Estos datos serán los que se utilizarán por el sistema de registro en España para cumplimentar los libros de registro de información clasificada controlada y para identificar correctamente dicha información. De los anteriores habrá datos que solo figuren o en el libro de registro o en el documento o material no documental clasificado, y otros que estarán en ambos.

En el caso del manejo electrónico de documentos en sistemas acreditados, el integrar esta información como «metadatos» en el propio documento facilita su manejo y la aplicación del principio de la garantía de la información, siempre que se sigan criterios normalizados a nivel nacional respecto a los formatos de documentos y criterios de uso de los metadatos.

Respecto a la información clasificada manejada por empresas, en el ámbito de la seguridad industrial, será necesario incluir datos adicionales de registro para cada documento o material no documental clasificado bajo su responsabilidad, en concreto:

- organismo de la Administración responsable del material clasificado,
- servicio de protección de la Administración del que depende funcionalmente el servicio de protección de la empresa con respecto a ese material clasificado concreto[3],
- originador de la información clasificada (distinguir si es un material clasificado generado por la empresa o si se ha recibido del organismo de la Administración),
- identificación de las instrucciones de seguridad del programa o proyecto por las que se rige,
- identificación de la guía de clasificación, si existe, tomada como referencia de clasificación.

Por tanto, el proceso de identificación y registro de la información clasificada a nivel nacional, aunque se cita de forma somera en estas normas, precisa de un desarrollo normativo más detallado, que habrá de ser único nacionalmente y de obligado cumplimiento.

En tanto dicho desarrollo se lleva a efecto, en el anexo IV se adjunta un modelo de ficha de datos necesarios para identificar correcta y completamente una información clasificada, y para llevar a efecto su registro y control del ciclo de vida. Al realizar un cambio de propiedad o de custodia de una información clasificada, estos datos deben transferirse igualmente. De otra forma es imposible dar el tratamiento y manejo adecuado a dicha información.

[3] Hay que tener en cuenta que una empresa puede tener información de distintos programas, contratos o actividades, y pertenecientes a distintos organismos de la Administración.

5. CIRCUITOS DE DISTRIBUCIÓN DE LA INFORMACIÓN CLASIFICADA

5.1. Distribución con organizaciones internacionales y otros estados

Con carácter general la circulación de información clasificada hacia organismos o entidades de otros estados u organizaciones internacionales o multinacionales, estará prohibida, salvo que exista una autorización expresa al efecto. Será requisito necesario el que exista un acuerdo, o garantías mutuas, de protección de la información clasificada entre las partes afectadas, tal como se definen en el **apartado 5.2** de la norma NS/00 de la ANPIC.

Normalmente estos intercambios de información clasificada se producirán en un marco establecido, que podrá tener un carácter amplio, como es el caso de la pertenecía de España a organizaciones internacionales o multinacionales, o un carácter más limitado, cuando se trata de ámbitos concretos de colaboración, o con ocasión de contratos, programas o proyectos clasificados internacionales.

La información clasificada de grado «equivalente a DIFUSIÓN LIMITADA» o superior, deberá entrar o salir, de la estructura nacional de protección, a través del Registro Central, o por otro medio de transmisión, físico o tecnológico, autorizado por la ANPIC. Los órganos de control de la estructura nacional de protección que reciban esta información directamente, sin haber circulado por el Registro Central, serán responsables de iniciar su registro y control, y de informar a su de control superior de las altas producidas, en los casos que así establece esta norma.

Solo se aportará al Registro Central la información precisa para el registro de la información clasificada de grado «equivalente a SECRETO», no siendo necesario comunicar los datos relativos a información de grado «equivalente a RESERVADO» o inferior, según se marca en el **apartado 4.3** de esta norma.

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.

Con carácter limitado, en los casos en que así se determine de forma explícita (especialmente en los acuerdos internacionales), el Registro Central será también responsable de la distribución de información clasificada nacional de grado RESERVADO o superior, intercambiada internacionalmente.

5.2. Distribución dentro de España

En el ámbito de las Administraciones y Fuerzas Armadas, y su personal, la información clasificada con grado «DIFUSIÓN LIMITADA o equivalente» puede circular libremente entre órganos de control y entre usuarios, siempre que no existan limitaciones previas a su difusión y que los destinatarios cumplan las condiciones de acceso (tener necesidad de conocer y haber sido instruidos en el manejo de la información clasificada), y las de manejo y custodia establecidas en estas normas para dicho grado, siendo responsabilidad de quien la entrega verificar que se cumplen dichas condiciones por parte del destinatario.

En el ámbito de la seguridad industrial, la información clasificada de grado «DIFUSIÓN LIMITADA o equivalente» puede circular entre usuarios de empresas contratistas únicamente si éstos, además de cumplir los requisitos del apartado anterior, son empleados del mismo contratista.

La distribución de la información clasificada controlada, definida anteriormente como la de grado «CONFIDENCIAL o equivalente» o superior, siempre se efectuará entre órganos de control, y nunca entre usuarios. En cualquier caso, estos órganos deberán verificar previamente que los contactos directos, o los envíos que se realicen, estén autorizados, y no existan limitaciones a dicha distribución.

En el caso de que información clasificada controlada tenga un destinatario concreto, el órgano de control al que llegue la información se lo comunicará al interesado, quien los examinará en las instalaciones autorizadas. Si de este examen el usuario deduce que los va a necesitar más tiempo, solicitará la autorización correspondiente al jefe de seguridad, quien determinará las condiciones y el plazo en los que podrá extraer la información del órgano de control. Esta autorización no se podrá conceder al personal de empresas contratistas, salvo de forma extraordinaria y con medidas adicionales de control.

Excepto para la información clasificada con grado «SECRETO o equivalente», los criterios de distribución podrán modificarse, bajo criterio y responsabilidad de la autoridad del organismo o entidad responsable de la información afectada, y solo dentro de su ámbito de responsabilidad, cuando existan fundados motivos operacionales o funcionales que así lo aconsejen, y sin menoscabo de la obligación de informar de los movimientos producidos en los casos y forma que prevé esta normativa.

La información clasificada de grado «equivalente a SECRETO» circulará siempre a través del Registro Central, no así la nacional de grado SECRETO, que sólo circulará por dicho Registro Central cuando deba ser entregada a otro estado u

organismo internacional, y así se haya establecido. Esta última circulará a través de los servicios centrales de protección de información clasificada.

La información clasificada de grado «RESERVADO o equivalente» podrá circular directamente entre subregistros principales o entre servicios centrales de protección. También podrá circular, excepto en el ámbito empresarial (salvo autorización expresa), entre subregistros secundarios, puntos de control y entre servicios generales o locales de protección, dependientes de un mismo órgano de control de nivel inmediato superior, al que informarán de los movimientos producidos, a efectos de control y registro.

La información clasificada de grado «CONFIDENCIAL o equivalente», con limitaciones para empresas contratistas, podrá circular directamente entre los órganos de control, no siendo preciso informar a su órgano de control de nivel inmediato superior de los movimientos producidos, bastando con su anotación en los registros respectivos. Como se indicó anteriormente, estos órganos deberán verificar previamente que los contactos directos, o los envíos que se realicen, estén autorizados, y no existan limitaciones a dicha distribución.

En el ámbito de la seguridad industrial, los órganos de control de un mismo contratista podrán intercambiar entre sí directamente información clasificada de grado «DIFUSIÓN LIMITADA o equivalente», quedando prohibido el intercambio para este grado, y por tanto también para cualquier otro grado superior, entre órganos de control de contratistas diferentes, salvo que el organismo propietario de la información clasificada lo autorice. Será preciso informar al órgano de control de nivel superior del que depende la empresa contratista sobre los intercambios de información clasificada de grado «CONFIDENCIAL o equivalente» efectuados directamente entre órganos de control del mismo contratista.

La distribución de la información clasificada estará adicionalmente sujeta a las propias limitaciones que cada organización responsable pueda poner al flujo de la información dentro de su ámbito de responsabilidad y hacia otras organizaciones, concretamente las derivadas de la autorización o no de contactos directos entre los organismos o entidades a los que sirven los órganos de control, o personas, afectados en cada caso.

5.3. Información clasificada recibida directamente por un usuario

En casos excepcionales en los que una persona, titular de una habilitación de seguridad adecuada, y con la debida acreditación para el transporte de documentación, si fuera el caso, reciba directamente información clasificada de grado «CONFIDENCIAL o equivalente» o superior, bien porque ha sido dirigida nominalmente a él, o

bien porque le sea entregada personalmente en mano (por ejemplo con ocasión de asistencia a una reunión), deberá inexcusablemente efectuar su registro inmediato ante el órgano de control del que dependa, el cual, si el tipo y grado de clasificación de la información lo requiere, la elevará al órgano de control superior para que se proceda a su correspondiente regularización, llegando al Registro Central o servicio central de protección, según corresponda, si fuera necesario.

6. TRANSMISIÓN DE LA INFORMACIÓN CLASIFICADA

6.1. Concepto

El envío por cualquier medio, sea físico o tecnológico, de información clasificada de un remitente a un destinatario, bien personas o bien órganos de control, constituye una **transmisión** de información clasificada.

Esta transmisión se puede hacer con medios físicos, como puede ser el correo postal, transporte personal, correo oficial diplomático o militar, etc., que es lo que se conoce habitualmente como **transporte**, y también puede realizarse por medios tecnológicos, por ejemplo: transmisión por fax, teléfono u otras tecnologías de la información y de las comunicaciones.

La seguridad de la transmisión por medios tecnológicos es objeto de una norma específica de la ANPIC sobre seguridad en los sistemas de información y comunicaciones (NS/05). Se utilizarán tecnologías de la información y de las comunicaciones (TIC) autorizadas para el grado de la información clasificada que se vaya a transmitir.

Como norma general, el método preferible de transmisión de información clasificada, no sólo por cuestiones de inmediatez, sino también por la mayor seguridad y menor riesgo que supone, será el de transmisión por medios tecnológicos.

En segunda preferencia estará el transporte en soportes informáticos protegidos por un producto criptológico aprobado, del grado adecuado. En este caso tendrá el mismo tratamiento y se podrá transportar por los mismos medios que si se tratara de información no clasificada, por lo que no precisará medidas especiales de protección de la confidencialidad. No obstante, cuando se transporte en mano, el portador llevará las autorizaciones necesarias que le identifiquen como persona autorizada, aunque no precise de HPS.

En adelante, al establecer criterios para el transporte, se hará sobre la base de que la información clasificada que se transmite está en claro, por ser el caso más desfavorable.

En el ámbito de la seguridad industrial, por sus especiales características o por necesidades operativas y de eficacia, se podrán establecer métodos o requisitos específicos de transporte, que garanticen un mayor control y seguimiento. Así, por ejemplo, algunos materiales clasificados, principalmente no documentales, por motivo de su naturaleza, criticidad, riesgo o presentación, pueden requerir normas específicas para su transporte, que habitualmente se incluyen dentro de lo que se denomina un **plan de transporte**, documento que se trata en la norma NS/06 de la ANPIC.

El objeto de la seguridad aplicada al transporte de la información clasificada es garantizar que se aplican las medidas de protección adecuadas que eviten la observación, modificación, sustracción o divulgación de la información durante su movimiento entre diferentes emplazamientos.

El transporte de información clasificada deberá efectuarse asegurándose que se cumplen todos los requisitos de protección física previstos y que se remite por los canales protegidos autorizados por la ANPIC.

No debe confundirse el concepto de transmisión con el de circulación por el sistema de registro, es decir, por los circuitos de distribución de la información clasificada definidos anteriormente, en el **apartado 5**. La transmisión está al servicio del sistema de registro, como elemento necesario para que la información clasificada circule, pero tiene una entidad diferente. La transmisión siempre se hará conforme a los circuitos de distribución autorizados.

6.2. Esquema básico de transmisión de la información clasificada

El proceso de transmisión de una información clasificada exige la actuación de unos elementos concretos y la realización de unos pasos definidos.

En toda transmisión hay un **remitente** y un **destinatario** (o varios). Remitente es la persona autorizada o cargo concreto, organismo o entidad que decide o inicia el envío de una información clasificada. Podrá ser de origen, si es quien ha confeccionado la información que se transmite, o no serlo, cuando simplemente transmita, a un tercero, información recibida anteriormente de otro remitente. En cualquier caso, cumplirá con las limitaciones de difusión que fije el propietario de la información. Destinatario es la persona o cargo concreto, organismo o entidad final a la que se envía dicha información clasificada.

El esquema básico de pasos a seguir para que una información clasificada se transmita de un remitente a un destinatario es el siguiente:

a) El remitente de origen decide y prepara la información clasificada a transmitir, identifica claramente al destinatario, y entrega todo ello al órgano de control del que dependa, en cumplimiento de la norma de que la información clasificada registrable circule por el Sistema de Registro (obligatorio si es información clasificada controlada, es decir, de grado «CONFIDENCIAL o equivalente» o superior).

b) El remitente es responsable de verificar que el órgano de control de destino está autorizado para el tipo, grado y especialidad de la información clasificada que le va a remitir.

c) El órgano de control remitente registra la salida y decide inicialmente el modo y vía de transmisión, que deberá ser uno autorizado para el grado de clasificación de la información a transmitir.

d) Si la transmisión es por medios tecnológicos, normalmente será responsabilidad de los CECOM dependientes en origen y destino de los respectivos órganos de control a efectos de protección de la información clasificada, hacerse cargo de la transmisión.

e) Si se va a realizar un transporte, definido anteriormente, el órgano de control de origen es responsable de preparar los sobres y paquetes a transportar conforme se indica en esta normativa.

f) Si la información clasificada es imputable y nominal, es decir, va dirigida a una persona o cargo concreto, obligatoriamente se adjuntará un **recibo de remitente de material clasificado** por cada destinatario (para devolver firmado), según formato publicado en la página «web» de la ONS o similar, como acuse de recibo del destinatario final de la información clasificada imputable recibida. Si no es nominal, este recibo no es necesario.

g) El servicio de transporte es responsable de que el contenido transmitido llegue intacto y sin manipulación no autorizada al destinatario final, o al órgano de control que sirve a dicho destinatario, debiendo quedar evidencia objetiva de ello. Para esto se hará uso de **recibos de transporte de material clasificado** (según formato publicado en la página «web» de la ONS, o similar, que más adelante se explica), **recibos de valija** (según formato publicado en la página «web» de la ONS, o similar), libros o recibos de entrega, registros de tramitación, etc., según el servicio del que se trate y de los procedimientos específicos de ejecución del transporte por los que se rija.

h) El servicio de transporte no accederá al contenido de los sobres o paquetes que se le encomienden, con las excepciones que se establecen para la información que deba ser visada y autorizada por un órgano de control superior y para la información que circule a través del Registro Central, con destinatario o remitente, de un estado, u organización internacional, extranjero. En este caso el Registro Central actúa como autoridad auditora y

de registro de la información que entra y sale de España, siendo su obligación el verificar y registrar la información clasificada controlada transmitida por esta vía.

i) El servicio de transporte en ocasiones deberá conocer el grado máximo de clasificación de la información contenida en cada paquete transportado, de forma que pueda determinar las vías de encaminamiento y los criterios de manejo y seguridad a utilizar. Por dicho motivo, cuando sea necesario, dicho grado debe venir también indicado en los recibos o libros de entrega.

j) El órgano de control de destino registra la entrada de la información clasificada, para lo cual, abre el sobre o paquete. Para la entrega al destinatario final actuará conforme a la normativa específica para la información que se trate, teniendo en cuenta las instrucciones especiales de tramitación que pueda haber en el sobre interior, donde figura el destinatario.

En el **apartado 7** de esta norma y, con mayor detalle, en el documento de la ONS denominado «OR-ASIP-04-02. Orientaciones para el uso de recibos y certificados de correos», se describen los criterios para el uso, confección y tramitación de recibos.

6.3. Preparación de sobres y paquetes

Toda información con grado de clasificación «CONFIDENCIAL o equivalente» o superior, se remitirá bajo doble sobre. Estos sobres serán opacos, resistentes y estarán cerrados con precintos (sellado de lacre, cinta adhesiva especial, etc.) que permitan identificar cualquier manipulación para acceder al contenido que pueda ocurrir durante el transporte.

Para la información de grado «DIFUSIÓN LIMITADA o equivalente» o inferior, podrá hacerse uso de doble sobre, cuando sea preciso ocultar cualquier evidencia del contenido, debido al sistema de transporte elegido.

Corresponde al órgano de control remitente preparar adecuadamente la información clasificada para su transporte. Previamente se anotarán en el registro de entrada y salida, como salida, los datos de identificación de dicha información.

Si la información clasificada es imputable y nominal, según se indicó anteriormente se adjuntará obligatoriamente un recibo de remitente de material clasificado dentro del sobre interior, que debe rellenar y firmar el destinatario y devolver al remitente, como acuse de recibo de la información clasificada imputable. Este recibo, al no ser información clasificada, se podrá devolver por cualquier vía (fax, correo postal, etc.).

En el sobre interior, sobre su lado anverso, constará:

- La marca del grado de clasificación, en rojo, estampillada en el borde superior e inferior, y que también irá en el reverso del sobre.
- La identificación del remitente (persona o cargo concreto, organismo o entidad, u órgano de control). Este dato podrá ir en el reverso del sobre.
- La referencia del material clasificado.
- El organismo o entidad destinatario, y si es nominal, la persona o cargo concreto destinataria.
- El órgano de control de destino (subregistro, punto de control o servicio de protección) que da servicio a dicho organismo o entidad, si se conoce.
- Posibles instrucciones especiales de tramitación, como «entregar en mano», «abrir sólo por…», etc.

El sobre exterior llevará la identificación y dirección del órgano de control de destino, o en su defecto el del organismo o entidad destinatario, así como un número de referencia de paquete (número de expedición) a efectos de control de transmisión. En su interior se incluirá, además del sobre interior con la información a transmitir (o sobres, si van varios a un mismo órgano de control de destino), el recibo de transporte de material clasificado, con relación de la información clasificada remitida, que habrá de devolverse al remitente firmado y sellado por el responsable del órgano de control de destino.

Los envoltorios que contienen los envíos de información se inspeccionarán a su recepción, para comprobar que no han sufrido manipulaciones. Cualquier manipulación se tratará como una **violación de la protección**.

Cuando el destino sea común, se podrán agrupar en un mismo sobre externo todos los internos dirigidos a dicho destino, de cualquier grado de clasificación, excepto aquellos clasificados de grado «SECRETO o equivalente», que irán en un sobre exterior específico.

Para la remisión de la información de grado «SECRETO o equivalente», en el sobre interior deberá figurar obligatoriamente la identificación de la persona o cargo concreto destinatario y, en el sobre exterior, la del jefe de seguridad del órgano de control destinatario.

En el caso anterior, cuando el sobre interior esté dirigido a un destinatario específico y lleve la anotación de «Personal» o «Abrir sólo por…» o análoga, deberá ser abierto, en presencia del OCC del órgano de control destinatario, por el propio interesado a quien va dirigida la información. El acuse de recibo de la información clasificada (recibo de remitente de material clasificado) será firmado en este caso,

también por el OCC, cuya firma estará reconocida. Al ser información clasificada imputable, se adjuntará y cumplimentará únala correspondiente ficha de control y acceso a información clasificada, como evidencia objetiva de estos accesos.

6.4. Tratamiento de los escritos de remisión

En muchas ocasiones se suele enviar información clasificada precedida de un oficio, carátula de fax o escrito de remisión, asignándosele una referencia nueva propia del remitente y distinta a la propia y específica de la información clasificada transmitida, cuando se ve claramente que esta última es verdaderamente la información que se quiere transmitir y la que debe estar sujeta a control. En estos casos es conveniente seguir unas pautas fijas y comunes de actuación, siempre que sea posible, que se indican a continuación:

- Cuando se envíe una información clasificada que tenga su referencia propia se tratará en lo posible de no añadir escritos de remisión. Se hará uso de los recibos de remitente y de transporte para incluir las instrucciones precisas para su tratamiento en destino.
- Cuando sea absolutamente preciso incluir un escrito de remisión (cualquier oficio, carátula de fax, escrito, etc.), se procurará no incluir información clasificada en el mismo. El escrito de remisión, en este caso, llevará la clasificación que le corresponda por agregación, pero con una **marca adicional de limitación**, similar a: «escrito no clasificado cuando esté separado del anexo», debajo de la marca de clasificación inferior.
- La referencia del escrito de remisión será la que figure en los recibos de paquetería o valija y en los libros en entrada y salida.
- A efectos de registro de información clasificada controlada a cargo en los órganos de control, se registrará la referencia propia de la información clasificada remitida, con indicación en observaciones de la referencia del escrito de remisión.
- En caso de que sea necesario hacer comentarios de carácter clasificado referidos a una información clasificada, se enviará un escrito distinto, con su propia identificación de registro de información clasificada, en lugar de incluir dichos comentarios en el oficio de remisión que acompaña a la información clasificada referida. Esta práctica señalada permite mantener la trazabilidad de cada información por separado y facilita el correcto control y registro de ambas, especialmente cuando el originador de cada información clasificada es distinto.

Es importante que los jefes de seguridad de los órganos de control instruyan convenientemente, sobre estos aspectos, a todo el personal responsable de generar

escritos y autorizar la transmisión de información clasificada, en el organismo o entidad al que sirven.

6.5. Transportes por territorio nacional

6.5.1. Dentro de un mismo recinto o edificio

Las informaciones clasificadas con grado de clasificación «CONFIDENCIAL o equivalente» o inferior, pueden ser transportados en mano por una persona con habilitación de seguridad del grado apropiado, en sobre cerrado, maletín o en una carpeta, que no permita ver su contenido. No se necesita una autorización formal por escrito. Se emitirán los correspondientes recibos de acuerdo con lo que se señala posteriormente, en el **apartado 7**.

Las informaciones clasificadas con grado de clasificación «RESERVADO o equivalente» o superior, serán transportadas por el personal de los órganos de control, con los mismos criterios de actuación.

6.5.2. Transporte fuera de un mismo recinto o edificio, pero en territorio nacional

Siempre que se realice el transporte de información clasificada fuera del perímetro de un mismo recinto o edificio, se deberán cumplir los requisitos indicados en los apartados anteriores (empaquetado, remisión, recepción, etc.). El transporte de la información clasificada deberá realizarse por alguno de los siguientes medios y de acuerdo a los requisitos establecidos para cada uno de ellos:

- **Correo autorizado (también denominado valija conducida)**. Servicio de carácter oficial **constituido, de forma permanente, por personal funcionario o empleado del estado,** con nivel de habilitación adecuado a la información transportada, instruido específicamente para este cometido y siendo portador de una autorización de correo, personal, que podrá ser permanente durante el destino en este servicio. La información de grado «RESERVADO o equivalente» e inferior, podrá transmitirse por este servicio. La información nacional de grado SECRETO podrá ser transportada por este servicio cuando el jefe de seguridad del que dependa el servicio central de protección de información clasificada del remitente lo autorice expresamente. La información de grado «equivalente a SECRETO», correspondiente a otros estados u organizaciones internacionales, normalmente será transportada por el servicio de valija conducida exterior del Registro Central, salvo que puntualmente y de forma expresa el jefe de éste autorice a otro.

- **Valija militar (estafeta militar) o gubernamental, no conducida**. La información nacional con grado de clasificación RESERVADO, y toda la información de grado «CONFIDENCIAL o equivalente» o inferior, puede ser transportada por este servicio. Dado que la valija no es conducida, se extremarán las medidas de preparación de contenedores, sobres y paquetería para evitar y detectar su posible manipulación. Los receptores de la información deberán inspeccionar detenidamente las valijas recibidas para detectar cualquier posible manipulación, e informar de ello, en caso de que se produzca dicho evento, como una violación de la protección.
- **Servicio comercial acreditado de correo y de transporte**. El servicio es prestado por una empresa que ha sido acreditada por la ANPIC, por lo que dispone de una Habilitación de seguridad de empresa (HSEM) y se reconoce su capacidad para transportar información clasificada de forma segura y conforme a la normativa, sea del tipo documento o mercancía. Dichos servicios podrán ser utilizados para el transporte de información clasificada de grado «RESERVADO o equivalente» o inferior, siempre y cuando el transportista se encuentre acreditado por la ANPIC para la realización de dicho servicio en el grado necesario. Las empresas acreditadas para la prestación de este servicio **deberán figurar inscritas en un registro específico de la ANPIC**.
- **Transporte personal**. La información clasificada con grado «CONFIDENCIAL o equivalente» o inferior, puede ser transportada por una persona con habilitación de seguridad del grado apropiado, y la autorización correspondiente, formal y por escrito, del jefe de seguridad del órgano de control de quien dependa, cuando esté autorizada su circulación. En el ámbito industrial esta autorización irá obligatoriamente como certificado de correo. Se seguirán las normas que más adelante se especifican para el transporte personal, en el **apartado 6.7** de esta norma. Con carácter limitado podrá autorizarse de igual forma el transporte personal de información con grado «RESERVADO o equivalente» (hasta diez documentos máximo, como norma general). Para el transporte personal nacional de información clasificada con grado «DIFUSIÓN LIMITADA o equivalente», no es necesaria habilitación de seguridad, ni autorización expresa, siempre que se haga en el cumplimiento de cometidos oficiales y no existan limitaciones a su circulación.
- **Transporte de mercancías clasificadas acompañado por correo**. Se rige por los mismos criterios de autorización y tiene las mismas limitaciones que el transporte personal. Se produce principalmente en el ámbito industrial, cuando la información clasificada a transportar constituye una mercancía, y por tanto precisa de medios específicos de transporte para llevar dicha carga a su destino, no haciéndose uso de un servicio de correo y transporte comercial acreditado, sino de medios propios o contratados. En la norma NS/06 de la ANPIC sobre seguridad industrial se

explica su uso y requisitos. Únicamente se cita la necesidad de que en el transporte vaya acompañado por un correo, responsable de la mercancía clasificada. Este tipo de transporte es extrapolable y utilizable en la Administración y Fuerzas Armadas, aunque se explique en detalle en el ámbito industrial.

– **Servicio comercial de correo y transporte, con capacidad de seguimiento y trazabilidad de los envíos**. La información de grado «CONFIDENCIAL o equivalente» e inferior, podrá remitirse por medio de estos servicios, viajando de «incógnito», es decir, que no se declara al transportista el carácter de información clasificada de la documentación o mercancía transportada. La empresa que presta el servicio debe ser de solvencia probada y haber sido aprobada por la ANPIC para prestar este servicio, por lo que **deberá figurar inscrita en un registro específico de la ANPIC**. No precisa disponer de HSEM, ni ser acreditada por tanto. Debe proporcionar trazabilidad de los transportes, verificable por el usuario en cualquier momento y por medios sencillos (acceso por Internet), permitiéndole hacer un seguimiento continuo del estado del envío en tiempo real.
– **Servicio estatal de correos**. La información de grado «DIFUSIÓN LIMITADA o equivalente» e inferior, podrá remitirse por correo nacional certificado.

Transporte Nacional	SECRETO O EQUIVALENTE	RESERVADO O EQUIVALENTE	CONFIDENCIAL O EQUIVALENTE	DIFUSION LIMITADA O EQUIVALENTE
VALIJA CONDUCIDA	Registro Central o Servicio Central de Protección	SÍ	SÍ	SÍ
VALIJA NO CONDUCIDA MILITAR O GUBERNAMENTAL	NO	Sólo RESERVADO	SÍ	SÍ
SERVICIO COMERCIAL ACREDITADO DE CORREO Y DE TRANSPORTE	NO	SÍ	SÍ	SÍ
TRANSPORTE PERSONAL O DE MERCANCÍAS (con HPS y autorización)	NO	Con carácter limitado (10 doc.)	SÍ	SÍ
SERVICIO COMERCIAL CON TRAZABILIDAD DE ENVÍO	NO	NO	SÍ	SÍ
TRANSPORTE PERSONAL O DE MERCANCÍAS (sin HPS ni autorización)	NO	NO	NO	SÍ
SERVICIO CORREO ESTATAL (por correo certificado)	NO	NO	NO	SÍ

6.6. Transportes con el extranjero

Siempre que se realice el transporte de información clasificada fuera del territorio nacional, se deberán cumplir los requisitos indicados en los apartados anteriores, relativos a empaquetado, remisión, recepción, etc. El transporte de la información clasificada deberá realizarse por alguno de los siguientes medios y de acuerdo a los requisitos establecidos para cada uno de ellos:

- **Correo autorizado (valija conducida), militar o diplomático, oficialmente constituido para este cometido**. Se rige por los mismos criterios indicados en el apartado anterior, especialmente en lo referido al grado de clasificación, con los siguientes condicionantes:

  a) Sólo podrán realizar este servicio internacional los correos autorizados constituidos expresamente por el Ministerio de la Presidencia, por el Ministerio de Asuntos Exteriores y de Cooperación o por el Ministerio de Defensa.
  b) Las valijas o contenedores serán precintados por su emisor, y llevarán un sello oficial que, reconocido por las autoridades aduaneras de los países de paso, acredite su contenido y facilite su tránsito. No obstante, las autoridades aduaneras podrán exigir la apertura del envío, en cuyo caso, el responsable del correo deberá intentar que sólo se inspeccione la carátula de los documentos y que la inspección la efectúe un responsable aduanero policial en un lugar discreto, en presencia del correo. En cualquier caso, se exigirá de las autoridades aduaneras la emisión de la correspondiente diligencia que acredite la apertura del envío. A la mayor brevedad posible se dará parte de la incidencia al órgano responsable del servicio de valija.
  c) La información de grado «equivalente a SECRETO», correspondiente a otros estados u organizaciones internacionales, será transportada por el servicio de valija conducida exterior del Registro Central.

- **Valija diplomática, o militar, no conducida**. El Ministerio de Asuntos Exteriores y de Cooperación y el Ministerio de Defensa, respectivamente, son responsables de la constitución y funcionamiento de estos servicios, especialmente en lo referido a la protección de la información clasificada. La información nacional con grado de clasificación RESERVADO, y toda la información de grado «CONFIDENCIAL o equivalente» o inferior, puede ser transportada por este servicio. Las valijas o contenedores serán precintados por su emisor, y llevarán un sello oficial que, reconocido por las autoridades aduaneras de los países de paso, acredite su contenido y facilite su tránsito. Dado que la valija no es conducida, se extremarán las

medidas de preparación de contenedores, sobres y paquetería para evitar y detectar su posible manipulación. Los receptores de la información deberán inspeccionar detenidamente las valijas recibidas para detectar cualquier posible manipulación, e informar de ello, en caso de que se produzca dicho evento, como una violación de la protección. Los responsables del servicio adoptarán las medidas necesarias para restringir el envío de información clasificada cuando haya evidencia de violaciones de la protección, en tanto se corrigen las causas y se restablece la seguridad del servicio.

- **Servicio comercial acreditado de correo y de transporte**. Definido anteriormente. Dichos servicios podrán ser utilizados para el transporte internacional de información clasificada de grado «RESERVADO o equivalente» o inferior, siempre y cuando el servicio de correo comercial se encuentre acreditado por la ANPIC para la realización de dicho transporte internacionalmente, o ésta haya reconocido su acreditación por una ANS de otro país.
- **Transporte personal**. La información «DIFUSIÓN LIMITADA o equivalente» puede ser transportada por una persona, con o sin habilitación de seguridad, instruida en su manejo, y con la autorización correspondiente, formal y por escrito, del jefe de seguridad del órgano de control de quien dependa. Con ocasión de asistencia a una reunión o actividad clasificada realizada en el extranjero, o bien por estar específicamente contemplado en las instrucciones de seguridad de un programa, o por urgencia u oportunidad operativa, se podrá autorizar a una persona, con habilitación de seguridad adecuada, a transportar información con grado de clasificación «CONFIDENCIAL o equivalente» incluido, siempre en un número limitado (hasta diez documentos máximo, como norma general). Con carácter excepcional, por iguales motivos, se podrá autorizar el transporte personal, por una persona con habilitación de seguridad adecuada, a transportar información con grado de clasificación «RESERVADO o equivalente» (hasta tres documentos máximo, como norma general). En ambos casos se debe asegurar que se cumplen las instrucciones para el transporte personal incluidas en el **apartado 6.7** de esta norma y, asimismo, se tendrá en cuenta:

  a) El portador debe estar provisto de un **certificado de correo** (según formato publicado en la página «web» de la ONS, en inglés o en español según las circunstancias) con sello oficial del Registro Central, documento que debe estar reconocido por todos los países del ámbito de información de que se trate, que le autorice a transportar información clasificada, para acreditar su condición ante cualquier control policial o aduanero que pretenda la apertura de la cartera o maleta. Los jefes de seguridad de los subregistros principales o de servicios centrales o generales de protección, solicitarán al Registro Central los certificados

de correo con sello oficial que precisen, siendo éstos los únicos válidos para esta función. En determinados ámbitos, programas o contratos, internacionales se podrán utilizar otros modelos específicamente autorizados y reconocidos en la normativa de seguridad aplicable.

b) Los jefes de seguridad de los órganos de control serán los **oficiales de autorización** que firman los certificados de correo para el transporte en mano de información con grado de clasificación «CONFIDENCIAL o equivalente». Para grado «RESERVADO o equivalente» deberá firmar como oficial de autorización el jefe de seguridad del subregistro principal o secundario, o del servicio central o general de protección del que dependa, salvo de empresas contratistas. El Jefe del Registro Central podrá autorizar con su firma cualquier certificado de correo. Para las empresas contratistas podrán asumir las competencias de oficial de autorización los responsables de la administración más directamente implicados en los proyectos o programas (por ejemplo, el jefe del órgano de control de la oficina del programa) en que participan las mismas.
c) A la finalización de la actividad para la que se emitió, se devolverá el certificado de correo al órgano de control que lo autorizó, junto con la documentación complementaria generada (documentos de envío y declaración final), debidamente cumplimentada.
d) El portador no viajará por vía terrestre a través de países que sean ajenos al tipo o ámbito de la información transportada, ni sobrevolará o navegará por países que representen riesgos para la seguridad. En caso de duda, la ANPIC determinará qué países se incluyen en esta categoría.
e) En el documento de la ONS denominado «OR-ASIP-04-02. Orientaciones para el uso de recibos y certificados de correos», se describen los criterios para el uso, confección y tramitación de estos certificados de correo.

- **Transporte de mercancías clasificadas acompañado por correo**. Definido anteriormente a nivel nacional, también puede ser utilizado a nivel internacional, cuando se autorice por el propietario de la información. Se rige por los mismos criterios de autorización y tiene las mismas limitaciones que el transporte personal internacional.
- **Servicio comercial de correo y transporte, con capacidad de seguimiento y trazabilidad de los envíos**. Definido anteriormente a nivel nacional, también puede ser utilizado a nivel internacional, cuando la capacidad de seguimiento y trazabilidad de la empresa que presta el servicio alcance hasta el destinatario final y puntos de paso.
- **Servicios estatales de correos**. La información de grado «DIFUSIÓN LIMITADA o equivalente» e inferior, podrá remitirse por correo certificado a través de servicios de correos internacionalmente reconocidos.

Transporte internacional	SECRETO O EQUIVALENTE	RESERVADO O EQUIVALENTE	CONFIDENCIAL O EQUIVALENTE	DIFUSION LIMITADA O EQUIVALENTE
VALIJA CONDUCIDA	Ver condiciones arriba	SÍ	SÍ	SÍ
VALIJA NO CONDUCIDA DIPLOMÁTICA O MILITAR	NO	Sólo RESERVADO	SÍ	SÍ
SERVICIO COMERCIAL ACREDITADO DE CORREO Y DE TRANSPORTE	NO	SÍ	SÍ	SÍ
TRANSPORTE PERSONAL O DE MERCANCÍAS (con HPS y autorización)	NO	Con carácter excepcional (3 doc.)	Con carácter limitado (10 doc.)	SÍ
SERVICIO COMERCIAL CON TRAZABILIDAD DE ENVÍO	NO	NO	SÍ	SÍ
TRANSPORTE PERSONAL O DE MERCANCÍAS (sin HPS y con autorización)	NO	NO	NO	SÍ
SERVICIO CORREO ESTATAL (por correo certificado)	NO	NO	NO	SÍ

6.7. Instrucciones para la realización del transporte personal

Por transporte personal se entenderá el realizado por una persona que, **sin ser éste su cometido oficial**, es específicamente autorizada, y transporta directamente la información clasificada, bajo su continua supervisión. El material clasificado a transportar deberá ser de tal tamaño, peso y configuración que pueda ser llevado en mano.

