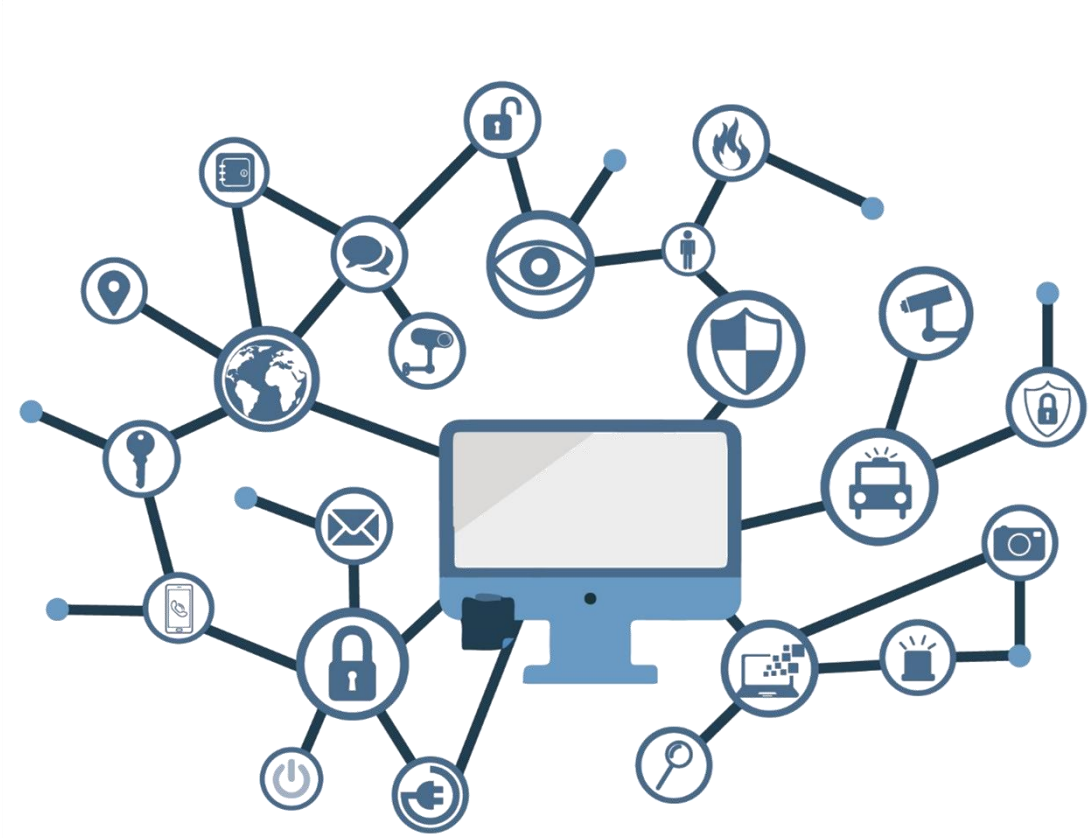
centro criptológico nacional

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

Plantilla del Informe Técnico de Evaluación de Productos en la Nube (CICLON)



Abril 2026

Edita:

centro criptológico nacional

Fecha de Edición: abril de 2026

centro criptológico nacional

CCN
c=ES, l=MADRID, o=CCN,
ou=SELLO ELECTRONICO,
2.5.4.97=VATES-S2800155J,
serialNumber=S2800155J,
cn=CCN
2026.04.24 11:09:16 +02'00'

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

ÍNDICE

1. Introducción

Este documento es una plantilla de referencia para la redacción del Informe Técnico de Evaluación (ETR) de un servicio en la nube en el marco de la Evaluación de Productos en la Nube (CICLON). La plantilla establece el contenido mínimo que debe incluirse en este ETR.

Su contenido deberá adaptarse y completarse en función de la tipología, alcance y características del producto o servicio objeto de evaluación.

