
# España y CCN como referentes en la evaluación de ciberseguridad de soluciones en la nube

GOBIERNO DE ESPAÑA · MINISTERIO DE DEFENSA

20 cni ANIVERSARIO

CCN centro criptológico nacional

CCN-CERT centro criptológico nacional

ESPDEF-CERT Mando Conjunto del Ciberespacio (MCCE)

UN CIBERESCUDO ÚNICO PARA ESPAÑA



# JAVIER TALLÓN GUERRI

*jtsec Beyond IT Security*

jtallon@jtsec.es


- Ingeniero en Informática (Universidad de Granada)
- Co-Fundador & Director Técnico en jtsec Beyond IT Security S.L.
- Experto en Common Criteria, LINCE, ...
- Miembros del grupo de trabajo Ad-hoc SOG-IS en la Agencia Europea de Ciberseguridad ENISA y del SCCG (Stakeholders Cybersecurity Certification Group)
- Colaboramos en diversos foros de estandarización como ISO o CEN/CENELEC
- OSCP/OSCE/CISSP

# ÍNDICE

# EL CATÁLOGO CPSTIC

## ¿Qué es?

El catálogo de Productos y servicios de Seguridad TIC (CPSTIC) ofrece un listado de productos con unas **garantías de seguridad contrastadas** por el **Centro Criptológico Nacional**. Este catálogo incluye los **productos aprobados** para manejar información nacional clasificada y los **productos cualificados** de seguridad TIC para uso en el ENS.

## Ventajas

1. Fácil adquisición de productos ciberseguros.
2. Evaluados por parte de un tercero confiable.
3. Disponible para todo el mundo.

# EL CATÁLOGO CPSTIC

## Metodologías de evaluación de ciberseguridad

- Metodología ligera
- Alcance nacional
- Estándar sencillo orientado al análisis de vulnerabilidades y test de penetración
- Duración y esfuerzo acotados
- Más viable económicamente
- Accesible a PYMEs
- Su uso principal es la entrada en el catálogo
- Estándar UNE

**Categoría media - básica ENS**

- Metodología pesada
- Reconocida en 31 países
- Distintos niveles de garantía
- Versátil, aplicable a todo tipo de productos
- Dificultad técnica para cumplir/entender el estándar
- Mayor tiempo para su obtención
- Mayor coste económico