Dado el especial riesgo que este tipo de transporte lleva asociado, por la falta de una dedicación habitual a estos cometidos por el portador, es necesario dar unas instrucciones precisas de obligado cumplimiento en su ejecución.

Como norma general se deberá tratar de hacer un ejercicio de previsión, de forma que, si es posible, toda aquella información clasificada de grado «CONFIDENCIAL o equivalente» o superior, que se prevea vaya a ser necesario utilizar en una actividad en otro emplazamiento, especialmente en el extranjero, se remita con la antelación suficiente por canales seguros al órgano responsable de la seguridad de la información del evento u otro próximo acreditado, de forma que el personal participante pueda recoger dicha información una vez en el destino.

En ningún caso se autorizará ni realizará un transporte personal de información de grado «SECRETO o equivalente».

Cuando con motivo de asistencia a una actividad o reunión clasificada en otro emplazamiento, especialmente en el extranjero, se prevea o conozca que durante la misma se va a hacer entrega en mano de información clasificada al asistente, para su transporte personal de regreso, se le proveerá en origen del correspondiente certificado de correo, que devolverá a su regreso, junto con la información clasificada recibida, al órgano de control responsable.

Cuando dicha entrega de información clasificada no esté prevista y, aún así, se haga entrega de ella al representante español participante, éste notificará al oficial de seguridad del evento la conveniencia de transmitir dicha información por un canal aprobado, no estando autorizado a hacer el transporte personal, salvo que no haya otra vía posible, en cuyo caso deberá proveerle de una autorización formal (si es en el extranjero: certificado de correo con sello oficial, debidamente relleno), que avale al portador en su transporte personal, y deberá entregarle asimismo la información debidamente empaquetada y precintada. En otro caso, no se recogerá la información, devolviéndola al oficial de seguridad.

Cuando haya que hacer uso del transporte personal, se debe asegurar el cumplimiento de las siguientes condiciones:

a) El transporte es conforme con los circuitos de distribución de la información clasificada definidos en el **apartado 5** de esta norma.
b) Se ha expedido la autorización necesaria para el transporte, con las formalidades requeridas según el grado de clasificación de la información a transportar y el tipo de transporte (nacional o internacional). Según el caso, podrá ser en forma de certificado de correo, autorización formal, o no ser precisa autorización.
c) El portador dispone de habilitación de seguridad, cuyo grado de clasificación, tipo y especialidad se adecuan a la información que va a transportar.
d) Los materiales clasificados a transportar se registran en el órgano de control del que dependa el usuario, tanto a la ida como a la vuelta.
e) Los materiales clasificados a transportar, tanto a la ida como a la vuelta, van en un sobre precintado preparado por el órgano de control, y en el interior de una cartera o maleta cerrada con llave, provista de una etiqueta de identificación personal.
f) El portador no se separa de la información, salvo cuando la deposite en un lugar seguro (órgano de control exterior, u otros designados) y no los deja sin vigilancia en el lugar de alojamiento, ni en los medios de transporte. Si el portador estima que hay condiciones adecuadas y no existen riesgos, podrá depositar información de grado «DIFUSIÓN LIMITADA o equivalente» o inferior, en cajas de seguridad de los hoteles o en las consignas, dentro de sobres precintados, que impidan intuir el contenido y permitan detectar su posible manipulación.

g) Los documentos no se leen en lugares públicos, como aviones, trenes, autobuses, restaurantes, estaciones, aeropuertos, etc.
h) El portador ha sido instruido y conoce las normas de seguridad a adoptar durante el transporte, dando fe con su firma en una **declaración de instrucción**.

6.8. Transporte entre Bruselas y Madrid

El Registro Central tiene establecido un servicio periódico de valija conducida exterior, para el transporte de información clasificada controlada de OTAN y UE, entre Bruselas y Madrid. Como norma general, no se utilizará este servicio para la remisión de información de grado «DIFUSIÓN LIMITADA o equivalente» o inferior, salvo por razón de oportunidad, debidamente acreditada.

Cuando sea preciso el transporte de información de grado «equivalente a SECRETO» a otros destinos fuera del entorno de Bruselas, el Jefe del Registro Central autorizará los servicios extraordinarios de valija conducida exterior que sean necesarios. Igualmente se podrá autorizar cuando, por urgencia, sea preciso el transporte inmediato de información «equivalente a RESERVADO», no existiendo otra vía de transmisión adecuada.

7. RECIBOS

7.1. Concepto de uso

El recibo es un mecanismo de control que permite garantizar el correcto transporte de la información, dejando evidencia objetiva de los cambios de responsabilidad que se van produciendo en la custodia de la información transmitida a lo largo del transporte.

El uso de recibos no eximirá a los órganos de control remitente y destinatario de la anotación de los movimientos en los registros de entrada y salida respectivos, ni de la actualización de los registros de información clasificada controlada.

En un mismo transporte se pueden utilizar hasta tres tipos diferentes de recibos, cada uno con un cometido específico, que son:

a) Recibo de remitente de material clasificado.
b) Recibo de transporte de material clasificado.
c) Recibo de valija o libro de entrega.

7.2. Recibo de remitente de material clasificado

Todo transporte de información clasificada que contenga información de grado «RESERVADO o equivalente» o superior, dirigida nominalmente a una persona o cargo concreto, por ser esta información imputable, requerirá la existencia de un recibo denominado recibo de remitente de material clasificado, por cada destinatario, que incluya la identificación de la información clasificada imputable dirigida a ese destinatario. Este recibo **irá dentro del sobre interior**, junto a la información a la que refiere.

Este tipo de recibo no será necesario para aquellos paquetes que contengan información de grado «CONFIDENCIAL o equivalente» o inferior, salvo que éste sea requerido por el remitente.

En el recibo constarán los datos de referencia, número de ejemplar o copia e idioma de los documentos, y será devuelto al remitente una vez haya sido fechado, sellado y firmado por el destinatario. Un modelo de este recibo se encuentra publicado en la página «web» de la ONS.

Cuando ambos, remitente y destinatario, sean órganos de control, u organismos o entidades a los que estos sirven, es decir, no vaya dirigida la información clasificada a una persona o cargo concretos, no será preciso el uso de recibo de remitente de material clasificado, cumpliendo dicha función el propio recibo de transporte de material clasificado.

7.3. Recibo de transporte de material clasificado

Con independencia de lo reflejado en el apartado anterior, cuando se transporte información clasificada de grado «CONFIDENCIAL o equivalente» o superior, entre órganos de control de la estructura nacional, incluidos los exteriores, irá acompañada de un recibo denominado recibo de transporte de material clasificado, donde se reflejan el número de expedición y la identificación de los documentos que ampara.

El órgano de control remitente confeccionará al menos un recibo por órgano destinatario. Si se estima oportuno, se relacionará también en dicho recibo la información de grado «DIFUSIÓN LIMITADA o equivalente» o inferior, transmitida al mismo destinatario. Este recibo estará fuera de los sobres interiores e **irá dentro del sobre exterior**.

Cuando el transporte se vaya a realizar a través del servicio de valija conducida exterior del registro central, toda la información remitida, clasificada o no, irá relacionada en dichos recibos.

El recibo será devuelto al órgano de control remitente una vez haya sido fechado y firmado por el responsable del órgano de control destinatario. Un modelo de este recibo se encuentra publicado en la página «web» de la ONS.

Estos recibos permiten conocer el movimiento de la información clasificada controlada, y establecer en cada momento la responsabilidad en su custodia, dando evidencia objetiva de su correcto transporte.

En caso de información con clasificación «equivalente a SECRETO», dirigida a un destinatario específico, los paquetes que la contengan llevarán en su cubierta interior una nota indicando que sólo podrá ser abierto por el individuo a quien va dirigido, y los recibos podrán ser firmados únicamente por el oficial de control COSMIC/TOP SECRET o su suplente. Este recibo una vez firmado y fechado por el órgano de control destinatario, servirá de documento de descarga de la responsabilidad de su custodia al órgano de control remitente.

7.4. Recibo de valija o libro de entrega

Cuando se envíen paquetes con información clasificada mediante un servicio de transporte ajeno a los propios órganos de control, estos paquetes llevarán un número de expedición exterior y los datos de la identificación y dirección del órgano de control destinatario, o en su defecto el del organismo o entidad destinatario.

Irán acompañados de un recibo de valija o, en su defecto, irán relacionados en un libro de entrega. En ellos se refleja el número de expedición y destinatario de cada paquete transportado. Un modelo de recibo de valija se encuentra publicado en la página «web» de la ONS.

El servicio, o servicios, responsable del transporte recabará la firma e identificación exacta de cada uno de los receptores, intermedios o final, que han participado en el transporte, como evidencia objetiva de los cambios de responsabilidad en su custodia que se han producido hasta la entrega final.

En cada una de las entregas que se realicen hasta llegar al punto de destino, es responsabilidad del que efectúa la entrega verificar que el receptor está debidamente autorizado e identificado para hacerse cargo de los paquetes y asegurar que se cumplimentan los datos correspondientes en el recibo de valija o libro de entrega, siendo el último de ellos el responsable de hacer la entrega en el lugar especificado como destino final (sede del órgano de control, organismo o entidad destinatario).

8. CONTROL, ALMACENAMIENTO Y CUSTODIA DE LA INFORMACIÓN CLASIFICADA

8.1. Generalidades

La seguridad de la información clasificada implica una eficaz implementación y cumplimiento de la normativa de seguridad vigente, en todos sus aspectos. Las medidas específicas de seguridad de la información son insuficientes sin el concurso de los otros aspectos de la seguridad, en concreto, la seguridad física, la seguridad en el personal, la seguridad en los sistemas de información y comunicaciones, la seguridad industrial o la seguridad criptológica.

Tendremos un adecuado control, almacenamiento y custodia de la información clasificada, cuando todos estos aspectos anteriores se apliquen de forma correcta y coordinada.

En los anteriores apartados se ha hablado del sistema de registro, y de la distribución y transmisión de la información clasificada, que son elementos de manejo que están directamente relacionados con el control y custodia de dicha información. En este sentido, se puede afirmar que la primera medida de control y custodia de la información clasificada es su correcto registro, es decir, saber que existe y quién es responsable de su custodia en cada momento. Cuando esté almacenada y custodiada dicha información en un órgano de control o por persona autorizada, así como cuando esté siendo transmitida, se deben cumplir los requisitos de protección que se mencionan en las normas de la ANPIC.

La información clasificada de grado «CONFIDENCIAL o equivalente» o superior, se manejará y almacenará, con las limitaciones que le afecten, en zonas de acceso restringido (ZAR), que deberán estar organizadas y estructuradas de acuerdo con lo señalado en la norma NS/03 de la ANPIC sobre seguridad física, configuradas y acreditadas como áreas de seguridad clase I o clase II, según corresponda.

La información clasificada de grado «DIFUSIÓN LIMITADA o equivalente», deberá manejarse y almacenarse en zonas administrativas de protección, que deberán estar organizadas y estructuradas de acuerdo con lo señalado en la norma NS/03 de la ANPIC sobre seguridad física.

En todo momento se debe garantizar la **compartimentación** de la información clasificada, de forma que se pueda asegurar el cumplimiento del principio de la «necesidad de conocer», tanto por el grado de clasificación, como por el tipo de información (nacional, OTAN, etc.), como por la pertinencia del acceso. En este

sentido, durante el caso concreto del almacenamiento, se tendrán en cuenta los siguientes aspectos de seguridad:

- **Información clasificada de un mismo tipo y de diferentes grados**. Se mantendrá una estricta compartimentación de la información clasificada de grado «SECRETO o equivalente» del resto, sin excepción posible. Esta compartimentación también es necesaria para grado «RESERVADO o equivalente», por lo que se llevará a efecto cuando no exista un motivo muy fundado para no hacerlo. Para «CONFIDENCIAL o equivalente» es conveniente y se aconseja. Para «DIFUSIÓN LIMITADA o equivalente», no es necesario establecer la compartimentación.
- **Información clasificada de diferentes tipos**. Se archivará por tipo de información, no autorizándose bajo ningún aspecto la mezcla de información clasificada de distintos tipos de grado «CONFIDENCIAL o equivalente» o superior. Para información «DIFUSIÓN LIMITADA o equivalente» es conveniente y se aconseja mantener la compartimentación.

Si por diferente «necesidad de conocer» es aconsejable la segregación de accesos, se hará uso de contenedores de seguridad distintos. Si las personas que acceden tienen la misma necesidad, se podrá hacer uso de estantes separados dentro del mismo contenedor.

Estas medidas facilitan en gran manera el control de la información y la actuación en caso de emergencia (evacuación o destrucción por prioridades). En caso de inspecciones evitan que se pueda acceder a información no autorizada (por ejemplo, una inspección de la Unión Europea).

La información clasificada puede ser almacenada en sistemas de información y comunicaciones y en soportes informáticos, siempre que el sistema se encuentre acreditado y esté autorizado por la autoridad competente, de forma que en su protección se garanticen medidas de seguridad no menos rigurosas que para los documentos sobre papel u otros soportes físicos. Estos sistemas han de asegurar igualmente, **de forma física o lógica**, la compartimentación indicada en los párrafos anteriores, así como cuanto se indica en la normativa específica sobre modos seguros de operación de los sistemas.

Todos los soportes externos o removibles, en caso de contener información clasificada, estarán marcados para el grado máximo de clasificación alguna vez contenida, y tendrán la **consideración de documentos**. Si es información clasificada controlada estarán identificados de forma unívoca, registrados en el órgano de control del que dependan y, cuando se constituyan como un medio de almacenamiento, irán acompañados de un listado de contenido o fichero que detalle, como

mínimo, la relación nominal de documentos de grado «RESERVADO o equivalente» o superior, que contiene.

Los soportes fijos (discos duros internos, discos ópticos, etc.) en que se maneje información clasificada controlada, estarán igualmente marcados, localmente registrados y controlados, conforme al grado máximo de clasificación de la información que hayan podido contener. Aunque fijos, están sujetos a procesos de sustitución por avería, o de enajenación del sistema, o lo que supone un mayor riesgo, de reutilización posible en otra función. En estos casos siempre se hará un borrado seguro del soporte.

A continuación se indican otras medidas generales a adoptar en función del grado de clasificación de la información manejada, que no han sido aún contemplados o no son objeto de otra norma específica, y que conviene resaltar por su importancia.

8.2. Información clasificada de grado «SECRETO o equivalente»

La información clasificada de grado «SECRETO o equivalente» sólo podrá ser custodiada por los órganos de control expresamente autorizados para el manejo de información clasificada de dicho grado y del mismo tipo (nacional, OTAN, UE, etc.). Dicha autorización implica que el órgano de control ha implantado unas medidas y procedimientos de protección acordes a la normativa y éstos han sido acreditados por la autoridad competente.

Bajo ningún concepto quedarán materiales clasificados de este grado en posesión de un usuario fuera de un órgano de control autorizado, o de una zona de acceso restringido acreditada a dicho nivel y controlada por éste, con la excepción establecida para el transporte por correo autorizado.

El Registro Central tendrá un control permanente e individualizado sobre cada documento o material no documental de grado «equivalente a SECRETO» existente en España, manteniendo un registro actualizado de su ciclo de vida (creación, recepción, distribución y destrucción). Podrá establecer en todo momento el órgano de control donde está depositado cada documento. Cada subregistro principal responde ante el Registro Central de toda la información clasificada de dicho grado que esté a su cargo directo, o de un órgano de control subordinado.

Los servicios centrales de protección de información clasificada llevarán el mismo control respecto a la información clasificada de grado SECRETO.

De forma análoga actuará cualquier órgano de control con la información clasificada de grado «SECRETO o equivalente», que esté a su cargo o de un órgano subordinado.

Cualquier variación (alta, transmisión, destrucción) en la situación de la información clasificada de este grado de clasificación será realizada a través del Registro Central o del servicio central de protección, según corresponda.

Todos los órganos de control informarán puntualmente, por el canal reglamentario, al Registro Central de cualquier incidencia producida en la información clasificada de grado «equivalente a SECRETO» (CTS, TS-UE/EU-TS, etc.) a su cargo, o al servicio central de protección del que dependa cuando afecte a información clasificada de grado SECRETO.

En el caso de tratarse de información manejada en un sistema de información y comunicaciones, el responsable de operación del sistema informará puntualmente, a efectos de registro, al órgano de control del que dependa sobre cualquier información clasificada de grado «SECRETO o equivalente» que se haya creado, recibido o transmitido. Asimismo, dado que se trata de información clasificada imputable, el responsable de gestión de la seguridad del sistema supervisará, e informará al OCC del órgano de control, que se crean y mantienen correctamente los registros o «logs» de acceso, que contienen la relación nominal fechada de todos los accesos realizados a la información de dicho grado.

La información clasificada de grado «SECRETO o equivalente», que se extraiga del sistema de información y comunicaciones, en cualquier tipo de soporte, deberá ser custodiada y registrada por el órgano de control autorizado, de acuerdo con lo establecido en estas normas.

Cuando un usuario reciba información clasificada de grado «SECRETO o equivalente» fuera de los canales establecidos, deberá poner inmediatamente el hecho en conocimiento del órgano de control de que dependa, al objeto de su remisión al Registro Central o servicio central de protección, según corresponda, para que se proceda a su registro, control y alta en la red, quedando así regularizada su situación.

Al menos una vez al año todos los órganos de control realizarán un inventario de toda la información clasificada de grado «SECRETO o equivalente» existente en la red a su cargo, incluidos los soportes informáticos removibles. Adicionalmente, de forma periódica los órganos de control realizarán chequeos de verificación.

A este respecto, un documento o material no documental de grado «SECRETO o equivalente» queda correctamente verificado por un órgano de control cuando se produzca alguna de las siguientes circunstancias:

a) Se constata visualmente su existencia, su correcto registro, y la no existencia de reproducciones, extractos o traducciones no autorizadas del mismo,
b) se guarda un acuse de recibo del órgano de control autorizado al que ha sido transferido el documento o material no documental,
c) se guarda un certificado de destrucción del mismo, o
d) se guarda una orden de reducción de la clasificación o de desclasificación del documento.

Dentro del mes de enero de cada año, los órganos de control autorizados para dicho grado de clasificación remitirán, por el canal jerárquico de protección, al Registro Central o servicio central de protección, según corresponda, el listado de información clasificada de grado «SECRETO o equivalente» a su cargo.

Salvo en casos muy excepcionales y expresamente autorizados por la ANPIC, las empresas contratistas no podrán tener información clasificada de grado «SECRETO o equivalente» en sus instalaciones. El acceso a dicha información, si lo precisan, deberán realizarse en las instalaciones autorizadas de la oficina de programa/proyecto u órgano equivalente de la parte oficial contratante.

8.3. Información clasificada de grado «RESERVADO o equivalente»

La información clasificada de grado «RESERVADO o equivalente» deberá ser custodiada por los órganos de control expresamente autorizados para el manejo de información clasificada de dicho grado o superior. Dicha autorización implica que el órgano de control ha implantado unas medidas y procedimientos de protección acordes a la normativa y éstos han sido acreditados por la autoridad competente. Asimismo, con autorización del jefe de seguridad del órgano de control responsable de su custodia, esta información podrá ser manejada y, con carácter limitado, almacenada, en una zona de acceso restringido acreditada a dicho nivel y controlada por el órgano de control.

De forma puntual y con carácter limitado, en horario de **presencia laboral del usuario**, y autorizado por el jefe de seguridad del órgano de control custodio, información clasificada de este grado podrá quedar en posesión de un usuario fuera del órgano de control o zona de acceso restringido acreditada. Las condiciones de seguridad serán evaluadas, de forma que el riesgo asumido sea mínimo y aceptable. El usuario será informado de las obligaciones de custodia continua de la información cedida y de devolución al órgano de control si se ausenta.

Los subregistros principales tendrán control sobre todos los documento clasificados de grado «equivalente a RESERVADO» existente en el organismo o entidad

al que da servicio, manteniendo un registro actualizado de su ciclo de vida (creación, recepción, distribución y destrucción). Podrá establecer en todo momento el órgano de control subordinado donde está depositado cada documento. Cada subregistro principal responde ante el Registro Central de toda la información clasificada de dicho grado que esté a su cargo directo, o de un órgano de control subordinado.

Respecto a la información clasificada de grado RESERVADO, los servicios centrales de protección de información clasificada, llevarán el mismo tipo de control y con similares criterios

Análogas responsabilidades asume cada órgano de control respecto a la información clasificada de grado «RESERVADO o equivalente», que esté a su cargo o de sus órganos subordinados.

Se exceptúan de todo lo anterior aquella información clasificada que se maneje al amparo de lo expresado en el **apartado 4.8** sobre casos especiales, de esta norma.

Todos los órganos de control informarán a su órgano de control superior de cualquier incidencia producida en la información clasificada de grado «RESERVADO o equivalente» a su cargo. Cuando sea pertinente, se elevará al Registro Central o servicio central de protección, según corresponda.

En el caso de tratarse de información manejada en un sistema de información y comunicaciones, el responsable de operación del sistema informará puntualmente, a efectos de registro, al órgano de control del que dependa sobre cualquier información clasificada de grado «RESERVADO o equivalente» que se haya creado, recibido o transmitido. Asimismo, dado que se trata de información clasificada imputable, el responsable de gestión de la seguridad del sistema supervisará, e informará al órgano de control, que se crean y mantienen correctamente los registros, o «logs» de acceso, que contienen la relación nominal fechada de todos los accesos realizados a la información de dicho grado.

La información clasificada de grado «RESERVADO o equivalente», que se extraiga del sistema de información y comunicaciones, en cualquier tipo de soporte, deberá ser custodiada y registrada por el órgano de control autorizado del que dependa, de acuerdo con lo establecido en estas normas.

Cuando un usuario reciba información clasificada de grado «RESERVADO o equivalente» fuera de los canales establecidos, deberá poner inmediatamente el hecho en conocimiento del órgano de control de que dependa al subregistro principal o

servicio central de protección, según corresponda, para que efectúe su registro, control y alta en la red, quedando así regularizada su situación.

Al menos una vez al año todos los órganos de control realizarán un inventario de toda la información clasificada de grado «RESERVADO o equivalente» existente en la red a su cargo, incluidos los soportes informáticos removibles. Adicionalmente, de forma periódica los órganos de control realizarán chequeos de verificación.

A este respecto, un documento o material no documental de grado «RESERVADO o equivalente» queda correctamente verificado por un órgano de control cuando se produzca alguna de las siguientes circunstancias:

a) Se constata visualmente su existencia y correcto registro,
b) se guarda un acuse de recibo del órgano de control al que ha sido transferido el documento o material no documental,
c) se guarda un certificado de destrucción del mismo, o
d) se guarda una orden de reducción de la clasificación o desclasificación del documento.

Dentro del mes de enero de cada año, los órganos de control remitirán, por el canal jerárquico de protección, el listado de información clasificada de grado «RESERVADO o equivalente» a su cargo. Cada órgano de control refundirá la información propia y la recibida de los órganos subordinados.

Al final y dentro del mismo mes, toda la información llegará a los subregistros principales y servicios centrales de protección, según corresponda.

8.4. Información clasificada de grado «CONFIDENCIAL o equivalente»

La información clasificada de grado «CONFIDENCIAL o equivalente» deberá ser custodiada por los órganos de control expresamente autorizados para el manejo de información clasificada de dicho grado o superior. Dicha autorización implica que el órgano de control ha implantado unas medidas y procedimientos de protección acordes a la normativa y éstos han sido acreditados por la autoridad competente. Asimismo, con autorización del jefe de seguridad del órgano de control responsable de su custodia, esta información podrá ser manejada y almacenada en una zona de acceso restringido acreditada a dicho nivel y controlada por el órgano de control.

Mediante autorización por el jefe de seguridad del órgano de control custodio, podrá quedar información clasificada de este grado en posesión de un usuario

fuera del órgano de control o zona de acceso restringido acreditada. Las condiciones de seguridad serán evaluadas, de forma que el riesgo asumido sea mínimo y aceptable. El usuario será informado de las obligaciones de custodia que asume.

Cada órgano de control es responsable del registro y control de toda la información clasificada de grado «CONFIDENCIAL o equivalente», que esté a su cargo, con las excepciones previstas para la información clasificada que se maneje al amparo de lo expresado en el anexo IV sobre mensajes clasificados.

La información clasificada de grado «CONFIDENCIAL o equivalente», que se extraiga de un sistema de información y comunicaciones, en cualquier tipo de soporte, deberá ser custodiada y registrada por el órgano de control autorizado del que dependa, de acuerdo con lo establecido en estas normas.

El responsable de operación del sistema informará periódicamente, a efectos de registro, al órgano de control del que dependa sobre cualquier información clasificada de grado «CONFIDENCIAL o equivalente» que se haya creado, recibido o transmitido.

Cuando un usuario reciba información clasificada de grado «CONFIDENCIAL o equivalente» fuera de los canales establecidos, deberá entregarla del órgano de control de que dependa, para registro y control.

Al menos una vez al año todos los órganos de control realizarán un inventario de toda la información clasificada de grado «CONFIDENCIAL o equivalente» existente a su cargo, incluidos los soportes informáticos removibles, no siendo necesaria su remisión al órgano superior. Adicionalmente, de forma periódica los órganos de control realizarán chequeos de verificación.

A este respecto, un documento o material no documental de grado «CONFIDENCIAL o equivalente» queda correctamente verificado por un órgano de control cuando se produzca alguna de las mismas circunstancias que se indicaban para el grado «RESERVADO o equivalente».

9. REPRODUCCIÓN, TRADUCCIÓN Y EXTRACTO DE LA INFORMACIÓN CLASIFICADA

9.1. Introducción

Con la finalidad de evitar la reproducción o copia incontrolada de información clasificada, así como las traducciones y extractos, se establecen una serie de

medidas por las que se regula dicha actividad, de manera que no se realice más que cuando sea estrictamente necesario y en la forma que se establece en esta norma.

Cada órgano de control es responsable del registro y control de las copias, traducciones y extractos que realice, informando al órgano superior cuando sea información clasificada imputable. En el caso de empresas contratistas, también existe la obligación de informar en el caso de información clasificada de grado «CONFIDENCIAL o equivalente».

Todas las copias, traducciones y extractos deberán quedar perfectamente identificadas, de forma unívoca y exclusiva. Para ello, lo normal será añadir a la referencia del documento un número de copia, traducción o extracto, sucesivo y diferente para cada una que se realice del mismo documento. Este número deberá figurar en el registro que se haga del nuevo documento creado.

Para mantener la trazabilidad de las numeraciones de copias, traducciones o extractos, que se vayan realizando, se deben seguir unos criterios concretos y conocidos, que permitan identificar al documento fuente, el órgano que realiza la copia, traducción o extracto, y el orden consecutivo que le corresponde.

Las reproducciones y traducciones **se registrarán y numerarán como un documento clasificado más** y tienen la misma consideración que el original. A efectos de control de la documentación, no existen diferencias entre original y copia.

Las reproducciones o copias, traducciones y extractos de información clasificada, siempre se realizarán bajo la estricta observación del principio de la «necesidad de conocer», aplicándose a los nuevos documentos generados las mismas medidas de seguridad que se aplican al original, y prestando especial atención a aquellas generadas sobre sistemas y soportes informáticos.

La normativa de desarrollo que se cita en el **apartado 3.8** de esta norma, incluirá con mayor detalle el tratamiento de las copias, traducciones y extractos.

9.2. Información clasificada de grado «SECRETO o equivalente»

La información clasificada de grado «SECRETO o equivalente» no podrá ser reproducida. En caso de necesitarse copias extras de una información determinada, éstas deberán ser solicitadas a la organización internacional, estado, organismo, o departamento ministerial, propietarios, a través del Registro Central o servicios centrales de protección, según corresponda.

Sólo en circunstancias excepcionales, con previa autorización del organismo propietario, se podrán realizar copias, traducciones o extractos, y exclusivamente por el Registro Central o servicio central de protección. El Registro Central, en el ámbito de su competencia, asignará a cada copia, traducción o extracto un número propio de Registro Central, único y diferente, distinto al asignado al documento original.

9.3. Información clasificada de grado «RESERVADO o equivalente»

Como norma general las copias de información clasificada de grado «RESERVADO o equivalente» se realizarán en el subregistro principal o en el servicio central o general de protección, quienes proveerán a los órganos de control subordinados de los ejemplares que puedan necesitar, debidamente numerados. Si fueran necesarias más copias, se procurará que sean realizadas por el mismo subregistro principal o servicio central o general de protección.

Los jefes de seguridad de los órganos de control subordinados (excepto en empresas contratistas) podrán realizar copias y autorizar extractos o traducciones, cuando sea necesario por motivos de trabajo y sean autorizados por el subregistro principal o el servicio central o general de protección, para uso exclusivo por la organización a la que sirven.

A cada copia, traducción o extracto se le asignará una referencia de copia, traducción o extracto, adicional a la referencia del documento de origen, y será convenientemente registrada. La referencia a asignar deberá ser consensuada con el órgano de control superior, de forma que no pueda haber documentos con iguales referencias. A la mayor brevedad posible se deberá regularizar su situación, informando al órgano superior para control y registro.

En el caso de empresas contratistas, los jefes de seguridad de los órganos de control, si cuentan con autorización previa expresa del órgano de control de la administración contratante del que dependen funcionalmente, podrán realizar copias, traducciones o extractos, pero nunca autorizar su realización a personal de la empresa.

Los órganos de control informarán puntualmente al órgano superior de las copias, traducciones y extractos realizados de información clasificada de grado «RESERVADO o equivalente».

Los subregistros principales y los servicios centrales de protección recibirán periódicamente, para su control y registro, las relaciones de las copias, traducciones

y extractos de grado «RESERVADO o equivalente» efectuados por los órganos de control subordinados. Al Registro Central no se le remitirá esta información.

9.4. Información clasificada de grado «CONFIDENCIAL o equivalente»

Los jefes de seguridad de los órganos de control, podrán autorizar las reproducciones o copias, traducciones o extractos de información clasificada de grado «CONFIDENCIAL o equivalente», cuando así sea necesario por motivos de trabajo, asegurándose de que a cada copia, traducción o extracto se le asigna un número de documento, o de copia, traducción o extracto, y que estos quedan convenientemente registrados. No será necesaria la comunicación al órgano de nivel superior, excepto en el ámbito empresarial, en que es preceptiva la comunicación al órgano superior del que depende el contratista.

9.5. Información clasificada de grado «DIFUSIÓN LIMITADA o equivalente»

Las reproducciones o copias, traducciones y extractos de información clasificada de grado «DIFUSIÓN LIMITADA o equivalente», podrán ser realizadas por el usuario siempre que se asegure su control de forma que no se produzcan accesos no autorizados a aquellas.

10. DESTRUCCIÓN O ARCHIVO DE LA INFORMACIÓN CLASIFICADA

10.1. Generalidades

Con objeto de evitar una acumulación excesiva de información clasificada que dificulte su pronta localización y su explotación eficaz, se propondrá la destrucción de aquella que los usuarios juzguen inútil o haya quedado obsoleta, en cuanto sea posible, y siempre en conformidad con los criterios que el Sistema Español de Archivos, que se regula por Real Decreto 1708/2011, disponga, conforme más adelante se indica.

El Sistema Español de Archivos establece la existencia de Comisiones Calificadoras de Documentos Administrativos, que serán los órganos que resuelvan sobre la eliminación o conservación permanente de documentos.

En tanto no exista una regulación normativa adecuada, la información clasificada que, por resolverse su conservación permanente, deba transferirse a un archivo superior (archivo general, central, intermedio o histórico), solo podrá ser transferi-

da en caso de que dicho archivo superior disponga de un órgano de control para custodia y registro de dicha información.

En el ámbito empresarial, los órganos de control de empresas contratistas, en ningún caso podrán destruir información clasificada controlada recibida de la Administración. Cuando no les sea necesaria su conservación la transmitirán al órgano de control de la administración responsable de dicha información.

Los órganos de control, así como los usuarios principales de la información clasificada, llevarán a cabo una revisión continua de esta para determinar la conveniencia de su destrucción y proponer la misma. Es responsabilidad del jefe de seguridad del órgano de control, supervisar que los usuarios revisen con regularidad la información que manejan, para evitar así la tendencia a acumularla.

En el caso de información clasificada de interés general, sin destinatarios o usuarios específicos, y que permanece depositada en un órgano de control sin utilizarse, será el jefe de seguridad del órgano de control, quien decidirá y autorizará su destrucción, siempre y cuando esté autorizado para el grado de clasificación concernido y se haga en conformidad con los criterios del Sistema Español de Archivos.

La destrucción de información clasificada se realizará con controles exhaustivos en dicho proceso y deberá ser efectuada de forma que se imposibilite su reconstrucción total o parcial. Estos controles se aplicarán con igual criterio sea un documento clasificado original o se trate de una copia, traducción o extracto.

Dadas sus especiales características, la destrucción de material no documental que constituya información clasificada se hará por procedimientos específicos, en función de su naturaleza y uso. Los planes de protección de los órganos e instalaciones en que se manejen estos materiales clasificados deberán contemplar los procedimientos de destrucción utilizables con cada material específico.

En adelante, aunque sólo se tratará de procedimientos para la destrucción de la documentación clasificada, en cualquier formato y soporte, los criterios de responsabilidad y control en su ejecución que se establecen, son válidos también para materiales no documentales clasificados.

Se excluye de esta norma la destrucción de emergencia de documentos y material no documental clasificados, tema que debe ser contemplado en los planes de protección de cada órgano o instalación en que se maneje información clasificada, aunque en ocasiones puedan coincidir los procedimientos de destrucción. Ello no exime de que en caso de destrucción de emergencia de información clasificada,

se informe a la mayor brevedad del evento, y se contabilice y regularice la situación de la información clasificada destruida de manera inmediata, una vez cesadas las circunstancias excepcionales que lo motivaron.

La documentación clasificada deberá ser destruida por procedimientos de incineración, reducción a pulpa, trituración en tiras o pulverización. La información grabada sobre soportes informáticos deberá, siempre que sea posible, ser borrada o sobrescrita mediante procedimientos aprobados por la autoridad competente (el Centro Criptológico Nacional – CCN -, en España), como paso previo a la destrucción del dispositivo sobre el que se encuentra almacenada.

Los borradores, extractos, copias o registros que se hayan generado como paso necesario para la creación de la información clasificada, se destruirán por los mismos procedimientos, sin precisar levantar acta de su destrucción.

El Jefe del Registro Central, o del servicio central de protección, está facultado para cursar instrucciones a los subregistros principales, o a los servicios generales de protección subordinados, respectivamente, para que cualquier órgano de control proceda a la destrucción inmediata de determinada información clasificada, dentro siempre de sus ámbitos de responsabilidad.

Para la destrucción de información clasificada se establecen unos criterios, según su grado de clasificación, que han de servir de orientación a los jefes de seguridad a la hora de proceder.

10.2. Destrucción según grado

10.2.1. Información clasificada de grado «SECRETO o equivalente»

La información clasificada de grado «SECRETO o equivalente» únicamente puede ser destruida bajo control del Registro Central o servicio central de protección, según corresponda. Cuando cualquier órgano de control necesite destruir un documento, solicitará su traslado al Registro Central o servicio central de protección, acompañado del original de la **ficha de control y acceso a información clasificada**, de la que se quedará con una copia. Esta circunstancia, se anotará en el libro de registro correspondiente. Si constan datos de identificación del documento en archivos informáticos, se deberá incluir una referencia a su destrucción.

A criterio del Registro Central o servicio central, la destrucción podrá realizarse «in situ», sin precisar su traslado, para lo cual deberá desplazarse el responsable de certificar la destrucción.

