
	<b>AUTORIDAD NACIONAL DE SEGURIDAD DELEGADA</b> <b>Oficina Nacional de Seguridad</b>		 autoridad nacional de seguridad delegada oficina nacional de seguridad
	<b>ORIENTACIONES PARA LA ACREDITACIÓN DE SISTEMAS DE INFORMACIÓN Y COMUNICACIONES PARA EL MANEJO DE INFORMACIÓN CLASIFICADA</b>	<b>3.3.2011</b>	

**OR-ASIP-03-01.03**

**ORIENTACIONES PARA LA  
ACREDITACIÓN DE SISTEMAS DE  
INFORMACIÓN Y COMUNICACIONES  
PARA EL MANEJO DE INFORMACIÓN  
CLASIFICADA**

## ÍNDICE

1.	INTRODUCCIÓN.....	3
2.	OBJETO .....	3
3.	ALCANCE .....	3
4.	ACREDITACIÓN DE CIS.....	4
5.	INFORMACIÓN DE CONTACTO.....	5

---

## 1. INTRODUCCIÓN

---

La acreditación de todo sistema destinado al manejo de Información Clasificada tiene como finalidad verificar la adecuada protección de la Información Clasificada cuando es manejada en Sistemas de Información y Comunicaciones (CIS).

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 la normativa aplicable en cada caso. En el ámbito de competencia de la Autoridad Nacional para la Protección de la Información Clasificada son de aplicación las siguientes normas:

- NS/01 Infraestructura Nacional de Protección de la Información Clasificada.
- NS/02 Seguridad en el Personal. Habilitación de Seguridad del Personal.
- NS/03 Seguridad Física.
- NS/04 Seguridad de la Información.
- NS/05 Seguridad en los Sistemas de Información y Comunicaciones.
- NS/06 Seguridad Industrial.

Esta normativa se complementa y desarrolla, en el aspecto técnico, en el conjunto de guías CCN-STIC del **Centro Criptológico Nacional (CCN)**, las cuales establecen los requisitos de Seguridad de las Tecnologías de la Información y Comunicaciones (STIC) aplicables a todo sistema que deba manejar Información Clasificada.

---

## 2. OBJETO

---

Las presentes orientaciones se proporcionan con el fin único de constituir una introducción al proceso de acreditación de sistemas, no sustituyendo en ningún caso a lo establecido en la normativa de referencia.

---

## 3. ALCANCE

---

Estas Orientaciones son de aplicación para todos los Sistemas que manejen o vayan a manejar Información Clasificada cuya protección sea responsabilidad de la Autoridad Nacional, según el ámbito de competencia establecido en el apartado 1 de la norma NS/01 de la Autoridad Nacional. Asimismo, son de aplicación para todos los Sistemas que manejen o vayan a manejar Información Clasificada del Ministerio de Defensa al amparo de la O.M.C. 17/2001 “Manual de Protección de Materias Clasificadas del Ministerio de Defensa en Poder de las Empresas”.

---

#### 4. ACREDITACIÓN DE CIS

---

A continuación se relacionan, a modo de resumen, las principales tareas que deberán ser abordadas para la acreditación de un sistema, debiendo estas ser adaptadas al estado de desarrollo del sistema y de la organización responsable:

1. En el ámbito de la seguridad industrial, estar en posesión de la *Habilitación de Seguridad de Establecimiento (HSES)*, o tener firmado Acuerdo de Seguridad con Defensa.
2. Constitución de la necesaria infraestructura de protección de la Información Clasificada (Servicio de Protección u Órgano de Control, y su Jefe de Seguridad y puestos o cargos de Seguridad del Sistema).
3. Tramitación de las correspondientes *Habilitaciones Personales de Seguridad (HPS)* para todo el personal con acceso al sistema.
4. Acreditación de los locales del sistema como *Zonas de Acceso Restringido* Clase I o Clase II, según corresponda.
5. En el caso de que el sistema vaya a manejar Información Clasificada de grado CONFIDENCIAL o equivalente o superior, también deberá obtenerse la correspondiente certificación ZONING de los locales y TEMPEST del equipamiento del sistema.
6. El uso de productos criptológicos deberá atenerse a la regulación aprobada por el CCN.
7. Elaboración y remisión, junto con la solicitud formal de acreditación, a la **Oficina Nacional de Seguridad (ONS)** de la **documentación de seguridad del sistema**.
8. El CCN, principalmente, y la ONS, podrán requerir correcciones a dicha documentación, que deberán ser tenidas en cuenta para la construcción del mismo. Una vez aceptada, y comunicada la disponibilidad del sistema, se procederá a su inspección.

Del resultado de esta inspección y del estado de seguridad global del sistema (seguridad documental, seguridad en el personal y seguridad física) dependerá la concesión del correspondiente certificado de acreditación del sistema.

Los sistemas acreditados deben mantener las condiciones de seguridad que dieron lugar a ésta, estando sujetos a las correspondientes inspecciones periódicas y reacreditaciones.

Durante la ejecución de este proceso de acreditación la ONS solventará cualquier duda respecto al mismo o sobre la constitución de la infraestructura de protección, la seguridad en el personal y la seguridad física. La normativa de seguridad referida en este escrito se encuentra accesible en la página Web de la ONS.

Para la resolución de dudas exclusivamente relacionadas con cuestiones técnicas del sistema, seguridad TIC, TEMPEST, ZONING o CRIPTO podrá contactarse directamente con el CCN, cuyas guías CCN-STIC pueden ser descargadas desde el portal del CCN-CERT, donde se encuentran publicadas sólo las guías de grado “SIN CLASIFICAR”. Para el acceso a guías CCN-STIC clasificadas será necesario su solicitud oficial al CCN.

El acceso al área de descargas del portal CCN-CERT requiere el registro previo del usuario, el cual se encuentra inicialmente limitado al personal de la administración pública. Para el registro de personal del sector privado se exigirá a la empresa estar en posesión del correspondiente Acuerdo de Seguridad con el Ministerio de Defensa (según O.M.C. 17/2001) o HSEM/HSES (según NS/06) y haber firmado un acuerdo de confidencialidad con el CCN.

La **tramitación de la solicitud** de acreditación de un sistema, y todo trámite documental subsiguiente, se realizará a través de la Infraestructura Nacional de Protección de la Información Clasificada (Órgano de Control o Servicio de Protección de Información Clasificada).

---

## 5. INFORMACIÓN DE CONTACTO

---

### Oficina Nacional de Seguridad

Página Web

<http://www.cni.es/es/ons>

Área de Seguridad de la Infraestructura y del Personal

[asip@cni.es](mailto:asip@cni.es)

Área de Seguridad Industrial

[asic@cni.es](mailto:asic@cni.es)

### Centro Criptológico Nacional

Portal CCN-CERT

<https://www.ccn-cert.cni.es>

Unidad de Seguridad TIC

[acreditacion.ccn@cni.es](mailto:acreditacion.ccn@cni.es)

Unidad de Seguridad de las Emanaciones

[emsec.ccn@cni.es](mailto:emsec.ccn@cni.es)

Unidad de Seguridad Criptológica

[criptosec.ccn@cni.es](mailto:criptosec.ccn@cni.es)

