centro criptológico nacional

# Guía de Seguridad de las TIC
# CCN-STIC 2010

# Metodología de Evaluación de Productos en la Nube (CICLON)

Marzo 2026

Edita:

centro criptológico nacional



Fecha de edición: Marzo de 2026



**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**

## CONTROL DE VERSIÓN

| Versión | Comentario | Fecha |
|---|---|---|
| 1.0 | Versión inicial | Marzo 2026 |

# ÍNDICE

# 1. OBJETO DEL DOCUMENTO

El Centro Criptológico Nacional (CCN) ha desarrollado la Metodología de Evaluación de Productos en la Nube (CICLON) como respuesta a la necesidad de evaluar productos desplegados en la nube para todos los niveles de amenaza establecidos por el Cybersecurity Act (Reglamento (EU) 2019/881 del Parlamento Europeo y del Consejo del 17 de abril 2019 sobre ENISA).

Este documento define la Metodología de Evaluación de Productos en la Nube (CICLON) para un producto de seguridad de las Tecnologías de la Información y Comunicaciones (TIC), incluyendo la definición de los actores involucrados, los diferentes elementos de entrada en el proceso de evaluación, las etapas que lo componen, así como las características específicas que lo distinguen.

La evaluación de seguridad de un producto en la nube es el único medio objetivo que permite valorar su capacidad para manejar información con el nivel de seguridad manifestado por el fabricante en su Declaración de Seguridad (DS).

Esta metodología define el procedimiento necesario para que una tercera parte confiable y técnicamente capacitada pueda llevar a cabo la evaluación de seguridad TIC.

Las principales características de la evaluación son las siguientes:

a) Está compuesta por dos fases diferenciadas: una fase de evaluación inicial y una fase de monitorización continua, de naturaleza periódica.
b) La estimación del esfuerzo de la evaluación dependerá de la complejidad del servicio.
c) Contempla la automatización de las actividades asociadas al proceso de evaluación.
d) El resultado de la evaluación se expresa mediante el Porcentaje de Garantía Compuesto (PGC), valor que integra los factores derivados de ambas fases.
e) El valor del PGC será objeto de actualización periódica como resultado de las sucesivas iteraciones de la fase de monitorización.

## 2. OBJETIVO DE LA METODOLOGÍA

La metodología de evaluación CICLON ha sido desarrollada en respuesta a la necesidad de evaluar productos desplegados en entornos de nube. Las metodologías de evaluación tradicionales —tales como LINCE, CC o EUCC— no resultan aplicables a dichos entornos, dado que requieren, entre otros, el acceso físico al producto evaluado o la existencia de una versión estática del mismo durante todo el periodo de evaluación.

La evaluación se basa en la verificación de las funciones de seguridad implementadas y en la ejecución de análisis de vulnerabilidades mediante pruebas funcionales y pruebas de penetración.

El objetivo del proceso de evaluación es permitir a un laboratorio verificar si el producto es conforme a su especificación —comprobando la correcta implementación de sus funciones de seguridad—, así como realizar un análisis de vulnerabilidades y un conjunto de pruebas de penetración que permitan determinar que el producto se encuentra libre de vulnerabilidades con un determinado nivel de garantía. Los resultados de este proceso se recogen en el Informe Técnico de Evaluación (ETR) y el Informe Técnico de Monitorización (MTR).

Para ello, el laboratorio de evaluación utilizará como base documental la Declaración de Seguridad (DS), que define el alcance de la evaluación; el Documento de Arquitectura del Servicio (DAS); el listado de librerías de terceros con sus correspondientes versiones; la información pública disponible del producto; así como el acceso al propio producto objeto de evaluación (TOE).

Adicionalmente, el laboratorio empleará toda la información pública accesible relacionada con el TOE, incluyendo, entre otras fuentes, la documentación publicada por el fabricante para el producto evaluado o productos equivalentes, información pública proporcionada por terceros y bases de datos públicas de vulnerabilidades aplicables a productos desplegados en la nube.

# 3. ACTORES Y RESPONSABILIDADES.

## 3.1 LISTA DE ACTORES

En el proceso de evaluación intervienen los siguientes actores:

a) **Solicitante:** entidad responsable de formalizar la solicitud de evaluación del producto en la nube.
b) **Fabricante:** entidad responsable del diseño, desarrollo y, en su caso, mantenimiento del producto en la nube.
c) **Laboratorio de evaluación:** entidad acreditada en el marco del ENECSTI conforme a la norma ISO/IEC 17025 y autorizada por el Organismo de Certificación para realizar la evaluación del producto.
d) **Centro Criptológico Nacional (CCN):** entidad responsable de validar el informe emitido por el laboratorio de evaluación y el porcentaje de garantía derivado de los resultados obtenidos.