El Registro Central, o servicio central de protección, procederá a la destrucción del documento y levantará acta (según formato publicado en la página «web» de la ONS), firmada por el Jefe del Registro Central (y oficial de control COSMIC/TOP SECRET), o jefe de seguridad del servicio central de protección, y por otro testigo oficial de la destrucción, preferiblemente con destino en órgano distinto, que deberá estar habilitado para tener acceso a información clasificada de dicho grado.

10.2.2. Información clasificada de grado «RESERVADO o equivalente»

Excepto en las empresas contratistas, la destrucción de la información clasificada de grado «RESERVADO o equivalente» puede realizarse bajo control de los subregistros principales y secundarios, o servicios generales de protección, según corresponda, y por los puntos de control o servicios locales de protección que ellos autoricen.

Se levantará acta de la destrucción, firmada por el jefe de seguridad del órgano de control y por un testigo oficial con grado de habilitación adecuado en vigor, siendo aconsejable que dicho testigo no pertenezca al órgano de control que efectúe la destrucción.

En la página «web» de la ONS se encuentra disponible un modelo de acta de destrucción para este grado.

Los órganos de control informarán puntualmente al órgano superior de la destrucción de información clasificada de grado «RESERVADO o equivalente».

Los subregistros principales y los servicios centrales de protección recibirán periódicamente, para su custodia, control y registro, los originales de las actas de destrucción y de las fichas de control y acceso a información clasificada de los documentos clasificados de grado «RESERVADO o equivalente» destruidos por los órganos de control subordinados, que conservarán copia de dichas actas y fichas. Al Registro Central no se le remitirá esta información.

10.2.3. Información clasificada de grado «CONFIDENCIAL o equivalente»

La destrucción de la información clasificada de grado «CONFIDENCIAL o equivalente» puede realizarse bajo control de cualquier órgano de control, excepto en el ámbito empresarial, según se indicó anteriormente.

El jefe de seguridad certificará con su firma e identificación inequívoca, en el correspondiente libro de registro, anotándose el acto y la fecha de la destrucción.

Si el registro se realiza en un sistema informático, o si se estima más conveniente para un adecuado control que la simple anotación en el libro de registro, se levantará acta de la destrucción, firmada por el jefe de seguridad. No se precisa la firma de ningún testigo, ni informar al órgano superior.

En la página «web» de la ONS se encuentra disponible un modelo de acta de destrucción para este grado.

10.2.4. Información clasificada de grado «DIFUSIÓN LIMITADA o equivalente»

La información clasificada de grado «DIFUSIÓN LIMITADA o equivalente» podrá ser destruida directamente por el órgano de control o el usuario que la tiene asignada, siempre y cuando esta destrucción se realice por un método de los autorizados en esta norma o en otra específica de la autoridad competente (CCN, si se trata de información contenida en sistemas o soportes informáticos o de comunicaciones), excepto en el ámbito empresarial, según se indicó anteriormente. No se precisa registrar dicha destrucción en libro o acta alguna, ni informar al órgano de control, salvo indicación en otro sentido.

La información clasificada de grado «DIFUSIÓN LIMITADA o equivalente» podrá ser destruida directamente por los jefes de seguridad de los órganos de control de los contratistas, caso de tener constituida dicha estructura de protección, o por el responsable de seguridad del contratista, si no existe ésta, sin que se precise en ningún caso, de un testigo oficial.

10.3. Procedimientos de destrucción

10.3.1. Generalidades

Los documentos y el material de desecho clasificado, tales como borradores, ejemplares deteriorados y documentos de trabajo, serán destruidos por los procedimientos de incineración, reducción a pulpa, trituración en partículas (micro-corte) o pulverización. Los residuos así obtenidos no deben permitir la identificación o reconstrucción siquiera parcial de la documentación, por lo que se aconseja destruir simultáneamente varios documentos. El jefe de seguridad ha de inspeccionar tanto el método como las operaciones de destrucción de forma periódica.

10.3.2. Trituradoras de corte en partículas

Las partículas resultantes, en función del grado de clasificación de la documentación a destruir, tendrán las siguientes **dimensiones máximas** de corte:

- Grado «SECRETO o equivalente»: 0,8 mm. x 12,0 mm. (nivel P-6 de la norma DIN 66399, con restricción de ancho de corte a 0,8 mm.), o 1,0 mm. x 5,0 mm. (nivel P-7, sin restricción).
- Grado «RESERVADO o equivalente»: 1,5 mm. x 20 mm. (nivel P-5 de la norma DIN 66399, con restricción de ancho de corte a 1,5 mm.).
- Grado «CONFIDENCIAL o equivalente», o inferior: ancho de corte hasta 2,0 mm. máximo y longitud hasta 20 mm. máximo, sin superar un área de 30 mm2 (nivel P-5 de la norma DIN 66399, sin restricción). Son válidos, por ejemplo, los cortes: 1,5 mm. x 20 mm, y 2,0 mm. x 15 mm.

Las trituradoras podrán accionarse manualmente y estarán construidas de forma que ningún documento introducido en la máquina quede intacto al final de la operación. Se deberán destruir simultáneamente varios documentos, con igual tipo de papel, aunque algunos no sean clasificados. Al final de cada operación se removerá el producto final, para dificultar su identificación y reconstrucción.

10.3.3. Trituradoras compactas

Deben permitir la amalgama de los desechos clasificados mediante desfibrado. La pulpa residual se desintegrará y se desfibrará con el fin de que sea imposible reconstruir e identificar la documentación. Se tendrá prevista la instalación de un sistema de cierre que quede bloqueado por medio de un candado doble, para proteger la tolva o cualquier otra abertura que dé acceso al depósito del aparato.

10.3.4. Incineradores

Se utilizarán para destruir los desechos de documentación clasificada, introducidos en sacas o bolsas precintadas. Las aberturas que permitan acceder a los desechos o a las cenizas durante o después de la combustión, deberán precintarse o cerrarse bajo candado, salvo que esté bajo supervisión continua por personal autorizado. Las cenizas residuales deberán tener un peso inferior al 5% del desecho vertido al incinerador y no permitir la identificación siquiera parcial de la documentación sometida al proceso de destrucción.

10.3.5. Destrucción de material informático

La información grabada sobre soportes informáticos deberá, siempre que sea posible, ser borrada o sobrescrita con procedimientos aprobados por el CCN, como paso previo a la destrucción del dispositivo sobre el que se encuentra almacenada.

Como métodos para su destrucción se sugieren los siguientes:

a) Cintas magnéticas: Deberán ser cortadas mecánicamente con los dispositivos apropiados, destruidas químicamente o mediante incineración. En este último caso deberán ser cortadas en pequeños trozos previamente a su introducción en el incinerador.
b) Disquetes: Los disquetes serán extraídos de su cubierta de plástico, cortados en pequeñas piezas e incinerados.
c) CD-ROM, DVD, etc.: Serán cortados en pequeñas piezas mediante la utilización de los dispositivos mecánicos adecuados, siendo sometidos posteriormente a incineración.
d) Discos duros y extraíbles: Se procederá a la extracción de las carcasas de los soportes que contienen las superficies magnéticas donde se encuentra almacenada la información, procediéndose a continuación a la eliminación de la superficie magnética mediante la utilización de papel de lija u otro dispositivo abrasivo.
e) Dispositivos de almacenamiento tipo «*pendrive*», tarjetas o circuitos integrados: Se procederá a su machacado con martillo, o cortado, según su naturaleza. Los restos serán incinerados.

10.4. Conservación de libros de registro, fichas de control y acceso a información clasificada y actas de destrucción

Las actas de destrucción y fichas de control y acceso a información clasificada originales de la información clasificada destruida de grado «SECRETO o equivalente», se conservarán en el Registro Central o servicio central de protección, según corresponda, durante un mínimo de **diez (10) años**. El órgano de control responsable de la destrucción se quedará con copia del acta de destrucción y de las fichas de control y acceso a información clasificada durante el mismo periodo de tiempo.

Las actas de destrucción y fichas de control y acceso a información clasificada originales de la información clasificada destruida de grado «RESERVADO o equivalente», se conservarán en los subregistros principales o servicios centrales de protección, según corresponda, durante un mínimo de **cinco (5) años**. Los órganos de control responsables de la destrucción conservarán durante el mismo periodo de tiempo las copias correspondientes.

Los libros de registro o actas de destrucción de la información clasificada destruida de grado «CONFIDENCIAL o equivalente» se conservarán por los órganos de control responsables de la destrucción durante un periodo mínimo de **tres (3) años** desde la última anotación efectuada.

11. COMPROMETIMIENTO DE LA INFORMACIÓN CLASIFICADA

11.1. Generalidades

Un **comprometimiento** (violación o fallo) de la protección de la información clasificada ocurre como resultado de una acción u omisión contraria a la normativa de seguridad, o por un fallo en los sistemas o medidas de protección, que puede suponer que aquella caiga, completa o en parte, en manos de persona no autorizada, e incluso, sin llegar a ocurrir tal cosa, que las circunstancias hayan ocasionado la simple posibilidad de que tal evento hubiera ocurrido.

También tendrán la consideración de comprometimiento los ataques contra la integridad o disponibilidad de la información clasificada, especialmente en el ámbito de los sistemas de información y comunicaciones.

Diremos que la información clasificada ha resultado **comprometida** cuando, como resultado de un comprometimiento de la protección, bien se ha producido una posibilidad de acceso a la misma por persona no autorizada y no puede determinarse de forma fehaciente que tal acceso no se haya producido, o bien se ha perdido el control sobre dicha información, por ejemplo por su pérdida, sustracción o indisponibilidad.

Por «persona no autorizada» se entenderá cualquiera que no cumpla los requisitos de acceso a determinada información clasificada, por lo que incluye también al personal de la propia organización (por ejemplo, personal que no tiene necesidad de conocer sobre un determinado asunto clasificado).

Todo usuario de información clasificada está obligado a informar inmediatamente a su oficial o responsable de seguridad, por el canal adecuado, de cualquier comprometimiento que pueda conocer.

Tras ser informado, el oficial o responsable de seguridad:

- Adoptará de manera inmediata las medidas necesarias en orden a restablecer la seguridad y a prevenir situaciones similares a la sucedida.
- Informará inmediatamente al jefe o responsable del organismo o entidad al que pertenece.
- Realizará una investigación preliminar para clarificar los hechos y responsabilidades y valorar en una primera estimación el daño potencial causado. En el menor plazo notificará todo ello, junto con las medidas iniciales adoptadas, a las autoridades apropiadas.
- Deberá determinar si la información clasificada ha resultado comprometida. Si este fuera el caso, informará también al jefe del órgano de control supe-

rior del que dependa. Se tomarán conjuntamente las medidas apropiadas, de acuerdo con las normas, para que se pueda informar al originador de la información comprometida, o al propietario, si no fuera el mismo.

11.2. Investigación y actuaciones complementarias

Cada comprometimiento del que se informe, deberá ser investigado por personal con experiencia en seguridad, en investigación y, si fuera necesario, en contrainteligencia. Dicho personal deberá ser independiente del que se haya visto involucrado en la violación o fallo. Su cometido será determinar:

a) Si la información clasificada ha resultado comprometida.
b) Si las personas no autorizadas que hayan podido tener acceso a la información tienen una HPS y son de tal fiabilidad y honradez que se puede suponer que no existe un riesgo de que se vaya a realizar un uso no autorizado de tal información.
c) Las medidas correctivas o disciplinarias que se estiman necesarias adoptar.

Cuando la investigación resulte en una respuesta positiva en los puntos a) y b) anteriores, el responsable de seguridad tomará los pasos necesarios para instruir a las personas concernidas sobre la protección de la información a la que tuvieron acceso y las responsabilidades asumidas. Si la información concernida es de grado «CONFIDENCIAL o equivalente» o inferior y no ha habido mayor amenaza, el responsable de la investigación podrá cerrar el caso sin ser necesario proponer el informar a la máxima autoridad competente, sino únicamente a su escalón superior en la estructura nacional de protección, quien decide si se escala o no a niveles superiores.

Cuando la investigación resulte en una respuesta positiva en el punto a) y una respuesta negativa en el punto b), se informará a la máxima autoridad competente, por el conducto reglamentario, del comprometimiento acaecido.

En el ámbito de la seguridad industrial, las empresas contratistas y, en particular, su personal responsable en materia de protección de la información clasificada, se abstendrán de realizar por cuenta propia investigaciones o actuaciones complementarias, debiendo esperar a recibir instrucciones detalladas por parte de los órganos responsables en la Administración.

11.3. Tramitación a la autoridad competente

La máxima autoridad competente para información clasificada procedente de organizaciones internacionales, de organizaciones multinacionales o de los acuer-

dos de protección de la información clasificada con otros países, será la ANPIC, a través de la ONS.

Para la información clasificada nacional, la máxima autoridad competente será aquella que determine cada departamento ministerial como responsable máximo de la seguridad de la información clasificada en dicho ministerio, a través del servicio central de protección de la información clasificada correspondiente.

Cuando la información afectada sea de categoría especial: CRIPTO, SIGINT, inteligencia, etc., se informará paralelamente a la correspondiente autoridad para dicha información: Autoridad Nacional de Distribución de Cifra, Autoridad Nacional SIGINT, Autoridad Nacional de Inteligencia, etc., en conformidad con las normas particulares que al respecto pudieran haber dictado dichas autoridades.

Todos los informes y comunicaciones relativos a comprometimientos de seguridad se canalizarán a través de los canales de la estructura nacional de protección de la información clasificada, con independencia de la comunicación de dichas actuaciones a los responsables en los canales jerárquicos de mando.

El plazo para la tramitación de la comunicación de un comprometimiento, del que sea necesario informar a la autoridad competente conforme a los criterios indicados en el punto anterior, siempre será el más corto posible, especialmente cuando se estime que las implicaciones puedan ser más graves conforme a lo que se indica seguidamente.

En concreto, se comunicarán de forma inmediata, antes de iniciar cualquier actuación derivada, aquellos casos en que se determine que ha ocurrido alguno de los siguientes supuestos:

a) Información clasificada de grado «RESERVADO o equivalente» o superior, ha resultado comprometida.
b) Hay indicios claros o sospechas fundadas de actividades de espionaje.
c) La información ha sido filtrada a la prensa u otros medios de comunicación o difusión social, o estos han accedido a ella por otros medios.

Por «actividades de espionaje» se entenderá, en este contexto, cualquier acción desarrollada por un elemento externo o personal desleal interno, contra los intereses nacionales, con el objeto de obtener una información, o de alterar su integridad o disponibilidad, y conseguir una posición de ventaja.

Los informes de comprometimiento de información clasificada de grado «CONFIDENCIAL o equivalente» serán remitidos, caso de ser necesaria su tramitación, una vez la investigación haya sido completada. En este caso no deberá transcurrir más

de un mes, desde la fecha de ocurrencia del comprometimiento, sin que, al menos, un informe provisional sea remitido, aunque no hayan finalizado las actuaciones.

No es necesario informar de los comprometimientos de información clasificada de grado «DIFUSIÓN LIMITADA o equivalente», a menos que se encuentren dentro de los casos contemplados en los puntos b) o c) anteriores.

11.4. Contenido de los informes

Los informes iniciales que se realicen sobre un comprometimiento de la protección de la información clasificada abarcarán los siguientes puntos:

a) Una descripción de la información que se estima comprometida, incluyendo su clasificación de seguridad, referencia y número de copia, fecha, originador o propietario, asunto y destinatarios.
b) Una breve descripción de las circunstancias del comprometimiento, incluyendo la fecha, o rango de fechas, del suceso, tiempo estimado o conocido de exposición al riesgo, descripción de las personas o ámbitos que han podido tener acceso no autorizado.
c) Indicación de si el originador o propietario de la información ha sido ya informado.

Los informes posteriores completarán esta información con datos ya debidamente contrastados y darán detalles de las investigaciones y actuaciones realizadas o en curso, alcance estimado del comprometimiento, conclusiones extraídas, medidas finales adoptadas, así como de cualquier otro dato pertinente al caso.

De las investigaciones realizadas sobre cualquier violación o fallo de seguridad se guardarán los registros e informes de las actuaciones realizadas y medidas correctivas adoptadas, al menos durante tres años. Dichos registros e informes serán presentados durante las inspecciones de seguridad que se reciban.

En anexo V se incluye un modelo de **informe de comprometimiento** para su uso como informe inicial.

12. CESIÓN DE INFORMACIÓN CLASIFICADA

12.1. Generalidades

Se entiende por **cesión de información clasificada** la entrega de dicha información, que está bajo la custodia del que la cede, a un tercero. Por tercero, en

este contexto, se entiende un tercer estado, una organización internacional, etc., e incluso una persona representante de los mismos, que tiene la característica fundamental de ser ajeno a quien ostenta la propiedad de dicha información y, por tanto, no está de antemano autorizado a acceder a esta. No es cesión la distribución de la información a un órgano o persona, autorizado y sin la consideración de tercero, dentro del propio país u organización que ostenta la propiedad.

Tanto el estado, organización internacional o representante de los mismos que realiza la cesión de la información clasificada, como el que la recibe, reciben la denominación de «**partes»**. La parte transmisora es la que cede, o realiza la cesión, mediante la entrega de la información a la parte receptora, que es la que recibe la información, con los requisitos que se determinen.

Los mecanismos por los que se realiza la cesión de información clasificada deberán estar definidos para cada tipo de información de que se trate, bien en las respectivas reglamentaciones de seguridad de aplicación en cada caso, o bien en los acuerdos de protección legalmente establecidos que contemplen dicho aspecto.

12.2. Principios que rigen la cesión de información clasificada

La cesión de información clasificada debe cumplir unos requisitos mínimos:

- La cesión de información clasificada debe estar **motivada, suficientemente justificada y ser necesaria** desde el punto de vista de los intereses nacionales o internacionales a cuyo amparo se produce.
- Siempre estará amparada por un acuerdo previo de protección de la información clasificada entre las partes, aprobado por las autoridades responsables de estas, quienes deberán tener capacidad suficiente para establecer dicho acuerdo, en la forma de tratado internacional.
- Sólo se realizará la cesión si se tiene la **suficiente confianza** en que la protección y uso que se va a dar a dicha información, por parte del tercero que la recibe, es suficiente, conforme a lo acordado y con garantías adecuadas, de forma que el riesgo final sea asumible. Por ello la necesidad de la existencia de acuerdos previos de protección de la información clasificada.
- La cesión de información clasificada está **expresamente prohibida salvo autorización** por escrito del propietario de dicha información. En determinados casos, si fuera preciso por algún motivo concreto y previsto (derechos de propiedad intelectual, derechos de control sobre la cesión o exportación a terceros, u otros), será necesario también recabar la autorización del originador (si es que es distinto del propietario).

- La cesión de información clasificada se regirá por las normas específicas de seguridad que le sean de aplicación (reglamentos o normas de seguridad y acuerdos de seguridad, por los que se regula su protección), bien sean de ámbito nacional o internacional, que deberán ser conocidas antes de proceder a dicha cesión. En particular debe cumplirse lo especificado en este **apartado 12**. de la presente norma.
- En el ámbito de la seguridad industrial, los contratistas no podrán estar autorizados en ningún caso a la cesión de información clasificada con carácter general, siendo precisa la validación caso por caso de la correspondiente oficina de programa u órgano de contratación, según corresponda.
- Para cada ámbito o tipo de información deberá conocerse quien es la autoridad competente para autorizar la cesión de información clasificada. En el caso de información no nacional, vendrá determinada por la legislación, reglamentos, normas, instrucciones o acuerdos de seguridad por los que se rige su protección y uso. En el caso de información nacional, cada departamento ministerial debe tener establecido quién puede ostentar dicha competencia.

12.3. Autorizaciones de cesión

Las autorizaciones de cesión se deben realizar individualmente, tras un análisis caso por caso.

Las solicitudes de cesión de información clasificada deben identificar claramente:

- La información que va a ser cedida.
- País u organización internacional a quien se cede la información.
- El organismo o entidad concreto, al que se entregará la información.
- Una justificación detallada que motiva la solicitud de cesión.

La autoridad competente para autorizar la cesión de información clasificada (autoridad que habrá que determinar, conforme se indica en el apartado anterior), dictaminará por escrito, caso por caso, la resolución adoptada ante cada solicitud que reciba, siempre que se corresponda con su ámbito. Dicha resolución contendrá, aparte de la decisión adoptada, una fundamentación de esta.

ANEXO I A LA NS/04. GRADOS DE CLASIFICACIÓN EN ESPAÑA

1. MATERIAS CLASIFICADAS

1.1. Grado SECRETO

La clasificación de **SECRETO** se aplicará a la información que precise del más alto grado de protección, toda vez que su revelación no autorizada o utilización indebida pueda dar lugar a una amenaza o perjuicio extremadamente grave para los intereses de España en los siguientes ámbitos:

a) La soberanía e integridad territorial;
b) el orden constitucional y la seguridad del estado;
c) el orden público y la vida de los ciudadanos;
d) la capacidad de combate o la seguridad de las Fuerzas Armadas de España o de sus aliados;
e) la efectividad o la seguridad de operaciones de excepcional valor de los servicios de inteligencia de España o de sus aliados;
f) las relaciones diplomáticas de España o situaciones de tensión internacional, o
g) cualquier otro cuya salvaguarda requiera de la más alta protección.

1.2. Grado RESERVADO

La clasificación de **RESERVADO** se aplicará a la información que precise de un alto grado de protección, toda vez que su revelación no autorizada o utilización indebida pueda dar lugar a una amenaza o perjuicio grave para los intereses de España en los siguientes ámbitos:

a) El orden constitucional y la seguridad del Estado;
b) el orden público y la seguridad de los ciudadanos;
c) la capacidad de combate o la seguridad de las Fuerzas Armadas de España o de sus aliados;
d) la efectividad o la seguridad de operaciones de los servicios de inteligencia de España o de sus aliados;
e) las relaciones diplomáticas de España o situaciones de tensión internacional;
f) los intereses económicos o industriales de carácter estratégico, o
g) cualquier otro cuya salvaguarda requiera de un alto grado de protección.

2. MATERIAS DE RESERVA INTERNA

2.1. Grado CONFIDENCIAL

La clasificación de **CONFIDENCIAL** se aplicará a la información cuya revelación no autorizada o utilización indebida pueda causar una amenaza o perjuicio para los intereses de España en los siguientes ámbitos:

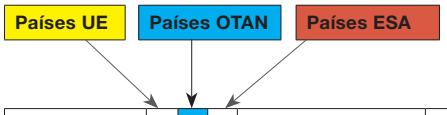
a) El efectivo desarrollo de las políticas del Estado o el funcionamiento del sector público;
b) negociaciones políticas o comerciales de España frente a otros Estados;
c) los intereses económicos o industriales;
d) funcionamiento de los servicios públicos;
e) dificultar la investigación o facilitar la comisión de delitos, o
f) cualquier otro que pueda causar una amenaza o perjuicio para los intereses de España.

2.2. Grado DIFUSIÓN LIMITADA

La clasificación de **DIFUSIÓN LIMITADA** se aplicará a la información cuya revelación no autorizada o utilización indebida pueda ser contraria a los intereses de España en cualquiera de los ámbitos relacionados en los apartados anteriores.

ANEXO II A LA NS/04. CUADROS DE EQUIVALENCIAS DE GRADOS DE CLASIFICACIÓN

Clasificación UE	Très Secret UE/ EU Top Secret	Secret UE/ EU Secret	Confidentiel UE/ EU Confidential	Restreint UE/ EU Restricted
Clasificación OTAN	COSMIC Top Secret	NATO Secret	NATO Confidential	NATO Restricted
Clasificación ESA	ESA Top Secret	ESA Secret	ESA Confidential	ESA Restricted



ALBANIA				Tepër Sekret	Sekret	Konfidencial	I Kufizuar
ALEMANIA				Streng Geheim	Geheim	VS[4]— Vertraulich	VS — Nur für den Dienstgebrauch
AUSTRIA				Streng Geheim	Geheim	Vertraulich	Eingeschränkt
BÉLGICA				Très Secret Zeer Geheim	Secret Geheim	Confidentiel Vertrouwelijk	-------[5]
BULGARIA				Строго секретно	Секретно	Поверително	За служебно ползване
CANADÁ				Top Secret Tres Secret	Secret Secret	Confidential Confidentiel	-------[5]
CHIPRE				Άκρως Απόρρητο Abr: (ΑΑΠ)	Απόρρητο Abr: (ΑΠ)	Εμπιστευτικό Abr: (ΕΜ)	Περιορισμένης Χρήσης Abr: (ΠΧ)
CROACIA				Vrlo Tajno	Tajno	Povjerljivo	Ograničeno
DINAMARCA				Yderst hemmeligt	Hemmeligt	Fortroligt	Til tjenestebrug
ESLOVAQUIA				Prísne tajné	Tajné	Dôverné	Vyhradené
ESLOVENIA				Strogo tajno	Tajno	Zaupno	Interno
ESPAÑA				Secreto	Reservado	Confidencial	Difusión Limitada
ESTADOS UNIDOS				Top Secret	Secret	Confidential	-------[5]
ESTONIA				Täiesti salajane	Salajane	Konfidentsiaalne	Piiratud
FINLANDIA				Erittäin salainen	Salainen	Luottamuksellinen	Käyttö rajoitettu
FRANCIA				Très Secret Défense	Secret Défense	Confidentiel Défense	--------[5]
GRECIA				Άκρως Απόρρητο Abr: ΑΑΠ	Απόρρητο Abr: (ΑΠ)	Εμπιστευτικό Abr: (ΕΜ)	Περιορισμένης Χρήσης Abr: (ΠΧ)
HOLANDA				STG Zeer Geheim	STG Geheim	STG Confidentieel	Departementaalvertrouwelijk
HUNGRÍA				Szigorúan titkos!	Titkos!	Bizalmas!	Korlátozott terjesztésű!
IRLANDA				Top Secret	Secret	Confidential	Restricted
ISLANDIA				Algert leyndarmal	Leyndarmal	Trunadarmal	Thjonustuskjal

[4] Alemania: VS = Verschlusssache.

[5] Bélgica, Canadá, EEUU y Francia no utilizan el grado de clasificación “RESTRICTED” en su sistema nacional. Bélgica, Canadá, EEUU y Francia manejan y protegen los documentos con grado “DIFUSIÓN LIMITADA o equivalente” acorde a sus leyes y reglamentos nacionales en vigor, que no son menos exigentes que lo establecido en las normativas de seguridad de OTAN, UE o ESA.

ITALIA				Segretissimo	Segreto	Riservatissimo	Riservato
LETONIA				Sevišķi slepeni	Slepeni	Konfidenciāli	Dienesta vajadzībām
LITUANIA				Visiškai slaptai	Slaptai	Konfidencialiai	Riboto naudojimo
LUXEMBURGO				Très Secret Lux	Secret Lux	Confidentiel Lux	Restreint Lux
MALTA				L-Ogħla Segretezza	Sigriet	Kunfidenzjali	Ristrett
NORUEGA				Streng Hemmelig	Hemmelig	Konfidensielt	Begrenset
POLONIA				Ściśle Tajne	Tajne	Poufne	Zastrzeżone
PORTUGAL				Muito Secreto	Secreto	Confidencial	Reservado
REINO UNIDO				Top Secret	Secret	-------[6]	Official-Sensitive
Rep. CHECA				Přísně tajné	Tajné	Důvěrné	Vyhrazené
RUMANÍA				Strict secret de importanţă deosebită	Strict secret	Secret	Secret de serviciu
SUECIA				Kvalificerat hemlig	Hemlig	Hemlig	Hemlig
SUIZA				Geheim	Geheim	Vertraulich	Vertraulich
TURQUÍA				Çok Gizly	Gizly	Özel	Hizmete Özel

[6] El Reino Unido no utiliza el grado de clasificación «UK CONFIDENTIAL» en su sistema nacional. Maneja y protege los documentos con grado «CONFIDENCIAL o equivalente» acorde a la normativa de seguridad nacional establecido para «UK SECRET».

ANEXO III A LA NS/04. TRATAMIENTO DE LOS MENSAJES CLASIFICADOS

1. DEFINICIÓN Y MANEJO

Por razones fundamentalmente de operativa diaria y de oportunidad, especialmente en el ámbito de asuntos exteriores, las Fuerzas Armadas, las Fuerzas y Cuerpos de Seguridad del Estado y los servicios de información, a menudo es preciso transmitir información clasificada en forma de mensajes.

El volumen de información transmitida en forma de mensajes se incrementa exponencialmente en situaciones de crisis, conflictos armados, despliegues de fuerzas o ejercicios, lo que, unido a la necesaria oportunidad de la información y en aras de la eficacia, aconseja la adopción de medidas extraordinarias que permitan afrontar estas situaciones, siempre que no constituya ello un riesgo no aceptable por la autoridad responsable del organismo o entidad.

Sería poco rentable un control exhaustivo de todo este tráfico por parte del sistema de registro, teniendo en cuenta el hecho de que, en los propios centros de mensajes de los centros de comunicaciones (CECOM), ya se lleva registro detallado. De igual modo, en los sistemas de mensajería acreditados para empleo directo por los usuarios, el propio sistema lleva o define el modo de registro de los mensajes tramitados.

Por ello se establece en este anexo un procedimiento especial de control por parte del sistema de registro para este tipo de información, en el que los mensajes, en función de su grado de clasificación, podrán tener un tiempo de demora antes de que se decida sobre su conservación como documentos o destrucción.

Un mensaje, a efectos de este anexo, es una comunicación entre dos o más autoridades, por la que se transmiten una información que suele tener, aunque no siempre es así, un plazo de validez temporal limitado, con ocasión de actividades que están en proceso, por lo que es de prever que el contenido de dicha comunicación pueda tener un ciclo de vida corto, y pueda ser destruido una vez superado dicho ciclo, o archivado en un expediente o bloque documental único junto con otros mensajes de la misma actividad.

Un expediente o bloque documental único de mensajes, a efectos de este anexo, es una compilación de mensajes en un solo conjunto, al que se asigna un grado de clasificación conforme a la agregación realizada y un número de registro específico, siendo registrado y manejado como un único documento clasificado a partir

de ese momento. Podrá llevar un índice de contenido, si se estima necesario, que será obligatorio al menos para la información de grado «RESERVADO o equivalente» contenida. Este compendio se hará en el soporte (papel, informático, etc.) que se estime más conveniente.

No tendrán consideración de mensaje cuando la transmisión incluya en el texto remitido, o como anexo, un documento clasificado ya registrado en origen como tal; en tal caso el texto o anexo se trataría conforme a los criterios generales de la norma, sin serle de aplicación lo establecido aquí.

Cuando se extraigan de un sistema los mensajes clasificados, pasando a un soporte externo en los locales del CECOM o del sistema de mensajería acreditado, se custodiarán conforme a las medidas de seguridad que establecen las normas de la ANPIC, y deberán contar con la autorización previa para ello del jefe de seguridad del órgano de control responsable.

Todos los mensajes de grado de clasificación «SECRETO o equivalente» se tratarán como documentos desde el primer momento de su recepción o preparación, no siéndoles de aplicación las normas especiales establecidas en este anexo para el resto de mensajes clasificados. Por tanto, se regirán por la normativa general.

Los procedimientos específicos que se describen en este anexo serán de aplicación a los mensajes clasificados de grado «RESERVADO o equivalente» o inferior, durante el primer mes natural desde su recepción, o transmisión. En caso de actividades u operaciones fuera de los asentamientos habituales de un organismo o entidad, este plazo se podrá aumentar hasta el periodo de duración de la actividad u operación realizada, siempre que lo autorice el jefe o responsable del organismo o entidad, asesorado por el jefe de seguridad del órgano de control responsable. Para cada actividad u operación se marcará previamente cuál es el **periodo autorizado**.

Si pasado este periodo un mensaje no ha sido destruido, pasará a considerarse como un documento clasificado o a incluirse en un expediente o bloque documental único, debiendo seguir a partir de ese momento los procedimientos generales de control y registro establecidos para cualquier información clasificada.

Todo organismo que disponga de un CECOM o sistema de mensajería acreditado, debe disponer igualmente de un órgano de control donde se registra la información clasificada que entra y sale, y donde se gestiona la destrucción de los soportes de almacenamiento (papel, cinta perforada, disco duro, disquete, u otros) de la información clasificada que cause baja. En el caso de un CECOM, este órgano de control puede formar parte del propio CECOM o ser un órgano separado.

El local donde se ubica el CECOM o sistema de mensajería acreditado, deberá estar acreditado como zona de acceso restringido, para el tipo y grado máximo de información clasificada que pueda ser manejada y almacenada en él. Entre otras medidas de seguridad, deberá disponer de mobiliario de seguridad y elementos de protección, de fortaleza suficiente para la información clasificada que esté bajo su custodia. Se exceptúan los casos en que, por estar desplegados con motivo de una actividad u operación fuera de los asentamientos permanentes, les son de aplicación las cautelas establecidas para instalaciones móviles en el **apartado 1** de la norma NS/03.

2. TRATAMIENTO DE LOS MENSAJES TRANSMITIDOS

Los mensajes para transmitir con propuesta de clasificación de grado «RESERVADO o equivalente» o «CONFIDENCIAL o equivalente», siempre que sea posible, se tramitarán primeramente a través del órgano de control, donde se procede a confirmar su clasificación y a su **registro temporal como mensajes clasificados**, y su posterior entrega al CECOM o sistema de mensajería acreditado para transmisión.

En caso de no estar disponible el órgano de control, el mensaje se trasmitirá directamente, con la clasificación propuesta. Una vez disponible aquel, si no ha transcurrido aún el periodo autorizado, se le entregará el mensaje, o un listado periódico de mensajes transmitidos en custodia, para su registro temporal. Un procedimiento particular elaborado por el jefe de seguridad del órgano de protección determinará la forma exacta de proceder en esta situación.

El originador de un mensaje con propuesta de clasificación de grado «RESERVADO o equivalente» o «CONFIDENCIAL o equivalente», salvo autorización y control del jefe de seguridad del órgano de control, no conservará copias en su poder. El CECOM o sistema de mensajería acreditado podrá mantener copias de los mensajes transmitidos, durante el periodo autorizado, por si fuera necesaria su retransmisión o repetición del envío. Los «*back-up*» podrán mantenerse más tiempo, según se indica más adelante.

Transcurrido el plazo del periodo autorizado, o antes si no fuera necesaria la demora, por parte del CECOM o sistema de mensajería acreditado se entregarán al órgano de control los mensajes y las copias contenidos en soportes externos (excepto «*back-up*» y aquellos que tiene autorización para destruir) y se borrarán de forma segura las copias contenidas en soportes internos.

Conforme a las instrucciones que reciba del organismo o entidad al que sirve, el jefe de seguridad del órgano de control procederá, con respecto a cada mensaje,

a su registro definitivo como documento, o a su destrucción conforme a la normativa, o a su archivo en un expediente o bloque documental único debidamente registrado y controlado.

Los mensajes que no precisen ser conservados de grado «CONFIDENCIAL o equivalente» o inferior, podrán ser destruidos en el propio CECOM o sistema de mensajería acreditado, junto con las copias y material borrador generado en cualquier soporte, anotando dicha destrucción, utilizando los procedimientos de destrucción aprobados. Los registros de destrucción se conservarán durante un mínimo de 3 años.

Los mensajes que pasen a ser documentos, a partir de su registro, se manejarán de acuerdo con las normas generales para el control de la información clasificada, comunicando su existencia al órgano de control superior en caso de clasificación de grado «RESERVADO o equivalente».

El órgano de control deberá supervisar el correcto cumplimiento de todos estos procesos, especialmente por parte del CECOM o sistema de mensajería acreditado y del originador.

3. TRATAMIENTO DE LOS MENSAJES RECIBIDOS

Los mensajes recibidos en un CECOM o sistema de mensajería acreditado, con clasificación de grado «RESERVADO o equivalente» o «CONFIDENCIAL o equivalente», **siempre que sea operativamente posible, se tramitarán a través del órgano de control**, donde se procede a su registro temporal como mensajes y a su comunicación al destinatario.

