
	AUTORIDAD NACIONAL DE SEGURIDAD DELEGADA Oficina Nacional de Seguridad		 ANS-D autoridad nacional de seguridad delegada oficina nacional de seguridad
	ORIENTACIONES PARA EL MANEJO DE INFORMACIÓN CLASIFICADA CON GRADO DE DIFUSIÓN LIMITADA	10.05.2009	

OR-ASIP-04-01.03

**ORIENTACIONES PARA EL MANEJO DE
INFORMACIÓN CLASIFICADA CON
GRADO DE DIFUSIÓN LIMITADA**

ÍNDICE

1.	INTRODUCCIÓN.....	3
2.	OBJETO.....	3
3.	ALCANCE.....	4
4.	ACCESO A LA INFORMACIÓN DIFUSIÓN LIMITADA	4
5.	CESIÓN DE INFORMACIÓN DIFUSIÓN LIMITADA	4
6.	RESPONSABLE DE SEGURIDAD.....	5
7.	SEGURIDAD EN EL PERSONAL	5
8.	SEGURIDAD FÍSICA	6
9.	SEGURIDAD DE LA INFORMACIÓN.....	7
9.1.	GENERALIDADES	7
9.2.	DISTRIBUCIÓN, REPRODUCCIÓN Y DESTRUCCIÓN.	8
9.2.1.	Distribución.....	8
9.2.2.	Reproducción	8
9.2.3.	Destrucción.....	8
9.3.	TRANSMISIÓN.....	9
9.4.	COMPROMETIMIENTO DE LA PROTECCIÓN DE LA INFORMACIÓN CLASIFICADA	9
10.	SEGURIDAD EN LOS SISTEMAS DE INFORMACIÓN Y COMUNICACIONES	10
11.	GLOSARIO	11
	ANEXO I - CERTIFICADO DE INSTRUCCIÓN Y COMPROMISO DE RESERVA...	14

1. INTRODUCCIÓN

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, dado el perjuicio que ello produciría a los intereses y seguridad nacionales. 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.

El sistema de clasificación de seguridad de la información 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.

El originador de la información es quien determina la clasificación de seguridad inicial de la misma, y establece quién ostenta su propiedad. El propietario de la Información Clasificada es el único que puede modificar su grado de clasificación o desclasificarla, a lo largo de su ciclo de vida.

El grado de clasificación de DIFUSION LIMITADA se aplicará a la información cuya revelación no autorizada o utilización indebida pueda ser contraria a los intereses de España. Aunque no suponga una amenaza o perjuicio para la seguridad, su divulgación a personas no autorizadas deberá limitarse.

La Información Clasificada procedente de Organizaciones Internacionales de las que España forma parte, o de Países con los que España ha firmado Acuerdos de Seguridad, se basa en grados de clasificación similares y asimilables a los utilizados en España, según se define en las respectivas Políticas de Seguridad. En este sentido, la Información Clasificada de grado DIFUSIÓN LIMITADA tiene equivalencia con NATO RESTRICTED, RESTREINT UE, ESA RESTRICTED, etc. Todos ellos estarán sometidos a requisitos de protección similares.

En este sentido, se utiliza la expresión Información Clasificada de grado “DIFUSIÓN LIMITADA o equivalente” para referirse a cuestiones que sean de igual aplicación y tengan el mismo tratamiento con independencia del tipo (ámbito de origen) de Información Clasificada a que se vaya a acceder, es decir, que sólo dependan del grado de clasificación de la misma.

2. OBJETO

El objeto de estas Orientaciones es refundir en un único documento y exponer de forma clara y concreta, las normas y prácticas de seguridad mínimas a aplicar por las personas, organismos y entidades, para garantizar una adecuada protección de la Información Clasificada con grado de “DIFUSION LIMITADA o equivalente”.

Las especiales características de la Información Clasificada con este grado, al no requerir de una Habilitación Personal de Seguridad (HPS) y un proceso formal de instrucción de las personas que han de acceder a la misma, aconsejan el hacer un documento específico que defina las pautas para el adecuado tratamiento de dicha información.

No obstante lo anterior, para un tratamiento más en detalle se pueden consultar las *Normas de la Autoridad Nacional para la Protección de la Información Clasificada*, promulgadas por la Autoridad Nacional de Seguridad Delegada española.

