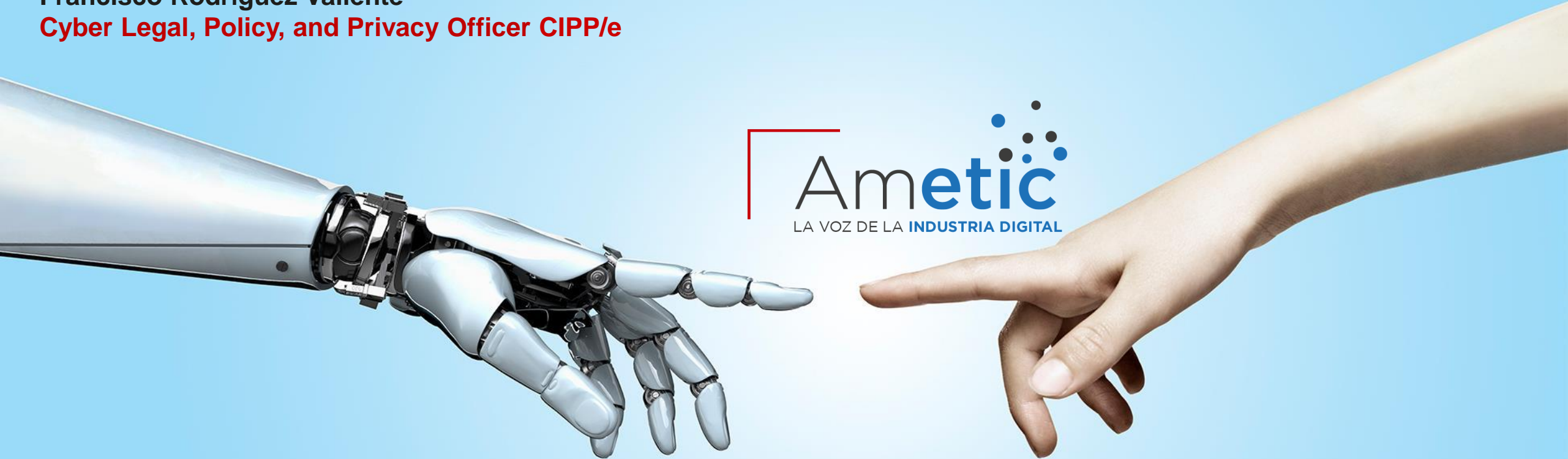


Buenas prácticas de la ciberseguridad Española

Contribución al desarrollo de talento y conocimiento

Francisco Rodríguez Valiente

Cyber Legal, Policy, and Privacy Officer CIPP/e



universidad
de león



Centro de Experiencia en Ciberseguridad de Huawei en la Universidad de León



MoU with University of León (ULE): increasing Cyber Security awareness and skills development

2023.01

MOU
Kick off
ceremony



2023.04-05

Professional development:
5G Security Training with attendees from ULE and other stakeholders

2023.06

Security Operations drill
5G Cyber Range event :
Spain CS stakeholders
participation

2023.10

León CSEC opening
(CS Experience Center)
1) **First use case: "Securing 5G Private Networks"**
methodology: L1 and L2
2) **Q&A for SME's Cybersecurity whitepaper presented at ENISE**

2024

New
workstreams

Training Agenda: 6 days

5G Cyber Security **Concept and Industry Consensus** Overview

- 5G Cyber Security Development Trend

0.5 day

5G Cyber Security **Standards and Certifications** Interpretation

- 3GPP 5G Security Standards
- NESAS&SCAS Security Certification Standards

1 day

5G Cyber Security **Threat Analysis and Countermeasures** Introduction

- Overview of Network Security Threat Analysis Methods
- App and Service Security Threat Analysis and Countermeasures
- 5G Mobile Terminal Security Threat Analysis and Countermeasures
- 5G Wireless Access Network Security Threat Analysis and Countermeasures
- 5G Core Network Security Threat Analysis and Countermeasures
- 5G Cloud Infrastructure Security Threat Analysis and Countermeasures
- 5G Network Operation and Management Security Threat Analysis and Countermeasures

