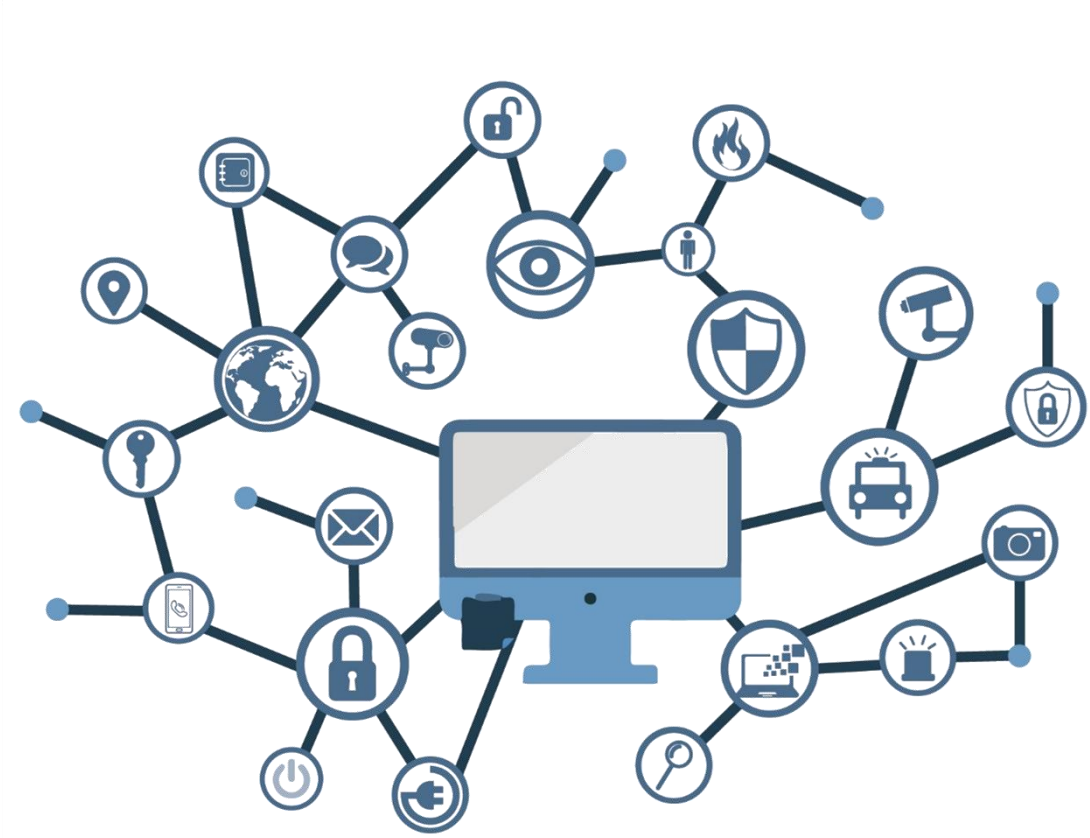
centro criptológico nacional

Guía de Seguridad de las TIC
Anexo A CCN-STIC 2010

Plantilla para la Declaración de Seguridad de Evaluación de Productos en la Nube (CICLON)



Marzo 2026

Edita:

centro criptológico nacional

© Centro Criptológico Nacional, 2026

Fecha de Edición: marzo 2026

CCN
c=ES, l=MADRID, o=CCN, ou=SELLO ELECTRONICO, 2.5.4.97=VATES-S2800155J, serialNumber=S2800155J, cn=CCN
2026.03.27 12:36:23 +01'00'

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

CONTROL DE VERSIÓN

Versión	Comentario	Fecha
1.0	Versión inicial	03/2026

ÍNDICE

1 INTRODUCCIÓN 4
1.1 INFORMACIÓN DEL SOLICITANTE, TOE Y EVALUACIÓN 4
1.2 METODOLOGÍA Y CRITERIOS DE LA EVALUACIÓN 4
2 DESCRIPCIÓN DEL TOE 5
2.1 DESCRIPCIÓN FUNCIONAL DEL TOE 5
2.2 IDENTIFICACIÓN DE LAS GUÍAS DE USO Y CONFIGURACIÓN SEGURAS DEL TOE 5
2.3 DESCRIPCIÓN DEL MODO DE USO DEL TOE 5
3 ENTORNO DE EJECUCIÓN 6
3.1 DESCRIPCIÓN DEL ENTORNO DE EJECUCIÓN 6
3.2 COMPONENTES DE INTEGRACIÓN (OPCIONAL) 6
4 PROBLEMA DE SEGURIDAD 7
4.1 HIPÓTESIS SOBRE EL ENTORNO DE EJECUCIÓN 7
4.2 ACTIVOS SENSIBLES A PROTEGER 7
4.3 DESCRIPCIÓN DE LAS AMENAZAS 7
5 FUNCIONES DE SEGURIDAD 9
5.1 FS. NOMBRE DE LA FUNCION DE SEGURIDAD 9
6 REFERENCIAS 11
7 ACRÓNIMOS 12

1 INTRODUCCIÓN

Este documento es una plantilla de referencia para redactar la Declaración de Seguridad del servicio en la nube para la Evaluación de Productos en la Nube (CICLON).