3. ALCANCE

Estas Orientaciones son de aplicación a todas las personas que por sus funciones deban acceder a Información Clasificada con el grado de “DIFUSION LIMITADA o equivalente”, y a los Organismos y Entidades en que se maneje.

En adelante se hará uso exclusivamente del término información DIFUSIÓN LIMITADA, para referirse al concepto de Información Clasificada con grado de “DIFUSIÓN LIMITADA o equivalente”, dado que los preceptos y criterios que se expresan son de aplicación general para todos los tipos (ámbitos de origen) de Información Clasificada que se maneje.

4. ACCESO A LA INFORMACIÓN DIFUSIÓN LIMITADA

Por difusión se entenderá la comunicación o distribución de Información Clasificada dentro de un determinado ámbito, departamento, organismo o entidad.

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.

La difusión será controlada por el Responsable de Seguridad del órgano custodio de la información.

5. CESIÓN DE INFORMACIÓN DIFUSIÓN LIMITADA

Se entiende por **Cesión de Información Clasificada** la entrega de dicha información, que está bajo la custodia del que la cede, a un tercero. Por tercero, en este contexto, se entiende un tercer Estado, una Organización Internacional, etc., e incluso una persona representante de los mismos, que tiene la característica fundamental de ser ajeno a quien ostenta la propiedad de dicha información y, por tanto, no está de antemano autorizado a acceder a la misma. No es cesión la distribución o difusión de la información a un órgano o persona, autorizado y sin la consideración de tercero, dentro del propio país u organización que ostenta la propiedad de la misma.

La cesión de Información Clasificada está **expresamente prohibida salvo autorización** por escrito del propietario de dicha información.

La cesión será controlada por el Responsable de Seguridad y se cederá, según el criterio de necesidad de conocer, sólo aquella información DIFUSION LIMITADA sujeta a dicha condición, una vez determinado que existe la autorización expresa para ello y que el órgano receptor cumple los requisitos reglamentarios para hacerse cargo de la misma.

En el ámbito de la Seguridad Industrial, los Contratistas no podrán estar autorizados en ningún caso a la cesión de Información Clasificada con carácter general, siendo precisa la validación caso por caso de la correspondiente Oficina de Programa u Órgano de Contratación, según corresponda.

6. RESPONSABLE DE SEGURIDAD

El organismo o entidad que vaya a manejar información DIFUSIÓN LIMITADA, y que no disponga previamente de un Servicio de Protección de Información Clasificada u Órgano de Control (Subregistro o Punto de Control) competente, deberá designar al menos un **Responsable de Seguridad** para la protección de la Información Clasificada con dicho grado, al que se encomendarán las siguientes misiones:

- Instruir a todo el personal que vaya a acceder a información DIFUSION LIMITADA sobre las medidas de protección necesarias, así como de las establecidas en el presente documento.
- Investigar las incidencias que hayan podido afectar a dicha información, así como aprobar las medidas tomadas para corregir los daños y evitar su repetición.
- Verificar el cumplimiento de las medidas de seguridad aplicables, resumidas en el presente documento.
- Controlar la relación del personal con acceso a esta información en su organismo o entidad y las correspondientes declaraciones formales de instrucción y de compromiso de reserva, cuando se utilicen (modelo en Anexo I, se explica posteriormente).
- Controlar la Información Clasificada manejada por el organismo o entidad.

Es potestad del responsable de seguridad inspeccionar las instalaciones donde se custodia información DIFUSION LIMITADA, cuando lo considere oportuno, lo que hará con cierta frecuencia.

7. SEGURIDAD EN EL PERSONAL

No se precisa disponer de HPS para acceder a información DIFUSIÓN LIMITADA.

El contenido de la información DIFUSION LIMITADA no debe ser revelado al público, a personal no autorizado o a cualquier otro organismo o entidad fuera de los cauces autorizados.