1.5 days

5G Cyber Security **Solution Design**

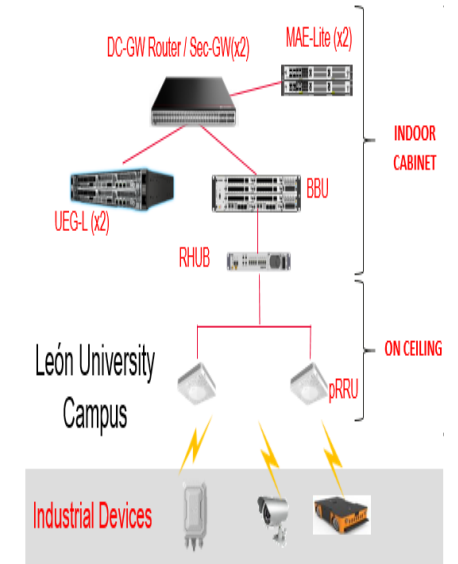
- 5G RAN Security Solution
- 5G Core Security Solution
- 5G Cloud Infrastructure Security Solution
- 5G Network Slicing Security
- 5G MEC Security Solution
- 5G Communication Capability Exposure Security

3 days

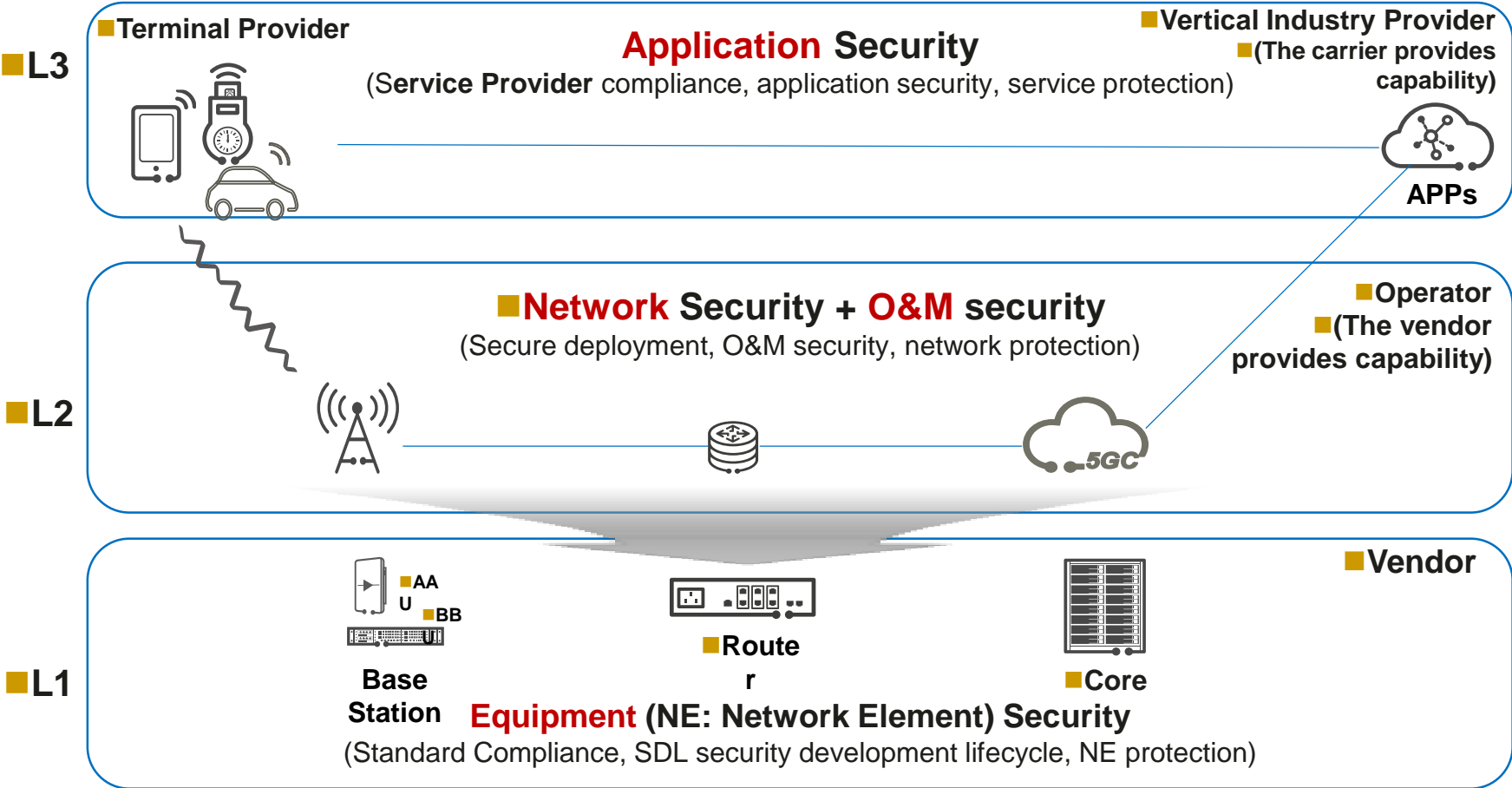


5G MPN Laboratory for University of León

INDOOR CABINET	
47U	Air Duct
46U	
45U	
44U	ETP48400CGA3 (BU) (Power System)
43U	
42U	
41U	
40U	Air Duct
39U	Air Duct
38U	Air Duct
37U	RHUB
36U	Cable trough
35U	
34U	BBU
33U	Cable trough
32U	FW - Eudemon