1.1 Información del Informe Técnico de Evaluación

Referencia ETR	Identificador único proporcionado por el laboratorio
Versión ETR	Versión del documento
Laboratorio Evaluador	Nombre Laboratorio Dirección de las dependencias donde se realiza la evaluación
Autor o autores	Nombre del autor del ETR
Revisado por	Nombre del revisor del ETR
Aprobado por	Nombre del responsable del ETR
Fecha	Fecha de modificación del ETR
Código de expediente	Identificador único proporcionado por el CPSTIC
Taxonomía del producto según CCN- STIC 140	Ej.- HERRAMIENTAS ANTI-VIRUS/EPP (ENDPOINT PROTECTIONPLATFORM) o NO APLICA[1] [2]

[1] En caso de que la declaración de seguridad no cumpla estrictamente con todos los requisitos marcados en los anexos definidos por los responsables del CPSTIC en la CCN-STIC-140.
[2] La declaración de seguridad deberá ser aprobada por parte de los responsables del CPSTIC.

1.2 Información del solicitante del TOE

Datos del Solicitante (Nombre y Dirección)	
Datos de contacto del Solicitante (Nombre del contacto y e-mail)	
Datos del Desarrollador (Nombre y Dirección)	
Nombre del TOE	

2. Descripción del TOE

El evaluador deberá indicar que la información incluida en esta sección ha sido obtenida a partir de la Declaración de Seguridad.

2.1 Descripción funcional del TOE

Se incluirá una descripción clara y concisa del TOE, en la que se identificarán, en lenguaje natural, sus componentes principales y todas funciones de seguridad que constituyen el TOE.

2.2 Inventario de las funciones de seguridad

Las funciones de seguridad recogidas en la Declaración de Seguridad deberán describirse y clasificarse según su funcionalidad. Asimismo, a cada una de ellas se le asignará un identificador único, que será utilizado de forma consistente a lo largo del informe para referenciar dicha función.

3. Entorno de ejecución

El evaluador deberá indicar que la información incluida en esta sección ha sido obtenida a partir de la Declaración de Seguridad.

3.1 Descripción del entorno de ejecución

Se deberá especificar el entorno operacional requerido para posibilitar la ejecución del producto.

3.2 Hipótesis sobre el entorno de ejecución

Se incluirán las hipótesis relativas al entorno en el que se ejecutará el producto. Asimismo, a cada una de ellas se le asignará un identificador único, que será utilizado de forma consistente a lo largo del informe para referenciar dichas hipótesis.

4. Resumen ejecutivo de la evaluación

Esta sección incluirá un resumen ejecutivo de la evaluación, en el que se recogerán los aspectos más relevantes de su desarrollo, así como los resultados obtenidos. En particular, deberán reflejarse las no conformidades detectadas, los informes de observación emitidos, las evidencias recibidas y aquellos hitos que resulten significativos durante el proceso de evaluación.

La información deberá presentarse siguiendo un criterio cronológico, de modo que se facilite la comprensión de la secuencia de actividades realizadas y de la evolución de la evaluación.

La finalidad de este apartado es ofrecer una visión sintética y ordenada del proceso de evaluación, permitiendo conocer, a alto nivel, su desarrollo y los hechos más relevantes asociados al mismo.

5. Veredicto de la evaluación

El evaluador deberá indicar en el Informe Técnico de Evaluación (ETR) el Porcentaje de Garantía de Evaluación (PGE), de conformidad con lo establecido en la metodología CICLON [CCN-STIC-2010]. Dicho porcentaje únicamente será válido cuando se cumplan de forma concurrente las siguientes condiciones:

1. La funcionalidad de seguridad del TOE cumple lo establecido en la Declaración de Seguridad y el TOE no es vulnerable a ninguno de los ataques descritos en [CCN-ITC-003].
2. Todas las actividades de evaluación definidas en la metodología han obtenido el veredicto de **PASA**.
3. No se ha superado el tiempo máximo de evaluación y las evidencias aportadas cumplen los requisitos esperados.

Si cualquiera de estas condiciones no se cumple, el veredicto de la evaluación será **FALLA** y, en consecuencia, el **Porcentaje de Garantía de Evaluación (PGE)** asignado será **0**, con independencia del porcentaje que pudiera haberse calculado.

