



**Autoridad Nacional de Seguridad
para la protección de la
información clasificada**

**- NS/08 -
Protección de la
información
clasificada OTAN
manejada en
sistemas de
información y
comunicaciones
(CIS)**

NORMA NS/08

PROTECCIÓN DE LA INFORMACIÓN CLASIFICADA OTAN MANEJADA EN SISTEMAS DE INFORMACIÓN Y COMUNICACIONES (CIS)

ÍNDICE

1. INTRODUCCIÓN.....	3
2. OBJETIVOS DE SEGURIDAD.....	3
3. ACREDITACIÓN DE SEGURIDAD.....	3
4. SEGURIDAD PERSONAL	4
5. SEGURIDAD FÍSICA.....	4
6. SERVICIOS DE SEGURIDAD.....	4
7. CONTROL E IMPUTABILIDAD DE LA INFORMACIÓN	5
7.1. MANEJO Y CONTROL DE LOS SOPORTES EXTRAIBLES DE ALMACENAMIENTO.....	5
8. SEGURIDAD DE LOS ORDENADORES PERSONALES (PC'S).....	5
9. UTILIZACIÓN DE EQUIPOS PARTICULARES	6
10. TRANSMISIÓN DE INFORMACIÓN CLASIFICADA.....	6
11. SEGURIDAD DE LAS EMISIONES ELECTROMAGNÉTICAS.....	6

PROTECCIÓN DE LA INFORMACIÓN CLASIFICADA OTAN MANEJADA EN SISTEMAS DE INFORMACIÓN Y COMUNICACIONES (CIS)

1. INTRODUCCIÓN

El contenido de esta norma es de aplicación a todos los sistemas de información y telecomunicaciones (sistemas CIS) que almacenen, procesen o transmitan (de aquí en adelante manejen) información clasificada de la Alianza.

La información clasificada de la OTAN manejada en un sistema de información y telecomunicaciones debe protegerse contra la pérdida de confidencialidad, integridad o disponibilidad, ya 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 la protección de seguridad adecuada se deberá implementar un conjunto equilibrado de medidas de seguridad de distinta naturaleza (física, de personal, de información de procedimientos e INFOSEC) que permitan la creación de un entorno seguro en el que opere el sistema de información, telecomunicaciones o cualquier otro sistema electrónico.

2. OBJETIVOS DE SEGURIDAD

Los objetivos de seguridad perseguidos con la aplicación de las medidas INFOSEC a la protección de la información clasificada son:

- a) mantener la confidencialidad de la información clasificada;
- b) mantener la integridad de la información clasificada y de los sistemas que la manejan y
- c) mantener la disponibilidad de la información clasificada y de los sistemas que la manejan.

3. ACREDITACIÓN DE SEGURIDAD

La ANS-D someterá a todos los sistemas de información que manejen información clasificada a un proceso de acreditación, previo a la concesión de autorización para manejar información clasificada, mediante el que se garantizará el adecuado nivel de protección y su mantenimiento.

La concesión de la autorización a un sistema de información para manejar información clasificada se denomina acreditación.

El proceso de acreditación se realizará de acuerdo a lo especificado en el correspondiente “Procedimiento de Acreditación de Sistemas CIS que manejan información clasificada OTAN”.

4. SEGURIDAD PERSONAL

Todos las personas que tengan acceso a los sistemas donde se maneja información clasificada, incluidas aquellas que no están autorizadas a acceder a la información manejada, deberán estar en posesión del nivel de habilitación adecuado.

5. SEGURIDAD FÍSICA

Aquellas áreas desde donde se pueda acceder o visualizar información clasificada mediante la utilización de las tecnologías de la información, deberán estar clasificadas de acuerdo al nivel de clasificación de la información accedida y a los requisitos de confidencialidad, integridad y disponibilidad requeridos.

6. SERVICIOS DE SEGURIDAD

Todos los sistemas de información que manejen información clasificada de la Alianza deberán disponer de un conjunto equilibrado de servicios de seguridad que proporcionen los objetivos de seguridad requeridos y protejan los sistemas de forma adecuada.

Estos servicios de seguridad permitirán, cuando sea apropiado, los siguientes:

- a) Identificar y autenticar a los individuos con acceso autorizado;
- b) Controlar los accesos a la información en base al principio de “la necesidad de conocer”;
- c) Verificar la integridad y el origen de la información y de los elementos del sistema;
- d) Mantener la integridad de la información clasificada y elementos del sistema;
- e) Garantizar y verificar el funcionamiento de los mecanismos de seguridad del sistema;
- f) Auditar la actividad de los usuarios y del sistema y
- g) Prevenir, detectar y corregir los impactos o incidentes que afecten a la confidencialidad, integridad o disponibilidad del sistema o de la información.

