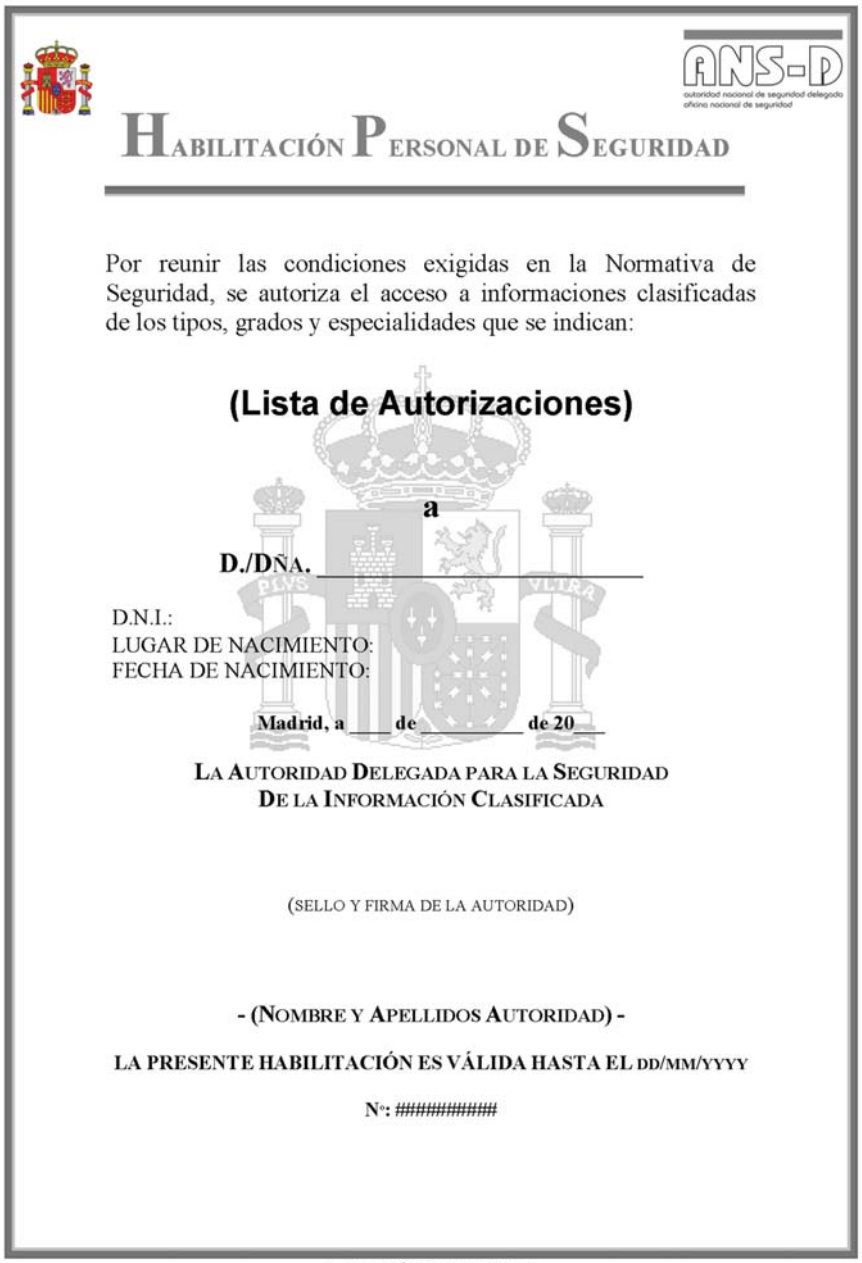
Para asistentes de nacionalidad española, la comunicación se podrá realizar directamente entre órganos de control, no siendo preciso informar de ello a la ONS.

Para cualquier reunión de carácter clasificado que se organice por parte de algún organismo, unidad o empresa, es competencia del subregistro principal su control, por lo que deberá asegurar y verificar que se da cumplimiento a los trámites que se indican en los siguientes puntos:

- Se comunica a los participantes en la reunión la obligación de notificar previamente, con las formalidades reglamentarias y a través de los canales adecuados, el hecho de la asistencia y el grado de HPS de que se dispone, debidamente acreditado, con la antelación suficiente para poder llevar a efecto el oportuno control del personal asistente.
- Se organiza la seguridad del evento, en función del grado de clasificación del mismo, nombrando un jefe de seguridad (preferentemente un jefe de seguridad de un órgano de control), responsable de que se adopten las medidas de protección requeridas (control de accesos, área de registro y custodia de la información clasificada, control de pases de asistencia, control de documentación, control de reproducciones y destrucciones de documentos, retirada de teléfonos móviles, estudio del local y definir si es preciso constituir un área técnicamente segura, «zoning», medidas «tempest», insonorización, etcétera), al objeto de evitar fugas de información.
- Para actividades internacionales donde se maneje información clasificada de grado «equivalente a RESERVADO» o superior, deberá informarse a la ONS de las medidas de seguridad finalmente adoptadas y del responsable de seguridad del evento.

ANEXO I A LA NS-02. MODELO DE HABILITACIÓN PERSONAL DE SEGURIDAD (HPS)

DIFUSIÓN LIMITADA



HABILITACIÓN PERSONAL DE SEGURIDAD

Por reunir las condiciones exigidas en la Normativa de Seguridad, se autoriza el acceso a informaciones clasificadas de los tipos, grados y especialidades que se indican:

(Lista de Autorizaciones)

a

D./DÑA. _____

D.N.I.:
LUGAR DE NACIMIENTO:
FECHA DE NACIMIENTO:

Madrid, a ___ de _____ de 20__

LA AUTORIDAD DELEGADA PARA LA SEGURIDAD DE LA INFORMACIÓN CLASIFICADA

(SELLO Y FIRMA DE LA AUTORIDAD)

- (NOMBRE Y APELLIDOS AUTORIDAD) -

LA PRESENTE HABILITACIÓN ES VÁLIDA HASTA EL DD/MM/YYYY

Nº: ##########

Certificado HPS – 200/11

DIFUSIÓN LIMITADA

C/ Argentona, 30
28023 MADRID
TEL: 91 3725000 FAX: 91 3725808
nsa-sp@areatec.com

ANEXO II A LA NS-02. MODELO DE CERTIFICADO DE HPS

CERTIFICADO DE HABILITACIÓN PERSONAL DE SEGURIDAD

EMITIDO POR:

DIRECCIÓN POSTAL:

-

-

1. POR EL PRESENTE SE CERTIFICA QUE:

Nombre y apellidos:

Fecha de nacimiento:

Lugar de nacimiento:

Nacionalidad:

Empleado en:

Poseedor de Pasaporte/DNI número:

Emitido en: **ESPAÑA** Fecha de expiración:

Rango Militar y número (si es de aplicación):

Es titular de una habilitación de seguridad, habiendo sido instruido, emitida por el Gobierno de **ESPAÑA** conforme a las leyes y reglamentos nacionales y a los reglamentos de seguridad de OTAN, incluido el Anexo de Seguridad C-M(64)39 caso de información ATOMAL, si fuera de aplicación, y puede acceder a información clasificada hasta el grado incluido:

2. OBJETO DEL CERTIFICADO Y DURACIÓN DE LA VISITA (si aplicable):
"Acceso a información clasificada debido a sus obligaciones en:

"

3. LA VALIDEZ DE ESTE CERTIFICADO EXPIRARÁ EL DÍA:

Firmado:
Cargo:.

DATOS DE CONTACTO:
- Teléfono.:
- Correo electrónico:
- Fax:

(Firma y sello oficial)

Lugar y Fecha de Expedición: **, a**

Nº: C/

Certificado CHS-300/13

MODELO DE CERTIFICADO DE HPS (REVERSO)

CERTIFICATE OF PERSONNEL SECURITY CLEARANCE

ISSUED BY:

ADDRESS:
-
-

1. CERTIFICATION IS HEREBY GIVEN THAT:

Full Name:

Date of Birth:

Place of Birth:

Nationality:

Where employed:

Holder of Passport/Identity Card ID No.:

Issued at: **ESPAÑA** Expiry Date:

Military Rank and Number (where applicable):

Has been granted a security clearance and briefed accordingly, issued by the Government of **SPAIN**, in accordance with national laws and regulations, and current NATO security regulations including the Security Annex to C-M(64)39 in the case of ATOMAL information (where applicable), and may have access to information classified up to and including:

2. PURPOSE OF THE CERTIFICATE AND DURATION OF VISIT (if applicable):
"Access to classified information due to his/her duties in:

"

3. THE VALIDITY OF THIS CERTIFICATE WILL EXPIRE NOT LATER THAN:

Signed:
Title:

CONTACT DETAILS:
- Phone No.:
- E-mail:
- Fax No.:

(Official government stamp)

Place and Date of Issue: ,

Nº: C/

Certificado CHS-300/13

NORMA NS/03

SEGURIDAD FÍSICA

1. INTRODUCCIÓN

La seguridad física es la condición que se alcanza en las instalaciones cuando se aplica a estas 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.

