



**AUTORIDAD DELEGADA PARA LA SEGURIDAD DE LA
INFORMACIÓN CLASIFICADA**

Oficina Nacional de Seguridad



**ORIENTACIONES PARA LA INSTRUCCIÓN
DE SEGURIDAD DEL PERSONAL**

15.12.2009

OR-ASIP-02-02.02

**ORIENTACIONES PARA LA
INSTRUCCIÓN DE SEGURIDAD DEL
PERSONAL PARA ACCESO
A INFORMACIÓN CLASIFICADA**

ÍNDICE

1.	INTRODUCCIÓN.....	3
1.1.	GENERALIDADES.....	3
1.2.	CONDICIONES PARA EL ACCESO A INFORMACIÓN CLASIFICADA	3
2.	OBJETO.....	4
3.	ALCANCE	4
4.	CONCIENCIACIÓN E INSTRUCCIÓN.....	4
4.1.	FASES	4
4.2.	FASE DE CONCIENCIACIÓN EN SEGURIDAD	4
4.3.	FASE DE INSTRUCCIÓN DE SEGURIDAD.....	5
4.3.1.	Concepto.....	5
4.3.2.	Ámbito de aplicación y registro	5
4.3.3.	Responsabilidad de los Jefes de Seguridad en la instrucción.....	6
	ANEXO I: CONCIENCIACIÓN DE SEGURIDAD	7
	ANEXO II: INSTRUCCIÓN DE SEGURIDAD	8
	ANEXO III: INSTRUCCIÓN DE SEGURIDAD CRIPTO.....	47
	ANEXO IV: INSTRUCCIÓN DE SEGURIDAD ATOMAL.....	72

1. INTRODUCCIÓN

1.1. Generalidades

La protección de la Información Clasificada y, por tanto, su seguridad, recae en último extremo en las personas que la manejan, o que acceden a ella de forma accidental. En este sentido, la Seguridad en el Personal se puede definir como el conjunto de medidas y procedimientos establecidos para reducir a un grado mínimo aceptable el riesgo de comprometimiento de la Información Clasificada por causa debida exclusivamente al personal que accede a la misma, ya sea voluntaria o involuntariamente, o de forma autorizada o no. Asimismo, Seguridad en el Personal es el estado alcanzado cuando dichas medidas y procedimientos se aplican de manera efectiva.

La Autoridad Nacional de Seguridad (ANS) es la responsable tanto de velar por que exista la normativa de seguridad necesaria en materia de protección de la Información Clasificada, como de asegurar su correcto cumplimiento.

Las Autoridades, Mandos o responsables de la custodia y correcto manejo de la Información Clasificada velarán por que todas las personas de su respectivo Organismo, Unidad o Empresa, que, en el cumplimiento de sus cometidos oficiales, necesiten o puedan tener acceso a Información Clasificada, asuman y cumplan de forma adecuada sus obligaciones en este sentido.

En este marco, la Instrucción de Seguridad del Personal es una parte fundamental, al ser su objeto el concienciar y formar a las personas que van a acceder a Información Clasificada, sobre las responsabilidades que se asumen, las normas por las que se rige el acceso y manejo de la misma, y las consecuencias de su no cumplimiento.

1.2. Condiciones para el Acceso a Información Clasificada

Una persona sólo podrá ser autorizada a acceder a la Información Clasificada de grado “CONFIDENCIAL o equivalente”, o superior, cuando se hayan cumplido los siguientes requisitos:

- le haya sido concedida una Habilitación Personal de Seguridad (HPS) adecuada,
- se haya determinado su “necesidad de conocer”, y
- haya recibido la instrucción de seguridad preceptiva.

Aquellas personas que sólo necesiten acceder a información con clasificación “DIFUSIÓN LIMITADA o equivalente”, sólo podrán ser autorizadas a acceder a la misma, cuando se hayan cumplido los requisitos de:

- haber sido instruidas en sus responsabilidades de seguridad y
- tener la “necesidad de conocer”.

2. OBJETO

Estas Orientaciones se han desarrollado al objeto de que sirvan como base, a los Jefes de Seguridad de los Órganos de Control y a los responsables de impartir la instrucción de seguridad, en la función de instruir, sobre la protección de la Información Clasificada, a las personas que puedan tener acceso a la misma.

3. ALCANCE

El presente texto servirá de referencia fundamental y de documento de apoyo al instructor, quien, a la vista del tipo de información, grado de clasificación, u otras condiciones del acceso al que se autoriza, podrá reducir su contenido, o bien añadir otros aspectos puntuales no incluidos en el mismo que estime necesarios, recurriendo para ello a la normativa de seguridad en vigor que le sea de aplicación.

4. CONCIENCIACIÓN E INSTRUCCIÓN

4.1. Fases

La indoctrinación en materia de seguridad para los usuarios de Información Clasificada contempla dos fases, ambas necesarias y obligatorias:

- Concienciación de Seguridad.
- Instrucción de Seguridad.

4.2. Fase de Concienciación en Seguridad

Esta fase se encuadra dentro del proceso de solicitud de la HPS y es **requisito previo para la concesión** de la misma. Supone la comprensión de los deberes y obligaciones básicos que se contraerán al ser futuro usuario de Información Clasificada.

Todo solicitante de HPS deberá declarar por escrito, como requisito previo para su concesión, que entiende plenamente cuáles son sus deberes de reserva respecto a la Información Clasificada a la que accede y las consecuencias penales y disciplinarias que le serían de aplicación si incurriese en la divulgación no autorizada de la Información Clasificada a la que tenga acceso, ya sea de forma intencionada o por negligencia, si incumpliera la normativa para su manejo, o si usase dicha información para fines distintos de los oficialmente autorizados. Esta concienciación previa se declara en el Certificado de Instrucción, parte integrante de los formularios de solicitud de HPS. La Oficina Nacional de Seguridad (ONS) conserva un registro de dichas declaraciones.

En el **Anexo I** se incluye un texto de Concienciación en Seguridad, como referencia para los instructores. Al finalizar la conferencia, el interesado deberá firmar el citado Certificado de Instrucción, que corresponde a la declaración de responsabilidad que realiza el solicitante.

4.3. Fase de Instrucción de Seguridad

4.3.1. Concepto

Esta fase se encuadra como **requisito previo para el acceso** efectivo a la Información Clasificada, una vez concedida la HPS.

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

El propósito de la instrucción de seguridad es concienciar al individuo de la necesidad de la seguridad, los procedimientos para llevarla a efecto y de sus responsabilidades personales respecto a ésta, de manera que, de forma consciente, adopte las necesarias precauciones de seguridad, como una parte normal de sus cometidos. Por todo ello, la instrucción deberá impartirse a los usuarios antes del acceso efectivo a la materia clasificada.

En el **Anexo II** se incluye un texto de Instrucción de Seguridad, como referencia para los instructores. Su contenido es general y deberá ampliarse con aquellos aspectos concretos que el responsable de seguridad instructor estime necesarios.

Cuando el solicitante precise y se le autorice para solicitar la especialidad **CRIPTO**, deberá recibir una instrucción especial en dicha materia, **con carácter previo a la concesión de la HPS**, es decir, debe ser impartida a la vez o próxima a la concienciación de seguridad. En el **Anexo III** se incluye un texto de Instrucción de Seguridad Cripto, como referencia para los instructores.

Cuando el solicitante precise y se le autorice para solicitar la especialidad **ATOMAL**, deberá recibir una instrucción especial en dicha materia, **con carácter previo a la concesión de la HPS**, es decir, debe ser impartida a la vez o próxima a la concienciación de seguridad. En el **Anexo IV** se incluye un texto de Instrucción de Seguridad Atomal, como referencia para los instructores.

La instrucción en una especialidad exige el recibir previamente la instrucción de seguridad del anexo II. Esto significa que, el solicitante de una HPS que incluya una especialidad, como caso especial, debe recibir la instrucción de seguridad completa, junto con la de las especialidades solicitadas, antes de que se tramite el expediente de solicitud de HPS.

4.3.2. Ámbito de aplicación y registro

Toda persona que ocupe un puesto con acceso a Información Clasificada, será instruida en los procedimientos y obligaciones de seguridad, en materia de protección de dicha información, antes de producirse dicho acceso. Cuando se ejerzan cometidos en una Zona de Acceso Restringido, esta instrucción incluirá la parte del Plan de Protección de dicha zona que pueda afectarle. Análogamente, cuando se maneje Información Clasificada en un sistema de información y comunicaciones, la instrucción incluirá los Procedimientos Operativos de Seguridad (POS) del sistema.

Debe quedar evidencia objetiva escrita de que dicha formación ha sido impartida por persona cualificada, en la forma de certificado de instrucción, libro de registro, o similar, que custodiará el responsable del Órgano de Control del que dependa la persona instruida, o que provea el acceso. Dichos registros estarán permanentemente actualizados y disponibles para su inspección.

Todas las personas autorizadas a acceder a Información Clasificada, o que tengan que manejar dicha información, serán informadas inicialmente, y se les recordará periódicamente, sobre los peligros que entrañan para la seguridad las conversaciones indiscretas con personas que no tengan necesidad de conocer, su relación con los medios de comunicación y la amenaza que representan las actividades de los servicios de inteligencia extranjeros. Las personas serán instruidas a conciencia sobre estos peligros y sobre su obligación de notificar inmediatamente, a las autoridades de seguridad pertinentes, cualquier aproximación o maniobra que consideren sospechosa o fuera de lo corriente.

4.3.3. Responsabilidad de los Jefes de Seguridad en la instrucción

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

Los Jefes de Seguridad de los Órganos de Control son los responsables de que la formación se imparta y de guardar evidencia objetiva de que se ha llevado a efecto, así como de las instrucciones periódicas de recuerdo.

La instrucción de seguridad de los Jefes de Seguridad de los Órganos de Control principales (Subregistros Principales, Servicios Centrales y Generales de Protección de Información Clasificada), dada la importancia y responsabilidad de los cargos, siempre será realizada directamente por parte de la ONS, para asegurar el mejor desempeño de sus funciones.

Los Jefes de Seguridad de los Órganos de Control principales, instruidos por la ONS, serán a su vez responsables directos de impartir la instrucción de seguridad a sus Suplentes o Adjuntos en el cargo de Jefe de Seguridad, así como a los Jefes de Seguridad de los Órganos de Control directamente subordinados, y éstos a su vez de los subordinados, hasta llegar al último escalón.

Esta instrucción será previa a la propuesta de nombramiento de cada nuevo Jefe de Seguridad de Órgano de Control, debiendo dejar constancia mediante certificado o escrito oficial de dicha instrucción.

La ONS podrá impartir los cursos de formación a los Jefes de Seguridad de cualquier órgano de seguridad, si se estima conveniente dicha centralización, pudiendo convocar cursos de formación colectivos, con carácter de obligada asistencia.

Los órganos y personas responsables de la instrucción deberán tener previstos programas periódicos de recordatorio y reciclaje en el conocimiento de estas materias. La forma de ejecución de dichos programas se adaptará a las necesidades operativas y de tiempo de los órganos afectados.

ANEXO I: CONCIENCIACIÓN DE SEGURIDAD

DECÁLOGO DE LA PROTECCIÓN DE LA INFORMACIÓN CLASIFICADA

1. La Información Clasificada es aquella información o material sobre el que, conforme a los procedimientos legales existentes al efecto, se ha decidido que requiere un grado de protección para evitar su revelación o acceso no autorizado, en base al daño o perjuicio que su divulgación puede causar a la seguridad e intereses de España o sus aliados. Dicho grado de clasificación irá marcado sobre la propia información o material.
2. Los grados de clasificación de la Información Clasificada, de mayor a menor, son:
 - SECRETO (son equivalentes COSMIC TOP SECRET, EU TOP SECRET, etc.).
 - RESERVADO (equivalentes NATO SECRET, SECRET UE, etc.).
 - CONFIDENCIAL (equivalentes NATO CONFIDENTIAL, CONFIDENTIEL UE, etc.).
 - DIFUSIÓN LIMITADA (equivalentes NATO RESTRICTED, RESTREINT UE, etc.).
3. Toda persona que tenga conocimiento de cualquier Información Clasificada, voluntaria o involuntariamente, deberá mantener la oportuna reserva sobre la misma. Dicho deber de reserva no expira mientras la información afectada no sea desclasificada.
4. La divulgación no autorizada de Información Clasificada, el incumplimiento de la normativa para su manejo, o su uso para fines no autorizados, tendrán la consideración de delito o falta, y llevará pareja unas responsabilidades penales o disciplinarias para la persona que lo cometa, conforme al código penal o disciplinario que le afecte.
5. El acceso por un individuo a Información Clasificada con grado de CONFIDENCIAL o superior, requiere:
 - Tener concedida una Habilitación Personal de Seguridad del grado adecuado.
 - Tener la “necesidad de conocer”.
 - Haber recibido la instrucción de seguridad preceptiva, antes de dicho acceso.
6. La información CONFIDENCIAL o superior debe circular bajo el control de los Servicios de Protección de Información Clasificada u Órganos de Control, que son los responsables de su registro y custodia, y de autorizar su transmisión, copia o destrucción.
7. La información DIFUSIÓN LIMITADA sólo puede ser manejada por individuos que han sido instruidos en materia de protección de la Información Clasificada.
8. La clasificación de información es un acto formal, y no puede ser realizada por los usuarios. Sólo pueden proponerla, y elevarla para aprobación, según el procedimiento por el que se regula.
9. La Información Clasificada sólo podrá ser manejada en zonas específicamente autorizadas para dicho fin. Se prohíbe su manejo fuera de las mismas, salvo en los casos de transporte autorizado (sin acceso) o de autorización expresa por el Jefe de Seguridad responsable.
10. En todas las instalaciones y órganos en que se maneje Información Clasificada existirá la figura del Responsable de Seguridad, que podrá ser el Jefe de Seguridad de un Servicio de Protección u Órgano de Control, y que se responsabilizará del correcto manejo de la Información Clasificada en su ámbito de responsabilidad.

ANEXO II: INSTRUCCIÓN DE SEGURIDAD

Se adjunta un documento separable, y con numeración propia, al objeto de que pueda desglosarse o copiarse como manual de instrucción del personal, separado del presente documento que es para uso exclusivo de los instructores.



INSTRUCCIÓN DE SEGURIDAD



INTRODUCCIÓN

OBJETO

La presente Instrucción de Seguridad se elabora como documento de apoyo de los Jefes de Seguridad de los Órganos de Control y de los Responsables de Seguridad de las Zonas de Acceso Restringido, al objeto de que puedan impartir, a las personas bajo su responsabilidad que vayan a tener acceso a Información Clasificada, la formación necesaria relativa a la protección de la Información Clasificada. También puede constituirse como manual del usuario.

El propósito de la instrucción de seguridad es concienciar al individuo de la necesidad de la seguridad, los procedimientos para llevarla a efecto y de sus responsabilidades personales respecto a ésta, de manera que, de forma consciente, adopte las necesarias precauciones de seguridad, como una parte normal de sus cometidos. Por todo ello, la instrucción deberá impartirse a los usuarios antes del acceso efectivo a la Información Clasificada.

La instrucción en seguridad es un proceso continuo que no permite que el sujeto se estanque en sus conocimientos y que asegura que es consciente, en todo momento, de sus responsabilidades.

En cualquier caso, esta instrucción no es un documento completo. El personal que trabaje habitualmente con Información Clasificada deberá disponer de un ejemplar actualizado de las Normas de la Autoridad Nacional para la Protección de la Información Clasificada, y de las Orientaciones publicadas por la Oficina Nacional de Seguridad, como herramientas habituales de trabajo.

DEFINICIONES

Acuerdo Bilateral. Documento, con categoría de 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.

Agencia Espacial Europea (ESA). Este organismo internacional es un consorcio formado por varios países, no todos miembros de la Unión Europea, con el fin de impulsar la industria espacial en los países miembro. La ESA clasifica sus propias materias y sus Estados miembros cuentan con una ANS para la protección de su Información Clasificada. La marca **ESA** junto al grado de clasificación, representa una marca propiedad de dicha Organización y que debe ser

protegida de acuerdo con los criterios por ésta establecidos. Dentro de esta categoría se incluye la información originada por la ESA, originada por una nación miembro y entregada a la ESA, así como la información entregada a la ESA procedente de terceros Estados u Organizaciones Internacionales.

Autoridad Nacional de Seguridad (ANS) española. Cargo ejercido conjuntamente por el Ministro de Asuntos Exteriores y de Cooperación y el Ministro de Defensa. Su misión es ser el máximo representante de la protección de la Información Clasificada OTAN/UE/ESA en España.

Autoridad Delegada para la Seguridad de la Información Clasificada (ANS-D). Nomenclatura que recae en el Secretario de Estado-Director del CNI. Su misión consiste en ejercer, por delegación, las funciones que le corresponden a la ANS. Vela, asimismo, por el cumplimiento de las normas adoptadas en los Acuerdos Bilaterales suscritos por nuestro país en materia de intercambio de materias clasificadas.

C-M(2002)49. Documento de la OTAN que establece las normas de seguridad en el tratamiento de la Información Clasificada de la Alianza. Forma, junto con el C-M (2002)50, la Política de Seguridad de la OTAN.

Centro Nacional de Inteligencia (CNI). Organismo del Estado que, en base lo establecido en el artículo 4º f de la Ley 11/2006 reguladora del Centro Nacional de Inteligencia, es responsable de *“Velar por el cumplimiento de la normativa relativa a la protección de la Información Clasificada”*.

Certificado de HPS. Documento por el que se certifica que a una persona se le ha concedido una Habilitación Personal de Seguridad (HPS).

Certificado de Resolución. Documento por el que la ANS-D comunica a la Dirección General de Seguridad del Consejo, o a la Comisión Europea, su dictamen, favorable o desfavorable, sobre el proceso de investigación de un candidato a HPS de la Unión Europea. Es aplicable sólo a españoles que hayan sido contratados, directamente, por cualquiera de los organismos de la UE. Un Certificado de Resolución desfavorable es vinculante para la UE por lo que al solicitante no podrá serle concedida la HPS. Un Certificado de Resolución favorable deja en manos de la Comisión o el Consejo la concesión o no de esa HPS, si así lo estima conveniente.

Clasificación de Seguridad. Escala que permite calificar a la información en función del perjuicio para los intereses nacionales que podría causarse si la misma fuera divulgada a personal no autorizado.

Concienciación de Seguridad. Supone la comprensión de los deberes y obligaciones básicos que se contraerán al ser futuro usuario de información clasificada. Es requisito previo para la concesión de la Habilitación Personal de Seguridad.

Decisión 2001/264/CE. Documento de la UE que establece las normas de seguridad en el tratamiento de la Información Clasificada en el seno del Consejo de la UE.

Decisión 2001/884/CE, CECA, EURATOM. Documento de la UE que establece las normas de seguridad en el tratamiento de la Información Clasificada en el seno de la Comisión Europea.

Documento. 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.

Grado de Clasificación. Es la calificación concreta de seguridad que se asigna a una determinada Información Clasificada, dentro de los grados de clasificación de seguridad establecidos en la normativa de seguridad que le sea de aplicación a dicha información. A mayor grado, mayor el perjuicio que se derivaría de su revelación no autorizada.

Habilitación Personal de Seguridad (HPS). Documento expedido por la Oficina Nacional de Seguridad (ONS), por el que se acredita que en su titular no se han encontrado circunstancias que aconsejen la denegación en el acceso a materias clasificadas “CONFIDENCIAL o equivalente” y superior.

Información. Es todo aquel conocimiento que puede ser comunicado de cualquier manera.

Información Clasificada. Es aquella información o material sobre el que se ha decidido que requiere un nivel de protección para evitar su revelación o acceso no autorizado. El nivel de protección viene determinado por su clasificación de seguridad. Su clasificación de seguridad, o grado de clasificación, será mayor en tanto que el perjuicio potencial resultante de su difusión no autorizada sea también mayor.

Instrucción de Seguridad. La instrucción de seguridad se define como aquellas consignas y conocimientos que deben ser impartidos a cada individuo para mantenerle informado de las amenazas contra la seguridad, hacerle consciente de sus vulnerabilidades y concienciarle de sus responsabilidades para prevenir unas y otras. Es requisito previo para el acceso a la información clasificada.

Investigación de Seguridad. 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.

Ley de Secretos Oficiales. Ley 9/1968, modificada por la Ley 48/78, que establece el marco de protección de las materias clasificadas españolas.

Material. Incluye documentos y también cualquier otro artículo de maquinaria, sustancia, equipo o armas, fabricados o en proceso de fabricación.

Materias Clasificadas o Información Clasificada. Son los asuntos, actos, documentos, informaciones, datos y objetos cuyo conocimiento por personas no autorizadas pueda dañar o poner en riesgo la seguridad y defensa del Estado o de países aliados.

