centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 140

Taxonomía de productos de STIC -
Anexo G: Servicios en la nube

Septiembre de 2022

MINISTERIO DE DEFENSA

Catálogo de Publicaciones de la Administración General del Estado
https://cpage.mpr.gob.es

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

CCN centro criptológico nacional

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2022.09.23 12:06:07 +02'00'

Pº de la Castellana 109, 28046 Madrid
Centro Criptológico Nacional, 2022
NIPO: 083-22-102-1

Fecha de Edición: septiembre de 2022

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 Y OBJETO

1. La adopción de servicios en la nube como estrategia para soportar los servicios TIC ofrecidos por distintos organismos presenta un amplio número de ventajas. Sin embargo, este nuevo paradigma tecnológico introduce nuevos riesgos que deben controlarse para poder prestar un servicio que garantice la seguridad de los activos sensibles del organismo que maneje el servicio en la nube, así como el cumplimiento de los requisitos exigidos por los marcos legales de aplicación.
2. Estos riesgos añadidos con respecto a los de un producto *on-premise* afectan a la confidencialidad, integridad, disponibilidad y trazabilidad de la información y por lo tanto, deben ser analizados y gestionados mediante la aplicación de medidas y procedimientos de seguridad.
3. El presente documento describe los Requisitos Fundamentales de Seguridad (RFS) exigidos a ***Servicios de Seguridad en la Nube***[1] para ser incluidos como servicios cualificados dentro del Catálogo de Productos de Seguridad de las Tecnologías de la Información y la Comunicación (CPSTIC), publicado por el Centro Criptológico Nacional.
4. Dichos requisitos son **aplicables** a cualquier servicio de seguridad en la nube y deben ser entendidos como **requisitos adicionales** que complementan a los requisitos definidos para cada una de las familias de productos incluidas en la taxonomía detallada en la presente guía.

[1] Se definen los servicios de seguridad como aquellos que forman parte de la arquitectura de seguridad de un sistema, entendida como el conjunto de elementos físicos y lógicos cuyo objetivo es la protección de sus activos.

2. DESCRIPCIÓN DE LOS SERVICIOS

2.1 FUNCIONALIDAD

5. Los servicios considerados en el presente documento comprenden cualquier servicio de seguridad, suministrado por un tercero, a través de la nube, independientemente de su modalidad: SaaS (*Software as a Service*), PaaS (*Platform as a Service*), o IaaS (*Infraestructure as a Service*).

6. Los servicios en la nube consisten en la disposición de software, plataformas o infraestructuras accesibles en red, con independencia de donde se encuentren alojados los sistemas de información y de forma transparente al usuario final.

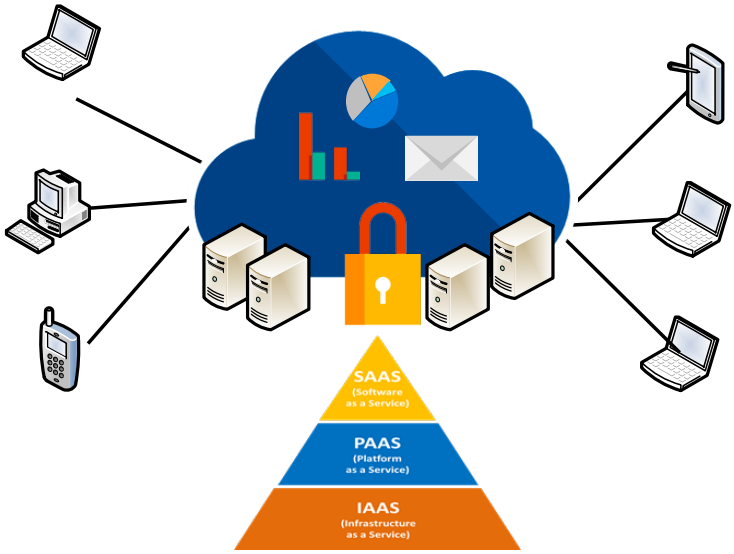

Figura 1.- Servicios en la nube

7. En función del tipo de despliegues posibles a la hora de crear un entorno de servicios en la nube, las infraestructuras se clasifican en nubes públicas[2], privadas[3], comunitarias o híbridas[4].

8. Las funciones de seguridad suministradas a través de la nube son muy amplias y variadas. Se incluyen, por ejemplo, mecanismos de protección de perímetro, monitorización y gestión centralizada de eventos de seguridad y almacenamiento de copias de seguridad.

---

[2] Esta modalidad está disponible para el público en general o para un gran grupo de industria y dicha infraestructura la controla un proveedor de servicios en la nube.

[3] La infraestructura es operada únicamente por y para una organización. Puede ser propiedad, ser administrado y operado por la organización, un tercero o alguna combinación de ellos, y puede existir dentro o fuera de las instalaciones.

[4] La infraestructura es compartida por varias organizaciones con intereses comunes. Puede ser propiedad, ser administrado y operado por una o más de las organizaciones de la comunidad, un tercero o alguna combinación de ellas, y puede existir dentro de las instalaciones.