31U	Cable trough
30U	FW - Eudemon
29U	Cable trough
28U	UEG - L (Active)
27U	
26U	Cable trough
25U	UEG - L (Active)
24U	
23U	Cable trough
22U	
21U	MAE Lite (OSS)



Ciberseguridad E2E en 5G: modelo por capas aceptado por la industria



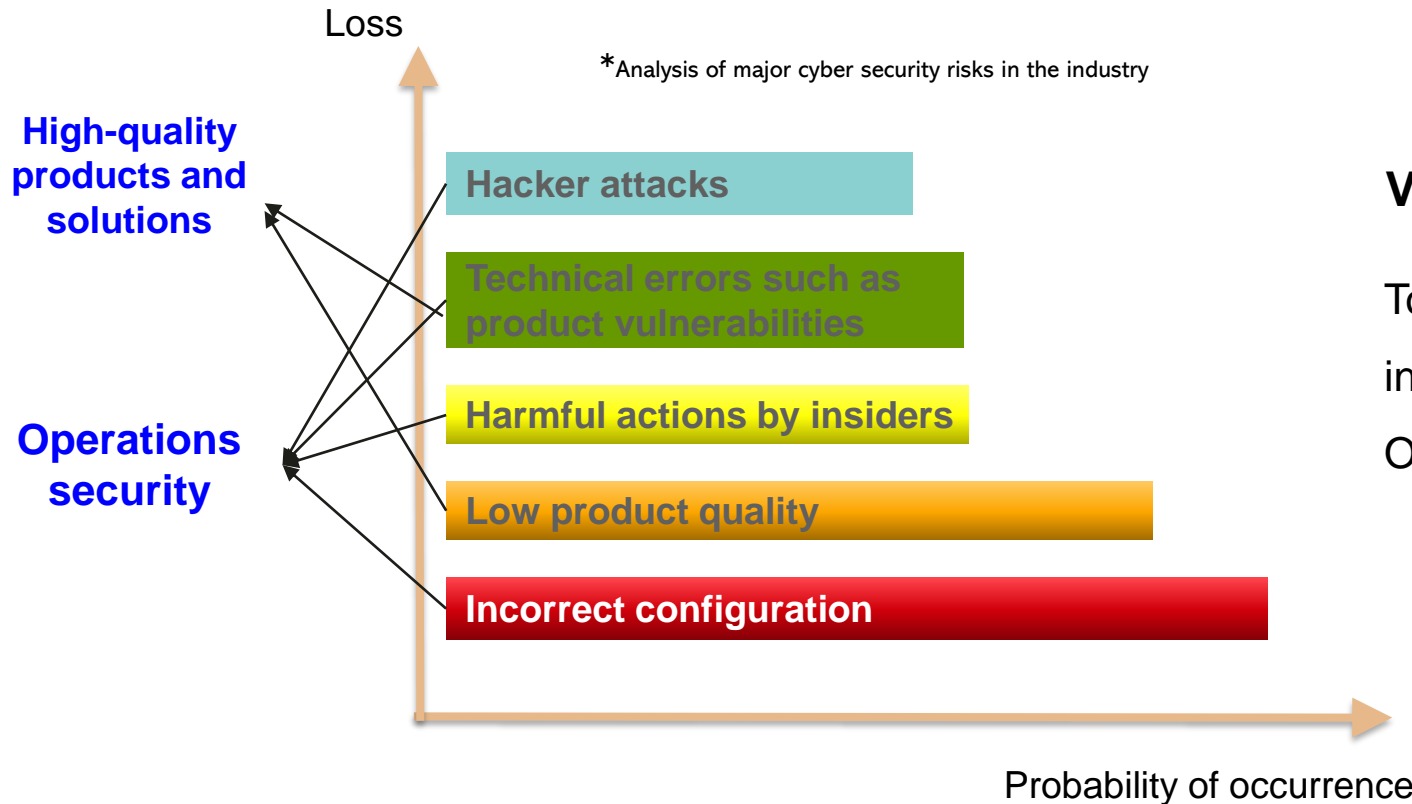
- Estándares y metodologías en la industria
- ISO/IEC 62443 IACS, ISO/IEC 27034
- NIST CSF, NCSC CAF, 3GPP, GSMA 5G CKB
- (5G Cybersecurity Knowledge Base)
- ISO19600, NIST SSDF, NIST SP800-160, 3GPP, GSMA NESAS / 3GPP SCAS
- (Network Equipment Security Assurance Scheme / SeCuriry Assurance Specification)