Normas de la Autoridad Nacional (NS,s). Conjunto de normativa que, sobre la base de la normativa nacional de seguridad, así como de OTAN, Unión Europea, Agencia Espacial

Europea, etc., constituye el marco de referencia básico para la protección de la Información Clasificada en España.

Oficina de Seguridad OTAN / NATO Office of Security (NOS): Organismo de OTAN, dependiente del Secretariado Internacional, responsable, entre otros aspectos de la seguridad, de la protección de la Información Clasificada OTAN.

Oficina Nacional de Seguridad (ONS). Órgano de trabajo de la ANS-D, encargado de la ejecución de sus cometidos.

Órgano de Control. Unidad integrada en la red nacional por la que se recibe, almacena y distribuye Información Clasificada OTAN, UE o ESA. Un Órgano de Control puede ser: el Registro Central, un Subregistro Principal, o un Punto de Control. Cada Órgano de Control cuenta con un Jefe de Seguridad, máximo responsable del cumplimiento de las normas de seguridad.

Organización del Tratado del Atlántico Norte (OTAN). Organismo internacional del que España es parte desde 1982. Entre otras muchas funciones en el ámbito de defensa, tiene la facultad de clasificar sus propias materias. Los países integrantes se comprometen a proteger estas informaciones conforme a la Política de Seguridad de la OTAN. La marca **NATO** junto al grado de clasificación (en inglés o en francés), representa una marca de propiedad de la Organización Atlántica, y que aquel material o documento que la lleva debe de ser protegido según los criterios establecidos por esta organización. Dentro de esta categoría se incluye la información originada por la OTAN, originada por una nación miembro y entregada a la OTAN, o entregada por una nación miembro a otra en apoyo de un programa, proyecto o contrato OTAN. También información entregada en propiedad a la Organización Atlántica procedente de fuentes no-OTAN.

Punto de Control (PC). Órgano de menor nivel de la red de Órganos de Control que componen la infraestructura de protección de la Información Clasificada. Depende de un Subregistro Principal o Secundario.

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.

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.

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.

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.

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.

Subregistro Principal (SP). Órgano de Control que se relaciona directamente con la Oficina Nacional de Seguridad y con el Registro Central en aquellas materias de su competencia. Puede ser nacional o, si está en el extranjero, exterior.

Subregistro Secundario (SS). Órgano de Control dependiente de un Subregistro Principal, que se crea como elemento intermedio, entre aquel y los Puntos de Control, normalmente por existir un número alto de estos, a efectos de un mayor control.

Unión Europea (UE). Organismo internacional del que España forma parte y al que ha cedido parte de su soberanía en determinadas materias. Tiene capacidad para clasificar sus propias materias. Los países integrantes se comprometen a proteger estas informaciones conforme a su normativa de seguridad. La marca **UE**, o **EU**, junto al grado de clasificación (en inglés y en francés, conjuntamente), representa una marca de propiedad de la Unión Europea, y que aquel material o documento que la lleva debe de ser protegido según los criterios establecidos por esta organización. Dentro de esta categoría se incluye la información originada por la UE, originada por una nación miembro y entregada a la UE, así como la información entregada a la Unión procedente de terceros Estados u Organizaciones Internacionales.

Zona de Acceso Restringido (ZAR). Local o conjunto de locales en los que, por sus específicas características de seguridad y por el hecho de que en su interior se custodia o maneja Información Clasificada, se encuentra limitado el acceso en función de parámetros de habilitación de seguridad y/o necesidad de conocer. Deberán contar con las medidas y procedimientos de seguridad adecuados y suficientes, para asegurar la protección de la Información Clasificada en todo momento.

PROTECCIÓN DE LA INFORMACIÓN CLASIFICADA EN ESPAÑA

La normativa reguladora de las materias clasificadas en nuestro país está recogida en la Ley 9/1968, modificada por la Ley 48/78, sobre Secretos Oficiales, en adelante LSO. Dicha ley, aunque vigente, nunca ha tenido un desarrollo e implantación adecuados en los diferentes Departamentos Ministeriales, excepto en el Ministerio de Defensa. En cualquier caso, el cumplimiento de cuanto en la misma se dispone, es obligatorio en toda la Administración, lo que queda patente toda vez que, en el Código Penal y en el Código Penal Militar, se contemplan responsabilidades derivadas del incumplimiento del deber de reserva sobre las materias clasificadas de las que se tenga conocimiento.

La LSO define como materias clasificadas los asuntos, actos, documentos, informaciones, datos y objetos cuyo conocimiento por personas no autorizadas pueda dañar o poner en riesgo la seguridad y defensa del Estado.

La LSO define los principios básicos para la adecuada protección de la Información Clasificada, en concreto:

- Las materias clasificadas serán calificadas en las categorías de SECRETO y RESERVADO en atención al grado de protección que se requiera.
- La clasificación corresponderá exclusivamente, en la esfera de su competencia, al Consejo de Ministros y a la Junta de Jefes de Estado Mayor. Esta facultad de clasificación no podrá ser transferida ni delegada.
- También constituirá materia clasificada aquella que así se determine por Ley.
- Las clasificaciones de SECRETO o RESERVADO, hechas con arreglo a los términos de la presente Ley y de las disposiciones que reglamentariamente se dicten para su aplicación determinarán, entre otros, los siguientes efectos:
 - Solamente podrán tener conocimiento de las materias clasificadas los órganos y las personas debidamente facultadas para ello y con las formalidades y limitaciones que en cada caso se determinen.
 - La prohibición de acceso y las limitaciones de circulación a personas no autorizadas en locales, lugares o zonas en que radiquen las materias clasificadas.
 - El personal que sirva en la Administración del Estado y en las Fuerzas Armadas estará obligado a cumplir cuantas medidas se hallen previstas para proteger las materias clasificadas.
- La persona a cuyo conocimiento o poder llegue cualquier materia clasificada, conforme a esta Ley, siempre que le conste esta condición, estará obligada a mantener el secreto y entregarla a la autoridad civil o militar más cercana y, si ello no fuese posible, a poner en conocimiento de ésta su descubrimiento o hallazgo. Esta autoridad lo comunicará sin dilación al departamento ministerial que estime interesado o a la Presidencia del Gobierno, adoptando entretanto las medidas de protección que su buen juicio le aconseje.
- Las clasificaciones, en cualquiera de sus grados, se conferirán mediante un acto formal y con los requisitos y materializaciones que reglamentariamente se determinen.
- La declaración de materias clasificadas no afectará al Congreso de los Diputados ni al Senado, que tendrán siempre acceso a cuanta información reclamen, en la forma que determinen los respectivos Reglamentos y, en su caso, en sesiones secretas. En la Resolución de la Presidencia del Congreso de los Diputados, 411/000001 de 11 de mayo de 2004, sobre secretos oficiales, publicada en el Boletín Oficial de las Cortes Generales nº 14 de 12 de mayo de 2004, se regula el acceso por el Congreso de los Diputados a materias clasificadas.
- Las materias clasificadas llevarán consigo una anotación en la que conste esta circunstancia y la calificación que les corresponda.
- Las copias o duplicados de una materia clasificada tendrán el mismo tratamiento y garantía que el original y solo se obtendrán previa autorización especial y bajo numeración.
- Las personas facultadas para tener acceso a una materia clasificada quedarán obligadas a cumplir con las medidas y prevenciones de protección que reglamentariamente se determinen, así como las particulares que para cada caso concreto puedan establecerse.

- Corresponde al Consejo de Ministros y a la Junta de Jefes de Estado Mayor conceder en sus respectivas dependencias las autorizaciones para el acceso a las materias clasificadas, así como para su desplazamiento fuera de las mismas.
- A toda persona que tenga acceso a una materia clasificada se le hará saber la índole de la misma con las prevenciones oportunas.
- El Consejo de Ministros y la Junta de Jefes de Estado Mayor atenderán al mantenimiento y mejora de los sistemas de protección y velarán por el efectivo cumplimiento de cuanto se dispone en LSO y en especial por la correcta aplicación de las clasificaciones de SECRETO o RESERVADO y porque se promuevan las acciones penales, las medidas disciplinarias y los expedientes administrativos para corregir las infracciones a esta Ley.

Aunque la Ley de Secretos Oficiales no contempla las materias clasificadas por otras naciones, la CONSTITUCIÓN ESPAÑOLA, promulgada en el año 1978, otorga validez en el ordenamiento legal interno a cuantas disposiciones se contengan en tratados y acuerdos internacionales suscritos por España, al establecer en el artículo 96.1 que “ los tratados internacionales válidamente celebrados, una vez publicados oficialmente en España, formarán parte del ordenamiento interno...”. En coherencia con dicho artículo, la legislación española sobre materias clasificadas es directamente aplicable a las materias clasificadas según tratados o acuerdos firmados por España y otras naciones.

En el ámbito del desarrollo normativo de la LSO realizado por el Ministerio de Defensa, se definen las Materias de Reserva Interna, cuya revelación no autorizada puede causar perjuicios a la seguridad e intereses de dicho departamento, y que podrán ser calificadas en las categorías de CONFIDENCIAL y DIFUSIÓN LIMITADA. Por lo que en dicho departamento, y en las condiciones que establecen, se pueden utilizar también dichas marcas de clasificación.

Asimismo, en los Acuerdos Bilaterales para la protección de la Información Clasificada firmados por España, se contempla la existencia de estas dos categorías, por lo que en base al citado artículo 96.1 de la Constitución también serían de aplicación a toda la Administración.

La estructura responsable en los distintos departamentos de la Administración y Fuerzas Armadas de la ejecución directa de lo establecido en la LSO, son los Servicios de Protección de Información Clasificada (o de Materias Clasificadas). Su existencia, composición y cometidos se definirán en la normativa de desarrollo de la LSO.

El artículo 4 f) de la ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia (CNI), asigna a este Centro la función de *“Velar por el cumplimiento de la normativa relativa a la protección de la Información Clasificada”*.

Dicho artículo, interpretado en su sentido más amplio, designa al CNI como el Organismo responsable de velar por el cumplimiento de la normativa relativa a la protección de la Información Clasificada, en todos sus ámbitos de aplicación y cualquiera que sea su origen o propiedad. En este sentido, el CNI es competente para impulsar y verificar el cumplimiento de la LSO en todos los departamentos ministeriales y Fuerzas Armadas, así como el de las políticas y normativas de protección de la Información Clasificada derivadas de los Acuerdos de Seguridad que España ha ratificado con otros Países u Organizaciones Internacionales.

A este respecto, las Normas de la Autoridad Nacional para la Protección de la Información Clasificada, promulgadas por la ANS-D, se presentan también como referencia normativa de desarrollo para aquellos departamentos de la Administración que no dispongan de una normativa propia. Estas normas definen también la existencia de los grados de clasificación CONFIDENCIAL y DIFUSIÓN LIMITADA, para uso nacional.

INFORMACIÓN CLASIFICADA DE ORGANIZACIONES INTERNACIONALES Y OTROS PAÍSES

La firma del **Tratado de Washington** el 4 de abril de 1949 y consiguiente creación de la Organización del Tratado del Atlántico Norte, implicaba el intercambio de Información Clasificada entre las Partes y el compromiso de protegerla, otorgándole el mismo grado de seguridad asignado por la Parte originadora.

Los Gobiernos de las naciones miembros necesitaban disposiciones para la protección y salvaguarda mutua de la Información Clasificada que intercambiaban y para ello firman el **Acuerdo de Seguridad de las Partes de la Organización del Tratado del Atlántico Norte**, el 2 de marzo de 1955. A partir de ese momento se desarrolla la política de seguridad de la Alianza Atlántica cuyo objetivo es establecer los principios y las normas para salvaguardar la Información Clasificada, originada por la OTAN o por una nación miembro, de los accesos y difusiones no autorizadas, modificaciones, copias y destrucción.

Las líneas fundamentales de esta política se establecieron en el Documento **C-M(55)15 (FINAL)**, que implementa el acuerdo antes mencionado, y que ha sido sometido recientemente a un proceso de revisión para adaptarse a la nueva estructura y misiones de la Alianza, y que dio como resultado el Documento C-M(2002)49. Este Documento contiene los principios básicos y las normas mínimas de seguridad que han de ser aplicadas por todas las naciones OTAN y por las organizaciones civiles y militares de la Alianza, para garantizar que se da un grado de protección común a la Información Clasificada intercambiada entre las partes, que sea equivalente al que le otorga el originador de la información.

La **adhesión de España** a la Organización del Tratado del Atlántico Norte se produce el **30 mayo de 1982**. En virtud de dicha adhesión nuestro país se comprometió al cumplimiento de las medidas contenidas en el documento inicial C-M(55)15 (Final) y actualmente en el C-M(2002)49, el cual establece que cada nación miembro debe designar una Autoridad Nacional de Seguridad, responsable de la seguridad de la Información Clasificada OTAN.

En nuestro país no existía tal autoridad. La legislación española en vigor sobre la protección de materias clasificadas, principalmente la Ley de Secretos Oficiales de 1968, sólo concebía la figura de un jefe de servicio de protección de materias clasificadas nacionales en el ámbito de cada departamento ministerial.

Las Autoridades de la OTAN no consideraron adecuado aplicar dicha ley como base para la protección de la Información Clasificada OTAN, por lo que recomendaron a las Autoridades españolas la creación de una Autoridad Nacional de Seguridad única, responsable de la seguridad de la Información Clasificada OTAN en el ámbito nacional.

Por otro lado, la incorporación de España a las Comunidades Europeas en el año 1986

no supuso, en un primer momento, la adopción de medidas específicas de protección de la Información Clasificada.

El desarrollo de una política de seguridad común elaborada por el Consejo de la UE y la Comisión se produjo de un modo más tardío y no fue hasta 2001 cuando se desarrolló una **Decisión del Consejo de la UE, la 2001/264/EC**, que establece un estándar mínimo de seguridad para la protección de la Información Clasificada para todos los Estados miembros de la Unión Europea, lo cual incluía a España como miembro de la misma.

La Decisión de la Comisión 2001/844/CE, basada en los principios establecidos en la Decisión del Consejo de la UE, garantiza la observancia de normas mínimas comunes de seguridad por parte de todos los destinatarios de Información Clasificada UE dentro de la institución y bajo su competencia, por ejemplo los servicios y contratistas, de tal modo que exista la certeza, al comunicarse la Información Clasificada de la UE, de que vaya a ser tratada con igual cautela. Estas normas mínimas incluirán criterios relativos a la habilitación del personal y los procedimientos referentes a la protección de la Información Clasificada de la UE.

En esta línea, los Estados parte de la Agencia Espacial Europea (ESA) y la propia Agencia, firman el **Acuerdo entre, los Estados Partes en el Convenio para el establecimiento de una Agencia Espacial Europea, y la Agencia Espacial Europea, para la protección y el intercambio de Información Clasificada**, hecho en París 19 de agosto del 2002. Basado en este Acuerdo, con modelo en las políticas de seguridad ya existentes de la OTAN y de la UE, se estableció la política de seguridad de la ESA, a través de sus Regulaciones de Seguridad, aprobadas por el Consejo de la ESA durante el mismo año 2002.

Por último, motivado por la necesidad de intercambio de Información Clasificada nacional con otros Países, España ha tenido que firmar Acuerdos Bilaterales de Seguridad, para la protección de la Información Clasificada, con diferentes Estados.

Un Acuerdo Bilateral para la Protección de la Información Clasificada es un tratado internacional ratificado por el Parlamento y, conforme al artículo 96.1 de la Constitución, con rango de Ley, firmado entre España y otro Estado, por medio del cual se dan garantías mutuas sobre la protección de la Información Clasificada que, sobre la base de dicho acuerdo, se intercambie entre las partes firmantes, obligándose las mismas a cumplir exactamente lo establecido en el articulado del mismo.

El Consejo de Ministros ha venido facultando al Secretario de Estado Director del CNI, mediante las correspondientes Plenipotencias, para firmar con otros Estados, en nombre del Reino de ESPAÑA, los Acuerdos Bilaterales para intercambio de Información Clasificada, y para velar por su cumplimiento. Estos Acuerdos, se constituyen en Tratados Internacionales de obligado cumplimiento y tienen efectos legales, por los que ESPAÑA se compromete a custodiar la Información Clasificada recibida conforme a los términos establecidos en dichos acuerdos.

Estos términos están en la línea de lo que, de forma general, se admite internacionalmente como estándar de seguridad, por lo que en su cumplimiento se adoptan medidas similares a las empleadas en otros ámbitos, no siendo preciso constituir estructuras específicas de protección.

CREACIÓN DE LA AUTORIDAD NACIONAL DE SEGURIDAD Y DEL REGISTRO CENTRAL

En el año 1982, en cumplimiento de establecido en la Política de Seguridad de la OTAN, mediante **Acuerdo de Consejo de Ministros de 25 de junio de 1982**, se creó en España la **Autoridad Nacional para la Seguridad de la Información Clasificada**, en adelante ANS, designando para tal cargo a los Ministros de Asuntos Exteriores y de Defensa conjuntamente, siendo facultados para delegar sus poderes en una Autoridad Delegada dentro del Ministerio de Defensa. Asimismo, en dicho acuerdo se creó un **Registro Central OTAN** para llevar a cabo la recepción, registro, archivo, distribución y remisión de la Información Clasificada OTAN.

En el año 2002, y con objeto de dar cumplimiento a los Reglamentos y Normas de Seguridad del Consejo de la Unión Europea y de la Comisión de las Comunidades Europeas, en los que se establecía la obligatoriedad de los Estados Miembros de adoptar las medidas nacionales necesarias, por **Acuerdo de Consejo de Ministros de 19 de abril de 2002** se creó la **Autoridad Nacional de Seguridad para la seguridad de la Información Clasificada para la Unión Europea y la Unión Europea Occidental**, en adelante ANS, ejercida por los Ministros de Asuntos Exteriores y de Defensa conjuntamente, siendo facultados para delegar sus poderes en una Autoridad Delegada dentro del Ministerio de Defensa. Asimismo, en dicho acuerdo se creó un **Registro Central UE** para llevar a cabo la recepción, registro, archivo, distribución y remisión de la Información Clasificada UE.

Análogamente, en el año 2005, a fin de cumplir con lo establecido en las Regulaciones de Seguridad de la Agencia Espacial Europea, por **Acuerdo de Consejo de Ministros de 18 de noviembre de 2005** se creó la **Autoridad Nacional de Seguridad para la Seguridad de la Información Clasificada de la Agencia Espacial Europea**, en adelante ANS, ejercida de nuevo conjuntamente por los Ministros de Asuntos Exteriores y de Cooperación y de Defensa, siendo facultados para delegar sus poderes en una Autoridad Delegada dentro del Ministerio de Defensa. Asimismo, en dicho acuerdo se creó un **Registro Central ESA** para llevar a cabo la recepción, registro, archivo, distribución y remisión de la Información Clasificada UE.

DESIGNACIÓN DE LA AUTORIDAD DELEGADA PARA LA SEGURIDAD DE LA INFORMACIÓN CLASIFICADA

La designación de la Autoridad Delegada para la Seguridad de la Información Clasificada, de aquí en adelante **ANS-D**, para la seguridad de la Información Clasificada OTAN, se produjo por primera vez por **Orden de la Presidencia del Gobierno de 11 de agosto de 1982** y le fueron confiadas las siguientes atribuciones:

- Asumir todas las responsabilidades y tareas encomendadas a la ANS.
- Elaborar las correspondientes normas para la protección de la Información Clasificada OTAN/UE de aplicación en el ámbito nacional.

En la misma Orden de la Presidencia del Gobierno se hizo recaer la designación de la ANS-D en la persona que ostentaba en aquel momento el cargo de Director del Centro Superior de Información de la Defensa.

Desde entonces, el nombramiento de la ANS-D siempre había recaído en la persona

que ocupaba el cargo de Director General del CESID (posteriormente Secretario de Estado Director del CNI – SEDCNI -), si bien como cargos independientes y diferentes para cada ámbito (OTAN, UE o ESA).

Sin embargo, en 2006, la Orden de Presidencia de delegación de la ANS de la ESA, hizo recaer la función de delegación en el cargo de SEDCNI, no en la persona. Análogamente ocurre en 2009 para OTAN y UE. Esta delegación de facultades, al no ser de tipo personal, tiene un carácter más permanente y estable en el tiempo.

Como consecuencia de la delegación de funciones previamente mencionada, la ANS-D depende funcionalmente de la ANS (Ministro de Defensa y Ministro de Asuntos Exteriores y de Cooperación).

LA OFICINA NACIONAL DE SEGURIDAD

Para poder llevar a cabo las misiones encomendadas, la ANS-D creó la Oficina Nacional de Seguridad (ONS), como su órgano ejecutivo de trabajo.

Dicha Oficina es responsable de la inspección y el control de la **Infraestructura de protección de la Información Clasificada** OTAN, UE y ESA en España, red encargada de la recepción, control, protección y distribución de la Información Clasificada OTAN, UE y ESA bajo la responsabilidad de nuestro país.