Por acceso se entenderá no solo la entrada física a la instalación, sino también la escucha u observación externas.

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:

- Disuadir e 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 y 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 disuasión, 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, contribuirá a reducir a un 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, en tiempo oportuno, 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, en los propios paramentos y accesos, así como dentro de ella, 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 interior.
- 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. 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 ONS 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 hacerlas frente.

5. ACREDITACIÓN DE UNA ZONA DE ACCESO RESTRINGIDO

La ONS o, por delegación expresa de aquella, 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 formato en vigor de «certificado de acreditación de locales», publicado en la página «web» de la ONS), de la capacidad de un determinado local, edificio, oficina, habitación u otra área para que en él 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.

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:

- **Informe de instalaciones**: 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.
- **Procedimientos 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 informe de instalaciones), 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.

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 y al riesgo evaluado, 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.

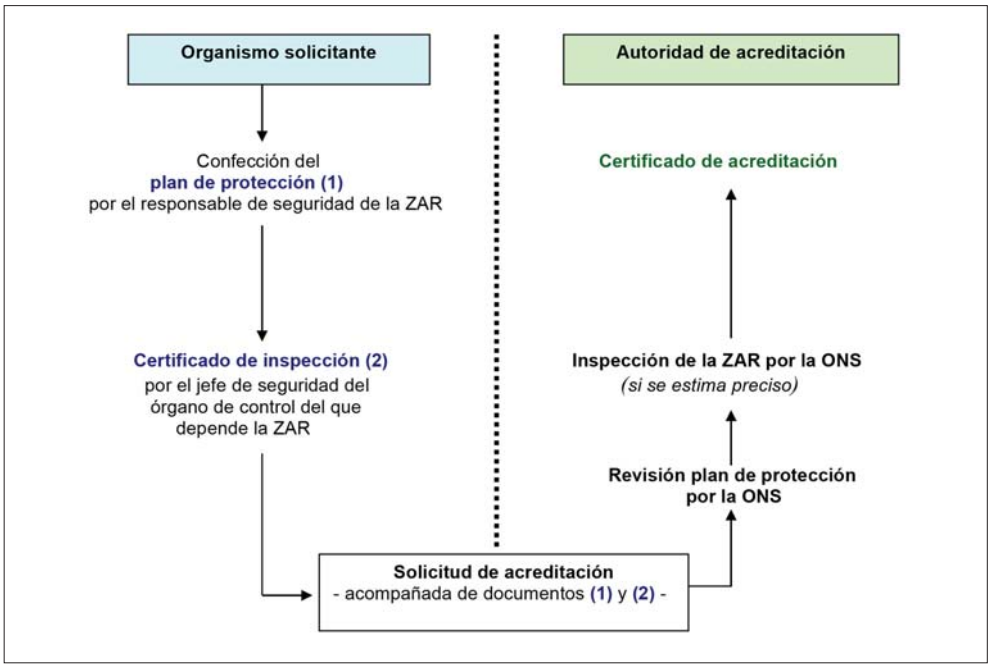
– Constituir un documento básico en los relevos de responsabilidades de seguridad, al definir y asegurar el cumplimiento de unas mismas medidas de seguridad, con independencia del personal destinado en cada momento.
– Constituir la guía de referencia para las inspecciones tanto de apertura como de correcto 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 la afecten (especialmente en cuanto a la evaluación del riesgo existente). El certificado de acreditación sólo tendrá validez si el plan de protección en el que está basado se encuentra debidamente actualizado.

En el documento de la ONS denominado «OR-ASIP-01-01. Orientaciones para el plan de protección de una zona de acceso restringido», se describe el modelo a seguir para la confección del plan de protección.

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 I 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 ONS.

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 su fecha de caducidad. **Si con antelación a la fecha de caducidad se hubiera recibido en la ONS, 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.

6. 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.

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

El responsable de seguridad de una zona de acceso restringido será el encargado de:

- Confeccionar el plan de protección.
- Establecer un procedimiento de control de visitas.
- Realizar 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 II 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 III de este documento.

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 de la ONS denominado «OR-ASIP-01-02. Orientaciones para la constitución de zonas de acceso restringido», se describen los estándares de

medidas de seguridad para la protección de zonas donde de almacena o maneja información clasificada, aprobados por la ANPIC, a aplicar según el grado de clasificación y otras condiciones que sea preciso atender.

En otro documento de la ONS denominado «OR-ASIP-04-01. Orientaciones para el manejo de información clasificada con grado de DIFUSIÓN LIMITADA», se incluyen 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 su parte superior como son: 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 ellas.

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 estas 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

El empleo de personas para control de accesos permite una mayor adaptabilidad al riesgo y flexibilidad de actuación.

Los guardias de seguridad, al realizar también una labor de protección de la zona de seguridad, deberán contar con una HPS del grado apropiado a la información clasificada manejada en la zona, cuando en sus cometidos sea preciso el acceso a su interior. En este caso, 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. 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 ingle-

sa 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.

En inmuebles, urbanizaciones, polígonos o cualquier tipo similar de infraestructura, que no dispongan de un servicio de vigilancia propio en el entorno de sus instalaciones, se contratará un servicio de vigilancia externo, 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 ANPIC, se deberán mantener cerrados cuando no estén bajo la supervisión de una persona autorizada.

No se almacenarán en ellos 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 ellas.
- Cuando personas no autorizadas hayan podido tener acceso a ellas, incluido el personal de las empresas mantenedoras.

Se llevará un libro de registro de los cambios realizados.

Deberán ocultarse la identificación del fabricante, el 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 las zonas de acceso restringido 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. Se indicará el número de serie y marca de cada llave, 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, ac-

cesible 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 II), 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 SISTEMAS DE INFORMACIÓN Y COMUNICACIONES

En instalaciones donde la información clasificada es visualizada, almacenada, procesada o transmitida (en adelante, 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.

ANEXO I A LA NS/03. 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 ONS, sobre la base de la normativa de seguridad en vigor.

En ....., a .. de .....de 20….

El Jefe de Seguridad

Fdo: .....

ANEXO II A LA NS/03. LISTA DE PERSONAL AUTORIZADO

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

Identificación de la ZAR:

– .....

– .....

– .....

– .....

– .....

– .....

– .....

– .....

– .....

– .....

– .....

– .....

– .....

ANEXO III A LA NS/03. 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:

NORMA NS/04

SEGURIDAD DE LA INFORMACIÓN

1. CONCEPTOS

1.1. Definición

La seguridad de la información es la condición que se alcanza cuando se aplica un conjunto de medidas y procedimientos establecidos para el correcto manejo y control de la información, en todo su ciclo de vida, así como para prevenir y detectar los posibles comprometimientos que puedan afectar a su confidencialidad, integridad o disponibilidad.

Por manejo de la información se entenderá el almacenamiento, custodia, elaboración, proceso, utilización, presentación, reproducción, acceso, transporte, destrucción o transmisión de aquella, sea cual fuere el método empleado.

1.2. Propiedad de la información

La información tendrá un originador, bajo cuya autoridad o tutela la información es producida, dentro del ámbito de una organización internacional, estado u organismo subordinado. El originador define quién ostenta la propiedad inicial de la información clasificada.

La información tendrá un propietario claramente establecido que, en este caso, es la organización internacional, estado u organismo dueño de la información, es decir, que ostenta su propiedad. En último extremo, si no es posible determinarlo, vendrá determinado por la propia marca de clasificación de origen.

El propietario de la información es el que define las reglas por las que se rige su manejo, en línea con la normativa aplicable, y define los criterios para que pueda producirse una transferencia de la propiedad, si admite esa posibilidad.

La propiedad de la información puede ser transferida. No debe confundirse con la distribución o la cesión de información, que no implica un cambio de propietario de la misma, sino únicamente de custodio. En este sentido, cuando España recibe por ejemplo información OTAN, con la marca NATO estampillada en su clasificación de seguridad (por ejemplo, NATO SECRET), la propiedad de dicha información continúa siendo de OTAN, aunque su custodia y usuarios serán de España.

1.3. Taxonomía de la información clasificada

1.3.1. Información

Información es todo conocimiento que puede ser comunicado, presentado o almacenado en cualquier forma.

1.3.2. Material

El concepto material engloba cualquier documentación, pieza, equipo, sustancia, programa, desarrollo, armamento, sistema o similar, fabricado o en proceso de fabricación, que es portador de una información o constituye una información en sí mismo.

