

***Autoridad Delegada
para la Seguridad de la Información Clasificada***

- NS/05 -

***Seguridad en los Sistemas de
Información y Comunicaciones***

SEGURIDAD EN LOS SISTEMAS DE INFORMACIÓN Y COMUNICACIONES

ÍNDICE

1. INTRODUCCIÓN.....	3
2. OBJETO.....	4
3. ÁMBITO	4
4. ACREDITACIÓN DE SISTEMAS.....	4
4.1. CONCEPTOS GENERALES.....	4
4.2. ESTRATEGIA DE ACREDITACIÓN.....	6
4.3. DELEGACIÓN DE LA AUTORIDAD DE ACREDITACIÓN	7
4.4. PROCEDIMIENTO DE ACREDITACIÓN.....	7
5. SEGURIDAD DE LA INFORMACIÓN CLASIFICADA MANEJADA EN SISTEMAS DE INFORMACIÓN Y COMUNICACIONES	9
5.1. SEGURIDAD DOCUMENTAL	9
5.2. SEGURIDAD EN EL PERSONAL.....	10
5.3. SEGURIDAD FÍSICA	11
5.4. SEGURIDAD EN LOS SISTEMAS DE INFORMACIÓN Y COMUNICACIONES	11
5.4.1. <i>Objetivos de Seguridad</i>	11
5.4.2. <i>Principios de Seguridad</i>	12
5.4.3. <i>Medidas de Seguridad</i>	12
5.4.4. <i>Organización de Seguridad</i>	13
5.4.5. <i>Gestión del Riesgo</i>	14
5.4.6. <i>Requisitos de Seguridad</i>	17
5.4.7. <i>Documentación de Seguridad</i>	20

SEGURIDAD EN LOS SISTEMAS DE INFORMACIÓN Y COMUNICACIONES

1. INTRODUCCIÓN

La Información Clasificada almacenada, procesada o transmitida (en adelante manejada) por Sistemas de Información y Comunicaciones (en adelante Sistemas), debe protegerse contra la pérdida de confidencialidad, integridad y disponibilidad, sea accidental o intencionada, y debe impedirse la pérdida de integridad y disponibilidad de los propios Sistemas que sustentan dicha información.

Al objeto de conseguir una adecuada protección, se deberá aplicar un conjunto equilibrado de medidas de seguridad, de distinta naturaleza (técnicas, físicas, en el personal y documentales), que permitan la creación de un entorno seguro para el manejo de la Información Clasificada en dichos Sistemas.

Corresponde a la Autoridad Nacional, responsable de la protección de la Información Clasificada en los ámbitos de su competencia, establecer las medidas de seguridad a implementar para la adecuada protección de la Información Clasificada manejada en Sistemas. Dichas medidas se traducirán en requisitos de seguridad a cumplir por los propios Sistemas, por el entorno físico en el cual se ubican, por el personal con acceso a dichos Sistemas y por el tratamiento documental asociado.

Asimismo, corresponde a la Autoridad responsable de la protección de la Información Clasificada verificar la correcta aplicación de las medidas de seguridad exigidas. Llegado el caso, si el resultado de esta verificación es satisfactorio, dicha Autoridad procederá a la emisión de un Certificado de Acreditación para el Sistema, por el que se autoriza a dicho Sistema para el manejo de Información Clasificada en las condiciones establecidas.

En este sentido se entiende por Acreditación la certificación, otorgada por la Autoridad de Acreditación de Seguridad (AAS, definida más adelante), de la capacidad de un Sistema para manejar, con la protección debida, Información Clasificada de un determinado propietario y hasta un determinado grado de clasificación, en unas condiciones determinadas y conocidas. Dicha Acreditación será concedida en base a las condiciones verificadas en los ámbitos de Seguridad en los Sistemas de Información y Comunicaciones, Seguridad en el Personal, Seguridad Física (de las instalaciones) y Seguridad de la Información (exclusivamente documental en el caso de Sistemas).

La presente norma, dentro de las Normas de la Autoridad Nacional para la Protección de la Información Clasificada, establece condiciones **específicas** para el manejo de Información Clasificada en los Sistemas. Los aspectos **generales**, u otros específicos, del manejo de la Información Clasificada, establecidos en el resto de normas de la Autoridad Nacional, serán igualmente de aplicación.

2. OBJETO

Esta Norma tiene por objeto establecer, de acuerdo con las responsabilidades adquiridas por la Autoridad Nacional, las condiciones de seguridad necesarias para el manejo de Información Clasificada por Sistemas, así como definir el procedimiento de Acreditación que obligatoriamente deberán superar todos los Sistemas antes de manejar Información Clasificada.

3. ÁMBITO

Esta Norma es de obligado cumplimiento para todos los Sistemas que manejen o vayan a manejar Información Clasificada cuya protección sea responsabilidad de la Autoridad Nacional, cuyo ámbito de competencia queda establecido en el apartado 1 de la norma NS/01 de la Autoridad Nacional.

Para las referencias a los distintos grados de clasificación de la Información Clasificada, se emplearán los criterios definidos en la norma NS/04 de la Autoridad Nacional. Será de aplicación la tabla de equivalencias establecida en dicha norma.