Asimismo, en cumplimiento de lo establecido en la **Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia (CNI)**, concretamente en el **artículo 4 f)**, donde se asigna al CNI la función de “Velar por el cumplimiento de la normativa relativa a la protección de la Información Clasificada”, la ONS es responsable en dicho Centro de su ejecución, en el ámbito de sus competencias respecto a la protección de la Información Clasificada.

La ONS es responsable de gestionar y expedir las habilitaciones personales de seguridad (HPS), nacionales u OTAN/UE/ESA. La HPS es el documento por el que la ANS-D, en nombre del Gobierno del Reino de España, reconoce formalmente la capacidad e idoneidad de una determinada persona para tener acceso a Información Clasificada del tipo o tipos que se indiquen, y para un grado de clasificación máximo igualmente indicado.

Este proceso incluye la investigación de seguridad de los solicitantes, para lo que hará uso de los procedimientos y apoyos que la legislación pone a su alcance.

NORMAS DE LA ANS-D PARA LA PROTECCIÓN DE LA INFORMACIÓN CLASIFICADA

Como ya se dijo anteriormente, cuando se designó la Autoridad Delegada para la Seguridad de la Información Clasificada, el 11 de agosto de 1982, se le confió la misión de elaborar las normas para la protección de la Información Clasificada OTAN en el ámbito nacional, tarea que ha sido llevada a cabo por la Oficina Nacional de Seguridad, y aprobado y refrendado por la ANS-D.

Las Normas de la Autoridad Nacional para la Protección de la Información Clasificada constituyen un mínimo normativo que cubre todas las obligaciones de protección de la Información Clasificada existentes en España o contraídas con otros Países u Organizaciones Internacionales y, por tanto, son de obligado cumplimiento para todas las Administraciones Públicas, Fuerzas Armadas y Organismos Públicos vinculados o dependientes de ella y entidades públicas o privadas, que manejen o tengan acceso a Información Clasificada proveniente o propiedad de:

- Organizaciones Internacionales de las que el Reino de España forma parte, en virtud de un Tratado, como son la Organización del Tratado del Atlántico Norte (OTAN), la Unión Europea (UE) y Unión Europea Occidental (UEO), la Agencia Espacial Europea (ESA), OCCAR, EUROFOR, etc., o
- España u otro país, intercambiada al amparo de un Acuerdo para la Protección de la Información Clasificada.

Asimismo, y en virtud de lo establecido en la Ley 11/2002 reguladora del Centro Nacional de Inteligencia, en su artículo 4, donde se le encomienda la función de “*Velar por el cumplimiento de la normativa relativa a la protección de la Información Clasificada*”, estas normas servirán de referencia obligada para la redacción de normativa específica para la protección de la Información Clasificada en todos los ámbitos de la Administración Central, Autonómica y Local del Estado, y serán de aplicación en todos aquellos ámbitos en los que no exista normativa departamental específica para la protección de la Información Clasificada.

REGISTRO CENTRAL DE LA INFORMACIÓN CLASIFICADA

En los mismos Acuerdos de Consejo de Ministros por los que se crea la ANS para cada una de las Organizaciones Internacionales que lo demandan, se constituye también el Registro Central, como órgano responsable de llevar a cabo la recepción, registro, archivo, distribución y remisión de la Información Clasificada tramitada en España de dichas Organizaciones Internacionales, especialmente aquella de alto grado de clasificación. Asimismo, los Acuerdos para la Protección de la Información Clasificada firmados con otros países, requieren la existencia de un Registro Central, con el fin indicado anteriormente.

LA INFORMACIÓN CLASIFICADA

GRADOS DE CLASIFICACIÓN Y EQUIVALENCIAS

El sistema de clasificación de seguridad de la información, sea nacional o sea OTAN/UE/ESA, indica la sensibilidad de la información y, en consecuencia, determina el grado de protección y la entidad de las medidas de seguridad que la información requiere.

Las clasificaciones de seguridad se aplican a la información para indicar el posible daño que causaría a la seguridad nacional, o de la OTAN, de la UE, de la ESA o de sus naciones miembros, la revelación no autorizada de la misma. En el caso de la Información Clasificada

nacional, es aplicable también al posible perjuicio que podría provocar su revelación no autorizada a los intereses de España.

En relación con la Información Clasificada española, a continuación se relacionan sus grados y las consecuencias de su revelación no autorizada:

- **SECRETO:** Se aplicará a la información que precise del más alto grado de protección, toda vez que su revelación no autorizada o utilización indebida, pudiera dar lugar a una amenaza o perjuicio extremadamente grave para la Seguridad del Estado, o pudiera comprometer los intereses fundamentales de la Nación en materia referente a la Defensa Nacional, la Paz Exterior o el Orden Constitucional.
- **RESERVADO:** Se aplicará a la información que precise de un alto grado de protección, toda vez que su revelación no autorizada o utilización indebida, pudiera dar lugar a una amenaza o perjuicio grave a los referidos intereses de España.
- **CONFIDENCIAL:** Se aplicará a la información cuya revelación no autorizada o utilización indebida, pudiera dar lugar a una amenaza o perjuicio a los intereses de España.
- **DIFUSIÓN LIMITADA:** Se aplicará a la información cuya revelación no autorizada o utilización indebida, pudiera ser contraria a los intereses de España.

Es el originador de la información quien determina la clasificación de seguridad inicial de la misma y su propiedad. El propietario es el único que puede modificar o desclasificar dicha información a lo largo de su ciclo de vida.

A continuación se relaciona tabla explicativa de los grados de clasificación más frecuentes y sus equivalencias según los organismos propietarios:

ESPAÑA	OTAN	UE	ESA
SECRETO (S)	COSMIC TOP SECRET (CTS)	EU TOP SECRET / TRES SECRET UE (TS-UE)	ESA TOP SECRET (ESA TS)
RESERVADO (R)	NATO SECRET (NS)	SECRET UE (S-UE)	ESA SECRET (ESA S)
CONFIDENCIAL (C)	NATO CONFIDENTIAL (NC)	CONFIDENTIEL UE (C-UE)	ESA CONFIDENTIAL (ESA C)
DIFUSIÓN LIMITADA (DL)	NATO RESTRICTED (NR)	RESTREINT UE (R-UE)	ESA RESTRICTED (ESA R)
-----	NATO UNCLASSIFIED	-----	-----

* Tanto CONFIDENCIAL como DIFUSIÓN LIMITADA son exclusivas del Ministerio de Defensa y Acuerdos Bilaterales, y se denominan “materias de reserva interna”. SECRETO y RESERVADO se consideran materias clasificadas en sentido estricto, y se aplican a toda España.

La información marcada como NATO UNCLASSIFIED es información que no lleva una clasificación de seguridad, sino una marca de propiedad que indica que dicha información

no puede ser difundida sin restricciones, ya que sólo debe ser utilizada para propósitos oficiales y sólo pueden acceder a ella personas u organizaciones que la requieran para propósitos relacionados con la OTAN.

El significado de las clasificaciones de seguridad es el siguiente:

- COSMIC TOP SECRET (CTS) / EU TOP SECRET (TS-UE) / ESA TOP SECRET (ESA-TS). Su revelación no autorizada ocasionaría daños excepcionalmente graves para dichas Organizaciones.
- NATO SECRET (NS) / SECRET UE(S-UE) / ESA SECRET (ESA S). Su revelación no autorizada ocasionaría daños graves para dichas Organizaciones
- NATO CONFIDENTIAL (NC)/ CONFIDENTIEL UE (C-UE) / ESA CONFIDENTIAL (ESA-C). Su revelación no autorizada dañaría a dichas Organizaciones.
- NATO RESTRICTED (NR)/ RESTREINT UE (R-UE)/ESA RESTRICTED (ESA-R). Su revelación no autorizada iría en detrimento de los intereses de dichas Organizaciones.

A efectos prácticos, en adelante se utilizará la nomenclatura española del grado de clasificación seguido de la expresión “o equivalente” (por ejemplo, “RESERVADO o equivalente”) para referirse a cuestiones que son comunes a todos los tipos de información (nacional, OTAN, UE, etc.) de grado equivalente.

Asimismo, se utilizará la expresión “equivalente a CONFIDENCIAL” o el grado que corresponda, para referirse a Información Clasificada, exceptuada la nacional.

MARCAS DE CLASIFICACIÓN

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

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

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

La documentación clasificada elaborada por Organizaciones Internacionales, o proporcionada a éstas por los Estados miembro de las mismas o por organismos a éstas vinculados, debe mantenerse, en lo posible, en los idiomas y formatos oficiales de las mismas. Las marcas de clasificación siempre se conservarán en su formato e idioma originales.

La documentación clasificada elaborada por los Estados soberanos, como originadores y propietarios de la misma, se difunde con su grado y marca de clasificación nacional. Cuando se reciba en España, se le asignará la protección equivalente, con las particularidades que en un Acuerdo para la Protección de Información Clasificada puedan haberse establecido. Normalmente, al llegar a España, se marcarán adicionalmente los documentos en su primera página con la marca del grado equivalente en España, de forma que se le aporte dicha protección. Este remarcado tiene el objeto de facilitar la labor a los destinatarios, pero en ningún caso supondrá una modificación en la propiedad de la información ni de las limitaciones de difusión previamente establecidas.

CLASIFICACIÓN

Toda información que se considere que deba ser protegida de revelación no autorizada, deberá someterse a un proceso de clasificación mediante la confección de la correspondiente **Propuesta de Clasificación**, que será presentada a la Autoridad de Clasificación, al objeto de obtener su aprobación mediante la emisión de la correspondiente **Diligencia de Clasificación**.

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

Cuando exista una Directiva de Clasificación, o Guía de Clasificación ya aprobada en una anterior Diligencia de Clasificación, que sea pertinente a la información que se propone para su clasificación, el procedimiento se simplifica, bastando con su anotación en el Registro de informaciones clasificadas y su marcado.

La Información Clasificada originada en España se constituirá como Información Clasificada nacional y, por tanto, se propondrá su clasificación conforme a los grados de clasificación establecidos en España, con independencia del destinatario. De este modo se indica de forma explícita que España es la propietaria y originadora de esa Información Clasificada.

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

Los mensajes o escritos de remisión, que acompañan a documentos anexos clasificados

con marcas de clasificación no nacionales y tienen entidad propia, pueden ir en idioma diferente, no debiendo contener Información Clasificada. Aunque lleven la clasificación que les corresponda por agregación, dicha marca incluirá una indicación de que el citado escrito no constituye Información Clasificada cuando se separen de los anexos.

CONDICIONES PARA EL ACCESO A INFORMACIÓN CLASIFICADA

En general, para tener acceso a Información Clasificada es necesario que se den los siguientes requisitos:

- Tener **“necesidad de conocer”** la información contenida en esos documentos, por razón de su puesto de trabajo. Esto significa que nadie en virtud de cargo, categoría en la Administración o en la empresa, o de ser titular de una **Habilitación Personal de Seguridad**, o de cualquier otra circunstancia análoga, tiene derecho a acceder a Información Clasificada. Es el jefe o responsable del organismo o empresa, asesorado por el Jefe de Seguridad, quien determina que la persona tiene necesidad de conocer.
- Ser instruido en los procedimientos de seguridad para la protección y el manejo de la Información Clasificada.
- Para el acceso a Información Clasificada de grado **“CONFIDENCIAL o equivalente”**, o superior, es imprescindible además **ser titular de una Habilitación Personal de Seguridad (HPS)**.

El acceso a información **DIFUSIÓN LIMITADA** y, por tanto su difusión, con carácter general deberá atenerse a las siguientes condiciones:

- Su contenido no debe ser revelado al público, o a personal no autorizado.
- Solamente estará a disposición del personal que requiera acceso a dicha información, quien deberá tener la oportuna **“necesidad de conocer”**.
- Las personas que dispongan de acceso a la misma deberán haber sido instruidas previamente en el manejo de dicho tipo de información, y serán conscientes de sus responsabilidades en la protección de la misma.

ESTRUCTURA PENAL QUE AMPARA LA PROTECCIÓN DEL SECRETO

Las conductas más graves contra la seguridad de las materias clasificadas de acuerdo con la Ley de Secretos Oficiales, encuentran su tipificación penal en el Código Penal (Ley Orgánica, 10/1995) y, para el caso de que dichas conductas se lleven a cabo por militares o por españoles en tiempo de guerra, en el Código Penal Militar (Ley Orgánica, 13/1987).

CÓDIGO PENAL

El Código Penal contempla y penaliza diversas conductas relativas a la obtención, revelación, falseamiento e inutilización de materias clasificadas.

El artículo 584 castiga como traidor, con la pena de prisión de seis a doce años, al español que con el propósito de favorecer a una potencia extranjera, se procure, falsee, inutilice

o revele Información Clasificada como secreta o reservada.

A su vez los artículos 598 a 603, contemplan similares conductas, llevadas a cabo sin propósito de favorecer a potencia extranjera, castigándolas con penas que van desde los seis meses a los cinco años de prisión.

CÓDIGO PENAL MILITAR

Similares conductas, pero con penas en general más graves, son contempladas en el Código Penal Militar, para el caso de que los autores de las mismas sean militares o personal civil en tiempo de guerra.

LA INFRAESTRUCTURA ESPAÑOLA DE PROTECCIÓN DE LA INFORMACIÓN CLASIFICADA

El Sistema de Registro en ESPAÑA está constituido por el Registro Central y todos los Órganos de Control autorizados por la ANS-D o creados en el ámbito de la Ley de Secretos Oficiales, hasta nivel Punto de Control, o Servicio Local de Protección, incluido, por los que se distribuye la Información Clasificada. Está estructurado jerárquicamente conforme al siguiente esquema de responsabilidad:

- Registro Central ESPAÑA.
- Subregistros Principales, o Servicios Centrales de Protección de Información Clasificada.
- Subregistros Secundarios, o Servicios Generales de Protección de Información Clasificada.
- Puntos de Control, o Servicios Locales de Protección de Información Clasificada.

Esta infraestructura de control es responsable de la recepción, contabilidad, custodia, distribución y destrucción de la Información Clasificada que se maneja en los Organismos y Entidades a los que sirve.

La red principal la forman el Registro Central y los Subregistros Principales/Servicios Centrales. De esta red principal dependen una serie de redes secundarias, agrupadas cada una de ellas bajo el control de un Subregistro Principal/Servicio Central, del que dependen los Subregistros Secundarios/Servicios Principales y los Puntos de Control/Servicios Locales, que sea necesario establecer. Los Puntos de Control pueden depender de un Subregistro Principal directamente o de un Subregistro Secundario.

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

En adelante, aunque no se mencionen los Servicios de Protección de Información Clasificada, su estructura y cometidos, serán similares a los que se mencionan para los Órganos de Control, estando regulados por la normativa específica aplicable en cada departamento ministerial. **En ausencia de normativa se seguiría la establecida por la ANS-D.**

REGISTRO CENTRAL

El Registro Central actúa como la cabeza de la red de protección de la Información Clasificada OTAN/UE/ESA en España, recepcionando las materias clasificadas procedentes de esas organizaciones que entran en nuestro país y distribuyéndolas a los Subregistros Principales, así como enviando documentos fuera de la red Española.

Es responsable, a la vez, de recepcionar y custodiar las materias clasificadas que procedan de países con los que España tenga suscrito un Acuerdo Bilateral en materia de seguridad, cuando no se haga a través de los Servicios de Protección de Información Clasificada nacionales.

El Registro Central tiene establecido un sistema de registro y control que le permite conocer en todo momento donde se encuentran las materias clasificadas de grado “equivalente a RESERVADO”, o superior, que se haya distribuido a la red española, por los cauces y procedimientos autorizados.

Entre sus principales cometidos está el de planificar y llevar a cabo la transmisión de los documentos clasificados a España a través del sistema de valija personal conducida, con carácter periódico, establecido entre Bruselas y Madrid.

ÓRGANOS DE CONTROL

En todo Organismo o Entidad, el Jefe del mismo es el responsable de la adecuada protección de la Información Clasificada, tanto en su custodia como en su manejo. Para asegurar el cumplimiento de sus cometidos en este aspecto, deberá disponer de los medios y recursos adecuados, es decir, de un órgano responsable de la ejecución de dicha protección. Este órgano recibe el nombre de Órgano de Control.

Un Órgano de Control es, por tanto, un elemento constituido por decisión del Jefe de un determinado Organismo o Entidad, para poder garantizar una adecuada protección de la Información Clasificada que tiene a su cargo y de la que es responsable, en cumplimiento de la normativa de protección de la Autoridad Nacional, y de la normativa o regulaciones de seguridad de su ámbito (Organizaciones Internacionales a las que España pertenece, Acuerdos para la Protección de la Información Clasificada, Ley de Secretos Oficiales, etc.).

La función del Órgano de Control OTAN/UE/ESA/etc., es compatible con la de Servicio de Protección de la Información Clasificada, por lo que, siempre que se cumplan los requisitos establecidos en las correspondientes normativas de seguridad aplicables, ambas funciones podrán estar centralizadas en un mismo órgano.

Unos y otros se constituyen como Registros, responsables del control de la Información Clasificada, por los que se distribuye y circula la misma, conforme a su ámbito de procedencia.

Su funcionamiento está basado en:

- Un personal con **dedicación preferente** a esta tarea, específicamente formado para sus cometidos de seguridad y con autoridad suficiente, emanada de la Dirección, para

cumplir con sus cometidos, destacando la figura clave del Jefe de Seguridad del Órgano de Control.

- Unos medios e instalaciones de seguridad específicamente adaptados y aprobados para la custodia, control y manejo de la Información Clasificada, constituidos como **Zona de Acceso Restringido (ZAR)**.
- Una exacta ejecución de la normativa de seguridad por la que se rigen, especialmente la relativa a la protección, registro, custodia, manejo y distribución de la Información Clasificada.
- El cumplimiento de unos procedimientos operativos expresados en un **Plan de Protección** específico del órgano.

SUBREGISTROS PRINCIPALES, SECUNDARIOS Y PUNTOS DE CONTROL

Los **Subregistros Principales** son de dos tipos: Nacionales o Exteriores.

Los Subregistros Principales Exteriores están localizados fuera de España. Son responsables de la protección, difusión y control de la Información Clasificada en las Delegaciones y Representaciones españolas ante la OTAN, Representación Permanente ante la UE, Embajadas u otros organismos donde están establecidos.

Por su ubicación en mandos o instalaciones de esas organizaciones internacionales reciben directamente documentos de las mismas que remiten a la red española, a través del Registro Central.

Los Subregistros Principales Nacionales están ubicados dentro de España. Difunden los documentos clasificados a sus Órganos de Control subordinados: los Subregistros Secundarios y los Puntos de Control.

Los Subregistros Secundarios dependen directamente de un Subregistro Principal, y a su vez tienen bajo su responsabilidad a sus órganos subordinados, los Puntos de Control.

Los Puntos de Control son las unidades elementales, ocupan el último escalón en la red de protección de la Información Clasificada, ya que no tienen otros Órganos de Control subordinados a los que difundan la información. Son los Órganos de Control que están más próximos al usuario de los documentos, al que se los difunden directamente. Usualmente reciben y envían documentos a través del Subregistro Principal o Secundario del que dependen.

Todos los Órganos de Control: Subregistros Principales, Secundarios y Puntos de Control, son responsables de la protección, control y difusión de la Información Clasificada OTAN, UE y ESA, según tengan autorizado, en aquellos Departamentos de la Administración o de las Fuerzas Armadas o en las empresas donde están ubicados.

Todos aquellos locales que alberguen en sus instalaciones Cuenta de Cifra, se considerarán a todos los efectos como Órganos de Control, debiendo de cumplir, por lo tanto, con todos los requisitos de seguridad, apertura, modificación, cierre, control y procedimientos señalados para éstos.

Los locales en que se maneje Información Clasificada de grado “CONFIDENCIAL o equivalente”, o superior, o que alberguen en sus instalaciones Sistemas de Información y Comunicaciones (CIS) que manejen Información Clasificada de dicho grado, no tendrán la consideración de Órganos de Control, pero deberán cumplir unos requisitos específicos, tanto de seguridad como de apertura, modificación, cierre y control. En todos los casos dependerán, a efectos de protección de la Información Clasificada, de un Órgano de Control responsable.

CIRCULACIÓN DE DOCUMENTOS DENTRO DE LA RED

La información de grado “equivalente a CONFIDENCIAL”, o superior, deberá entrar en la red española a través del Registro Central OTAN/UE/ESA de España u otros medios de transmisión, físicos o electrónicos, específicamente autorizados. Los documentos que se envían a esta red proceden de los Subregistros Principales Exteriores, de las Agencias y los Mandos de la OTAN, del Consejo de la UE o de la Comisión, de los órganos de dirección de la ESA o de otros Registros Centrales establecidos en las naciones miembros.

La distribución de Información Clasificada de grado “equivalente a CONFIDENCIAL”, o superior, siempre y sin excepción se efectuará entre los Órganos de Control, y nunca directamente entre los usuarios finales de los mismos.