1.3.3. Información sensible

Información sensible es cualquier información o material respecto del cual se decida que requiere protección contra su divulgación o acceso no autorizados, con independencia de que se le haya asignado o no una clasificación de seguridad.

1.3.4. Información clasificada

Información clasificada es cualquier información o material respecto del cual se decida que requiere protección contra su divulgación o acceso no autorizados, por el daño o riesgo que esto supondría a los intereses del Estado, y al que se ha asignado, con las formalidades y requisitos previstos en la legislación, una clasificación de seguridad.

Toda información clasificada es información sensible, pero no toda la información sensible es información clasificada.

1.3.5. Documentación clasificada

Documentación clasificada es cualquier soporte que contenga información clasificada registrada, en cualquier formato físico (escrito, impreso, cinta, fotografía, mapa, dibujo, esquema, nota, soporte informático, óptico o vídeo, etc.). La más tradicional es en formato papel, aunque cada día se hace un uso más extensivo de los soportes informáticos.

1.3.6. Material clasificado

El concepto material clasificado engloba cualquier material cuyo contenido o conocimiento necesite protección frente a difusión o acceso no autorizados, por el daño o riesgo que esto supondría a los intereses del Estado, y al que se ha asignado, con las formalidades y requisitos previstos en la legislación, una clasificación de seguridad. Es un concepto más amplio que el de documentación clasificada, pero menos que el de información clasificada, dado que no incluye, por ejemplo, a la información clasificada en las personas (almacenada en la mente o comunicada verbalmente).

1.3.7. Materias clasificadas

Definidas en la Ley 9/68, de 5 de abril, modificada por la Ley 48/78, de 7 de octubre, sobre Secretos Oficiales (en adelante, Ley de Secretos Oficiales), como los asuntos, actos, documentos, informaciones, datos y objetos cuyo conocimiento por personas no autorizadas pueda dañar o poner en riesgo la seguridad y defensa del Estado, y que se califican en las categorías de SECRETO y RESERVADO, en atención al grado de protección que requieren, según se definen en el anexo I.

Este concepto se correspondería con el de información clasificada de grado RESERVADO o superior.

1.3.8. Materias objeto de reserva interna

Con precedente de uso en la «Política de Seguridad de la Información del Ministerio de Defensa», en los acuerdos para la protección de la información clasificada

con otros países y en políticas de seguridad de organizaciones internacionales, se definen como los asuntos, actos, documentos, informaciones, datos y objetos cuyo conocimiento por personas no autorizadas pueda afectar a la seguridad del Estado, amenazar sus intereses o dificultar el cumplimiento de su misión. Se clasifican en las categorías de CONFIDENCIAL y DIFUSIÓN LIMITADA, en atención al grado de protección que requieren, según se definen en el anexo I.

Este concepto se correspondería con el de información clasificada de grado CONFIDENCIAL o inferior.

1.4. Principio de la garantía de la información

La información será protegida mediante la aplicación del principio de la **garantía de la información** (en inglés: «*Information Assurance*»), que se describe como el conjunto de medidas a aplicar para alcanzar un nivel dado de confianza en la confidencialidad, integridad, disponibilidad, no repudio y autenticación de la información durante su almacenamiento, proceso o transmisión.

1.5. Custodia de la información clasificada

La información clasificada, a lo largo de todo su ciclo de vida, siempre estará asignada a un responsable (órgano o persona) de su custodia, quien podrá variar, pero nunca dejar de existir. Dicho custodio manejará y cederá la información bajo su custodia conforme a la normativa establecida por el propietario de la información, o acordada con el mismo.

Cuando el custodio sea también quien almacena la información, podrá recibir el nombre de **depositario**.

1.6. Usuario de la información clasificada

El usuario es la persona que, en el cumplimiento de sus cometidos oficiales, tiene que acceder a la información clasificada y, en consecuencia, está debidamente autorizado por su organismo o entidad y cumple los requisitos de acceso.

La condición de usuario no implica ningún derecho o prerrogativa especial sobre la propiedad de la información clasificada. El usuario tendrá la custodia de la información clasificada, en tanto esté asignada a su cargo.

El usuario asume las siguientes responsabilidades:

- Dar la adecuada protección a la información clasificada a su cargo.
- Conocer y cumplir la normativa nacional y las normas específicas de seguridad de su organismo o entidad, referentes a la protección de la información clasificada.
- Mantener la debida reserva ante terceros sobre su condición de titular de una habilitación de seguridad.
- No manejar información clasificada al margen de los canales oficialmente establecidos (estructura nacional de protección).
- Cooperar con el jefe de seguridad del órgano de control de su organismo o entidad en todo aquello que se relacione con la seguridad de la información clasificada en su puesto de trabajo, en su entorno laboral y en las actividades y foros en que intervenga.
- Mantener la reserva sobre la información clasificada a la que tuvo acceso, incluso una vez haya caducado su habilitación de seguridad.

1.7. Acceso a la información clasificada

El acceso de un usuario a la información clasificada se realizará conforme a las condiciones que se indican en la norma NS/02 de la ANPIC, en su **apartado 3**, donde se definen, y que básicamente se resumen en que se podrá autorizar dicho acceso si el usuario:

- tiene concedida una habilitación personal de seguridad (HPS) adecuada, si el acceso es a información clasificada de grado «CONFIDENCIAL o equivalente» o superior,
- se ha determinado su «necesidad de conocer», y
- ha recibido la instrucción de seguridad preceptiva.

En cualquier caso, el jefe o responsable del organismo o entidad tiene la potestad de no autorizar el acceso, aun cuando se den las condiciones necesarias anteriores, si estima o aprecia que pueda existir un riesgo no aceptable para la seguridad de la información.

Las personas que sólo necesiten acceder a información con clasificación «DIFUSIÓN LIMITADA o equivalente» deberán haber sido instruidas en sus responsabilidades de seguridad y habrán de tener «necesidad de conocer». No se necesitará HPS para acceder a la información con clasificación de dicho grado.

1.8. Principio de la responsabilidad de compartir

La información es un recurso corporativo, un activo de gran valor para la organización. El objeto de la información es aportar el conocimiento necesario para poder actuar con seguridad, eficacia y oportunidad, tanto en el cumplimiento de la misión como en el proceso de toma de decisiones o consultas. Existe una responsabilidad individual y colectiva de que la información esté accesible, disponible y utilizable para aquellas entidades que requieran dicha información para acometer sus tareas y servicios oficiales. Ello constituye el principio de la responsabilidad de compartir (en inglés: «*Responsibility to Share*»), que estará limitado en su alcance por el cumplimiento previo de las condiciones de acceso, especialmente la **necesidad de conocer** (en inglés: «*Need to Know*»).

La responsabilidad de compartir lleva implícita una difusión mínima de la información; ésta sólo se difundirá a quien la precise para cumplir con sus cometidos oficiales, al objeto de evitar las duplicaciones o difusiones innecesarias, que suponen una vulneración de la seguridad.

2. ALCANCE

En esta norma se tratará exclusivamente de la información clasificada, quedando la no clasificada regulada por la normativa específica del organismo internacional o país originador o propietario, o los acuerdos adoptados con estos.

En concreto, la presente norma es de aplicación a:

a) Información clasificada con marca de propiedad de las organizaciones internacionales en las que el Reino de España es parte, en virtud de un tratado.
b) Información clasificada recibida en España al amparo de un acuerdo para la protección de información clasificada suscrito con otro estado.
c) Información clasificada nacional de España.

La información clasificada entregada a contratistas con motivo de su participación en actividades, programas y proyectos clasificados, especialmente en el ámbito internacional, podrán requerir medidas adicionales de seguridad, que se reflejarán en las instrucciones de seguridad específicas para cada programa o contrato.

La información clasificada manejada en sistemas de información y comunicaciones requiere medidas adicionales de seguridad, por lo que, aparte de lo estable-

cido en esta norma, se fijan otras medidas específicas en la norma NS/05 de la ANPIC, sobre seguridad en los sistemas de información y comunicaciones.

Por la especial sensibilidad del material de cifra, éste requerirá la aplicación de medidas adicionales de seguridad más exigentes y circulará por canales específicos de distribución y custodia. En este sentido, estará sujeta a requisitos adicionales establecidos por las correspondientes autoridades de control y órganos de distribución del material de cifra.

La información clasificada de OTAN, de categoría especial ATOMAL, requiere medidas adicionales de seguridad, que se tratarán conforme a la normativa específica de OTAN existente al respecto.

Por último, la información relativa a inteligencia de señales (conocida por su sigla inglesa, SIGINT), estará adicionalmente sujeta a los requisitos establecidos por las correspondientes autoridades SIGINT que sean competentes, que podrán dictar normas propias específicas, pero en ningún caso contrarias a las establecidas en la normativa de seguridad.