4. ACREDITACIÓN DE SISTEMAS

4.1. Conceptos Generales

La Acreditación de Sistemas tiene como finalidad verificar la adecuada protección de la Información Clasificada cuando es manejada en Sistemas de Información y Comunicaciones.

Esta verificación se realizará de acuerdo a los criterios de seguridad (tanto en los Sistemas como de procedimiento, física, del personal y documental) establecidos en las normas de la Autoridad Nacional y en otros documentos referidos en las mismas.

Se entiende por **Autoridad de Acreditación de Seguridad (AAS)**, la autoridad competente para autorizar el uso de un Sistema para manejar Información Clasificada, tras verificar la correcta aplicación de las medidas de seguridad necesarias para su protección. Si el resultado de esta verificación es satisfactorio y el riesgo residual final es admisible, dicha Autoridad procederá a la emisión de un Certificado de Acreditación para dicho Sistema.

Corresponde a la Autoridad Nacional actuar como AAS, dentro de su ámbito de competencia, especificado en la norma NS/01, pudiendo delegar dicha función. Cuando dicha capacidad sea delegada, será la autoridad delegada quien asuma las competencias, en los términos y con las limitaciones que se definan, no pudiendo delegar a su vez esta función.

La Acreditación es, por tanto, el acto formal por el que la Autoridad competente o delegada (en adelante AAS), reconoce la capacidad de un Sistema para manejar Información Clasificada de un determinado ámbito o propietario (nacional, OTAN, etc.), hasta un determinado grado de clasificación y en unas condiciones determinadas, para lo que otorgará el correspondiente Certificado de Acreditación, por el que se autoriza dicho uso.

La Acreditación es concedida en base a unas determinadas condiciones de seguridad de la Información Clasificada, tanto en el ámbito de Seguridad de las Tecnologías de la Información y las Comunicaciones (STIC), como en el de la Seguridad en el Personal, la Seguridad Física de las instalaciones y la Seguridad de la Información, que deberán ser previamente acreditadas, y de las que el solicitante deberá aportar las evidencias y documentación necesarias para su valoración y aprobación.

La tramitación hacia la AAS de la solicitud de Acreditación para un Sistema, se realizará a través de la Infraestructura Nacional de Protección de la Información Clasificada (Órgano de Control o Servicio de Protección de Información Clasificada) correspondiente, siendo esta tramitación parte de la responsabilidad de la Autoridad Operativa del Sistema de las TIC (AOSTIC), en su calidad de responsable de la Estructura Operacional del Sistema, definida en el apartado **5.4.4.** de la presente norma.

Como resultado de cada proceso de Acreditación, la AAS resolverá dicho proceso en uno de los siguientes sentidos:

- **Acreditación:** declaración de Acreditación para un periodo de tiempo especificado, en las condiciones operativas y ámbitos reflejados en la documentación correspondiente. Estos periodos varían en función del grado de clasificación, siendo normalmente:
 - “SECRETO o equivalente” 3 años.
 - “RESERVADO o equivalente” 3 a 4 años.
 - “CONFIDENCIAL o equivalente” 4 a 5 años.
 - “DIFUSIÓN LIMITADA o equivalente” 5 a 7 años.
- **Acreditación Provisional para Operar (APO;** en sus siglas inglesas IATO – Interim Approval to Operate): declaración de Acreditación parcial, por un plazo de tiempo limitado (normalmente hasta 6 meses, y nunca superior a 1 año), motivada por la existencia de deficiencias leves determinadas durante el proceso de acreditación.
- **Acreditación Temporal con Propósitos Operacionales (ATPO):** esta autorización es apropiada para situaciones en la que no se ha finalizado el proceso de acreditación y sólo se otorgará en situaciones muy excepcionales, cuando prima la operatividad sobre la seguridad (hasta 6 meses y prorrogable). Al menos debe disponerse del Concepto de Operación (CO).
- **Acreditación para Pruebas (AP):** autorización para poder operar el Sistema para la realización de pruebas técnicas (funcionales y de seguridad), sin manejar Información Clasificada. Debe estar redactada toda la documentación de seguridad del Sistema.
- **Denegación:** no se autoriza al Sistema a operar. Expresa las deficiencias graves específicas y las acciones correctivas que deben llevarse a cabo.

La AAS seguirá supervisando las disposiciones de seguridad de los Sistemas bajo su responsabilidad, principalmente llevando a cabo nuevas valoraciones de los riesgos e inspecciones/revisiones periódicas de las disposiciones de seguridad en vigor, de acuerdo con

los requisitos de las políticas de seguridad. Los Sistemas autorizados deberán someterse a las inspecciones y análisis de seguridad que la AAS considere oportunos para asegurar el cumplimiento de lo estipulado en la documentación de seguridad del Sistema.

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

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

4.2. Estrategia de Acreditación

Serán objeto de Acreditación específica, por un lado, los Sistemas dedicados al manejo de Información Clasificada (típicamente estaciones aisladas, redes de área local y redes de área extensa), y por otro, las interconexiones entre dos o más de estos Sistemas.

Para cada Sistema e interconexión de Sistemas se emitirá, una vez aprobadas sus condiciones seguridad (Seguridad de la Información, concretamente documental, Seguridad en el Personal, Seguridad Física de las instalaciones y Seguridad en los Sistemas), el correspondiente Certificado de Acreditación, de acuerdo al procedimiento de Acreditación descrito en esta Norma.

