



# STORMSHIELD

Network

Endpoint


Data

# Stormshield Iberia



**Borja PÉREZ**  
Country Manager

[Borja.perez@stormshield.eu](mailto:Borja.perez@stormshield.eu)



**Soluciones de  
ciberseguridad soberanas y  
certificadas para  
cumplimiento de ENS**

# Filial de la mayor historia de **éxito industrial de Europa**

AERONAVES

**AIRBUS**

HELICÓPTEROS

DEFENCE  
& SPACE

CONNECTED  
INTELLIGENCE  
Defence Digital  
& Cyber



**STORMSHIELD**



# ¿Qué sucede con la soberanía en **ciberseguridad**?

**Control de los  
datos**

**Autonomía  
tecnológica**

**Protección de  
infraestructuras  
críticas**

**Regulación y  
cumplimiento**

**Cooperación  
internacional**

# ¿Cuáles son los riesgos de la tecnología no soberana?

## Dependencia del extranjero

Tensiones geopolíticas, riesgo de interrupciones del suministro.

## Desigualdades competitivas

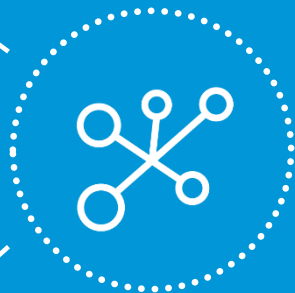
Retraso económico debido a la falta de tecnología

## Influencia cultural e ideológica

Afectando el pensamiento, valores y usos locales

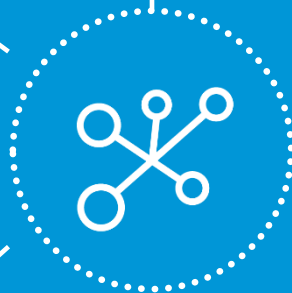
## Innovación limitada

Dependencia extranjera que frena la creación de valor, la innovación local y la motivación para desarrollar nuevas soluciones.



**Vulnerabilidades**  
Exposición de las infraestructuras críticas a ciberataques, vía sistemas que pueden contener fallos de seguridad

**Incrementos de precio**  
Riesgo de aumento de aranceles que tendrían un impacto en la compra de materiales. La pérdida de competitividad puede llevar a una caída del valor de la moneda.



**Pérdida de datos y confidencialidad**

Empresas extranjeras pueden almacenar y procesar datos sensibles. Preocupación legítima sobre privacidad y soberanía del dato.

**Espionaje**

La exposición de infraestructuras críticas a ciberataques vía sistemas que puedan contener puertas traseras

# Soluciones de seguridad cualificadas y certificadas



France CyberSecurity

---



Common Criteria

---



UE Restricted

---



NATO / OTAN

---



Certificación  
**CCN** (España)



VISA de sécurité ANSSI

---

Certifications EAL3+ / EAL4+  
**Qualification Standard**



Bundesamt  
für Sicherheit in der  
Informationstechnik

---

Certificación  
**BSI** (Alemania)

# Soluciones de ciberseguridad **cualificadas** y **certificadas**



Certificación  
**CCN** (España)

# Soluciones de ciberseguridad **cualificadas** y **certificadas**



mediante suscripciones a [noticias](#) podremos estar informados diariamente de las últimas vulnerabilidades detectadas en dispositivos.

### Título

### Fecha publicación

#### Min

dd/mm/aa

#### Max

dd/mm/aa

### Fabricante

### Productos

- Cualquiera -

### Severidad CVSS

## CVE-2026-47311

#### Fecha de publicación:

19/05/2026

Idioma: Inglés

**\*\*\* Pendiente de traducción**  
**\*\*\* Heap-based buffer overflow vulnerability in Samsung Open Source Escargot allows Overflow Buffers. This issue affects...**



#### Gravedad CVSS v3.1: ALTA

Última modificación:

19/05/2026

## CVE-2026-8813

#### Fecha de publicación:

19/05/2026

Idioma: Inglés

**\*\*\* Pendiente de traducción**  
**\*\*\* This affects versions of the package exifreader before 4.39.0. A crafted image containing an ICC mluc tag can set an attacker...**



#### Gravedad CVSS v4.0: ALTA

Última modificación:

19/05/2026

## CVE-2026-8814

#### Fecha de publicación:

19/05/2026

Idioma: Inglés

**\*\*\* Pendiente de traducción**  
**\*\*\* Versions of the package exifreader before 4.39.0 are vulnerable to Improper Handling of Highly Compressed Data (Data...**



#### Gravedad CVSS v4.0: MEDIA

Última modificación:

19/05/2026



# ¿Cómo **mitigar los riesgos**?



## **Elección soberana**

Optar por una **solución europea** y **mantener control** de los datos



## **Cumplimiento**

El cumplimiento regulatorio **limita los riesgos de ciberseguridad**



## **Opción inteligente**

Elegir una solución **a medida de las necesidades**, no aquella con el mayor número de funcionalidades.

*En 2024, más de la mitad de operaciones de ciberdefensa de la ANSSI tuvieron su origen en una vulnerabilidad de equipos de seguridad... Es inaceptable éticamente porque a menudo compramos, a un precio considerablemente alto, equipo de seguridad en el que confiamos. Cuando se convierte en el punto de entrada para el atacante, hay algo sorprendente.*

Vincent Strubel – Forum InCyber 2025

# Gracias

Estamos a su disposición



**STORMSHIELD**

## Contacto



Paseo de la Castellana, 200  
28046 Madrid ESPAÑA



+34 91 902 72 44



iberia@stormshield.eu