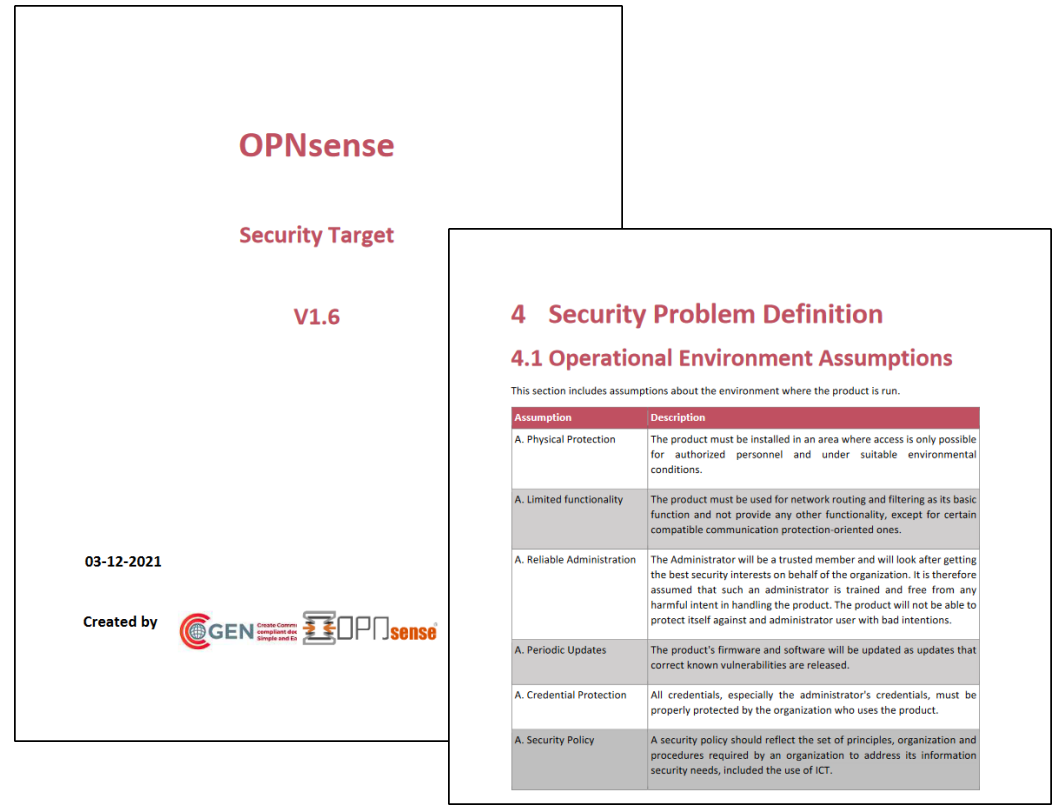
**Categoría alta ENS**

# EL CATÁLOGO CPSTIC
## La declaración de seguridad

- La ST (Security Target) recoge los requisitos funcionales de seguridad que implementa el TOE, así como el problema de seguridad.
- Las taxonomías definen un conjunto de requisitos funcionales de seguridad. ***Ej***: *La taxonomía de EDR/EPP define el siguiente requisito (uno entre tantos) que deberá cumplir todo TOE que quiera entrar en catálogo bajo la familia EDR/EPP*:

38. **MAL.1** En caso de que se detecte contenido malicioso en el espacio de memoria de un proceso, se deberá interrumpir la ejecución del mismo.

- Es **crucial** definir el alcance del TOE, así como la funcionalidad que implementa él mismo y la funcionalidad que implementa el entorno operacional. Un alcance mal definido provoca varias iteraciones sobre la ST y esfuerzo perdido en evaluación, lo que conlleva a un retraso considerable de la certificación/cualificación.


OPNsense

Security Target

V1.6

03-12-2021

Created by

4 Security Problem Definition

4.1 Operational Environment Assumptions

This section includes assumptions about the environment where the product is run.

| Assumption | Description |
|---|---|
| A. Physical Protection | The product must be installed in an area where access is only possible for authorized personnel and under suitable environmental conditions. |
| A. Limited functionality | The product must be used for network routing and filtering as its basic function and not provide any other functionality, except for certain compatible communication protection-oriented ones. |
| A. Reliable Administration | The Administrator will be a trusted member and will look after getting the best security interests on behalf of the organization. It is therefore assumed that such an administrator is trained and free from any harmful intent in handling the product. The product will not be able to protect itself against and administrator user with bad intentions. |
| A. Periodic Updates | The product's firmware and software will be updated as updates that correct known vulnerabilities are released. |
| A. Credential Protection | All credentials, especially the administrator's credentials, must be properly protected by the organization who uses the product. |
| A. Security Policy | A security policy should reflect the set of principles, organization and procedures required by an organization to address its information security needs, included the use of ICT. |

# EL CATÁLOGO CPSTIC

## Evaluación, certificación, cualificación

**Evaluación**

Un laboratorio independiente y acreditado verifica si un producto cumple la funcionalidad de seguridad declarada en un tiempo y esfuerzo acotados.

**Certificación**

El Organismo de Certificación emite un certificado de acuerdo a la funcionalidad de seguridad declarada por el fabricante.

**Cualificación**

Se ha superado una certificación de acuerdo a la funcionalidad de seguridad requerida por CCN.

# ¿Y LA NUBE QUÉ?

## Cada vez hay más SaaS

- El mercado de SaaS crece en la actualidad un 18% cada año.
- A finales de 2021, el 99% de las organizaciones utilizan una o más soluciones SaaS.
- Casi el 78% de las pequeñas empresas ya han invertido en opciones SaaS.

## Las metodologías existentes son de producto

- Common Criteria
- España (LINCE), Francia (CSPN), Alemania (BSZ), Países Bajos (BSPA).