La información clasificada de grado “equivalente a SECRETO” no podrá circular entre Subregistros Principales directamente, sino siempre a través del Registro Central, y sólo será remitida a aquellos Órganos de Control que estén especialmente autorizados para ello.

La Información Clasificada de grado “equivalente a RESERVADO”, o inferior, podrá circular entre Subregistros Principales directamente, informando de ello al Registro Central. También podrá circular entre Subregistros Secundarios y Puntos de Control dependientes de un mismo Subregistro Principal, informando a su Órgano de Control de nivel superior de los movimientos producidos.

La información de grado “equivalente a CONFIDENCIAL”, excepto en el ámbito empresarial, podrá circular entre Puntos de Control directamente, informando de ello a su Órgano de Control de nivel superior.

La información de grado “equivalente a DIFUSIÓN LIMITADA”, excepto en el ámbito empresarial, podrá circular entre usuarios, siempre que el que hace la entrega tenga absoluta seguridad de que el receptor está autorizado a su recepción y cumple los criterios para el acceso a dicha información.

JEFE DE SEGURIDAD DE SUBREGISTROS Y PUNTOS DE CONTROL

El Jefe de Seguridad del Órgano de Control es la persona que, por delegación del Jefe del Organismo o Empresa donde está establecido dicho órgano, es responsable de la adecuada implementación de las medidas de seguridad necesarias para lograr la protección de la Información Clasificada, de acuerdo con las normas e instrucciones emanadas de la Autoridad Delegada para la Seguridad de la Información Clasificada.

Su nombramiento se realizará por la ANS-D en el caso de los Subregistros Principales, a propuesta del Jefe del Organismo o empresa, y por la ONS en el caso de los demás Órganos de Control, a propuesta del Jefe de Seguridad del Subregistro Principal del que dependa el Órgano de Control.

LA HABILITACIÓN PERSONAL DE SEGURIDAD

DEFINICIÓN

La Habilitación Personal de Seguridad (HPS) es un documento por el que la ANS-D, en nombre del Gobierno español, reconoce formalmente la capacidad e idoneidad de una persona para tener acceso a Información Clasificada del tipo concedido hasta un determinado grado de clasificación.

La HPS certifica:

- Que a su titular, por las condiciones que reúne, se le puede confiar, dentro de un riesgo asumible, el acceso a informaciones clasificadas.
- Que la persona habilitada ha sido debidamente concienciada en materia de seguridad y conoce sus responsabilidades penales y disciplinarias, contempladas en el Código Penal (si es funcionario público o particular) y en el Código de Justicia Militar (si es miembro de las Fuerzas Armadas).

NECESIDAD DE LA HABILITACIÓN

Todas las personas, con independencia de su cargo y jerarquía, que precisen acceder a Información Clasificada de grado “CONFIDENCIAL o equivalente”, o superior, deberán estar en posesión de una HPS del grado requerido.

No sólo las personas que vayan a consultar la documentación clasificada, sino también los encargados de su custodia y traslado y, en general, cualquiera que, en su trabajo ordinario, pudiera contar con la posibilidad física de acceder a la misma.

El personal que realice tareas de limpieza y mantenimiento de locales o equipos que se encuentren en Zonas de Acceso Restringido clasificadas como Área Clase II no necesitará estar en posesión de Habilitación Personal de Seguridad. Los responsables de la seguridad de dichas zonas tomarán todas las medidas necesarias para garantizar la supervisión permanente de dicho personal y la seguridad de la Información Clasificada. Es conveniente la firma de un Compromiso de Seguridad, por el que se comprometan a mantener la reserva sobre cualquier información a la que, de forma accidental o no, puedan haber accedido.

El personal que realice tareas de limpieza y mantenimiento de locales o equipos que se encuentren en Zonas de Acceso Restringido clasificadas como Área Clase I necesitará estar en posesión de Habilitación Personal de Seguridad de grado adecuado con la Información Clasificada que se maneje en dichas zonas. Ello no exime a los responsables de la seguridad de

dichas zonas de tomar las medidas necesarias para garantizar la supervisión permanente de dicho personal y para mantener una seguridad adecuada de la Información Clasificada.

También se necesita habilitación para:

- 1) **La asistencia a determinadas actividades y foros** relacionados con OTAN, UE o ESA, o con Programas industriales clasificados, que se celebren en sus organismos oficiales o en los de las naciones miembros, puede requerir una Habilitación de Seguridad, con independencia de que los asuntos a tratar sean, o no, materia clasificada.

La Oficina Nacional de Seguridad es quien garantiza que los representantes españoles que asisten a estas actividades están en posesión de la habilitación correspondiente, y al objeto de que los servicios de seguridad faciliten el pase al lugar donde se celebre la reunión, la ONS remite una “Certificación para Asistencia” comunicando la identidad de los desplazados, su grado de Habilitación Personal de Seguridad, las fechas de comienzo y final de la actividad y el organismo concreto donde se desarrolle. Para ello es necesario que el personal que va a asistir a una determinada actividad clasificada lo comunique, con suficiente antelación, al Jefe de Seguridad de su Órgano de Control para que éste a su vez lo comunique a la ONS para su tramitación.

- 2) **Las visitas internacionales** en el ámbito industrial a determinadas instalaciones, donde se desarrollan programas o proyectos clasificados que se encuentran ubicadas en organismos oficiales de una organización o de otra nación miembro, o que pertenezcan a un contratista de otra nación miembro.

El procedimiento para autorizar la visita se basa en la utilización de un formulario denominado “Request for Visit” (RFV), el cual debe enviarse, a través de la ONS, a la Autoridad Nacional de Seguridad del país que va a ser visitado. El cuestionario incluye, entre otros, los siguientes datos:

- Identidad de los visitantes y su grado de Habilitación Personal de Seguridad.
- Agencia gubernamental o instalación industrial que va a ser visitada.
- Tipo de visita.
- Grado de clasificación de los temas que van a ser tratados.

Es la Autoridad Nacional de Seguridad, o una designada, del país que solicita la visita quien refrenda estos datos, salvo que por acuerdo se establezca otro procedimiento.

De la necesidad de HPS para acceder a Información Clasificada de grado “CONFIDENCIAL o equivalente”, o superior, sólo están exentos el Ministro de Defensa y el Ministro de Asuntos Exteriores y de Cooperación, en cuanto son Autoridad Nacional de Seguridad, y el Secretario de Estado Director del CNI, en tanto que Autoridad de Seguridad Delegada.

GRADOS DE HABILITACIÓN

En función del grado de clasificación de la información que un usuario necesite conocer, necesita disponer previamente de una Habilitación de grado al menos igual al del grado de dicha información.

Los grados de las Habilitaciones se corresponden con los tres primeros grados de clasificación de seguridad:

- SECRETO o equivalente,
- RESERVADO o equivalente,
- CONFIDENCIAL o equivalente.

ESPECIALIDADES

Asimismo, existen tres autorizaciones especiales que complementan a las Habilitaciones:

- El acceso a informaciones sobre planes, despliegues y características de las armas nucleares que ESTADOS UNIDOS y el REINO UNIDO ponen a disposición de la OTAN, precisa una autorización que se denomina **“ATOMAL/ATOMIC”** (por ejemplo: NATO SECRET ATOMAL). No existe la especialidad ATOMAL en el ámbito de las Habilitaciones UE ni de la ESA.
- El conocimiento y manejo de las claves de cifra y equipos de cifra de las comunicaciones necesita también una autorización especial denominada **“CRYPTO”** (por ejemplo: NATO SECRET-CRYPTO, EU SECRET-CRYPTO, ESA SECRET-CRYPTO). Para información nacional existe la especialidad **“CRIPTO”**, con igual criterio (por ejemplo: RESERVADO CRIPTO).
- Para la asistencia a determinadas reuniones nacionales o de OTAN, en las que se tratan asuntos relacionados con la guerra electrónica y la utilización de los medios electrónicos y de comunicaciones para la obtención de información, los organizadores exigen una garantía de que los asistentes son conscientes de la específica confidencialidad del tema y están dotados de los conocimientos técnicos precisos para seguir sin dificultad los contenidos de las reuniones. Esta garantía, que acompaña a la habilitación de seguridad, se denomina **“COMINT INDOCTRINATED”** en el ámbito de la OTAN, usando igual término o **“SIGINT”** para nacional. Esta garantía no existe en el ámbito UE, ni de la ESA

TRAMITACIÓN DE HABILITACIONES

Cumplimentar la documentación

El Jefe del organismo o entidad del que depende el Subregistro o Punto de Control, asesorado por el Jefe de Seguridad del Órgano de Control OTAN/UE, es el responsable de determinar qué personas tienen necesidad de acceder a la documentación clasificada, y de autorizar la solicitud de Habilitación Personal de Seguridad (HPS).

Todo aspirante a disponer de una Habilitación debe rellenar el Cuestionario Personal de Seguridad que sirve de base a las investigaciones preceptivas sobre los peticionarios.

La documentación que se debe cumplimentar está compuesta por los siguientes documentos:

- Solicitud de Habilitación Personal de Seguridad.
- Cuestionario Personal de Seguridad (CPS).
- Certificado de Instrucción de Seguridad.

En el caso del personal de empresas, también deberán aportar la Propuesta de Personal.

Se debe también cumplimentar el cuestionario cada vez que se solicite una renovación, ya que ésta exige una nueva investigación de antecedentes del titular de la Habilitación y su entorno.

Previamente a la tramitación de la solicitud de HPS, el personal peticionario será informado por el Jefe de Seguridad del Órgano de Control correspondiente, sobre las obligaciones y responsabilidades que contrae como titular de una HPS, y recibirá la concienciación de seguridad que le capacite para manejar adecuadamente la Información Clasificada. El Jefe de Seguridad garantizará con su firma en cada impreso de Certificado de Instrucción de Seguridad que el peticionario ha recibido la instrucción preceptiva. En aquellos casos en que, por imposibilidad manifiesta, esta instrucción de seguridad previa deba ser auto-impartida por el propio solicitante, éste deberá firmar la correspondiente Declaración de Lectura y Conocimiento, sobre la base de la cual, el Jefe de Seguridad podrá firmar el Certificado de Instrucción del expediente de solicitud de HPS.

Es importante que el solicitante, y el Jefe de Seguridad, o el personal del Subregistro, revise la documentación y se asegure que está correctamente cumplimentada, al objeto de evitar demoras innecesarias en el procedimiento, por devolución de los formularios incorrectamente cumplimentados.

Remitir la documentación

Una vez cumplimentado el cuestionario el interesado remite la documentación a su Punto de Control correspondiente, para que éste lo remita al Subregistro Principal del que depende que es, finalmente, el encargado de su envío a la ANS-D, adjuntando además, en el caso del personal militar, el certificado que acredite el resultado de las investigaciones.

Realizar las investigaciones

Teniendo como base el CPS cumplimentado por el interesado se procede a realizar las investigaciones preceptivas para determinar la idoneidad del peticionario para acceder a documentación clasificada. El procedimiento es diferente según se trate de personal civil o militar.

En el caso del personal militar el resultado de la investigación realizada se refleja en un certificado que lo acredita, extendido por el Segundo Jefe del Estado Mayor correspondiente, o bien por el Director Adjunto Operativo de la Guardia Civil para el personal de esa Institución,

o por el Director Adjunto Operativo de la Policía, para su personal. En el caso de estos organismos, no es obligatorio el envío del CPS con el expediente de solicitud, dado que el mencionado Certificado avala la investigación, salvo que lo requiera la ONS. En cualquier caso, el CPS siempre será cumplimentado por el solicitante, como herramienta necesaria para la investigación, quedando éste custodiado en los Subregistros respectivos, a disposición de su organismo o de la ONS.

Certificado de Habilitación

Finalizadas las investigaciones y siendo favorables los informes, la ANS-D extiende una Habilitación Personal de Seguridad que remite al Subregistro Principal del que depende el peticionario. En el caso de no concederse la habilitación por no cumplirse alguno de los requisitos de seguridad, la ANS-D no extiende un certificado de denegación sino que lo comunica al organismo que gestionó la solicitud, remitiendo una Resolución de Denegación, para su entrega al solicitante.

En el caso del personal que trabaja para los diferentes organismos de la Unión Europea (funcionarios comunitarios), en lugar del Certificado de Habilitación, la ONS expedirá un Certificado de Resolución, vinculante en el caso de que sea negativo y orientativo en el caso de un Certificado favorable, para que sea el Consejo de la UE o la Comisión Europea quien conceda dicha HPS.

Validez

Las habilitaciones de seguridad se extienden, inicialmente por un periodo de validez de cinco años. Si al finalizar este periodo se mantiene la necesidad de seguir disponiendo de la habilitación, se solicitará su renovación a la ANS-D, quién iniciará el proceso de renovación por periodos de validez de cinco años, en el caso de las Habilitaciones de grado SECRETO, y de diez años en el caso de habilitaciones de grado inferior.

Retirada de la HPS

La ANS podrá proceder a la retirada de una HPS si considera que existen motivos que lo justifican, bien de oficio, bien a petición de un Órgano de Control principal. Dichos motivos habrán de ser conocidos con posterioridad a la concesión de la HPS o sobrevenidos a la misma, e incompatibles con los criterios para la determinación de idoneidad para una HPS.

Suspensión de la HPS

En caso de necesidad, y por motivo de circunstancia sobrevenida o conocida que pueda afectar a la seguridad de la Información Clasificada, la ANS-D podrá proceder, en cualquier momento, a la suspensión de los efectos de una HPS en vigor, a la que seguirá el inicio por la ONS de un proceso de investigación del que se derivará la retirada o continuación en vigor de la HPS afectada.

Durante el periodo de suspensión, a todos los efectos el usuario carece de Habilitación Personal de Seguridad, lo que deberá ser comunicado al Órgano responsable de la custodia de la HPS, a los Organismos que dispongan de certificaciones en vigor sobre esta HPS y al propio usuario.

PROTECCIÓN DE LA INFORMACIÓN CLASIFICADA

La protección de la Información Clasificada objeto de la presente instrucción requiere que se implementen un conjunto integrado de medidas que abarquen diversos aspectos de la seguridad: Seguridad Física, Seguridad en el Personal y Seguridad de la Información. La creciente utilización de los Sistemas de Información y de Comunicaciones (Sistemas CIS) para manejar o transmitir la Información Clasificada, requiere que también se implementen estas mismas medidas a las instalaciones donde se ubican estos sistemas para dotarles de un entorno seguro.

SEGURIDAD FÍSICA

La Seguridad deberá ser concebida de forma global, mediante una combinación de medidas físicas complementarias que garanticen un grado de protección suficiente, coordinando su aplicación con el resto de medidas de seguridad: Seguridad en el Personal, Seguridad de la Información y Seguridad en los Sistemas de Información y Comunicaciones.

Las instalaciones en las que material e Información Clasificada vayan a ser almacenados o manejados deberán ser protegidas mediante las apropiadas medidas de Seguridad Física, teniendo en cuenta los siguientes factores:

- Grado de clasificación de la información.
- Origen de la información.
- Cantidad y formato de la información (papel, dispositivos informáticos... etc.)
- Necesidad de conocer del personal.
- Amenazas y Vulnerabilidades.
- Medios de almacenamiento de la información.

La seguridad se constituye según un esquema de defensa en profundidad, en diferentes entornos sucesivos, desde el perímetro exterior de la Base, Acuartelamiento, Edificio o Local, hasta llegar al recinto final de la instalación. Se distinguen los siguientes entornos:

- **Entorno Global de Seguridad (EGS):** Se refiere al perímetro o perímetros de seguridad exteriores, que es necesario sobrepasar para llegar a la propia Zona de Acceso Restringido.
Se compone de elementos de seguridad tales como elementos estructurales de protección (vallas, iluminación de seguridad, detectores de presencia y paso, circuitos cerrados de TV perimétricos, etc.), control general de accesos y de identificación, guardias de seguridad, patrullas y fuerzas de reacción.
- **Entorno Local de Seguridad (ELS):** Viene referido a la seguridad inmediata e interior de la propia Zona de Acceso Restringido, por lo que incluye las medidas instaladas en las zonas adyacentes a la misma, en los propios paramentos y accesos, así como en el interior de la propia instalación, impidiendo el acceso a la Información Clasificada allí manejada.
Se compone de elementos de seguridad tales como elementos estructurales de protección (paramentos de fortaleza adecuada, puertas blindadas, cerraduras de

seguridad, etc.), sistema de control de acceso, detectores de intrusión, cámaras CCTV, cajas y armarios de seguridad.

- **Entorno Electrónico de Seguridad (EES):** Medidas implementadas para evitar fugas de información relacionadas con fenómenos TEMPEST, o establecidas contra escuchas activas o pasivas.

Toda instalación en la que se vaya a almacenar o manejar material o información clasificados deberá someterse a un proceso de acreditación por el que se declara su constitución como **Zona de Acceso Restringido (ZAR)**.

Las ZAR son instalaciones donde se almacena o maneja Información Clasificada “CONFIDENCIAL o equivalente”, o superior, por lo que deberán contar con las medidas y procedimientos de seguridad adecuados y suficientes, para asegurar la protección de la Información Clasificada en todo momento.

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

- a) **ÁREA CLASE I:** área en la que se maneja y almacena Información Clasificada de tal forma que la entrada a la zona supone, a todos los efectos, el acceso a la Información Clasificada, por lo que sólo puede acceder personal debidamente habilitado y autorizado. Este tipo de área precisa:
 - Un perímetro claramente definido y protegido a través del cual se controlen todas las entradas y salidas.
 - Un sistema de control de entrada que admita exclusivamente a aquellas personas debidamente habilitadas y específicamente autorizadas para acceder a dicha área.
 - Que las personas que accedan a la zona sean informadas previamente del tipo y grado de clasificación de la información a la que da acceso la entrada.

- b) **ÁREA CLASE II:** área en la que se maneja y almacena Información Clasificada de tal forma que pueda estar protegida del acceso de personas no autorizadas mediante controles establecidos internamente, por lo que se podrá admitir la entrada a personal visitante debidamente controlado. Este tipo de área precisa:
 - un perímetro claramente definido y protegido a través del cual se controlen todas las entradas y salidas;
 - un sistema de control de entrada que sólo permite el acceso sin escolta a aquellas personas con habilitación de seguridad y con autorización específica para acceder a la zona. A todas las demás personas se les proporcionará escolta o controles equivalentes a fin de evitar el acceso no autorizado a la Información Clasificada y la entrada, no controlada, a las zonas sujetas a inspección de seguridad técnica.

Una Zona de Acceso Restringido siempre estará bajo del control de un Órgano de Control (Servicio de Protección de Materias Clasificadas, Subregistro Principal... etc.)

La Acreditación es la autorización expresa que se otorga a una instalación, configurada como Área Clase I ó Área Clase II, especificando el origen y grado máximo de clasificación de la información que puede ser almacenada o manejada en la misma.

La competencia de Acreditación recae en la Oficina Nacional de Seguridad (ONS) como órgano de trabajo de la Autoridad Delegada para la Seguridad de la Información Clasificada (ANS-D), pudiendo ser delegada esta competencia.

El proceso de Acreditación exigirá la elaboración, por parte del Responsable de Seguridad de la Zona de Acceso Restringido de un **Plan de Protección**. Dicho plan se deberá redactar conforme al modelo elaborado por la ONS, el cual consta de tres documentos básicos:

- **Plan de Acondicionamiento:** Su objeto es describir los sucesivos entornos de seguridad existentes, las características físicas y las medidas técnicas adoptadas, que permiten alcanzar un nivel de protección suficiente. No debe incluir, en ningún caso, procedimientos, normas o medidas organizativas, que sean objeto de los otros planes.
- **Plan de Seguridad:** Su objeto es describir las medidas organizativas de seguridad, es decir, los procedimientos de control, gestión, trabajo, guarda, salvaguarda, etcétera, establecidos en el Órgano, Local o Área de Seguridad para, en conjunción con las medidas de Seguridad Física existentes (explicadas en el Plan de Acondicionamiento), permitir y garantizar la protección de la Información Clasificada y su adecuado manejo, en condiciones de trabajo habituales.
- **Plan de Emergencia:** Su objeto es describir las medidas organizativas de seguridad a adoptar o seguir para mantener la protección de la Información Clasificada ante contingencias de tipo extraordinario que puedan afectar a la misma, incluyendo los métodos y prioridades para el traslado, custodia y, en su caso destrucción, de esa información clasificada en caso de que tuviera lugar una situación de emergencia durante la cual la información pudiera verse comprometida.

El Jefe de Seguridad del Órgano de Control (Servicio de Protección de Materias Clasificadas, Subregistro Principal... etc.) bajo cuyo control esté la Zona de Acceso Restringido, será responsable de verificar y declarar que el Plan de Protección es completo, correcto y está adecuadamente implantado. Cuando el propio Jefe de Seguridad sea a su vez Responsable de Seguridad de la Zona de Acceso Restringido, la responsabilidad será del Jefe de Seguridad del Órgano de Control superior.