3. CLASIFICACIÓN DE SEGURIDAD DE LA INFORMACIÓN

3.1. Clasificación de la información

3.1.1. Conceptos generales

Por **clasificación** se entiende el acto formal por el cual la autoridad de clasificación, u órgano legislativo, asigna a una información un grado de clasificación en atención al riesgo que supone su revelación no autorizada para la seguridad y defensa del Estado o sus intereses, con la finalidad de protegerla.

En este sentido, según se determina en el artículo 2 de la Ley de Secretos Oficiales, tendrán carácter de información clasificada, sin necesidad de previa clasificación por una autoridad de clasificación, las materias que así sean declaradas por Ley.

La clasificación se puede aplicar sobre un asunto o tema más o menos general, o sobre una documentación o material no documental concreto. En cualquier caso, la autoridad de clasificación, u órgano legislativo, deberá sopesar, asesorado por personal experto en el tema, las implicaciones que dicha clasificación conlleva respecto a la complejidad del manejo y protección de la información una vez clasificada, en aras de evitar por todos los medios la posible sobreclasificación de la información.

Una vez aprobado por la autoridad u órgano legislativo correspondiente, el grado de clasificación de la información no podrá cambiarse, reducirse ni eliminarse sin un nuevo acto formal por parte de dicha autoridad u órgano, salvo que en el acto de su clasificación inicial se indique que el grado de clasificación de la información puede reducirse o eliminarse en cierta fecha o ante ciertos eventos.

Es prerrogativa del propietario de la información proponer a la autoridad correspondiente la modificación de la clasificación de seguridad durante su ciclo de vida.

Algunas organizaciones y países contemplan una gradación de sensibilidad en materias que, sin ser llegar a ser clasificadas, necesitan un control en su difusión. Esta información se rige por normativas específicas que están fuera del objeto de la presente norma.

Las clasificaciones de seguridad y el marcado de la información clasificada, en cada caso se aplicarán de conformidad con la normativa de seguridad que le sea de aplicación y en las condiciones que en esta se establezcan.

Reclasificación es el acto formal por el cual la autoridad de clasificación u órgano legislativo modifica el grado de clasificación de una información clasificada.

Desclasificación es el acto formal por el cual la autoridad de clasificación u órgano legislativo retira todo grado de clasificación asignado a una información.

3.1.2. Grados de clasificación de seguridad

Las clasificaciones de seguridad, internacionalmente, se establecen en cuatro grados fundamentales, con una equivalencia en la mayoría de los estados y organizaciones internacionales de ámbito occidental. En el anexo II se incluye un cuadro de equivalencias de grados de clasificación de diferentes organizaciones internacionales y estados, con los que España mantiene relación.

El originador de la información es responsable de aplicar los criterios de clasificación definidos en una norma de ley, directiva o diligencia/guía de clasificación, al proponer la clasificación de seguridad de una información.

Una vez asignado el grado de clasificación a una determinada información, se **marcará** sobre el soporte de la misma, de forma adecuada y claramente visible, y se registrará en un órgano de control competente para el grado de clasificación.

Los grados de clasificación nacional en España, de mayor a menor, son los siguientes:

- **SECRETO (S)** [1]
- **RESERVADO (R)** [1]
- **CONFIDENCIAL (C)** [2]
- **DIFUSIÓN LIMITADA (DL)** [2]

Su significado y criterios de uso se definen en el anexo I.

3.1.3. Capacidad para clasificar

Autoridad de clasificación

Con independencia de la facultad que confiere la Ley de Secretos Oficiales de poder declarar por ley una información como clasificada, la capacidad para clasificar es exclusiva de las autoridades de clasificación, pudiendo únicamente delegarse dicha capacidad cuando la normativa de seguridad aplicable así lo contemple.

Ámbito nacional

En el ámbito nacional, la facultad para clasificar de SECRETO y RESERVADO corresponde, por ley, al Consejo de Ministros y a la extinta Junta de Jefes de Estado Mayor, **no pudiendo ser transferida ni delegada**. La Ley de Secretos Oficiales no contempla grados de clasificación inferiores, por lo que éstos se definen y rigen por normativa de desarrollo de dicha Ley.

Tendrán facultad para clasificar de CONFIDENCIAL o DIFUSIÓN LIMITADA las siguientes autoridades en el ámbito de su competencia, **pudiendo delegar** oficialmente dicha atribución:

a) Presidente y Vicepresidente del Gobierno
b) Los Ministros, Secretarios de Estado y Subsecretarios en sus respectivos Departamentos.
c) Jefe del Estado Mayor de la Defensa.

---

[1] Definidos en la Ley de Secretos Oficiales (LSO). Se transcriben en el Anexo I.

[2] Definidos en esta norma NS/04 de la Autoridad Nacional, así como en Políticas de Seguridad de Organizaciones Internacionales y Acuerdos para Protección de la información clasificada, y en determinados Departamentos Ministeriales (MINISDEF) como desarrollo de la LSO. Se definen en el Anexo I.

d) Jefe del Estado Mayor del Ejército.
e) Almirante Jefe del Estado Mayor de la Armada.
f) Jefe del Estado Mayor del Ejército del Aire.
g) Presidente del Consejo de Seguridad Nuclear.

Las autoridades de clasificación tendrán las siguientes atribuciones:

a) Aprobar o desestimar las propuestas de clasificación.
b) Emitir la diligencia de clasificación.
c) Modificar el grado de clasificación de la información o su plazo de vigencia.
d) Disponer las directivas de clasificación.
e) Delegar la facultad de clasificación, si está autorizado.

Ámbito de organizaciones internacionales

Las organizaciones internacionales establecen en su normativa la necesidad de seguir unos criterios restrictivos al asignar esta función y delegan la responsabilidad de designar a las autoridades de clasificación en los responsables de los componentes militares y agencias (caso de OTAN), o en los directores generales (caso del Consejo de la UE, Comisión Europea o Agencia Espacial Europea), y en los propios estados miembros. No establecen diferencias en este sentido en cuanto al grado de clasificación.

En este sentido, en España como estado miembro, las autoridades de clasificación para estos ámbitos han de ser las mismas que las establecidas en el ámbito nacional para cada grado de clasificación equivalente, y con las mismas prerrogativas de delegación.

3.1.4. Procedimiento nacional de clasificación, reclasificación y desclasificación

Toda información que se considere que deba ser protegida de revelación no autorizada y de la que no exista una norma de ley, directiva o diligencia, previa, que la clasifique, deberá someterse a un proceso de clasificación mediante la confección de la correspondiente **propuesta de clasificación**, que será presentada a la autoridad de clasificación, al objeto de obtener su aprobación mediante la emisión de la correspondiente **diligencia de clasificación**.

La **propuesta de clasificación** es el documento por el que se somete a aprobación por la autoridad de clasificación correspondiente, la asignación de un grado de clasificación a informaciones individuales o agrupadas en un conjunto, así como su vigencia. Puede ir acompañada de una guía de clasificación.

La **diligencia de clasificación** es el documento por el que se certifica la aprobación, por la autoridad de clasificación, de una propuesta de clasificación y se definen las condiciones de aplicación.

La **guía de clasificación** es el documento que enumera y describe los elementos clasificados de un asunto, contrato o programa clasificado, con especificación de los grados de clasificación asignados a cada uno de ellos. Recoge los datos relevantes de la información clasificada (los grados de clasificación asignados, las vigencias de las clasificaciones, las autoridades facultadas que la han clasificado, etc.), y sirve de referencia para el marcado de los documentos.

La **directiva de clasificación** es el documento mediante el cual la autoridad de clasificación asigna un grado de clasificación a la información que, por su naturaleza, y a juicio de la citada autoridad, no requiera la elaboración de la propuesta de clasificación, constituyéndose formalmente en diligencia de clasificación.

El proceso para la clasificación de una información, cuando no existe una norma de ley, directiva o diligencia, previa, que la clasifique, se compone básicamente de los siguientes pasos:

a) Decisión del ámbito.
b) Elaboración de la guía de clasificación, cuando así se requiera.
c) Preparación de la propuesta de clasificación.
d) Elevación de la propuesta de clasificación a la autoridad de clasificación.
e) Formalización de la diligencia de clasificación.
f) Anotación de la nueva diligencia en el **registro de diligencias de clasificación**.
g) Anotación de cada material clasificado concreto en el **libro de registro de información clasificada** y marcado.

Al objeto de facilitar el proceso de clasificación, las autoridades facultadas para clasificar pueden aprobar directivas de clasificación, que son documentos en los que se establecen, con carácter más o menos detallado, determinados asuntos, materias o elementos que por su especial naturaleza, contenido, o simplemente repetición, se clasifican previamente, de forma que cualquier información que incluya, o trate, dichos asuntos, materias o elementos deberá clasificarse con el grado indicado. Las directivas de clasificación aprobadas se anotarán en el **registro de directivas de clasificación**.