6. Acceso y configuración del entorno de pruebas

La información que deberá incluirse en esta sección es, como mínimo, la siguiente:

a) Identificación del evaluador o de los evaluadores responsables de la realización de esta actividad.
b) Fecha o periodo de ejecución de la actividad.
c) Descripción del entorno de pruebas facilitado para la evaluación, indicando si se trata de un entorno de producción o de un entorno de preproducción equivalente, así como las condiciones de acceso al TOE, incluyendo, en su caso, la existencia de acceso a través de WAF.
d) Descripción de la configuración aplicada al TOE durante la evaluación, con referencia expresa a la configuración o configuraciones definidas en la Declaración de Seguridad, así como identificación de las no conformidades detectadas en relación con el acceso y la configuración del entorno de pruebas.
e) Resultado de las tareas realizadas por el evaluador en esta etapa, incluyendo, al menos:
    1. La comprobación de que el solicitante ha proporcionado el acceso requerido al entorno de pruebas.
    2. La comprobación de que el producto puede configurarse de acuerdo con la configuración o configuraciones descritas en la Declaración de Seguridad.
    3. La comprobación de la inexistencia de no conformidades en el acceso y configuración del entorno de pruebas.
f) Porcentaje de Garantía de Evaluación correspondiente a esta etapa, indicando la fórmula aplicada, los valores asignados a las variables empleadas y la justificación del resultado obtenido.
g) Esfuerzo dedicado por el evaluador para acceder al entorno de pruebas y configurar el TOE de acuerdo con las instrucciones recogidas en la Declaración de Seguridad.

7. Análisis de conformidad

7.1 Análisis de la Declaración de Seguridad

La información que deberá incluirse en esta sección es, como mínimo, la siguiente:

a) Identificación del evaluador o de los evaluadores responsables de la realización de esta actividad.
b) Fecha o periodo de ejecución de la actividad.
c) Referencia al identificador y versión de la Declaración de Seguridad evaluada.
d) Resultado de las tareas realizadas por el evaluador en esta etapa, incluyendo la justificación del veredicto asignado para cada una de ellas. En particular, deberá quedar constancia de las comprobaciones efectuadas sobre:
    1. La presencia de los elementos descritos en el [Anexo A CCN-STIC-2010].
    2. La identificación del nombre del TOE.
    3. La verificación del uso de la versión de la Declaración de Seguridad validada por los responsables de CPSTIC.
    4. La claridad y suficiencia de la descripción del TOE.
    5. La delimitación entre el TOE y su entorno operacional, así como la descripción del soporte que este último presta a su ejecución.
    6. La coherencia del problema de seguridad, incluyendo activos, hipótesis, amenazas y funciones de seguridad.
    7. El nivel de detalle con el que se describen las funciones de seguridad implementadas en el TOE.
    8. La inexistencia de no conformidades en relación con el análisis de la Declaración de Seguridad.
e) Listado de las no conformidades detectadas, indicando para cada una de ellas su descripción, justificación y, en su caso, su impacto sobre la evaluación.
f) Porcentaje de Garantía de Evaluación correspondiente a esta etapa, incluyendo el detalle de la fórmula aplicada, los valores utilizados para sus variables y la justificación del resultado obtenido.
g) Esfuerzo dedicado por el evaluador al análisis de la Declaración de Seguridad.

7.2 Análisis del Documento de Arquitectura del Sistema

La información que deberá incluirse en esta sección es, como mínimo, la siguiente:

a) Identificación del evaluador o de los evaluadores responsables de esta actividad.
b) Fecha o periodo de ejecución de la actividad.
c) Referencia al identificador y versión del Documento de Arquitectura del Servicio (DAS) analizado.
d) Resultado de las comprobaciones realizadas sobre el DAS, incluyendo, al menos:

1. La verificación de que el documento es completo y se corresponde con el TOE evaluado.
2. La verificación de que el DAS define la posibilidad de acceso al TOE evitando el WAF.
3. La comprobación de la correcta delimitación entre los elementos que forman parte del TOE y aquellos que pertenecen al entorno operacional, así como de la adecuada descripción del soporte que este último presta a la ejecución del TOE.
4. La comprobación de la inexistencia de no conformidades en relación con el Documento de Arquitectura del Servicio.

e) Listado de las no conformidades detectadas, indicando para cada una de ellas su descripción, justificación y, en su caso, su impacto sobre la evaluación.
f) Conclusión del evaluador sobre la suficiencia y adecuación del DAS para la evaluación.
g) Esfuerzo dedicado por el evaluador al análisis de la Declaración de Seguridad.