Las personas con acceso a información DIFUSION LIMITADA deberán contar con los siguientes requisitos:

- Tener la “Necesidad de Conocer”. La información DIFUSION LIMITADA estará a disposición sólo del personal que requiera acceso a dicha información en el

cumplimiento de sus cometidos. Nadie, en virtud de su cargo, categoría en la Administración, o cualquier otra circunstancia similar, contará con derecho a acceder a Información Clasificada. La necesidad de conocer normalmente vendrá determinada por el superior jerárquico del interesado, asesorado por el responsable de seguridad del organismo o entidad.

- Haber sido instruidas en el manejo de dicho tipo de información y ser conscientes de sus responsabilidades en la protección de la misma, conforme a la normativa aplicable, resumida en el presente documento.
- Declarar que comprenden y conocen las responsabilidades penales y disciplinarias en que pudieran incurrir por la divulgación no autorizada de esta clase de informaciones, bien sea voluntariamente o por negligencia, por acción u omisión. En el Anexo I se incluye un modelo de declaración formal de instrucción recibida y compromiso de seguridad adquirido. El responsable de seguridad determinará la necesidad o no de uso de una declaración formal, en función de las posibilidades de instrucción periódica del personal. Para Contratistas y entidades no oficiales, esta declaración tendrá carácter obligatorio.

8. SEGURIDAD FÍSICA

La información DIFUSIÓN LIMITADA sólo se manejará, como mínimo, en Zonas Administrativas de Protección, con las excepciones previstas para las instalaciones no oficiales (por ejemplo Contratistas) y para los transportes de Información Clasificada.

Las **Zonas Administrativas de Protección** son instalaciones con un perímetro claramente definido dentro del cual existe un control de las personas, materiales y vehículos.

Cuando la información se maneje en instalaciones oficiales de la Administración la custodia se podrá realizar en mobiliario de oficina provisto de cerradura con llave.

Si la información es almacenada en instalaciones no oficiales, deberá estar dentro de una **Zona de Acceso Restringido (ZAR)**, que contará con las siguientes medidas:

- Las paredes, techo y suelo, deberán ofrecer el mismo nivel de resistencia, siendo las paredes de ladrillo macizo, como mínimo de medio pie. Las paredes irán desde el verdadero suelo hasta el verdadero techo.
- Cuando los mismos muros de un edificio constituyen, en parte o por completo, el perímetro de seguridad, todas las ventanas y conductos situados en zonas sin vigilancia permanente y a menos de 5,5 metros por encima del nivel del suelo, o a igual distancia de tejados o cornisas accesibles, deberán protegerse con una **reja de seguridad**, constituida por barras de acero soldadas formando cuadro, sujetas firmemente con pernos a la estructura en el interior de la ventana o abertura. Las barras tendrán 25mm. de espesor y estarán espaciadas 150mm. de centro a centro, apoyándose en unas pletinas horizontales de 45 x 6mm., espaciadas 200mm. de centro a centro.
- Las ventanas existentes en los paramentos de una Zona de Acceso Restringido estarán provistas de un sistema de alarma contra apertura, rayado o rotura, salvo que dispongan de reja de seguridad. Los cristales deberán ser opacos o translúcidos, de forma que se impida cualquier visión nítida desde el exterior. En caso de ubicarse en zonas sin vigilancia permanente y a alturas o distancias inferiores a las indicadas

- anteriormente para ventanas en muros del perímetro de seguridad, o en el caso de no disponer de sistemas de alarma adicionales, deberán protegerse con rejas de seguridad.
- Todos los conductos de ventilación deberán protegerse con barras de acero soldadas formando cuadro, sujetas firmemente con pernos a la estructura en el interior de la abertura. Las barras tendrán 25mm. de espesor y estarán espaciadas 150mm. de centro a centro, apoyándose en unas pletinas horizontales de 45 x 6mm, espaciadas 200mm. de centro a centro.
 - La puerta de acceso a la Zona de Acceso Restringido será blindada para interior de Grado 4 según norma europea UNE-EN-1627, de características RF-30 según las normas UNE-EN-13501, provista de una cerradura mecánica de alta seguridad con al menos 5 puntos de cierre al frente. Este mecanismo será obligatoriamente accionado cuando no haya nadie presente en la misma. También dispondrá de un dispositivo que obligue a la puerta a permanecer cerrada cuando no se esté franqueando.
 - La Zona de Acceso Restringido dispondrá de detectores de presencia y/o de movimiento (IDS) como mínimo de doble tecnología, conectados al Centro de Control de Alarmas, que estarán instalados en función de la superficie y configuración, de manera que se cubra la zona en su totalidad, salvo que la instalación esté ocupada por personal presente las 24 horas al día. Estos sistemas dispondrán de dispositivos antisabotaje.
 - En el interior de la Zona de Acceso Restringido se instalará una caja fuerte de al menos Nivel I, conforme a la norma UNE-EN 1143, y cerradura Clase A homologada conforme a la norma UNE-EN-1300, o equivalentes en vigor, donde se custodiarán obligatoriamente las materias clasificadas durante los períodos de tiempo en que no se estén manejando.