1.1 INFORMACIÓN DEL SOLICITANTE, TOE Y EVALUACIÓN

Nombre del solicitante	
Nombre del desarrollador	
Nombre del TOE	
Tipo de evaluación	CICLÓN versión 1
Esfuerzo estimado (Jornadas)	
Guías y versiones (opcional)	
Familia de la taxonomía de la guía CCN-STIC-140	

1.2 METODOLOGÍA Y CRITERIOS DE LA EVALUACIÓN

CCN-STIC-2010	Metodología de Evaluación de Productos en la Nube (CICLON)

2 DESCRIPCIÓN DEL TOE

2.1 DESCRIPCIÓN FUNCIONAL DEL TOE

Se incluirá una descripción clara y concisa del TOE en la nube incluyendo en lenguaje natural sus componentes principales y las principales funciones de seguridad que son objeto de la evaluación.

2.2 IDENTIFICACIÓN DE LAS GUÍAS DE USO Y CONFIGURACIÓN SEGURAS DEL TOE

Se incluirá una tabla en la que se identificarán las guías de uso y configuración (cuando sean necesarias) que permiten operar al TOE en su configuración evaluada. Estas guías deberán poder ser accesibles para los consumidores del servicio en la nube.

En la tabla se incluirá al menos el tipo de documento, nombre, y un resumen criptográfico del documento.

Tipo de Documento	Nombre del Documento	HASH (SHA256)

En caso de que no se dispongan de guías de uso y configuración seguras esta sección deberá indicar claramente que no existen dichas guías y cuál es su motivo.

2.3 DESCRIPCIÓN DEL MODO DE USO DEL TOE

En caso de que se deba configurar algún parámetro específico del TOE para su uso debe usarse esta sección para dejarlo reflejado.

En caso de que el servicio ofrezca las funcionalidades necesarias para cumplir con su objetivo de seguridad sin necesidad de configurar ningún parámetro, se deberá dejar reflejado esta situación.

3 ENTORNO DE EJECUCIÓN

3.1 DESCRIPCIÓN DEL ENTORNO DE EJECUCIÓN

La Declaración de Seguridad debe especificar el entorno operacional que se requiere para hacer posible la ejecución del servicio en la nube.

El entorno deberá indicar el proveedor de la plataforma en la nube donde se despliegue el TOE y todos los componentes necesarios para que el TOE pueda ofrecer su servicio.

Se deberá incluir un diagrama que muestre a alto nivel el entorno del TOE (este diagrama puede ser una versión simplificada del Documento de Arquitectura del Servicio, DAS).

3.2 COMPONENTES DE INTEGRACIÓN (OPCIONAL)

En los casos en los que un requisito de seguridad esté cubierto por otro producto evaluado o en proceso de evaluación, dicho producto deberá describirse en este apartado como componente de Integración y las características de la integración e indicar que requisitos de seguridad cubre (Ej. ADM.1).

4 PROBLEMA DE SEGURIDAD

4.1 HIPÓTESIS SOBRE EL ENTORNO DE EJECUCIÓN

La Declaración de Seguridad deberá incluir las hipótesis sobre el entorno en el que se ejecutará el producto, determinando el alcance de la evaluación. Dependiendo de las hipótesis que se declaren sobre el entorno de ejecución, el TOE puede verse limitado en su capacidad de proporcionar algunas las funcionalidades de seguridad declaradas.

Las posibles hipótesis sobre el entorno de ejecución pueden ser relativas a medidas de seguridad física, procedimentales, seguridad en el personal o seguridad lógica que se apliquen en el entorno de ejecución.

Se deberá indicar cada una de las hipótesis sobre el entorno de ejecución de acuerdo con la siguiente tabla:

Hipótesis	Descripción

4.2 ACTIVOS SENSIBLES A PROTEGER

La Declaración de Seguridad debe describir los activos que las funciones de seguridad del TOE protegen. Deben especificarse las propiedades de seguridad que se protegen para cada uno de los activos (confidencialidad, integridad, disponibilidad, autenticidad y/o trazabilidad).