# ¿Y LA NUBE QUÉ?

## IT-015 Requisitos para la certificación de productos que se despliegan en la nube

**REQ-2**

Desplegado en el laboratorio

**REQ-3**

Control total de la infraestructura

**REQ-5**

La funcionalidad proporcionada por la infraestructura está fuera del alcance

**REQ-6**

Identificación unívoca

# ¿Y LA NUBE QUÉ?

## Esfuerzos en common criteria

Existe un Working Group llamado The CC in the Cloud Technical Work Group (CCitC) que está desarrollando una guía de Requisitos Esenciales de Seguridad para Common Criteria en la nube.

*https://github.com/CC-in-the-Cloud/CC-in-the-Cloud.github.io/blob/main/ESR/CC_in_the_Cloud_ESR.pdf

The National Information Assurance Partnership (NIAP), Canada Common Criteria Scheme (CCCS), and Australian Certification Authority (ACA) agree with the content of the CC in the Cloud Essential Security Requirements (ESR), version 0.3, dated 2 March 2022.

*https://www.niap-ccevs.org/MMO/GD/CC%20in%20the%20Cloud%20Position%20Statement%20v1.0.pdf

# ¿Y LA NUBE QUÉ?

## Evaluación, certificación, cualificación

**Known evaluation gaps**

- Analysis is static
- Use of cryptograpy
- Platform abstraction
- Environmental evoluation

**New threat models**

- Configuration
- Credentials
- Data sovereignty
- Key management
- Insider threat
- Multi-tenant

# ¿Y LA NUBE QUÉ?

## Diferencias con otras certificaciones operacionales en la nube

Son certificaciones centradas en SGSI (Sistema de Gestión de Seguridad de la Información), no en producto.

Algunas de las más aplicadas son (27001, ENS, BSI Cloud C5, ANSSI SecNumCloud, SOC2, CSA EUCS…)

# POR LO TANTO, ¿CÓMO PODEMOS CUALIFICAR SERVICIOS?

# CUALIFICANDO SERVICIOS


# CUALIFICANDO SERVICIOS
## Historia de la Guía CCN-STIC 106

**Planteamiento naive**

1.1 Certificamos on – premise (incluye pentest de la metodología)
1.2 Desplegamos en la nube
1.3 Pentest en la nube (5 días)
1.4 + ENS del proveedor de la nube

**Problema: La mayoría de los servicios en la nube son cloud nativos**


**Lo más común**

2.1 Utilizamos LINCE adaptada a la nube sobre el servicio ya desplegado
2.2 No es necesario pentest adicional puesto que ya está incluido en la evaluación basada en LINCE inicial
2.3 +ENS del proveedor de la nube

**Problema: ¿quién cualifica los servicios de los hiperescalares?**


**Cerrando el círculo**

3.1 Los servicios de los hiperescalares también requieren ser cualificados

# CUALIFICANDO SERVICIOS

## Tarea 1: Análisis de Requisitos

- La primera tarea consiste en definir a qué taxonomía pertenece el servicio a cualificar. Además de la taxonomía adecuada, todo servicio en la nube debe adecuarse a otra taxonomía: "Servicios en la nube" (Anexo G).

- El siguiente paso consiste en analizar el servicio, definiendo sus componentes y el alcance del TOE. Tras esto, se genera el **RFS Rationale** en el que se listan todos los RFS que lista la taxonomía y se les aplica las siguientes etiquetas:

**APPLICABLE** | **NOT APPLICABLE** | **COVERED** | **CANNOT BE TESTED**

# CUALIFICANDO SERVICIOS

## Tarea 2.1 Generación de la ST

- Tras finalizar con el RFS Rationale, se genera la declaración de seguridad. Esta declaración de seguridad recoge los RFS Applicable y Cannot be Tested (son necesarios para definir el problema de seguridad).
- La ST solo recoge los RFS relacionados con la taxonomía a la que se adecua el producto (no los que aparecen en el Anexo G: Servicios en la nube).
- Los RFS que se definen en la ST se verifican posteriormente en el laboratorio mediante las pruebas funcionales y de penetración. Para ello se hace uso de toda interfaz disponible en el TOE.