7.3 Pruebas funcionales

Esta sección recogerá los resultados de las pruebas funcionales realizadas sobre las funciones de seguridad definidas en la Declaración de Seguridad (DS), de conformidad con la metodología CICLON.

La información que deberá incluirse en esta sección es, como mínimo, la siguiente:

a) Identificación del evaluador o de los evaluadores responsables de esta actividad.
b) Fecha o periodo de ejecución de las pruebas.
c) Identificación de las funciones de seguridad objeto de prueba, indicando para cada una de ellas si su verificación se ha realizado mediante Comprobación Directa (CD) o Comprobación Indirecta (CI), así como la justificación del criterio de designación (CD o CI) aplicado.
d) Información detallada de cada prueba realizada, incluyendo su objetivo, escenario, procedimiento, resultados esperados, resultados obtenidos y conclusión.
e) Listado de las no conformidades detectadas y su asociación con las pruebas, funciones de seguridad o evidencias correspondientes.
f) Esfuerzo dedicado a la ejecución y análisis de las pruebas funcionales.

Para cada función probada, el evaluador deberá cumplimentar la siguiente plantilla de “Caso de Prueba”:

Código de la prueba:	**(Ej.- PF_0xx)**
Función de seguridad probada:	**Evaluador:**
	Objetivo de la prueba:
Escenario de prueba:	
Contexto	
Tipo de comprobación: CD / CI	**Tipo de prueba:** Estándar / Manipulación (tampering) / Elusión (bypassing)
Procedimiento	
Resultados esperados	
Resultados obtenidos	
Conclusión y veredicto:	

Ejemplo:

Código de la prueba:	
Función de seguridad probada: Protección del servicio web frente a intentos de inyección SQL en parámetros de entrada HTTP/HTTPS	**Evaluador:** PF_WAF_001
	Objeto de la prueba: Verificar, mediante Comprobación Directa (CD), que el TOE bloquea intentos de inyección SQL dirigidos a parámetros de entrada de la aplicación y que dicha protección no puede ser eludida mediante variaciones de codificación, normalización o ubicación del vector de entrada.
Escenario de prueba: Entorno de preproducción equivalente al de producción. Aplicación web corporativa publicada a través de un WAF en modo bloqueo, con terminación TLS en el frontal y encaminamiento hacia backend de aplicación y base de datos.	
Contexto	
Tipo de comprobación: CD	**Tipo de prueba:** Bypassing
Procedimiento	

1. Verificar que la política de protección frente a inyecciones se encuentra habilitada en el WAF para los métodos GET y POST, así como para parámetros de consulta, formularios y cuerpos JSON.
2. Enviar peticiones legítimas de referencia para confirmar el comportamiento normal del servicio y disponer de una línea base de funcionamiento.
3. Ejecutar un conjunto de peticiones maliciosas controladas con patrones de inyección SQL sobre distintos puntos de entrada de la aplicación.
4. Repetir la prueba utilizando variantes semánticamente equivalentes orientadas a la elusión del mecanismo de seguridad, incluyendo cambios de codificación, representación alternativa de caracteres reservados, alteraciones de mayúsculas y minúsculas, inserción de espacios o separadores, y envío del vector en distintos puntos de entrada de la petición.
5. Comprobar si el WAF bloquea las solicitudes antes de que alcancen el backend, y verificar adicionalmente en los registros del WAF, de la aplicación y de la base de datos si se ha producido procesamiento parcial o completo de alguna de las peticiones enviadas.
6. Registrar las reglas disparadas, el identificador del evento, la marca temporal, el origen de la petición y el recurso afectado.