El modelo de seguridad por capas es ampliamente aceptado en la industria de las telecomunicaciones.

La seguridad en redes 5G se sustenta en la "responsabilidad compartida" entre los diferentes actores.



¿Qué hace a una red insegura?



Viewpoints of the security industry:

To ensure cyber security across the industry, it is necessary to focus on both O&M security and product security.

Network operators shall first consider purchasing **high-quality and secure products** and then pay attention to the **secure operations of equipment**, including correct security configuration and prompt vulnerability remediation.

Security Configuration Check Tool (5G RAN Base Station):

Helps Customers Implement Baseline Management More Conveniently and Intelligently



Flexible and customizable Baseline management

Manually configured based on network requirements



Auto Fast Identify risks.

Automatic check, minute-level/10,000 base stations



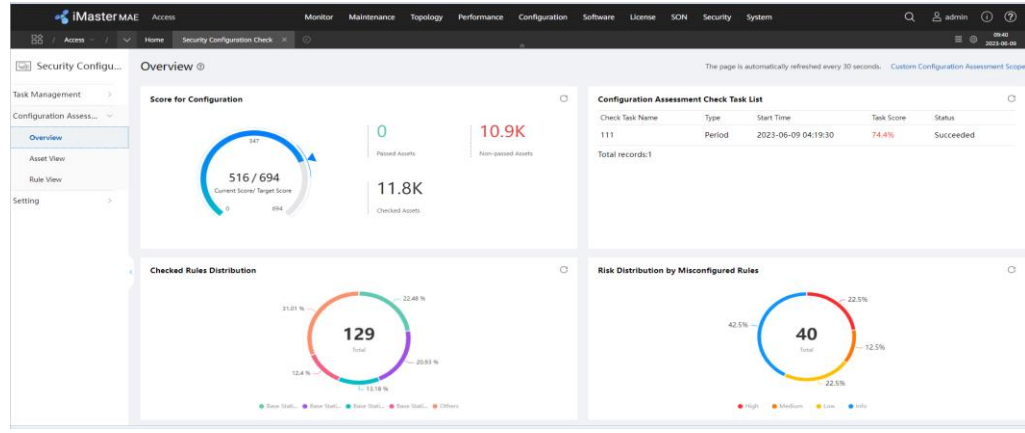
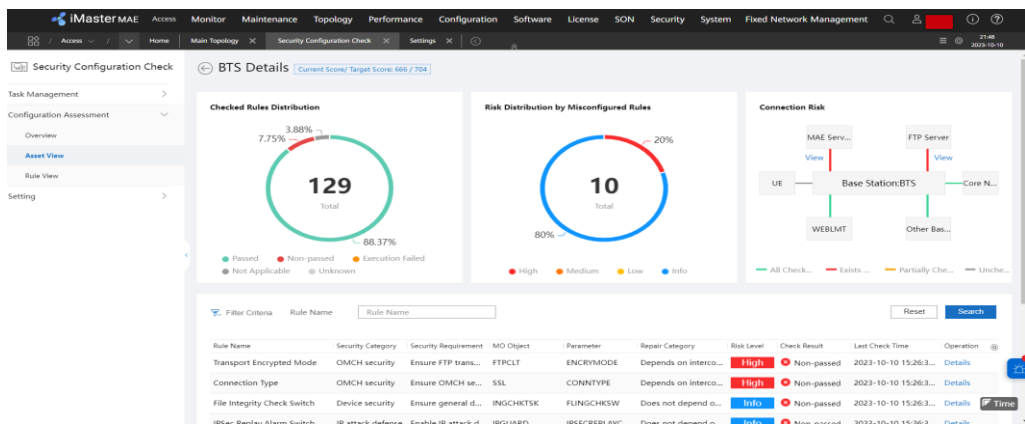
multi-dimensional Risk Quantification