Para redes de área extensa y comunidades de redes de área local, y para Sistemas que por su complejidad y extensión así lo requieran, la Autoridad Nacional decidirá, caso por caso, la estrategia de Acreditación a seguir. Esta estrategia de Acreditación será acordada junto con la AOSTIC en base a la documentación aportada inicialmente por ésta (Concepto de Operación del Sistema).

Durante el proceso de Acreditación, la comunicación oficial entre la AOSTIC y la AAS deberá encauzarse principalmente a través del Órgano de Control de la Información Clasificada del que dependa directamente la AOSTIC, salvo en temas técnicos de detalle, que podrán tramitarse directamente entre los órganos directamente afectados. Este Órgano de Control será parte activa en el proceso de Acreditación, supervisando su evolución y apoyando a la AOSTIC a lo largo del mismo.

Para aquellos Sistemas bajo supervisión de un Panel de Acreditación específico, será de aplicación la estrategia de Acreditación establecida por éste. Corresponde a la Autoridad Nacional prestar el apoyo necesario en la Acreditación de los nodos del Sistema ubicados en su ámbito de responsabilidad, así como la comunicación de este extremo al Panel de Acreditación.

La seguridad de los Sistemas que traten información cedida a España al amparo de Acuerdos Internacionales para la Protección de la Información Clasificada, se regirá por los principios establecidos en los mismos, aplicándose en todo lo posible la presente normativa.

4.3. Delegación de la Autoridad de Acreditación

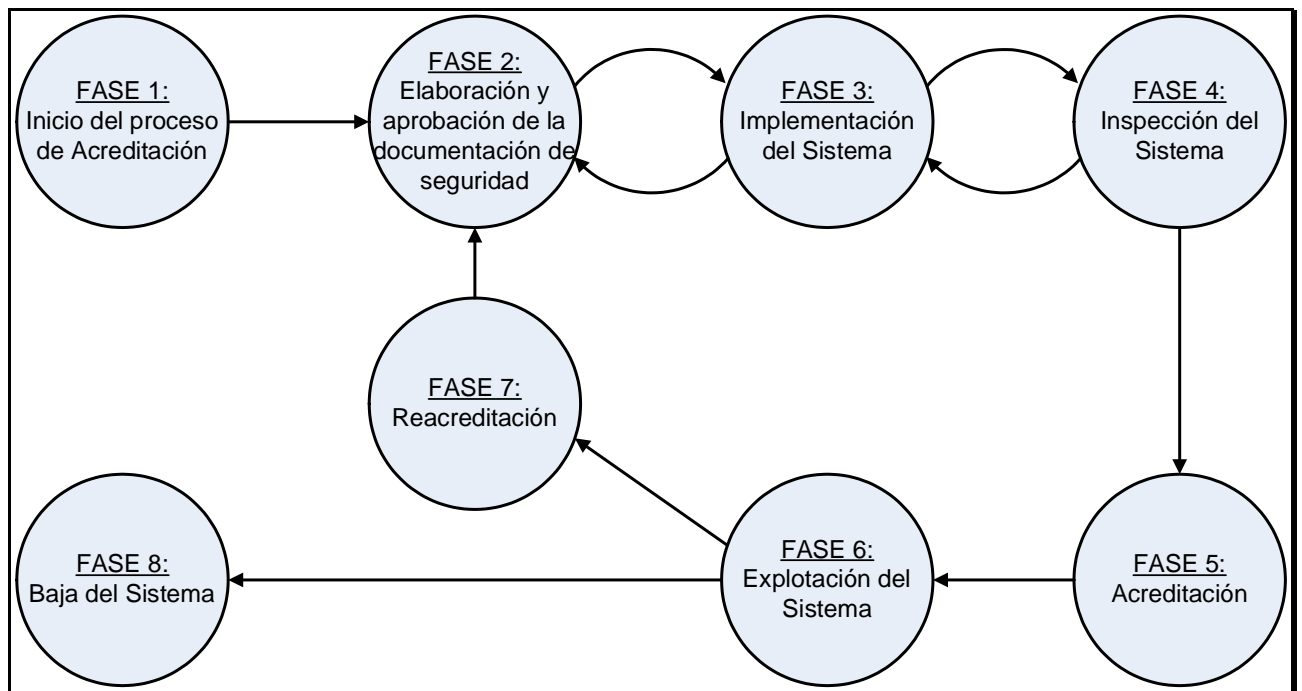
En aquellos casos en que la necesidad lo justifique, la Autoridad Nacional podrá delegar las competencias de Acreditación de Sistemas que manejen Información Clasificada de grado “DIFUSIÓN LIMITADA o equivalente” en la autoridad pertinente.

Para que esta delegación se materialice dicha autoridad deberá disponer de la infraestructura de protección de Información Clasificada necesaria.

4.4. Procedimiento de Acreditación

Todo proceso de Acreditación de Sistemas abordado por la AAS deberá registrarse por las disposiciones establecidas en la presente Norma.

Con el fin de homogeneizar y estructurar dichos procesos, se establece el siguiente procedimiento de Acreditación, el cual define cada una de las fases de los procesos de Acreditación.