# CUALIFICANDO SERVICIOS

## Tarea 2.2 Evaluación de la ST y generación del ETR

El laboratorio es el responsable de validar la ST y de generar el ETR (Evaluation Test Report).


Para ello usaremos la metodología LINCE adaptada a la nube

- Se elimina el límite de esfuerzo y duración de la metodología, adaptándolo al tamaño del TOE
- Ciertas tareas no son aplicables, e.g. fase de instalación
- Se admite mayor flexibilidad en ciertos aspectos, e.g. versiones del producto

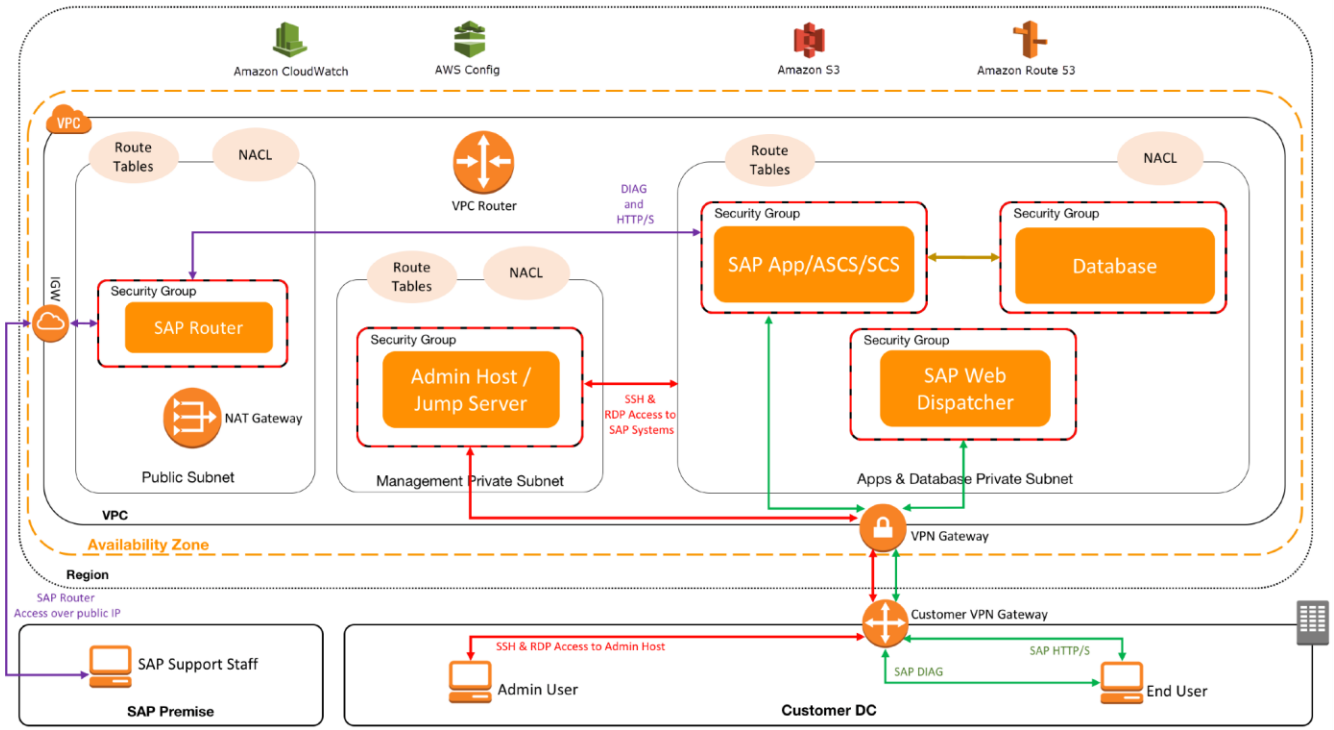
# CUALIFICANDO SERVICIOS

## Tarea 3. Arquitectura de seguridad

El fabricante debe garantizar la seguridad de la parte de la solución que se encuentre en la nube. Para ello el fabricante definirá en el documento "Arquitectura de seguridad:

a) La descomposición en bloques de la solución.
b) La relación entre los bloques.
c) Qué servicios de terceros que usa la solución están cualificados (ej: AWS S3).
d) Qué datos sensibles maneja la solución y cómo se produce el flujo de estos.