Cuanto más alto sea el grado de clasificación que se quiera dar a una determinada información, más específica deberá ser una directiva de clasificación en su definición, para evitar la sobre-clasificación que suele derivarse de la generalización. Por ello

se desaconseja la promulgación de directivas de clasificación generalistas para los grados superiores. Para grado «SECRETO o equivalente», la aplicación más adecuada de la directiva de clasificación es la que refiere a informaciones concretas, como pueden ser un documento, un elemento de un equipo o una instalación concreta.

Cuando exista una directiva de clasificación, o guía de clasificación ya aprobada en una anterior diligencia de clasificación, que sea pertinente a la información que se propone para su clasificación, el procedimiento se simplifica, bastando con su anotación en el libro de registro de información clasificada y su marcado.

Toda información clasificada deberá llevar su marca de grado de clasificación estampillada o unida a la misma, salvo imposibilidad física u operativa derivada de las características del material o del uso previsto.

Toda información registrable que se marque como clasificada, sólo adquirirá formalmente dicho carácter cuando esté correctamente anotada en un registro, para su distribución posterior.

No obstante, los borradores, copias previas, anotaciones, grabaciones en soportes u otra información adicional que se puedan haber generado previamente para obtener la versión final registrable, tendrán también la consideración de información clasificada, y deberán ser destruidos en plazo breve con procedimientos aprobados para el grado de clasificación de que se trate. En tanto no se produzca su destrucción, se les dará la protección adecuada conforme a su grado de clasificación, aunque no estén marcados.

El jefe de seguridad del órgano de control es responsable de verificar que la información para registrar corresponde a algunos de los criterios o elementos contenidos en una norma de ley, directiva de clasificación o en una diligencia de clasificación. Si no fuera así, deberá realizarse una propuesta de clasificación y elevarla a la autoridad de clasificación que corresponda.

Cuando el grado de clasificación sea «RESERVADO o equivalente» o superior, se añadirá la referencia de la norma legal, guía, diligencia o directiva, de clasificación por la que se clasifica dicha información. Para otros grados de clasificación inferiores es recomendable también la inclusión de esta referencia, especialmente para grado «CONFIDENCIAL o equivalente», aunque no obligatoria si son claros los motivos que avalan la clasificación.

La información clasificada originada en España se constituirá como información clasificada nacional y, por tanto, se propondrá su clasificación conforme a los grados de clasificación establecidos en España, con independencia del destinatario.

De este modo se indica de forma explícita que España es la propietaria y originadora de esa información clasificada.

Sólo se harán propuestas de uso de marcas de clasificación no nacionales cuando se elabore información clasificada en el marco de una operación, programa, proyecto, u otra colaboración específica. En este caso, la información deberá elaborarse conforme a los requisitos establecidos en el acuerdo para la protección de información clasificada aplicable, en cuanto a idiomas oficiales admitidos, criterios de marcado, identificación de documentos, paginado, etc.

Los mensajes o escritos de remisión, que acompañan a documentos anexos clasificados con marcas de clasificación no nacionales que tienen su entidad propia, pueden ir en idioma diferente, no debiendo contener información clasificada. Aunque lleven la clasificación que les corresponda por agregación, dicha marca incluirá una indicación de que el citado escrito no constituye información clasificada cuando se separe de los anexos.

El procedimiento de clasificación nacional establecerá los criterios para la reclasificación y desclasificación de la información. La autoridad de clasificación podrá señalar en la diligencia de clasificación el tiempo de vigencia del grado de clasificación que ha otorgado a la información, o las circunstancias que lo condicionen, así como mantener o, en cualquier momento, modificar dicho grado o desclasificar la información, con una nueva diligencia.

3.1.5. Registros de clasificaciones

El procedimiento de clasificación nacional impondrá la obligación de la anotación, en un registro nacional único de clasificaciones, de todas las decisiones de ámbito nacional adoptadas, en acuerdos de Consejo de Ministros, Junta de Jefes de Estado Mayor o por ley, respecto a la clasificación de la información.

Por su parte, los servicios de protección de información clasificada de cada departamento ministerial y Fuerzas Armadas, serán responsables de mantener, dentro de su ámbito y para sus autoridades de clasificación:

a) El registro de directivas de clasificación, y
b) el registro de diligencias de clasificación.

Estos registros, junto con el registro nacional único de clasificaciones, deberán poder ser consultados por los órganos subordinados autorizados, para ser utilizados como criterio y autorización, en su caso, de clasificación.

No deberán confundirse los registros de clasificaciones, que aquí se presentan, con los libros de registro de información clasificada que se indican posteriormente, al tratar sobre el sistema de registro en el **apartado 4** de esta norma. En los primeros se registran decisiones de clasificación y en los segundos se registran informaciones concretas clasificadas sobre la base de esas decisiones.

3.2. Marcas de clasificación

Los grados de clasificación estampillados sobre un determinado material clasificado, se denominan **marcas de clasificación**. La forma de realizar el estampillado se hará conforme a la normativa específica que lo regule. Como norma general, en los documentos, la marca de clasificación figurará en el encabezamiento y en el pie de cada página, diapositiva, gráfico o elemento que conforme dicho documento.

La marca de clasificación normalmente consta de diferentes partes, siendo las principales las que se indican a continuación, y que no siempre están explícitamente presentes, salvo el grado, que es obligatorio. En este contexto, se entenderá por:

- **TIPO**: es el ámbito de origen al que pertenece la información, es decir, la organización o estado propietario de la información clasificada. Por ejemplo, NATO, UE, NACIONAL (esta última suele ir implícita en el GRADO, por tener un idioma o nombres específicos).
- **GRADO**: la clasificación de seguridad de la información. Por ejemplo RESERVADO.
- **ESPECIALIDAD**: determinadas informaciones pertenecen a ámbitos más concretos que exigen una especial preparación y control más exhaustivo. Por ejemplo: ATOMAL, CRIPTO.

La documentación clasificada elaborada por organizaciones internacionales, o proporcionada a éstas por los estados miembros, debe mantenerse, en lo posible, en los idiomas y formatos oficiales. Las marcas de clasificación siempre se conservarán en su formato e idioma originales. En caso de que sea preciso realizar traducciones, se tratarán conforme se indica más adelante.

La documentación clasificada elaborada por los estados soberanos, como originadores y propietarios de la misma, se difunde con su grado y marca de clasificación nacional. Cuando se reciba en España, se le asignará la protección equivalente, según cuadro anexo II, con las particularidades que en un acuerdo para la protección de información clasificada puedan haberse establecido. Nor-

malmente, al llegar a España, se marcarán adicionalmente los documentos en su primera página con la marca del grado equivalente en España, de forma que se le aporte dicha protección. Este remarcado tiene el objeto de facilitar la labor a los destinatarios, pero en ningún caso supondrá una modificación en la propiedad de la información ni de las limitaciones de difusión previamente establecidas.

3.3. Marcas de clasificación más usuales

Aunque en el anexo II se encuentran las equivalencias de grados de clasificación, a continuación se indican los que están en vigor en las principales organizaciones internacionales de las que España es parte y ha ratificado la correspondiente política o regulación de seguridad, por ser los de más amplia difusión.

Los grados de clasificación OTAN, son los siguientes, en inglés o francés:

- **COSMIC TOP SECRET (CTS) / COSMIC TRÈS SECRET (CTS)**
- **NATO SECRET (NS) / NATO SECRET (NS)**
- **NATO CONFIDENTIAL (NC) / NATO CONFIDENTIEL (NC)**
- **NATO RESTRICTED (NR) / NATO DIFFUSION RESTREINTE (NDR)**

Los grados de clasificación UE, son los siguientes, en francés o inglés, o ambos simultáneamente (depende de la organización):

- **TRÈS SECRET UE/EU TOP SECRET/ (TS-UE/EU-TS)**
- **SECRET UE/EU SECRET (S-UE/EU-S)**
- **CONFIDENTIEL UE/EU CONFIDENTIAL (C-UE/EU-C)**
- **RESTREINT UE/EU RESTRICTED (R-UE/EU-R)**

Los grados de clasificación ESA, son los siguientes, en inglés:

- **ESA TOP SECRET (ESA TS)**
- **ESA SECRET (ESA S)**
- **ESA CONFIDENTIAL (ESA C)**
- **ESA RESTRICTED (ESA R)**

Existen otras organizaciones internacionales (o multinacionales), de ámbito militar o industrial, con regulaciones de seguridad específicas, que establecen sus propias marcas de clasificación, con criterios similares a los empleados en OTAN, como son por ejemplo: EUROPEAN CORPS, EUROGENDFOR, OCCAR, etc. Las peculiaridades de cada uno se establecen en su normativa o regulaciones específicas de seguridad.