FASE 1: Inicio del proceso de Acreditación

La AOSTIC deberá comunicar formalmente a la AAS la petición de Acreditación del Sistema. Dicha petición deberá incluir una descripción del Sistema a autorizar, la cual se ajustará al formato de Concepto de Operación definido en la correspondiente guía CCN-STIC (ver apartado 5.4.7. de la presente norma NS/05, más adelante).

A la recepción de dicha documentación, la AAS dará por iniciado el proceso de Acreditación, pudiendo a su vez solicitar cuantas aclaraciones y rectificaciones estime oportunas. Asimismo, cualquiera de las partes podrá plantear una reunión de coordinación que ayude al desarrollo del proceso de Acreditación.

Para aquellos Sistemas donde sea factible, en esta fase podrá remitirse para aprobación

la documentación exigida en la FASE 2 del proceso de Acreditación.

Una vez aprobada la documentación aportada, la AAS comunicará este hecho a la AOSTIC, que deberá proceder con el siguiente paso en el proceso de Acreditación.

FASE 2: Elaboración y aprobación de la documentación de seguridad

La AOSTIC, una vez aprobado el Concepto de Operación, será responsable de la elaboración del resto de documentación de seguridad exigida en cada caso.

Dicha documentación, junto con aquella complementaria que en su caso autorice la certificación del personal y locales del Sistema, deberá ser enviada a la AAS para su aprobación.

En el apartado **5.4.7.** de la presente norma se detalla la documentación necesaria para la Acreditación de todo sistema destinado a manejar Información Clasificada.

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

Una vez aprobada la documentación de seguridad del Sistema, la AOSTIC será responsable de la puesta en funcionamiento de éste, de acuerdo a dicha documentación y a las condiciones de seguridad en ella especificadas.

La AOSTIC comunicará a la AAS, con antelación suficiente, la fecha a partir de la cual el Sistema y su entorno de seguridad (entornos de seguridad local, global y electrónico) estará listo para su inspección, a fin de que esta última pueda planificar adecuadamente su calendario de inspecciones.

Asimismo, la AOSTIC deberá comunicar a la AAS todo condicionante adicional (p.e. necesidades operacionales, comerciales o estratégicas) que ésta deba considerar con el fin de priorizar adecuadamente los distintos procesos de Acreditación en ejecución.

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

El Sistema a autorizar será inspeccionado por la AAS a fin de verificar su correcta implementación de acuerdo a la documentación de seguridad aprobada.

El resultado de dicha inspección será comunicado oficialmente a la AOSTIC. Aun resultando positiva la evaluación realizada, ésta no constituye en sí una autorización al Sistema para operar, la cual será comunicada por la AAS una vez verificado el resto de condicionantes (seguridad física, seguridad en el personal y seguridad documental).

FASE 5: Acreditación

Tras la verificación positiva por parte de la AAS de las condiciones de seguridad del Sistema (seguridad documental, seguridad física, seguridad en el personal y seguridad técnica), ésta procederá a la emisión del correspondiente Certificado de Acreditación, el cual constituye a todos los efectos la única autorización para que el Sistema maneje Información Clasificada.

FASE 6: Explotación del Sistema

Una vez obtenido el Certificado de Acreditación, se deberán mantener las condiciones de seguridad iniciales que dieron lugar a dicha autorización. En caso contrario, este Certificado de Acreditación pierde automáticamente toda validez, siendo imprescindible la superación de un proceso de reacreditación, destinado a la obtención de un nuevo Certificado de Acreditación del Sistema.

Con el fin de verificar que los Sistemas autorizados para el manejo de Información Clasificada mantienen las condiciones de seguridad que dieron lugar a la Acreditación, éstos se someterán a un proceso de inspecciones de seguridad periódicas.

FASE 7: Reacreditación

Transcurrido el periodo de validez del Certificado de Acreditación, el Sistema pierde su autorización para manejar Información Clasificada. Es responsabilidad de la AOSTIC el iniciar con la antelación suficiente los trámites para la reacreditación del mismo.

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

FASE 8: Baja del Sistema

Una vez llega a su fin la vida útil de un Sistema autorizado para el manejo de Información Clasificada, es responsabilidad de la AOSTIC del mismo garantizar la correcta desclasificación de sus activos y la destrucción de la Información Clasificada almacenada en éste.

Los procedimientos a seguir en este caso estarán recogidos en el Documento de Requisitos de Seguridad el Sistema o interconexión, tal y como se indica en la guía CCN-STIC 202.

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

Este apartado tiene por objeto describir todos los aspectos de seguridad a implementar en la protección de la Información Clasificada manejada en Sistemas de Información y Comunicaciones, tanto desde el punto de vista de seguridad documental, como de seguridad en el personal, de seguridad física y de seguridad de los sistemas propiamente dicha.

5.1. Seguridad Documental

Dentro de los Sistemas, la información manejada siempre es en la forma de documentos, por ello se habla de forma habitual en esta norma de Seguridad Documental, que constituiría un apartado específico dentro del concepto más amplio de Seguridad de la Información.

Todo Sistema destinado al manejo de Información Clasificada deberá tener claramente identificado el Órgano de Control del que depende a efectos de protección de la Información Clasificada.