SEGURIDAD EN EL PERSONAL

Las medidas de Seguridad en el Personal garantizarán que las siguientes personas disponen de Habilitación Personal de Seguridad:

- El personal que pertenece al Órgano de Control, es decir, el personal que está permanentemente asignado al mismo.
- Los usuarios de los documentos clasificados del organismo, empresa, etc., al que sirve dicho Órgano de Control.

- El personal que realiza las rondas de vigilancia fuera del horario laboral, en previsión de que pudiera tener un acceso fortuito a la documentación clasificada.

Además, se establecerán procedimientos de control para:

- Las visitas que accedan a la zona de seguridad donde se encuentra ubicado el Órgano de Control o al propio órgano.
- El personal que tenga que realizar tareas de limpieza o de mantenimiento.

Estos procedimientos consistirán en:

- Facilitar escoltas para las visitas, y en el caso del personal de limpieza y mantenimiento que realice sus tareas dentro del horario laboral, se garantizará que esté presente el personal propio del Órgano de Control y que la documentación esté custodiada apropiadamente. No se autorizará nunca el trabajo del personal de limpieza sin escolta en zona de seguridad de Clase I.
- Proveer de tarjetas de identificación y registrar los datos personales de las visitas.

SEGURIDAD DE LA INFORMACIÓN

La Seguridad de la Información se obtiene cuando se aplica un conjunto de medidas y procedimientos para el correcto manejo de la Información Clasificada y para prevenir y detectar los posibles comprometimientos de la misma, que puedan afectar a su confidencialidad, integridad o disponibilidad. La Información Clasificada debe ser protegida y manejada a lo largo de todo su ciclo de vida de forma apropiada con su grado de clasificación.

Lo que sigue es un resumen de la reglamentación de seguridad para el acceso y manejo de la documentación clasificada según los diferentes grados de clasificación.

Información “SECRETO o equivalente”

- Como norma general no podrá extraerse del Órgano de Control: Subregistro o Punto de Control autorizado por la ANS-D, para custodiar y manejar este tipo de información.
- Se almacenará en un contenedor de seguridad aprobado por la ANS-D, de forma separada del resto de la documentación clasificada, es decir, si en el contenedor se custodian otros documentos del mismo tipo, la información “SECRETO o equivalente” se guardaría en carpetas separadas y por tipos (según origen: nacional, OTAN, etc.).
- Sólo puede circular a través del Registro Central o Servicio Central de Protección, según corresponda, nunca directamente entre Órganos de Control.
- Sólo el Registro Central está autorizado para la realización de copias y la destrucción de documentos.
- Cada vez que un usuario consulte un documento de grado máximo deberá firmar en la ficha de control y acceso que va unida al documento.

Información “RESERVADO o equivalente”

- Se manejará en Zonas de Acceso Restringido, configuradas como Clase I ó Clase II.
- Se almacenará en contenedores de seguridad aprobados por la ANS-D.

- Su transmisión al exterior se realizará a través de correos oficiales de las organizaciones propietarias de la Información Clasificada respectivamente, diplomáticos o militares, o a través de sistemas de transmisión electrónica cifrados acreditados por la ANS-D. Dentro del territorio nacional también se podrán utilizar servicios de correo comerciales, siempre que **hayan sido acreditados** por la ANS-D para la realización de dicho transporte.
- Sólo los Órganos de Control están autorizados a realizar copias, que deberán ser controladas y registradas como un documento más. El Órgano de Control deberá informar de ello al Subregistro Principal del que dependa.
- Cada vez que se consulte se deberá firmar la ficha de control y acceso.

Información “CONFIDENCIAL o equivalente”

- Se manejará en Zonas de Acceso Restringido, Clase I o Clase II.
- Se almacenará en contenedores de seguridad aprobados por la ANS-D.
- Su transmisión se realizará de la misma forma que para la documentación RESERVADO, pero se pueden utilizar sistemas de transmisión electrónica cifrados autorizados por la ANS-D. Dentro del territorio nacional es posible el transporte personal de documentos, siempre que se cuente con la autorización del Jefe de Seguridad del Subregistro correspondiente.
- Sólo los Órganos de Control están autorizados a realizar copias que deberán ser registradas y controladas como un documento más.

Información “DIFUSIÓN LIMITADA o equivalente”

- Puede acceder a ella personal sin Habilitación Personal de Seguridad, siempre que tenga necesidad de conocer por motivos de trabajo y haya sido instruido en las normas de seguridad.
- Podrá manejarse en Zonas Administrativas de Protección oficiales.
- Se puede almacenar en muebles provistos de cerradura.
- Para su transmisión se pueden utilizar los mismos medios que para la transmisión de la información CONFIDENCIAL, pero además, dentro del territorio nacional se puede remitir a través del correo nacional certificado.
- Los usuarios por motivos de trabajo pueden realizar copias de la misma.

Información NATO UNCLASSIFIED (NU)

- Puede acceder a ella el personal que acredite poseer una necesidad de conocer para la realización de trabajos oficiales.
- Se puede almacenar en muebles provistos de cerradura.
- Para su transmisión se pueden utilizar los mismos medios que para la información DIFUSIÓN LIMITADA.
- Los usuarios por motivos de trabajo pueden realizar copias de la misma.

MANEJO DE LA INFORMACIÓN CLASIFICADA

USUARIO DE LA INFORMACIÓN CLASIFICADA

El usuario es la persona que, en el cumplimiento de sus cometidos oficiales, tiene que acceder a la Información Clasificada y, en consecuencia, está debidamente autorizado por su Organismo o Entidad y cumple los requisitos de acceso a la Información Clasificada.

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

El usuario asume las siguientes responsabilidades al acceder a Información Clasificada:

- Dar la adecuada protección a la Información Clasificada a su cargo.
- Conocer y cumplir la normativa nacional y las normas específicas de seguridad de su Organismo o Entidad, referentes a la protección de la Información Clasificada.
- Mantener la debida reserva ante terceros sobre su condición de titular de una habilitación de seguridad.
- No introducir ni extraer de ESPAÑA Información Clasificada al margen de la Infraestructura Nacional de protección.
- Cooperar con el Jefe de Seguridad del Órgano de Control de su Organismo o Entidad en todo aquello que se relacione con la seguridad de la Información Clasificada en su puesto de trabajo, en su entorno laboral y en las actividades y foros en que intervenga.
- Mantener la reserva sobre la Información Clasificada a la que tuvo acceso, incluso una vez haya caducado la habilitación de seguridad.
- Informar al Jefe de Seguridad de cuantas circunstancias puedan afectar negativamente a la adecuada protección de la Información Clasificada.

Nos ocuparemos a continuación de las normas establecidas para el manejo de la documentación clasificada de forma adecuada por el usuario.

REGISTRO Y DIFUSIÓN DE LA INFORMACIÓN

Como ya se dijo anteriormente la distribución de la Información Clasificada siempre se efectuará entre los Órganos de Control. En el caso de que un usuario reciba directamente documentos clasificados sin pasar por el Órgano de Control, éste tiene la obligación de proceder a su regularización, de forma que sean dados de alta y registrados. Para ello lo comunicará al Órgano de Control del que dependa, quien a su vez deberá informar al Registro Central si el documento es de clasificación “CONFIDENCIAL o equivalente”, o superior, para que éste proceda a su registro.

En cuanto a la **difusión** el usuario asume las siguientes obligaciones:

- No difundir información, ya sea en forma oral o escrita, a ningún otro usuario sin la autorización del Jefe de Seguridad de su Órgano de Control.

- No introducir ni extraer de España documentos de ningún grado de clasificación al margen de la infraestructura nacional.

CONSULTA

Como norma general los documentos con clasificación “CONFIDENCIAL o equivalente”, o superior, no se custodiarán fuera del Órgano de Control, realizándose la consulta de los mismos en las instalaciones de éste, o en Zonas de Acceso Restringido autorizadas para dicho fin. En los casos excepcionales en que un usuario necesite disponer de documentos clasificados en su puesto de trabajo, solicitará la autorización del Jefe de Seguridad, quien podrá autorizarlo, por un plazo determinado, siempre que se cumplan las condiciones de seguridad requeridas para la custodia de dicha documentación según su grado de clasificación.

CONTROL DE ACCESO A LA INFORMACIÓN

Debido a que tanto la información “RESERVADO o equivalente”, o superior, son informaciones imputables, es preceptivo que los documentos con este grado de clasificación lleven unida una Ficha de Control y Acceso, donde queden registrados todos los accesos a los mismos. Cuando un usuario acceda a un documento con estos grados de clasificación deberá firmar en dicha ficha, una vez rellena con sus datos y la fecha y hora inicial y final de acceso.

El objetivo de esto es proveer de suficiente información para poder realizar una investigación en el caso en que se produzca un compromiso de la información imputable, es decir, una pérdida de la misma o su revelación a personas no autorizadas.

Tratándose de documentos de grado de clasificación inferior será el Jefe de Seguridad quien determine la forma en que se controla el acceso a los mismos.

REPRODUCCIÓN, TRADUCCIÓN Y EXTRACTOS DE DOCUMENTOS CLASIFICADOS

Se debe evitar la reproducción incontrolada de documentos clasificados, no haciendo más copias que las estrictamente necesarias.

Las copias, traducciones y extractos de documentos clasificados se controlarán de la misma forma que el documento original, se registrarán y numerarán, no existiendo a efectos de seguridad diferencias entre original y copia.

El usuario está autorizado a realizar las copias, extractos y traducciones de documentos con grado de clasificación “DIFUSIÓN LIMITADA o equivalente” y NATO UNCLASSIFIED, siempre que se asegure su control de forma que no se produzcan accesos no autorizados a los mismos.

El Jefe de Seguridad de su Órgano de Control es quien tiene que autorizar las reproducciones, traducciones y extractos de documentos con grados de clasificación CONFIDENCIAL y RESERVADO, o equivalentes.

Los documentos de grado “equivalente a SECRETO” no podrán ser reproducidos. En caso de necesitarse copias estas se solicitarán a través del Registro Central.

DESTRUCCIÓN DE LA DOCUMENTACIÓN CLASIFICADA

Con objeto de evitar una acumulación excesiva de documentación clasificada, que dificulte su localización y explotación eficaz, el principal usuario de la misma es el responsable de su revisión periódica, para decidir cuales son los documentos que por obsoletos o no útiles se deben destruir.

Sólo los documentos con grado de clasificación “DIFUSIÓN LIMITADA o equivalente” y NU pueden ser destruidos directamente por el usuario, sin la autorización del Jefe de Seguridad, siempre que se utilice un procedimiento de destrucción aprobado por la ANS-D.

El Jefe de Seguridad es el único que puede autorizar la destrucción de cualquier documento con grado de clasificación “CONFIDENCIAL o equivalente”, o superior, cuya destrucción haya sido previamente decidida por el usuario.

Para la destrucción de documentos RESERVADO y CONFIDENCIAL, o equivalentes, se cumplimentará un acta de destrucción que irá siempre firmada por el Jefe de Seguridad del Órgano de Control. Los documentos del “equivalente a SECRETO” sólo pueden ser destruidos por el Registro Central.

TRANSPORTE PERSONAL DE DOCUMENTACIÓN CLASIFICADA

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 las comunicaciones.

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.

Cuando con motivo de asistencia a una actividad o reunión clasificada en otro emplazamiento, especialmente en el extranjero, se haga entrega en la misma al representante español participante, de información de grado “CONFIDENCIAL o equivalente” o superior, éste notificará al Oficial de Seguridad del evento la obligación 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.

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 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 aprobados.
- 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**.

Transporte dentro de un mismo edificio o recinto

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 (si porta información “CONFIDENCIAL o equivalente”), en sobre cerrado, maletín o en una carpeta, que no permita ver su contenido.

Transporte fuera de un mismo edificio pero dentro del territorio nacional

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, quien garantizará que los documentos a transportar se empaquetan y preparan de forma adecuada y que van acompañados del correspondiente recibo en caso necesario.

Con carácter limitado podrá autorizarse el transporte personal de información con grado “RESERVADO o equivalente”.

Cuando los documentos sean de grado “CONFIDENCIAL o equivalente” se transportarán, dentro del correspondiente maletín, en un sobre opaco, resistente y cerrado con precinto de lacre o cinta adhesiva especial, y la persona que realiza el transporte nunca se separará de los mismos.

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.

Transporte con motivo de la asistencia a actividades clasificadas en el extranjero

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).

El usuario deberá solicitar del Órgano de Control del que depende, un **Certificado de Correo**, y entregar una relación de todos los documentos a transportar, para que sean registrados. Al finalizar la actividad devolverá el certificado de correo al Órgano en que lo tramitó, quien comprobará la existencia de todos los documentos que salieron, y procederá, en caso de existir nuevos documentos, a su registro y alta en la red.

Certificado de Correo

Es emitido por el Registro Central y firmado por el Oficial de Autorización.

Los Jefes de Seguridad de los Órganos de Control, salvo de empresas contratistas, 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.

El Certificado de Correo con el sello oficial que corresponda acredita, ante cualquier control aduanero que pretenda la apertura de la cartera en la que se transportan los documentos clasificados, que el portador del mismo está autorizado a su transporte.

MANEJO DE LA INFORMACIÓN CLASIFICADA MEDIANTE SISTEMAS CIS

OBJETIVOS DE SEGURIDAD

Los objetivos de seguridad perseguidos cuando la Información Clasificada es manejada en los sistemas de información y telecomunicaciones (sistemas CIS) son:

- Mantener la confidencialidad de la Información Clasificada.
- Mantener la integridad de la Información Clasificada, así como de los sistemas que la manejan.
- Mantener la disponibilidad de la Información Clasificada y de los sistemas que la manejan.

Confidencialidad. Es la propiedad de la información por la cual no está disponible o no es revelable a personas o entidades no autorizadas.

Integridad. Es la propiedad de la información de no ser alterada ni destruida de forma no autorizada.

Disponibilidad. Es la propiedad de la información por la cual es accesible o utilizable bajo demanda de personas o entidades que estén autorizadas a acceder a la misma, cuando es preciso. Cuando falla la disponibilidad se tiene una denegación de servicio.

Estos objetivos de seguridad pueden perderse debido a una brecha de seguridad, sin que medie una actividad hostil, o como resultado de una actividad hostil, tal como espionaje, actos de terrorismo, sabotaje o robo.

AUTORIZACIÓN DE SISTEMAS

Para conseguir estos objetivos de seguridad todos los sistemas de información y comunicaciones (CIS), que almacenan, procesan y transmiten Información Clasificada, así como el entorno y condiciones en que se encuentra, estarán sujetos a un proceso de acreditación de su seguridad previo, en el que se tendrán en cuenta los objetivos de confidencialidad, integridad y disponibilidad.

La Autorización es la aprobación concedida a un determinado sistema para manejar Información Clasificada hasta un determinado grado de clasificación y en unas condiciones específicas. Conlleva unos procesos previos de Acreditación técnica del Sistema y de Acreditación de la Seguridad Física, Documental y en el Personal, sobre la base de la documentación de seguridad del sistema y su entorno:

- Concepto de Operación, Documento de Requisitos de Seguridad y Procedimientos Operativos de Seguridad del Sistema y
- Plan de Protección de la ZAR.

La Autorización de los sistemas CIS nacionales que manejan información “equivalente a DIFUSIÓN LIMITADA”, o superior, será realizada por la ANS-D, o autoridad oficialmente designada.

Todo usuario que deba manejar Información Clasificada en un sistema de información y comunicaciones, además de los requisitos generales para el acceso a la información del grado de clasificación de que se trate, deberá cumplir los siguientes:

- Haber leído y entendido los Procedimientos Operativos de Seguridad del Sistema, dejando constancia firmada de ello, y ejecutarlos en la parte que le corresponda.
- Haber leído y entendido el Plan de Protección de la ZAR donde se despliega el sistema, dejando constancia firmada de ello, y ejecutarlo en la parte que le corresponda.

CONTROL Y MANEJO DE LOS SOPORTES INFORMÁTICOS

La Información Clasificada requiere ser protegida no sólo cuando se encuentra en el interior de un sistema CIS, donde se almacena o procesa, sino también cuando se extrae del mismo y se convierte en un documento bajo soporte informático.

Para ello todos los soportes de almacenamiento informático (discos duros, disquetes, CDROM, “pen-drives”, etc.) que contengan información con clasificación “CONFIDENCIAL o equivalente”, o superior, deberán estar identificados, registrados y controlados, de acuerdo con el mayor grado de la clasificación que contengan, en el Órgano de Control al que pertenezcan.

Identificación de soportes informáticos extraíbles

Dichos controles e identificación deberán incluir como mínimo:

- Para “CONFIDENCIAL o equivalente”, y superior, se utilizará un sistema de identificación para cada soporte por separado que incluya un número de registro y la

clasificación de seguridad. Además cada Órgano de Control debe establecer procedimientos para el registro, control de la emisión, acceso y destrucción de los soportes.

- Para “RESERVADO o equivalente”, y superior, se mantendrá, además, un registro donde figuren todos los detalles relativos a los soportes, incluyendo su contenido general y clasificación.
- Se realizarán inspecciones periódicas para verificar que el contenido de los soportes coincide con su identificación y con los datos que figuran en el registro.



ANEXO III: INSTRUCCIÓN DE SEGURIDAD CRIPTO

Se adjunta un documento separable, y con numeración propia, al objeto de que pueda desglosarse o copiarse como manual de instrucción del personal, separado del presente documento que es para uso exclusivo de los instructores.



INSTRUCCIÓN DE SEGURIDAD CRIPTO



INTRODUCCIÓN

El objeto del presente documento es dar la instrucción básica necesaria para poder manejar Material de Cifra como usuario y, asimismo, constituir el manual para recibir la instrucción CRIPTO, dentro del proceso de solicitud de una Habilitación Personal de Seguridad (HPS) con la especialidad CRIPTO (o Autorización Criptológica). Este manual debe ser complementado con los procedimientos concretos relativos al Material de Cifra que se va a manejar y que deban ser ejecutados por el usuario que está siendo instruido, los cuales, por depender de diferentes ámbitos y con procedimientos específicos, no se contemplan en esta instrucción.

El personal que vaya a ocupar cargos de responsabilidad en el manejo de Material de Cifra, como pueden ser el Criptocustodio o el Alterno Criptocustodio, deberá recibir una instrucción específica en dichos cometidos, siendo el presente manual insuficiente para aportar la formación necesaria para ocupar dichos puestos.

En este documento se contienen requisitos mínimos para el manejo y control del Material de Cifra y las instrucciones básicas por las que se regulan los procedimientos de Seguridad Criptológica, así como las medidas a adoptar por los usuarios de dichos sistemas para preservar la Seguridad Física y Criptológica del Material de Cifra.

El manejo del Material de Cifra está regulado en la normativa específica que le es de aplicación en función de su procedencia (nacional, OTAN, UE, etc.). No se permite el empleo de normas o procedimientos menos estrictos, aunque los Jefes o Responsables de los correspondientes departamentos, organismos o entidades pueden imponer requisitos adicionales sobre aquellos artículos que se encuentren bajo su contabilidad.

El Material de Cifra se manejará habitualmente en las Cuentas de Cifra, Centros de Cifra, Centros de Comunicaciones, Puntos de acceso remotos o estaciones aisladas de enlace, Zonas de Acceso Restringido donde se ubican Sistemas de Información y Comunicaciones, etc. En todos ellos, las condiciones de seguridad deben estar debidamente acreditadas e implantadas y existir la figura del Responsable de Seguridad, así como una estructura de Seguridad Criptológica.

SEGURIDAD CRIPTOLÓGICA

La Seguridad de las Tecnologías de la Información y Comunicaciones o STIC, es el resultado de un conjunto de medidas, entre ellas las **criptológicas**, orientadas a proteger la información almacenada, procesada o transmitida por Sistemas de Información y

Comunicaciones, de manera que se aseguren o garanticen la confidencialidad, integridad y disponibilidad de la información y la integridad y disponibilidad de los propios sistemas.

Dependiendo del sistema donde se encuentre la información, hablaremos de la Seguridad de los Sistemas de Información (SSI), Seguridad de los Sistemas de Comunicaciones (COMSEC) y Seguridad Electrónica (ELSEC). En todos ellos se pueden emplear procedimientos criptológicos para asegurar que la información está protegida.

La criptología es la ciencia que estudia la ocultación, disimulación o cifrado de la información, así como el diseño de sistemas que realicen dichas funciones, e inversamente, la lógica y álgebra aplicada para la obtención de la información protegida.

En este sentido, la Seguridad Criptológica es una componente de la Seguridad de las Tecnologías de la Información y Comunicaciones que resulta de utilizar un criptosistema adecuado para los requerimientos de protección de la información y de su correcto empleo.

La información y materiales criptológicos, utilizados para garantizar la Seguridad Criptológica, por su naturaleza y por las implicaciones de su revelación no autorizada, deben estar controlados y ser manejados conforme a reglas y procedimientos más restrictivos que los utilizados para el resto de la Información Clasificada.