## 3.2 RESPONSABILIDADES

### 3.2.1 SOLICITANTE O FABRICANTE

El solicitante deberá proporcionar, como mínimo, los siguientes elementos y evidencias necesarios para la realización del proceso de evaluación:

a) Una solicitud de evaluación al CCN, utilizando el formulario de solicitud de evaluación de producto en la nube [FOR-CIC-001].
b) El producto en la nube objeto de evaluación.
c) La documentación asociada al producto.
d) La Declaración de Seguridad (DS), de carácter público.
e) El Documento de Arquitectura del Servicio (DAS), de carácter privado.
f) La certificación del Esquema Nacional de Seguridad (ENS) u otra certificación reconocida en el marco del ENECSTI.
g) El fichero de librerías de terceros utilizadas, con indicación de sus versiones.
h) El entorno para la evaluación de seguridad del producto. El solicitante deberá facilitar al laboratorio de evaluación acceso al entorno de pruebas del TOE, el cual deberá corresponderse con el descrito en la Declaración de Seguridad o ser equivalente en términos funcionales y de configuración, permitiendo la validación de las funciones de seguridad implementadas y la ejecución de las actividades de evaluación previstas.
i) La gestión de la realización de la evaluación con un laboratorio autorizado por el CCN, así como el soporte necesario durante todo el proceso.
j) Las evidencias necesarias para llevar a cabo la evaluación.

**Nota**: En determinados casos, el fabricante y el solicitante de la certificación pueden ser entidades diferentes. Por simplicidad, se han listado como un único rol. En estos casos y en términos generales, el solicitante será el encargado de financiar la evaluación y el fabricante en dar el soporte técnico necesario para poder realizar el proceso de evaluación.

### 3.2.2 LABORATORIO DE EVALUACIÓN

Dado el elevado nivel de especialización requerido para la ejecución y validación de las tareas de evaluación, así como la complejidad del equipamiento necesario para la realización de determinadas pruebas, resulta necesario garantizar que los laboratorios dispongan de las capacidades mínimas y de los medios materiales adecuados para aplicar la presente metodología.

A tal efecto, el documento [PO-CIC-010] establece los requisitos y procedimientos que deben cumplir los laboratorios para ser autorizados por el CCN para la evaluación de productos en la nube conforme a la metodología CICLON.

Estas responsabilidades son las siguientes:

a) Mantener la competencia técnica para la realización de evaluaciones conforme a la metodología CICLON.

b) Aplicar los procedimientos, guías y documentación necesarios para realizar la evaluación incluyendo, al menos:

    a. El procedimiento de certificación de productos en la nube [PO-CIC-005].

    b. El procedimiento de acreditación de laboratorios [PO-006].

    c. El procedimiento de autorización de laboratorios para evaluaciones CICLON [PO-CIC-010].

c) Verificar que el acceso al entorno de pruebas del TOE proporcionado por el solicitante resulta adecuado y permite la ejecución completa de las tareas de evaluación requeridas.

### 3.2.3 CCN

Las responsabilidades del equipo certificador son las siguientes:

a) Elaborar los criterios y la metodología de evaluación aplicables a los productos desplegados en la nube. Dicho equipo tiene la potestad de exigir la aplicación de métodos de evaluación específicos en función de las características del producto a evaluar.

b) Generar los procedimientos, formularios, guías y documentación necesarios para la correcta implementación del proceso de evaluación, entre los que se incluyen:

   a. El procedimiento de certificación de productos en la nube [PO-CIC-005].
   b. El procedimiento de acreditación de laboratorios [PO-006].
   c. El procedimiento de autorización de Laboratorios para evaluaciones CICLON [PO-CIC-010].

c) Comprobar y verificar que los laboratorios cumplen los criterios establecidos en el procedimiento de acreditación de laboratorios [PO-006].
d) Revisar las solicitudes de autorización de laboratorio y otorgar o retirar la condición de laboratorio autorizado por el CCN.
e) Revisar las solicitudes de evaluación y autorizar o denegar el inicio de la evaluación.

# 4. PREPARACIÓN DE LA EVALUACIÓN

## 4.1 EVIDENCIAS MÍNIMAS NECESARIAS

### 4.1.1 DECLARACIÓN DE SEGURIDAD (DS)

La Declaración de Seguridad se utiliza para especificar el problema de seguridad del producto desplegado en la nube que será sometido a evaluación, así como describir las relaciones existentes entre el producto y el entorno de ejecución.

Dicho problema de seguridad define:

a) Los activos a proteger.
b) Las amenazas a las que pueden verse sometidos dichos activos.
c) Las hipótesis del entorno de ejecución que aplican al TOE.
d) Los requisitos funcionales de seguridad que mitigan las amenazas detectadas y que serán objeto de evaluación.

Además, se deberá identificar de forma inequívoca tanto el TOE como el entorno en el que se llevará a cabo la evaluación, especificando si corresponde a un entorno de producción o preproducción.

Para cada una de las funciones de seguridad objeto de evaluación, deberá indicarse el método de comprobación mediante el que será verificada, conforme a los siguientes criterios:

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.