En caso de no ser posible, el contenido del mensaje se comunicará directamente al interesado, siempre que dicho procedimiento estuviera previsto, regulado y autorizado por el jefe de seguridad del órgano de control, de forma que quede asegurado el control, protección y custodia de la información clasificada en todo momento. Una vez disponible el órgano de control, si no ha transcurrido aún el periodo autorizado, se le entregará la información, o un listado periódico de mensajes recibidos en custodia, para su registro temporal.

El destinatario de un mensaje con propuesta de clasificación «RESERVADO o equivalente» o «CONFIDENCIAL o equivalente», salvo autorización y bajo estricto control, no conservará el mensaje en su poder, ni copias del mismo. El CECOM o sistema de mensajería acreditado podrá mantener los mensajes recibidos, durante el periodo autorizado, por si fuera necesario su reenvío o nueva consulta. Los «*back-up*» podrán mantenerse más tiempo.

Transcurrido ese plazo, o antes si no fuera necesaria la demora, por parte del CECOM o sistema de mensajería acreditado se entregarán al órgano de control los mensajes y las copias contenidos en soportes externos (excepto «*back-up*» y aquellos que tiene autorización para destruir) y se borrarán de forma segura las copias contenidas en soportes internos.

Conforme a las instrucciones que reciba del organismo o entidad al que sirve, el jefe de seguridad del órgano de control procederá, con respecto a cada mensaje, a su registro definitivo como documento, o a su destrucción conforme a la normativa, o a su archivo en un expediente o bloque documental único debidamente registrado y controlado.

Los mensajes que no precisen ser conservados de grado «CONFIDENCIAL o equivalente» o inferior, podrán ser destruidos en el propio CECOM o sistema de mensajería acreditado, junto con las copias y material borrador generado en cualquier soporte, anotando dicha destrucción, utilizando los procedimientos de destrucción aprobados. Los registros de destrucción se conservarán durante un mínimo de 3 años.

A partir de su registro, se manejarán de acuerdo con las normas generales para el control de la información clasificada, comunicando su existencia al órgano de control superior en caso de clasificación de grado «RESERVADO o equivalente».

El órgano de control deberá supervisar el correcto cumplimiento de todos estos procesos, especialmente por parte del CECOM o sistema de mensajería acreditado y del destinatario.

4. CONSERVACIÓN DE «*BACK-UP*»

En aquellos CECOM o sistemas de mensajería acreditados que se mantenga «*back-up*» de todo el tráfico de mensajes cursados, se adoptarán medidas especiales y específicas de registro, protección, almacenamiento, control y destrucción de los soportes, que serán aprobadas e inspeccionadas periódicamente por el jefe de seguridad del órgano de control del que dependa. Estas medidas estarán contenidas en los procedimientos operativos de seguridad del sistema concernido, o bien en los procedimientos de seguridad del plan de protección del local donde se ubica, especialmente cuando afecte a varios. Cuando el «*back-up*» sea un sistema en sí mismo, habrá sufrido un proceso específico de acreditación y autorización para operar.

De los registros de soportes de «*back-up*» de tráfico de mensajería sólo se notificará al órgano de control superior su existencia, no siendo preciso el contenido,

que queda bajo el control del propio CECOM, supervisado por el órgano de control directamente responsable.

No es preciso notificar al Registro Central la existencia de soportes de «*back-up*» de mensajes de grado «RESERVADO o equivalente», ni su contenido, aunque sí se mencionará en caso de inspección o consulta.

Cualquier mensaje que se recupere de un «*back-up*» deberá ser tratado conforme a su grado de clasificación, como si se recibiera nuevamente, no tratándose ya como mensaje, sino como documento, desde el primer momento.

No podrán conservarse mensajes de grado «SECRETO o equivalente» en los sistemas de «*back-up*», salvo que esté específicamente autorizado por la autoridad de acreditación del sistema.

Los soportes de «*back-up*» estarán identificados de forma inequívoca, con indicación del grado máximo y tipo de información clasificada contenida.

No es conveniente la conservación indefinida de los «*back-up*». Los procedimientos marcarán plazos o condiciones para su destrucción, que se hará siempre conforme a procedimientos y técnicas aprobados.

ANEXO IV A LA NS/04. FICHA DE ALTA, CONTROL Y REGISTRO DE MATERIAL CLASIFICADO

	FICHA DE ALTA, CONTROL Y REGISTRO DE MATERIAL CLASIFICADO	
	SERVICIO DE PROTECCIÓN DE I.C. (SPIC) COMPETENTE DE ALTA EN REGISTRO:	NÚMERO DE FICHA:

DATOS DE CLASIFICACIÓN				
NÚM. / REFERENCIA DEL MATERIAL CLASIFICADO:		CLASIFICACIÓN ASIGNADA:		ESPECIALIDAD:
MARCAS ADICIONALES DE LIMITACIÓN:		INSTRUCCIONES ESPECIALES DE MANEJO:		IDIOMA:
NÚMERO DE REGISTRO EN SPIC:	FECHA DE REGISTRO:	ASUNTO / DESCRIPCIÓN DEL MATERIAL CLASIFICADO:		
AUTORIDAD DE CLASIFICACIÓN:		IDENTIFICACIÓN DE LA NORMA DE LEY, DIRECTIVA O DILIGENCIA / GUÍA DE CLASIFICACIÓN POR LA QUE SE CLASIFICA:		
INSTRUCCIONES DE DES/RE-CLASIFICACIÓN:		ORGANISMO/EMPRESA ORIGINADOR:		
ORGANISMO PROPIETARIO:		SERVICIO DE PROTECCION DE INFORMACIÓN CLASIFICADA CUSTODIO:		
FORMATO SOPORTE:	NÚM. DE PÁGINAS:	NÚM. DE SOPORTES:	OTROS DATOS DE IDENTIFICACIÓN:	
OBSERVACIONES:			El Jefe del SPIC competente de alta en Registro (firma y sello oficial)	

DATOS DE SEGURIDAD INDUSTRIAL (si procede)		
ACTIVIDAD, CONTRATO, PROGRAMA O PROYECTO:	EMPRESA:	IDENTIFICACIÓN DE LAS INSTRUCCIONES DE SEGURIDAD DEL PROGRAMA/PROYECTO:
ÓRGANISMO DE LA ADMINISTRACIÓN RESPONSABLE (OFICINA DE PROYECTO, ÓRGANO DE CONTRATACIÓN, ETC.):	SERVICIO DE PROTECCIÓN DE I.C. DE LA ADMINISTRACIÓN RESPONSABLE:	

ALTA EN REGISTRO CENTRAL / SERVICIO CENTRAL DE PROTECCIÓN I.C. (si procede)			
NÚMERO REG.CENTRAL ☐ / SCPIC ☐		CLASIFICACIÓN:	El Jefe del Reg. Central / SCPIC (firma y sello oficial)
FECHA DE REGISTRO:	OBSERVACIONES:		

DILIGENCIAS DE RECLASIFICACIÓN (R) Y DESCLASIFICACIÓN (D)				
D/R	FECHA	OBSERVACIONES	AUTORIDAD o Responsable	La Autoridad o Responsable (Firmar solo en la desclasificación final)
(D)		Desclasificación final		(firma y sello oficial)

ANEXO V a la NS/04. INFORME DE COMPROMETIMIENTO

	**INFORME DE COMPROMETIMIENTO**	
	Identificación del Organismo o Entidad y del Servicio de Protección de Información Clasificada (SPIC):	**Fecha Informe:**

Fecha o periodo de ocurrencia del incidente:	Fecha y lugar del descubrimiento del incidente:
Grado de clasificación y marcas:	
Descripción de las circunstancias:	
Detallar la Información posiblemente comprometida con el suficiente detalle para facilitar la valoración del daño producido o proporcionar una copia de la lista con el informe del incidente:	
En el caso de que la pérdida o compromiso esté relacionado con un documento, detallar a continuación: originador, asunto, referencia, fecha, número de copia, idioma de redacción etc.	
Medidas tomadas para proteger la información o material y limitar el daño ocasionado:	
Valorar la posibilidad de que haya resultado comprometida la información clasificada: "seguro", "probable", "posible" o "improbable".	Declaración para informar si el originador ha sido informado:
Motivos o posibles motivos del comprometimiento:	
Enumerar las medidas tomadas para impedir la repetición del compromiso:	
Vº Bº **El Jefe del Organismo o Entidad:** **Fdo:**	**El Jefe del SPIC:** **Fdo:**

Pág. Núm. 1 de 1

NORMA NS/05

SEGURIDAD EN LOS SISTEMAS DE INFORMACIÓN Y COMUNICACIONES

1. INTRODUCCIÓN

Esta norma establece las condiciones **específicas** de manejo de información clasificada en sistemas de información y comunicaciones (CIS, por su sigla más conocida, en inglés). Los aspectos **generales**, u otros específicos, del manejo de la información clasificada, establecidos en el resto de la normativa de la ANPIC, serán igualmente de aplicación.

La información clasificada almacenada, procesada o transmitida (en adelante manejada) por sistemas de información y comunicaciones (en otros documentos o normativas se utiliza la expresión tecnologías de la información y las comunicaciones), en adelante sistemas, debe protegerse contra la pérdida de confidencialidad, integridad y disponibilidad, sea accidental o intencionada. Asimismo, debe impedirse la pérdida de integridad y disponibilidad de los propios sistemas que sustentan dicha información, y garantizarse la autenticidad y no repudio de las personas, dispositivos, servicios y entidades que acceden o procesan dicha información.

Con el objetivo de conseguir una adecuada protección, se deberá aplicar en los sistemas un conjunto equilibrado de medidas de seguridad, de distinta naturaleza (técnicas, físicas, en el personal y documentales), que permitan la creación de un entorno seguro para el manejo de la información clasificada, sostenido en el tiempo.

Corresponde a la ANPIC, responsable de la protección de la información clasificada en los ámbitos de su competencia, establecer cuáles habrán de ser las medidas de seguridad a implementar en los sistemas y verificar su correcta aplicación, a través de un proceso de evaluación, que podrá ser delegado en la forma que más adelante se indica.

Llegado el caso particular de un sistema dado, si el resultado de esta verificación es satisfactorio, la ANPIC, o la autoridad en quien haya podido delegar, en tanto autoridad de acreditación de seguridad (AAS, definida más adelante), procederá a la emisión de un certificado de acreditación para el sistema, por el que se le autoriza para el manejo de información clasificada en las condiciones establecidas.

A los efectos de la presente norma y por si pudiera haber conflictos de alcance con otras normativas que los tratan de forma separada, se considera que la seguridad criptológica y la seguridad de las emanaciones están incluidas dentro de la seguridad en los sistemas de información y comunicaciones, aunque más adelante se puedan citar de forma separada porque convenga dicha especificación. Asimismo, el concepto de seguridad en los sistemas de información y comunicaciones se considerará sinónimo del de seguridad de las tecnologías de la información y las comunicaciones (STIC).

2. OBJETO

Esta norma tiene por objeto establecer, de acuerdo con las responsabilidades adquiridas por la ANPIC, las condiciones de seguridad necesarias para el manejo de información clasificada por sistemas, así como definir el procedimiento de acreditación que obligatoriamente deberán superar estos antes de manejar dicha información.

3. ÁMBITO

Esta norma es de obligado cumplimiento para todos los sistemas que manejen o vayan a manejar información clasificada cuya protección sea responsabilidad de la ANPIC.

Para las referencias a los distintos grados de clasificación de la información clasificada, se emplearán los criterios definidos en la norma NS/04 de la ANPIC sobre seguridad de la información. Será de aplicación la tabla de equivalencias establecida en dicha norma.

4. PROCESO DE ACREDITACIÓN DE SISTEMAS

4.1. Conceptos Generales

El proceso de acreditación de un sistema tiene como finalidad determinar que se ha alcanzado, y que se mantiene, una adecuada protección de la información clasificada cuando es manejada en dicho sistema.

Esta verificación se realizará de acuerdo a los criterios de seguridad establecidos en las normas de la ANPIC y en otros documentos que se refieren en estas.

Se entiende por **autoridad de acreditación de seguridad (AAS)**, la autoridad competente para autorizar, o no, el uso de un sistema para manejar información clasificada, en unas condiciones determinadas y definidas, tras el proceso de su acreditación. Si el resultado de este proceso es satisfactorio y el riesgo residual final es admisible, dicha autoridad procederá a la emisión de un certificado de acreditación para dicho sistema.

Corresponde a la ANPIC actuar como AAS, dentro de su ámbito de competencia, pudiendo delegar dicha función. Cuando dicha capacidad sea delegada, será la autoridad delegada quien asuma las competencias, en los términos y con las limitaciones que se definan, no pudiendo delegar a su vez esta función.

La **acreditación** es el acto formal por el que la AAS, reconoce, tras el proceso de acreditación, la capacidad de un sistema para manejar información clasificada de un determinado ámbito o propietario (nacional, OTAN, etc.), hasta un determinado grado de clasificación y en unas condiciones determinadas, para lo que otorgará el correspondiente certificado de acreditación, por el que se autoriza dicho uso.

Como se ha indicado anteriormente, la acreditación es concedida basándose en el cumplimiento de unas determinadas condiciones de seguridad, tanto en el ámbito de seguridad en los sistemas de información y comunicaciones, como en el de la seguridad en el personal, de la seguridad física de las instalaciones y de la seguridad de la información, que deberán ser previamente acreditadas, y de las que el solicitante deberá aportar las evidencias y documentación necesarias para su valoración y aprobación.

La tramitación hacia la AAS de la solicitud de acreditación para un sistema, estará supervisada por los servicios de protección de información clasificada correspondientes, a través de los que se canalizarán todas las solicitudes. El inicio de la tramitación es responsabilidad de la autoridad operativa del sistema de las tecnologías de la información y las comunicaciones (AOSTIC), en su calidad de responsable de la estructura operacional del sistema, quien habrá contado y contará con el trabajo, apoyo, dirección y supervisión técnicas de la estructura STIC de su organización, en todas las fases del ciclo de vida del sistema, desde su concepción hasta su baja definitiva. Ambas figuras u órganos se definen en el **apartado 5.4.4** de la presente norma.

Como resultado de cada proceso de acreditación, la AAS podrá resolver en uno de los siguientes sentidos:

- **Acreditación de seguridad (AS)**: Declaración de acreditación para un periodo de tiempo especificado, en las condiciones operativas y ámbitos reflejados en la documentación correspondiente. Según la clasificación de la información que manejen los sistemas acreditados, se establece el período máximo de validez de una acreditación, independientemente de las evaluaciones que puedan sufrir. Se establece un período máximo de la validez de las acreditaciones de todos los sistemas de treinta y seis (36) meses, independientemente del grado de clasificación de la información que manejen.
- **Autorización provisional de seguridad (APS)**: Declaración de acreditación parcial, por un plazo de tiempo limitado (normalmente hasta seis -6- meses, y nunca superior a un -1- año), motivada por la existencia de deficiencias leves determinadas durante el proceso de acreditación.
- **Acreditación para pruebas** (AP): Autorización para poder operar el sistema para la realización de pruebas técnicas (funcionales y de seguridad), sin manejar información clasificada, aunque integrado o interconectado con otras redes o sistemas clasificados. Debe estar redactada toda la documentación de seguridad del sistema.
- **Denegación**: No se autoriza al sistema a operar. Expresa las deficiencias graves específicas y las acciones correctivas que deben llevarse a cabo.
- **Cancelación.** Situación en la que se deja en suspenso o se revoca permanentemente la acreditación de que ya disponía ese sistema. Se comunicarán las deficiencias encontradas y las acciones correctivas para solucionarlas.

La AAS seguirá supervisando las disposiciones de seguridad de los sistemas bajo su responsabilidad, principalmente llevando a cabo nuevas valoraciones de los riesgos e inspecciones/revisiones periódicas de las disposiciones de seguridad en vigor, de acuerdo con los requisitos de las políticas de seguridad. Los sistemas autorizados deberán someterse a las inspecciones y análisis de seguridad que la AAS considere oportunos para poder asegurar que se cumple lo estipulado en la documentación de seguridad del sistema.

La acreditación tiene un carácter temporal, por lo que deberá renovarse siempre que transcurra su plazo de validez o que se produzcan cambios que supongan una modificación suficientemente relevante de las condiciones de seguridad.

Todo cambio significativo en las condiciones de seguridad del sistema invalida su acreditación. Se deberá informar con antelación a la AAS de cualquier cambio previsto en la configuración del sistema, en sus requisitos de operación o en el grado de clasificación de la información que va a manejar. La AAS aconsejará sobre las implicaciones que los mencionados cambios puedan tener para la seguridad de la información clasificada manejada por el sistema.

4.2. Estrategia de acreditación

Serán objeto de acreditación específica, por un lado, los sistemas de una organización dedicados al manejo de información clasificada (típicamente estaciones aisladas, redes de área local y redes de área extensa), y por otro, las interconexiones entre dos o más de estos sistemas, o con sistemas de otras organizaciones.

Para cada sistema e interconexión de sistemas se emitirá, una vez aprobadas sus condiciones de seguridad, el correspondiente certificado de acreditación, de acuerdo al procedimiento de acreditación descrito en esta norma.

En adelante, aunque hablemos únicamente de sistemas, se entiende que lo indicado es aplicable igualmente a las interconexiones de sistemas, con sus especificidades.

Para redes de área extensa y comunidades de redes de área local, y para sistemas que por su complejidad y extensión así lo requieran, la ANPIC decidirá, caso por caso, la estrategia de acreditación de seguridad (EAS) a seguir. Esta estrategia de acreditación será acordada junto con la estructura STIC de la organización, la AOSTIC y el servicio de protección de información clasificada, basándose en la documentación de seguridad aportada inicialmente (concepto de operación del sistema).

Durante el proceso de acreditación, la comunicación oficial entre la AOSTIC y estructura STIC, y la AAS deberá encauzarse principalmente a través del servicio de protección de información clasificada del que dependan, especialmente en los pasos fundamentales del proceso, como son la solicitud de acreditación, remisión de la documentación de seguridad y acreditación final. Los temas técnicos de detalle y de seguimiento del proceso podrán tramitarse directamente entre los órganos directamente afectados.

La documentación básica de seguridad de un sistema estará constituida por el concepto de operación (CO), la declaración de requisitos específicos de seguridad (DRES) y los procedimientos operativos de seguridad (POS), que se mencionan más adelante.

El servicio de protección de información clasificada tiene responsabilidades en el proceso, en cuanto responsable último en su organismo o entidad de la protección de la información clasificada, con independencia del formato, lugar o medio en que se maneje ésta.

Asimismo, la estructura STIC de cada organización asumirá las responsabilidades que se le asignan en el **apartado 5.4.4** de la presente norma.

Como norma general la AAS, a través de sus órganos de trabajo, se implicará en mayor medida en los sistemas más complejos o más críticos, siendo su participa-

ción menor en sistemas sencillos (redes o estaciones aisladas, etc.), que puedan ser evaluados por la propia estructura STIC de la organización. Es responsabilidad y obligación de cada organización el dotarse de estas capacidades.

Para aquellos sistemas bajo supervisión de un panel de acreditación específico, será de aplicación la estrategia de acreditación establecida por éste. Corresponde a la ANPIC prestar el apoyo necesario en la acreditación de los nodos de los sistemas ubicados en su ámbito de responsabilidad, así como la comunicación de este extremo al panel de acreditación.

La seguridad de los sistemas que traten información cedida a España al amparo de acuerdos internacionales para la protección de la información clasificada, se regirá por los principios establecidos en dichos acuerdos, aplicándose en lo posible la presente normativa.

4.3. Modos seguros de operación

Los sistemas que manejen información clasificada deben trabajar en lo que se denominan modos seguros de operación. Dichos modos vienen determinados por la autorización y la necesidad de conocer de los usuarios, y por el mayor grado de clasificación de la información manejada en el sistema.

Estos modos determinan la forma en la que un sistema que maneje información clasificada debe llevar a cabo el control de acceso y la separación de la información.

De esta forma se pueden definir los siguientes modos seguros de operación:

- **Dedicado**: Es aquel modo en el que todo el personal con acceso al sistema:
  - está autorizado para acceder al grado más elevado de clasificación de la información manejada en el sistema,
  - y además posee la misma necesidad de conocer.
  - La separación de los datos no es un requisito del sistema.
- **Unificado al nivel superior**: es aquel en el que las personas con acceso al sistema:
  - están autorizadas para acceder al grado más elevado de clasificación de la información manejada en el sistema,
  - no todos tienen la misma necesidad de conocer,

- la necesidad de conocer se garantiza por medio de procesos informales, que hacen que el sistema realice la separación de datos de una de manera fiable, disponga de un control de accesos selectivo a la información conforme a la diferente «necesidad de conocer» y cumpla con lo establecido en la normativa de seguridad vigente y en sus políticas correspondientes fundamentalmente por medios procedimentales.

– **Compartimentado**: es aquel en el que las personas con acceso al sistema:

- están autorizadas para acceder al grado más elevado de clasificación de la información manejada en el sistema,
- no todos tienen la misma necesidad de conocer,
- la necesidad de conocer se garantiza por medio de una autorización formal para acceder a la información manejada en el sistema, y se materializa, además de en una gestión centralizada formal para el control de accesos, en el uso de herramientas y mecanismos adicionales que refuercen globalmente el cumplimiento de las políticas y la normativa de seguridad.

– **Multinivel**: Es aquel modo de operación en el que el sistema:

- maneja información con diferentes grados de clasificación,
- permite el acceso selectivo y simultáneo a dicha información al personal autorizado con diferentes grados de clasificación y distintas necesidades de conocer,
- realiza de manera fiable la completa separación de los datos y el control del acceso selectivo.

Este modo de operación no es de aplicación para los sistemas acreditados para manejar información DIFUSIÓN LIMITADA o equivalente.

4.4. Delegación de la autoridad de acreditación

En aquellos casos en que la necesidad lo justifique, y solo en aquellos organismos o entidades que dispongan de los medios, formación y recursos necesarios para su adecuada ejecución, la ANPIC podrá delegar las competencias de acreditación de sistemas que manejen información clasificada en la autoridad pertinente de dicho organismo o entidad.

Cuando la información manejada pertenezca a una organización internacional o multinacional, o a un país con el que hay establecido un acuerdo para la protec-

ción de la información clasificada, esta delegación solo podrá producirse para sistemas que manejen información clasificada de grado «DIFUSIÓN LIMITADA o equivalente» como máximo.

Para que esta delegación se materialice, el organismo o entidad deberá disponer de la infraestructura de protección de información clasificada necesaria para la información manejada, y de las estructuras STIC de la organización, de operación STIC y de control de material de cifra.

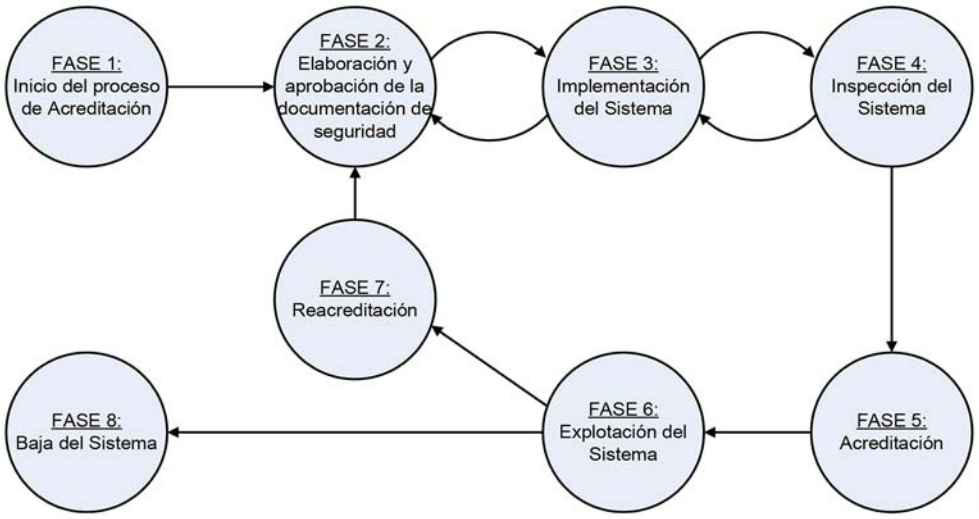
La ANPIC será informada puntualmente por cada autoridad delegada de todos los sistemas que acrediten derivado de estas delegaciones, para lo que remitirán copia de cada certificado de acreditación emitido.

4.5. Procedimiento de acreditación

Todo proceso de acreditación de sistemas abordado por la AAS se rige por las disposiciones establecidas en la presente norma, por lo que será referencia obligada y primera en la documentación de seguridad que se presente.

Asimismo será de aplicación la normativa CCN-STIC (especialmente la norma CCN-STIC-101, relativa a Acreditación de Sistemas TIC, en cuanto a procedimientos).

Con el fin de homogeneizar y estructurar las distintas tareas que implica una acreditación, se establece el presente procedimiento de acreditación, el cual define cada una de las fases del proceso a seguir, que se resumen en el gráfico adjunto.



Los sistemas en los que se vaya a manejar información clasificada de grado «DIFUSIÓN LIMITADA o equivalente», podrán acogerse al procedimiento de acreditación simplificado que se contempla en la norma CCN-STIC-101 indicada anteriormente, en las condiciones que allí se establecen.

FASE 1: Inicio del proceso de acreditación

La AOSTIC, en coordinación y con la participación activa de la estructura STIC de su organización, deberá remitir formalmente a la AAS, a través de su servicio de protección de información clasificada, la petición de acreditación del sistema que se quiere acreditar. Dicha petición deberá incluir la descripción del sistema, la cual se ajustará al formato de concepto de operación definido en la correspondiente guía CCN-STIC (ver más adelante **apartado 5.4.7** de la presente norma).

A la recepción de dicha documentación, la AAS dará por iniciado el proceso de acreditación, pudiendo a su vez solicitar cuantas aclaraciones y rectificaciones estime oportunas. Asimismo, cualquiera de las partes podrá plantear la realización de una reunión de coordinación que ayude al desarrollo de dicho proceso, especialmente cuando la complejidad o criticidad del sistema concernido excede las capacidades de la organización.

Para aquellos sistemas donde sea factible, en esta fase podrá remitirse para aprobación la documentación exigida en la FASE 2 del procedimiento de acreditación.

Una vez aprobada la documentación aportada, la AAS lo comunicará al organismo peticionario a través del servicio de protección de información clasificada del que dependa.

FASE 2: Elaboración y aprobación de la documentación de seguridad

La AOSTIC, en coordinación y con la participación activa de la estructura STIC de su organización, una vez aprobado el concepto de operación, será responsable de la elaboración y remisión del resto de documentación de seguridad exigida en cada caso.

En el **apartado 5.4.7** se detalla la documentación de seguridad necesaria, a remitir, o generada durante el proceso, para la acreditación de todo sistema destinado a manejar información clasificada.

Dicha documentación, junto con aquella otra complementaria que se precise para la certificación del personal y locales del sistema, deberá ser enviada a la AAS para su aprobación.

FASE 3: Implementación del sistema y de su entorno de seguridad

Una vez aprobada la documentación de seguridad del sistema, la AOSTIC junto con la estructura STIC de su organización serán responsables de la puesta en funcionamiento de éste, de acuerdo a dicha documentación y a las condiciones de seguridad en ella especificadas.

La AOSTIC / estructura STIC, comunicarán a la AAS, con antelación suficiente, la fecha a partir de la cual el sistema y su entorno de seguridad (entornos local, global y electrónico, de seguridad) estarán listos para su inspección y evaluación, a fin de que esta última pueda planificar adecuadamente su calendario de inspecciones, o pueda autorizar la delegación de dicha inspección en la propia estructura STIC de la organización.

Asimismo, la AOSTIC deberá responsabilizarse de escalar convenientemente a la AAS todo condicionante adicional (por ejemplo, necesidades operacionales, comerciales o estratégicas) que ésta deba considerar con el fin de priorizar adecuadamente los distintos procesos de la acreditación en ejecución.

FASE 4: Inspección del sistema y de su entorno de seguridad

El sistema a acreditar será técnicamente inspeccionado por la AAS, u órgano en que haya delegado, a fin de evaluar y verificar su correcta implementación de acuerdo a la documentación de seguridad aprobada. El resultado de dicha inspección técnica será comunicado oficialmente a la AOSTIC / estructura STIC.

Aun resultando positiva la evaluación técnica realizada, ésta no constituye en sí una autorización al sistema para operar, la cual será explícita y claramente comunicada por la AAS, una vez verificado el resto de aspectos necesarios (seguridad física, seguridad en el personal y seguridad de la información).

FASE 5: Acreditación

Tras la verificación positiva por parte de la AAS de las condiciones de seguridad del sistema, ésta procederá a la emisión del correspondiente certificado de acreditación del sistema, el cual constituye a todos los efectos la única autorización para que el sistema maneje información clasificada, en las condiciones establecidas en su documentación de seguridad.

FASE 6: Explotación del sistema

Una vez obtenido el certificado de acreditación, se deberán mantener las condiciones de seguridad iniciales que dieron lugar a dicha autorización. En caso de

cambios significativos, este certificado de acreditación pierde automáticamente toda validez.

Con el fin de verificar que los sistemas autorizados para el manejo de información clasificada mantienen las condiciones de seguridad que dieron lugar a la acreditación, éstos se someterán a un proceso de evaluaciones de seguridad periódicas.

FASE 7: Renovación de la acreditación

Transcurrido el periodo de validez del certificado de acreditación, el sistema pierde su autorización para manejar información clasificada. Es responsabilidad de la AOSTIC el iniciar con la antelación suficiente los trámites para la renovación de la acreditación.

También son motivo de renovación de la acreditación del sistema los cambios en éste que afecten a las condiciones de seguridad del mismo. Antes de proceder a realizar dichos cambios, éstos deben ser aprobados por la AAS correspondiente, que verificará el impacto de dichos cambios en las condiciones de seguridad exigidas al sistema.

FASE 8: Baja del sistema

Una vez llegue a su fin la vida útil de un sistema autorizado para el manejo de información clasificada, es responsabilidad de la AOSTIC garantizar la correcta destrucción o borrado seguro de la información clasificada almacenada.

Los procedimientos a seguir en este caso estarán recogidos en el documento de requisitos de seguridad del sistema o interconexión, tal y como se indica en la guía CCN-STIC 202.

5. SEGURIDAD DE LA INFORMACIÓN CLASIFICADA MANEJADA EN SISTEMAS DE INFORMACIÓN Y COMUNICACIONES

Este apartado tiene por objeto destacar, de forma resumida, algunos aspectos de seguridad a considerar en la protección de la información clasificada manejada en sistemas de información y comunicaciones, desde los diferentes puntos de vista de la seguridad de la información (documental), de seguridad en el personal, de seguridad física (instalaciones) o de seguridad en los sistemas propiamente dicha.

En cualquier caso, como se indicó en el apartado de introducción de esta norma, los aspectos **generales**, u otros específicos, del manejo de la información clasificada, establecidos en el resto de normas de la ANPIC, serán igualmente de aplicación.

5.1. Seguridad de la información (documental)

Dentro de los sistemas, la información manejada siempre es en la forma de documentos, por ello a veces se habla en otras normas de seguridad documental, que constituiría un apartado específico dentro del concepto más amplio de seguridad de la información.

Todo sistema destinado al manejo de información clasificada de grado «CONFIDENCIAL o equivalente» o superior deberá tener claramente identificado el órgano de control del que depende. La contabilidad, distribución y manejo de los documentos clasificados, sea en formato papel o en soportes electrónicos de almacenamiento, se realizará por parte del órgano de control competente, o bajo su control.

Dicho órgano de control para la protección de la información clasificada se deberá haber constituido de acuerdo a lo establecido en la norma NS/01 de la ANPIC sobre infraestructura nacional de protección de la información clasificada.

Para sistemas destinados al manejo de información clasificada con grado de «DIFUSIÓN LIMITADA o equivalente» que no estén bajo dependencia de un órgano de control, estas responsabilidades serán ejercidas por el responsable de seguridad designado.

La información clasificada deberá estar almacenada en soportes debidamente etiquetados según el grado de clasificación que le corresponda o en sistemas autorizados.

Todos los medios clasificados de almacenamiento informático estarán adecuadamente identificados, registrados, almacenados y protegidos de manera proporcional al máximo grado de clasificación de la información almacenada.

Es responsabilidad del usuario que los soportes removibles que utilice estén correctamente etiquetados.

Los soportes removibles de almacenamiento, mientras no sean desclasificados conforme a procedimientos aprobados, mantendrán el máximo grado de clasificación para el que hayan sido empleados.

La información clasificada grabada en medios de almacenamiento informático reutilizables sólo podrá borrarse de conformidad con los procedimientos aprobados por la AAS.

5.2. Seguridad en el personal

Todas las personas que tengan acceso a sistemas donde se maneje información clasificada de grado «CONFIDENCIAL o equivalente» o superior, o a locales donde se ubiquen estos sistemas, deberán estar en posesión de la Habilitación Personal de Seguridad (HPS) correspondiente al máximo grado de clasificación de la información clasificada a la que pueda tener acceso en dicho sistema o local.

Este requisito es de aplicación incluso para aquellas personas no autorizadas a acceder a dicha información clasificada (por ejemplo, personal de administración, mantenimiento o limpieza). Este personal podrá prescindir de la HPS cuando la AOSTIC implemente un procedimiento de actuación que garantice que en el momento en que dicho personal acceda a las instalaciones del sistema no exista información clasificada a la vista y que este personal está permanentemente escoltado por personal con la HPS adecuada y la formación técnica necesaria para garantizar que no se compromete la confidencialidad, integridad y disponibilidad de la información. Este procedimiento de actuación deberá estar recogido en los procedimientos operativos de seguridad del sistema (POS).

El particular estatus de acceso privilegiado a la información clasificada manejada en el sistema, por parte del personal dedicado a tareas de administración y mantenimiento de los sistemas y tecnologías de la información y de las comunicaciones, podría aconsejar, en ciertos casos, la exigencia de que dispongan de una HPS en un grado de clasificación superior a la máxima clasificación de la información manejada en el sistema. Este no será un criterio general sino una consecuencia del análisis de riesgos previo o como requisito de seguridad de un sistema específico, a propuesta de la AOSTIC y aprobado por la AAS.

La habilitación de seguridad del personal con acceso a información clasificada se realizará de acuerdo al procedimiento establecido en la norma NS/02 de la ANPIC sobre seguridad en el personal, y con los criterios y particularidades que allí se marcan.

Siempre que sea posible, las tareas de administración del sistema, de administración de seguridad del sistema y de supervisión de seguridad del sistema recaerán en distintas personas. Esta distinción de supervisores, administradores, usuarios y sus cometidos estará reflejada en los POS del sistema.

La relación detallada de personas autorizadas a acceder al sistema y/o a la información en él contenida, así como sus derechos y permisos de acceso, deberá figurar, y mantenerse actualizada, como anexo a los POS del sistema.

5.3. Seguridad física

Aquellas instalaciones fijas o semipermanentes donde se ubiquen los distintos componentes de los sistemas que manejen información clasificada «CONFIDENCIAL o equivalente» o superior, deberán estar acreditadas como zonas de acceso restringido, que podrán estar configuradas como área clase I o área clase II, según los criterios que se marcan en la norma NS/03 de la ANPIC sobre seguridad física.

No obstante, existen otros requisitos por los cuales 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 como área clase I, o implementar especiales medidas de protección para evitar la posibilidad de acceso no autorizado a los equipos considerados como críticos. Los criterios serán los que la AAS en cada momento establezca, bien mediante normativa específica existente, o como requisito de seguridad para la acreditación de un determinado sistema.

Aquellas instalaciones fijas o semipermanentes donde se ubiquen sistemas que manejen información clasificada de grado «DIFUSIÓN LIMITADA o equivalente», deberán estar constituidas como zonas administrativas de protección, salvo que sean ZAR.

El acondicionamiento y acreditación de estos locales se realizará de acuerdo al procedimiento establecido en la norma NS/03.