Dicho Órgano de Control para la protección de la Información Clasificada se deberá haber constituido de acuerdo a lo establecido en la norma NS/01 de la Autoridad Nacional.

La contabilidad, distribución y manejo de soportes electrónicos de almacenamiento de Información Clasificada se realizará por parte del Órgano de Control competente.

La Información Clasificada deberá estar almacenada en soportes debidamente etiquetados según el nivel de clasificación que le corresponda o en Sistemas autorizados.

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

Los soportes removibles de almacenamiento, mientras no sean desclasificados, mantendrán el máximo nivel de clasificación para el que hayan sido empleados.

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

La Información Clasificada grabada en medios de almacenamiento informático reutilizables sólo podrá borrarse de conformidad con los procedimientos que apruebe la Autoridad de Seguridad de las TIC.

5.2. Seguridad en el Personal

Todas las personas que tengan acceso a Sistemas donde se maneje Información Clasificada, o a locales donde se ubiquen estos Sistemas, deberán estar en posesión de la Habilitación Personal de Seguridad (HPS) correspondiente al máximo grado de clasificación de la Información Clasificada manejada en dicho Sistema o local.

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

En el caso particular del personal dedicado a tareas de administración de Sistemas, administración de seguridad y mantenimiento del Sistema, deberá estar en posesión de una HPS adecuada para el acceso a Información Clasificada un grado de clasificación superior a la máxima clasificación de la información manejada en el Sistema, ya que su particular estatus privilegiado del que goza este personal en el Sistema le permite acceder al total de la Información Clasificada manejada por éste con independencia del criterio de necesidad de

conocer, definido en la norma NS/02 de la Autoridad Nacional.

La habilitación de seguridad del personal con acceso a Información Clasificada se realizará de acuerdo al procedimiento establecido en la norma NS/02 de la Autoridad Nacional.

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

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

5.3. Seguridad Física

Aquellas áreas donde se ubiquen los distintos componentes de los Sistemas que manejen Información Clasificada “CONFIDENCIAL o equivalente” o superior, deberán estar acreditadas como Zonas de Acceso Restringido “Área Clase I” o “Área Clase II”, según el siguiente criterio:

- Área Clase I cuando las instalaciones alojen servidores o equipos de red, de comunicaciones o de cifra, o cuando, independientemente del tipo de Sistema o equipamiento de que se trate, la información manejada esté clasificada como “SECRETO o equivalente”.
- Área Clase II cuando las instalaciones alojen terminales cliente o estaciones aisladas.

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

5.4. Seguridad en los Sistemas de Información y Comunicaciones

5.4.1. Objetivos de Seguridad

Los objetivos de seguridad perseguidos con la aplicación de medidas de seguridad en los Sistemas de Información y Comunicaciones son:

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

5.4.2. Principios de Seguridad

Todo Sistema en el que se vaya a manejar Información Clasificada deberá atenerse a unos principios básicos dirigidos a asegurar la debida protección de la Información Clasificada:

- a) Todos los Sistemas deberán ser sometidos a un proceso de Acreditación que garantice que se encuentran protegidos mediante un conjunto apropiado de elementos hardware y software, adecuadamente configurados, de forma que permitan garantizar la confidencialidad, integridad y disponibilidad de la Información Clasificada manejada por el Sistema, así como la integridad y disponibilidad del propio Sistema.
- b) El manejo de Información Clasificada en un Sistema requerirá la previa autorización para ello por la Autoridad de Acreditación de Seguridad.
- c) La interconexión de Sistemas que manejen Información Clasificada requerirá la previa Acreditación por las Autoridades competentes para cada Sistema. Cada Sistema tratará a los otros Sistemas como de no-confianza y aplicará medidas de protección para controlar el intercambio de información con otros Sistemas.
- d) A los usuarios del Sistema sólo se les concederán los privilegios y autorizaciones que necesiten para llevar a cabo sus tareas y cometidos. Deberán estar habilitados sólo hasta el mayor grado de clasificación de la información de la que éstos tengan necesidad de conocer.
- e) Los responsables de Equipos de Cifra, Material de Claves o de los elementos de seguridad utilizados para la protección de los Sistemas, requerirán de una Acreditación especial, de acuerdo a lo especificado en el apartado **5.4.6.3** de esta Norma.
- f) Los locales destinados a alojar Sistemas que manejen Información Clasificada “CONFIDENCIAL o equivalente” o superior deberán estar acreditados como Zonas de Acceso Restringido “Área Clase I” o “Área Clase II”.
- g) Toda la Información Clasificada “CONFIDENCIAL o equivalente” o superior extraída de un Sistema deberá quedar registrada en el Sistema de Registro correspondiente, constituido por los Órganos de Control.
- h) Se aplicará una Gestión del Riesgo de Seguridad en los Sistemas, para controlar, reducir, eliminar y evitar o aceptar riesgos.

La aplicación de estos principios y la posterior aplicación de las medidas de protección se verificarán, inicial y periódicamente, por la Autoridad de Acreditación de Sistemas.