La Declaración de Seguridad deberá ser conforme a la Plantilla de la Declaración de Seguridad [Anexo A CCN-STIC-2010].

### 4.1.2 VALIDACIÓN DE LA DECLARACIÓN DE SEGURIDAD

La validación de la declaración de seguridad será realizada en primera instancia por los responsables del Catálogo de Productos y Servicios STIC del CCN (CPSTIC).

El documento resultante de dicha validación servirá como evidencia acreditativa del inicio de la evaluación junto a la propia Declaración de Seguridad (DS).

### 4.1.3 DOCUMENTO DE ARQUITECTURA DEL SERVICIO (DAS)

Este documento constituye una declaración responsable firmada que debe contener la siguiente información:

a) La estructura del TOE y su entorno operativo: en términos de subsistemas e interfaces.
b) Descripción de los flujos de información: declarados entre los componentes del servicio.
c) La jurisdicción de los datos del producto desplegado en la nube.
d) Cláusulas de transparencia.
e) Autorización de acceso directo al producto desplegado en la nube si WAF.
f) Certificación de conformidad con el ENS o EUCS.
g) Información sobre mecanismos y algoritmos criptográficos empleados, así como servicios de cifra.

El DAS deberá ser conforme a la Plantilla para el Documento de Arquitectura del Servicio de la Evaluación de Productos en la Nube [Anexo B CCN-STIC-2010].

### 4.1.4 FICHERO DE LIBRERÍAS

El Fichero de Librerías será un *Software Bill of Materials* (SBOM), conforme al estándar CycloneDX, con el fin de proporcionar trazabilidad completa sobre la totalidad de las dependencias de terceros del TOE.

El SBOM documenta y organiza la composición software del producto, permitiendo verificar versiones, procedencias y riesgos asociados a cada componente.

El SBOM deberá incluir los siguientes elementos:

a) **Identificación general:** versión, fecha de generación, herramienta empleada e identificador único (UUID).

b) **Información del TOE:** datos de identificación del producto evaluado.

c) **Inventario de componentes de terceros:** relación exhaustiva de librerías, con indicación del nombre, versión, tipo, proveedor, licencias, valores de hash, identificadores estandarizados (purl, CPE), dependencias transitivas y contexto de uso.

d) **Relación entre componentes:** vínculos de tipo *depends-on* e *includes* entre los distintos elementos del software.

e) **Metadatos de integridad:** firma digital, valores hash y origen de cada componente, a efectos de verificación y no repudio.

Siempre que resulte aplicable, se documentarán adicionalmente las capas de contendores, los *runtimes* y los sistemas base sobre los que opera el TOE.

## 4.2 FASES DE LA PREPARACIÓN

### 4.2.1 ELECCIÓN DE UN LABORATORIO DE EVALUACIÓN

El solicitante deberá contactar con el laboratorio de evaluación acreditado en el ENECSTI y autorizado por el CCN antes de enviar la solicitud de evaluación del producto.

El solicitante y el laboratorio deberán acordar conjuntamente:

a) El alcance de la evaluación tomando como base la Declaración de Seguridad (DS), el Documento de Arquitectura del Servicio (DAS) y el fichero de librerías de terceros aportados.

b) El esfuerzo necesario. Para lo cual, se considerarán los siguientes factores:

    a. La complejidad tecnológica del TOE.

    b. La diversidad de configuraciones.

    c. La cantidad de interfaces y protocolos utilizados.

    d. La existencia de módulos propietarios o vulnerabilidades recientes.

No obstante, la evaluación siempre deberá cumplir con el mínimo de pruebas exigido por CCN para la metodología y, en consecuencia, el tiempo mínimo asociado a su ejecución.

### 4.2.2 SOLICITUD DE LA EVALUACIÓN

Con carácter previo a la formulación de una solicitud de evaluación, el solicitante deberá:

a) Elaborar la Declaración de Seguridad (DS) conforme a la Plantilla para la Declaración de Seguridad de la Evaluación de Productos en la Nube (CICLON), recogida en el [Anexo A CCN-STIC-2010].
b) Elaborar el Documento de Arquitectura del Servicio (DAS) conforme a la Plantilla para el Documento de Arquitectura del Servicio de la Evaluación de Productos en la Nube (CICLON), recogida en el [Anexo B CCN-STIC-2010].
c) Contratar con un laboratorio autorizado la realización de las pruebas de evaluación.
d) Preparar el entorno necesario para la realización de las pruebas de evaluación.
e) Elaborar el fichero de librerías de terceros en formato SBOM, conforme a lo establecido en el apartado correspondiente de la presente metodología.

A efectos de formalizar la solicitud de evaluación, deberá entregarse la documentación anteriormente mencionada junto a la siguiente:

a) Solicitud de evaluación cumplimentada [FOR-CIC-001].

b) Certificación del Esquema Nacional de Seguridad (ENS) o, en su defecto, otra certificación reconocida en el marco del ENECSTI.
c) Resultado favorable del informe de revisión de la DS generado por el equipo del CPSTIC.