El comprometimiento de un criptosistema conlleva que toda la información que ha sido protegida con el mismo queda igualmente comprometida, constituyendo, por tanto, un perjuicio mucho más grave.

Consecuencia de ello es que, estos criptosistemas son objetivo principal de los servicios de inteligencia contrarios o enemigos. En este sentido, siempre debe tenerse en cuenta que el elemento más vulnerable de un criptosistema y sobre el que se ejercen la mayoría de las acciones de ataque lo constituyen las personas que manejan dicho criptosistema. Por este motivo, es fundamental que las mismas estén adecuadamente instruidas en la importancia de lo que manejan y conozcan los peligros a los que se está sometido, así como las responsabilidades inherentes al cargo desempeñado.

Para alcanzar la Seguridad Criptológica es necesario:

- a.** Contar con una estructura u organización responsable del funcionamiento de los procesos asociados a la Seguridad Criptológica.
- b.** Tener definida la jerarquía de responsabilidades para los asuntos criptológicos.
- c.** Planificar y ejecutar ejercicios periódicos de instrucción para cerciorarse de que el personal de cifra y operadores de criptosistemas manejan perfectamente los sistemas disponibles, incluso de los que raramente se hace uso.
- d.** Contar con elementos adecuados de Seguridad Física del Material de Cifra.
- e.** Instalar y mantener los equipos en las debidas condiciones y de conformidad con los procedimientos prescritos.

- f. Empleo exclusivo de personal de la máxima confianza y lealtad, y cuidadosamente instruido y examinado en cuanto a su pericia en el empleo de los sistemas de cifra antes de que se les permita operar con el equipo.
- g. Constante alerta del personal sobre la importancia de la seguridad y las normas que se espera que sigan.

EL MATERIAL DE CIFRA

El Material de Cifra puede agruparse en las tres categorías principales siguientes:

- a. **Material de Claves.** Incluye todas las cintas de clave, 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 grado de clasificación “RESERVADO o equivalente” o superior.
 - Claves de Bajo Nivel: son aquellas claves con grado de clasificación “CONFIDENCIAL o equivalente” o inferior.
- b. **Equipo de CIFRA.** El término equipo de CIFRA significa cualquier equipo o programa empleado para proteger la información transmitida a través de un sistema de telecomunicación, o manejada en un sistema de información, convirtiéndola en ilegible y volviendo a convertirla a su forma original. Además del equipo de CIFRA básico, esta categoría incluye los siguientes:
 - (1) Equipo auxiliar de CIFRA que se emplea en unión del equipo básico para facilitar una operación eficaz, pero que no puede realizar por sí mismo una función de cifrado.
 - (2) Equipo de producción de CIFRA, empleado en la generación, fabricación y prueba del Material de Claves.
 - (3) Equipo de autenticación, diseñado para facilitar protección contra la transmisión fraudulenta o para establecer la validez de un mensaje, remitente o sistema de telecomunicación.
 - (4) Algunos equipos auxiliares constituyen un artículo esencial en una instalación criptológica, pero no caen estrictamente dentro de la definición de equipo auxiliar de CIFRA y precisan de manejo o controles especiales para proteger ciertas características especiales de seguridad, pudiendo ser manejados de la misma forma que el equipo auxiliar por motivos de conveniencia, por ejemplo, el equipo que cuente con protección TEMPEST.
- c. **Publicaciones.** Esto incluye toda la documentación asociada a un sistema de cifra, como son las instrucciones de funcionamiento, manuales del usuario, manuales de instalación, manuales de mantenimiento, instrucciones de seguridad de cifra y todo el

restante Material de Cifra impreso, (a excepción del Material de Claves a que se ha hecho referencia en el párrafo anterior).

La marca de manejo especial "**CRIPTO**" se aplica a la correspondencia, mensajes, informes, u otros documentos o materiales, que contengan información relativa a cifra, de naturaleza sensible, y que de darse a conocer a personas no autorizadas, podrían conducir o ayudar a descifrar las comunicaciones cifradas. El acceso al material marcado de esta forma queda restringido a las personas que dispongan de la apropiada "acreditación" de seguridad y autorización CRIPTO.

Como orientación general, algunos ejemplos de los tipos de información que pueden justificar la aplicación de esta marca, son los siguientes:

- a. Especificaciones de Seguridad de Sistemas de Cifra.
- b. Detalles relativos a características de Seguridad Criptológica de naturaleza sensible, relativas al equipo y sistemas de cifra, incluyendo principios criptológicos, descripciones, fotografías, diagramas, cambios o modificaciones recomendados, etc.
- c. Resultados de ensayos de seguridad en sistemas cripto.
- d. Datos específicos de claves y especificaciones de normas de seguridad para la producción del Material de Claves.
- e. El propio Material de Claves.
- f. Procesos y métodos de criptoanálisis.

ESTRUCTURA DE SEGURIDAD CRIPTOLÓGICA

En todo departamento, organismo o entidad, que maneje Material de Cifra, debe existir una estructura u organización responsable de la Seguridad Criptológica. Esta organización se establece en los siguientes niveles:

- a. **Autoridad de Control de Material de Cifra (ACMC).** Es el máximo responsable único en cada departamento ministerial, organismo principal o Cuartel General, del registro, contabilidad y seguimiento de todo el Material de Cifra creado y utilizado bajo su responsabilidad para la protección de la información, estableciendo los procedimientos adecuados.
- b. **Órgano de Distribución de Material de Cifra (ODMC).** Da servicio a la ACMC. Se constituirá en cada departamento ministerial, organismo principal o Cuartel General, que cuente con una ACMC. Tiene los siguientes cometidos:
 - Generación y confección de claves.
 - Establecimiento de periodos de vigencia de las claves.
 - Distribución y control de claves.

- Control de los procesos de introducción, utilización y destrucción de las claves.
- c. Criptocustodio y Alternativo.** Se constituyen en cada organismo o entidad que disponga de una Cuenta de Cifra. Posteriormente se definen sus cometidos.
- d. Usuarios de Material de Cifra.** Responsables últimos del manejo de Material de Cifra. Normalmente estarán encuadrados en Centros de Comunicaciones, Centros de Cifra, Centros de Procesos de Datos, etc. Posteriormente se definen sus cometidos.

En determinadas instalaciones, especialmente donde existe un número elevado de Sistemas de Información y Comunicaciones con Criptosistemas asociados (como puede ser un CECOM), existe la figura del **Oficial COMSEC**, o en algunos casos **Oficial INFOSEC**, que se responsabiliza de la explotación de todo el Material de Claves en dicha instalación. Incluso, existen en determinadas ocasiones Centros de Cifra, donde se centraliza toda la operación de cifrado y descifrado dentro de un CECOM. Cuando así lo estime el Mando, este cargo podrá asumir las funciones de Criptocustodio. Si existen ambas figuras, las responsabilidades de uno y otro deben estar plenamente definidas y separadas. Más adelante se especifican los cometidos concretos de cada uno.

Con independencia de toda esta estructura, los Mandos y Responsables de los departamentos, organismos o entidades en que se constituyen estas figuras, son los responsables de la Seguridad Criptológica, por lo que en todo momento velarán porque cumplan adecuadamente con sus cometidos y designarán para dichos puestos a personal con formación y de fiabilidad reconocida.

En general, unos y otros, cada uno en su función, serán responsables de:

- a.** Solicitar la apertura de Cuentas de Cifra.
- b.** Relacionarse con las Autoridades responsables de la generación y distribución de claves, en su ámbito.
- c.** Recibir, custodiar, gestionar, controlar, distribuir y, en su caso destruir, el Material de Cifra.
- d.** Instruir a los usuarios para el manejo de Material de Cifra.
- e.** Auditar la utilización del Material de Cifra a su cargo.
- f.** Gestionar los incidentes de seguridad relativos al Material de Cifra a su cargo.
- g.** Coordinar sus actuaciones con el Servicio de Protección de Información Clasificada del que dependan.

APERTURA DE CUENTAS DE CIFRA

Una Cuenta de Cifra entendida como órgano y no como lista de activos disponibles a cargo, es un elemento formalmente constituido, que dispone de personal cualificado,

instalaciones y medios, y que, sobre la base del exacto cumplimiento de unos procedimientos establecidos, es responsable de la custodia, manejo, protección y contabilidad del Material de Cifra.

Cada Cuenta de Cifra dará servicio a un determinado estamento (Organismo, Centro, Unidad, Instalación, Empresa o Grupo de Empresas). El Mando (Jefe o Director) de dicho estamento es el responsable de la adopción de todas las medidas necesarias para alcanzar y mantener la seguridad de todo el Material de Cifra dentro de su jurisdicción y, por tanto, será quien determine si debe establecerse o no una Cuenta de Cifra, delegando, normalmente, en el Criptocustodio para el ejercicio de las funciones que se deriven de su establecimiento. De dicha Cuenta Principal dependerán las Cuentas de Cifra subordinadas que se establezcan en Unidades dependientes de dicho Organismo, Centro, etc.

Cuando se haya tomado la determinación de que es preciso crear una Cuenta de Cifra en una ubicación nacional (dentro del territorio nacional, en plaza de soberanía, o en recinto de embajada), el Mando de la organización presentará una petición formal a la Autoridad que sea competente en la materia, en conformidad con la normativa por la que se rija. Normalmente, se debe incluir la siguiente información:

- a. El título corto y la dirección completa de la organización que precisa la Cuenta de Cifra.
- b. Los artículos concretos de Material de Cifra, y la fecha en que se desea disponer de ellos.
- c. El propósito (justificación) para la creación de una Cuenta de Cifra.
- d. La aprobación por parte de la Autoridad competente del Plan de Protección (constituido por el Plan de Acondicionamiento, Plan de Seguridad y Plan de Emergencia), del local donde se ubicará físicamente la Cuenta de Cifra.
- e. Los nombres y rango o cargo de las personas expresamente habilitadas por la Autoridad competente, para los cometidos de Criptocustodio y Alterno Criptocustodio.
- f. Modelo de la firma del Criptocustodio y del Alterno Criptocustodio validada por el Mando de la Unidad.

Si la Cuenta de Cifra se solicita para una entidad u organismo civil, se considera Mando al cargo que ejerza funciones equivalentes.

El Oficial responsable de Seguridad del organismo o entidad a la que pertenece la Cuenta de Cifra, inspecciona las medidas de Seguridad Física adoptadas en las instalaciones de dicha Cuenta de Cifra e informa a la Autoridad competente del estado en que se encuentran.

Una vez comprobado que el informe de inspección realizado por el Oficial responsable de Seguridad es favorable y que las habilitaciones del personal responsable de la Cuenta de Cifra son adecuadas, la Autoridad competente registra la apertura de la Cuenta de Cifra y el nombramiento del Criptocustodio y del Alterno Criptocustodio.

Cada Cuenta de Cifra podrá mantener abiertas cuentas de activos (Material de Cifra) con diferentes Órganos de Distribución de Material de Cifra (ODMC). En este caso se mantendrá la separación física entre unas y otras, custodiándose en contenedores diferentes.

Un ejemplo puede ser una Cuenta de Cifra en un Escuadrón Aéreo que tiene material de claves y equipos de cifra de OTAN, de su propio Ejército y de la Armada. La misma Cuenta de Cifra tiene tres cuentas abiertas, una con cada estamento mencionado, y con los que mantiene relación y ejecuta los procesos específicos de cada uno relativos a su Material de Cifra.

PERSONAL RESPONSABLE

PERSONAL CRIPTO

El personal Criptocustodio y las personas que en el curso normal de sus funciones necesiten tener acceso regular a soportes de claves de alto nivel, y su documentación correspondiente, tendrán la habilitación en grado de “SECRETO o equivalente”.

Debido a lo delicado del Material de Cifra y a los rígidos controles requeridos, el Criptocustodio y su Alterno deben estar dotados de cualidades ejemplares. El Mando está obligado a seleccionar cuidadosamente el personal para cerciorarse de que las personas escogidas cumplen con los siguientes requisitos:

- a. No han sido destituidos con anterioridad de las obligaciones de Criptocustodio por razones de negligencia o falta de cumplimiento de sus deberes.
- b. Se trata de personas responsables, calificadas para asumir las obligaciones y responsabilidades de un Criptocustodio.
- c. Están en un cargo o nivel de autoridad que les permite ejercer la debida jurisdicción en el cumplimiento de sus responsabilidades.
- d. Están en un destino que les permite una permanencia en el mismo (que no sea inferior a un año), ya sea como Criptocustodio o Alterno, reduciéndose con ello la posibilidad de una sustitución frecuente.
- e. Están cumpliendo básicamente con la función de Criptocustodio día a día. El cargo de Criptocustodio o de su Alterno no se asumen solamente con el fin de mantener control administrativo o de gestión de las funciones de contabilidad.
- f. No se les podrán asignar obligaciones que interfieran con sus obligaciones como Criptocustodio y Alterno

El personal nombrado como Criptocustodio deberá tener la categoría de Oficial, Suboficial o personal civil de categoría equivalente, debiendo estar en posesión de una Habilitación Personal de Seguridad de grado apropiado a los materiales que pueda controlar y con autorización criptológica.

INSTRUCCIÓN DEL CRIPTOCUSTODIO Y DEL ALTERNO CRIPTOCUSTODIO

Antes de la presentación de una solicitud de una Cuenta de Cifra, el Mando se asegurará de que tanto el Criptocustodio, como el Alterno, están completamente familiarizados con los requisitos del presente documento y de otros documentos relacionados

RESPONSABILIDADES Y OBLIGACIONES DEL CRIPTOCUSTODIO

El Criptocustodio será responsable de la custodia, tratamiento, protección y, cuando sea necesaria, la destrucción de todo el Material de Cifra clasificado a cargo de la Cuenta de Cifra.

También es responsable de la recepción y, cuando sea aplicable, de la distribución del Material de Cifra. Además es responsable de la contabilidad, del mantenimiento de un registro exacto y puesto al día y la preparación y el envío de todos los informes relacionados con el Material de Cifra a cargo de la Cuenta de Cifra.

El Criptocustodio es responsable del manejo real, despacho, protección, contabilidad y, cuando sea necesario, de la destrucción del Material de Cifra clasificado existente en una Cuenta de Cifra. A continuación se presenta una lista detallada de las responsabilidades de los Criptocustodios:

- a.** Recibir, acusar recibo, almacenar y manejar el Material de Cifra para evitar su pérdida o posible comprometimiento físico.
- b.** Asegurarse de que el Material de Cifra es enviado solamente a personas debidamente acreditadas o autorizadas individualmente cuyas obligaciones lo requieren y asesorarles sobre la responsabilidad que tienen sobre la debida protección y control del Material de Cifra que obre en su poder.
- c.** Mantenerse informados de cualesquiera requisitos nuevos o modificaciones a los ya existentes que el Criptocustodio debe mantener
- d.** Preparar y remitir todos los informes de contabilidad necesarios, relativos al Material de Cifra.
- e.** Mantener un inventario de Material de Cifra y los correspondientes archivos, incluyendo un inventario al día. (Registro de Artículos) de todo el Material de Cifra, tanto registrado como sin registrar, su ubicación o destrucción.
- f.** Comprobar físicamente el inventario y preparar y cursar los informes pertinentes.
- g.** Efectuar la destrucción rutinaria o en emergencia, así como la disposición oportuna del Material de Cifra, en la forma necesaria.
- h.** Preparar y cursar los informes oportunos relativos al Material de Cifra

- i.** Inspeccionar la envoltura protectora o empaquetado del Material de Cifra durante la recepción inicial, durante cada uno de los inventarios y antes de su uso, para asegurarse de su integridad.
- j.** Trabajar con el Oficial COMSEC (INFOSEC) del usuario, si no ejerce él mismo esta función, para asegurarse de que existe una necesidad continua de una clave específica y, en caso de que esta necesidad no existiera ya, recomendar a la autoridad de contabilidad que la Cuenta de Cifra sea dada de baja para la distribución de dicha clave específica.
- k.** Efectuar con prontitud y precisión todas las enmiendas en las Publicaciones de Cifra empleadas por su organización. Cuando no están anotadas de entrada, las enmiendas se distribuirán a los usuarios junto con las Publicaciones para que se efectúe dicha anotación.
- l.** Asegurarse de que todas las comprobaciones de páginas exigidas, son realizadas en todo el Material de Claves y en todas las publicaciones cuando se reciban, devuelvan mediante recibo en mano, o sean transferidas o destruidas. Las comprobaciones de páginas deben también realizarse cuando se produzca un cambio de Criptocustodio y cuando se publiquen enmiendas que impliquen la sustitución de páginas. Todo el Material de Cifra, a excepción de las claves, será comprobado en lo que respecta a su paginado, al menos una vez al año.
- m.** Emitir o transferir el Material de Cifra tal como se disponga a las Cuentas de Cifra o a las personas autorizadas. Si el material es clasificado, verificará que los individuos tienen una Habilitación Personal de Seguridad de grado apropiado al material. Cuando se emita o transfiera el material, se exigirá un recibo firmado por el Criptocustodio de la Cuenta de Cifra, o un recibo en mano, igualmente firmado por la persona que reciba el material. Los usuarios de recibos en mano deberán ser informados de su responsabilidad en la protección y salvaguarda del material hasta que éste sea devuelto al Criptocustodio. Si el material ha de ser destruido por el usuario que lo recibió en mano, dicho usuario será también advertido de los requisitos exigidos para la destrucción.
- n.** Iniciar procedimientos organizativos para asegurar que las personas no abandonen la organización sin antes devolver o destruir el material COMSEC que se les envió o que les fuera entregado mediante recibo en mano.
- o.** Estar enterados en todo momento de la localización de cualquier artículo de Material de Cifra contabilizable, incluido en la Cuenta de Cifra y del propósito general para el que se emplea.
- p.** Estar familiarizado con los planes actuales para la destrucción, disposición, evacuación o protección del Material de Cifra en caso de incendio, desastre u otra emergencia.
- q.** Establecer procedimientos para asegurar el estricto control de todos los artículos del Material de Claves, siempre que los requisitos operativos precisen que el material sea entregado de un turno de trabajo a otro, o de una persona a otra.

- r. Informar de inmediato al Mando de cualquier comprometimiento físico conocido o sospechado, pérdida o destrucción/disposición no autorizadas de Material de Cifra. Al recibir tal notificación, el Mando, presentará un informe detallado de los hechos conocidos.
- s. Destruir el Material de Claves y demás material de cifra, en cuanto sea necesario, de acuerdo con los métodos de destrucción acordados y preparar el informe de la destrucción.

RESPONSABILIDADES Y OBLIGACIONES DEL ALTERNO CRIPTOCUSTODIO.

El Alterno Criptocustodio no comparte las responsabilidades del Material de Cifra con el Criptocustodio; cuando éste se halla presente es el único responsable. En ausencia del Criptocustodio, el Alterno asume todas las responsabilidades y obligaciones relacionadas con el Material de Cifra a cargo de la Cuenta de Cifra.

La persona nombrada Alterno de un Criptocustodio será responsable de asistir al titular en el cumplimiento de sus obligaciones y de facilitar la continuidad de las operaciones en ausencia del Criptocustodio. El Criptocustodio Alterno no comparte la responsabilidad del material con el Criptocustodio titular. Cuando se encuentre presente, el Criptocustodio es plenamente responsable. Las obligaciones específicas del Alterno Criptocustodio son las siguientes:

- a. Estar informado de la actividad cotidiana de la Cuenta de Cifra, con el fin de asumir las obligaciones del Criptocustodio titular, siempre que sea necesario, sin que se produzca una interrupción indebida de las operaciones.
- b. Realizar las obligaciones descritas anteriormente para el Criptocustodio, durante las ausencias temporales del mismo.
- c. Asegurarse de que los inventarios son firmados y debidamente atestiguados, en ausencia del Criptocustodio.
- d. Realizar las obligaciones indicadas anteriormente, en caso de un cese repentino, abandono permanente o ausencia no autorizada del Criptocustodio, antes del nombramiento de un nuevo Criptocustodio.

RESPONSABILIDADES DEL OFICIAL COMSEC (INFOSEC)

En cada escalón de mando y dentro de los organismos usuarios, el Mando es responsable de mantener la seguridad en los Sistemas de Información y Comunicaciones, así como del control de cualquier área en la que se almacene o manipule Material de Cifra. Para ayudar en el cumplimiento de estas responsabilidades, el Mando nombrará personas responsables para cumplir las obligaciones de Oficial COMSEC o INFOSEC. Un Oficial COMSEC (INFOSEC) puede actuar también como Criptocustodio.

El oficial COMSEC (INFOSEC) es responsable de servir como asesor del Mando en todos los asuntos relacionados con la explotación del Material de Cifra en las instalaciones de

su responsabilidad, incluyendo, cuando sea también el Responsable de Seguridad de la Zona, la Seguridad Física del Material de Cifra, inspecciones y puesta en práctica de las restantes medidas de seguridad.