5.4.3. Medidas de Seguridad

Todo Sistema en el que se vaya a manejar Información Clasificada deberá implementarlas siguientes medidas de protección mínimas:

- a) Dispondrá de los medios necesarios para identificar y autenticar de forma fiable a las personas cuyo acceso esté autorizado, asegurando que se cumple el principio de la necesidad de conocer.
- b) Toda información y equipamiento que permita el acceso a los Sistemas deberá ser protegida de acuerdo al mayor grado de clasificación de la Información Clasificada a la que pudiera dar acceso.
- c) Todo medio de almacenamiento utilizado en Sistemas será protegido de acuerdo al

- máximo grado de clasificación de la información que contiene.
- d) Deberá contar con los dispositivos necesarios para realizar el registro automático de los accesos e intentos de acceso a la Información Clasificada.
 - e) Todo dispositivo de seguridad destinado a su empleo en Sistemas que manejen Información Clasificada deberá haber sido aprobado por el Centro Criptológico Nacional (CCN).
 - f) La interconexión entre Sistemas ubicados en distintas Zonas de Acceso Restringido requerirá la utilización de elementos de cifra certificados por el CCN, de acuerdo al grado de clasificación de la información a transmitir.
 - g) La Información Clasificada contenida en los dispositivos de almacenamiento removibles deberá estar protegida mediante una herramienta de cifrado adecuada a su grado de clasificación.
 - h) Los Sistemas que manejen Información Clasificada “CONFIDENCIAL o equivalente” o superior, deberán ser protegidos contra las amenazas derivadas de emanaciones radiológicas no deseadas, cuyo estudio y control se conoce como TEMPEST.
 - i) Todo Sistema deberá contar con programas actualizados de detección de virus y de software malicioso.
 - j) No se permitirá el uso de equipos o dispositivos electrónicos particulares, incluidos soportes de almacenamiento, para el manejo de Información Clasificada.
 - k) No se permitirá la entrada de equipos o dispositivos electrónicos, incluidos soportes de almacenamiento, a Zonas de Acceso Restringido (ZAR), excepto los pertenecientes a los Sistemas autorizados para el manejo de Información Clasificada existentes en la propia ZAR.
 - l) Las tareas de instalación, administración, mantenimiento y reparación de los Sistemas que manejen Información Clasificada deberán ser llevadas a cabo por personal con Habilitación Personal de Seguridad (HPS) de grado igual o superior al grado de clasificación de la información que manejen los Sistemas a que dicho personal tenga acceso.
 - m) Los Sistemas que manejan Información Clasificada estarán sujetos a una valoración y gestión de riesgos acorde con los requisitos especificados en la norma CCN-STIC correspondiente.
 - n) Se adoptarán medidas adicionales, adecuadas a las circunstancias, allí donde una valoración de los riesgos haya establecido que la Información Clasificada, o los servicios y recursos de apoyo al Sistema, están sujetos a mayores riesgos, procedentes de amenazas y vulnerabilidades concretas.

5.4.4. Organización de Seguridad

Se determinan una serie de autoridades y responsables relacionados con la seguridad de los Sistemas a lo largo de su ciclo de vida. Se distingue entre estas estructuras:

- a) Estructura STIC Nacional
- b) Estructura STIC de la organización.
- c) Estructura de operación STIC del Sistema.
- d) Estructura de Control de Material de Cifra de la organización.
- e) Infraestructura de Protección de la Información Clasificada de la organización.

En cada departamento, organismo o entidad existirá una estructura de seguridad específica, responsable de aplicar la normativa de protección de la información clasificada

manejada en sus Sistemas de información y comunicaciones.

La estructura de seguridad establecida en el párrafo anterior será responsable, respecto a los Sistemas, de:

- a) Solicitar la autorización para operar o Acreditación del Sistema.
- b) Definir el Concepto de Operación.
- c) Elaborar la documentación de seguridad.
- d) Gestionar la configuración de seguridad.
- e) Formar en materia de seguridad a los usuarios autorizados.
- f) Auditar los registros de acceso a la información y de eventos de seguridad.
- g) Gestionar los incidentes de seguridad.
- h) Coordinar sus actuaciones con el Servicio de Protección de Información Clasificada que corresponda.

La Infraestructura Nacional de protección de la Información Clasificada, constituida por los Órganos de Control (que incluyen a los Servicios de Protección de Información Clasificada), será responsable, en cada ámbito de competencia, de supervisar la correcta aplicación de la normativa de protección de la Información Clasificada en los Sistemas. Llevarán registro de:

- a) Los Sistemas autorizados a manejar Información Clasificada en su ámbito de protección.
- b) La Información Clasificada manejada en los Sistemas.
- c) La Información Clasificada extraída de los Sistemas.
- d) Los usuarios autorizados para acceder a los Sistemas.
- e) Las Zonas de Acceso Restringido donde se ubican los Sistemas.

5.4.5. Gestión del Riesgo

Todos los Sistemas que manejen Información Clasificada estarán sujetos a una gestión de riesgos. A efectos de esta Norma, se utilizan las siguientes definiciones:

- Riesgo de seguridad – la probabilidad de que la vulnerabilidad inherente a un Sistema de Información y Comunicaciones sea explotada por cualquier amenaza y que su consecuencia sea que el Sistema quede comprometido.
- Gestión del riesgo de seguridad – proceso completo de identificación, control y minimización de eventos inciertos que puedan afectar a los recursos del Sistema.