Para ello, se determinarán los requisitos de seguridad que deberán satisfacer los sistemas que manejan información clasificada de la Alianza. Dichos requisitos se agruparán en las siguientes categorías:

- a) Requisitos de identificación y autenticación.
- b) Requisitos de control de accesos
- c) Requisitos de auditoría de seguridad
- d) Requisitos de integridad
- e) Requisitos de protección de las funciones de seguridad
- f) Requisitos de gestión de la configuración
- g) Requisitos de disponibilidad
- h) Requisitos de gestión de la seguridad

Las autoridades responsables de los sistemas CIS nacionales que manejen información OTAN tendrán en cuenta que se satisfacen dichos requisitos en las diferentes fases del ciclo de vida de un sistema CIS, y deberán reflejarlos en la documentación de seguridad del sistema.

7. CONTROL E IMPUTABILIDAD DE LA INFORMACIÓN

Se mantendrán registros de auditoría automáticos o manuales del sistema, como control de acceso a la información clasificada NATO SECRET (NS) o superior. Dichos registros se mantendrán durante un periodo mínimo de cinco años.

7.1. Manejo y control de los soportes extraíbles de almacenamiento

Todos los soportes de almacenamiento informático (discos duros, disquetes, ordenadores portátiles, CDROM, copias impresas, etc...) que contengan información con clasificación NATO CONFIDENTIAL (NC) o superior, deberán estar apropiadamente identificados, controlados y registrados en el Organismo de Control correspondiente de acuerdo con el mayor nivel de clasificación de la información que contengan. Dichos controles e identificación deberán incluir como mínimo:

- a) Para NATO CONFIDENTIAL y superior, se utilizará un sistema de identificación (número de serie y marca de clasificación) para cada soporte por separado. Los Subregistros y Puntos de Control establecerán procedimientos para el registro y control de la emisión, recepción, utilización y destrucción final de los soportes.
- b) Para NATO SECRET y superior, se mantendrá un registro con todos los detalles relativos a los soportes extraíbles de almacenamiento incluyendo su contenido general y clasificación.
- c) Se establecerán controles aleatorios que aseguren la consistencia del contenido de los soportes con su identificación y los datos que figuran en el registro.
 - Para NATO CONFIDENTIAL, los soportes serán inspeccionados periódicamente de forma aleatoria para comprobar su presencia física y contenido (a fin de garantizar que en el soporte no se almacena información con un nivel de clasificación superior);
 - Para NATO SECRET, todos los soportes serán inspeccionados periódicamente para comprobar su presencia física y contenido (a fin de garantizar que en el soporte no se almacena información con un nivel de clasificación superior); y
 - Para COSMIC TOP SECRET (CTS) e información de categorías especiales, todos los soportes serán inspeccionados anualmente para comprobar su presencia física y contenido (a fin de garantizar que en el soporte no se almacena información de categoría diferente a la declarada).

8. SEGURIDAD DE LOS ORDENADORES PERSONALES (PC´s)

Los Ordenadores Personales, incluyendo los portátiles, agendas electrónicas, etc..., con discos fijos u otros dispositivos de almacenamiento no volátiles, operando de forma aislada o conectados en red, serán considerados como dispositivos de almacenamiento de información en el mismo sentido que los disquetes u otro dispositivo de almacenamiento extraíble.

9. UTILIZACIÓN DE EQUIPOS PARTICULARES

Queda expresamente prohibida la utilización de equipos (hardware y software) y sistemas extraíbles de almacenamiento particulares para el manejo de información clasificada de nivel NATO RESTRICTED o superior.

Queda expresamente prohibida la introducción de equipos (hardware y software) y sistemas extraíbles de almacenamiento particulares en zonas clasificadas como Clase I o Clase II donde se maneje información clasificada de la Alianza.

En el presente contexto, se entiende por equipos particulares los medios citados que no son propiedad del Organismo responsable de los sistemas de información acreditados.

10. TRANSMISIÓN DE INFORMACIÓN CLASIFICADA

Se implementarán medidas especiales para la protección de la información clasificada cuando esta se transmita mediante la utilización de sistemas CIS. La utilización de métodos criptográficos para la protección de la confidencialidad, integridad o disponibilidad de la información clasificada deberá ser específicamente aprobada por la ANS-D para dicho propósito.

La conexión de sistemas que manejan información CTS a redes públicas queda totalmente prohibida.

La protección de la confidencialidad de la información clasificada NS durante su transmisión se garantizará mediante la utilización de métodos o productos criptográficos aprobados por el Comité Militar de la OTAN (NAMILCOM).

La protección de la confidencialidad de la información clasificada NC o NR durante su transmisión garantizará mediante la utilización de métodos o productos criptográficos aprobados por la ANS-D o por el Comité Militar de la OTAN (NAMILCOM).

11. SEGURIDAD DE LAS EMISIONES ELECTROMAGNÉTICAS

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 NC o superior contra los fenómenos de radiación electromagnética no deseados.