Resultados esperados

- El TOE debe identificar y bloquear las peticiones maliciosas dirigidas a explotar inyección SQL.
- La protección debe mantenerse ante variantes de evasión basadas en codificación, normalización o ubicación alternativa del vector.
- Las peticiones bloqueadas no deben alcanzar la lógica de aplicación ni generar ejecución de consultas en el backend.
- El evento debe quedar registrado con suficiente detalle para su trazabilidad y análisis posterior.
- No debe observarse fuga de información, mensajes de error reveladores ni alteración del comportamiento funcional del servicio.

Resultados obtenidos

Las peticiones de referencia fueron procesadas correctamente. El WAF bloqueó las variantes directas de inyección SQL enviadas en parámetros de consulta y formularios HTTP. Sin embargo, durante la prueba de bypassing se observó que una variante equivalente introducida en un atributo anidado del cuerpo JSON no fue bloqueada por el TOE y alcanzó la aplicación backend, que devolvió un error controlado de validación.

[Incluir evidencias obtenidas durante la realización de procedimiento]

La revisión de evidencias mostró que el WAF registró la solicitud como evento anómalo, pero no aplicó la acción de bloqueo al no encontrarse habilitada la inspección profunda del cuerpo JSON para dicho recurso. No se observaron evidencias de ejecución satisfactoria de la consulta maliciosa ni exfiltración de

datos, pero sí una elusión parcial del mecanismo preventivo declarado.

Conclusión y veredicto:

La función de seguridad se considera implementada de forma parcial. El TOE demuestra capacidad de detección y bloqueo frente a intentos directos de inyección SQL, pero la prueba de bypassing evidencia que existen escenarios de evasión en entradas JSON no inspeccionadas con la misma profundidad que los parámetros convencionales. En consecuencia, el resultado de la prueba es **FALLA**, al haberse demostrado una vía de elusión del mecanismo de seguridad declarado.

7.4 Análisis criptográfico de las comunicaciones

La información que deberá incluirse en esta sección es, como mínimo, la siguiente:

a) Identificación del evaluador o de los evaluadores responsables de esta actividad.
b) Fecha o periodo de ejecución de las pruebas.
c) Identificación y definición de los canales de comunicación. El evaluador deberá documentar los canales de comunicación externos e internos respecto al TOE que se encuentran definidos e identificados en la Declaración de Seguridad, verificando que dicha identificación es inequívoca y completa.
d) Coherencia entre documentos. El evaluador deberá dejar constancia del resultado de la verificación de coherencia entre lo establecido en la Declaración de Seguridad y lo declarado en el Documento de Arquitectura del Servicio, indicando las discrepancias detectadas, si las hubiera.
e) Resultado del análisis criptográfico. Descripción detallada del proceso de análisis llevado a cabo, incluyendo las herramientas utilizadas, los canales analizados, los protocolos y algoritmos identificados, los tamaños de clave, los modos de operación y las evidencias obtenidas. Se deberá indicar expresamente si los mecanismos criptográficos identificados son clasificados como Recomendados, No Recomendados (NR) o Heredados (L) a fecha de realización de la evaluación.
f) Listado de las no conformidades detectadas, indicando para cada una de ellas su descripción, justificación y, en su caso, su impacto sobre la evaluación.
g) Porcentaje de Garantía resultante de esta etapa. Valor calculado por el evaluador mediante la fórmula establecida en la metodología, con indicación explícita de los valores utilizados en el cálculo.
h) Esfuerzo dedicado a la ejecución y análisis de las pruebas funcionales.

8. Pruebas de penetración del TOE

La información que debe incluirse en esta sección es, como mínimo, la siguiente:

a) Identificación del evaluador o de los evaluadores responsables de esta actividad.
b) Fecha o periodo de ejecución de las pruebas.
c) Ejecución de pruebas de penetración. El evaluador deberá ejecutar, como mínimo, el conjunto de pruebas descrito en la Instrucción Técnica de Evaluación de seguridad en entornos web y nube [CCN-ITC-003].
d) Listado de las no conformidades detectadas, indicando para cada una de ellas su descripción, justificación y, en su caso, su impacto sobre la evaluación. Se deberá verificar expresamente que ninguna no conformidad tiene origen en un ataque que haya tenido éxito.
e) Esfuerzo dedicado a realizar las pruebas de penetración.