### 4.2.3 ANÁLISIS DE LA SOLICITUD DE EVALUACIÓN

El CCN analizará las solicitudes de evaluación, la declaración de seguridad, el documento de arquitectura del servicio y el fichero de librerías de terceros.

Una solicitud de evaluación podrá ser rechazada por el CCN y podrá ser subsanada en los siguientes casos:

a) Solicitud incompleta.
b) Documentación incompleta o no cumple con los requisitos.

Después de que sea aceptada la solicitud de evaluación por el CCN, el proyecto de evaluación se registra y se informa a los participantes sobre su aceptación.

# 5. PROCESO DE EVALUACIÓN

## 5.1 INFORMACIÓN GENERAL SOBRE EL PROCEDIMIENTO DE LA EVALUACIÓN

La evaluación deberá ser ejecutada por un laboratorio acreditado en el ENECSTI y autorizado por el CCN, con el fin de garantizar la homogeneidad y comparabilidad de los resultados entre los distintos laboratorios autorizados.

El CCN podrá resolver el cierre del expediente de evaluación en las circunstancias descritas en el [PO-CIC-005] con independencia de las obligaciones contractuales que pudieran existir entre el solicitante y el laboratorio.

El proceso de evaluación comprende las siguientes fases:

a) Fase de evaluación:
    a. Análisis de la Declaración de Seguridad (DS).
    b. Análisis del Documento de Arquitectura del Servicio (DAS).
    c. Acceso y configuración del entorno de pruebas.
    d. Ejecución de pruebas funcionales.
    e. Análisis criptográfico.
    f. Ejecución de pruebas de penetración sobre el TOE, conforme a la [CCN-ITC-003].
b) Fase de monitorización:
    a. Análisis del fichero de librerías de terceros (SBOM).
    b. Verificación de los componentes integrados en el entorno operacional.
    c. Revisión de las certificaciones aplicables al entorno de ejecución.

Los resultados se presentarán en dos informes técnicos:

a) Informe Técnico de evaluación (ETR).

b) Informe Técnico de Monitorización (MTR).

El proceso de evaluación se realiza de forma iterativa:

a) En la primera iteración, se realizará la Fase de Evaluación junto a la Fase de Monitorización, obteniéndose un Porcentaje de Garantía Compuesto (PGC) inicial.

b) En las posteriores iteraciones se realizará únicamente la Fase de Monitorización que actualizará el valor de dicho PGC.

El laboratorio evaluador podrá convocar sesiones de trabajo con el fabricante y/o el solicitante con el objeto de profundizar en el conocimiento del TOE y optimizar el desarrollo del proceso de evaluación.

Asimismo, el fabricante deberá facilitar el acceso al TOE con anterioridad al inicio de la evaluación y prestar el soporte técnico necesario durante el transcurso de la misma.

## 5.2 FASE DE EVALUACIÓN

El laboratorio debe comenzar por esta fase en la primera iteración del proceso.

El resultado de esta fase será un Porcentaje de Garantía de Evaluación (PGE) del producto desplegado en la nube y será plasmado en el Informe Técnico de Evaluación (ETR), definido en la Plantilla del Informe Técnico de Evaluación de Productos en la Nube (CICLON) [Anexo C CCN-STIC 2010].

A continuación, se definen las etapas y **tareas a realizar por el evaluador**.

### 5.2.1 ETAPA 1 – ANÁLISIS DE LA DECLARACIÓN DE SEGURIDAD

**Tarea 1.** Comprobar que la Declaración de Seguridad contiene los elementos descritos en el [Anexo A CCN-STIC-2010].

**Tarea 2.** Comprobar que se proporciona el nombre del TOE.

**Tarea 3.** Comprobar que la Declaración de Seguridad (DS) ha sido validada por los responsables de CPSTIC.

**Tarea 4.** Comprobar que la descripción del TOE no es confusa y que describe al menos la funcionalidad mínima para la que está diseñado.

**Tarea 5.** Comprobar que existe una correcta delimitación de las partes que pertenecen al TOE y las partes que pertenecen al entorno operacional, así como una adecuada descripción de cómo el entorno operacional da soporte a la ejecución del TOE.

**Tarea 6.** Comprobar la coherencia del problema de seguridad (Activos, Hipótesis, Amenazas y Funciones de seguridad).

**Tarea 7.** Comprobar que las funciones de seguridad se describen con el suficiente nivel de detalle para permitir al evaluador entender cómo han sido implementadas en el TOE.

**Tarea 8.** Comprobar que las funciones de seguridad delegadas en el entorno operacional se describen con el suficiente nivel de detalle para permitir al evaluador entender cómo son provistas por el entorno operacional.