Para proteger los activos enumerados, el producto puede hacer uso de otra información que deberá ser considerada un activo en sí misma.

Se deberá indicar cada uno de los activos sensibles a proteger de acuerdo con la siguiente tabla:

Activo	Descripción	Dimensión de Seguridad

4.3 DESCRIPCIÓN DE LAS AMENAZAS

La Declaración de Seguridad debe describir las amenazas que se pretenden mitigar con las funciones de seguridad del TOE. Una amenaza se puede caracterizar con los siguientes elementos:

a) Un actor (usuario autorizado, administrador, usuario malintencionado, atacante externo, etc.).
b) La acción adversa que ejecutaría el actor (inyección de datos, acceso malicioso, extracción de información, etc.).
c) El activo o activos a los que afectaría la acción adversa.

Se deberá indicar cada una de las amenazas de acuerdo con la siguiente tabla:

Amenaza	Descripción	Activo

5 FUNCIONES DE SEGURIDAD

La Declaración de Seguridad debe incluir las funciones de seguridad específicas que el producto desplegado en la nube ofrece. Estas funciones deben describirse en lenguaje natural.

La especificación de las funciones de seguridad debe ser suficientemente completa como para que el evaluador entienda, sin lugar a duda, cómo ha sido implementada la funcionalidad, es decir, se debe describir a alto nivel cómo el TOE proporciona la funcionalidad de seguridad específica.

Las funciones de seguridad deben estar presentes en el modo de uso previsto del TOE y dentro del alcance de la evaluación. Es decir, no se describirán las funciones de seguridad que no van a ser evaluadas.

El fabricante puede no querer incluir en la Declaración de Seguridad información sensible o propietaria, ya que se trata de un documento público. En estos casos, se incluirá en el Anexo B de la guía CCN-STIC-2010 Diseño de Arquitectura del Servicio (DAS) el detalle esperado sobre la implementación de las funciones de seguridad sensibles o propietarias y se referenciará dicho anexo durante la Declaración de Seguridad. En todo caso, un consumidor del servicio evaluado tiene que ser capaz de conocer el alcance de la evaluación del servicio en la nube con la lectura de la Declaración de Seguridad, por lo que el laboratorio verificará que la información proporcionada en la Declaración de Seguridad permite conocer las funcionalidades de seguridad certificadas.

El método de verificación de cada uno de los requisitos a evaluar se define mediante el siguiente criterio:

a) **Comprobación Indirecta (CI):** modalidad aplicable cuando el laboratorio no puede comprobar directamente la función de seguridad.
b) **Comprobación Directa (CD):** modalidad aplicable cuando el laboratorio puede realizar las pruebas de la función de seguridad sobre el TOE, incluyendo pruebas funcionales y pruebas de penetración.
c) **Integración (Int.):** modalidad aplicable cuando la función de seguridad es cubierta por un componente definido en el entorno como elemento de integración y ha sido configurado por el propio fabricante del producto.

Se deberá indicar en cada uno de los requisitos a evaluar cómo van a ser probados en la evaluación de acuerdo con la siguiente tabla:

5.1 FS. NOMBRE DE LA FUNCION DE SEGURIDAD

En el título de esta sección se indicará el nombre de la Función de seguridad correspondiente. Deberán existir tantas secciones como funciones de seguridad.

ID Requisito	Método de Verificación	Descripción

6 REFERENCIAS

En esta sección se deberán referenciar todos aquellos documentos que hayan sido empleados para el análisis de la justificación de los diferentes requisitos.

[CCN-STIC-2010]	Definición de Proceso de Evaluación de Servicios en la Nube (Ciclón)
[CCN-STIC-140-X]	Taxonomía de referencia para servicios de Seguridad TIC

7 ACRÓNIMOS

CCN	Centro Criptológico Nacional
CNI	Centro Nacional de Inteligencia
ENS	Esquema Nacional de Seguridad
LINCE	Certificación Nacional Esencial de Seguridad
MCF	Módulo Revisión de Código Fuente
MEB	Módulo de Evaluación Biométrica
MEC	Módulo de Evaluación Criptográfica
ST	Security Target - Declaración de Seguridad
STIC	Seguridad de las Tecnologías de la Información y Comunicación
TIC	Tecnologías de la Información y Comunicación
TOE	Target Of Evaluation – Objeto a evaluar
DAS	Diseño Arquitectura del Servicio