Para cada prueba de penetración realizada, el evaluador deberá rellenar la siguiente plantilla de "Caso de Prueba":

Código de la prueba:	(Ej.- PT_0xx)
Vulnerabilidad de [CCN-ITC-003] asociada:	**Evaluador:**
	Objetivo de la prueba:
Escenario de ataque:	
Procedimiento	
Resultados esperados	
Resultados obtenidos	
Conclusión y veredicto:	

9. Cálculo del porcentaje de garantía de evaluación (PGE)

La información que deberá incluirse en esta sección es, como mínimo, la siguiente:

a) Porcentajes de Garantía Parciales. El evaluador deberá registrar los Porcentajes de Garantía obtenidos en cada una de las etapas anteriores de la fase de evaluación, indicando explícitamente los valores de PGE1, PGE3 y PGE5, así como los factores de peso asociados a cada uno de ellos (w1, w3, w5).

b) Porcentaje de Garantía de Evaluación (PGE). Valor calculado por el evaluador mediante la fórmula establecida en la Metodología de Evaluación de Productos en la Nube [CCN-STIC-2010], con indicación explícita de los valores utilizados en el cálculo.

10. Consideraciones al Procedimiento de Empleo Seguro (PES)

Esta sección deberá contener las consideraciones sobre el funcionamiento seguro del TOE.

El evaluador deberá documentar todas las consideraciones sobre el funcionamiento seguro identificadas a lo largo de la evaluación que deban ser incorporadas a la guía de Procedimiento de Empleo Seguro (PES).

Dichas consideraciones deben ser necesarias para que el TOE pueda satisfacer la totalidad de las funciones de seguridad definidas en su Declaración de Seguridad.

11. Referencias

[CC]	Common Criteria for Information Technology Security Evaluation. Se debe considerar su última versión aprobada y publicada en la web del Organismo de Certificación (https://oc.ccn.cni.es).
[CCN-STIC-2010]	Metodología de Evaluación de Productos en la Nube (CICLON).
Anexo A [CCN-STIC-2010]	Plantilla para la Declaración de Seguridad de la Evaluación de Productos en la Nube (CICLON).
Anexo B [CCN-STIC-2010]	Plantilla para el Documento de Arquitectura del Servicio de la Evaluación de Productos en la Nube (CICLON).
Anexo C [CCN-STIC-2010]	Plantilla del Informe Técnico de Evaluación de Productos en la Nube (CICLON).
Anexo D [CCN-STIC-2010]	Plantilla del Informe Técnico de monitorización de Productos en la Nube (CICLON).
CCN-ITC-003	Instrucción Técnica de Evaluación de seguridad en entornos web y nube.
FOR-CIC-001	Formulario de solicitud de evaluación de Productos en la Nube (CICLON).
PO-006	Procedimiento de acreditación de laboratorios.
PO-CIC-005	Procedimiento de certificación de productos en la nube.
PO-CIC-010	Procedimiento de autorización de laboratorios para evaluaciones CICLON.
SBOM CycloneDX	Estándar para composición software.

12. Acrónimos

CCN	Centro Criptológico Nacional
CD	Comprobación Directa
CI	Comprobación Indirecta
CICLON	Certificación Iterativa Cloud Nacional
CPSTIC	Catálogo de Productos y Servicios STIC
DAS	Documento de Arquitectura del Servicio
DIAS	Diagrama de Arquitectura del Servicio
DS	Declaración de Seguridad
ENS	Esquema Nacional de Seguridad
ENECSTI	Esquema Nacional de Evaluación y Certificación de Seguridad TIC
ETR	Informe Técnico de Evaluación
EUCC	Esquema Europeo de Certificación (European Cybersecurity Certification Scheme)
ITC	Instrucción Técnica
MTR	Informe Técnico de Monitorización
PGC	Porcentaje de Garantía Compuesto
PGE	Porcentaje de Garantía de Evaluación
PGM	Porcentaje de Garantía de Monitorización
SBOM	*Software Bill of Materials*
STIC	Seguridad de las Tecnologías de la Información y las Comunicaciones
TOE	Producto objeto de evaluación (*Target of Evaluation*)
WAF	*Web Application Firewall*