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

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

riesgos se aumenta la concienciación en materia de seguridad, que debe estar presente en todos los niveles de la organización, desde el más alto nivel de gestión hasta el personal auxiliar y de operaciones.

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

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

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

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

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

La gestión del riesgo supone planificación, organización, dirección y control de recursos para garantizar que el riesgo permanece dentro de unos límites y de un coste aceptables. Es también un proceso ejecutado en colaboración, en el que representantes de diversos grupos de interés desarrollan una comprensión común de requerimientos y opciones. El aumento de la conciencia de seguridad refuerza la seguridad y la hace más compatible con las necesidades de los usuarios.

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

Los procesos de gestión y de análisis de riesgos son un ejercicio de recolección y

valoración de datos que aborda dos cuestiones básicas: los activos que corren peligro y cuáles serían el impacto o las consecuencias si las vulnerabilidades identificadas fueran explotadas con éxito.

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

- Identificar el ámbito y objetivos del análisis de riesgos; el objetivo se acordará entre las autoridades de planificación y aplicación de seguridad en los Sistemas, las autoridades de operación de los Sistemas, por el personal de proyectos y por las autoridades de certificación de seguridad.
- Determinar los activos físicos y de información que contribuyen al cumplimiento de la misión de un Sistema o una misión de la organización.
- Determinar el valor de los activos físicos.
- Determinar el valor de los activos de información respecto al impacto en las siguientes dimensiones: confidencialidad, integridad y disponibilidad.
- Identificar las amenazas y vulnerabilidades del Sistema y el nivel de dichas amenazas y vulnerabilidades.
- Identificar las contramedidas existentes.
- Determinar las contramedidas necesarias y compararlas con las ya existentes.
- Revisar los riesgos y las contramedidas recomendadas, teniendo en cuenta las siguientes opciones y considerando que las políticas de seguridad exigen la aplicación de un estándar mínimo de protección a la Información Clasificada:
 - Eliminación del riesgo – el objetivo es minimizar las vulnerabilidades reales o potenciales aplicando la totalidad de las contramedidas identificadas.
 - Prevención de la degradación de los activos físicos y de información – el objetivo es la aplicación de contramedidas con el fin de evitar, en la medida posible, que se produzcan estas degradaciones, teniendo en cuenta que algunos riesgos no pueden eliminarse debido a razones técnicas u operativas.
 - Limitación de la degradación de los activos físicos y de información – el objetivo es la aplicación de contramedidas con el fin de limitar estas degradaciones a un nivel aceptable.
 - Aceptación del riesgo de degradación de activos físicos y de información – cuando debe tomarse la decisión de aceptar las consecuencias de la materialización de una amenaza, ya sea porque el coste o impacto de la degradación asociada es insignificante, porque la probabilidad de que se materialice la amenaza se considera suficientemente baja, o porque el coste de las contramedidas es mucho más elevado que el coste o impacto de las pérdidas asociadas a la materialización de la amenaza.
- Elaborar un Informe de Gestión de Riesgos que incluya la descripción de las contramedidas que van a implementarse y la descripción del riesgo residual.

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

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

5.4.6. Requisitos de Seguridad

5.4.6.1. Seguridad de los Sistemas

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

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

5.4.6.2. Interconexión de Sistemas

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

Se produce una interconexión entre Sistemas cuando existe una conexión y se habilitan flujos de información entre los mismos.

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

- Se incrementa el número de usuarios (autorizados y no autorizados) que acceden a los Sistemas.
- El nuevo Sistema que se interconecta puede tener conexiones o vías de acceso desconocidas para los administradores y supervisores de seguridad del Sistema que se considere.
- El nuevo Sistema que se interconecta puede tener unas amenazas distintas a las que en su día se consideraron para establecer los requisitos de seguridad del

Sistema en cuestión.

- El flujo de información entre ambos Sistemas puede requerir restricciones concretas.
- Ambos Sistemas pueden tener distintas políticas de seguridad, diferentes niveles de confianza, diferentes AOSTIC o una combinación de las anteriores.

Por ello es necesaria la Acreditación de la interconexión de Sistemas al mayor nivel de clasificación de la información que manejen.

Todos los Sistemas que manejen Información Clasificada, como paso previo a la solicitud de Acreditación de su interconexión a otro Sistema, redes públicas o similares, deberán estar en posesión de un Certificado de Acreditación al nivel correspondiente a la información que manejen.

La Acreditación de la interconexión de un Sistema es responsabilidad de la AAS. El procedimiento de Acreditación y los requisitos de seguridad serán los que se indican o refieren en esta Norma.

5.4.6.3. Seguridad Criptológica

Solamente se podrán utilizar los productos y Sistemas de cifra certificados, cualquiera que sea el nivel de clasificación de la información manejada. No está autorizado el uso de productos de cifra comerciales no certificados para la protección de Información Clasificada. Las excepciones a esta norma requerirán la aprobación de la Autoridad de Seguridad de las TIC.

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

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

Los Servicios de Protección de la Información Clasificada serán responsables, en su ámbito de competencia, de asegurar la correcta aplicación de la normativa de protección del Material de Cifra.