El Oficial COMSEC (INFOSEC) tiene a su cargo las siguientes obligaciones para asegurar el funcionamiento seguro, exacto y eficaz en sus instalaciones:

- a.** Trazar los procedimientos operativos normales que especifiquen la manera en que los mensajes deben ser cursados y procesados a través del Centro de Cifra y definir otros varios procedimientos que pudieran ser de aplicación.
- b.** Asegurarse de que todo el material clasificado y Material de Cifra son debidamente manipulados y protegidos.
- c.** Asegurarse de que todo el equipo de cifra se mantiene en las debidas condiciones de funcionamiento.
- d.** Asegurarse que las violaciones de la seguridad tanto física como de cifra son debidamente informadas.
- e.** Adoptar precauciones para limitar el acceso a los mensajes clasificados como SECRETO (así como al Material de Claves empleado para tal tráfico) dentro de los centros de cifra, a aquellas personas autorizadas para el acceso a dicho grado.
- f.** Preparar las instrucciones de funcionamiento para la destrucción rutinaria de material de cifra.
- g.** Asegurarse de que el personal está entrenado en lo que se refiera a sus obligaciones en relación con el Plan de Emergencia y cerciorarse de que los suministros y equipo necesarios están disponibles para dar cumplimiento al plan.
- h.** Informar sobre los requisitos para redactar los mensajes, así como de los que deben cumplirse cuando los mensajes se desclasifican; solicitar a los que preparan los borradores que introduzcan las modificaciones pertinentes en la clasificación de los mensajes o en su prioridad, según proceda.
- i.** Asegurarse de que el personal se encuentra presente en el Centro de Cifra durante todo su tiempo de operación, debiendo dicho personal estar cualificado para cumplir las instrucciones precedentes.
- j.** Facilitar y supervisar la instrucción de todo el personal relacionado con el Material de Cifra; cerciorarse de que todos están familiarizados con las instrucciones aplicables a los sistemas de cifra empleados en el centro de cifra.
- k.** Poner en conocimiento del Mando todos los mensajes pertinentes (incluyendo los servicios de cifra) en su cuartel general, cuando una autoridad superior haya declarado el comprometimiento de un sistema de cifra particular y ordene una revisión de los mensajes cifrados en ese sistema.

RESPONSABILIDADES DEL USUARIO DEL MATERIAL DE CIFRA

El éxito o el fracaso de la seguridad que aporta el empleo del Material de Cifra descansa en el usuario del mismo. Deberá tener siempre presente que el Material de Cifra (equipos, soportes de claves, registros de consumo de claves, y documentos técnicos relativos a su manejo) forma parte esencial de los medios de Seguridad de los Sistemas de Información y Comunicaciones.

Toda la seguridad y la eficacia proporcionada por la excelencia del equipo y del material, por el cuidadoso control y tratamiento dispensado por la Autoridad competente y los Criptocustodios hasta llegar al usuario, quedarán anulados si éste no tiene cuidado o no sigue los procedimientos establecidos para su empleo, protección y destrucción en caso necesario.

Cualquier usuario de Material de Cifra es directamente responsable de su protección mientras lo tiene; garantizará que la persona a la cual entrega dicho material está autorizada para recibirlo y será responsable de cumplir en todo momento la normativa de seguridad, así como de informar a sus superiores, y al Criptocustodio respectivo, de las circunstancias, sucesos, actos intencionados, y errores de operación que pudieran llevar a la revelación de la información o del material clasificados a personas no autorizadas.

ACCESO DEL PERSONAL A MATERIAL DE CIFRA - AUTORIZACIONES

SELECCIÓN E IDONEIDAD DEL PERSONAL

El Material de Cifra y la información criptológica de carácter sensible siempre ha sido un objetivo de la inteligencia enemiga, y existen numerosas pruebas demostrando que las personas con acceso a dicho material son los principales objetivos de ataque. Por tanto, es importante prestar especial atención a la selección del personal para realizar funciones donde se requiera autorización criptológica.

Se debe prestar la debida atención a los posibles defectos del carácter no detectados por los procedimientos de habilitación de seguridad. Puesto que el oficial al mando tiene la responsabilidad última de la seguridad, a continuación se resume en líneas generales las normas mínimas aceptables de **habilitación de seguridad del personal**, necesarias para las personas que necesiten tener acceso al Material de Cifra.

HABILITACIÓN DE SEGURIDAD DEL PERSONAL

El principio de ‘Necesidad de Conocer’

Es consustancial a la noción de seguridad que la divulgación de la Información Clasificada no sea más amplia de lo necesario para el eficaz desempeño del trabajo.

El acceso a la información no sólo debe limitarse a las personas con adecuada Habilitación de Seguridad, sino que de entre estas debe restringirse a las que justifiquen ‘necesidad de conocer’ para el eficaz desempeño sus funciones. Ninguna persona en virtud de

su graduación o cargo, nombramiento, o Habilitación de Seguridad, tiene derecho de acceso a la Información Clasificada, salvo que se le determine una válida necesidad de conocer.

La necesidad de conocer se basa en tres principios fundamentales:

- a. El conocimiento sobre los sistemas cifrados estará limitado a los que estén autorizados a tener tal conocimiento. No podrá revelarse información relativa a tales sistemas cifrados a ciudadanos o autoridades de una nación que no estén autorizados para conocerla.
- b. Aquellos individuos autorizados para conocer o manejar los Criptosistemas, no deberán nunca divulgar información relativa a la Seguridad Criptológica a cualquier otra persona que no esté autorizada para recibir tal conocimiento. Esta prohibición permanecerá en vigor aun cuando las personas autorizadas dejen de desempeñar trabajo de cifra o de tener acceso al Material de Cifra.
- c. Un principio fundamental de seguridad es que la diseminación de Información Clasificada no será nunca más extensa de la necesaria para el desempeño eficaz de la misión. El acceso debe quedar reducido a las personas que posean Habilitación Personal de Seguridad de grado apropiado a la información de que se trate y que tengan una "necesidad de conocer" justificada para llevar a cabo sus obligaciones. Nadie tendrá derecho, por el sólo hecho de su categoría, nombramiento, cargo o acreditación de seguridad, para lograr acceso a la Información Clasificada, a menos que esté establecida una necesidad de conocer válida.

Habilitación de Seguridad

La Autoridad Delegada para la Seguridad de la Información Clasificada (ANS-D) es responsable de conceder Habilitación Personal de Seguridad (HPS) a los nacionales españoles antes de autorizarles el acceso a la Información Clasificada como SECRETO, RESERVADO o CONFIDENCIAL, o sus equivalentes de otras Organizaciones o Países.

Las personas destinadas en puestos donde se maneje Información Clasificada necesitarán una HPS que les será proporcionada con un certificado actualizado, declarando la máxima clasificación de información a la cual pueden acceder. Las Normas de Seguridad para la protección de la Información Clasificada, publicadas por la ANS-D, establecen los procedimientos de habilitación hasta grado "SECRETO o equivalente" inclusive.

AUTORIZACIÓN CRIPTOLÓGICA

El principio de "necesidad de conocer" se refuerza con la utilización y aplicación de una marca de tratamiento especial **CRIPTO**, adicional a la correspondiente clasificación de seguridad, para indicar que el acceso se limita a las personas específicamente autorizadas para conocer información relativa a esa especialidad.

Por tanto, las personas que en el curso normal de sus funciones necesitan acceder a equipos de cifra y soportes de claves, o a documentos criptológicos de naturaleza sensible, que lleven esta marca CRIPTO deben tener el correspondiente certificado de HPS y deben estar específicamente autorizadas por el oficial/cargo al mando, responsable de garantizar que esas

personas son de su confianza y de probada competencia a la hora de proteger y manejar el Material de Cifra asignado. En esto consiste la "**autorización criptológica**".

Los elementos esenciales para obtener una autorización criptológica son:

- a. Estar en posesión de un certificado actualizado con la adecuada habilitación de seguridad correspondiente a la clasificación de información para la cual se requiere acceso regular y constante.
- b. Haber recibido instrucción sobre la amenaza contra el Material de Cifra y estar completamente familiarizados con las medidas protectoras necesarias para protegerlo. Se registrará por escrito, en la parte del Certificado de Instrucción de Seguridad del formulario de HPS, correspondiente a instrucción CRIPTO. Este documento es parte fundamental de dicha instrucción, como se indicaba en la introducción.
- c. Cuando por alguna razón una persona deje de trabajar en funciones que necesiten una autorización criptológica recibirá otra sesión de información y firmará un Certificado de Cese de Compromiso, por el cual se compromete a no revelar información criptológica a personas no autorizadas.
- d. Cuando una persona deje de estar desempeñando funciones criptológicas debido a razones disciplinarias o de seguridad, se presentará un informe de las circunstancias a través de los canales adecuados.

ACCESO AL MATERIAL DE CIFRA

El personal debe ser instruido sobre la amenaza al Material de Cifra y estar versado en las medidas de protección pertinentes.

Los usuarios que vayan a tener acceso regular a material e información marcados "**CRIPTO**", necesitan una autorización formal CRIPTO. Esto debe aplicarse de forma especialmente estricta a los usuarios que tengan un acceso regular al Material de Cifra clasificado como "**RESERVADO** o equivalente" o superior (**Alto Nivel**).

Las personas que trabajen con Material de Cifra requerirán instrucción, enseñanza, práctica y ejercicio, tanto orales como por escrito. Es menos probable que se produzcan negligencias si todo el personal de cifra es consciente de la importancia de la seguridad y de las razones por las que se espera el cumplimiento de las normas establecidas

Se requiere la adecuada Habilitación de Seguridad y Autorización Criptológica (Instrucción CRIPTO) para todo el personal que en el normal ejercicio de sus funciones deba tener:

- a. Necesidad de acceso de forma regular al Material de Cifra de Alto Nivel y a la información marcada como CRIPTO (Material de Claves clasificado "**RESERVADO** o equivalente" o superior).
- b. El Mando puede autorizar el acceso puntual y controlado, en situaciones operativas, al personal debidamente habilitado, pero sin Autorización Criptológica, a:

- Resúmenes de material de claves.
- Sistemas de libretas de un único uso, señales de llamada, sistemas de cintas de claves de un solo uso y criptosistemas de Bajo Nivel.

ACCESO A CRIPTOSISTEMAS DE BAJO NIVEL

En casos de necesidad operativa, los oficiales al mando pueden dejar de lado el requisito de la habilitación de seguridad para las personas que vayan a utilizar criptosistemas de Bajo Nivel con una clasificación no superior a “CONFIDENCIAL o equivalente”.

Cuando se extinga la necesidad, el criptosistema deberá operar con personal debidamente habilitado.

PROTECCIÓN DE INSTALACIONES FIJAS

Todas las instalaciones fijas en que se maneje Material de Cifra cumplirán con unos requisitos mínimos de construcción, a los cuales se deberían añadir medidas adicionales cuando sea posible. Unos niveles mínimos nunca deberían ser el objetivo de ningún Oficial COMSEC (INFOSEC) o Criptocustodio meticoloso.

Las medidas de protección de las instalaciones criptológicas fijas deben estar en consonancia con sus vulnerabilidades ante amenazas reales, tanto de infiltración abierta como encubierta. Aunque sería inabarcable relacionar las configuraciones de protección contra todas las posibles amenazas, se aconseja:

- a. Disponer todas las instalaciones criptológicas en el mismo lugar. En las instalaciones en las que las funciones criptológicas y comunicaciones se llevan a cabo en el mismo área, se puede declarar todo el área como instalación criptológica, utilizándose en tal caso una puerta única para acceder al recinto.
- b. Para evitar la penetración no autorizada y para mostrar las pruebas de un intento de la misma, las instalaciones criptológicas fijas se deben construir con materiales sólidos y resistentes. Deben proporcionar la atenuación adecuada de los sonidos internos que podrían divulgar la Información Clasificada a través de las paredes, las puertas, las ventanas, los techos, los agujeros y conductos de la ventilación. La máxima seguridad física se alcanza cuando se utilizan construcciones del tipo bóveda. Estas construcciones se emplearán para los centros de distribución de claves y para otras instalaciones en las que las autoridades responsables consideran aconsejable el máximo de seguridad.
- c. Como mínimo la construcción, o la modificación, de un área que contenga una instalación criptológica fija se ajustará al requisito siguiente: las paredes se construirán desde el verdadero suelo al verdadero techo. Cuando se utilicen falsos techos podrá ser necesario utilizar protecciones adicionales para resistir la entrada no autorizada (por ejemplo, la instalación de un sistema de detección de intrusiones encima del falso techo).

- d. Proponer a la Autoridad competente la necesidad de establecimiento de una Zona de Acceso Restringido configurada como Área CLASE I para el recinto donde se ubique el material a cargo de la Cuenta de Cifra.

ZONAS DE ACCESO RESTRINGIDO

Las áreas en las cuales se almacena Material de Cifra deben ser declaradas como Zonas de Acceso Restringido, configuradas como Áreas CLASE I ó CLASE II, que se definen de acuerdo a las siguientes características:

a. ÁREA CLASE I:

- Perímetro claramente definido y protegido a través del cual se controle toda entrada y salida.
- Un Sistema de Control de Acceso que admita sólo a aquellas personas adecuadamente habilitados y especialmente autorizados a entrar en el Área.
- Especificación del grado de clasificación y categoría del Material de Cifra allí almacenado, es decir, de la información a la que da acceso la entrada en la Zona.

b. ÁREA CLASE II:

- Perímetro claramente definido y protegido a través del cual se controle toda entrada y salida.
- Un Sistema de Control de Acceso que admita sólo a aquellas personas adecuadamente habilitados y autorización para entrar en la Zona. Para todos los demás, se establecerán sistemas de escolta o controles equivalentes que eviten su acceso a Información Clasificada.

La entrada al Área Clase I implica el acceso a Material de Cifra clasificado existente en el recinto, por lo que conviene recordar que solamente personal habilitado y especialmente autorizado puede ser admitido. Cuando personal no autorizado para acceder a ese Material de Cifra clasificado deba entrar de forma inexcusable en un Área Clase I, además de ser escoltado, el Material de Cifra quedará oculto y fuera de su alcance.

La entrada al Área Clase II no implica el acceso al Material de Cifra existente en el recinto, por lo que conviene recordar que, además de admitir personal habilitado y especialmente autorizado, puede admitir visitas escoltadas.

La seguridad de las Áreas Clase I y Clase II se incluirán en un entorno que habrá de contar con una serie de medidas de protección físicas, electrónicas y de personal que constituirán un Perímetro de Protección Global contra el espionaje, penetraciones desde el exterior y filtraciones desde el interior.

Dichas medidas de Protección Global deberán recogerse y describirse en el Plan de Protección, requeridos para el establecimiento y acreditación de la Zona de Acceso Restringido en las que se almacene o maneje Material de Cifra.

Dentro del Entorno Global, el Material de Cifra deberá ocupar locales que cuenten con medidas de protección física, electrónicas y de personal apropiadas. Cada Entorno Local dispondrá de un perímetro definido, control de acceso al perímetro, detección de intrusiones fuera de la jornada laboral y mobiliario de seguridad apropiado para el Material de Cifra.

ALMACENAMIENTO DE MATERIAL DE CIFRA

Cuando el Material de Cifra clasificado está siendo manejado de forma continua por personas debidamente habilitadas y autorizadas, o estas tienen posesión física del mismo, se presupone que está adecuadamente protegido, siempre que se cumplan a los procedimientos establecidos.

La noción de ‘almacenamiento’ significa el uso de contenedores de seguridad, cámaras acorazadas, alarmas, guardias, etc., para proteger la información criptológica clasificada durante las horas fuera de trabajo, o cuando no está bajo el control directo y continuo de personal autorizado y debidamente acreditado.

El Material de Claves de Alto Nivel será almacenado de acuerdo con la protección otorgada a los materiales con grado de “SECRETO o equivalente”. La sala en la que están almacenadas será una ‘instalación criptológica’, que en el ámbito de España se denomina Cuenta de Cifra.

Los requisitos de seguridad de la instalación se regirán por la normativa de Seguridad Física que le sea de aplicación, y en su defecto, por las Normas de Seguridad de la ANS-D española. Contará con un Plan de Protección aprobado, y la Zona estará acreditada por la Autoridad competente.

En todas las instalaciones que contienen Material de Clave de Alto Nivel los contenedores utilizados para albergar material de alto nivel estarán cerrados con llave siempre que el material de clave no esté siendo utilizado. En las instalaciones operativas de 24 horas, el contenedor podrá ser cerrado con una cerradura de llave en vez de una cerradura de combinación. Podrían ser necesarias dos cerraduras para mantener una zona "con dos personas", (no-lone), en aquellas instalaciones en las cuales al menos dos personas no están presentes continuamente. Sólo una de las llaves será utilizada y estará en posesión del supervisor del turno. La llave pasará de turno a turno cuando los materiales sean inventariados y firmados por el supervisor de turno entrante. Una segunda copia de la llave se guardará en un sobre en el contenedor maestro del Criptocustodio para su uso si la llave se pierde o se rompe.

ZONA ‘ATENDIDA’ (NO-LONE)

Una actividad de distribución criptológica se define como aquella cuyo papel principal es la distribución del futuro Material de Cifra a Cuentas de Cifra subordinadas.

Todas las actividades de distribución criptológica deben mantener el Material de Claves en una zona "atendida" (no-lone). Una zona "atendida" significa la adopción de una serie de procedimientos que impidan el acceso de una persona sola al futuro Material de Claves. Esto no excluye a personas trabajando en otras actividades dentro del mismo área.

En el caso de otros poseedores de claves, los procedimientos de zona "atendida" deben aplicarse sólo si se da una o más de las siguientes condiciones:

- a. Una máquina reproductora de claves está situada en las instalaciones criptológicas, o bien en el caso de que un contenedor de seguridad constituya la instalación criptológica aprobada, en la misma sala.
- b. Los responsables de Cuentas de Cifra, o usuarios, tienen futuro Material de Claves. Señalar, en tal caso, que sólo las ediciones futuras de Material de Claves deben estar protegidas en una zona "atendida". Esto podría conseguirse almacenando el futuro Material de Claves en un contenedor de seguridad independiente con dos cerraduras o en una caja sellada metida en un contenedor oficialmente aprobado. La caja sólo será abierta/cerrada cuando haya al menos dos personas presentes. Esto quedará reflejado en una hoja de inventario adjunta firmada al menos por dos personas. Además, la propia caja debe estar sellada y llevar en el sello las mismas firmas que las del inventario.
- c. Si así lo ordena la Autoridad competente. En tal caso, esta orden debe darse por escrito y razonar por qué se solicita una zona "atendida", por ejemplo, debido a una contabilidad no satisfactoria, aumento de las amenazas o cualquier otra condición específica.

No se concederá ninguna exención de los requisitos de zona "atendida" contemplados en este apartado.

A todos los poseedores de claves se les aconseja utilizar procedimientos de zona "atendida" en todo momento incluyendo aquellos casos en los cuales no se exige.

ALMACENAMIENTO DE EQUIPOS DE CIFRA Y ACCESORIOS

Cuando no están instalados en una configuración operativa, los componentes del equipo criptológico sin clave que no sean ECC, deben almacenarse de la misma manera que cualquier otro material de la misma clasificación.

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, como forma de asegurar su correcta protección.

El equipo sin clasificación (ECC) debe ser almacenado de forma tal que sea suficiente para impedir toda oportunidad razonable de robo, sabotaje, manipulación, o acceso no autorizado. El equipo criptológico y el dispositivo de almacenaje de clave serán almacenados una vez se les haya sido retirada la clave.

ALMACENAMIENTO A BORDO Y EN VEHÍCULOS

Cuando esté instalado en una configuración operativa, por ejemplo a bordo de un buque, un avión, vehículo, edificio, etc., el equipo criptológico sin clave, aun cuando no sea específicamente un ECC, podrá quedarse sin vigilancia siempre que esté protegido hasta un punto en el cual, a juicio del mando, sea suficiente para evitar toda oportunidad razonable de robo, sabotaje, manipulación o acceso no autorizado.

El equipo criptológico no debe ser retirado de vehículos para cumplir un requisito de almacenaje de seguridad. La retirada frecuente de equipo criptológico y su posterior reinstalación aumenta el mantenimiento del equipo y reduce su disponibilidad operativa. Básicamente la misma protección ofrecida por los vehículos es suficiente para el equipo criptológico sin clave instalado en este tipo de instalaciones móviles. Estos factores deben ser considerados por el Mando en su decisión, relativa a los requisitos aceptables de seguridad y los métodos para conseguirlos.

El equipo criptológico con clave incorporada debe, además de lo descrito anteriormente, estar protegido hasta el punto necesario para impedir su uso no autorizado o la extracción no autorizada de sus variables de clave.