Automatically displaying check results



Precise risk Closed-loop guidance

Manually fix the problem according to the customer's process.



Details

Overview

Asset name: BTS, Asset IP: 10.56.49.28.
Check Rules: 129 items, 112 items passed.

Check Result

Rule Name	Security Category	Risk Level	Check Result	Last Check Time	Operation
Transport Encrypted Mode	OMCH security	High	Non-passed	2023-10-10 15:26:3...	Details
Connection Type	OMCH security	High	Non-passed	2023-10-10 15:26:3...	Details
File Integrity Check Switch	Device security	Info	Non-passed	2023-10-10 15:26:3...	Details

Details

Rule Name
NG Interface Control-Plane Transmission Security

Rule Description
Indicates whether to enable IPsec or DTLS for ciphertext transmission on the control plane of the NG interface.

Risk Description
NG-C transmission security indicates whether NG-C data may be transmitted in plaintext. If the check result of NG-C transmission security is not satisfied, NG-C data may be transmitted in plaintext. That is, DTLS or IPsec is not used for encryption, which may cause data leakage and tampering.

If the check result is not satisfied, the possible causes are as follows:
1. DTLS and IPsec are not enabled.
2. DTLS has been enabled, but the DTLSCONNPOLICY parameter is set to DTLS_PRIORITY.
3. IPsec has been enabled, but data flows on the service link are not directed to IPsec tunnels.

Repair Category
Depends on the overall planning of the transport network.

Repair Suggestions
You are advised to enable and check DTLS and IPsec according to the official product documentation. If plaintext connections must be used due to service requirements and the security risk is acceptable, this check item can be skipped so that the risk warning message for the rule item is not displayed during the check. If DTLS or IPsec has been enabled, you can perform the following operations:
Due to differences between versions, the following operations are for reference only. For actual operations, see the official product documentation of each version.
1. If DTLS has been enabled, run the LST SCTP:HOST command to check whether the DTLSCONNPOLICY parameter is set to DTLS_PRIORITY. If the parameter is set to DTLS_PRIORITY, run the MOD SCTP:HOST command to modify it.
2. If IPsec has been enabled but data flows on the service link are not directed to IPsec tunnels, you are advised to check the route (for the old model, run the LST IPRT and LST SRCPRT commands for the new model, run the LST IPROUTE4, LST SRCPROUTE4, and LST SRCPROUTE6 commands) and ACL rule configurations (run the LST ACLRULE and LST ACLRULE6 commands).
---End

Repair Impact
Before the modification, evaluate the feasibility of the solution, make a detailed reconstruction plan, and ensure that the parameter settings at the local end are consistent with those at the peer end. Otherwise, services or the remote OM channel will be interrupted.

