

**ACREDITACIÓN
SIMPLIFICADA
DE SISTEMAS TIC
DE GRADO
RESTRICTED/
DIFUSIÓN
LIMITADA**



Oficina Nacional de Seguridad
Centro Nacional de Inteligencia

CONTEXTO

El manejo de información clasificada de grado NATO RESTRICTED, RESTREINT UE/EU RESTRICTED y ESA RESTRICTED, así como su equivalente nacional DIFUSION LIMITADA¹, requiere de personal con la formación adecuada y de unas instalaciones con las medidas de seguridad apropiadas.

El creciente intercambio de información clasificada en formato electrónico hace necesaria la acreditación de sistemas de las tecnologías de la información y la comunicación (TIC) para que el manejo de esa información se efectúe con las adecuadas condiciones de seguridad.

En estas circunstancias, la Oficina Nacional de Seguridad (ONS) ha elaborado un nuevo procedimiento simplificado para la acreditación de sistemas TIC para el manejo de información clasificada de grado RESTRICTED/DIFUSIÓN LIMITADA².

Este procedimiento, no obstante, no simplifica el conjunto de acciones de seguridad en los sistemas TIC necesarias para la obtención de la declaración de cumplimiento del Centro Criptológico Nacional.

¹ Solo en aquellos organismos que así lo hayan desarrollado en sus respectivas políticas de seguridad de la información clasifica.

² En esta guía, el término RESTRICTED hace referencia a la información NATO RESTRICTED, EU RESTRICTED y ESA RESTRICTED y el término DIFUSIÓN LIMITADA es su equivalente nacional solo en aquellos organismos que así lo hayan desarrollado en sus respectivas políticas de seguridad de la información clasificada.

1. ÁMBITO DE APLICACIÓN

Esta guía es de aplicación para entidades que soliciten la acreditación de sistemas TIC para el manejo de información clasificada de grado RESTRICTED/DIFUSIÓN LIMITADA a través del procedimiento simplificado.

Este procedimiento se apoya en la figura del oficial de seguridad/jefe de seguridad del órgano de control (OC) de la entidad, que se deberá comprometer a establecer y mantener las condiciones de seguridad para la información clasificada de este grado en la utilización del sistema TIC.

2. TRAMITACIÓN DE LA SOLICITUD

El procedimiento consta de los siguientes pasos:

1. **Solicitud de número de expediente de acreditación de sistemas TIC (NEASTIC).** Corresponde al oficial de seguridad/jefe de seguridad del OC cumplimentar el formulario de solicitud³ y remitirlo al correo electrónico de la ONS cis@ons.cni.es.

Admitida la solicitud, la ONS comunicará al interesado el NEASTIC asignado al sistema, para su identificación a lo largo de su vida útil.

2. **Tramitación de la conformidad del Centro Criptológico Nacional (CCN).** Para la obtención de la declaración de cumplimiento que habilita al sistema para obtener la acreditación de seguridad, el oficial de seguridad/jefe de seguridad deberá llevar a cabo las acciones y trabajos definidos utilizando los distintos mecanismos técnicos y normativos especificados y habilitados por el CCN para tal fin.

En caso de requerir alguna aclaración, se recomienda contactar través de la cuenta de correo electrónico del CCN acreditacion.ccn@cni.es.

3. **Cumplimentación de la declaración responsable** (modelo en anexo). El oficial de seguridad/jefe de seguridad del OC firmará electrónicamente este documento, en el que asume las siguientes obligaciones en relación con la protección de la información clasificada:

- Se responsabiliza de que los procedimientos y la seguridad física de los locales que albergan los sistemas TIC cumplen con las condiciones de seguridad establecidas por la normativa vigente, incluido lo dispuesto por el Esquema Nacional de Seguridad.
- Adicionalmente, para manejar este tipo de información clasificada se podrán contemplar escenarios alternativos que, a través de la implementación de medidas compensatorias de seguridad y complementarias de vigilancia, permitan reducir al mínimo el riesgo de pérdida o comprometimiento de la información.

³ Documento publicado en la página web www.cni.es/ons.

- Se compromete a impartir la formación sobre el manejo de información clasificada RESTRICTED/DIFUSIÓN LIMITADA al personal de la entidad que acceda al sistema TIC.
4. **Remisión de la declaración responsable y la declaración de conformidad del CCN** a la dirección de correo electrónico cis@ons.cni.es.
 5. **Acreditación del sistema TIC.** La ONS, una vez analizada y validada la documentación aportada, tramitará ante la Autoridad Delegada para la Seguridad de la Información Clasificada la firma del certificado de acreditación, que se remitirá al solicitante.

ANEXO. Modelo de declaración responsable

[NOMBRE Y APELLIDOS], con DNI [inserte número], en calidad de oficial de seguridad/jefe de seguridad [señálese lo que proceda] de [ÓRGANO DE CONTROL (si procede)] de [ORGANISMO/EMPRESA], realizo la siguiente declaración responsable:

- a) El sistema con número de expediente [inserte número] denominado [nombre del sistema] cumple con las medidas y procedimientos de seguridad descritos en la documentación de seguridad siguiente:

[inserte la referencia interna, como mínimo, de los procedimientos operativos de seguridad (POS)].
- b) Las personas que acceden a información clasificada hasta el grado RESTRICTED/DIFUSIÓN LIMITADA han sido instruidas en la normativa aplicable y han recibido concienciación.
- c) Los locales que albergan elementos del sistema están declarados como zona administrativa de protección (ZAP) o acreditados como zona de acceso restringido (ZAR), o bien se adoptan las medidas de seguridad complementarias descritas en los POS⁴:

[inserte referencia de las ZAP/ZAR que procedan]
- d) El Centro Criptológico Nacional (CCN) ha emitido su conformidad sobre las medidas técnicas y procedimentales de este sistema, la cual se adjunta a esta declaración.

Anexo: Declaración de conformidad del CCN

⁴ En el caso de escenario alternativo, este tendrá que estar claramente descrito en los POS referenciados en el apartado a).