CAJAS DE SEGURIDAD Y COMBINACIONES

Restricciones al uso de las Cajas de Seguridad

Se prohíbe expresamente almacenar en cajas de seguridad, armarios de archivo u otros contenedores utilizados para el almacenaje de Material de Cifra, los artículos que son invariablemente objetivo de los ladrones, por ejemplo: dinero, joyas, metales preciosos, armas, drogas, etc.

Combinaciones de las cerraduras

Las combinaciones de las cerraduras utilizadas para proteger la información criptológica clasificada en zonas o contenedores de almacenaje, serán protegidas, modificadas y registradas de acuerdo con la normativa de la Autoridad competente.

Los discos de las cerraduras de combinación deberían estar cubiertos de tal forma que las operaciones se puedan hacer sin dejar huellas dactilares en el disco o botón. En caso de no contar con la cubierta, el disco se limpiará todos los días al finalizar el trabajo. Las combinaciones serán difundidas al mínimo posible de personal autorizado que cumpla los requisitos operativos establecidos por la Autoridad competente.

Las combinaciones están preparadas de acuerdo con lo establecido por la Autoridad competente. Serán almacenadas de acuerdo con su clasificación en un lugar seguro que permita la entrada autorizada en caso de emergencia.

INSTALACIONES MÓVILES/TRANSPORTABLES PARA ALMACENAMIENTO DE EQUIPOS DE CIFRA Y ACCESORIOS

Las protecciones de las que trata este apartado están concebidas principalmente para las instalaciones de Sistemas de Información y Comunicaciones y Cuentas de Cifra, transportables y móviles, pero también se pueden aplicar a cualquier otra instalación transportable y móvil que contenga Material de Cifra clasificado (por ejemplo, instalaciones de mantenimiento criptológico transportable o un centro de distribución de claves transportable o móvil). Salvo que se haga referencia a tipos específicos de instalaciones, estas normas se aplican por igual a todas las instalaciones con Material de Cifra, transportables y móviles.

Las instalaciones con Material de Cifra, transportables y móviles, se pueden situar dondequiera que las necesidades operativas así lo dicten.

No se establecen requisitos de construcción específicos para las mismas, debido a los distintos requisitos operativos que estas instalaciones deben cumplir. Sin embargo, se deben construir de tal forma que se impida el acceso no autorizado a las mismas o se facilite la detección de dicho acceso, en caso de producirse.

Las instalaciones transportables o móviles deberán disponer de un Plan de Protección básico que determine de forma precisa las medidas de seguridad a establecer en los despliegues operativos que se realicen, siendo el Mando responsable de su adaptación a cada situación operativa presente.

Aprobación, inspección y prueba de las instalaciones transportables y móviles

Generalmente no es necesaria la aprobación de las instalaciones transportables y móviles. El único requisito de inspección allí solicitado es la comprobación diaria de seguridad.

Sin embargo, si una instalación transportable o móvil continúa operativa en un lugar fijo durante un período de seis (6) meses o más, se debe considerar como una instalación fija y se aplicarán los requisitos de las aprobaciones, inspecciones y pruebas de las instalaciones descritos para éstas.

Almacenamiento del Material de Cifra en instalaciones transportables y móviles

El Material de Cifra se almacenará en instalaciones transportables y móviles de acuerdo con los requisitos de la Autoridad competente, con los requisitos complementarios siguientes:

- a.** Las cajas de seguridad deben estar firmemente unidas a la instalación.
- b.** Las tenencias de Material de Cifra se limitarán a las que sean necesarias operativamente para desempeñar los requisitos de la misión. Normalmente, no se debe guardar más de una edición del Material de Clave.

- c. No se llevarán en las instalaciones transportables y móviles los manuales completos de mantenimiento (nivel de depósito).

PROTECCIÓN DE LAS INSTALACIONES MÓVILES DESATENDIDAS

Cuando las instalaciones con Material de Cifra, transportables y móviles, deban quedar desatendidas durante un tiempo, normalmente se retirarán el Material de Clave y las publicaciones clasificadas, se cerrarán las instalaciones y se protegerán contra el acceso no autorizado. Debido a las distintas estructuras de estas instalaciones (por ejemplo, furgonetas, aviones, y vehículos abiertos), no se pueden fijar unos criterios normalizados para su protección.

En general, si las instalaciones se encuentran dentro de una estructura sólida (por ejemplo, una furgoneta o contenedor de equipos), todos los puntos de acceso distintos de la puerta de entrada se cerrarán desde el interior de la instalación móvil y la puerta de entrada se protegerá con una cerradura aprobada. Cuando esto no sea factible (por ejemplo, en un vehículo abierto o en un avión), se utilizará una barra de cierre aprobada u otro dispositivo de cierre para evitar la supresión o la manipulación del equipo de cifra. Además, las instalaciones de Material de Cifra transportables y móviles desatendidas se protegerán en todo momento de acuerdo con lo siguiente:

- a. Cuando las instalaciones contienen Material de Claves o Equipo de Cifra con claves, se emplearán guardias debidamente habilitados. El empleo de guardias armados es responsabilidad del Mando, a requerimiento del Responsable de Seguridad. Para instalaciones en territorio nacional controlado es suficiente con establecer rondas de seguridad frecuentes, siempre que se haya evaluado el riesgo de asumir esta decisión.
- b. Cuando las instalaciones no contengan Material de Clave y sólo contengan Equipo de Cifra sin claves, no será necesario que los guardias estén habilitados. Las rondas podrán ser menos frecuentes, pero nunca dejar de existir.

PÉRDIDA O SOSPECHA DE COMPROMETIMIENTO

Se produce un comprometimiento físico cuando el Material de Cifra es, deliberada o accidentalmente, puesto a disposición de personas no autorizadas por pérdida, robo, captura, espionaje, recuperación, deserción de personas, observación, fotografía o cualquier otro medio. Toda sospecha de comprometimiento físico de Material de Cifra debe ser informada de inmediato al Oficial COMSEC (INFOSEC) o al Criptocustodio, los cuáles, a su vez, lo notificarán al Mando, presentando un informe de sospecha de comprometimiento.

Es esencial que cualquier sospecha de comprometimiento sea informada inmediatamente, de forma que pueda tomarse una rápida acción para limitar la pérdida de seguridad producida; por ejemplo, el Material de Claves puede ser anulado y sustituido, revisado su tráfico y tomarse medidas para limitar el daño.

Cuando falte un artículo o documento, existe la posibilidad de que haya sido accidentalmente destruido con otros artículos o documentos cuya destrucción hubiera sido autorizada. Sin embargo, a menos que tal destrucción pueda ser confirmada, más allá de toda

posible duda, deberá informarse como sospechoso de comprometimiento, cualquier artículo que no pueda ser contabilizado satisfactoriamente, para poder tomarse la acción oportuna con la mayor brevedad.

TRANSPORTE DE MATERIAL DE CIFRA

MEDIOS DE TRANSPORTE

Son de aplicación los criterios generales para el Transporte de Información Clasificada del mismo grado de clasificación, aunque se extremarán las medidas de protección aplicadas.

El envío de material y correspondencia de cifra marcados CRIPTO se hará a través de un correo oficialmente nombrado como tal por la autoridad competente o por otros medios aprobados por la autoridad, mando o servicio nacionales. Cuando se empleen otros medios de transporte aprobados, es responsabilidad del organismo remitente asegurarse de lo siguiente:

- a. Que los medios de transporte empleados se encuentran bajo control total de Naciones aliadas o con Acuerdo de Seguridad vigente con España.
- b. Que el material es abierto solamente por personas autorizadas para el acceso a la información de cifra.
- c. Que el material no es en ningún momento objeto de inspección (incluyendo la de Aduanas) o censura.
- d. Que existen medidas seguras para la entrega, recibo y almacenaje. Cuando exista trasbordo, se adoptarán cuidados especiales para asegurarse de que se emplean canales seguros y que existen instalaciones de almacenaje seguras en cada uno de los puntos de trasbordo.

A ser posible, no se asignarán otras misiones a los Correos Autorizados nombrados oficialmente durante un transporte. Si se les confirieran otras obligaciones, éstas deberán ser secundarias y no interferirán con sus deberes y responsabilidades como Correos Autorizados.

Los organismos expedidores instruirán completamente a sus Correos Autorizados sobre la necesidad y los medios de proteger continuamente el material que se les confía. En estas instrucciones se incluirán los métodos apropiados para destruir el material en caso de una emergencia. Por ejemplo, si fuera inminente la captura o comprometimiento no autorizado del material y esta circunstancia no pudiera ser evitada, si el tiempo y las circunstancias lo permiten, el mensajero destruirá el material quemándolo, rompiéndolo hasta hacerlo totalmente irreconocible (sólo en caso de que sea imposible la quema), o, en caso de estar a bordo de un barco, arrojándolo en aguas profundas debidamente lastrado.

Los Correos Autorizados informarán inmediatamente sobre la destrucción o disposición en emergencia a los organismos remitente o destinatario (según resulte más conveniente), por teléfono o enviando un mensaje.

CORREOS AUTORIZADOS

Los Correos Autorizados de Material de Cifra deben ser nombrados específicamente por escrito por la Autoridad competente. Es responsabilidad del funcionario que autorice a los Correos Autorizados que éstos dispongan de la oportuna "acreditación" de seguridad, que sean de la máxima confianza y hayan sido adoctrinados sobre sus responsabilidades en la protección del material que se les confía. Los Correos Autorizados recibirán instrucciones concretas para casos de emergencia, incluyendo la posibilidad de pérdida o comprometimiento del material que transporten.

Cuando transporten Material de Claves, deberán mantener personal y constantemente su custodia.

Cuando transporten Material de Cifra que no sea de claves, los Correos Autorizados son responsables de la seguridad del mismo en todo momento. También podrán almacenar el material en bloque en un contenedor cerrado con llave, siguiendo el procedimiento de hacer las entregas del material más reciente en primer lugar.

Los Correos Autorizados deben asegurarse que se presta al material la máxima protección posible durante el tránsito, no dejándolo desatendido en ningún momento en muelles de carga, andenes de estaciones, consignas zonas de almacenaje de carga, depósitos de equipajes, autobuses, trenes o aviones.

Los Correos Autorizados deberán asegurarse de que todas las inspecciones se realizan en su presencia y solamente por personal autorizado para ello. Se permite el examen externo y el empleo de los equipos normales de Rayos X empleados en los aeropuertos para revisión del equipo y del Material de Claves empaquetados.

REQUISITOS DE SEGURIDAD DURANTE EL TRANSPORTE

Con el fin de reducir las posibilidades de comprometimiento físico y disminuir los efectos de la pérdida o comprometimiento de un transporte, todos los envíos de Material de Cifra, en condiciones normales, se harán de conformidad con los siguientes requisitos mínimos de seguridad:

- a. El Equipo de Cifra no será enviado con el Material de Claves instalado, a menos que la configuración física del equipo haga imposible la retirada de la clave o su puesta a cero.
- b. Los componentes de un sistema (por ejemplo, equipo de cifra, claves, e instrucciones de funcionamiento) se transportarán por separado y, siempre que sea posible, en diferentes fechas.

RECIBO DE MATERIAL DE CIFRA

A la entrega de Material de Cifra, el Criptocustodio del mismo examinará cuidadosamente el paquete en busca de evidencia de manipulación o exposición de su contenido. Si existiera alguna evidencia, se preparará un informe de posible comprometimiento

o violación. En espera de la acción oportuna por la autoridad de investigación, el envío permanecerá en el mismo estado que cuando se descubrió la evidencia de manipulación y todo manejo del mismo se reducirá al mínimo compatible con la salvaguarda del envío.

Los paquetes recibidos por cualquier persona que no sea el Criptocustodio, serán entregados a éste sin abrir.



ANEXO IV: INSTRUCCIÓN DE SEGURIDAD ATOMAL

Se adjunta un documento separable, y con numeración propia, al objeto de que pueda desglosarse o copiarse como manual de instrucción del personal, separado del presente documento que es para uso exclusivo de los instructores.

	<h1>INSTRUCCIÓN DE SEGURIDAD ATOMAL</h1>	 autoridad nacional de seguridad delegada autoritatea națională de securitate
---	--	--

DEFINICIÓN

Se entiende por información ATOMAL aquella categoría especial de información, suministrada por el Gobierno de los Estados Unidos a otras Naciones Miembros de la OTAN, o bien, información “ATOMIC” del Reino Unido que es suministrada por este Gobierno a otras Naciones Miembros de la OTAN, con objetivos operacionales, de formación o de industria de armamentos.

Esta información es relativa a armas atómicas e información de carácter atómico, y se manejará al amparo y conforme al *Acuerdo entre las Partes del Tratado del Atlántico Norte para la Cooperación sobre Información Atómica*, de 18 de junio de 1964, recogido en el documento **C-M(64)39**, y complementado mediante los Acuerdos Administrativos recogidos en el documento **C-M(68)41-REV7** (o versión posterior que pueda editarse).

De ambos documentos deberá hacer una lectura detallada el solicitante de la especialidad, como parte de su instrucción de seguridad ATOMAL, especialmente si va a ocupar puestos de responsabilidad en dicha materia.

Todos los documentos ATOMAL son Información Clasificada controlada, es decir, debe circular sólo por los órganos de registro, y llevarse registro de sus movimientos y existencia. Asimismo, los documentos ATOMAL con grado COSMIC TOP SECRET y NATO SECRET, y aquellos NATO CONFIDENTIAL sobre los que se hayan impuesto limitaciones especiales, se consideran documentos “imputables”, por lo que se debe llevar control de los accesos que se producen a los mismos, mediante el uso de la Ficha de Control y Acceso a Información Clasificada, que siempre acompañará a estos documentos.

ACCESO Y MANEJO DE LA INFORMACIÓN ATOMAL.

CONDICIONES DE ACCESO

Una persona sólo podrá ser autorizada a acceder a la Información Clasificada de grado NATO CONFIDENTIAL o superior, y marcada como ATOMAL, cuando se hayan cumplido los siguientes requisitos:

- le haya sido concedida una **Habilitación Personal de Seguridad** adecuada no sólo del grado de la Información Clasificada, sino también con la especialidad ATOMAL,
- se haya determinado su “necesidad de conocer” información ATOMAL y
- haya recibido la instrucción de seguridad preceptiva .

Nadie podrá tener acceso a Información Clasificada como ATOMAL únicamente en virtud de su rango, posición o Habilitación Personal de Seguridad.

El acceso a una determinada información ATOMAL estará determinado por el grado de habilitación del usuario y por su necesidad de conocer dicha información. Sobre esta base, el Registro Central ATOMAL, Subregistros y Puntos de Control ATOMAL mantendrán un listado actualizado de los usuarios que tengan acceso a información ATOMAL, especificando aquellos que tienen acceso autorizado a información ATOMAL sujeta a Limitaciones Especiales.

Cuando cese la necesidad de acceso a la información ATOMAL, el Órgano de Control mantendrá una entrevista con el interesado al objeto de señalar la continuación de las responsabilidades de protección de la información ATOMAL a la que tuvo acceso. Tras la instrucción el interesado firmará un “**Certificado de Cese de Compromiso**”

INFRAESTRUCTURA DE PROTECCIÓN DE LA INFORMACIÓN ATOMAL

El control de la información ATOMAL en España se lleva a cabo del mismo modo que el resto de la Información Clasificada OTAN, es decir, a través de un Registro Central, Subregistros Principales y Secundarios y Puntos de Control, todos ellos autorizados a ATOMAL. Cada Órgano de Control ATOMAL deberá nombrar un **Oficial de Control ATOMAL**, que será el responsable del control y custodia de toda la documentación ATOMAL que tiene asignada dicho Órgano de Control.

Como norma general la información ATOMAL deberá entrar o salir de España a través del Registro Central ATOMAL, siendo éste responsable de su control y canalización a través de la Red.

La documentación clasificada de grado COSMIC TOP SECRET ATOMAL (CTS-A) circulará siempre a través del Registro Central.

La documentación clasificada de grado NATO SECRET ATOMAL (NS-A) y NATO CONFIDENTIAL ATOMAL (NC-A) podrá circular entre Subregistros Principales con autorización ATOMAL directamente, informando de ello al Registro Central. También podrá circular entre Puntos de Control dependientes de un mismo Subregistro Principal, informando a su Órgano de Control de nivel superior de los movimientos producidos.

Si, excepcionalmente, un usuario recibiera información ATOMAL por alguna otra vía distinta a las anteriormente descritas (Sistema CIS, correo OTAN, reunión OTAN, etc.), éste la entregará al Órgano de Control ATOMAL del que dependa el cual, a través de su Subregistro Principal ATOMAL, lo hará llegar al Registro Central ATOMAL para el correspondiente registro y control.

CUSTODIA Y MANEJO DE LA INFORMACIÓN ATOMAL

La información ATOMAL se almacenará de forma separada al resto de los documentos clasificados de la Alianza y dentro de una Zona de Acceso Restringido establecida como Área Clase I o Área Clase II. Esta separación no tiene por qué significar una Zona de Acceso

Restringido específica, salvo que por criterios de segregación de accesos se decida que sean personas diferentes las responsables de cada tipo de información. Lo normal es que sea suficiente con el uso de contenedores separados, que pueden estar incluso dentro del mismo mueble o caja de seguridad.

Como norma general, la información ATOMAL no podrá permanecer fuera del Subregistro o Punto de Control al margen de la jornada laboral del usuario, salvo autorización expresa del Oficial de Control ATOMAL.

Las copias, traducciones y extractos de documentos ATOMAL serán contabilizados en la misma forma que el documento original, se les asignará un número de documento, fecha, y tendrán su mismo grado de clasificación.

Los documentos CTS-A no podrán ser reproducidos por ningún Órgano de Control. En caso de necesitarse copias extras deberán ser solicitadas a la nación que originó el documento a través del Registro Central ATOMAL.

Los Oficiales de Control ATOMAL de los Subregistros Principales ATOMAL podrán autorizar las copias, extractos o traducciones de documentos NS-A y NC-A.

Los Subregistros Principales ATOMAL comunicarán mensualmente al Registro Central ATOMAL una relación de las copias, extractos y traducciones efectuadas por ellos y por sus Órganos de Control subordinados.

Los documentos ATOMAL sometidos a limitaciones especiales, independientemente del grado de clasificación de los mismos, sólo podrán ser reproducidos con el consentimiento previo del Gobierno de EE.UU.

Los documentos ATOMIC conteniendo información atómica del Reino Unido no podrán ser reproducidos salvo instrucciones específicas del Gobierno del Reino Unido que así lo permita.

La información ATOMAL que ya no sea necesaria a efectos oficiales, incluyendo material sobrante, excedentes o información sustituida por actualización, será destruida de tal forma que se asegure que no pueda ser reconstruida.

MANEJO DE INFORMACIÓN ATOMAL EN SISTEMAS CIS

La información ATOMAL remitida mediante sistemas CIS debe estar cifrada. Se deben tomar medidas para asegurar estos sistemas y que los puntos de transmisión y recepción de la información ATOMAL estén acreditados al máximo grado de la información que se vaya a tramitar.

La información ATOMAL sólo debe ser enviada después de confirmar que el receptor tiene en vigor una HPS de nivel apropiado y con la especialidad ATOMAL, así como la pertinente “necesidad de conocer”.

La información almacenada en carpetas personales o compartidas debe ser protegida mediante una contraseña de acceso.

LIMITACIONES ESPECIALES PARA ACCESO A INFORMACIÓN ATOMAL

Determinada información ATOMAL, especialmente sensible por razones de seguridad, es cedida a la OTAN por EE.UU. bajo Limitaciones Especiales, que serán marcadas en cada documento que sea cedido. Así mismo, contará con una hoja anexa, que permita su correcta identificación y en la que se registrará el personal que haya accedido a dicho documento.

La Lista de Control ATOMAL deberá indicar aquellas personas con HPS ATOMAL y que han sido autorizadas a acceder a información con Limitaciones Especiales.

Los documentos con Limitaciones Especiales no requieren ser almacenados y custodiados separados del resto de la documentación ATOMAL, aunque se prestará especial atención a que sólo las personas autorizadas puedan acceder a dicha documentación durante su custodia, almacenaje, transporte, etc.

COMPROMETIMIENTOS Y BRECHAS DE SEGURIDAD

Una brecha de seguridad es un acto u omisión contrario a la regulaciones de seguridad de la OTAN y que pueda poner en peligro o comprometer información ATOMAL:

El comprometimiento se define como la pérdida de confidencialidad, integridad o disponibilidad, debido a una brecha de seguridad o actividad adversa (tales como espionaje, actos de terrorismo, sabotaje, etc.) de la información ATOMAL.

Cualquier brecha de seguridad en la que se vea involucrada información ATOMAL deberá ser inmediatamente comunicada a la autoridad de seguridad apropiada para que sean investigadas todas las circunstancias que rodean dicha brecha de seguridad para determinar si la información ATOMAL se haya visto comprometida, si se han producido accesos no autorizados a información ATOMAL, así como para aplicar las medidas correctivas y disciplinarias (incluidas las legales) pertinentes.