3. REQUISITOS FUNDAMENTALES DE SEGURIDAD (RFS)

9. A continuación, se recogen los requisitos fundamentales de seguridad que deben cumplir los servicios de seguridad en la nube que quieran optar a la inclusión en el CPSTIC.

3.1 CERTIFICACIÓN DE CONFORMIDAD CON EL ENS

10. **ENS. 1** El sistema que suministra el servicio en la nube deberá disponer de una Certificación de Conformidad con el Esquema Nacional de Seguridad para categoría MEDIA o ALTA, 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.

11. **ENS. 2** La certificación de conformidad con el ENS debe estar vigente en el momento de la solicitud de inclusión en el CPSTIC.

3.2 REQUISITOS CRIPTOGRÁFICOS Y GESTIÓN DE CLAVES

12. **CRI.1** El servicio deberá disponer de mecanismos de cifra que permitan que la información declarada como Parámetro de Seguridad Crítico (PSC) del TOE esté protegida, en tránsito y en reposo, para que no pueda ser leída o modificada en caso de acceso ilegítimo.

    El servicio deberá disponer de mecanismos de cifra que permitan que la información declarada como Parámetro de Seguridad Crítico (PSC) del TOE esté protegida, en tránsito y en reposo, para que no pueda ser leída o modificada en caso de acceso ilegítimo.

13. **CRI.2** Si el servicio que se suministra a través de la nube es un servicio de cifra, este debe cumplir una de las siguientes condiciones:

    a) Ser capaz de garantizar el funcionamiento de los mecanismos de cifra sin que las claves sean almacenadas en la nube. Estas estarán en disposición del cliente, quien es el encargado de su gestión y almacenamiento.

    b) Almacenar las claves de cifra en dispositivos HSM (Hardware Security Modules), no accesibles por terceros. Dichos dispositivos deberán estar cualificados por el Centro Criptológico Nacional, incluidos en el Catálogo de Productos de Seguridad (CPSTIC).

3.3 REQUISITOS DE TRANSPARENCIA

14. **TRA.1** El proveedor del servicio de seguridad en la nube debe ser capaz de proporcionar al organismo contratante del servicio:

    a) 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.

    b) La descripción o especificación de la virtualización utilizada y del nivel y mecanismos de segregación de sus datos o aplicaciones alojadas en la nube.

    c) 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.

    d) La ubicación geográfica de sus datos (incluido *backups* y almacenamiento de *logs*), antes y durante el suministro del servicio.

    e) 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.

3.4 CERTIFICACIONES DE PRODUCTO

15. **CER.1** El producto o productos que suministren la funcionalidad principal del servicio o formen parte de su arquitectura de seguridad deberán disponer de una certificación funcional de seguridad o una Evaluación STIC adecuada que cumpla con los requisitos establecidos en la familia correspondiente de la presente taxonomía.

3.5 AUDITORÍA DE PENTESTING

16. **PEN.1** El servicio en la nube deberá superar, con éxito, una auditoría de *pentesting* de caja negra, en la que se comprobará la ausencia de vulnerabilidades públicas que permitan comprometer la información manejada o el servicio prestado. Esta será realizada por un laboratorio independiente acreditado por ENAC, siguiendo metodologías de evaluación reconocidas por el Organismo de Certificación del ENECSTI.
17. Las pruebas de *pentesting* realizadas deberán incluir las definidas en la última versión del proyecto OWASP[5].

[5] *Open Web Application Security Project (www.owasp.org)*

> Nota: este requisito es únicamente aplicable en aquellos casos en los que el producto se haya certificado en su versión *on premise* y sea utilizado para dar un servicio en la nube. En el resto de los casos, se considerará que esta evaluación está cubierta por las pruebas de *pentesting* incluidas en la evaluación STIC realizada en un laboratorio acreditado.

3.6 JURISDICCIÓN DE LOS DATOS

18. **JUR.1** En cuanto a las limitaciones geográficas de los datos, se deberá cumplir lo dispuesto en:

    a) 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;

    b) Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de derechos digitales.

    c) Real Decreto-ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones.

4. ABREVIATURAS

CC	Common Criteria
CCN	Centro Criptológico Nacional
CPSTIC	Catálogo de Productos de Seguridad de las Tecnologías de Información y las Comunicaciones
ENAC	Entidad Nacional de Acreditación
ENECSTI	Entidad Nacional de Evaluación y Certificación STIC
ENS	Esquema Nacional de Seguridad
HSM	*Hardware Security Module*
RFS	Requisitos Fundamentales de Seguridad
SaaS	*Software as a Service*
PaaS	*Platform as a Service*
IaaS	Infraestructure as a Service
UE	Unión Europea

PUBLICACIONES DE DEFENSA

GOBIERNO DE ESPAÑA MINISTERIO DE DEFENSA SUBSECRETARÍA DE DEFENSA SECRETARÍA GENERAL TÉCNICA SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y PATRIMONIO CULTURAL