5.4. Seguridad en los sistemas de información y comunicaciones

5.4.1. Objetivos de seguridad

Los objetivos de seguridad perseguidos con la aplicación de medidas de seguridad en los sistemas de información y comunicaciones son:

a) Proporcionar **confidencialidad** a la información manejada por el sistema.
b) Proporcionar **integridad** a la información manejada por el sistema, así como a los recursos y servicios del mismo.
c) Mantener la **disponibilidad** de la información manejada por el sistema, así como de los recursos y servicios del mismo.
d) **Autenticar** a las personas que acceden a la información manejada por el sistema o a los recursos del mismo.
e) Proporcionar al sistema el servicio de **no repudio**, mediante el cual es posible proporcionar la prueba de que una determinada acción ha sido realizada, no pudiendo los agentes participantes negar que se haya producido.

5.4.2. Principios de seguridad

Todo sistema en el que se vaya a manejar información clasificada deberá atenerse a unos principios básicos dirigidos a asegurar la debida protección de la información clasificada:

a) Todos los sistemas deberán ser sometidos a un proceso de acreditación que garantice que se encuentran protegidos mediante un conjunto apropiado de elementos «*hardware*» y «*software*», adecuadamente configurados, de forma que permitan garantizar la confidencialidad, integridad y disponibilidad de la información clasificada manejada por el sistema, así como la integridad y disponibilidad del propio sistema.
b) El manejo de información clasificada en un sistema requerirá la previa autorización para ello por la autoridad de acreditación de seguridad.
c) La interconexión de sistemas que manejen información clasificada requerirá la previa acreditación por las autoridades competentes para cada sistema. Cada sistema tratará a los otros sistemas como de no confianza y aplicará medidas de protección para controlar el intercambio de información con otros sistemas.
d) A los usuarios del sistema sólo se les concederán los privilegios y autorizaciones que necesiten para llevar a cabo sus tareas y cometidos. Deberán estar habilitados sólo hasta el mayor grado de clasificación de la información de la que éstos tengan necesidad de conocer.
e) Los responsables de equipos de cifra, material de claves o de los elementos de seguridad utilizados para la protección de los sistemas, requerirán de una acreditación especial, de acuerdo a lo especificado en el **apartado 5.4.6** de esta norma.
f) Los locales destinados a alojar sistemas que manejen información clasificada «CONFIDENCIAL o equivalente» o superior deberán estar acreditados como zonas de acceso restringido «área clase I» o «área clase II». Si únicamente van a manejar información clasificada de grado «DIFUSIÓN LIMITADA o equivalente», bastará su constitución como zonas administrativas de protección.
g) Toda la información clasificada «CONFIDENCIAL o equivalente» o superior extraída de un sistema deberá quedar registrada en el sistema de registro correspondiente, constituido por los órganos de control.
h) Se aplicará una gestión del riesgo de seguridad en los sistemas, para controlar, reducir, eliminar y evitar o aceptar riesgos.

La aplicación de estos principios y la posterior aplicación de las medidas de protección se verificarán, inicial y periódicamente, por la autoridad de acreditación de seguridad de cada sistema.

5.4.3. Medidas de seguridad

Todo sistema en el que se vaya a manejar información clasificada deberá implementarlas siguientes medidas de protección mínimas:

a) Dispondrá de los medios necesarios para identificar y autentificar de forma fiable a las personas cuyo acceso esté autorizado, asegurando que se cumple el principio de la necesidad de conocer.
b) Toda información y equipamiento que permita el acceso a los sistemas deberá ser protegida de acuerdo al mayor grado de clasificación de la información clasificada a la que pudiera dar acceso.
c) Todo medio de almacenamiento utilizado en sistemas será protegido de acuerdo al máximo grado de clasificación de la información que contiene.
d) Deberá contar con los dispositivos necesarios para realizar el registro automático de los accesos e intentos de acceso a la información clasificada.
e) Todo dispositivo de seguridad (producto que aporta seguridad) destinado a su empleo en sistemas que manejen información clasificada deberá haber sido aprobado por el Centro Criptológico Nacional (CCN).
f) La interconexión entre sistemas ubicados en distintas zonas de acceso restringido requerirá la utilización de elementos de cifra certificados por el CCN, de acuerdo al grado de clasificación de la información a transmitir.
g) La información clasificada contenida en los dispositivos de almacenamiento removibles deberá estar protegida mediante una herramienta de cifrado adecuada y aprobada para su grado de clasificación.
h) Los sistemas que manejen información clasificada «CONFIDENCIAL o equivalente» o superior, deberán ser protegidos contra las amenazas derivadas de emanaciones electromagnéticas no deseadas, cuyo estudio y control se conoce como TEMPEST, acorde con el nivel de riesgo de explotación existente.
i) Todo sistema deberá contar con programas actualizados de detección de virus y de «*software*» malicioso.
j) No se permitirá el uso de equipos o dispositivos electrónicos particulares, incluidos soportes de almacenamiento, para el manejo de información clasificada.
k) No se permitirá la entrada de equipos o dispositivos electrónicos, incluidos soportes de almacenamiento, a zonas de acceso restringido (ZAR), excepto los pertenecientes a los sistemas autorizados para el manejo de información clasificada existentes en la propia ZAR.
l) Las tareas de instalación, administración, mantenimiento y reparación de los sistemas que manejen información clasificada deberán ser llevadas a cabo por personal con HPS de grado igual o superior al grado de clasificación de la información que manejen los sistemas a que dicho personal tenga acceso.

m) Los sistemas que manejan información clasificada estarán sujetos a una valoración y gestión de riesgos acorde con los requisitos especificados en la norma CCN-STIC correspondiente.
n) Se adoptarán medidas adicionales, adecuadas a las circunstancias, allí donde una valoración de los riesgos haya establecido que la información clasificada, o los servicios y recursos de apoyo al sistema, están sujetos a mayores riesgos, procedentes de amenazas y vulnerabilidades concretas.

5.4.4. Organización de seguridad

Aparte de la estructura STIC nacional, que se encuentra bajo la dependencia directa de la ANPIC como autoridad de acreditación de seguridad, en cada organización con una cierta entidad (como mínimo a nivel de departamento ministerial y en fuerzas armadas) deberá existir una organización STIC específica, responsable de que se implante y aplique en dicha organización la normativa de seguridad en los sistemas de información y comunicaciones. Esta organización STIC estará coordinada con el servicio de protección de información clasificada de la organización.

En concreto, deberán contar con:

a) Estructura STIC de la organización.
b) Estructura de operación STIC del sistema.
c) Estructura de control de material de cifra de la organización.

La estructura de seguridad establecida en el párrafo anterior será responsable, respecto a los sistemas y en el ámbito de su organización, de:

a) Implantar, aplicar y velar por el cumplimiento de la normativa STIC.
b) Solicitar la autorización para operar o acreditación de los sistemas.
c) Definir el concepto de operación.
d) Llevar a cabo el análisis y gestión de riesgos de seguridad en los sistemas.
e) Definir los requisitos de seguridad para los sistemas, además de verificar y supervisar su correcta implementación y mantenimiento.
f) Elaborar la documentación de seguridad.
g) Gestionar la configuración de seguridad.
h) Formar en materia de seguridad a los usuarios autorizados de los sistemas.
i) Auditar los registros de acceso a la información y de eventos de seguridad.
j) Gestionar los incidentes de seguridad.
k) Mantener las condiciones de seguridad de los sistemas.
l) Coordinar sus actuaciones con el órgano de control del que dependa.

El servicio de protección de información clasificada, constituido por los órganos de control, será responsable, en cada ámbito de competencia, de supervisar que la normativa de protección de la información clasificada se aplica de forma correcta en los sistemas.

Llevarán registro de:

a) Los sistemas autorizados a manejar información clasificada en su ámbito de protección.
b) La información clasificada manejada en los sistemas, incluidos los soportes informáticos.
c) La información clasificada extraída de los sistemas.
d) Los usuarios autorizados para acceder a los sistemas.
e) Las zonas de acceso restringido donde se ubican los sistemas.

La estructura STIC de la organización ejerce una función fundamental, dado que es donde residen el conocimiento, las capacidades y la experiencia técnicas, de dicha organización, relativas a la acreditación de sistemas, no solo en cuanto proceso de tramitación, sino, y principalmente, en cuanto a la determinación y aplicación de la normativa técnica de seguridad aplicable a los sistemas en desarrollo. Sus responsabilidades abarcan desde el sistema más complejo hasta la última estación aislada de su organización en que se vaya a manejar información clasificada y deba ser acreditada.

La asunción de esta funcionalidad es fundamental y obligatoria, unida a la asignación de los recursos y con la complejidad que cada organización precise, motivado por el hecho de que la ANPIC, con sus órganos de trabajo, no puede asumir la dirección de ejecución, el asesoramiento y la inspección, incluida la relación que ello implica con los responsables directos, de todos y cada uno de los sistemas nacionales existentes, por lo que es necesaria la existencia de una jerarquía de responsables en los que delegar funciones. Por otro lado, es el único medio para que los sistemas puedan ser acreditados en plazos de tiempo aceptables, y de acuerdo con esquemas de prioridades.

5.4.5. Gestión de riesgos de seguridad

Todos los sistemas que manejen información clasificada estarán sujetos a una gestión de riesgos. A efectos de esta norma, se utilizan las siguientes definiciones:

– Riesgo de seguridad: La probabilidad de que la vulnerabilidad inherente a un sistema de información y comunicaciones sea explotada por cualquier amenaza y que su consecuencia sea que el sistema quede comprometido.

– Gestión del riesgo de seguridad: Proceso completo de identificación, control y minimización de eventos inciertos que puedan afectar a los recursos del sistema.

El análisis de riesgos es el proceso por el que se identifican las amenazas y vulnerabilidades contra la seguridad de un sistema, se determina su magnitud y se descubren las áreas que necesitan salvaguardas o contramedidas. El análisis de riesgos sirve para identificar el riesgo existente y evaluar la actual seguridad del sistema en relación con el manejo de información clasificada, para a continuación reunir la información necesaria para seleccionar las contramedidas de seguridad más eficaces, basándose en la política de seguridad del sistema y en las directivas y guías de apoyo publicadas.

El análisis de riesgos ayuda a decidir las medidas de seguridad que deben adoptarse y el modo en que puede lograrse la conjunción de medidas técnicas y medidas de seguridad alternativas, y ofrece una valoración objetiva del riesgo residual. 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.

El análisis de riesgos no es una tarea que se haga una única vez. Debe realizarse periódicamente, de acuerdo con los requisitos exigidos por el proceso de acreditación que se haya acordado, con objeto de que se mantenga actualizado frente a los cambios que experimenta el entorno en el que se maneja la información clasificada (aparición de nuevas amenazas y vulnerabilidades, cambios en la evaluación del impacto y frecuencia, modificaciones en locales y en sistemas, etc.).

Los principales recursos necesarios para realizar un análisis de riesgos son el tiempo, una mano de obra especializada y, si es posible, una herramienta de análisis de riesgos automatizada que utilice una metodología sólida. Por esta razón, el primer análisis de riesgos que se realice para un proyecto o para una organización será el que requiera una mayor cantidad de recursos. Las actualizaciones subsiguientes pueden basarse en informaciones previas, con una posible disminución en requisitos de tiempo y recursos.

El tiempo dedicado a realizar el análisis de riesgos deberá ser proporcional a sus objetivos. El análisis de riesgos de un sistema complejo, con importantes volúmenes de información y un gran número de usuarios, requerirá mayor cantidad de recursos que el de uno menor, aislado, que maneje una cantidad limitada de información y que cuente con un pequeño número de usuarios.

El éxito de un análisis de riesgos depende, en gran medida, del papel que desempeñe en el proceso el nivel más alto de dirección de la organización. La dirección debe llegar a un acuerdo para lograr el objetivo y abarcar el ámbito del análisis de riesgos expresando su apoyo a todos los niveles de la organización, y deberá revisar y refrendar los resultados de dicho proceso.

La gestión del riesgo contempla distintas opciones, incluyendo su reducción, transferencia, eliminación, prevención y aceptación. El riesgo puede reducirse implementando una arquitectura de sistemas gestionada que incluya seguridad en el personal, seguridad física, seguridad documental y seguridad técnica.

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. Es también un proceso ejecutado en colaboración, en el que representantes de diversos grupos de interés desarrollan una comprensión común de requerimientos y opciones. El aumento de la conciencia de seguridad refuerza la seguridad y la hace más compatible con las necesidades de los usuarios.

La gestión del riesgo para los sistemas presenta una serie de dificultades específicas que surgen de la naturaleza dinámica de los factores de riesgo y de la rápida evolución de la tecnología. El fallo a la hora de considerar los factores de riesgo de manera oportuna y adecuada puede llevar a que se adopten unas medidas de seguridad ineficaces e innecesariamente costosas. Por tanto, la gestión del riesgo de seguridad debe ser considerada como una parte integral del proceso global de vida útil del sistema.

Los procesos de gestión y de análisis de riesgos son un ejercicio de recolección y valoración de datos que aborda dos cuestiones básicas: los activos que corren peligro y cuál sería el impacto o las consecuencias si las vulnerabilidades identificadas fueran explotadas con éxito.

Los procesos de gestión y de análisis de riesgos serán realizados de forma conjunta por las autoridades de planificación y aplicación de seguridad en los sistemas, por las autoridades de operación de los sistemas, por el personal de proyectos y por las autoridades de certificación de seguridad. Los procesos de gestión y de análisis de riesgos seguirán un enfoque estructurado (manualmente o con una herramienta automatizada) que deberá incluir las siguientes etapas:

– Identificar el ámbito y objetivos del análisis de riesgos; el objetivo se acordará entre las autoridades de planificación y aplicación de seguridad en los sistemas, las autoridades de operación de los sistemas, por el personal de proyectos y por las autoridades de certificación de seguridad.

- Determinar los activos físicos y de información que contribuyen al cumplimiento de la misión de un sistema o una misión de la organización.
- Determinar el valor de los activos físicos.
- Determinar el valor de los activos de información respecto al impacto en las siguientes dimensiones: confidencialidad, integridad y disponibilidad.
- Identificar las amenazas y vulnerabilidades del sistema y el nivel de dichas amenazas y vulnerabilidades.
- Identificar las contramedidas existentes.
- Determinar las contramedidas necesarias y compararlas con las ya existentes.
- Revisar los riesgos y las contramedidas recomendadas, teniendo en cuenta las siguientes opciones y considerando que las políticas de seguridad exigen la aplicación de un estándar mínimo de protección a la información clasificada:

  - Eliminación del riesgo: El objetivo es minimizar las vulnerabilidades reales o potenciales aplicando la totalidad de las contramedidas identificadas.
  - Prevención de la degradación de los activos físicos y de información: El objetivo es la aplicación de contramedidas con el fin de evitar, en la medida posible, que se produzcan estas degradaciones, teniendo en cuenta que algunos riesgos no pueden eliminarse debido a razones técnicas u operativas.
  - Limitación de la degradación de los activos físicos y de información: El objetivo es la aplicación de contramedidas con el fin de limitar estas degradaciones a un nivel aceptable.
  - Aceptación del riesgo de degradación de activos físicos y de información: Cuándo debe tomarse la decisión de aceptar las consecuencias de la materialización de una amenaza, ya sea porque el coste o impacto de la degradación asociada es insignificante, porque la probabilidad de que se materialice la amenaza se considera suficientemente baja, o porque el coste de las contramedidas es mucho más elevado que el coste o impacto de las pérdidas asociadas a la materialización de la amenaza.

- Elaborar un informe de gestión de riesgos que incluya la descripción de las contramedidas que van a implementarse y la descripción del riesgo residual.

El resultado del proceso de gestión del riesgo puede facilitar los detalles a incluir en la documentación de seguridad requerida durante el proceso de acreditación de seguridad de sistemas.

Tras completar el proceso inicial de análisis de riesgos de un sistema, se conservará la información resultante y se utilizará como base para futuras actualizaciones.

5.4.6. Requisitos de seguridad

Seguridad de los sistemas

Todos los sistemas deberán disponer de un conjunto equilibrado de servicios de seguridad que permitan alcanzar los objetivos de seguridad requeridos:

- Identificar y autenticar a los individuos con acceso autorizado.
- Controlar los accesos a la información de acuerdo con el principio de la necesidad de conocer.
- Verificar y mantener la integridad de la información clasificada y de los elementos del sistema.
- Mantener la disponibilidad requerida para la información y los elementos del sistema.
- Garantizar y verificar el funcionamiento de los mecanismos de seguridad del sistema.
- Registrar y auditar la actividad de los usuarios del sistema.
- Controlar las conexiones y los enlaces de los sistemas.
- Prevenir, detectar y corregir los impactos o incidentes que afecten a la confidencialidad, integridad y disponibilidad de la información o a la integridad y disponibilidad del sistema que la maneja.

Interconexión de sistemas

Se produce una conexión entre sistemas cuando se proveen medios físicos y lógicos de transmisión (por ejemplo enlace satélite, fibra óptica, etc.) susceptibles de ser empleados para el intercambio de información entre ambos sistemas.

Se produce una interconexión entre sistemas cuando existe una conexión y se habilitan flujos de información entre ellos.

Cuando se produce una interconexión entre sistemas surgen nuevas vulnerabilidades y amenazas que afectan a la confidencialidad, integridad y disponibilidad de la información manejada por dichos sistemas, principalmente por las siguientes razones:

- Se incrementa el número de usuarios (autorizados y no autorizados) que acceden a los sistemas.
- El nuevo sistema que se interconecta puede tener conexiones o vías de acceso desconocidas para los administradores y supervisores de seguridad del sistema que se considere.

- El nuevo sistema que se interconecta puede tener unas amenazas distintas a las que en su día se consideraron para establecer los requisitos de seguridad del sistema en cuestión.
- El flujo de información entre ambos sistemas puede requerir restricciones concretas.
- Ambos sistemas pueden tener distintas políticas de seguridad, diferentes niveles de confianza, diferentes AOSTIC o una combinación de las anteriores.

Por ello es necesaria la acreditación de la interconexión de sistemas al mayor grado de clasificación de la información que manejen.

Todos los sistemas que manejen información clasificada, como paso previo a la solicitud de acreditación de su interconexión a otro sistema, redes públicas o similares, deberán estar en posesión de un certificado de acreditación al nivel correspondiente a la información que manejen.

La acreditación de la interconexión de un sistema es responsabilidad de la AAS. El procedimiento de acreditación y los requisitos de seguridad serán los que se indican o refieren en esta norma.

Seguridad criptológica

Solamente se podrán utilizar los productos y sistemas de cifra certificados, cualquiera que sea el nivel de clasificación de la información manejada. No está autorizado el uso de productos de cifra comerciales no certificados para la protección de información clasificada. Las excepciones a esta norma requerirán la aprobación de la AAS.

La naturaleza sensible de la información y de los productos y mecanismos criptográficos utilizados para proteger la confidencialidad, la integridad y la disponibilidad de la información clasificada requiere la aplicación de precauciones especiales de seguridad que van más allá de las que se necesitan para proteger otro tipo de información clasificada.

La protección que habrá que proporcionar a la información y a los productos y mecanismos criptográficos será proporcional al daño que se podría causar si fallara dicha protección. Habrá medios positivos de valorar y verificar la protección y el adecuado funcionamiento de los productos y mecanismos criptográficos y la protección y el control de la información criptográfica.

Los servicios de protección de información clasificada serán responsables, en su ámbito de competencia, de asegurar la correcta aplicación de la normativa de

protección en las instalaciones de las cuentas de cifra; por ello tramitarán hacia la ANPIC las solicitudes de apertura y cierre de estas. No serán responsables, sin embargo, del registro y control del material de cifra en ellos almacenados, al depender dicha función de las autoridades específicas de control y distribución del material de cifra.

Los servicios de protección de información clasificada llevarán registro de:

- Las zonas de acceso restringido donde se ubican las cuentas de cifra.
- El personal autorizado para acceder a las cuentas de cifra.

Podrán inspeccionar dichas instalaciones y serán responsables de la formación en seguridad de su personal, no pudiendo inspeccionar el material de cifra, salvo que se le haya asignado específicamente esa función.

En cada departamento, organismo o entidad que necesite manejar material de cifra, existirá una estructura de seguridad específica, responsable del control y gestión del material de cifra. Esta estructura de seguridad será responsable de:

- Decidir que existe la necesidad de establecer una cuenta de cifra.
- Relacionarse con las autoridades responsables de la generación y distribución de claves en su ámbito.
- Recibir, custodiar, gestionar, controlar, distribuir y, en su caso destruir, el material de cifra.
- Instruir a los usuarios para el manejo de material de cifra.
- Auditar la utilización del material de cifra a su cargo.
- Gestionar los incidentes de seguridad relativos al material de cifra a su cargo.
- Coordinar sus actuaciones con el órgano de control del que dependan, especialmente para gestionar las aperturas y cierres de las cuentas de cifra.

La apertura de una cuenta de cifra requerirá el nombramiento de un criptocustodio responsable, así como de un criptocustodio suplente, que asumirá todas las responsabilidades y obligaciones de aquel en su ausencia.

El material de cifra puede dividirse en:

- Material de claves, que incluye soportes de claves, sistemas de códigos, sistemas de autenticación y demás tipos de claves que deben cambiarse a intervalos previamente determinados y se emplean directamente en el proceso de cifrado y descifrado. Dentro del material de claves se puede distinguir entre:

  - Claves de alto nivel: Son aquellas claves con un grado de clasificación de «RESERVADO o equivalente» o «SECRETO o equivalente»
  - Claves de bajo nivel: Son aquellas claves con un grado de clasificación no superior a «CONFIDENCIAL o equivalente»

- Equipos de cifra, que incluye cualquier dispositivo o mecanismo empleado para cifrar y descifrar la información.
- Publicaciones de cifra, que incluye toda la documentación controlada, principalmente técnica, asociada a los equipos de cifra y material de claves, relativa a su uso, instalación, mantenimiento o composición, que no tenga carácter público, y en la que la información que porta debe ser protegida.

El acceso a material de cifra de grado «CONFIDENCIAL o equivalente» o superior, quedará restringido a las personas que dispongan de HPS de grado apropiado y, en los casos en que se especifique, podrá requerir la especialidad CRIPTO.

El material de cifra requiere de medios de almacenamiento específicos, por lo que se almacenará de forma independiente y físicamente separada de cualquier otra información clasificada.

Todo material de cifra utilizado para la protección de información clasificada estará a su vez clasificado, como mínimo con el grado de «DIFUSIÓN LIMITADA o equivalente».

El material de claves y las publicaciones de cifra llevarán, además de la marca correspondiente a su grado de clasificación, la marca adicional CRIPTO.

Por equipo de cifra controlado (ECC) se entenderá aquel elemento o dispositivo que, al no tener incorporados los elementos de cifra clasificados necesarios para su funcionamiento seguro, tendrá la consideración de equipo no clasificado. Cuando en una instalación responsable no se puede asegurar que existan las condiciones para un adecuado control y custodia de estos equipos ECC, se les obligará a darle tratamiento de «CONFIDENCIAL o equivalente», como forma de asegurar su correcta protección.

Los ECC serán contabilizados en las cuentas de cifra y deben ser almacenados de forma tal que sea suficiente para impedir toda oportunidad razonable de robo, sabotaje, manipulación, o acceso no autorizado.

Seguridad de las emanaciones

De acuerdo con el riesgo de explotación y la sensibilidad de la información manejada, se implementarán medidas de seguridad adecuadas que permitan la protec-

ción de la información clasificada contra los fenómenos de radiación electromagnética no deseados.

Cuando existan requisitos de protección contra la emisión de radiaciones o señales no deseadas (requisitos TEMPEST), solamente se podrán utilizar productos y sistemas certificados. Asimismo, los locales donde se ubiquen estos equipos deberán disponer de la correspondiente certificación ZONING.

Se aplicarán medidas concretas de seguridad para proteger la información clasificada de grado «CONFIDENCIAL o equivalente» o superior frente a situaciones de peligro derivadas de emisiones electromagnéticas. Estas medidas serán proporcionales al riesgo de explotación y al grado de sensibilidad de la información.

5.4.7. Documentación de seguridad

Todo sistema que maneje información clasificada deberá tener actualizada la siguiente documentación de seguridad:

	SECRETO/RESERVADO o equivalente	**CONFIDENCIAL o equivalente**	**DIFUSIÓN LIMITADA o equivalente**
Declaración de requisitos de seguridad comunes (DRSC)	Sí	Sí	Sí
Declaración de requisitos de seguridad de la interconexión (DRSI)	Sí	Sí	Sí
Análisis de riesgos	Formal	Formal	No formal
Concepto de operación (CO)	Sí	Sí	Sí
Declaración de requisitos específicos de seguridad (DRES)	Sí	Sí	Opcional
Procedimientos operativos de seguridad (POS)	Sí	Sí	Sí
Certificado de acreditación de zonas de acceso restringido	Sí	Sí	No *
Certificación ZONING de locales	Sí	Sí	No
Certificación TEMPEST de equipamiento	Sí	Sí	No
Certificado de acreditación	Sí	Sí	Sí

* En este caso se presentará la declaración de constitución de las zonas administrativas de protección.

La declaración de requisitos de seguridad comunes (DRSC) es un documento sólo exigido cuando existe un conjunto de sistemas interconectados (un sistema de sistemas), o cuando la complejidad y extensión del sistema así lo requieran. Este documento se ajustará al modelo definido en la guía CCN-STIC 202.

La declaración de requisitos de seguridad de la interconexión (DRSI) se redactará cuando se requiera interconectar varios sistemas autorizados. Este documento se ajustará al modelo definido en la guía CCN-STIC 202.

El análisis de riesgos se ajustará a la metodología descrita en la guía CCN-STIC 410.

El documento de concepto de operación (CO) se ajustará al modelo definido en la guía CCN-STIC 207.

El documento de declaración de requisitos de seguridad (DRES) se ajustará al modelo definido en la guía CCN-STIC 202.

El documento de procedimientos operativos de seguridad (POS) se ajustará al modelo definido en la guía CCN-STIC 203.

En los casos en que se cumplan todos y cada uno de los criterios relacionados a continuación, podrán reemplazarse los documentos CO, DRES y POS por un único documento abreviado CO/DRES/POS (definido en la guía CCN-STIC 204):

- Equipos aislados o pequeñas redes (máximo 1 servidor y 10 estaciones), y
- que manejen información clasificada de grado «RESERVADO o equivalente» o inferior, y
- que estén ubicados dentro del mismo entorno global de seguridad, y
- que trabajen en el modo seguro de operación «unificado al nivel superior» o «dedicado».

Adicionalmente, para sistemas encuadrados en programas de organismos internacionales, el correspondiente panel de acreditación podrá exigir cuanta documentación adicional estime oportuna.

NORMA NS/06

SEGURIDAD INDUSTRIAL

1. INTRODUCCIÓN

La Seguridad industrial es la condición que se alcanza cuando se aplica un conjunto de medidas y procedimientos necesarios para establecer y verificar los requisitos que deben cumplirse por todas las partes intervinientes tanto en las negociaciones pre-contractuales como a lo largo de la duración de los contratos, proyectos o programas clasificados.

Los aspectos generales para el manejo de la información clasificada se rigen conforme a lo establecido en el desarrollo de las normas (NS/01 a NS/05) de la ANPIC. La presente norma NS/06 sobre seguridad industrial regula las condiciones **específicas** que el manejo de información clasificada presenta en las actividades, contratos y programas clasificados encomendados a la industria para su desarrollo y ejecución.

La razón del establecimiento de una norma específica sobre protección de la información clasificada para este ámbito radica en las especiales connotaciones presentes en este tipo de relaciones con las empresas. Por un lado, se da la circunstancia de que entidades y personal ajeno al propietario o depositario principal de la información (la propia Administración, país u organización) necesitan acceder a la información clasificada. Por otro lado, estas entidades o personas que acceden con ocasión de un contrato o actividad, lo hacen en virtud de un interés puramente comercial. Ambas circunstancias constituyen un elemento adicional de riesgo para la información clasificada, por lo que las medidas de protección y control de las actividades, contratos y programas clasificados han de tener un carácter especial, más restrictivo que en otras circunstancias ya reguladas por el resto de la normativa.

Por tanto, en el marco establecido por la norma NS/01 sobre la estructura nacional de protección de la información clasificada, la presente norma regula la seguri-

dad de la información clasificada que se genere, maneje o acceda por empresas o entidades privadas radicadas en España en el desarrollo de actividades, contratos o proyectos en los que intervengan:

a) Entes, organismos o entidades que conforman el sector público, tal y como se define en la Ley de Contratos del Sector Público, así como entidades privadas debidamente autorizadas para manejar información clasificada.
b) Organizaciones internacionales de las que el Reino de España forma parte, en virtud de un tratado, como son la Organización del Tratado Atlántico Norte (OTAN), la Unión Europea (UE), la Agencia Espacial Europea (ESA), la Organización Conjunta de Cooperación en materia de Armamento (OCCAR), etc.
c) Países extranjeros al amparo de tratados internacionales, bilaterales o multilaterales, para la protección de información clasificada.

En este contexto, las disposiciones de esta norma afectan, tanto a los contratistas o subcontratistas que optan a participar o participan en actividades, contratos, programas o proyectos clasificados, como a los entes, organismos o entidades que conforman el sector público, que ofertan dichos contratos o que, en nombre de la ANPIC, han de supervisar y avalar dicha participación en un contexto internacional.

2. ORGANIZACIÓN DEL SECTOR PÚBLICO PARA LA SEGURIDAD INDUSTRIAL

La participación de la industria nacional en las actividades, contratos, programas y proyectos clasificados implica el establecimiento de especiales relaciones entre las empresas y el sector público.

En el sector público, los órganos con capacidad de contratación son múltiples y no están centralizados, ni tan siquiera a nivel ministerial. Ello conlleva que la relación de la industria con el sector público se realice habitualmente a través de un órgano competente para cada actividad o contrato en curso.

Esto, desde el punto de vista de la seguridad de la información clasificada en el ámbito industrial, aconseja el establecimiento de unas estructuras a nivel estatal que permitan centralizar el proceso de habilitación de las empresas, de forma que dicha habilitación sea reconocida por cualquier órgano con capacidad de contratación, y avalada ante otros países y organizaciones internacionales.

2.1. Órganos y autoridades

Los órganos y autoridades con responsabilidades en la protección de la información clasificada en el ámbito industrial son los siguientes:

a) ANPIC: Es la Autoridad responsable de desarrollar la política para la protección de la información clasificada, garantizar su cumplimiento, y definir y establecer la estructura funcional necesaria para la protección de la información clasificada en las administraciones públicas y en los organismos públicos vinculados o dependientes de ella, así como en las entidades públicas o privadas que precisen disponer de información clasificada.

b) Oficina Nacional de Seguridad (ONS): Es el órgano de trabajo de la ANPIC para el ejercicio de las funciones señaladas en el apartado 2.2 de la NS01.

c) Área de seguridad de la información clasificada en el ámbito industrial: Dentro de cada departamento ministerial es el organismo de protección específico, responsable del seguimiento y control de la información clasificada que se deba entregar o esté en poder de la industria, así como de comunicar a la misma la política de seguridad industrial y de proporcionar dirección y apoyo en su aplicación. De dicho organismo de protección específico dependerán los órganos de control para la protección de la información clasificada por él establecidos en las empresas. Deberá constituirse cuando por un departamento ministerial se lleven a cabo actividades, contratos, programas o proyectos clasificados. En la esfera internacional esta figura se conoce bajo el nombre de Autoridad de Seguridad Designada (ASD) en el ámbito de la seguridad industrial.

d) Órganos de control de la información clasificada del contratista: Son los elementos constituidos dentro de cada empresa que maneja información clasificada, para garantizar la adecuada protección de la información clasificada custodiada y manejada por dicha empresa, o a la que pudiera acceder personal de la empresa en el ejercicio de su trabajo. Cada órgano de control estará dotado de medios humanos y materiales necesarios para cumplir su función**.**

e) Oficina de programa: Entidad del sector público responsable de la dirección, ejecución y control de todos los contratos clasificados que se derivan de un programa o proyecto clasificado, de mantener actualizada la guía de clasificación y de verificar el cumplimiento de las instrucciones de seguridad del programa, si existiesen, así como de conocer las directivas de clasificación que puedan afectar al mismo. Toda oficina de programa que gestione contratos clasificados deberá estar asignada a un órgano de control de información clasificada o disponer de uno propio para el adecuado control de la información clasificada.

f) Órgano de contratación: Entidad del sector público unipersonal o colegiada que en virtud de norma legal o reglamentaria o disposición estatutaria tenga atribuida la facultad de celebrar contratos. Todo órgano de contratación que celebre contratos clasificados deberá estar asignado a un órgano de control de información clasificada o disponer de uno propio para el adecuado control de la información clasificada que maneje. Asumirá las misiones de la oficina de programa si esta última no existe.
g) Organismo o ente responsable de una actividad clasificada: Entidad del sector público responsable de la seguridad de la información clasificada que se accede, maneja o genera en el desarrollo una actividad clasificada.
h) Inspector de seguridad industrial: Será el representante ante la empresa del departamento ministerial al que pertenezca la información clasificada manejada por el contratista en los aspectos relativos a la seguridad de la información del departamento. Será nombrado por el área de seguridad de la información clasificada en el ámbito industrial.

En los siguientes apartados se establecen y definen los cometidos de los diferentes órganos y autoridades que intervienen en la protección de la información clasificada en el ámbito de la seguridad industrial.

2.1.1. Autoridad Nacional de Seguridad para la Protección de la Información Clasificada

En el ámbito de la seguridad industrial, tiene los siguientes cometidos, que serán desarrollados por la Oficina Nacional de Seguridad.

a) Conceder, modificar, denegar, cancelar, suspender temporalmente o reactivar la HSEM y la HSES de las empresas que participen o vayan a participar en actividades, programas, proyectos o contratos, clasificados.
b) Certificar, a instancias de los organismos nacionales o extranjeros, el grado y la validez de la HSEM y HSES de las empresas españolas, y el grado y validez de la HPS del personal de las empresas.
c) Reconocer, al amparo de la normativa internacional vigente, las habilitaciones expedidas por otros estados, así como certificar al órgano de contratación dicha circunstancia.
d) Autorizar, a propuesta del área de seguridad de la información clasificada en el ámbito industrial de los distintos departamentos ministeriales, las aperturas, cierres o modificaciones de los órganos de control, cuentas de cifra y sistemas de información y comunicaciones acreditados correspondientes a las empresas.

e) Nombrar o retirar el nombramiento de director de seguridad de grupo empresarial, de director de seguridad del servicio de protección y de jefe de seguridad del servicio de protección de información clasificada de empresa, así como de los suplentes de cada uno de los anteriores.

f) Aprobar, previa solicitud del área de seguridad de la información clasificada en el ámbito industrial de los distintos departamentos ministeriales, el nombramiento de los jefes de seguridad de los órganos de control establecidos en las empresas, de los administradores de seguridad de los sistemas acreditados para el manejo de información clasificada, de los criptocustodios, y de los suplentes de cada uno de ellos.

g) Aprobar los planes de protección y emitir los correspondientes certificados de acreditación de locales de la estructura establecida por las empresas.

h) Asesorar al área de seguridad de la información clasificada en el ámbito industrial de los distintos departamentos ministeriales sobre la elaboración e interpretación de la normativa sobre protección de la información clasificada en poder de las empresas.

i) Asesorar al área de seguridad de la información clasificada en el ámbito industrial de los distintos departamentos ministeriales en la formación y sensibilización de las distintas partes implicadas en la protección de la información clasificada en poder de las empresas.

j) Aprobar las medidas correctivas que se establezcan como resultado de las inspecciones ordinarias que el área de seguridad de la información clasificada en el ámbito industrial de los distintos departamentos ministeriales realice a aquellos órganos de control establecidos en las empresas y dependientes de ella.

k) Realizar inspecciones ordinarias a las empresas con HSEM concedida.

l) Realizar inspecciones extraordinarias de los órganos de control establecidos en las empresas.

m) Aprobar las instrucciones de seguridad de programas internacionales, así como asesorar en su elaboración y aplicación.

n) Tramitar, hacia los organismos extranjeros competentes para su aprobación, las solicitudes de visita de personal de empresas y organismos españoles a empresas extranjeras y de personal de empresas españolas a organismos extranjeros. Dicha tramitación podrá ser delegada en el área de seguridad de la información clasificada en el ámbito industrial de los distintos departamentos ministeriales cuando las circunstancias así lo aconsejen.

o) Tramitar al área de seguridad de la información clasificada en el ámbito industrial de los distintos departamentos ministeriales implicados, las solicitudes de visitas de personal de empresas y organismos extranjeros a empresas españolas, recibidas de los organismos extranjeros compe-

tentes. Dicha recepción podrá ser delegada en el área de seguridad de la información clasificada en el ámbito industrial de los distintos departamentos ministeriales cuando las circunstancias así lo aconsejen.

p) Aprobar las visitas de personal de la industria extranjera a organismos de los departamentos ministeriales españoles, recibidas de los organismos extranjeros competentes. Este proceso podrá ser delegado en el área de seguridad de la información clasificada en el ámbito industrial de los distintos departamentos ministeriales cuando las circunstancias así lo aconsejen.

q) Tramitar hacia los organismos extranjeros para su aprobación, los planes de transporte de material clasificado que se remita a empresas sitas en el extranjero. Este proceso podrá ser delegado en el área de seguridad de la información clasificada en el ámbito industrial de los distintos departamentos ministeriales cuando las circunstancias así lo aconsejen.

r) Aprobar, los planes de transporte de material clasificado proveniente del extranjero con destino a las empresas españolas, recibidos de los organismos extranjeros competentes. Dicha recepción y aprobación podrá ser delegada en el área de seguridad de la información clasificada en el ámbito industrial de los distintos departamentos ministeriales cuando las circunstancias así lo aconsejen.

s) Aprobar los planes de transporte de material clasificado de terceros países u organizaciones internacionales que se realicen dentro del territorio nacional. Dicha aprobación podrá ser delegada en el área de seguridad de la información clasificada en el ámbito industrial de los distintos departamentos ministeriales cuando las circunstancias así lo aconsejen.

t) Aprobar los planes marco de transportes internacionales de material clasificado.

u) Emitir, tramitar y controlar los certificados de correo que deberán portar los transportistas de información clasificada en sus desplazamientos a terceros países así como dentro de territorio nacional cuando dicha información pertenezca a otros países u organizaciones internacionales, esta facultad podrá ser delegada.