La nube donde se hostea el servicio debe disponer de la certificación ENS y cumplir con la GDPR.



# CUALIFICANDO SERVICIOS

## Tarea 4. Declaración responsable

El fabricante deberá firmar responsablemente que:

**1**

La veracidad de los datos presentados en la Arquitectura de seguridad.

**2**

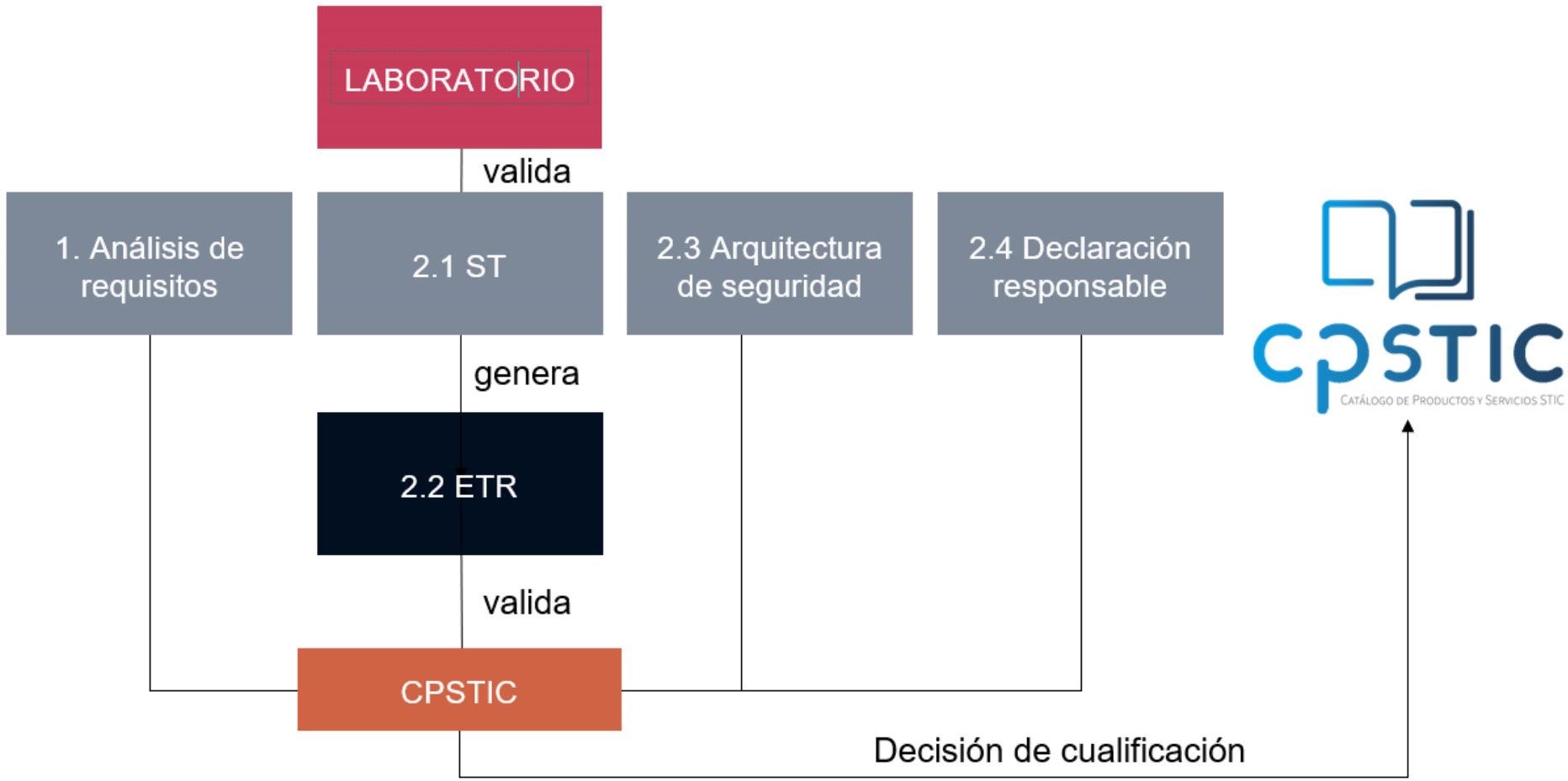
Los datos manejados por la solución cumplen con los límites geográficos estipulados.