**Tarea 9.** Comprobar que no existen no conformidades en relación con el análisis de la declaración de seguridad.

**Tarea 10.** Calcular el Porcentaje de Garantía correspondiente a esta etapa utilizando la siguiente fórmula.

$$PGE_1 = 1 - \mathrm{k_{CI}} \frac{CI}{R}$$

Donde:

> **$K_{CI}$** → Factor de escalado que permite ajustar la pendiente de la curva asociada a los requisitos satisfechos mediante Comprobación Indirecta (CI).

**CI** → Número de requisitos satisfechos por el fabricante mediante Comprobación Indirecta (CI).

**R** → Número total de requisitos definidos en la Declaración de Seguridad (DS).

### 5.2.2 ETAPA 2 – ANÁLISIS DEL DOCUMENTO DE ARQUITECTURA DEL SERVICIO

**Tarea 1.** Comprobar que el Documento de Arquitectura del Servicio (DAS) es completo y se corresponde con el TOE evaluado.

**Tarea 2.** Comprobar que el Documento de Arquitectura del Servicio define la posibilidad de acceso al TOE evitando el WAF.

**Tarea 3.** Comprobar que existe una correcta delimitación de las partes que pertenecen al TOE y las partes que pertenecen al entorno operacional, así como una adecuada descripción de cómo el entorno operacional da soporte a la ejecución del TOE.

**Tarea 4.** Comprobar que no existen no conformidades en relación con el Documento de Arquitectura del Servicio.

### 5.2.3 ETAPA 3 – ACCESO Y CONFIGURACIÓN DEL ENTORNO DE PRUEBAS

**Tarea 1.** Comprobar que el solicitante ha proporcionado acceso al entorno de pruebas requerido para llevar a cabo las pruebas en el producto.

**Tarea 2.** Comprobar que es posible configurar el producto de acuerdo con la configuración o configuraciones descritas en la Declaración de Seguridad. Si el producto permite varios modos de configuración, la identificación de este modo deberá estar indicado en la Declaración de Seguridad.

**Tarea 3.** Comprobar que no existen no conformidades en el acceso y configuración del entorno de pruebas.

**Tarea 4.** Calcular el Porcentaje de Garantía correspondiente a esta etapa utilizando la siguiente fórmula.

$$PGE_3 = \begin{cases} 1 - W, & Entorno\ de\ producción \\ P - W, & Entorno\ de\ preproducción\ equivalente \end{cases}$$

Donde:

**P** → Valor asociado a la utilización de un entorno de preproducción equivalente.

**W** → Representa el acceso al TOE a través del WAF en el entorno de evaluación.

Se considera Entorno de producción cuando el utilizado para la evaluación es el mismo que el que luego será proporcionado al usuario final del TOE.

Por otro lado, se considera Entorno de preproducción cuando el entorno de evaluación tiene características similares al que será proporcionado al usuario final del TOE, pero sin ser el mismo.

### 5.2.4 ETAPA 4 – PRUEBAS FUNCIONALES

**Tarea 1.** El evaluador deberá ejecutar, para la totalidad de las funciones de seguridad definidas en la Declaración de Seguridad (DS) y marcadas como Comprobación Directa (CD), las siguientes pruebas:

a) **Prueba estándar**. El evaluador deberá comprobar que la función de seguridad descrita en el requisito correspondiente se encuentra correctamente implementada en el TOE.
b) **Prueba de manipulación/elusión**. El evaluador, tomando como referencia el mecanismo de seguridad implementado por el TOE, deberá intentar:
    a. Subvertir el comportamiento del mecanismo de seguridad mediante alteraciones o modificaciones sobre la interfaz correspondiente (***tampering***).
    b. Impedir la aplicación del mecanismo de seguridad explotando debilidades en la lógica de su implementación (***bypassing***).

**Tarea 2.** El evaluador deberá ejecutar, para la totalidad de las funciones de seguridad definidas en la Declaración de Seguridad (DS) y marcadas como Comprobación Indirecta (CI), las siguientes pruebas:

a) Comprobar que las evidencias proporcionadas han sido firmadas por el fabricante y cubren el requisito de seguridad declarado. A estos efectos, únicamente tendrán la consideración de evidencias válidas las siguientes, siempre que resulten aplicables al requisito objeto de verificación:
    a. Manuales del producto.
    b. Código fuente.
    c. Capturas de imagen o video del funcionamiento específico del TOE.
    d. Sesiones telemáticas o presenciales donde el fabricante muestre al evaluador la implementación de la función de seguridad.
b) Comprobar que la evidencia aportada es completa, coherente y técnicamente adecuada para justificar el cumplimiento de la función de seguridad.

### 5.2.5 ETAPA 5 – ANÁLISIS CRIPTOGRÁFICO DE LAS COMUNICACIONES

**Tarea 1.** El evaluador deberá comprobar que la totalidad de los canales de comunicación externos e internos respecto al TOE se encuentran definidos e identificados de forma inequívoca en la Declaración de Seguridad.

**Tarea 2.** El evaluador deberá verificar que lo establecido en la Declaración de Seguridad es coherente con lo declarado en el Documento de Arquitectura del Servicio.