Con independencia del ámbito, existe una equivalencia entre todos ellos según el orden en que se han expresado. Es decir, son equivalentes y, desde el punto de vista de las medidas de protección aplicables, tendrán un tratamiento similar:

–	**CTS**	**|**	**TS-UE/EU-TS**	**|**	**ESA TS**	**| S**
–	**NS**	**|**	**S-UE/EU-S**	**|**	**ESA S**	**| R**
–	**NC**	**|**	**C-UE/EU-C**	**|**	**ESA C**	**| C**
–	**NR**	**|**	**R-UE/EU-R**	**|**	**ESA R**	**| DL**

NOTA IMPORTANTE:

En adelante, se utilizarán las expresiones **«SECRETO o equivalente»**, «RESERVADO o equivalente», «CONFIDENCIAL o equivalente» y «DIFUSIÓN LIMITADA o equivalente» para referirse a cuestiones clasificadas que merezcan el mismo tratamiento de seguridad, con independencia de su tipo (ámbito de origen). Sólo dependerán del grado de clasificación.

Asimismo, se utilizará la expresión **«equivalente a SECRETO»** (e igual para RESERVADO, CONFIDENCIAL y DIFUSIÓN LIMITADA), cuando se excluya a la información clasificada nacional (España).

3.4. Información de categoría especial – marcas adicionales de categoría especial

En determinados ámbitos de información clasificada, se establecen categorías especiales de información, al ser necesario establecer una limitación en el acceso sólo a aquellas personas específicamente preparadas y autorizadas para ello. La información clasificada correspondiente a estas categorías especiales llevará marcas adicionales, estampilladas en la forma que se regule en la normativa específica de aplicación.

En el ámbito **OTAN** existen las siguientes marcas adicionales para categorías especiales:

- **ATOMAL (A)**: para información relativa a los activos nucleares a disposición de la Alianza.
- **CRYPTO (C) («*cryptosecurity*»)**: documentación, equipos y claves utilizados en sistemas criptográficos de la OTAN.
- **BOHEMIA (B)**: asuntos sobre guerra electrónica y la utilización de medios de comunicaciones y señales para la obtención de información en la Alianza.

En el ámbito **UE** existen las siguientes marcas de categorías especiales:

- **CRYPTO (C) («*cryptosecurity*»)**: documentación, equipos y claves utilizados en sistemas criptográficos de la UE.

En el ámbito **ESA** existen las siguientes marcas de categorías especiales:

- **CRYPTO (C) («*cryptosecurity*»)**: documentación, equipos y claves utilizados en sistemas criptográficos de la ESA.

En el ámbito **NACIONAL**, existen las siguientes marcas de categorías especiales:

- **CRIPTO (C)**: documentación, equipos y claves utilizados en sistemas criptográficos nacionales, o al amparo de un acuerdo de seguridad válido con otra nación.
- **SIGINT (B)**: equivalente al BOHEMIA de OTAN, pero en el ámbito nacional.

3.5. Marcas adicionales de limitación

La información clasificada podrá estar sujeta a determinadas limitaciones en su utilización cuando, de forma expresa, se haya definido en la normativa de seguridad aplicable. Para ello se hará uso de marcas adicionales de limitación, estampilladas en la forma que se regule en la normativa específica de aplicación, a continuación o bajo la marca de clasificación de seguridad (y marca de categoría especial, si la hubiera).

En las marcas de limitación normalmente se indican los destinatarios, organismos o estados autorizados (por ejemplo, «*Releasable to EU and CHILE*»), aunque también pueden referirse a canales autorizados (por ejemplo, «*Releasable for Internet Transmission*»).

Es competencia del originador, en el momento de la clasificación, establecer las limitaciones iniciales de difusión. El propietario podrá, en cualquier momento, modificar dichas limitaciones. En este sentido, se tendrá en cuenta que, según se indicó en el **apartado 2.1**, tener la custodia o ser usuario de una determinada información clasificada, no supone ostentar su propiedad.

3.6. Agregación de documentos

La clasificación de seguridad de un documento que se haya constituido por agregación de varios, corresponderá como mínimo al grado de clasificación que tenga el

componente con clasificación más alta. Dicha clasificación deberá figurar en la cubierta del documento y cada parte componente conservará su clasificación inicial, para facilitar las decisiones relativas a nuevas difusiones de secciones independientes.

El documento que forma la cubierta de un documento constituido por agregación, además de la clasificación global del documento, establecida conforme a lo indicado en el párrafo anterior, podrá tener una indicación adicional relativa a la clasificación que le corresponde, conforme a la información contenida en el mismo, cuando esté separado de la información a la que acompaña.

Cuando se agregue en un único documento información procedente de diversas fuentes, se revisará el producto para establecer una clasificación de seguridad global ya que puede justificar un grado de clasificación superior al que tienen sus componentes.

Se conservarán las marcas adicionales de limitación cuando se utilice información para preparar documentos por agregación de otros.

En cualquier caso, como norma general práctica, se tratará de evitar en lo posible la agregación en la preparación de documentos. Desde el punto de vista de la protección de la información, es preferible preparar un documento exclusivo con los elementos de mayor clasificación o, si esto no es posible, al menos agruparlos en anexos específicos; especialmente cuando el mayor volumen del documento que se pretende generar corresponde a información no clasificada o con grado bajo de clasificación.

Otro uso común, derivado del anterior, que igualmente se deberá evitar es la compilación de documentos de distinta clasificación o con distintos destinatarios, en un mismo soporte electrónico (DVD, CD-ROM, etc.). El pequeño beneficio de ahorro en transporte y material que supone el reunir en un mismo soporte multitud de documentos, y su identificación conjunta como uno único, conlleva un aumento enorme de la complejidad en el manejo, control y registro de esta información, especialmente porque posteriormente debe ser desglosada y registrada de forma independiente, para su correcto control y para su difusión conforme al principio de la «necesidad de conocer».

3.7. Integración de documentos

La información clasificada recibida en España de otras fuentes, según se ha indicado anteriormente, vendrá con una marca de clasificación y, en su caso, unas marcas adicionales (de categoría especial o de limitación). En cualquier caso, siempre está claramente establecido el propietario de la información, y las limitaciones en la difusión del documento.

Asimismo, la normativa de seguridad que rige para dicha información, podrá definir las condiciones generales que deben cumplirse para la entrega de dicha información a terceros estados.

Teniendo siempre en cuenta estas limitaciones, y de acuerdo con el criterio de la responsabilidad de compartir, los destinatarios en España de esta información, que sean responsables y custodios de la misma, podrán integrar extractos de la información contenida en dichos documentos dentro de un nuevo documento con una clasificación de seguridad nacional adecuada al grado de protección que le corresponda, con los siguientes condicionantes:

- La integración siempre se hará por transcripción, y nunca mediante recorte, fotocopia o similar.
- La información clasificada de grado «equivalente a SECRETO», bajo ninguna premisa podrá ser objeto de integración.
- En ningún caso un documento completo podrá ser integrado como información nacional.
- Dicha integración es necesaria para poder cumplir las misiones y cometidos oficiales.

Se utilizará el nombre de **integración** para referirse a este proceso. La integración supone un ejercicio de alta responsabilidad por quien la ejecuta, toda vez que debe asegurarse no se vulnere ningún principio o limitación de seguridad que afectara a la documentación original, especialmente las limitaciones de difusión y de cesión a terceros. Por dicho motivo, estas decisiones se tomarán al nivel adecuado de responsabilidad del organismo o entidad integradora de la información, asesorado por el jefe de seguridad del órgano de control a su servicio, supervisando el resultado final de la integración.

3.8. Desarrollo normativo

El proceso de clasificación de seguridad de la información a nivel nacional, aunque se describe en estas normas, precisa de un desarrollo normativo más detallado, que habrá de ser único nacionalmente y de obligado cumplimiento.

Dicho desarrollo, entre otros aspectos que se determinen, definirá:

- el procedimiento completo de clasificación, desde la elaboración de la propuesta, hasta la promulgación de la diligencia, directiva o norma de ley que clasifica,
- las características físicas de las marcas de clasificación,

- datos adicionales a incluir en una clasificación y forma (identificación de ley, diligencia o directiva por la que se clasifica, tiempo de vigencia de la clasificación, número de registro de clasificación, etc.),
- formatos de las propuestas, guías, diligencias o directivas,
- criterios de identificación de un documento clasificado (referencia de registro, organismo o entidad de origen, identificación de páginas, identificación de copias, traducciones o extractos, etc.),
- divulgación y acceso a los registros de clasificaciones (compendios de normas de ley, guías, directivas y diligencias promulgadas),
- cualquier otro aspecto que deba ser regulado y normalizado.