**3**

Los futuros usuarios de la solución podrán requerir y recibir logs de auditoría relacionados con el uso del servicio. Además, de que estos logs no presentarán información de otros usuarios.

# CUALIFICANDO SERVICIOS

## Validación de documentos



# EXPERIENCIAS

**1**

Falta de control sobre el TOE y sus versiones

**2**

Interoperabilidad vs seguridad (los servicios en la nube tienen que ser compatibles con software obsoleto) (e.g versiones antiguas de SSL/TLS)

**3**

Hay que pedir permiso para probar (riesgos de DoS)

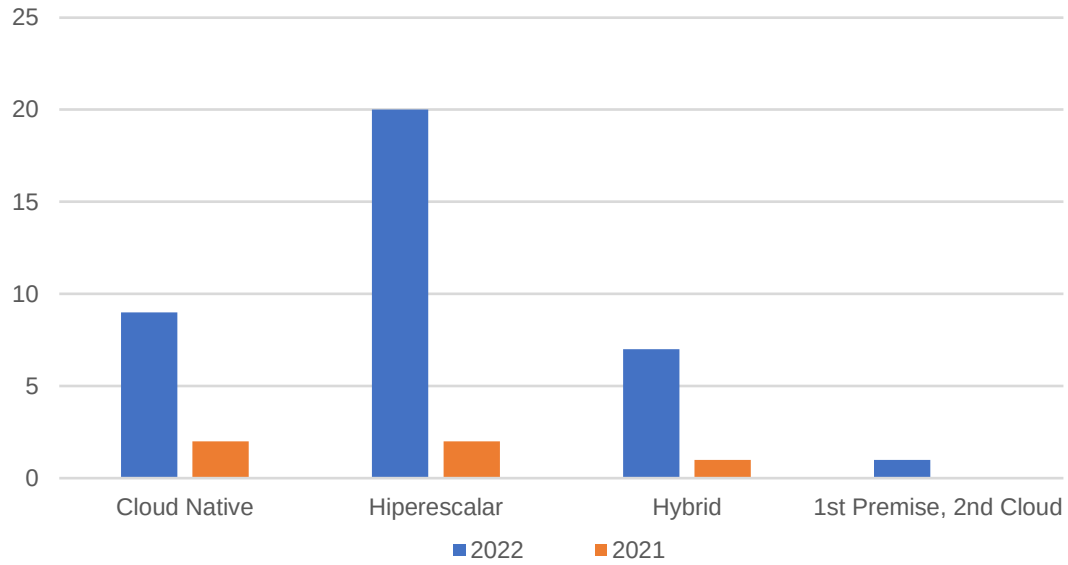
**4**

Productos mixtos agente + server (e.g. la taxonomía de AV/EDR exige que se cualifiquen ambas partes)

# EXPERIENCIAS

- Average number of tests: 31
  - Average failed tests: 5
- Average number of pentests: 22
  - Average failed pentests: 4