Los documentos o materiales, o soportes informáticos, o material provisional no inmediatamente destruido, conteniendo información DIFUSION LIMITADA, no deben quedar desatendidos o ser manejados de modo que permita el acceso no autorizado.

Durante los viajes o transportes los documentos y materiales estarán bajo la custodia permanente del titular y no deben quedar desatendidos en habitaciones de hotel o vehículos, ni ser exhibidos en público.

9. SEGURIDAD DE LA INFORMACIÓN

9.1. Generalidades

Los documentos o materiales, así como anexos, copias, traducciones o extractos de los mismos, con información DIFUSIÓN LIMITADA, serán marcados en forma de sellado, mecanografiado, impreso o escrito, con la marca DIFUSIÓN LIMITADA en negrita y con mayúsculas, en la cabecera y el pie de cada página.

El material o los soportes informáticos, ópticos, acústicos o registros electrónicos que contengan información DIFUSION LIMITADA, serán debidamente marcados, bien sobre el propio material o, de no ser factible, sobre el contenedor que lo albergue, de modo que cualquier destinatario del mismo perciba inequívocamente la presencia de la clasificación.

Para el resto de los casos se deberá consultar la normativa de seguridad correspondiente que le sea de aplicación o, en su defecto, aplicar criterios equivalentes a los aquí establecidos.

9.2. Distribución, Reproducción y Destrucción.

9.2.1. Distribución

La información DIFUSIÓN LIMITADA se manejará en los distintos órganos de recepción, una vez determinado que éstos cumplen los requisitos reglamentarios para hacerse cargo de la misma.

La información será registrada a la entrada y salida de los distintos órganos de recepción, supervisado por parte del Responsable de Seguridad.

La Información Clasificada con grado DIFUSIÓN LIMITADA puede circular entre usuarios, siempre que los destinatarios cumplan las condiciones de acceso (tener necesidad de conocer y haber sido instruido en el manejo de la Información Clasificada), y las de manejo y custodia establecidas para dicho grado, siendo responsabilidad de quien la entrega verificar que se cumplen dichas condiciones por parte del destinatario.

La información DIFUSIÓN LIMITADA distribuida a entidades no oficiales, como por ejemplo empresas contratistas con ocasión de su participación en proyectos o programas clasificados, se registrará por criterios más restrictivos, no estando autorizados los usuarios a distribuir la información de este grado que reciban, la cual deberá circular siempre por los registros autorizados.

No será necesario realizar ni mantener **Actas de Destrucción, ni Hojas de Control de Acceso** de la Información Clasificada con este grado, a menos que sea expresamente requerido por el propietario de la misma.

No será necesario el empleo de **Recibos de Recepción**, a menos que sea requerido por el remitente de la Información Clasificada.

9.2.2. Reproducción

Las copias, extractos y traducciones de información DIFUSIÓN LIMITADA podrán ser realizadas por individuos con acceso autorizado a la información. Estarán sujetos y deberán manejarse con los mismos requisitos de seguridad que los originales.

Los equipos utilizados para la reproducción deberán estar físicamente protegidos para evitar un uso no autorizado respecto a la Información Clasificada (especialmente si tienen dispositivos de memoria o conexión remota).

9.2.3. Destrucción

La información DIFUSIÓN LIMITADA deberá ser físicamente destruida de manera que se imposibilite su reconstrucción total o parcial.

Los borradores, anotaciones, o copias anuladas, con información DIFUSION LIMITADA, deberán destruirse. La información DIFUSION LIMITADA obsoleta o ya no útil, deberá destruirse con la mayor brevedad posible.