4. REGISTRO DE LA INFORMACIÓN CLASIFICADA

4.1. El sistema de registro

El sistema de registro, organizado sobre la base de los órganos de control de información clasificada, es responsable de la recepción, contabilidad, custodia, distribución y destrucción de la información clasificada registrable que maneje, conforme a lo que establecen estas normas. Los órganos de control, por tanto, actúan también como organización responsable de la distribución interna de la información clasificada y del mantenimiento de los libros de registro de información clasificada de su responsabilidad.

Se utiliza el término de **información clasificada registrable** para designar a la información clasificada susceptible de ser anotada en un registro, es decir, que cumpla las condiciones de ser tangible (esté contenida en un soporte), se le pueda asignar, o ya disponga, de un número de registro y no se rija expresamente por otros criterios particulares que la eximan de esa condición.

La información clasificada registrable, con carácter general, circulará a través de un **sistema de registro**. No obstante, la información clasificada con grado «DIFUSIÓN LIMITADA o equivalente», puede circular entre usuarios, en las condiciones que más adelante se establecen.

Cuando el grado de clasificación de la información sea igual o superior a «CONFIDENCIAL o equivalente» **será obligatoria** su circulación por el sistema de registro.

Se considera **información clasificada controlada** aquella de grado igual o superior a «CONFIDENCIAL o equivalente» y de la que, cuando esté a su cargo, los órganos de control habrán de poder establecer en todo momento cuál es su localización.

4.2. Organización y competencias del sistema de registro en España

El sistema de registro en España está constituido por el Registro Central y todos los órganos de control autorizados por la ANPIC o creados en el ámbito de la Ley de Secretos Oficiales, hasta nivel punto de control, o servicio local de protección, incluido.

A través de ellos se distribuye la información clasificada. Es parte fundamental de la estructura nacional para la protección de la información clasificada y está estructurado jerárquicamente conforme al siguiente esquema de responsabilidades:

– Ámbito nacional:

  • Servicios centrales de protección.
  • Servicios generales de protección.
  • Servicios locales de protección.

– Ámbito internacional:

  • Registro Central España.
  • Subregistros principales.
  • Subregistros secundarios.
  • Puntos de control.

El sistema de registro es responsable de la recepción, contabilidad, custodia, distribución y destrucción de la información clasificada que se maneja en los organismos y entidades a los que sirve. La constitución, dependencia y cometidos de estos órganos se han definido previamente en la norma NS/01 de la ANPIC.

La red principal la forman el Registro Central y los subregistros principales, junto con los servicios centrales de protección. De esta red principal dependen una serie de redes secundarias, agrupadas cada una de ellas bajo el control de un subregistro principal o servicio central de protección, del que dependen los subregistros secundarios o servicios generales y los puntos de control o servicios locales, respectivamente, que sean necesarios establecer. Los puntos de control pueden depender de un subregistro principal directamente o de un subregistro secundario, igualmente que los servicios locales de protección respecto a los servicios central o generales.

Esta red podrá modificarse y ampliarse en función de las necesidades que manifiesten otros organismos de disponer de información clasificada.

La competencia de registro de la información clasificada de nueva creación corresponde, como mínimo y con carácter general:

- Grado «equivalente a SECRETO», al Registro Central.
- Grado SECRETO, a los servicios centrales de protección.
- Grado «RESERVADO o equivalente», a los subregistros principales y secundarios, o servicios generales de protección.
- Grado «CONFIDENCIAL o equivalente» o inferior, a cualquier órgano de control.

Con carácter limitado, esta competencia se podrá delegar formalmente en un órgano de control inferior, sin perjuicio de la obligación de este último de informar a su órgano de control superior.

En el caso especial de la información clasificada manejada en empresas con motivo de actividades, contratos o programas clasificados, en el ámbito de la seguridad industrial, las anteriores competencias podrán modificarse. Dado el carácter tan específico de esta información, su tratamiento normalmente estará regulado de forma específica por unas **instrucciones de seguridad del programa o contrato**, que serán las que se aplicarán e indicarán la forma de aplicar la normativa general. También mediante las propias cláusulas de seguridad del contrato se podrán fijar las competencias de registro de la empresa.

4.3. El Registro Central España

A tenor de los acuerdos internacionales en materia de protección de la información clasificada, España se compromete a crear un registro central, que actuará como la principal autoridad de **recepción y distribución** de información clasificada para la nación, dentro del ámbito de sus competencias. En este sentido, será el Registro Central COSMIC/TOP SECRET de España ante las organizaciones internacionales y ante otros estados.

El Registro Central España (en adelante Registro Central), es responsable de llevar el libro de registro de información clasificada de grado «equivalente a SECRETO», perteneciente a organizaciones internacionales o intercambiada al amparo de un acuerdo para la protección de la información clasificada.

Cuando esta información no se tramite a través del propio Registro Central, el órgano de control nacional, originador o custodio de la información, le comunicará, por el canal funcional jerárquico de protección, los datos necesarios para su registro u otros adicionales que le solicite, y quedará a la espera de instrucciones para el traslado o inspección visual del documento por el Registro Central.

El Registro Central asignará un número de registro propio a todo documento tramitado y controlado conforme a lo indicado en los párrafos previos. Este número es distinto del número o referencia de origen del documento y deberá figurar en la carátula, etiqueta, superficie o primera página (según formato) del documento que se trate, como evidencia de su control.

Con carácter limitado, cuando así se exprese de forma explícita en los acuerdos internacionales, el Registro Central podrá ser también responsable del registro de información clasificada nacional de grado SECRETO intercambiada internacionalmente.

En el **ejercicio de su responsabilidad y dentro de su ámbito de su competencias**, el Registro Central está facultado por la ANPIC para exigir el acceso inmediato a cualquier información clasificada, para verificar su existencia y correcto control, con independencia de cuál sea el organismo o entidad que lo custodia o el destinatario.

4.4. Sistema de registro COSMIC/TOP SECRET

Este sistema se crea como requisito de las políticas y regulaciones de seguridad de organizaciones internacionales. El objetivo de los órganos de control COSMIC/TOP SECRET que configuran el sistema, es asegurar y dar evidencia objetiva del correcto registro, uso y distribución de la información con grado «equivalente a SECRETO» (CTS, TS-UE/EU-TS, etc.).

La difusión de información clasificada de grado «equivalente a SECRETO» se realizará exclusivamente a través de los registros autorizados a dicho grado. Estos registros remitirán al Registro Central, una vez al año, el inventario de toda la información clasificada «equivalente a SECRETO» de la que son responsables, sin perjuicio de las comunicaciones inmediatas de cualquier novedad que afecte a este tipo de información.

Tanto el Registro Central como aquellos órganos de control autorizados por la ANPIC para manejar información clasificada «equivalente a SECRETO», deberán proponer a la ONS el nombramiento de un «oficial de control COSMIC/TOP SECRET» (OCC), responsable del control y custodia de toda la información clasificada «equivalente a SECRETO» que tenga asignada. El OCC deberá estar en posesión de una habilitación de seguridad de dicho grado.

Cuando el propio jefe de seguridad del órgano de control actúe como OCC, no será preciso proponer su nombramiento como tal a la ONS. Análogamente, si no

se propone el nombramiento de un OCC específico, el cargo lo ostentará automáticamente el jefe de seguridad del órgano de control.

4.5. Contabilidad y registro de la información clasificada

Cada órgano de control deberá tener registrada y perfectamente localizada la información clasificada de grado «CONFIDENCIAL o equivalente» o superior (o **información clasificada controlada**), que esté a su cargo. Asimismo, deben tener controlada la **información clasificada imputable** (definida más adelante como la de grado «RESERVADO o equivalente» o superior) bajo responsabilidad de los órganos de control directamente subordinados.

Todo órgano de control deberá mantener actualizado el **libro de registro de información clasificada controlada**, en formato papel o electrónico, que permita conocer las existencias a cargo en el propio órgano de control y su localización, con registro separado, física o lógicamente, para cada tipo (nacional, OTAN, UE, etc.).

En dicho libro de registro, o en otro específico, se llevará el control de la información clasificada imputable existente en los órganos de control directamente subordinados, con la excepción de lo que más adelante se establece para la información de grado «equivalente a SECRETO».

En este punto y relacionado con dicho libro de registro, se recuerda la obligación marcada en el **apartado 5** de la norma NS/01 de remitir a la ONS, con un mes de antelación a la fecha de inspección bienal al SPIC, registro informático actualizado de la información imputable, de grado «equivalente a RESERVADO», custodiada o a cargo en toda su estructura de protección dependiente, de la que es responsable.

La información clasificada de grado «DIFUSIÓN LIMITADA o equivalente» no necesita ser registrada en registros específicos de información clasificada.