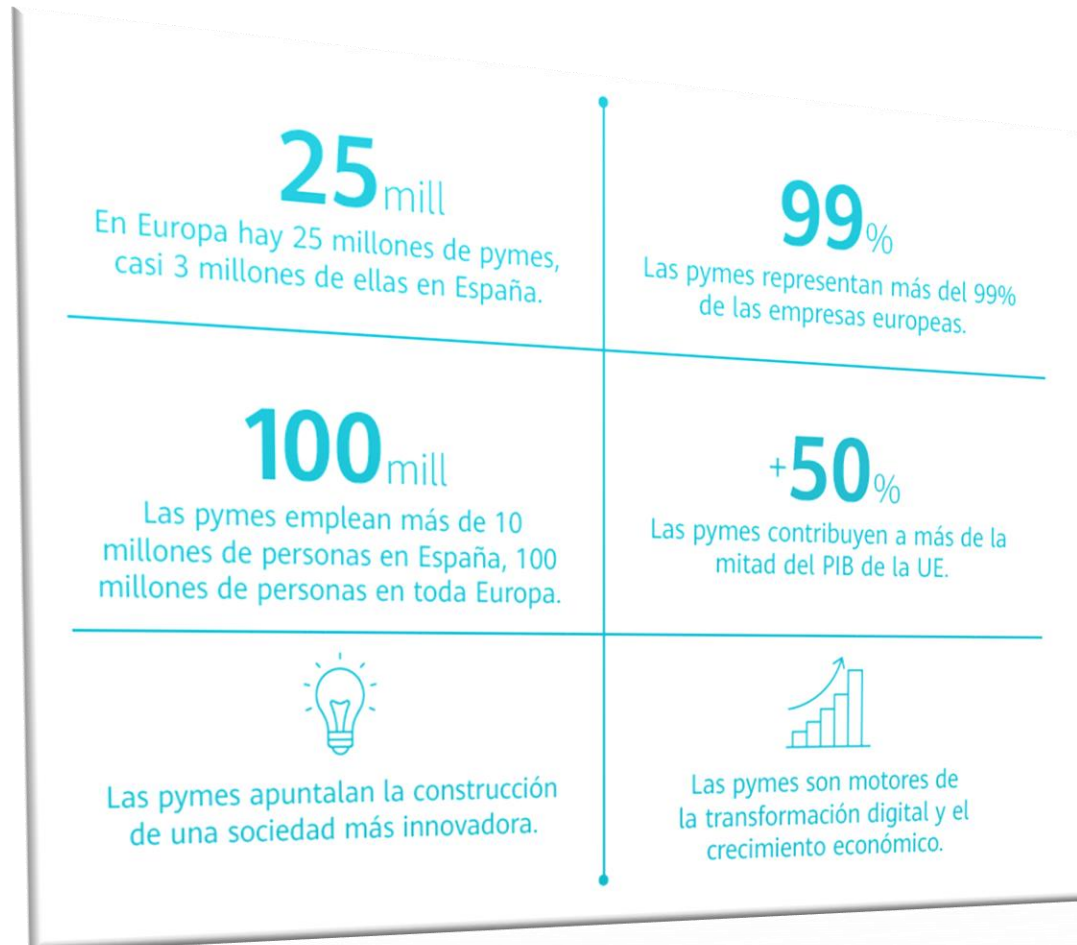


Guía para la Ciberseguridad en las PYMES (SME)



¿Por qué las PYMES (SME) son tan importantes?

■ **Ciberseguridad de la cadena de suministro:** Resistencia de cada empresa, producto o servicio que interviene en la entrega de un producto o solución al usuario final.