Los documentos, materiales y soportes informáticos que contengan información DIFUSION LIMITADA deberán ser revisados periódicamente para determinar su posible destrucción.

Las trituradoras a utilizar deberán realizar un corte máximo de 3 mm. de ancho y 25 mm. de largo. La superficie del material cortado no deberá exceder los 60 mm². Las máquinas dispondrán de capacidad para operar manualmente y su diseño no permitirá almacenar documentación sin destruir. El material triturado debe ser removido para mezclar su contenido, y de esta manera dificultar su posible reconstrucción.

9.3. Transmisión

La información DIFUSION LIMITADA podrá ser enviada a sus destinatarios en sobre sencillo, opaco, sin marca exterior de clasificación, ni indicios de su contenido, mediante:

- Correo certificado, a través del Servicio Estatal de Correos, con origen y destino en ESPAÑA.
- Correo certificado internacional, a través de servicios de correos internacionalmente reconocidos.
- Servicio de Correo Comercial específicamente autorizado.
- Transporte por persona formalmente autorizada, sin Certificado de Correo. No precisa HPS.
- Cualquiera de los métodos aprobado para el transporte de información CONFIDENCIAL o superior.

La información DIFUSION LIMITADA no deberá transmitirse por sistemas de comunicación no autorizados para dicho grado o superior, en especial vía Internet. Será obligatorio el que se utilicen medios de cifra expresamente autorizados por el Centro Criptológico Nacional (CCN) y se someta al sistema de información y comunicaciones a un proceso no formal de acreditación.

9.4. Comprometimiento de la Protección de la Información Clasificada

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

También tendrán la consideración de comprometimiento los ataques contra la integridad o disponibilidad de la Información Clasificada, especialmente en el ámbito de los Sistemas de Información y Comunicaciones.

Todo usuario de Información Clasificada está obligado a informar inmediatamente a su Oficial o Responsable de Seguridad, por el canal adecuado, de cualquier comprometimiento que pueda conocer.

Tras ser informado, el Oficial o Responsable de Seguridad:

- Adoptará de manera inmediata las medidas necesarias en orden a restablecer la seguridad y a prevenir situaciones similares a la sucedida.

- Informará inmediatamente al Jefe del Organismo o Entidad al que pertenece.
- Realizará una investigación preliminar para clarificar los hechos y responsabilidades y valorar en una primera estimación el daño potencial causado. En el menor plazo notificará todo ello, junto con las medidas iniciales adoptadas, a las autoridades apropiadas.

Se informará a la Autoridad competente, a través del Oficial o Responsable de Seguridad, de la pérdida o comprometimiento de información DIFUSIÓN LIMITADA, cuando se cumpla alguno de los siguientes criterios:

- El comprometimiento se ha producido bajo circunstancias inusuales, que pudieran hacer sospechar de una **voluntariedad**.
- Existen indicios o sospechas de **espionaje**.
- Se ha revelado de manera no autorizada información a **medios de comunicación social**.
- Pérdida de medios electromagnéticos, por ejemplo, dispositivos removibles u **ordenadores portátiles**.
- El comprometimiento es originado por personal de una entidad no oficial, ajena a la Administración, por ejemplo de una **empresa contratista**, o se ha producido en sus instalaciones.

10. SEGURIDAD EN LOS SISTEMAS DE INFORMACIÓN Y COMUNICACIONES

Los organismos y entidades en que se vaya a manejar información DIFUSIÓN LIMITADA en sistemas de información y comunicaciones, deberán contar con una mínima estructura de seguridad, responsable de la correcta aplicación de la normativa de seguridad en dichos sistemas.

Para ello, el personal que compone dicha estructura de seguridad debe estar nombrado e instruido para dicha función, tanto en el ámbito técnico, como operacional.

La composición y cometidos de esta estructura queda fuera del alcance de estas Orientaciones, estando regulado en normativa de seguridad específica.

Los sistemas de información y comunicaciones que manejan Información Clasificada con grado de DIFUSION LIMITADA deberán cumplir con los requisitos establecidos en el documento CCN-STIC 301, elaborado por el CCN.

La interconexión de estos sistemas con otros sistemas de menor clasificación o Internet, deberá cumplir los requisitos establecidos en el documento CCN-STIC 302, del CCN.