**Tarea 3.** El evaluador deberá comprobar que no existen no conformidades en relación con las características criptográficas de los canales de comunicación.

**Tarea 4.** El evaluador deberá calcular el Porcentaje de Garantía correspondiente a esta etapa ($PGE_5$) mediante la siguiente fórmula.

$$PGE_5 = e^{-(w_L \cdot L + w_{NR} \cdot NR)}$$

Donde:

**$w_L$** → Impacto de criptografía Heredada sobre el porcentaje de garantía.

**$w_{NR}$** → Impacto de criptografía No Recomendada sobre el porcentaje de garantía.

**L** → Número de mecanismos criptográficos utilizados por el TOE que son considerados como Heredada a fecha de la realización de la evaluación.

**NR** → Número de mecanismos criptográficos utilizados por el TOE que son considerados como No Recomendados a fecha de la realización de la evaluación.

### 5.2.6 ETAPA 6 – PRUEBAS DE PENETRACIÓN DEL TOE

**Tarea 1.** El evaluador deberá ejecutar, como mínimo, el conjunto de pruebas descritas en la Instrucción Técnica Evaluación de seguridad en entornos web y nube [CCN-ITC-003], conforme a lo establecido en la Plantilla del Informe Técnico de Evaluación de Productos en la Nube (CICLON), recogida en el [Anexo C CCN-STIC 2010].

**Tarea 2.** El evaluador deberá que no existen no conformidades porque algún ataque haya tenido éxito.

### 5.2.7 ETAPA 7 – CÁLCULO DEL PORCENTAJE DE GARANTÍA DE EVALUACIÓN

**Tarea 1.** El evaluador deberá calcular el Porcentaje de Garantía de Evaluación (PGE) del producto desplegado en la nube basándose en los resultados de las etapas anteriores mediante la siguiente fórmula:

$$PGE = e^{-(w_1(1-PGE_1)+w_3(1-PGE_3)+w_5(1-PGE_5))}$$

Donde:

**$w_1$** → Peso de $PGE_1$ en el cálculo de PGE.

**$w_3$** → Peso de $PGE_3$ en el cálculo de PGE.

**$w_5$** → Peso de $PGE_5$ en el cálculo de PGE.

**$PGE_1$** → Porcentaje de Garantía de la Etapa 1 de la Fase de Evaluación.

**$PGE_3$** → Porcentaje de Garantía de la Etapa 3 de la Fase de Evaluación.

**$PG5_5$** → Porcentaje de Garantía de la Etapa 5 de la Fase de Evaluación.

**Tarea 2.** El evaluador deberá registrar los distintos Porcentajes de Garantía Parciales ($PGE_1$, $PGE_3$, $PGE_5$) y el Porcentaje de Garantía de Evaluación (PGE) en el Informe Técnico de Evaluación acorde a lo estipulado en el [Anexo C CCN-STIC 2010].

### 5.2.8 ETAPA 8 – GENERACIÓN DEL INFORME TÉCNICO DE EVALUACIÓN

**Tarea 1.** El evaluador deberá emitir un Informe Técnico de Evaluación (ETR) que contiene y presenta los resultados de la fase de evaluación. Este informe debe contener la información requerida en la plantilla [Anexo C CCN-STIC-2010].

## 5.3 FASE DE MONITORIZACIÓN

El producto desplegado en la nube deberá someterse a la Fase de Monitorización después de pasar por la Fase de Evaluación.

Durante la vigencia de la evaluación, esta fase será repetida de forma iterativa.

El resultado de esta fase será un Porcentaje de Garantía del producto desplegado en la nube y será plasmado en la Plantilla del Informe Técnico de Monitorización de Productos en la Nube (CICLON) [Anexo D CCN-STIC 2010].

A continuación, se definen las etapas y **tareas a realizar por el evaluador**.

### 5.3.1 ETAPA 1 – ANÁLISIS DE LIBRERÍAS DE TERCEROS

**Tarea 1.** El evaluador deberá procesar el Fichero de Librerías (SBOM) proporcionado por el fabricante para buscar vulnerabilidades públicas conocidas.

**Tarea 2.** El evaluador deberá categorizar la criticidad (alta, media, baja) de cada vulnerabilidad pública encontrada. Entendiendo por criticidad los siguientes rangos definidos por CVSS v4.0:

a) **Crítica:** Desde 9.0 hasta 10.0
b) **Alta:** Desde 7.0 hasta 8.9
c) **Media:** Desde 4.0 hasta 6.9
d) **Baja:** Desde 0.1 hasta 3.9

**Tarea 3.** El evaluador deberá calcular el Porcentaje de Garantía correspondiente a esta etapa ($PGM_1$) utilizando la siguiente fórmula:

$$PGM_1 = C \cdot e^{-\left(w_H \cdot H + \frac{w_M \cdot M}{T} + \frac{w_L \cdot L}{T}\right)}$$

Donde:

**$w_H$** → Impacto de las vulnerabilidades de criticidad alta sobre el porcentaje de garantía.

**$w_M$** → Impacto de las vulnerabilidades de criticidad media sobre el porcentaje de garantía.

**$w_L$** → Impacto de las vulnerabilidades de criticidad baja sobre el porcentaje de garantía.

**C** → Vale 0 si existe alguna vulnerabilidad crítica y 1 en caso contrario.

**H** → Número de vulnerabilidades de criticidad alta.

**M** → Número de vulnerabilidades de criticidad media.

**L** → Número de vulnerabilidades de criticidad baja.

**T** → Número total de librerías de terceros declaradas por el solicitante en la Declaración de Seguridad (DS).

### 5.3.2 ETAPA 2 – VERIFICACIÓN DE LOS COMPONENTES DE INTEGRACIÓN

**Tarea 1.** El evaluador deberá verificar que los componentes de integración que se encuentran declarados en la Declaración de Seguridad estén evaluados bajo la Metodología CICLON.

**Tarea 2.** El evaluador deberá calcular el Porcentaje de Garantía correspondiente a esta etapa ($PGM_2$) utilizando la siguiente fórmula.

$$PGM_2 = \sum_{0}^{n} (PGC_{COMPn} \cdot \frac{RFS_{COMPn}}{R})$$

Donde:

**$PGC_{COMPn}$** → Porcentaje de Garantía Compuesto (PGC) del componente n.

**$RFS_{COMPn}$** → Número de requisitos fundamentales de seguridad que son implementados por el componente n.

**R** → Número total de requisitos definidos en la Declaración de Seguridad.

**n** → Número componentes externos que contribuyen a implementar funcionalidad de seguridad.

### 5.3.3 ETAPA 3 - REVISIÓN DE LAS CERTIFICACIONES APLICABLES AL PROVEEDOR DE LA PLATAFORMA NUBE

**Tarea 1.** El evaluador deberá comprobar la vigencia de los diferentes certificados aplicables entregados por el fabricante.

**Tarea 2.** El evaluador deberá calcular el Porcentaje de Garantía correspondiente a esta etapa ($PGM_3$) mediante la siguiente fórmula.

$$PGM_3 = \prod_{1}^{n} C_n$$

Donde:

**C** → Certificación de conformidad con el Esquema Nacional de Seguridad (ENS) o equivalente. Vale 1 si la certificación está en vigor y 0 en caso contrario.

### 5.3.4 ETAPA 4 – CÁLCULO DEL PORCENTAJE DE GARANTIA DE MONITORIZACIÓN

**Tarea 1.** El evaluador deberá calcular el Porcentaje de Garantía de Monitorización (PGM) del producto desplegado en la nube basándose en los resultados de las etapas anteriores mediante la siguiente fórmula:

$$PGM = PGM_3 \cdot e^{-(w_1(1-PGM_1)+w_2(1-PGM_2))}$$

Donde:

**$w_1$** → Peso de $PGM_1$ en el cálculo de PGM.

**$w_2$** → Peso de $PGM_2$ en el cálculo de PGM.

**$PGM_1$** → Porcentaje de Garantía de la Etapa 1 de la Fase de Monitorización.

**$PGM_2$** → Porcentaje de Garantía de la Etapa 2 de la Fase de Monitorización.

**$PGM_3$** → Porcentaje de Garantía de la Etapa 3 de la Fase de Monitorización.

**Tarea 2.** El evaluador deberá registrar los distintos Porcentajes de Garantía Parciales ($PGM_1$, $PGM_2$, $PGM_3$) y el Porcentaje de Garantía de Monitorización (PGM) en el Informe Técnico de Monitorización acorde a lo estipulado en el [Anexo D CCN-STIC 2010].

### 5.3.5 ETAPA 4 – CÁLCULO DEL PORCENTAJE DE GARANTÍA COMPUESTO

**Tarea 1.** El evaluador deberá calcular el Porcentaje de Garantía Compuesto (PGC) del producto desplegado en la nube basándose en los resultados del Porcentaje de Garantía de Evaluación (PGE) y del Porcentaje de Garantía de Monitorización (PGM) mediante la siguiente fórmula:

$$PGC = (w_e \cdot PGE + (1 - w_e) \cdot PGM) \cdot 100$$

Donde:

**PGE** → Es el Porcentaje de Garantía de Evaluación (PGE).

**PGM** → Es el Porcentaje de Garantía de Monitorización (PGM).

**$w_e$** → Peso de PGE en el cálculo de PGC.

### 5.3.6 ETAPA 5 - GENERACIÓN DEL INFORME TÉCNICO DE MONITORIZACIÓN

**Tarea 1.** El evaluador deberá emitir un Informe Técnico de Monitorización (MTR) que contiene y presenta los resultados de la fase de monitorización. Este informe debe contener la información requerida en la plantilla [Anexo D CCN-STIC-2010].

