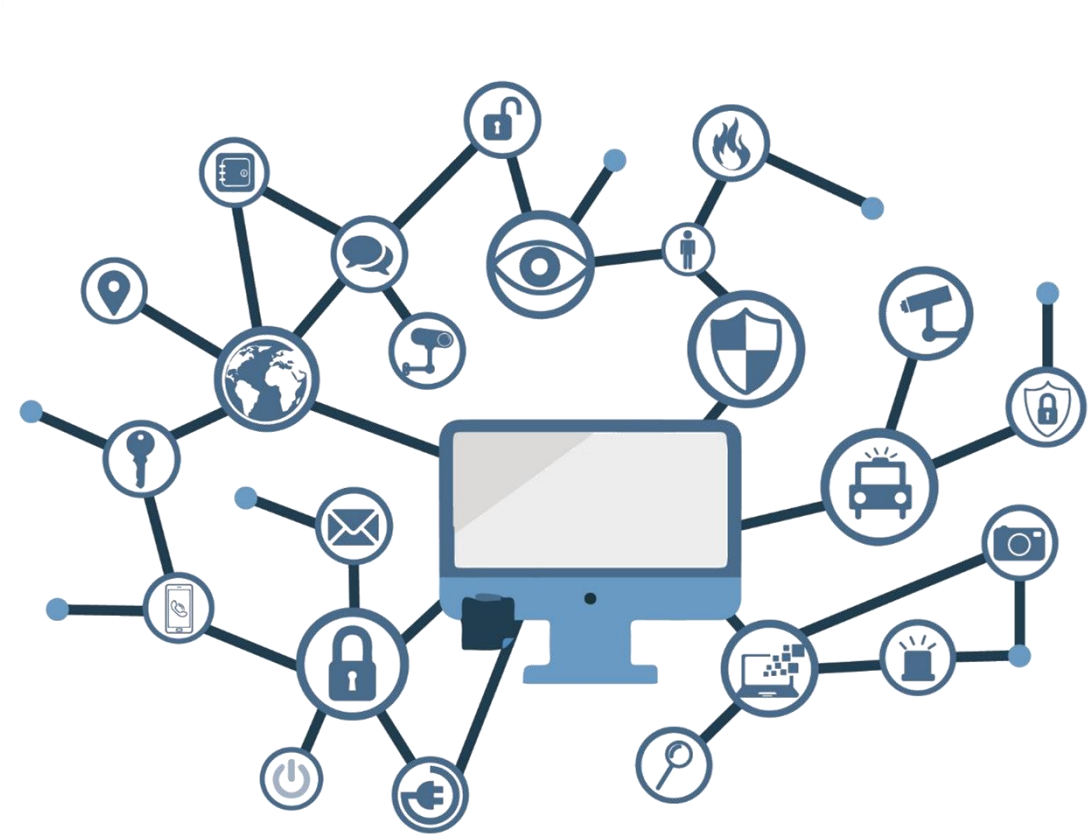
centro criptológico nacional

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

Plantilla para el Documento de Arquitectura del Servicio de la Evaluación de Productos en la Nube



Marzo 2026

Edita:

centro criptológico nacional

Fecha de edición: Marzo 2026

centro criptológico nacional

CCN
c=ES, l=MADRID, o=CCN,
ou=SELLO ELECTRONICO,
2.5.4.97=VATES-S2800155J,
serialNumber=S2800155J,
cn=CCN
2026.03.27 12:36:58 +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

CONTROL DE VERSIÓN

Versión	Comentario	Fecha
1.0	Versión Inicial	Marzo 2026

ÍNDICE

1 DATOS DEL FABRICANTE, TOE Y EVALUACIÓN

DATOS DEL FABRICANTE	
Razón Social	
Dirección Postal	
Personalidad Jurídica	
C.I.F.	
REPRESENTANTE LEGAL DEL FABRICANTE	
Nombre	
D.N.I	
DATOS DEL TOE Y EVALUACIÓN	
Nombre del TOE	
Tipo de Evaluación	CICLON versión 1.0

2 DECLARACIÓN RESPONSABLE DE CONFORMIDAD DEL FABRICANTE

Mediante la firma del siguiente documento por parte del representante legal de ***[nombre del fabricante]*** se garantiza la fiabilidad y veracidad de toda la información proporcionada en el presente documento.

La información declarada en este documento está alineada con la proporcionada en la Declaración de Seguridad e indica lo siguiente:

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) Cumplimiento con los requisitos de transparencia establecidos.
e) Autorización de acceso directo al producto desplegado en la nube si WAF.
f) Certificación de conformidad con el ENS o EUCS.
g) Requisitos criptográficos.
h) Servicios de cifra.

2.1 DIAGRAMA DE ARQUITECTURA DEL SERVICIO (DIAS)

Se deberá incluir un diagrama de la arquitectura del producto desplegado en nube y su integración con los componentes del entorno ya sean propietarios o de terceros necesarios para la operación normal del servicio. Todo componente que se considere parte del TOE deberá ser identificado claramente.