En organizaciones ajenas a la Administración, los sistemas deberán contar con documentación de seguridad según los parámetros establecidos en el documento CCN-STIC 204.

Con objeto de limitar el riesgo de comprometimiento de la información manejada en estos sistemas, se aconseja adoptar las siguientes medidas mínimas, obligatorias en caso de transporte del equipo fuera de las instalaciones autorizadas:

- Cifrado del disco duro del equipo mediante un mecanismo autorizado para dicho grado o superior, ó llevar la información en soporte removible adecuadamente cifrado y etiquetado.
- Aplicación de la configuración de seguridad aprobada al equipo que maneje esta información.

11. GLOSARIO

Autoridad Nacional de Seguridad (ANS): Cargo ejercido conjuntamente por el Ministro de Asuntos Exteriores y el Ministro de Defensa. Su misión es ser el máximo representante de la protección de la Información Clasificada OTAN/UE/ESA en España. Vela, asimismo, por el cumplimiento de las normas adoptadas en los Acuerdos para la Protección de la Información Clasificada suscritos por nuestro país en materia de intercambio de materias clasificadas.

Autoridad Nacional de Seguridad Delegada (ANS-D): Nombramiento que recae en la persona que ejerce el cargo de Secretario de Estado-Director del CNI. Su misión consiste en ejercer, por delegación, las funciones que le corresponden a la ANS.

CCN: Centro Criptológico Nacional

Confidencialidad: Aseguramiento de que la información es accesible sólo para aquellos autorizados a tener acceso.

Disponibilidad: Aseguramiento de que los usuarios autorizados tienen acceso cuando lo requieran a la información y sus activos asociados.

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 niveles 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. Los grados de clasificación en España, de mayor a menor, según Ley de Secretos Oficiales son SECRETO y RESERVADO. En Acuerdos Internacionales y en Ordenes e Instrucciones Ministeriales, se añaden CONFIDENCIAL y DIFUSIÓN LIMITADA.

HPS: Habilitación Personal de Seguridad. 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 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.

Integridad: Garantía de la exactitud y completitud de la información y los métodos de su procesamiento.

Necesidad de conocer: Determinación positiva por la que se confirma que un posible destinatario requiere el acceso a, el conocimiento de, o la posesión de la información para desempeñar servicios, tareas o cometidos oficiales.

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, 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 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.

STIC: Seguridad de las Tecnologías de la Información y las Comunicaciones.

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, 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.

ANEXO I - CERTIFICADO DE INSTRUCCIÓN Y COMPROMISO DE RESERVA

El Jefe o Responsable de Seguridad, D/D^a _____, del Organismo/Entidad _____, certifica que ha procedido a la verificación de los datos contenidos en el Documento de Identidad (en vigor) del interesado (fotografía, firma, n° del DNI/TRE/Pasaporte, nombre y apellidos) y que los mismos se corresponden con los reflejados debajo, en este impreso. Asimismo, declara haber instruido a dicho interesado sobre los compromisos y obligaciones que adquiere al tener acceso a Información Clasificada con grado de DIFUSIÓN LIMITADA.

De lo que doy fe con mi firma:

En, a ... dede 20.....

Firma del Responsable/Jefe de Seguridad

D/Dña _____

con DNI (o Tarjeta/Permiso Residente Extranjeros, o Pasaporte) número _____

y destinado/a en _____

con la categoría o cargo _____

DECLARA:

Se comprometo a mantener la debida reserva y a no revelar ninguna Información Clasificada a que pudiera tener, o haber tenido, acceso con motivo del cumplimiento de sus obligaciones o por otro motivo cualquiera, siendo consciente de que dicho deber de reserva permanecerá vigente de forma permanente. Asimismo declara que comprende perfectamente y conoce las responsabilidades penales y disciplinarias en que pudiera incurrir por la divulgación no autorizada de esta clase de informaciones, bien sea voluntariamente o por negligencia, por acción u omisión, con arreglo a las disposiciones legales y administrativas vigentes.

Y para que conste y surta los debidos efectos ante la Autoridad competente para resolver cualquier incumplimiento, firma la presente declaración.

En, a ... dede 20.....

Firma del interesado