Los Servicios de Protección de la Información Clasificada llevarán registro de:

- Las Zonas de Acceso Restringido donde se ubican las Cuentas de Cifra.
- El personal autorizado para acceder a las Cuentas de Cifra.

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

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

La apertura de una Cuenta de Cifra requerirá el nombramiento de un Criptocustodio como responsable de la misma, así como de un Criptocustodio suplente, que asumirá todas las responsabilidades y obligaciones de aquel en su ausencia.

El Material de Cifra puede dividirse en:

- Material de Claves, que incluye soportes de claves, sistemas de códigos, sistemas de autenticación y demás tipos de claves que deben cambiarse a intervalos previamente determinados y se emplean directamente en el proceso de cifrado y descifrado. Dentro del Material de Claves se puede distinguir entre:
 - Claves de Alto Nivel: son aquellas claves con un grado de clasificación de “RESERVADO o equivalente” o “SECRETO o equivalente”
 - Claves de Bajo Nivel: son aquellas claves con un grado de clasificación no superior a “CONFIDENCIAL o equivalente”
- Equipos de Cifra, que incluye cualquier dispositivo empleado para cifrar y descifrar la información.
- Publicaciones de Cifra, que incluye toda la documentación, principalmente técnica, asociada a los Equipos de Cifra y Material de Claves, relativa a su uso, instalación, mantenimiento o composición.

El acceso a Material de Cifra de grado “CONFIDENCIAL o equivalente” o superior, quedará restringido a las personas que dispongan de Habilitación Personal de Seguridad (HPS) de grado apropiado y con la especialidad CRIPTO.

El Material de Cifra requiere de medios de almacenamiento específicos, por lo que se almacenará de forma independiente y físicamente separada de cualquier otra Información Clasificada.

Todo Material de Cifra utilizado para la protección de Información Clasificada estará a su vez clasificado, como mínimo, con el grado de “DIFUSIÓN LIMITADA o equivalente”.

El Material de Claves y las Publicaciones de Cifra llevarán, además de la marca correspondiente a su grado de clasificación, la marca adicional CRIPTO.

Los Equipos de Cifra Controlados serán contabilizados en las Cuentas de Cifra y protegidos con medidas de seguridad equivalentes a las requeridas para la protección de la Información Clasificada con grado de “DIFUSIÓN LIMITADA o equivalente”.

5.4.6.4. Seguridad de las Emanaciones

De acuerdo con el riesgo de explotación y la sensibilidad de la información manejada, se implementarán medidas de seguridad adecuadas que permitan la protección de la Información Clasificada contra los fenómenos de radiación electromagnética no deseados.

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

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

5.4.7. Documentación de Seguridad

Todo Sistema que maneje Información Clasificada deberá tener actualizada la siguiente documentación de seguridad:

	SECRETO/RESERVADO o equivalente	CONFIDENCIAL o equivalente	DIFUSIÓN LIMITADA o equivalente
Declaración de Requisitos de Seguridad Comunes (DRSC)	Sí	Sí	Sí
Declaración de Requisitos de Seguridad de la Interconexión (DRSI)	Sí	Sí	Sí
Análisis de riesgos	Formal	No Formal	No Formal
Concepto de Operación (CO)	Sí	Sí	Sí
Declaración de Requisitos Específicos de Seguridad (DRES)	Sí	Sí	Opcional
Procedimientos Operativos de Seguridad (POS)	Sí	Sí	Sí
Documento abreviado CO/DRES/POS	“RESERVADO o equivalente”	Sí	Sí
Certificado de Acreditación de Zonas de Acceso Restringido	Sí	Sí	No *
Certificación ZONING de locales	Sí	Sí	No
Certificación TEMPEST de equipamiento	Sí	Sí	No
Certificado de Acreditación	Sí	Sí	Sí

* En empresas contratistas y entidades fuera de la Administración y Fuerzas Armadas, sí se requerirá.

La Declaración de Requisitos de Seguridad Comunes (DRSC) es un documento sólo exigido cuando existe un conjunto de Sistemas interconectados (un Sistema de Sistemas), o cuando la complejidad y extensión del Sistema así lo requieran. Este documento se ajustará al modelo definido en la guía CCN-STIC 202.

La Declaración de Requisitos de Seguridad de la Interconexión (DRSI) se redactará cuando se requiera interconectar varios Sistemas Autorizados. Este documento se ajustará al modelo definido en la guía CCN-STIC 202.

El Análisis de Riesgos se ajustará a la metodología descrita en la guía CCN-STIC 410.

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

El documento de Declaración de Requisitos de Seguridad (DRES) se ajustará al modelo definido en la guía CCN-STIC 202.

El documento de Procedimientos Operativos de Seguridad (POS) se ajustará al modelo definido en la guía CCN-STIC 203.

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

- Equipos aislados o pequeñas redes (máximo 1 servidor y 10 estaciones), y
- que manejen Información Clasificada de grado “RESERVADO o equivalente” o inferior, y
- que estén ubicados dentro del mismo Entorno Global de Seguridad, y
- que trabajen en el modo seguro de operación “Unificado al Nivel Superior” o “Dedicado”.

Adicionalmente, para Sistemas encuadrados en programas de organismos internacionales, el correspondiente Panel de Acreditación podrá exigir cuanta documentación adicional estime oportuna.