El propósito del diagrama será detallar claramente las integraciones del entorno operacional con la plataforma en la nube donde el TOE está desplegado.

Se deberá indicar cada componente mencionado en el diagrama de acuerdo con la siguiente tabla:

Componente / servicio	Propietario	Incluido en CPSTIC	Uso del componente	Interfaces y sus protocolos	Interacciones
		Indicar SI / NO		Listar las interfaces externas e internas que cada componente proporciona y cuáles son sus protocolos usados	Describir las interacciones con otros componentes o servicios (si las hay)

2.2 JURISDICCIÓN DE LOS DATOS

Se garantiza que **el producto desplegado en nube** cumple con las limitaciones geográficas relativas a los datos de acuerdo con:

- El Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos);
  b) La Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales;

El Real Decreto-Ley 14/2019, de 31 de octubre, que adopta medidas urgentes por razones de seguridad pública en el ámbito de la administración digital, la contratación del sector público y las telecomunicaciones.

2.3 TRANSPARENCIA

Se garantiza que el fabricante **del producto desplegado en nube** es capaz de proporcionar al cliente, si así se requiere:

1) El listado de las herramientas de seguridad de las que dispone, incluyendo aquellas destinadas a la monitorización, análisis, recuperación y notificación de incidentes de seguridad.
2) La descripción o especificación de la virtualización utilizada y del nivel y mecanismos de segregación de sus datos o aplicaciones alojadas en la nube.
3) El listado y especificación de los mecanismos y procedimientos de borrado seguro de la información almacenada por el proveedor, que serán utilizados en el momento de la terminación del vínculo contractual.
4) La ubicación geográfica de sus datos (incluido backups y almacenamiento de logs), antes y durante el suministro del servicio.
5) El acceso y análisis de los logs, registros de acceso y cualquier otra información que pudiera ser solicitada para garantizar el cumplimiento de las obligaciones legales. En caso de incidente de seguridad, toda la información requerida (configuración, logs, etc…) de los equipos físicos, dispositivos de red, servicios compartidos y dispositivos de seguridad debe ser entregada al cliente.

2.4 AUTORIZACIÓN DE ACCESO DIRECTO SIN WAF

Este apartado recoge la confirmación por parte de la entidad sobre si permite el acceso directo al servicio desplegado en la nube sin la protección del WAF.

Su objetivo es determinar si dicho acceso puede habilitarse para realizar las pruebas necesarias durante la fase de evaluación dentro del contexto de la solicitud realizada.

Para estos accesos controlados, puede emplearse *whitelisting*, que consiste en autorizar únicamente direcciones IP o rangos concretos para acceder al servicio sin pasar por el WAF, reduciendo así la superficie de exposición.

Alternativamente, pueden habilitarse mecanismos como túneles seguros, VPN corporativa o accesos temporales con restricciones horarias, siempre orientados a minimizar riesgos mientras se permite la operativa necesaria.

☐ **Sí**, autorizo el acceso directo sin WAF.

☐ **No**, no autorizo el acceso directo sin WAF.

2.5 CERTIFICACIÓN DE CONFORMIDAD CON EL ENS O EUCS

El sistema que suministra el producto desplegado en la nube dispone y tiene en vigor una certificación de conformidad con el Esquema Nacional de Seguridad (ENS) o EUCS, según se define en la Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad.

Proveedor de la Plataforma	Nivel ENS	Fecha de Validez	Ubicación Geográfica de los datos

2.6 REQUISITOS CRIPTOGRÁFICOS

El producto desplegado en la nube dispone de mecanismos de cifra que permiten que los activos declarados como Parámetro de Seguridad Crítico (PSC) o Parámetro de Seguridad Sensible (PSS) del TOE estén protegidos, en tránsito y en reposo, para que no puedan ser leídos o modificados en caso de acceso ilegítimo del siguiente modo:

Componente / servicio	Activos protegidos	Protección en Tránsito	Protección en reposo
Componente	Activo 1	Indicar si o no y en caso afirmativo, indicar protocolo y ciphersuites	Indicar si o no y la forma de protección (AES256)
	Activo 2		

2.7 SERVICIO DE CIFRA

El producto desplegado en la nube:

☐ **Sí,** es un servicio de cifra**.**

☐ **No,** no es un servicio de cifra.

Si el producto desplegado en nube es un servicio de cifra, se deberá describir:

a) El funcionamiento de los mecanismos de cifra sin que las claves sean almacenadas en la nube e Indicar arquitectura del sistema utilizado que debe incluir detalle de marca, modelo y versión del HSM utilizado (Hardware Security Module).

b) El proceso para garantizar que el cliente pueda gestionar y almacenar los mecanismos de cifra.

Y para que conste, firmo el presente documento.