2.1.2. Área de seguridad de la información clasificada en el ámbito industrial.

Tiene los siguientes cometidos:

a) Verificar que en cada órgano de contratación y en cada oficina de programa se ha constituido un órgano de control de la información clasificada, o bien verificar que dichos órganos de contratación u oficinas de programa están asignados a otro órgano de control ya existente.

b) Establecer, en el caso de que no existan, los órganos de control de la información clasificada de los contratistas. Cada órgano de control de los contratistas dependerá funcionalmente del área de seguridad de la información clasificada en el ámbito industrial del departamento que lo constituyó.
c) Velar que se mantienen las condiciones de seguridad en los órganos de control de la información clasificada de su dependencia, mediante la realización de inspecciones periódicas.
d) Organizar los cursos de formación necesarios para el personal de los órganos de control de la información clasificada de su dependencia.
e) Designar al inspector de seguridad industrial ante los contratistas que proceda.
f) Tramitar ante la Autoridad Nacional las solicitudes de HSEM, HSES y HPS presentadas por los contratistas, y establecer el registro correspondiente para su control y custodia.
g) Asumir las funciones correspondientes al inspector de seguridad industrial, para aquellas empresas que no lo tuvieren asignado.
h) Tramitar, por delegación de la ONS, las solicitudes de visitas y planes de transporte.
i) Canalizar hacia la ONS los informes sobre incidentes de seguridad de la información clasificada, provenientes de los órganos de control de los contratistas de su ámbito.
j) Elaborar informe anual sobre el estado de la seguridad de la información clasificada en poder de contratistas que se remitirá antes del 31 de enero a la ONS.
k) Realizar, a requerimiento de la ONS, la investigación de los comprometimientos de la información clasificada en poder de las empresas cedida por su Ministerio, de acuerdo con lo estipulado en la norma NS04 sobre seguridad de la información.
l) Tramitar y controlar, por delegación de la ONS, los certificados de correo que deberán portar los transportistas de información clasificada en sus desplazamientos.

De manera excepcional, la ONS asumirá las funciones del área de seguridad de la información clasificada en el ámbito industrial de aquellos departamentos ministeriales que no hayan constituido aún dicho área, cuando existan actividades, contratos, programas o proyectos que impliquen acceso o generen información clasificada. Esta asunción de funciones se efectuará durante el tiempo imprescindible para que el departamento ministerial afectado establezca dicha estructura de protección. En este caso, la ANPIC requerirá a los responsables de tales actividades, programas o contratos el establecimiento de los órganos de control imprescindibles para el cumplimiento de la presente norma.

2.1.3. Inspector de seguridad industrial.

Sus cometidos serán:

a) Controlar el marcado de la información clasificada que genere o reproduzca el contratista, previa autorización del órgano responsable del contrato, programa o proyecto clasificado, con arreglo a la guía de clasificación.
b) Controlar las modificaciones que puedan producirse en los sistemas de protección de la información clasificada del contratista establecidos en el correspondiente plan de protección.
c) Certificar la necesidad que tienen los empleados del contratista de solicitar HPS en relación a la función que desempeñan o puedan desempeñar, firmando en su caso las solicitudes de HPS.
d) Informar sobre los incidentes de seguridad que afecten o puedan afectar a la información clasificada, que se produzcan en las instalaciones del contratista, y sobre posibles riesgos que afecten o puedan afectar a la misma.
e) Velar por el cumplimiento de las instrucciones de seguridad relativas a los contratos, programas o proyectos clasificados que esté desarrollando el contratista.

2.1.4. Oficinas de programa

La oficina de programa, como responsable del control de todos los contratos clasificados que gestiona, designará un oficial de seguridad que la representará ante el contratista en los aspectos relativos a la seguridad de la información manejada durante el desarrollo del programa o proyecto.

El oficial de seguridad designado será responsable de los siguientes cometidos:

a) Actuar como vocal técnico de seguridad de la información clasificada, en las mesas de contratación relativas al programa o proyecto clasificado para el cual ha sido designado.
b) Velar por que el contratista proporcione un adecuado tratamiento a la información clasificada del programa o proyecto que le hayan sido asignados.
c) Firmar las expectativas para acceder a información clasificada de potenciales contratistas, de manera que éstos puedan solicitar la concesión de la HSEM, y en caso necesario la HSES, que le permita licitar a contratos clasificados derivados del programa o proyecto.
d) Firmar las autorizaciones de acceso a la información clasificada del personal habilitado del contratista y de los subcontratistas.

e) Comunicar al área de seguridad de la información clasificada en el ámbito industrial de su departamento ministerial cualquier incidencia que estime pueda comprometer la seguridad de la información clasificada del programa o proyecto.
f) Establecer las condiciones específicas de seguridad de los contratos así como participar en la elaboración de las instrucciones de seguridad del programa que habrá de remitir al área de seguridad de la información clasificada en el ámbito industrial de su departamento ministerial.
g) Remitir al área de seguridad de la información clasificada en el ámbito industrial de su departamento ministerial antes del 15 de enero de cada año el inventario anual de la información clasificada que durante el año anterior se haya confiado a los distintos contratistas o haya sido generada por éstos.
h) En caso de no disponer de un órgano de control propio, informar al órgano de control del que dependa de la información clasificada entregada a los contratistas en el marco de los programas y proyectos por ellos gestionados.
i) Retirar a través del órgano de control correspondiente la información clasificada que obre en poder del contratista a la finalización, no adjudicación o suspensión del contrato, o bien a la cancelación o suspensión temporal de la HSEM o HSES.
j) Tramitar y controlar, en base a los planes de transporte aprobados, los certificados de correo que deberán portar los transportistas, en sus desplazamientos por el territorio nacional, de información clasificada de aquellos contratos y programas clasificados de su responsabilidad.

2.1.5. Órganos de contratación

Los órganos de contratación en el sector público son responsables de:

a) Certificar las expectativas para acceder a información clasificada de potenciales contratistas, de manera que éstos puedan solicitar la concesión de la HSEM y en caso necesario, la HSES, que le permita licitar al contrato clasificado.
b) Exigir el requisito de tenencia de HSEM y en su caso de HSES para un determinado grado de clasificación en las cláusulas administrativas particulares de cualquier contrato clasificado.
c) Comprobar que todo contrato clasificado lleve anexo la correspondiente «Comunicación de Contrato Clasificado» al contratista, según modelo de la ONS, disponible en la página web: www.cni.es/es/ons, que incluye:
  – Declaración de clasificación del contrato.
  – Cláusulas de seguridad.
  – Guía de clasificación.

d) Remitir una copia de las comunicaciones de contrato clasificado a la Oficina Nacional de Seguridad a través del Área de Seguridad de la Información Clasificada en el ámbito industrial de su departamento ministerial.
e) Establecer las condiciones específicas de seguridad en los contratos o proyectos que habrá de remitir al área de Seguridad de la información clasificada en el ámbito industrial de su departamento ministerial.
f) Remitir al área de seguridad de la información clasificada en el ámbito industrial de su departamento ministerial antes del 15 de enero de cada año el inventario anual de la información clasificada que durante el año anterior se haya confiado a los distintos contratistas o haya sido generada por éstos.
g) En caso de no disponer de un órgano de control propio, informar al órgano de control del que dependa de la información clasificada entregada a los contratistas en el marco de los programas y proyectos por ellos gestionados.
h) Retirar a través del órgano de control correspondiente la información clasificada que obre en poder del contratista a la finalización, no adjudicación o suspensión del contrato, o bien a la cancelación o suspensión temporal de la HSEM o HSES.
i) Tramitar y controlar, en base a los planes de transporte aprobados, los certificados de correo que deberán portar los transportistas, en sus desplazamientos por el territorio nacional, de información clasificada de aquellos contratos clasificados de su responsabilidad.

2.1.6. Organismos o entes responsables de una actividad clasificada

Existen determinadas situaciones en las que es necesario asignar el desarrollo de una determinada actividad clasificada a empresas designadas al efecto. Hablaremos entonces de actividades clasificadas, las cuales no se derivan de contrato, programa o proyecto clasificado.

Dicha actividades siempre estarán promovidas por un organismo o ente del sector público que será responsable de controlar la seguridad de la información clasificada generada o maneja en el desarrollo de dicha actividad.

Para el desarrollo de una actividad clasificada, todo organismo o ente promotor de la misma deberá estar asignado a un órgano de control de información clasificada, o disponer de uno propio para el adecuado control de la información clasificada que sea generada o manejada.

En el marco del desarrollo de dichas actividades clasificadas, los entes u organismos promotores ejercerán los siguientes cometidos en el ámbito de la seguridad industrial:

a) Elaborar la propuesta de la guía de clasificación para aprobación por la autoridad de clasificación, en la que se detalle la clasificación de los elementos de la actividad clasificada.
b) Establecer las condiciones específicas de seguridad de la actividad clasificada.
c) Velar por el adecuado tratamiento de la información clasificada generada o manejada.
d) Comprobar que las empresas implicadas en el desarrollo de la actividad clasificada están en posesión de la HSEM y, en caso necesario, de la HSES.
e) Firmar las autorizaciones de acceso a la información clasificada del personal habilitado de las empresas implicadas.
f) Remitir al órgano de control del que dependa antes del 15 de enero de cada año el inventario anual de la información clasificada que durante el año anterior se haya entregado a las empresas implicadas o haya sido generada por éstas.
g) Designar un oficial de seguridad que representará al ente u organismo ante las empresas implicadas en los aspectos relativos a la seguridad de la información siendo responsable de los siguientes cometidos:

– Controlar el marcado de la información clasificada con arreglo a la guía de clasificación.
– Controlar las modificaciones que puedan producirse en los sistemas de protección de la información clasificada de las empresas implicadas establecidas en el correspondiente plan de protección.
– Certificar la necesidad que tienen los empleados de las empresas implicadas de solicitar HPS en relación a la función que desempeñan o puedan desempeñar, firmando en su caso las solicitudes de HPS.
– Firmar las autorizaciones de acceso a la información clasificada del personal habilitado de las empresas implicadas.
– Informar de las incidencias de seguridad de la información clasificada que se produzcan o puedan producirse en las instalaciones de las empresas implicadas.
– Velar por el cumplimiento de las instrucciones de seguridad relativas a la actividad clasificada.

h) Tramitar, por delegación de la ONS, las solicitudes de visitas y planes de transporte.
i) Tramitar y controlar, en base a los planes de transporte aprobados, los certificados de correo que deberán portar los transportistas, en sus desplazamientos por el territorio nacional, de información clasificada de aquellos contratos y programas clasificados de su responsabilidad.

j) Canalizar hacia la ONS los informes de incidencias de seguridad de la información clasificada.
k) Elaborar un informe anual sobre el estado de la seguridad de la información clasificada en las empresas implicadas que remitirá antes del 31 de enero de cada año a la ONS.
l) Realizar, a requerimiento de la ONS, la investigación de los comprometimientos de la información clasificada conforme a lo estipulado en la norma NS04 sobre seguridad de la información.
m) Retirar a través del órgano de control correspondiente la información clasificada que obre en poder del contratista a la finalización, no adjudicación o suspensión del contrato, o bien a la cancelación o suspensión temporal de la HSEM o HSES.

3. REQUISITOS DE SEGURIDAD EN LA INDUSTRIA

3.1. Actividades, contratos, programas y proyectos clasificados

Para participar en cualquier actividad, contrato, programa o proyecto clasificado de grado «CONFIDENCIAL o equivalente» o superior, el contratista deberá disponer de la HSEM del grado adecuado a la información que vaya a manejar. Las HSEM podrán ser de uno de los siguientes grados: «SECRETO o equivalente», «RESERVADO o equivalente» y «CONFIDENCIAL o equivalente».

La concesión de una HSEM implica que la ANPIC ha determinado positivamente la capacidad y fiabilidad de un contratista para generar y acceder a información clasificada hasta un determinado grado, sin que le habilite para manejar o almacenar dicha información en sus propias instalaciones.

Aquellos contratistas que necesiten manejar, almacenar o generar información clasificada en sus instalaciones necesitarán disponer, además, de HSES del grado adecuado.

La concesión de una HSES implica que el contratista ha implantado un sistema de protección basado en órganos de control del tipo y grado adecuados al grado de la información clasificada que se vaya a manejar, almacenar o generar dentro de su organización de acuerdo con las exigencias de seguridad física establecidas en la normativa aplicable, y que dicho sistema de protección ha sido evaluado de manera positiva por el organismo correspondiente.

Un mismo contratista que disponga de HSEM podrá solicitar varias HSES, una por cada instalación en la que vaya a manejar, almacenar o generar información clasificada.

En ningún caso, el grado de la HSES concedido a un contratista será de grado superior al de la HSEM del mismo.

La HSES y la HSEM serán siempre concedidas, modificadas, suspendidas o canceladas por la ANPIC, y serán inspeccionadas de manera periódica.

Los empleados que deban acceder a información clasificada deberán solicitar la HPS del grado y tipo correspondiente a la información para cuyo acceso vayan a ser autorizados.

3.2. Actividades y contratos clasificados de grado «SECRETO o equivalente».

Para que un contratista pueda acceder a información clasificada de grado «SECRETO o equivalente», deberá disponer de una HSEM de dicho grado.

Salvo casos excepcionales, autorizados expresamente por la ANPIC, la información clasificada de grado «SECRETO o equivalente» nunca será entregada al contratista, debiendo ser manejada en la zona de acceso restringido (ZAR) del órgano responsable de la actividad, contrato, programa o proyecto clasificado.

El personal del contratista que acceda a información clasificada de grado «SECRETO o equivalente» estará debidamente habilitado para este grado.

3.3. Actividades y contratos clasificados de grado «DIFUSIÓN LIMITADA o equivalente»

Para poder participar en cualquier actividad, contrato, programa o proyecto clasificado de grado «DIFUSIÓN LIMITADA o equivalente», no será necesario que el contratista disponga de HSEM ni de HSES, pero deberá firmar un Compromiso de Seguridad con la ANPIC, por el que se compromete a implantar en su organización una estructura de protección y a cumplir con los siguientes requisitos:

1. Efectuar el registro de la empresa ante la ANPIC y a firmar el Compromiso de Seguridad.
2. Designar de un oficial de seguridad responsable ante la ANPIC, que convocado a los cursos de instrucción y perfeccionamiento.
3. El oficial de seguridad será responsable de instruir, a su vez, a los empleados que necesiten acceder a la información clasificada manteniendo control y registro por medio de un documento acreditativo de dicha instrucción firmado por el interesado.

4. El oficial de seguridad será responsable de establecer las «Zonas Administrativas de Protección» precisas para el manejo de la información clasificada en sus propias instalaciones, y declararlas formalmente, conforme a los procedimientos y criterios de las Normas de la ANPIC.
5. Cuando se vaya a procesar información en sistemas CIS, el oficial de seguridad será responsable de iniciar el proceso de acreditación de dicho sistema, así como señalar al oficial INFOSEC responsable del mismo.

4. RESPONSABILIDADES DEL CONTRATISTA

4.1. Compromiso de seguridad

Todo contratista adjudicatario de un contrato, programa, proyecto o actividad que implique el acceso a información clasificada deberá firmar ante la ANPIC un Compromiso de Seguridad como paso previo a la adjudicación del contrato.

El compromiso de seguridad es el documento por el que el contratista o empresa se obliga voluntariamente ante la ANPIC al exacto cumplimiento de las disposiciones relativas a la protección de la información clasificada y, en particular, a las disposiciones de la presente normativa, mediante la firma del documento denominado «compromiso de seguridad» (anexos I y II). Dicho documento será firmado por un apoderado con poderes suficientes para la representación del contratista ante la Administración.

4.2. Obligaciones del contratista con HSEM

El contratista tras la firma del Compromiso de Seguridad y como requisitos para la concesión de la HSEM se compromete a:

a) Aplicar las medidas de seguridad exigidas por las normas de la ANPIC.
b) Implantar un servicio de protección de información clasificada conforme a los requerimientos de las normas de la ANPIC.
c) Proponer a la ANPIC para su nombramiento, un jefe de seguridad del servicio de protección (JSSP), así como un suplente del mismo, encargado de llevar a cabo las tareas y responsabilidades que el contratista contrae voluntariamente al firmar el compromiso de seguridad.
d) Proponer a la ANPIC para su nombramiento a un jefe de seguridad (JS) para cada órgano de control acreditado para el grado y tipo que corresponda, así como un suplente para cada uno de ellos. Los JS dependerán del JSSP cuando los nombramientos no recaigan en la misma persona.

e) Proponer a la ANPIC para su nombramiento a un director de seguridad del servicio de protección del grupo (DSSG) cuando sea requerido, así como su suplente.

f) Informar a la ANPIC sobre cualquier cambio socio-jurídico y especialmente los cambios de tipo societario, de capital social, de objeto social, domicilio, delegaciones y sucursales, accionistas, consejo de administración o administradores, personal directivo y terminación del negocio, en el plazo máximo de 30 días naturales.

g) Proponer, a la mayor brevedad posible, el nombramiento de un nuevo JSSP o JS cuando alguno de ellos cause baja, con el fin de evitar situaciones de inseguridad que conduzcan al incumplimiento de las Normas de la ANPIC.

h) Solicitar a la ANPIC:

- Las HPS de los empleados que deban manejar información clasificada.
- Las HSES para las instalaciones que así lo requieran.
- La apertura de los órganos de control y sus correspondientes zonas de acceso restringido (ZAR) necesarias para el manejo de información clasificada del tipo y grado adecuados.
- La acreditación de los sistemas de información y comunicaciones que manejen información clasificada.
- El nombramiento de los administradores de seguridad del sistema de información y los suplentes de éstos.
- El nombramiento de los criptocustodios y los suplentes de éstos.

i) Mantener actualizada la lista de empleados con HPS en vigor.

j) Informar a la ANPIC de cualquier modificación en los datos aportados para la obtención de la HSEM, la HSES, la HPS de sus empleados, y para el establecimiento de los órganos de control.

k) Remitir una copia de las comunicaciones de contrato clasificado recibidas así como de las cláusulas de seguridad de dichos contratos a la ONS a través del Área de Seguridad de la Información Clasificada en el ámbito industrial del departamento ministerial correspondiente.

l) Denegar el acceso a la información clasificada a cualquier persona que no esté expresamente autorizada, no esté debidamente habilitada o no tenga «necesidad de conocer».

m) Informar a la ONS de las visitas que, aun cuando no accedan a información clasificada o a una ZAR, puedan constituir una amenaza a la información clasificada, o que hayan sido requeridas por la ONS.

n) Informar inmediatamente a la ONS, de cualquier incidencia que pueda derivar en comprometimiento de la información clasificada, en especial:

- Intentos de acceso no autorizados, actos de sabotaje, o actividades que supongan un riesgo para dicha información.
- Vulneraciones o retrasos injustificados en la transmisión de información clasificada.
- Modificaciones que considere realizar en la ZAR.

o) Asegurarse de que al término de la actividad, o del contrato, o del proceso de concurso en que no haya sido adjudicatario, sea devuelta al órgano de control correspondiente, toda la información clasificada que se encuentre en su poder. Una vez cumplimentada esta obligación, se comunicará a la ONS.

p) No hacer publicidad de la formalización del compromiso de seguridad ni de las HPS, HSEM o HSES.

q) Colaborar en las investigaciones que se realicen para esclarecer posibles comprometimientos de la información clasificada en poder del contratista.

r) Colaborar en las inspecciones periódicas de la HSEM por parte de la ONS.

El cumplimiento de estas obligaciones no exime al contratista de observar cuantos requisitos de seguridad le sean impuestos en las cláusulas o instrucciones de seguridad de los contratos o programas clasificados.

La vulneración de cualquiera de las responsabilidades por parte del contratista podrá suponer la cancelación, temporal o definitiva, de la HSEM, de la HSES o el cierre temporal o definitivo de los órganos de control establecidos.

4.3. Composición del servicio de protección de información clasificada.

El servicio de protección del contratista está formado por el conjunto de personal, instalaciones, recursos materiales y procedimientos que, actuando coordinadamente, tienen como finalidad proteger la información clasificada en poder del contratista de los accesos no autorizados a la misma, y de la pérdida de su integridad y disponibilidad.

Formarán parte del servicio de protección de información clasificada del contratista, el jefe de seguridad del servicio de protección (JSSP) del contratista, el suplente del JSSP, así como el director de seguridad del servicio de protección (DSSP) y el director de seguridad del servicio de protección del grupo (DSSG) si los hubiera. Igualmente formarán parte del servicio de protección los jefes de seguridad (JS) de los órganos de control establecidos por el contratista, y todos los responsables de cada uno de los sistemas informáticos acreditados (administradores de seguridad de sistemas de información y comunicaciones, administradores del sistema, etc.).

Todos ellos ocuparán un puesto orgánico en la empresa con autoridad legalmente reconocida por la dirección de la empresa para establecer las medidas necesarias para una adecuada protección de la información clasificada, así como determinar la selección de personal que vaya a ocupar puestos de trabajo con acceso a información clasificada.

Todo el personal de la empresa que forme parte del servicio de protección deberá ostentar la nacionalidad española, tener HPS conforme al grado de la HSEM, y mantener una relación contractual estable con la empresa.

El contratista propondrá a la ANPIC las personas que considere adecuadas para formar parte del servicio de protección, en el caso en que la ANPIC descarte alguna persona propuesta, el contratista deberá proponer una nueva candidatura.

La ONS será responsable de proporcionar a los componentes del servicio de protección la instrucción necesaria para llevar a cabo sus misiones, estando su nombramiento efectivo supeditado a la asistencia y superación de los cursos de instrucción que la ANPIC determine.

4.4. Jefe de seguridad del servicio de protección

Corresponde al JSSP organizar, dirigir y controlar el servicio de protección así como cumplir y hacer cumplir la normativa vigente y llevar a cabo las responsabilidades del contratista descritas en el **apartado 4.2** de esta norma. Entre sus cometidos se encuentra, además de lo señalado en la norma NS/01 sobre estructura nacional de protección de la información clasificada:

a) Garantizar que todo el personal del contratista que acceda a información clasificada dispone de HPS adecuada y la oportuna necesidad de conocer, y que han sido debidamente instruidos en la protección de la información clasificada.
b) Recabar de los órganos responsables de la Administración las correspondientes autorizaciones de acceso a información clasificada para el personal del contratista.
c) Impartir periódicamente los cursos de formación para el manejo de información clasificada al personal del contratista que tenga concedida una HPS.
d) Gestionar las solicitudes de visita con acceso a información clasificada o a instalaciones clasificadas.
e) Establecer los procedimientos necesarios para el control de las visitas con acceso a información clasificada a las dependencias del contratista.

f) Organizar los transportes que impliquen el traslado de información clasificada.
g) Organizar y dirigir el sistema de registro y control de la información clasificada a cargo del contratista.
h) Relacionarse con los jefes de seguridad de otros órganos de control así como los JSSP de otros contratistas y subcontratistas.
i) Aplicar las instrucciones de seguridad de los programas clasificados y las cláusulas de seguridad relativas a la protección de la información clasificada en las encomiendas de gestión o contratos clasificados.
j) Revisar las cláusulas de seguridad de los contratos clasificados que celebre el contratista.

El suplente del JSSP asumirá los cometidos y responsabilidades del JSSP en caso de ausencia.

La inadecuación o inobservancia de sus cometidos podrá motivar el cese de los responsables del servicio de protección por parte de la ANPIC, previa notificación escrita al contratista, sin perjuicio de otras responsabilidades que se pudieran derivar.

4.5. Director de seguridad del servicio de protección

Cuando el contratista disponga de varios órganos de control bajo la responsabilidad de personas distintas podrá proponer que el JSSP sea nombrado director de seguridad del servicio de protección (DSSP).

El DSSP tendrá como misión principal la de coordinar la actuación de los diversos órganos de control establecidos en cada una de las instalaciones con HSES, sin que ello suponga merma de las responsabilidades que a dichos órganos de control les corresponde.

El cargo de DSSP se podrá compatibilizar con el de JS de alguno de los órganos de control establecidos.

4.6. Director de seguridad del servicio de protección de un grupo empresarial

Cuando el contratista forme parte de un grupo empresarial en el que exista más de una empresa que tenga HSEM, podrá proponer un director de seguridad del servicio de protección del grupo (DSSG), responsable de coordinar la acción de los distintos DSSP o JSSP.

Cuando el grupo empresarial esté implantado en más de una nación, el DSSG deberá tener representación en la estructura internacional de seguridad del mismo.

El DSSG remitirá con periodicidad anual a la ONS el esquema actualizado de la estructura y política de seguridad del grupo empresarial.

5. ÓRGANOS DE CONTROL DE LA INFORMACIÓN CLASIFICADA DEL CONTRATISTA

5.1. Generalidades

El establecimiento de los órganos de control de la información clasificada del contratista constituye uno de los requisitos tras la concesión de la HSEM, que deberán seguir lo estipulado en la norma NS/01 sobre estructura nacional de protección de la información clasificada.

Cada órgano de control está formado por el conjunto de personal, recursos materiales y procedimientos que, actuando coordinadamente, tienen como finalidad proteger la información clasificada del grado y tipo correspondiente al órgano de control de los riesgos que pueda provocar el acceso no autorizado a la misma, o afectar a su integridad y disponibilidad.

Cada órgano de control estará a cargo de un jefe de seguridad (JS) siendo compatible este cargo con el de JSSP.

Cuando así lo aconseje la distribución geográfica de la empresa o la dispersión de una instalación de la misma, el contratista podrá solicitar la constitución de varios órganos de control. El contratista podrá además disponer de varias ZAR dependientes del mismo órgano de control.

5.2. Personal

5.2.1. Personal del órgano de control

El órgano de control estará constituido por el jefe de seguridad, el suplente del jefe de seguridad, así como los administradores de seguridad de cada uno de los sistemas de información y comunicaciones acreditados para el manejo de Información Clasificada ubicados en el Órgano de Control, estos últimos cargos exigidos en la normativa STIC relativa a la acreditación de sistemas.

Todo el personal del órgano de control deberá estar en posesión de HPS acorde al grado de la HSEM y ostentar la nacionalidad española.

El contratista remitirá la propuesta de las personas que considere adecuadas para formar parte del órgano de control. En el caso de que la ANPIC descarte alguna persona propuesta, el contratista propondrá nueva candidatura.

El personal del órgano de control recibirá la instrucción necesaria para llevar a cabo sus misiones, y su nombramiento está supeditado a la superación de los cursos de instrucción que la ANPIC determine.

5.2.2. Jefe de seguridad

El JS del órgano de control dependerá funcionalmente del JSSP de la empresa y tendrá como misiones las establecidas en la norma NS01 sobre estructura nacional de protección de la información clasificada.

El incumplimiento de sus cometidos podrá motivar su cese por parte de la ANPIC, previa notificación escrita al contratista, sin perjuicio de otras responsabilidades que se pudieran derivar.

5.2.3. Administrador de seguridad del sistema de información

Cuando un órgano de control disponga de uno o varios sistemas autorizados para procesar información clasificada será preceptivo que cada uno de ellos disponga de un Administrador de Seguridad del Sistema de Información conforme a lo estipulado en la NS05 y las normas STIC.

Corresponde a los administradores de seguridad del sistema de información dirigir y controlar la seguridad de cada sistema de información y comunicaciones del contratista bajo su responsabilidad que maneje información clasificada, asegurándose de que estos sistemas se encuentren debidamente acreditados por la ANPIC.

Deberá actuar bajo la supervisión del JS del órgano de control, salvo que lo sea él mismo. Entre sus cometidos se encuentra, además de los señalados en la norma NS/05 sobre seguridad en los sistemas de información y comunicaciones los siguientes:

a) Elaborar, organizar e implantar los requisitos y procedimientos relativos a la seguridad de cada sistema de información y comunicaciones del con-

tratista bajo su responsabilidad, bien para obtener su autorización, o teniendo concedida dicha autorización, para mantener su eficacia a lo largo del tiempo.

b) Controlar que todo el personal con acceso a sistemas de información y comunicaciones está debidamente autorizado.

c) Investigar los incidentes que pudieran afectar al sistema de información y comunicaciones, evaluando en su caso las pérdidas de integridad, confidencialidad y disponibilidad que afectan a la información clasificada, e informando al JS de la situación.

d) Llevar a cabo un programa de formación continua de los usuarios del sistema de información y comunicaciones, sobre la observancia de los procedimientos de seguridad.

e) Gestionar y proporcionar los códigos de acceso u otras medidas de control de acceso al sistema de información y comunicaciones, asegurándose de que son cambiados periódicamente de acuerdo con el grado de clasificación de la información.

f) Supervisar la gestión de claves de cifra utilizadas en el sistema de información y comunicaciones, cuando estuviese en su ámbito de competencia. Para ello controlará su generación, almacenamiento, distribución, expiración y destrucción.

g) Controlar tanto las modificaciones que se realicen en cualquier componente del sistema de información y comunicaciones, asegurándose de que no se vea afectada la seguridad, como los aspectos de gestión de configuración de dichas modificaciones.

h) Comprobar que el mantenimiento de los sistemas de información y comunicaciones se realiza conforme a los procedimientos operativos de seguridad establecidos.

i) Verificar que los soportes de almacenamiento de información clasificada se custodian en ZAR debidamente acreditadas.

j) Evaluar los registros de seguridad del sistema de información y comunicaciones, asegurándose que son suficientes para un control eficaz.

k) Controlar y registrar las copias periódicas de seguridad.

5.3. Estructura

5.3.1. Concepto

Son los medios y medidas materiales de que dispone el órgano de control para ejercer su misión de proteger la información clasificada que deba ser manejada en sus instalaciones.

5.3.2. Sistema de protección física

Composición

Está formado por el conjunto de instalaciones y medidas de protección física del contratista que, actuando coordinadamente, tienen como finalidad proteger la información clasificada de los riesgos que pudieran afectarla.

Zona de acceso restringido (ZAR)

Cuando el contratista deba custodiar la información clasificada de grado «CONFIDENCIAL o equivalente» o superior en sus instalaciones, deberá solicitar una HSES y la apertura de un órgano de control con capacidad de almacenamiento del grado y tipo que corresponda, e incluir en la documentación de solicitud el plan de protección en el que se incluya la ZAR.

Las características constructivas de la ZAR, así como las medidas de seguridad adoptadas en la misma deben estar descritas en el plan de protección y ser conformes a lo que se indica en la norma NS/03 sobre seguridad física.

Operación y mantenimiento del sistema de protección física

La operación y el mantenimiento del sistema de protección física deben estar descritos en los procedimientos correspondientes, en conformidad con la norma NS/03 sobre seguridad física.

El plan de protección deberá detallar los procedimientos para el acceso del personal de mantenimiento y vigilancia a las ZAR, así como el grado de la HPS requerido.

5.3.3. Protección de los sistemas de información y comunicaciones

Cuando se haga uso de un sistema de información y comunicaciones para el almacenamiento, procesamiento o transmisión de información clasificada, obligatoriamente deberá cumplir con lo establecido en la norma NS/05 sobre sistemas de información y comunicaciones.

Para el manejo y custodia de información clasificada en un sistema de información y comunicaciones, el contratista deberá tener concedida una HSEM y una HSES del grado correspondiente, en donde se instalarán dichos sistemas. Deberá solicitar además a la ANPIC la acreditación del sistema de información y comuni-

caciones, según lo dispuesto en la norma NS/05 sobre sistemas de información y comunicaciones.

5.4. Organización

El contratista deberá elaborar un plan de protección, que deberá ser aprobado por la ONS, de forma previa a la obtención de la HSES. Dicho plan se ajustará a lo establecido en la norma NS/03 sobre seguridad física.

5.5. Inspecciones al órgano de control

Las inspecciones al órgano de control constituyen el mecanismo por el cual se controla y supervisa la estructura de protección de la información clasificada, para favorecer el cumplimiento de la presente normativa.

Las inspecciones a los órganos de control establecidos por las empresas seguirán lo estipulado en las normas NS01 a NS05, excepto para los órganos de control sin capacidad de almacenamiento de información clasificada, cuya inspección será efectuada mediante un cuestionario abreviado en el que no figurarán apartados relativos a seguridad física o seguridad documental. Junto con el cuestionario, la empresa inspeccionada deberá enviar una actualización de la «ficha del contratista» al órgano de control superior del que dependa, la cual será enviada a la ONS por el canal habitual establecido.

Las inspecciones pueden ser de dos tipos:

a) Ordinarias: Realizadas de forma periódica en un plazo no superior a sesenta (60) meses.
b) Extraordinarias: Realizadas a iniciativa de la ONS con motivo de incidencias o eventos que afecten o puedan afectar a la protección de la información clasificada.

En las inspecciones, tanto ordinarias como extraordinarias, es obligatoria la presencia del JS, o del suplente en caso de ausencia debidamente justificada del titular, así como otro personal dependiente del contratista que sea designado en la convocatoria.

Al término de cada inspección se realizará un informe indicando al contratista las acciones correctivas que debe implementar y requiriéndole un informe sobre los plazos en que va ejecutar las acciones. Salvo que el JS del órgano de control y el

JSSP sean la misma persona, el JS del órgano de control remitirá al JSSP a la mayor brevedad un informe sobre el cumplimiento de las acciones correctivas con los plazos previstos para llevarlas a cabo. Dicho informe de cumplimiento se remitirá por el JSSP, al término de cada plazo, a la ONS, a través del área de seguridad de la información clasificada en el ámbito industrial del departamento ministerial del que depende o del organismo o ente responsable de la actividad clasificada.

La falta de cumplimiento de las acciones correctivas señaladas en el informe de inspección puede ser determinante para la suspensión temporal o cancelación de la HSEM, así como las HSES y HPS correspondientes, sin perjuicio de las acciones legales que pueda llevar a cabo la ANPIC.