## 5.4 RESULTADO DE LA EVALUACIÓN

El veredicto de la evaluación será un Porcentaje de Garantía Compuesto (PGC), que tendrá en cuenta factores de la evaluación y monitorización continua.

Si durante el Proceso de Evaluación se encuentran NO Conformidades el veredicto de la evaluación será **FALLA y, por tanto, el Porcentaje de Garantía Compuesto será 0.**

## 6. CÁLCULO DEL ESFUERZO

A modo orientativo, se destacan los siguientes factores para tener en cuenta a la hora de calcular el esfuerzo necesario. Se marcan con una **[R]** aquellos elementos que deberían dar lugar a una reducción del esfuerzo, y con una **[A]** aquellos que, por el contrario, deberían aumentarlo:

**[A]** Si hay una gran cantidad de requisitos fundamentales de seguridad definidos en la Declaración de Seguridad (DS).

**[A]** Si la tecnología empleada por el TOE es compleja.

**[A]** Si el entorno operacional es complejo.

**[A]** Si hay múltiples configuraciones evaluadas.

**[A]** Si el TOE hace uso de múltiples protocolos de comunicación.

**[A]** Si el TOE tiene múltiples interfaces.

**[A]** Si el TOE hace uso de módulos de carácter propietario a los que tiene acceso directo un potencial atacante.

**[A]** Si ha habido publicaciones de seguridad recientes que puedan presentar nuevos vectores de ataques para el tipo de TOE evaluado.

**[R]** Si el laboratorio dispone de suites de pruebas para los protocolos empleados por el TOE.

**[R]** Si el laboratorio tiene experiencia previa en evaluaciones similares al TOE.

**[R]** Si el laboratorio dispone de herramientas automáticas que faciliten la evaluación de funciones de seguridad implementadas por el TOE.

Con el fin de estandarizar el cálculo de esfuerzos, se entenderá el esfuerzo como llevado a cabo por un evaluador experimentado y con un amplio conocimiento de la metodología y de la tecnología evaluada. Por lo tanto, se espera que, si la evaluación es realizada por un evaluador que no cumple con dicho estándar, el laboratorio deberá realizar el cálculo de esfuerzos ponderándolo acordemente.

## 7. GLOSARIO

| | |
|---|---|
| **Actores** | Roles involucrados en la evaluación: solicitante, fabricante, laboratorio y CCN. |
| **Activo** | Elemento del TOE o del entorno que debe ser protegido frente a amenazas. |
| **Amenazas** | Elementos del problema de seguridad que describen posibles acciones que pueden comprometer los activos del TOE. |
| **Canal de Comunicación** | Flujo de información entre componentes internos o externos del TOE cuya seguridad debe ser analizada. |
| **Comprobación Directa** | Modo de evaluación donde el laboratorio puede probar directamente el requisito. |
| **Comprobación Indirecta** | Modo de evaluación basado en evidencias del fabricante. |
| **Componente de Integración** | Elemento externo al TOE que aporta parte de la funcionalidad de seguridad declarada. |
| **Declaración de Seguridad** | Documento que define el problema de seguridad, alcance, amenazas, activos y requisitos del TOE. |
| **Documento de Arquitectura del Servicio** | Documento que describe la arquitectura, proveedor en la nube y conformidad del servicio. |
| **Entorno de Preproducción** | Entorno similar al de producción, pero no idéntico. |
| **Entorno de Producción** | Entorno real utilizado por el usuario final. |
| **Entorno Operacional** | Componentes externos al TOE que dan soporte a su funcionamiento. |

| | |
|---|---|
| **Función de Seguridad** | Mecanismo técnico implementado por el TOE para mitigar amenazas y proteger activos. |
| **Fichero de Librerías** | Listado de librerías de terceros utilizadas por el TOE, con sus versiones. |
| **Hipótesis** | Condiciones asumidas como ciertas en el entorno del TOE. |
| **Informe Técnico de Evaluación** | Documento que recoge los resultados de la fase de evaluación. |
| **Informe Técnico de Monitorización** | Documento que recoge los resultados de la fase de monitorización. |
| **No Conformidad** | Incumplimiento detectado en el proceso de evaluación o monitorización que invalida el resultado. |
| **Porcentaje de Garantía Compuesto** | Valor final de garantía del TOE, actualizado periódicamente. |
| **Porcentaje de Garantía de Evaluación** | Resultado de la fase de evaluación inicial. |
| **Porcentaje de Garantía de Monitorización** | Resultado de la fase de monitorización. |
| **Pruebas de Penetración** | Ataques controlados para identificar vulnerabilidades explotables. |
| **Pruebas Funcionales** | Pruebas para verificar que los requisitos de seguridad están implementados correctamente. |
| **Solicitante** | Entidad que solicita la evaluación del producto. |
| **Vulnerabilidad** | Debilidad del TOE o de sus librerías que puede ser explotada mediante un ataque. |

## 8. 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* |

## 9. REFERENCIAS

| | |
|---|---|
| **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. |