jtsec
BEYOND IT SECURITY

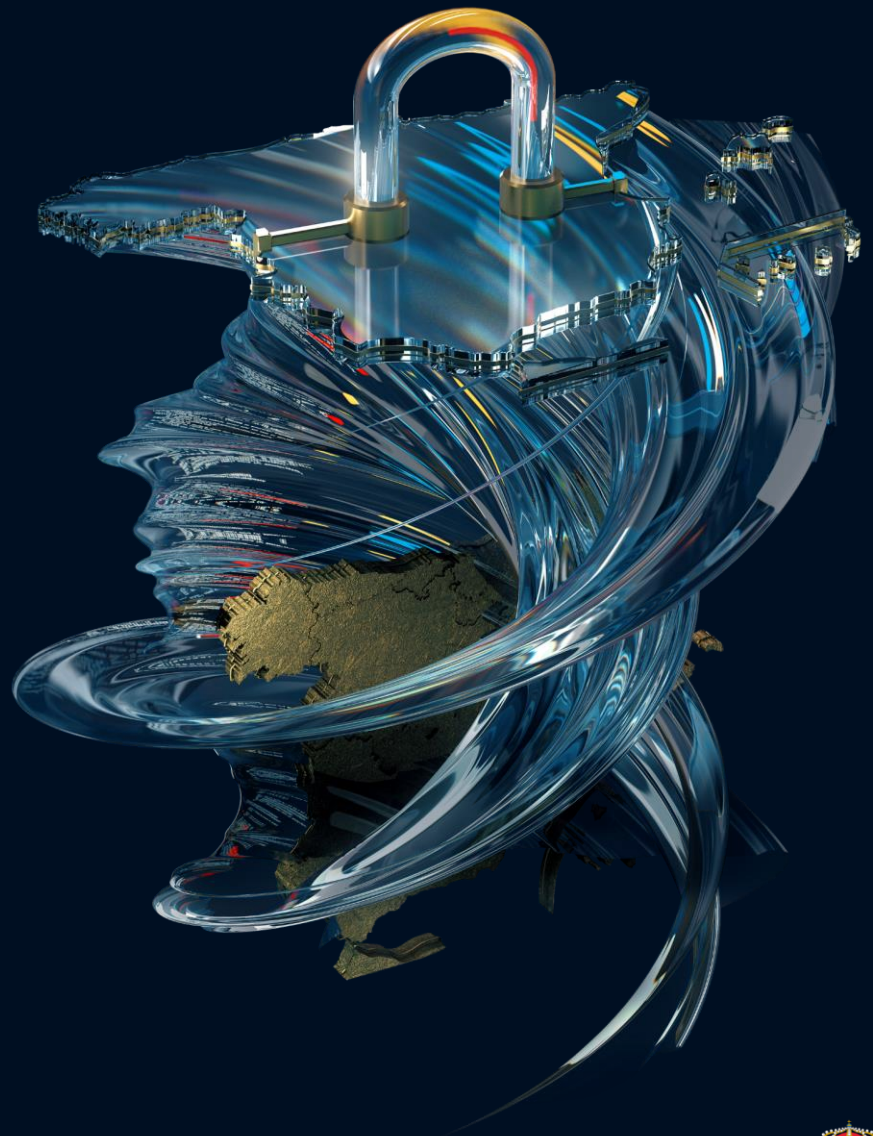


# CONCLUSIONES

- Todas las metodologías que existen son para evaluar productos on premise
- No se espera a nivel europeo ninguna metodología que evalúe productos en la nube.
- Common Criteria tardará años en publicar los requisitos Esenciales de Seguridad para Common Criteria en la nube en los que están trabajando.
- España es pionera en cualificar servicios en la nube

# CONCLUSIONES

CRA (9) “This Regulation ensures a high level of cybersecurity of products with digital elements. **It does not regulate services, such as Software-as-a-Service (SaaS)**, except for remote data processing solutions relating to a product with digital elements understood as any data processing at a distance for which the software is designed and developed by the manufacturer of the product concerned or under the responsibility of that manufacturer, and the absence of which would prevent such a product with digital elements from performing one of its functions” […] **[Directive XXX/XXXX (NIS2)] applies to cloud computing services and cloud service models, such as SaaS**. All entities providing cloud computing services in the Union that meet or exceed the threshold for medium-sized enterprises fall in the scope of that Directive.



# Muchas gracias

GOBIERNO DE ESPAÑA · MINISTERIO DE DEFENSA

20 cni ANIVERSARIO

CCN centro criptológico nacional

CCN-CERT centro criptológico nacional

ESPDEF-CERT Mando Conjunto del Ciberespacio (MCCE)

UN **CIBERESCUDO ÚNICO** PARA **ESPAÑA**