6. HABILITACIONES DE SEGURIDAD DE EMPRESA Y ESTABLECIMIENTO.

6.1. Habilitación de seguridad de empresa (HSEM)

6.1.1. Tramitación

Cuando una empresa o contratista quiera tomar parte en un contrato, programa o proyecto clasificado en el que se vaya a manejar información clasificada de grado «CONFIDENCIAL o equivalente», o superior, y no disponga previamente de HSEM, deberá presentar su solicitud de HSEM ante el área de seguridad de la información clasificada en el ámbito industrial, o servicio de protección de la información clasificada del departamento ministerial que origine el contrato, programa o proyecto clasificado al que pretenda concursar.

Cuando un organismo o ente del sector público desee promover una actividad clasificada de grado «CONFIDENCIAL o equivalente», o superior, deberá comprobar previamente a su adjudicación que la empresa adjudicataria cuenta con la HSEM, y en su caso con la HSES de los niveles apropiados para el desempeño de dicha actividad. En caso de que la empresa seleccionada para la ejecución de la actividad clasificada carezca de HSEM, ésta deberá tramitar su solicitud de HSEM a través del servicio de protección de materias clasificadas del organismo o ente promotor.

Si no existiera un servicio de protección de información clasificada en el departamento ministerial, o ente del sector público correspondiente, el contratista podrá presentar la solicitud directamente a la ANPIC.

La concesión de una HSEM implica al menos la solicitud por parte del contratista de un órgano de control sin capacidad de almacenar información clasificada, que

servirá como órgano de control para la centralización de sus gestiones relativas a la protección de la información clasificada, siéndole de aplicación cuanto se dispone en el punto 6 relativo a personal y procedimientos.

La solicitud de la HSEM no implica responsabilidad de la Administración por los gastos y perjuicios derivados de la no formalización de la misma.

En el caso de que el contrato, programa o proyecto se haya clasificado de grado «DIFUSIÓN LIMITADA o equivalente» no se requerirá al contratista estar en posesión de HSEM salvo que el propietario de la información lo exija.

En dicho supuesto, será responsabilidad del órgano contratante, del área de seguridad de la información clasificada en el ámbito industrial o del servicio de protección de la información clasificada del departamento ministerial que origine el contrato clasificado comprobar que se incluyen en dicho contrato las clausulas de seguridad correspondientes, así como comprobar que se cumplen, por parte del contratista, las condiciones mínimas de seguridad especificadas en el documento Orientaciones OR-ASIP-04.01 sobre el manejo de información clasificada de grado de difusión limitada o en la normativa de seguridad aplicable.

6.1.2. Requisitos para la concesión de una HSEM

Serán necesarios para la concesión de la HSEM los siguientes requisitos:

a) Cumplir con las condiciones de aptitud para contratar, exigidas en la Ley de Contratos del Sector Público y no estar incurso en ninguno de los supuestos sobre prohibición de contratar especificados en la citada Ley.
b) Cumplir las condiciones de seguridad establecidas por la ANPIC.
c) Tener constituidos y aprobados por la ANPIC tanto el servicio de protección de información clasificada como los órganos de control del grado y tipo necesarios.
d) Estar en posesión de la HPS correspondiente al grado asignado al contratista los propietarios, administradores, los miembros del consejo de administración y cualquier otra persona que pueda conocer, participar o estar presente en las deliberaciones del órgano ejecutivo del contratista. A criterio de la ANPIC, la HPS de las personas antes mencionadas podrá ser sustituida por un acta notarial de renuncia al conocimiento de información clasificada, si bien será necesario que al menos un miembro del consejo de administración, de los propietarios o de los administradores tenga concedida una HPS.
e) Haber firmado el correspondiente compromiso de seguridad.

6.1.3. Documentación necesaria para la solicitud de la HSEM

Persona jurídica

Cuando el contratista solicitante de una HSEM, se trate de una persona jurídica, deberá presentar la siguiente documentación:

a) Documento acreditativo, suscrito por un organismo de la Administración relacionado con el contrato, o por un organismo o ente público responsable de una actividad clasificada, que justifique la viabilidad/necesidad de que el contratista pueda participar en una actividad o contrato que implique acceso a información clasificada.
b) Solicitud de HPS de las personas elegidas por el contratista para el desempeño del cargo de JSSP y del suplente de dicho JSSP, y del JS del órgano de control y su suplente cuando no sean los anteriores.
c) Solicitud de HPS de los propietarios, administradores, ya sean únicos, solidarios o mancomunados, de los miembros (o sus representantes) del consejo de administración u órgano ejecutivo equivalente al de la forma jurídica del contratista (sociedad, fundación, asociación, organismo público etc.) así como de cualquier otra persona que tuviera otorgada capacidad jerárquica o ejecutiva por el citado órgano de gestión del contratista. A criterio de la ANPIC, la solicitud de HPS podrá ser sustituida por un acta notarial de renuncia al acceso a información clasificada de las personas antes mencionadas, si bien será necesario que al menos un miembro del consejo de administración, de los propietarios o de los administradores tenga concedida una HPS.
d) Copia del poder notarial, o fotocopia compulsada, que autorice a la persona designada por el contratista para firmar el compromiso de seguridad.
e) Copia simple notarial, o fotocopia compulsada, de la escritura de constitución de la sociedad, así como documentación acreditativa de las ampliaciones o variaciones sufridas posteriormente, tanto propias como de aquellas sociedades que participen en la solicitante, o sean participadas de ella.
f) Certificado de inscripción en el Registro Mercantil, caso de no estar reflejada en las escrituras especificadas en el punto anterior.
g) Última declaración completa del Impuesto de Sociedades, si se trata de persona jurídica.
h) Memoria del contratista que abarque los aspectos que expliquen su experiencia y capacidad profesional, así como las referencias que estime oportunas.
i) «Ficha del contratista», según formato de la ONS disponible en la página web www.cni.es/es/ons, rellena con datos veraces aportando la docu-

mentación que la justifica, en especial en lo que se refiere al capital y a los miembros del consejo de administración, identificando al accionista último y sus representantes en caso de que la empresa proceda de una matriz o grupo de empresas que no estén en línea directa.

j) Certificado vigente de la Agencia Estatal de Administración Tributaria correspondiente u organismo autonómico equivalente, de que se encuentra al corriente de pago de sus obligaciones tributarias.

k) Certificado emitido por la Tesorería de la Seguridad Social de que se encuentra al corriente de sus obligaciones.

l) En el caso de las empresas de seguridad privada los siguientes documentos:

- Certificado vigente de inscripción en el Registro General de Empresas de Seguridad del Ministerio del Interior, conforme al artículo 7 de la Ley 23/1992 de 30 de julio de Seguridad Privada y las modificaciones posteriores del mismo. Quedan exentas de dicho ámbito las empresas ubicadas únicamente en Ceuta, Melilla o en territorios insulares.
- Certificado del Ministerio del Interior que atestigüe las sanciones que se hayan incoado a la empresa, conforme a la sección segunda del capítulo cuarto de la Ley 23/1992 de 30 de julio de Seguridad Privada, en los diez (10) años previos a la solicitud del compromiso de seguridad.

m) Cualquier otra que le sea solicitada por la ANPIC, por ser necesaria para determinar que cumple los requisitos para la concesión de la HSEM.

Persona física

Cuando el contratista solicitante de una HSEM, se trate de una persona física, deberá presentar la siguiente documentación:

a) Documento acreditativo, suscrito por un organismo de la Administración relacionado con el contrato, o por un organismo o ente público responsable de una actividad clasificada, que justifique la viabilidad/necesidad de que el contratista pueda participar en una actividad o contrato que implique acceso a información clasificada.

b) Solicitud de HPS de las personas elegidas por el contratista para el desempeño del cargo de JSSP y del suplente de dicho JSSP, y del JS del órgano de control y su suplente cuando no sean los anteriores.

c) Solicitud de HPS o renuncia notarial de las personas que tuviera contratadas consideradas como «vinculadas», es decir, familiares hasta segundo grado incluido (abuelos, padres, cónyuges, hijos, nietos o hermanos). A criterio de la ANPIC, la solicitud de HPS podrá ser sustituida por un acta

notarial de renuncia al acceso a información clasificada de las personas antes mencionadas.

d) Copia del poder notarial, o fotocopia compulsada, que autorice a la persona designada por el contratista para firmar el compromiso de seguridad cuando no sea la propia persona física que solicita la HSEM.

e) Declaración censal (modelos 036 ó 037) presentado en la Agencia Tributaria cuando se inicia, se modifica o se da de baja una actividad económica, acreditativa de la inscripción en el censo de empresarios, profesionales y retenedores, con identificación de la actividad, los regímenes y obligaciones tributarias del IRPF e IVA, así como el domicilio.

f) Última declaración del IRPF e impuesto sobre el patrimonio, acompañada de los siguientes documentos:

- CIRBE y certificado bancario de solvencia emitido por el banco o bancos con los que tenga una mayor relación comercial.
- Modelo 190: Retenciones de IRPF efectuadas a sus trabajadores.
- Modelo 347: Declaración de operaciones con terceros. Compras o ventas superiores a 3.000€. Sólo cuando la persona física declare mediante estimación objetiva o módulos.

g) Memoria del contratista que abarque los aspectos que expliquen su experiencia y capacidad profesional, así como las referencias que estime oportunas.

h) «Ficha del contratista», según formato de la ONS disponible en la página web www.cni.es/es/ons.

i) Certificado vigente de la Agencia Estatal de Administración Tributaria correspondiente u organismo autonómico equivalente, de que se encuentra al corriente de pago de sus obligaciones tributarias.

j) Certificado emitido por la Tesorería de la Seguridad Social de que se encuentra al corriente de sus obligaciones, emitido como máximo tres (3) meses antes de la presentación de la documentación.

k) Cualquier otra que le sea solicitada por la ANPIC, por ser necesaria para determinar que cumple los requisitos para la concesión de la HSEM.

6.1.4. Criterios de valoración de fiabilidad y seguridad

Se considera que un contratista no satisface los criterios de fiabilidad cuando incurra en alguna de las siguientes circunstancias:

a) No cumpla las condiciones de seguridad requeridas en la normativa aplicable.

b) No sea solvente desde el punto de vista económico, financiero, técnico o profesional según las condiciones establecidas en la Ley de Contratos del Sector Público.
c) Se haya incurrido en falsedad al facilitar cualquier declaración o documentación exigible para la concesión de la HSEM o de la HSES.
d) El contratista o alguno de sus administradores o representantes, vigente su cargo o representación, mantenga relación de cualquier naturaleza con estados, o con personas o entidades, nacionales o extranjeras, cuyas actividades puedan suponer un riesgo para la seguridad o los intereses nacionales de España.
e) Alguno de sus administradores, o de los miembros del consejo de administración o del órgano ejecutivo del contratista, no reúnan las condiciones de elegibilidad o fiabilidad para la concesión de HPS.
f) Alguno de sus propietarios, o administradores, o miembros del consejo de administración, o del órgano ejecutivo del contratista, o la propia entidad, contravenga las limitaciones que se derivan del derecho internacional, entre otras el que estén incluidos en listados de sanciones o embargos de la ONU o de la UE.
g) Se le haya cancelado previamente una HSEM por motivos de interés y seguridad del Estado.
h) Cualquier otra circunstancia que a criterio de la ANPIC suponga una vulnerabilidad.

6.2. Habilitación de seguridad de establecimiento (HSES)

6.2.1. Requisitos para la concesión de la HSES

La concesión de una HSES implica como mínimo la solicitud, por parte del contratista, de un órgano de control con capacidad de almacenamiento, que implica la constitución de una ZAR, y de la solicitud de acreditación de al menos una estación aislada para el manejo de información clasificada en soporte informático. El contratista podrá además disponer de varias ZAR dependientes del mismo órgano de control.

Para que a un contratista se le conceda una HSES deberá reunir los siguientes requisitos:

a) Tener concedida una HSEM de grado igual o superior al de la HSES que se solicite.
b) Tener la necesidad de manejar, almacenar o generar información clasificada en sus instalaciones.

c) Disponer de tantos órganos de control con sus correspondientes ZAR como sean necesarios, adecuados al grado de clasificación solicitado, aprobados por la ANPIC.
d) Solicitar la acreditación de los sistemas de información y comunicaciones donde se vaya a manejar información clasificada, si los tuviera.

6.2.2. Documentación para la solicitud de la HSES

Por cada HSES solicitada, el contratista solicitante deberá presentar la siguiente documentación:

a) Plan de protección que incluya todos los órganos de control del establecimiento así como las ZAR de éstos. Se elaborará un plan de protección específico para cada ZAR, salvo que estas se encuentren en instalaciones adyacentes y compartan medidas de seguridad.
b) Documento COS-DRES POS (Concepto de Operación- Declaración de Requisitos específicos de Seguridad-Procedimientos Operativos) conforme a lo establecido en la NS05 y las guías STIC de aplicación para la acreditación de un sistema CIS para el manejo y almacenamiento de Información Clasificada del grado y tipo de la HSES solicitada.
c) Cualquier otra que le sea solicitada por la ANPIC, por ser necesaria para determinar que cumple los requisitos de seguridad para manejar información clasificada en sus instalaciones.

Esta documentación acompañará a la correspondiente a la solicitud de HSEM en el caso de que se hayan solicitado la HSEM y la HSES de manera simultánea.

6.3. Habilitación personal de seguridad (HPS)

6.3.1. Generalidades

El contratista solicitará HPS únicamente para aquellos empleados que necesiten acceder a información clasificada de grado «CONFIDENCIAL o equivalente», o superior para el desarrollo de una actividad o contrato clasificado. Para la solicitud de dichas HPS regirá lo dispuesto en la norma NS/02 sobre seguridad en el personal. En este sentido, se indica lo allí establecido relativo a la necesidad de que, con cada solicitud de HPS, se acompañe una «propuesta de personal».

Los certificados de HPS para personal del contratista serán emitidos con validez sólo en el ámbito de la empresa con HSEM para la que trabaja, por el área de seguridad

de la información clasificada en el ámbito industrial o, en su defecto, por la ANPIC. Este certificado tendrá el mismo formato que el definido en la norma NS/02 para el caso general, con la única salvedad de que ha de incluir una indicación expresa de la empresa para la que se emite y de las actividades, contratos o programas clasificados a los que está autorizado dicha persona, detalles que se incluirán en el apartado relativo a objeto del certificado del modelo propuesto en la norma citada.

También podrán ser tramitadas por el contratista las solicitudes correspondientes a:

a) Los asesores o consultores externos que acceden a información clasificada en la sede del contratista para realizar sus cometidos, y que no dispongan de la HPS necesaria en su empresa, u organismo, de procedencia.
b) El personal de servicios (limpieza, mantenimiento) que no dispone de HPS en su empresa de procedencia y que deba acceder a una ZAR configurada como área clase I en la sede del contratista para realizar sus cometidos.
c) Otros casos no contemplados en los puntos anteriores, a criterio de la ANPIC.

En todos los casos anteriores, la solicitud irá acompañada de un informe del contratista sobre la empresa prestataria de servicios.

La solicitud de HPS para un empleado de nacionalidad extranjera, aparte de lo establecido sobre las condiciones de elegibilidad en la norma NS/02 sobre seguridad en el personal, deberá acompañarse de un escrito donde el contratista justifique la necesidad de que dicha persona participe en la actividad, el contrato o el proyecto clasificado concreto que implique el acceso a información clasificada. Deberá además presentar una autorización escrita del organismo propietario de la información, y cumplir, en su caso, con lo establecido en las instrucciones de seguridad y cláusulas del contrato.

6.3.2. Autorización de acceso

Autorización de acceso es la autorización expresa por la que el órgano de contratación, oficina de programa, o el organismo o ente responsable de una actividad clasificada autoriza el acceso a una persona en posesión de una HPS a una información clasificada determinada.

Es requisito necesario que el personal del contratista que haya de trabajar con información clasificada esté sujeto a un criterio restrictivo de autorización de acceso. Por ello, para que una persona acceda a información clasificada, además de estar en posesión de HPS del grado adecuado, de tener necesidad de conocer,

y de haber recibido la correspondiente instrucción de seguridad, deberá disponer de una autorización de acceso.

La solicitud del contratista para el acceso a información clasificada de su personal se realizará cumplimentando el formulario «autorización de acceso», según formato de la ONS disponible en la página web www.cni.es/es/ons, que deberá ser entregado al órgano de contratación, a la oficina de programa, o al organismo o ente responsable de una actividad clasificada, tanto al inicio como cada vez que se produzca una modificación de los datos requeridos en dicho formulario. Este será devuelto al contratista o empresa, debidamente cumplimentado con la autorización o denegación de acceso.

El contratista, a través de su JSSP o DSSP, es responsable de que la información clasificada sea conocida únicamente por las personas autorizadas, y deberá impedir el acceso a aquellas zonas o dependencias donde se maneja información clasificada a toda persona a quien no se haya concedido la debida autorización de acceso, con las excepciones que se establecen en esta norma NS/06 para el personal de las empresas de servicios.

En el caso de programas o contratos internacionales, se procederá según lo establecido en las instrucciones de seguridad de los mismos.

6.4. Modificación de la HSEM y HSES

6.4.1. Elevación del grado de la HSEM

Cuando el contratista solicite la elevación de grado de su HSEM, deberá presentar una solicitud en el área de seguridad de la información clasificada en el ámbito industrial del departamento ministerial del que dependa o al organismo o ente responsable de una actividad clasificada, para su tramitación a la ANPIC. Dicha solicitud deberá acompañarse de la siguiente documentación:

a) Documento de un órgano de la Administración o ente, responsable del contrato o actividad clasificada, justificando la conveniencia de que el contratista participe en un contrato o actividad que implique acceso a información clasificada de mayor grado al de la HSEM vigente.
b) Solicitud de HPS del nuevo grado de las personas elegidas por el contratista para el desempeño del cargo de JSSP y de su suplente, y de los JS de los órganos de control y de sus suplentes en el caso de que no fueran las mismas personas.
c) Solicitud de HPS del nuevo grado de las personas que inicialmente vayan a acceder a información clasificada.

d) Solicitud de HPS conforme al nuevo grado de los administradores sociales y personal directivo. A criterio de la ANPIC, la HPS de las personas antes mencionadas podrá ser sustituida por un acta notarial de renuncia al conocimiento de información clasificada.
e) Cualquiera otra documentación que le fuera requerida con el fin de verificar que se satisfacen los criterios de solvencia y fiabilidad según lo establecido en el apartado 6.1.4.

6.4.2. Elevación del grado de la HSES

Si el contratista tiene concedida HSES de un determinado grado y necesita elevarlo, deberá presentar al área de seguridad de la información clasificada en el ámbito industrial del departamento ministerial del que dependa o al organismo o ente responsable de una actividad clasificada, para su tramitación a la ONS:

a) Solicitud de elevación de grado la HSES
b) Solicitud de elevación de grado de la HSEM según lo dispuesto en el apartado 6.4.1, en caso de que la HSES solicitada sea de grado superior al de la HSEM concedida.
c) Solicitud de acreditación de la/las ZAR, una vez adaptadas al nuevo grado.
d) Solicitud de autorización de los sistemas de información y comunicaciones, una vez adaptados al nuevo grado de clasificación, si los tuviera.
e) Plan de protección adecuado a las nuevas medidas y grado.

6.4.3. Reducción del grado de la HSEM o HSES

Cuando el contratista desee la reducción de grado de la HSEM o HSES, deberá solicitarlo al área de seguridad de la información clasificada en el ámbito industrial del departamento ministerial del que dependa o al organismo o ente responsable de una actividad clasificada, para su tramitación a la ONS.

El contratista deberá entregar toda la información clasificada de grado superior al nuevo solicitado que obrara en su poder al órgano de control de la información clasificada que se la hubiera entregado.

6.4.4. Compartimentación de la información

Cuando el contratista necesite manejar información clasificada de distintos tipos (OTAN, UE, ESA, nacional, cifra, etc) deberá tener en cuenta las servidumbres

derivadas de la «necesidad de conocer», según lo establecido en la norma NS/04 sobre seguridad de la información.

Se podrá aprobar por la ANPIC la utilización de una misma ZAR para manejar información clasificada de distintos tipos siempre que las servidumbres derivadas y las medidas de seguridad adoptadas queden plasmadas en el plan de protección correspondiente a dicha ZAR, así como las medidas adoptadas para garantizar la compartimentación de cada tipo de información almacenada.

Solo se autorizará que información clasificada de distinto tipo comparta ZAR cuando la responsabilidad de los diferentes órganos de control recaiga en la misma persona.

6.5. Vigencia

La HSEM y la HSES permanecerán en vigor hasta que sean canceladas por la ANPIC o el contratista renuncie expresamente a la misma, por lo que serán inspeccionadas de manera periódica.

Los órganos de control establecidos al amparo de la HSES que custodien información clasificada de grado CONFIDENCIAL o equivalente, o superior, habrán de ser inspeccionados periódicamente en unos plazos no superiores a sesenta (60) meses, según el apartado 5.5 de esta norma.

La HSES será cancelada en caso de que no se realice la renovación de los certificados de acreditación de las ZAR, según lo establecido en la norma NS/03 sobre seguridad física.

6.6. Suspensión de la HSEM o HSES

La HSEM y la HSES podrán quedar en suspenso temporalmente cuando se determine por la ANPIC que las condiciones de seguridad del contratista son inadecuadas para garantizar la protección de la información clasificada, o concurran circunstancias que aconsejen su revisión.

Al serle comunicada la suspensión temporal, el contratista deberá devolver la información clasificada al órgano de control de información clasificada que se la hubiera entregado.

Esta situación se mantendrá mientras permanezcan las circunstancias que la motivaron y durante un plazo máximo de un año. Transcurrido el período máximo de

suspensión sin que el contratista haya corregido las deficiencias que dieron lugar a la misma, se procederá a la cancelación.

La suspensión temporal de la HSEM supondrá la suspensión temporal automática de las HSES que tuviera el contratista y el cierre temporal de los órganos de control que tuviera establecidos.

6.7. Solicitud de suspensión de HPS de empleados del contratista.

El contratista solicitará al área de seguridad de la información clasificada en el ámbito industrial del departamento ministerial del que dependa o al organismo o ente responsable de una actividad clasificada, la suspensión de la HPS de un empleado cuando incurra en alguna de las siguientes situaciones:

a) Cause baja como personal del contratista.
b) Cambie de actividad laboral como personal del contratista y no vaya a manejar información clasificada.

El contratista deberá devolver a la Autoridad emisora el certificado de HPS correspondiente, en caso de que hubiera sido emitido.

6.8. Cancelación de la HSEM, HSES y HPS

6.8.1. Cancelación de la HSEM

La HSEM se cancelará cuando concurra alguna de las siguientes circunstancias:

a) Cuando el contratista deje de cumplir alguno de los requisitos solicitados para la concesión de la HSEM.
b) Por la renuncia escrita del contratista.
c) Por extinción de la sociedad.
d) Cuando el contratista no haya optado a ningún contrato clasificado durante un período de cinco años consecutivos.
e) Por incumplimiento de las obligaciones adquiridas por el contratista con la firma del compromiso de seguridad.
f) Cuando haya transcurrido más de un año de suspensión temporal sin que el contratista haya subsanado las deficiencias encontradas.
g) Cuando lo exija el interés o la seguridad del Estado.

Si la cancelación se produce en virtud de lo señalado en d) y e), el contratista no podrá optar a una nueva HSEM hasta pasados tres (3) años desde la fecha de cancelación de la HSEM anterior.

La cancelación de la HSEM supondrá la cancelación automática de todas las HSES que tuviera concedidas el contratista, el cierre de todos los órganos de control establecidos, y la suspensión de las HPS de sus empleados. El contratista devolverá la información clasificada que posea al órgano de control del que dependa, y devolverá a la Autoridad emisora los certificados de HPS de sus empleados y los certificados de acreditación de locales.

6.8.2. Cancelación de la HSES

La HSES podrá ser cancelada, a petición del contratista, cuando no necesite manejar información clasificada en sus instalaciones.

Será cancelada de oficio cuando:

- se haya cancelado la HSEM al contratista,
- cuando la ANPIC estime que no se cumplen las medidas de seguridad establecidas en la norma NS/03 sobre seguridad física, o
- cuando la ANPIC estime que no se cumplen las medidas de seguridad establecidas en la norma NS/04 sobre seguridad de la información.

6.9. Supuestos particulares

6.9.1. Unión temporal de empresas

Cuando una unión temporal de empresas (UTE) vaya a presentar oferta a un contrato que requiera acceso a información clasificada de grado «CONFIDENCIAL o equivalente» o superior, se precisará que alguna de las empresas participantes en la UTE tenga concedida la correspondiente HSEM.

Una vez adjudicado el contrato, todas aquellas empresas de la UTE deberán estar en posesión de la HSEM correspondiente, y aquellas que vayan a manejar información clasificada en sus instalaciones necesitarán disponer además de la HSES correspondiente.

Todo el personal de UTE o de cualquiera de las empresas constitutivas de la UTE que precise acceder a información clasificada deberá estar en posesión de la correspondiente HPS.

Todo el personal que necesite acceder a información clasificada de un contrato adjudicado a una UTE, solicitará su HPS a través de su empresa correspondiente.

El personal propio de la UTE canalizará sus solicitudes a través de alguna de las empresas integrantes de esta.

6.9.2. Grupo empresarial

Para crear una estructura de seguridad de grupo empresarial será necesario que un único apoderado represente a todas las empresas del grupo que vayan a formar parte de dicha estructura de grupo empresarial, por lo que será necesario que disponga de poderes suficientes concedidos ante notario de todas y cada una de las empresas del grupo.

Cada una de las empresas que conformen el grupo y que vaya a acceder a información clasificada deberá solicitar una HSEM, y tantas HSES como sean precisas.

El contratista que pertenezca a un grupo empresarial deberá acreditar que las condiciones requeridas para la concesión de la HSEM no se ven afectadas por su pertenencia al grupo empresarial.

Cuando las decisiones que se tomen en la empresa matriz puedan afectar a la seguridad de los contratos clasificados, el JSSP tendrá obligación de comunicarlo a la ONS. La falta de notificación a la ONS podrá ser motivo de suspensión o cancelación de la HSEM.

Se designará un director de seguridad del servicio de protección del grupo (DSSG) debidamente habilitado, para todas aquellas empresas del grupo que estén en posesión de HSEM, con el fin de unificar y coordinar la toma de decisiones del grupo que pueda afectar a la protección de la información clasificada.

6.9.3. Subcontratistas

El JSSP del contratista, antes de iniciar las negociaciones para suscribir subcontratos que impliquen el acceso a información clasificada, deberá solicitar:

a) La autorización expresa por escrito del órgano de contratación competente o del organismo o ente responsable de una actividad clasificada.
b) La certificación de que el subcontratista con el que se pretende iniciar la negociación dispone de las habilitaciones de seguridad necesarias para

acceder, almacenar o manejar la información clasificada relativa al subcontrato.

En la solicitud de autorización comunicará los datos de identificación del subcontratista, así como detalles sobre el mayor grado de clasificación de la información que vaya a ser manejada, la naturaleza y volumen de la información y una explicación de la necesidad del potencial subcontratista de recibir la información.

En el caso de que se formalice el subcontrato, el JSSP del contratista deberá remitir copia de las cláusulas de seguridad relativa a la protección de la información clasificada a la ONS según formato «comunicación de contrato clasificado» de la ONS disponible en la página web www.cni.es/es/ons.

El contratista es el responsable de solicitar la autorización de acceso del personal del subcontratista. Será igualmente responsabilidad del contratista informar al área de seguridad de la información clasificada en el ámbito industrial del departamento ministerial propietario de la información correspondiente o al organismo o ente responsable de una actividad clasificada, y a la ONS de toda incidencia que haya podido poner en riesgo la información clasificada a la que haya accedido el subcontratista.

El subcontratista se relacionará con el área de seguridad de la información clasificada en el ámbito industrial del departamento ministerial propietario de la información o con el organismo o ente responsable de una actividad clasificada para todas las gestiones relativas a la concesión de HSEM, HSES y HPS.

El contratista, una vez obtenida la autorización para subcontratar, y previo a la cesión de información clasificada al subcontratista, solicitará al órgano de control del que dependa la certificación de que el subcontratista dispone de las habilitaciones necesarias para acceder o manejar la información clasificada relativa al subcontrato.

Al término del contrato, el subcontratista devolverá al contratista toda la información clasificada que obre en su poder relativa al contrato clasificado.

6.9.4. Empresas de servicios y consultoría.

Como norma general, las empresas de servicios y de consultoría no necesitan HSEM.

El personal de estas empresas que necesite manejar información clasificada en el ejercicio de sus funciones deberá solicitar HPS del grado correspondiente a través del organismo contratante.

El personal de estas empresas que, para el ejercicio de sus funciones, deba acceder a una ZAR configurada como área de seguridad clase II, pero no necesite acceder a información clasificada, no necesitará disponer de HPS pero deberá estar escoltado permanentemente por una persona con HPS adecuada al grado y tipo de acreditación de la ZAR.

Cuando se trate de acceder a una ZAR configurada como área de seguridad clase I, el órgano de control del que dependa la ZAR deberá tramitar las solicitudes de HPS de dicho personal según lo dispuesto en la norma NS/02 sobre seguridad en el personal, teniendo en cuenta que dicho personal será siempre el mismo, su número reducido al mínimo posible, y no podrá acceder ni permanecer en la ZAR sin escolta.

Las empresas de servicios y consultoras que para llevar a cabo su labor deban manejar información clasificada de grado «CONFIDENCIAL o equivalente», o superior en sus propias instalaciones, deberán disponer de HSEM, HSES, tener establecido un órgano de control y, aquellos de sus empleados que accedan a la misma deberán estar habilitados.

6.9.5. Empresas de seguridad

Las empresas de seguridad que presten servicios de vigilancia en una ZAR de empresas o instalaciones oficiales y no necesiten manejar información clasificada en sus propias instalaciones, deberán disponer de HSEM de grado «CONFIDENCIAL o equivalente».

El personal de empresas de seguridad que preste servicio de vigilancia en una ZAR deberá tener HPS de grado igual o superior al de la ZAR a la que prestan servicio, permitiéndose en estos casos que se cursen solicitudes de HPS para el personal de las empresas de seguridad de grado superior al de su HSEM.

Las empresas de seguridad que prestan servicios como instaladoras de sistemas de seguridad en ZAR de empresas o instalaciones oficiales, deberán disponer de HSEM como mínimo en grado «RESERVADO o equivalente».

7. VISITAS NACIONALES E INTERNACIONALES

7.1. Generalidades

Se consideran visitantes aquellas personas que, sin tener relación de dependencia directa con el contratista, acceden física y circunstancialmente por te-

mas profesionales a la información clasificada en las instalaciones del mismo. Dicho acceso requerirá autorización previa y estará sujeto a las siguientes condiciones:

a) La visita estará debidamente justificada en relación con un contrato o programa clasificado.
b) La empresa visitada deberá poseer la correspondiente HSES.
c) El personal visitante deberá tener necesidad de conocer y estar en posesión de la HPS adecuada al grado de la información a la que se vaya a tener acceso.

Es responsabilidad del JSSP o JS que solicita la visita asegurarse de que la instalación visitada está en posesión de la necesaria HSES, mediante la tramitación a través de la Autoridad competente del formulario «hoja de información de habilitación de empresas, organismos y/o establecimientos» según formato de la ONS disponible en la página web www.cni.es/es/ons.

Es responsabilidad de los JSSP o JS solicitante y receptor confirmar que existe la necesidad de que se efectúe la visita.

Las visitas se inscribirán en un libro registro de visitas, donde se recogerán las fechas de la visita, el nombre completo del visitante, número de DNI o pasaporte, nacionalidad, empresa/organismo o dirección del visitante, HPS concedida y fecha de validez de la misma, y nombre de la persona visitada. Este registro estará disponible durante al menos dos años.

El visitante deberá presentar documento válido identificativo, pasaporte o documento nacional de identidad, que permita al JSSP o JS de la instalación visitada confirmar su identidad.

El acceso a una ZAR clase I, o a la información clasificada, se registrará en el libro registro, conforme a lo establecido en la norma NS/03 sobre seguridad física.

En el caso de visitas que impliquen el acceso a información clasificada de grado «DIFUSIÓN LIMITADA» o equivalente, o de forma puntual, y cuando así lo permitan la disposiciones de seguridad aplicables al caso, estas visitas podrán acordarse directamente entre los JSSP o JS de las empresas involucradas. El JSSP o JS receptor podrá confirmar que las visitas disponen de la adecuada HPS mediante la tramitación, a través de la autoridad competente, del formulario de la ONS «hoja de información de habilitación personal de seguridad» disponible en la página web www.cni.es/es/ons.

7.2. Visitas nacionales

De manera previa, y con una antelación mínima de tres (3) días laborables a la llegada a la instalación visitada, el JSSP o JS solicitante deberá remitir al JSSP o JS receptor un formulario de «comunicación de visita» según el modelo de la ONS disponible en la página web www.cni.es/es/ons, que incluya confirmación del grado de HPS de los visitantes.

7.3. Visitas internacionales

7.3.1. Tramitación

El procedimiento estándar consiste en que el JSSP o JS solicitante, con una antelación mínima de cinco (5) días laborables a la llegada a la instalación visitada, deberá remitir al JSSP o JS receptor, a través de sus respectivas autoridades nacionales, el formulario de la ONS de «solicitud de visita» disponible en la página web www.cni.es/es/ons, el cual incluye confirmación del grado de HPS de los visitantes. La antelación para cursar una visita internacional a través de las autoridades nacionales podrá ser superior a los cinco (5) días laborables dependiendo de la normativa específica que sea de aplicación a la visita, de acuerdo con tratado bilateral, el tratado multilateral o las instrucciones de seguridad del programa o contrato.

No obstante, las autoridades nacionales implicadas en un contrato o programa clasificado podrán acordar un procedimiento que permita la concertación directa de las visitas entre los JSSP o JS, mediante el formulario de la ONS «comunicación de visita» disponible en la página web www.cni.es/es/ons.

7.3.2. Tipos de visita

Las visitas internaciones se catalogan en tres tipos:

a) Visitas por una sola vez, de corta duración (normalmente inferior a treinta -30- días) y para un propósito específico, respecto a la cual no se prevé su repetición durante el año.
b) Visitas recurrentes, que se producen de forma intermitente a una misma instalación, por un mismo motivo y durante un período de tiempo especificado, sujetas a revisión y validación anuales.
c) Visitas de emergencia, que se producen a un solo efecto por motivos de urgencia, y de gran importancia, a las que no resulta aplicables el procedimiento habitual.

d) Visitas extendidas por un periodo de tiempo superior a treinta (30) días, habitualmente para asistir a cursos de formación o a ensamblajes de sistemas o equipos complejos.

7.3.3. Visita de emergencia

Ocasionalmente se dan circunstancias en las que no resulta posible respetar el tiempo previo mínimo para la tramitación de una visita. Ante esta eventualidad se puede recurrir a tramitar la visita como «visita de emergencia». Para que una visita sea calificada como de emergencia debe estar relacionada con un programa o contrato clasificado en el que la no realización de la visita tenga unas consecuencias graves para el desarrollo del programa o suponga la pérdida de una oportunidad de negocio (presentación de ofertas). Las visitas de emergencia serán aprobadas como visitas por una sola vez. Toda visita que se derive de la visita de emergencia deberá ser tramitada por el procedimiento ordinario.

Las visitas de emergencia deberán ir acompañadas de la correspondiente justificación, que será evaluada por la autoridad competente.

8. TRANSPORTES NACIONALES E INTERNACIONALES

8.1. Generalidades

Los procedimientos generales por los que se regula el transporte de la información clasificada se encuentran recogidos en la norma NS/04 sobre seguridad de la información. En el ámbito de la seguridad industrial, las normas para la realización del transporte de información clasificada se complementan con los procedimientos establecidos en la presente norma.

Los JSSP o JS remitente y destinatario de un transporte de información clasificada deberán acordar y organizar los detalles del transporte de acuerdo a los requisitos marcados en la normativa y las directrices marcadas por la autoridad competente.