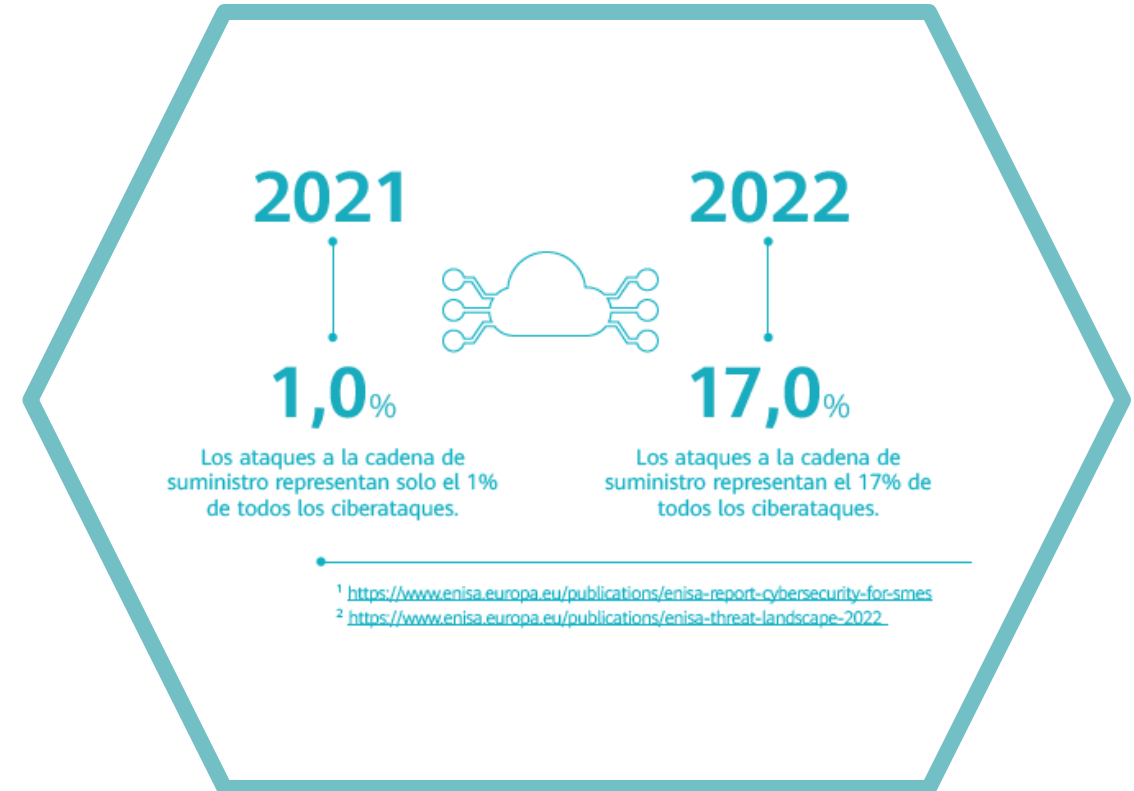


<https://www.huawei.com/-/media/corporate/local-site/es/pdf/guia-de-ciberseguridad-para-pymes-huawei.pdf?la=es>

Desafíos



Ciber-resiliencia en la UE



01

Cifrado, robo o modificación de la información, por ejemplo, para pedir un rescate o revender los datos.

02

Supervisión de los flujos de datos, por ejemplo, en beneficio del atacante.

03

Tomar el control de un dispositivo, por ejemplo, para provocar un incidente.

Identificar procesos y recursos críticos de la empresa (Riesgos)

Implantar medidas de seguridad

Herramientas y dispositivos

Planes de recuperación y de comunicación

- Control de acceso estricto, gestión segura de contraseñas
- Gestión vulnerabilidades
- Copia de seguridad de los datos
- Instalación y mantenimiento de cortafuegos
- Acceso Wifi protegido
- Redes privadas (VPN)



Dirección



Reconocer

Amenazas

- DDOS
- Malware
- Phishing
- Ransomware

Qué hacer



¿Cuál es la política de la UE y España en materia de apoyo a las PYMES desde el punto de vista de la ciberseguridad?

Regulación

Cyber Security Act

Directiva NIS2

Cyber Resilience Act

Inversión Europa y España

INVEST EU | **HORIZONTE EUROPA**

€10 bil

La UE ha asignado 10.000 millones de euros para acciones de colaboración en materia de ciberseguridad dentro del programa de investigación, innovación y ciencia Horizonte Europa 2021-2027.

España digital 2026

Activa Ciberseguridad

KIT DIGITAL

<https://www.industriaconectada40.gob.es/programas-apoyo/Paginas/ACTIVA-Ciberseguridad.aspx>

<https://www.red.es/es/iniciativas/proyectos/kit-digital>

Organismos de Referencia

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

incibe
INSTITUTO NACIONAL DE CIBERSEGURIDAD