Todo órgano de control deberá mantener actualizado el **libro de registro de entrada y salida**, en formato papel o electrónico, donde figurarán los movimientos de información clasificada registrable recibida como destinatario, o emitida como originador o remitente, por el organismo o entidad al que sirve dicho órgano de control, con la excepción de lo que más adelante se establece para la información de grado «equivalente a SECRETO».

La información clasificada que se tramite a través de un órgano de control donde éste sólo actúe como punto de paso, es decir, que no sea el del organismo o entidad

originador o destinatario final del documento, no precisa ser registrada en el libro de registro de entrada y salida, siendo suficiente conservar los recibos y acuses de recibo de entrega de valijas o paquetería entre órganos de control, o las anotaciones en libros de entrega, sin perjuicio de lo establecido anteriormente respecto al control de la información clasificada imputable con destino a un órgano de control subordinado.

Los órganos de control COSMIC/TOP SECRET deben establecer mecanismos que permitan la separación de esta información del resto, tanto desde el punto de vista físico como del administrativo. Para ello dispondrán de medios de registro específicos para dicho grado, y para cada tipo (OTAN, UE, etc.).

Los órganos de control exteriores, radicados en embajadas españolas, o en delegaciones y representaciones españolas destacadas ante organizaciones internacionales, son parte de la estructura nacional de protección, por lo que estarán sujetos a los mismos criterios y supuestos anteriores.

4.6. Requisitos de imputabilidad

La información clasificada de grado «RESERVADO o equivalente» o superior, es **información clasificada imputable**, es decir, está sujeta al requisito de la imputabilidad, por lo que, además del control llevado a cabo por el sistema de registro, de forma adicional debe ser registrado todo acceso que se produzca a dicha información, con indicación inequívoca de la persona que accede, fecha-hora en que se produce el acceso y registro de firma o de acceso electrónico.

Toda información clasificada imputable debe tener una **ficha de control y acceso a información clasificada** adjunta («log» de accesos, si es un sistema), según formato publicado en la página «web» de la ONS, o similar, la cual, en caso de destrucción del material clasificado habrá que conservar disponible durante los mismos plazos de tiempo que se establecen, según el grado de clasificación, para las **actas de destrucción de materiales clasificados**, y que se indican más adelante.

El acceso a información clasificada imputable disponible en sistemas de información y comunicaciones será registrado por los propios controles de seguridad del sistema, que deben poder determinar la identidad del usuario que accede y fecha-hora de dicho acceso, así como permitir emitir listados de acceso. Se establecen los mismos plazos de conservación para dichos registros que los referidos en el párrafo anterior.

Otras informaciones clasificadas adicionales, por su especial sensibilidad, también se declaran como imputables, aunque tengan un grado menor de clasificación. Así

ocurre con la información clasificada con marca especial ATOMAL de OTAN de grado «CONFIDENCIAL con ***Limitaciones Especiales***».

El principal objetivo de la imputabilidad es proporcionar suficiente información para poder investigar un comprometimiento, deliberado o accidental, de información clasificada imputable y valorar el daño que dicho comprometimiento haya causado. El requisito de la imputabilidad sirve para imponer disciplina en el manejo y el control de acceso a la información clasificada imputable.

El objetivo secundario es llevar cuenta del acceso a la información clasificada imputable, es decir, quién ha tenido acceso, o ha podido tenerlo, a esta información y quién ha tratado de acceder a esta información.

4.7. Coexistencia de información clasificada de diferentes tipos y grados

Cuando en un mismo órgano de control coexista, de forma autorizada, información clasificada de diferentes tipos, ésta se custodiará en contenedores separados, con las limitaciones que imponga la necesidad de conocer del personal destinado en el órgano de control responsable de la custodia, o de otro personal externo que necesite acceder a la misma, por ejemplo, en su función inspectora.

Habrá de mantenerse en todo momento una estricta compartimentación, dentro de cada tipo (nacional, OTAN, UE, etc.), de la información de grado «SECRETO o equivalente», del resto, tanto a nivel de archivo y custodia (contenedores separados), como de registro (registro separado del resto).

Esta compartimentación también es obligatoria para la información clasificada CRIPTO y para ATOMAL, siempre con las limitaciones que imponga la necesidad de conocer.

La necesidad de conocer, el análisis de riesgos de seguridad física de la instalación donde se ubique el órgano de control, y las medidas establecidas en el plan de protección, determinarán la naturaleza exacta de la compartimentación requerida en cada caso, que podrá variar desde la simple ubicación en estantes separados sin acceso visual posible a contenidos, hasta la necesidad de establecer cajas fuertes diferenciadas de determinado grado de protección.

4.8. Casos especiales

La información clasificada que se maneje en sistemas de información y comunicaciones, proceso que se regula en la norma NS/05, estará bajo la supervisión de

un órgano de control, que verificará que dicha información esté adecuadamente registrada y controlada en todo momento, y que se mantiene registro (normalmente electrónico) de los accesos de los usuarios a la información clasificada de grado «RESERVADO o equivalente» o superior. La **documentación de seguridad del sistema** deberá definir expresamente cómo se realiza el tratamiento de la información clasificada, incluida la que de forma temporal o permanente quede residente en los discos de almacenamiento, y la que se grabe en soportes de respaldo, o «back-up». Los propios soportes de información, sean externos, removibles o fijos, estarán sujetos a normas de identificación, marcado y registro.

El procedimiento de **acreditación del sistema** permitirá verificar que las medidas adoptadas son correctas y suficientes.

Cuando la información clasificada se transmita y maneje en forma de formularios, datos con formato, etc., entre centros de situación, sistemas de armas o elementos de naturaleza similar, el control y manejo estará normalmente implementado en el propio sistema donde se maneja dicha información. En este caso será de aplicación lo indicado anteriormente para los sistemas de información y comunicaciones, aunque no siempre será posible un control exhaustivo, incluso ni de forma electrónica, siendo sólo posible el control de acceso al sistema, no a la información.

Esto ocurre, por ejemplo, con sistemas de información de combate o de seguimiento de operaciones en tiempo real, en que se recibe simultáneamente información clasificada de diferentes fuentes (OTAN, nacional o de otros estados), la cual se muestra de forma conjunta en paneles de situación. Es evidente que en estos casos, u otros similares, el control exhaustivo conforme a normativa es imposible. De cualquier forma, la documentación de seguridad de los sistemas debe contemplar este evento y acreditarse en dichas condiciones.

Cuando la información clasificada se transmita y maneje en forma de mensajes entre centros de comunicaciones (CECOM) o en sistemas de mensajería acreditados para empleo directo por los usuarios, por razones operativas y de oportunidad, podrán llevar un tratamiento especial, el cual se define en el anexo III.

Otro caso especial es el de la información clasificada manejada con motivo de actividades, contratos o programas clasificados, principalmente en el ámbito de la seguridad industrial. Esta información puede adoptar formatos y usos muy variados y difíciles de controlar conforme a la normativa general. Es el caso, por ejemplo, de los materiales, repuestos, componentes de armas, componentes electrónicos, programas informáticos, datos de resultados de pruebas, etc. Dado el carácter y formato de esta información, su tratamiento normalmente estará

regulado de forma específica por unas instrucciones de seguridad del programa, proyecto o contrato, que serán las que se aplicarán e indicarán la forma de aplicar la normativa general.

El acceso infrecuente o temporal a información clasificada no precisa necesariamente el establecimiento de un órgano de control, siempre que funcionen los procedimientos destinados a garantizar que la información se mantiene bajo el control del sistema de registro.

Por último, en lo que respecta a la responsabilidad del control y distribución del material de cifra, se ha establecido un sistema diferente y específico para llevarlo a efecto, por lo que no se requiere ninguna responsabilidad de control por parte del sistema de registro del material que se transfiera a través de este sistema.

4.9. Identificación y datos de registro

Para poder llevar a cabo un adecuado control, tratamiento y registro de cualquier información clasificada, es condición indispensable que esta esté perfectamente identificada. Por ello es necesario determinar los datos necesarios para identificar de forma completa y correcta una información clasificada concreta, y que permitan darle el tratamiento y protección adecuados:

- la identificación inequívoca de la información, por su referencia única,
- el tipo, grado y especialidad,
- marcas adicionales de limitación,
- la determinación del originador, propietario y custodio, cuando sea preciso,
- la identificación de la norma de ley, directiva de clasificación o diligencia de clasificación por la que se ha clasificado,
- la distinción entre original, copias (o subcopias), traducciones o extractos
- propiedades del documento o material no documental: asunto, idioma, formato, etc.,
- números de registro en Registro Central (si procede) y en servicio de protección custodio,
- fechas y datos relevantes de su tramitación (creación, recepción, reclasificación, destrucción, etc.),
- instrucciones especiales de manejo (difusión, cesión, reclasificación, destrucción, etc.),
- observaciones generales o particulares,
- otros datos que se definan normativamente.