De igual forma, los JSSP o JS solicitarán oportunamente a la oficina de programa, órgano de contratación, servicios generales de protección o subregistro principal del cual dependa, los certificados de correo que prevean vayan a necesitar para realizar los transportes de materias clasificadas. Asimismo se encargarán de gestionarlos, controlarlos y remitirlos a su emisor a final de año.

Será obligatorio en el ámbito industrial que el transportista lleve consigo un certificado de correo tanto en los desplazamientos en ámbito nacional como internacional.

Los certificados de correo serán autorizados por la oficina de programa, órgano de contratación, servicios generales de protección o subregistros principales, y emitidos por la ONS.

8.2. Transporte de información clasificada de grado CONFIDENCIAL o equivalente o RESERVADO o equivalente

8.2.1. Transporte personal

Previa autorización del organismo contratante u oficina de programa, o si así está establecido en las instrucciones de seguridad del programa, el transporte de información clasificada, podrá ser realizado por personal del contratista remitente o destinatario o de un organismo participante en el programa o contrato clasificado que motive el transporte, que será designado como «correo».

Este tipo de transmisión será supervisada por los respectivos JSSP remitente y destinatario y de acuerdo a las reglas generales establecidas en la norma NS/04 sobre seguridad de la información.

Adicionalmente se deberán seguir las siguientes instrucciones:

El correo debe estar en posesión de HPS adecuada al máximo grado de la información clasificada transportada.

El correo deberá llevar a lo largo del recorrido el documento «certificado de correo» de acuerdo con las instrucciones establecidas en la norma NS/04 sobre seguridad de la información así como en las Orientaciones correspondientes.

Es responsabilidad del JSSP remitente asegurarse de que el correo y escoltas autorizados (si los hubiere) tienen toda la documentación necesaria para efectuar el transporte (pasaporte, visado, seguro médico, moneda, licencias de exportación, etc.)

Antes de hacer entrega del certificado de correo el JSSP remitente debe:

a) Informar al correo sobre cualquier riesgo concerniente al transporte concreto (basándose en los países que debe cruzar si fuese el caso, debido a

las especiales características de la información que se transporta o cualquier otra amenaza identificada).

b) Instruir al correo en lo referente a la normativa de seguridad aplicable y responsabilidades que asume.

En el caso de que se haya producido algún incidente durante el recorrido se informará a los JSSP remitente y destinatario que a su vez lo pondrán inmediatamente en conocimiento de la Autoridad Nacional.

8.2.2. Transporte de información clasificada como mercancía

8.2.2.1. Generalidades

Cuando la información clasificada a transportar sea de un tamaño, peso o cualquier otra característica que aconseje su transporte como mercancía, los JSSP remitente y destinatario deberán elaborar conjuntamente un plan de transporte, que será remitido para su aprobación a la ANPIC correspondiente con una antelación mínima de:

a) Siete (7) días naturales al inicio previsto del transporte cuando se trate de un transporte nacional.

b) Diez (10) días naturales al inicio previsto del transporte cuando se trate de un transporte internacional.

La antelación para comunicar el transporte a través de las autoridades nacionales podrá ser superior a los tiempos establecidos dependiendo de la normativa específica que sea de aplicación al transporte, de acuerdo con tratado bilateral o multilateral así como a las instrucciones de seguridad del programa o contrato.

Al mismo tiempo el JSSP remitente deberá preparar dos copias de un recibo de transporte de material clasificado, según lo establecido en la norma NS/04.

8.2.2.2. Plan de Transporte

El plan de transporte podrá confeccionarse según el formato de la ONS «plan de transporte» disponible en la página web www.cni.es/es/ons, y al menos deberá contener los siguientes datos:

a) Fecha de comienzo y final del mismo, con indicación del horario previsto.

b) Grado de clasificación de la información transportada.

c) Identificación completa y exacta tanto del remitente como del destinatario de la información clasificada.
d) Identificación completa del transportista comercial, en su caso.
e) Direcciones exactas de salida y llegada, con descripción de los itinerarios previstos y alternativos, las paradas, lugares de pernocta y en su caso hora aproximada de paso por fronteras.
f) Identificación de las ZAR que se utilizarán en caso necesario para depósito de la información durante el itinerario.
g) Medio de transporte y datos identificativos del mismo. En caso de transporte por carretera, identificación completa de los conductores y matrículas de los vehículos.
h) Descripción del embalaje que contiene la información clasificada.
i) Identificación del correo o correos y del escolta o escoltas autorizados, con el grado de HPS concedida, organismo o contratista a la que pertenece, con descripción de la dotación y medio de transporte disponible.
j) Medios y procedimientos de enlace del responsable del transporte con los contratistas remitente y destinatario.
k) Tipo de transporte.

8.2.2.3. Tipos de transporte como mercancía

Transportes por una sola vez: Son aquellos que se realizan con un propósito específico, y no se prevé su repetición durante el año. Su comunicación a la ONS para su aprobación se realizará a través de un plan de transporte cuyo modelo aparece recogido en la página web www.cni.es/es/ons.

Transportes recurrentes o marco: Aquellos que se producen de forma intermitente, por un mismo motivo y durante un período de tiempo especificado, sujetos a revisión y validación anual. Incluidos en estos se encuentran los llamados «transportes marco» que son aquellos transportes recurrentes que se negocian en el marco de un programa, proyecto o contrato clasificado concreto y con un propósito determinado. Para la aprobación de la ONS se utilizará el mismo modelo de plan de transporte que el que se emplea para los transportes simples.

Cuando un plan de transporte recurrente haya sido aprobado, cada movimiento que se realice debe ser anunciado por el JSSP remitente mediante una notificación de transporte al JSSP destinatario mediante el mismo modelo que el utilizado para solicitar la aprobación del plan de transporte recurrente aunque, en este caso, se rellenarán aquellos campos relativos al envío en concreto (fechas, horas, etc.).

Esta notificación será remitida como copia a la ONS con un propósito informativo sin que se requiera aprobación previa.

Cuando un transporte esté escoltado (ya sea un transporte por carretera o cualquier otro medio) el JSSP remitente deberá instruir y formar al personal de la escolta y podrá emitirles certificado de correo de acuerdo a lo expuesto en el punto anterior referente a transporte personal para beneficiar los eventuales pasos por frontera que se tuvieran que realizar.

8.2.2.4. Medios de transporte

Transporte por carretera

El cargamento o vehículo debe estar protegido permanentemente mientras contenga información clasificada.

El traslado se procurará realizar directamente de origen a destino. No obstante, si la distancia o las instrucciones de seguridad del programa o contrato aplicables al transporte lo exigen, se podrán realizar paradas intermedias, observándose las siguientes medidas:

a) Durante las paradas en ruta de corta duración, el transporte estará constantemente protegido por al menos un correo o escolta autorizado.
b) Las paradas para pernoctar, o en las que los correos o escoltas autorizados no puedan vigilar la mercancía, deberán realizarse en una ZAR u otra zona específicamente autorizada por la ONS.

Transporte por ferrocarril, mar o aire

El transporte aéreo, marítimo o por ferrocarril de información clasificada se hará en la bodega o vagón de carga de un avión, barco o tren perteneciente a una compañía de los países participantes en el programa o contrato clasificado. En caso de que no sea posible, deberá recibirse la autorización correspondiente del Originador de la información clasificada. Un correo o escolta autorizado acompañará, en la medida de lo posible, el cargamento hasta la bodega y permanecerá hasta que ésta se encuentre cerrada y lista para despegar o zarpar. En el aeropuerto o puerto de destino también se debe supervisar la descarga del cargamento.

8.2.2.5. Servicio comercial acreditado de correo y transporte

Para el transporte de información clasificada, se podrá utilizar un servicio comercial acreditado de correo y transporte, conforme se define en la NS/04 sobre seguridad de la información.

Para constituir dicho servicio, el contratista o empresa interesada deberá:

a) Disponer de HSEM y de personal debidamente habilitado, en caso de que se vaya a transportar información clasificada de grado «CONFIDENCIAL o equivalente» y superior
b) Proteger permanentemente el cargamento o vehículo mientras contenga información clasificada. Este servicio podrá ser prestado por personal del contratista o por personal de una empresa de seguridad privada. Regirá para este personal la necesidad de HPS para el máximo grado de información a proteger durante el transporte, y deberá disponer del correspondiente certificado de correo.
c) Establecer las ZAR que le sean requeridas por la ONS, para el almacenamiento temporal de la información clasificada objeto del transporte.

Salvo que deba almacenar la información clasificada en sus instalaciones, no será necesario que disponga de HSES.

8.2.2.6. Servicio de transporte acompañado por correo

Previa autorización del organismo contratante u oficina de programa, o si así está establecido en las instrucciones de seguridad del programa, el transporte de mercancías clasificadas, podrá ser realizado por una empresa no habilitada siempre y cuando el transporte esté acompañado por personal del contratista remitente o destinatario o de un organismo participante en el programa o contrato clasificado que motive el transporte, que será designado como «correo».

El correo debe estar en posesión de HPS adecuada al máximo grado de la mercancía clasificada transportada.

El correo deberá llevar a lo largo del recorrido el documento «certificado de correo» de acuerdo con las instrucciones establecidas en la norma NS/04 sobre seguridad de la información.

El transportista se comprometerá por escrito ante el contratista remitente a:

a) Cumplir el plan de transporte.
b) Proporcionar un vehículo de transporte con las medidas de seguridad correspondientes a la carga.
c) Poner en conocimiento del contratista remitente los datos identificativos del vehículo utilizado y de sus conductores.
d) Observar durante el transporte las indicaciones del correo autorizado relativas a la protección de la información clasificada.

8.2.2.7. Servicio comercial de correo y transporte, con capacidad de seguimiento y trazabilidad de los envíos

La información clasificada de grado «CONFIDENCIAL o equivalente» e inferior podrá ser transmitida haciendo uso de transportistas comerciales que no estén en posesión de HSEM, ni que su personal posea HPS. La empresa transportista comercial deberá cumplir, no obstante, con los siguientes criterios:

a) Deberá estar domiciliada en España y tener implementada una política de seguridad para el manejo de material valioso. Esta política debe incluir un sistema de recibo, monitorización, control y contabilidad de la mercancía a lo largo del recorrido.
b) Debe aportar al remitente un recibo de recepción firmado de la mercancía.
c) La entrega debe producirse en el plazo de tiempo requerido.
d) Podrá subcontratar siempre y cuando exista el compromiso de respetar los criterios arriba establecidos. La responsabilidad en todo caso permanecerá en la empresa de transporte comercial contratista.

8.3. Transporte de información clasificada de grado DIFUSIÓN LIMITADA o equivalente

Los JSSP remitente y destinatario deberán acordar los detalles del transporte y serán responsables de la correcta remisión y recepción del mismo para lo que deberán acordar con detalle el medio de transmisión.

La información clasificada será transmitida de tal forma que esté sometida a continua contabilidad y trazabilidad. Es necesario que la transmisión y custodia de esta información clasificada sea controlada por un sistema de recibos

Se podrá hacer uso del servicio de correo certificado para ello tal y como establece la NS/04.

ANEXO I A LA NS/06. COMPROMISO DE SEGURIDAD PARA EL MANEJO DE DIFUSIÓN LIMITADA

COMPROMISO DE SEGURIDAD

D/Dª. (Nombre y apellidos), con D.N.I. (----------), en calidad de apoderado de la empresa (Nombre de la Empresa), con CIF (----------) (en adelante «el Contratista»), según poder que le ha sido conferido ante el Notario de (Localidad / Ciudad) Don/Doña (Nombre y apellidos) bajo el número (------) de su Protocolo y de fecha (dd de mes de año).

Considerando que el Contratista está interesado en participar en contratos que impliquen el acceso a información clasificada nacional así como información clasificada cuyo manejo y protección se encuentren regulados por tratados internacionales de carácter bilateral o multilateral, y teniendo en cuenta las disposiciones contenidas en la Ley 9/68 de 5 de abril, reguladora de los Secretos Oficiales, modificada por la Ley 48/78 de 7 de Octubre; el Decreto 242/1969, de 20 de Febrero, por el que se desarrollan las disposiciones de la Ley 9/1968, la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia y el Código Penal español,

SE COMPROMETE A CUMPLIR DILIGENTEMENTE LAS SIGUIENTES OBLIGACIONES Y ESTIPULACIONES:

CLÁUSULA PRIMERA – PROTECCIÓN DE LA INFORMACIÓN CLASIFICADA.

a) El Contratista se obliga a salvaguardar la información clasificada de acuerdo con las exigencias de las NORMAS DE SEGURIDAD DE LA ANS-D, y demás reglamentos de seguridad aplicables, cuyos contenidos conozco y asumo.

b) El Contratista se compromete a manejar y custodiar la información clasificada exclusivamente en las zonas especialmente habilitadas para ello y aprobadas según las citadas NORMAS DE SEGURIDAD DE LA ANS-D.

c) El Contratista se compromete a instruir en el manejo de información clasificada a toda persona que deba acceder a la misma, y a mantener un control y registro del documento acreditativo de dicha instrucción firmado por el interesado.

d) El Contratista se compromete a exigir a todo Subcontratista, antes de facilitarle información clasificada de grado «DIFUSIÓN LIMITADA o equivalente», que tenga concedida una autorización por la Autoridad Nacional para el manejo de dicha información, en consonancia con lo dispuesto en las NORMAS DE SEGURIDAD DE LA ANS-D.

CLÁUSULA SEGUNDA – REGISTRO DE EMPRESAS QUE ACCEDAN A DIFUSIÓN LIMITADA O EQUIVALENTE

a) La firma del presente Compromiso de Seguridad es condición necesaria para que el Contratista pueda acceder a información clasificada de grado «DIFUSIÓN LIMITADA o equivalente».

b) El Contratista se obliga a implantar y mantener una estructura de protección dentro de su organización, que se compondrá de lo siguiente:

a. Un Oficial de Seguridad, con las misiones y responsabilidades que figuran en la normativa en vigor.
b. Unas Zonas Administrativas de Protección para el manejo de información clasificada «DIFUSIÓN LIMITADA o equivalente», si necesita manejar y custodiar dicha información en sus propias instalaciones.
c. Unos procedimientos de trabajo que contemplará como mínimo la gestión de las instrucciones al personal que acceda a información clasificada de grado «DIFUSIÓN LIMITADA o equivalente» y el registro y control del documento acreditativo de dicha instrucción firmado por el interesado.

Dicha estructura de protección será aprobada y periódicamente revisada por la ANS-D.

CLÁUSULA TERCERA – INSPECCIONES

El Contratista se compromete a facilitar las inspecciones que la ANS-D estime necesarias para la comprobación del cumplimiento de las obligaciones y deberes que contrae con la firma del presente Compromiso. Si como consecuencia de dichas inspecciones, la ANS-D determinara que los métodos y normas de seguridad del Contratista no satisfacen lo prescrito, el Contratista será notificado por escrito de tales extremos, a los efectos, de su correspondiente subsanación en los términos que se establezcan en la notificación.

CLÁUSULA CUARTA –INCUMPLIMIENTO

a) El Contratista asume que el incumplimiento de las obligaciones que aparecen recogidas en las NORMAS DE SEGURIDAD DE LA ANS-D, una vez haya sido previamente advertido por la ANS-D, y comprobado por ésta que las subsanaciones a que se refiere la Cláusula Tercera no han sido llevadas a cabo, podrá determinar la retirada de la autorización para participar en contratos/programas clasificados de grado «DIFUSIÓN LIMITADA o equivalente».

b) El Contratista asume que el incumplimiento de la normativa detectado en alguno de sus empleados, podrá determinar la retirada de la capacidad de acceder a información clasificada de dicho empleado, sin perjuicio de otras responsabilidades que se pudieran derivar.

CLÁUSULA QUINTA – DEVOLUCIÓN DE LA INFORMACIÓN CLASIFICADA

El Contratista se compromete a devolver cualquier información clasificada facilitada o generada con ocasión del cumplimiento de los contratos clasificados o durante el desarrollo de programas clasificados, o con motivo de procesos precontractuales, en caso de retirada de la autorización para participar en contratos/programas clasificados de grado «DIFUSIÓN LIMITADA o equivalente, previo expreso requerimiento por escrito de la ANS-D.

CLÁUSULA SEXTA – COSTES

La firma de este Compromiso de Seguridad no implica responsabilidad de la Administración en los gastos del Contratista que se produzcan con motivo del mismo, o como consecuencia del cumplimiento de las obligaciones aquí señaladas.

EL CONTRATISTA SE OBLIGA A NO UTILIZAR CON FINES PUBLICITARIOS LA EXISTENCIA DEL PRESENTE COMPROMISO DE SEGURIDAD O DE LAS HABILITACIONES DE SEGURIDAD DE SU EMPRESA O DE SUS EMPLEADOS.

En fe de lo cual, se firma el presente Compromiso de Seguridad, en Madrid, a (dd) de (mes) de (año).

Por el Contratista,

Fdo. (Nombre y apellidos)

ACUSE DE RECIBO

D/Dª. (Nombre y apellidos), con D.N.I. (----------), en calidad de apoderado de la empresa (----------), con CIF (----------) (en adelante «el Contratista»), según poder que le ha sido conferido ante el Notario de (Localidad / Ciudad) Don/Doña (Nombre y apellidos) bajo el número (------) de su Protocolo y de fecha (dd de mes de año), MANIFIESTA:

Haber recibido un ejemplar de las NORMAS DE SEGURIDAD DE LA ANS-D.

Por el Contratista, RECIBÍ:

Fdo.

ANEXO II A LA NS/06. COMPROMISO DE SEGURIDAD PARA EMPRESAS CON HSEM

COMPROMISO DE SEGURIDAD

D/Dª. (Nombre y apellidos), con D.N.I. (----------), en calidad de apoderado de la empresa (Nombre de la Empresa), con CIF (----------) (en adelante «el Contratista»), según poder que le ha sido conferido ante el Notario de (Localidad / Ciudad) Don/Doña (Nombre y apellidos) bajo el número (------) de su Protocolo y de fecha (dd de mes de año).

Considerando que el Contratista está interesado en participar en contratos que impliquen el acceso a información clasificada nacional así como información clasificada cuyo manejo y protección se encuentren regulados por tratados internacionales de carácter bilateral o multilateral, y teniendo en cuenta las disposiciones contenidas en la Ley 9/68 de 5 de abril, reguladora de los Secretos Oficiales, modificada por la Ley 48/78 de 7 de Octubre; el Decreto 242/1969, de 20 de Febrero, por el que se desarrollan las disposiciones de la Ley 9/1968, la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia y el Código Penal español,

SE COMPROMETE A CUMPLIR DILIGENTEMENTE LAS SIGUIENTES OBLIGACIONES Y ESTIPULACIONES:

CLÁUSULA PRIMERA – PROTECCIÓN DE LA INFORMACIÓN CLASIFICADA

a) El Contratista al que se le conceda una HSEM se obliga a implantar y mantener una estructura de protección dentro de su organización para salvaguardar la información clasificada de acuerdo con las exigencias de las NORMAS DE SEGURIDAD DE LA ANS-D, y demás reglamentos de seguridad aplicables, cuyos contenidos conozco y asumo. Dicha estructura de protección será aprobada y periódicamente revisada por la ANS-D

b) El Contratista se compromete a manejar y custodiar la información clasificada exclusivamente en las zonas especialmente habilitadas para ello y aprobadas según las citadas NORMAS DE SEGURIDAD DE LA ANS-D.

c) El Contratista se compromete a exigir la Habilitación Personal de Seguridad apropiada a toda persona que deba acceder a la información clasificada de grado «CONFIDENCIAL o equivalente» o superior de la que fuera responsable.

d) El Contratista se compromete a instruir en el manejo de información clasificada a toda persona que deba acceder a la misma, y a mantener un control y registro del documento acreditativo de dicha instrucción firmado por el interesado.

e) El Contratista se compromete a exigir a todo Subcontratista, antes de facilitarle información clasificada de grado «CONFIDENCIAL o equivalente» o superior, que tenga concedido una habilitación de seguridad en consonancia con lo dispuesto en las NORMAS DE SEGURIDAD DE LA ANS-D.

f) El Contratista se compromete a exigir a todo Subcontratista, antes de facilitarle información clasificada de grado «DIFUSIÓN LIMITADA o equivalente», que tenga concedida una autorización por la Autoridad Nacional para el manejo de dicha información, en consonancia con lo dispuesto en las NORMAS DE SEGURIDAD DE LA ANS-D.

CLÁUSULA SEGUNDA – HABILITACIÓN DE SEGURIDAD DE EMPRESA

a) La firma del presente Compromiso de Seguridad es condición necesaria para la concesión al Contratista de una Habilitación de Seguridad de Empresa, que lo habilite para manejar información clasificada de grado «CONFIDENCIAL o equivalente» o superior.

b) El Contratista al que se le conceda una HSEM se obliga a implantar y mantener una estructura de protección dentro de su organización con la siguiente composición:

a. Un Jefe de Seguridad del Servicio de Protección y un suplente, con las misiones y responsabilidades que figuran en la normativa en vigor.
b. Unas Zonas Administrativas de Protección para el manejo de información clasificada de grado «DIFUSIÓN LIMITADA o equivalente, si necesita manejar y custodiar dicha información en sus propias instalaciones.
c. Unas Zonas de Acceso Restringido para el manejo de información clasificada de grado «CONFIDENCIAL o equivalente o superior», si necesita manejar y custodiar dicha información en sus propias instalaciones.
d. Unos procedimientos de trabajo que contemplará como mínimo la gestión de las Habilitaciones Personales de Seguridad así como la formación de los empleados.

Dicha estructura de protección será aprobada y periódicamente revisada por la ANS-D

c) El grado de seguridad otorgado al Contratista podrá quedar temporalmente en suspenso cuando concurran circunstancias que puedan afectar negativamente a la protección de la información clasificada. Dicha suspensión requerirá notificación por parte de la ANS-D.

CLÁUSULA TERCERA – INSPECCIONES

El Contratista se compromete a facilitar las inspecciones que la ANS-D estime necesarias para la comprobación del cumplimiento de las obligaciones y deberes que contrae con la firma del presente Compromiso. Si como consecuencia de dichas inspecciones, la ANS-D determinara que los métodos y normas de seguridad del Contratista no satisfacen lo prescrito, el Contratista será notificado por escrito de tales extremos, a los efectos, de su correspondiente subsanación en los términos que se establezcan en la notificación.

CLÁUSULA CUARTA –INCUMPLIMIENTO

a) El Contratista asume que el incumplimiento de las obligaciones que aparecen recogidas en las NORMAS DE SEGURIDAD DE LA ANS-D, una vez haya sido previamente advertido por la ANS-D, y comprobado por ésta que las subsanaciones a que se refiere la Cláusula Tercera no han sido llevadas a cabo, podrá determinar la retirada de la Habilitación de Seguridad de Empresa otorgada, inhabilitándole para su participación en contratos/programas clasificados.

b) El Contratista asume que el incumplimiento de la normativa detectado en alguno de sus empleados, podrá determinar la retirada de la Habilitación Personal de Seguridad de dicho empleado, sin perjuicio de otras responsabilidades que se pudieran derivar.

c) El Contratista asume que la suspensión temporal o la retirada de la HSEM implica la suspensión de las Habilitaciones Personales de Seguridad de sus empleados.

CLÁUSULA QUINTA – DEVOLUCIÓN DE LA INFORMACIÓN CLASIFICADA

El Contratista se compromete a devolver cualquier información clasificada facilitada o generada con ocasión del cumplimiento de los contratos clasificados o durante el desarrollo de programas clasificados, o con motivo de procesos precontractuales, en caso de suspensión o retirada de la Habilitación de Seguridad de Establecimiento o de suspensión o retirada de la Habilitación de Seguridad de Empresa, previo expreso requerimiento por escrito de la ANS-D.

CLÁUSULA SEXTA – COSTES

La firma de este Compromiso de Seguridad no implica responsabilidad de la Administración en los gastos del Contratista que se produzcan con motivo del mismo, o como consecuencia del cumplimiento de las obligaciones aquí señaladas.

EL CONTRATISTA SE OBLIGA A NO UTILIZAR CON FINES PUBLICITARIOS LA EXISTENCIA DEL PRESENTE COMPROMISO DE SEGURIDAD O DE LAS HABILITACIONES DE SEGURIDAD DE SU EMPRESA O DE SUS EMPLEADOS.

En fe de lo cual, se firma el presente Compromiso de Seguridad, en Madrid, a (dd) de (mes) de (año).

Por el Contratista,

Fdo. (Nombre y apellidos)

ACUSE DE RECIBO

D/Dª. (Nombre y apellidos), con D.N.I. (----------), en calidad de apoderado de la empresa (----------), con CIF (----------) (en adelante «el Contratista»), según poder que le ha sido conferido ante el Notario de (Localidad / Ciudad) Don/Doña (Nombre y apellidos) bajo el número (------) de su Protocolo y de fecha (dd de mes de año), MANIFIESTA:

Haber recibido un ejemplar de las NORMAS DE SEGURIDAD DE LA ANS-D.

Por el Contratista, RECIBÍ:

Fdo.

GLOSARIO

DEFINICIONES

1. **Acuerdo para la protección de la información clasificada** es un tratado internacional, firmado entre España y otro estado, por el que ambos se comprometen a proteger, dentro de unos estándares mínimos acordados, la información clasificada mutuamente cedida.
2. **Cesión** es la comunicación o entrega de información clasificada fuera de un determinado ámbito, departamento, organismo o entidad.
3. **Clasificación** es el acto formal por el cual se 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.
4. **Cláusulas de seguridad de la información** de contratos clasificados es el documento en el que se especifican los requisitos para la seguridad de la información clasificada manejada en el desarrollo de un contrato clasificado específico, e incluirá, necesariamente, una guía de clasificación adecuada.
5. **Contrato clasificado** es todo contrato cuya ejecución implique la generación, manejo o acceso a información clasificada por parte del contratista. Las fases de actividad precontractual así como la actividad posterior a la conclusión del contrato se consideran parte del contrato clasificado
6. **Comprometimiento de la información** es cualquier violación de la seguridad que acontece como resultado de una acción u omisión que infrinja las normas de seguridad establecidas y que puede poner en riesgo la integridad, confidencialidad o disponibilidad de dicha información. Ello incluye el acceso de personas no autorizadas a la información clasificada o a las zonas donde se maneja la misma.
7. **Compromiso de seguridad** es el documento mediante la firma del cual el contratista se obliga formalmente a proteger la información clasificada que genere, acceda o maneje en razón de la ejecución de un contrato o programa clasificado, según los requerimientos exigidos por la normativa de protec-

ción de la información clasificada en vigor, así como a recibir inspecciones periódicas y a devolver la información clasificada requerida por la Autoridad Nacional.

8. **Concepto de operación** se entenderá la declaración expresa sobre el objeto o función del sistema de información y comunicaciones, el tipo de información que va a ser manejada, las condiciones de explotación, y las amenazas a las que estará sometido.
9. **Concienciación en seguridad** es la comprensión de los deberes y obligaciones básicos que se contraerán al ser usuario de información clasificada. Es requisito previo para la concesión de la habilitación personal de seguridad.
10. **Confidencialidad** es el aseguramiento de que la información clasificada es accesible sólo para aquellos autorizados a tener acceso.
11. **Contratista** es toda entidad debidamente habilitada para estar en condiciones de licitar en contratos clasificados.
12. **Contrato clasificado** es todo contrato cuya ejecución implique la generación, manejo o acceso a información clasificada por parte del contratista. Las fases de actividad precontractual (negociación, licitación, presupuesto, propuesta, etc.) así como la actividad posterior al contrato se considerarán parte del contrato clasificado.
13. **Criptocustodio** es el responsable de la custodia, tratamiento, protección, distribución, registro, transmisión y, cuando sea necesaria, destrucción del material de cifra a cargo de la cuenta de cifra de la que sea titular.
14. **Cuenta de cifra** o **cuenta criptológica** es el órgano responsable de la custodia, manejo y contabilidad del material de cifra en el ámbito del organismo o entidad al que sirve.
15. **Declaración de requisitos específicos de seguridad (DRES)** es un documento con la exposición completa y detallada de los principios de seguridad que deben observarse y de los requisitos de seguridad que se han de implantar en un sistema de información y comunicaciones conforme al correspondiente análisis de riesgos realizado previamente.
16. **Desclasificación** es el acto formal por el cual la autoridad de clasificación retira todo grado de clasificación asignado a una información.
17. **Difusión** es la comunicación o entrega de información clasificada dentro de un determinado ámbito, departamento, organismo o entidad.
18. **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 de la misma.
19. **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 de la misma.

20. **Disponibilidad** es el aseguramiento de que los usuarios autorizados tienen acceso cuando lo requieran a la información clasificada y a sus activos asociados.
21. **Documento** es cualquier información registrada sobre un soporte, independientemente de la naturaleza del mismo o de sus características. Se incluye en este concepto, sin limitación, cualquier material escrito o impreso, tarjetas de proceso de datos, mapas, planos, fotografías, pinturas, dibujos, grabados, notas de trabajo, copias en carbón o cintas de impresora, reproducciones de todo tipo, grabaciones en sonido o vídeo, ordenadores portátiles con dispositivo residente para el almacenamiento de datos y dispositivos removibles de almacenamiento de datos.
22. **Equipo de cifra controlado (ECC)** es aquel elemento o dispositivo que, al no tener incorporados los elementos de cifra clasificados necesarios para su funcionamiento seguro, tendrá la consideración de equipo no clasificado.
23. **Grado de clasificación** es la calificación concreta de seguridad que se asigna a una determinada información clasificada, dentro de los niveles de clasificación de seguridad establecidos en la normativa de seguridad que le sea de aplicación a dicha información. A mayor grado, será mayor el perjuicio que se derivaría de su revelación no autorizada.
24. **Guía de clasificación** es el documento que enumera y describe los elementos clasificados de un asunto, contrato, programa o proyecto clasificado, con especificación de los grados de clasificación asignados a cada uno de ellos.
25. **Habilitación personal de seguridad (HPS)** es la determinación positiva por la que se reconoce formalmente la capacidad, idoneidad y fiabilidad de una persona para tener acceso a información clasificada, en el ámbito o ámbitos y grado máximo autorizado, que se indiquen expresamente, al haber superado el oportuno proceso de acreditación de seguridad y haber sido adecuadamente concienciado en el compromiso de reserva que adquiere y en las responsabilidades que se derivan de su incumplimiento.
26. **Habilitación de seguridad de empresa (HSEM)** es la determinación positiva por la que se reconoce formalmente la capacidad y fiabilidad de un contratista para generar y acceder a información clasificada hasta un determinado grado, sin que pueda manejarla en sus propias instalaciones.
27. **Habilitación de seguridad del establecimiento (HSES)** es la determinación positiva por la que se reconoce formalmente la capacidad y fiabilidad de un contratista poseedor de una HSEM para manejar información clasificada hasta un determinado grado en aquellas de sus propias instalaciones que hayan sido habilitadas a ese efecto.
28. **Información** es todo conocimiento que puede ser comunicado, presentado o almacenado en cualquier forma.

29. **Información clasificada** es cualquier información o material respecto de la cual se decida que requiere protección contra su divulgación no autorizada y a la que se ha asignado una clasificación de seguridad.
30. **Instrucción de seguridad** son 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. es requisito previo para el acceso a la información clasificada.
31. **Instrucciones de seguridad del programa** es el documento en el que se recogen y detallan la normativa y procedimientos de seguridad de la información clasificada aplicables a todos los participantes en un programa o proyecto clasificado. Estas instrucciones incluirán, necesariamente, una guía de clasificación adecuada.
32. **Integridad** es la garantía de la exactitud y completitud de la información clasificada y de los métodos de su procesamiento.
33. **Investigación de seguridad** se entenderá la fase por la que atraviesan todas las solicitudes de HPS, en la que son investigados los datos aportados por los peticionarios. Las investigaciones son el pilar en el que se apoya la concesión o denegación de la HPS.
34. **Manejo** de información se entenderá el almacenamiento, custodia, elaboración, proceso, utilización, presentación, reproducción, acceso, transporte, destrucción o transmisión de la misma, sea cual fuere el método empleado.
35. **Material** es cualquier elemento, dispositivo o sustancia del que se puede extraer información. Esto incluye documentos, equipos, piezas, armamento, sistema o componentes.
36. **Material de cifra** es cualquier dispositivo, claves, equipo o documento relacionado con el cifrado de la información.
37. **Necesidad de conocer** es la determinación positiva por la que el propietario o, en su defecto, el responsable de la custodia confirma que una persona necesita manejar determinada información clasificada para desempeñar servicios, tareas o cometidos oficiales.
38. **Normas de la Autoridad Nacional (NSs)** son el conjunto de reglas que, sobre la base de la normativa nacional de seguridad, así como de OTAN, Unión Europea y Agencia Espacial Europea, constituye el marco de referencia básica para la protección de la información clasificada en España.
39. **Oficina Nacional de Seguridad (ONS)** es el órgano de trabajo de la Autoridad Nacional, encargado de la ejecución de sus cometidos.
40. **Órgano de control** es una unidad funcional en la que se recibe, almacena y distribuye información clasificada. Un órgano de control puede ser el registro central, un subregistro principal, un punto de control o un servicio de protección. Cada órgano de control cuenta con un jefe de seguridad, máximo responsable del cumplimiento de las normas de seguridad.

41. **Originador** es el estado, organismo internacional o entidad bajo cuya autoridad se genera la información clasificada y que determina quien ostenta su propiedad.
42. **Procedimientos operativos de seguridad (POS)** es un conjunto de documentos que describen las operaciones concretas sobre cada sistema de información y comunicaciones, mediante las cuales se materializa el cumplimiento de la declaración de requisitos específicos de seguridad (DRES).
43. **Programa o proyecto clasificado** es un programa o proyecto encaminado a proporcionar bienes o servicios para cuya ejecución es necesario el acceso o manejo de información clasificada. Un programa clasificado podrá dar lugar a uno o más contratos clasificados.
44. **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.
45. **Reclasificación** es el acto formal por el cual la autoridad de clasificación modifica el grado de clasificación de una información clasificada.
46. **Seguridad criptológica** es la condición que se alcanza cuando se aplica un conjunto de medidas y procedimientos para garantizar la confidencialidad de la información clasificada mediante la utilización de métodos y materiales criptológicos durante el almacenamiento o la transmisión de la misma.
47. **Seguridad de la información** es la condición que se alcanza cuando se aplica un conjunto de medidas y procedimientos establecidos para el correcto manejo de la información clasificada en todo su ciclo de vida, así como para prevenir y detectar los posibles comprometimientos de la misma, que puedan afectar a su confidencialidad, integridad o disponibilidad.
48. **Seguridad en el personal** es la condición que se alcanza cuando se aplica un conjunto de medidas eficaces y los 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 la misma, ya sea voluntaria o involuntariamente, o de forma autorizada o no.
49. **Seguridad en los sistemas de información y comunicaciones** es la condición que se alcanza cuando se aplica un conjunto de medidas y procedimientos diseñados para garantizar la confidencialidad, integridad y disponibilidad de la información manejada mediante sistemas que incorporan tecnologías de la información y de las comunicaciones (TIC), así como la integridad y disponibilidad de los propios sistemas.
50. **Seguridad física** es la condición que se alcanza en las instalaciones cuando se aplica un conjunto de medidas de protección eficaces para la prevención de posibles accesos a información clasificada por parte de personas no autorizadas, así como para proporcionar las evidencias necesarias cuando se produzca un acceso o un intento de acceso.

51. **Sistema de información y comunicaciones** es cualquier sistema capaz de manejar información en forma electrónica. Un sistema de información y comunicaciones comprenderá todos los elementos necesarios para operar, incluyendo la infraestructura, organización, el personal y las fuentes de información.
52. **Transmisión** es la transferencia de información clasificada entre entidades por medios físicos o técnicos.
53. **Zona de acceso restringido (ZAR)** es la instalación formalmente autorizada para que se pueda manejar en la misma información clasificada en unas condiciones de seguridad establecidas.

PUBLICACIONES DE DEFENSA

GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA
SECRETARÍA GENERAL TÉCNICA
SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y PATRIMONIO CULTURAL