



MINISTERIO
DE INDUSTRIA
Y TURISMO



Oficina Española
de Patentes y Marcas

Cyber Resiliency and Best Practices



WIPO ICT Leadership Dialogue (WILD) 2025

WIPO FOR OFFICIAL USE ONLY



ABOUT THE SPTO

The SPTO is an Autonomous Body of the General State Administration that promotes and supports technological and economic development by granting legal protection to the different types of industrial property.

SPTO Today: An Overview

We are the official body responsible for granting the following industrial property rights: patents, utility models, trademarks, trade names, designs, and semiconductor product topographies.

In addition, we promote economic development, innovation, and competitiveness by encouraging the awareness and use of industrial property.



MINISTERIO
DE INDUSTRIA
Y TURISMO



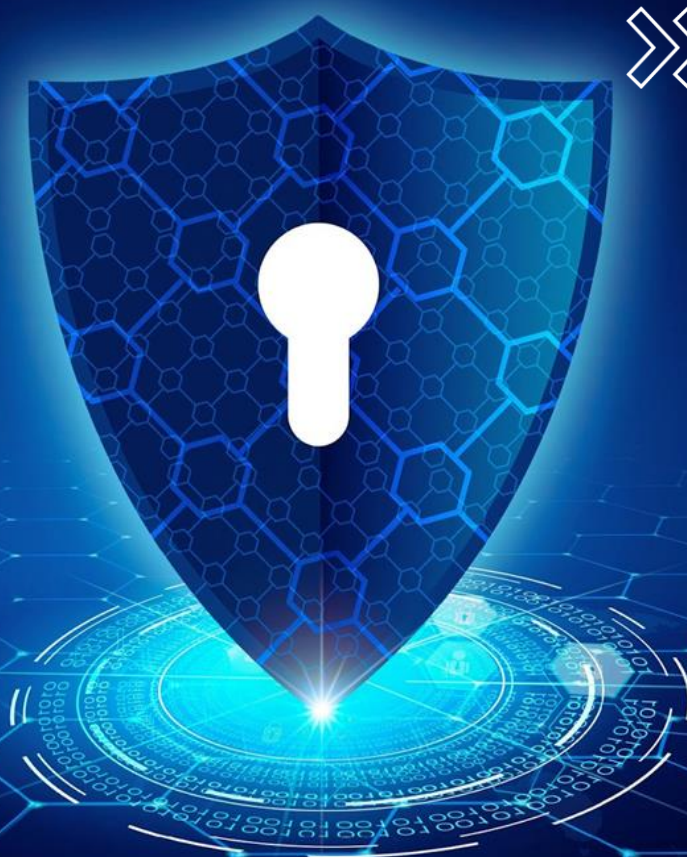
Oficina Española
de Patentes y Marcas

oepm.es



360° SECURITY AT THE OEPM

SPANISH PATENT AND TRADEMARK
OFFICE



TOWARDS AN INTEGRATED SECURITY FRAMEWORK



2017

High-Impact
Attack.

YES/NO

Physical Security
Information Security
Employee Security
Incident
Management and
Crisis Response

Cybersecurity
Awareness and
Training
Regulatory
Compliance
Assessment and
Continuous
Improvement

2018

August: First
Cybersecurity Contract.
The OTSI was created.
September:

- First Security
Architecture Audit
- Initial Application
Vulnerability Audits
- Planning of Regulatory
Compliance Audit

2019

Initial Version of the
Approved Crisis Plan.

Start of the Awareness
Program.

Security by Design (SDLC)
Rollout.

Beginning of the
Regulatory Compliance
Evaluation.

YES/NO

Physical Security
Information Security
Employee Security
Incident Management and
Crisis Response
Cybersecurity
Awareness and Training
Regulatory Compliance
Assessment and Continuous
Improvement

2020

Continuous
Improvement

360-Degree
Model



2021 - 2024

2021: Establishment of the AGE
Cybersecurity Operations Center (COCS)
2023: Beginning of the Service Integration
Plan
2024: Establishment of the Cybersecurity
Unit at the OEPM.

- Perimeter Architecture Integration.
- Synergies Between Cybersecurity
Services.
- Adaptation of Policies

REGULATORY COMPLIANCE AND STANDARDS

NATIONAL SECURITY FRAMEWORK (ENS)

The ENS establishes the basic principles and minimum requirements for the adequate protection of information managed by Public Administrations.

ENS Adaptation

- Assessment of the current compliance level
- Implementation of technical and organizational controls
- Internal audit to validate conformity

Implementation of NIS2 and Reinforcement of ISO 27001/27002

- Adaptation to the requirements of the NIS2 Directive
- Development of incident response strategies
- Certification or improvement of the ISMS based on ISO 27001



PATENT CHALLENGES



Stop the Rise of Cyberattacks

Public administrations have experienced a significant increase in the number of cyberattacks, with over 25,000 incidents reported recently—representing a 190% rise compared to the previous year.



Increase in Cybersecurity Investment

The digital transformation of public administration is challenged by budget limitations, preventing the deployment of essential infrastructures and technologies for effective security.



Continuous Cyber Awareness and Talent Acquisition

A shortage of qualified cybersecurity experts in the public sector hampers effective incident management and response.



Protection of Sensitive Data

Secure management of confidential information is critical, especially in the face of threats like ransomware, which can encrypt essential data and demand ransoms for its release.



PRESENT AND FUTURE CHALLENGES

- > Ongoing Development of the 360-Degree Security Model
- > Continuous Regulatory Alignment: Security Policies in Line with European Standards (NIS2)
- > Adoption of Emerging Technologies
- > Cyber Resiliency and Best Practices

Do we have a plan?

There is no single plan for every scenario



LESSONS LEARNED FROM THE ATTACKS WE HAVE EXPERIENCED...

- 1 Agile reaction time is key to reducing the impact.
- 2 It is essential to have learned and practiced the procedures.
- 3 The human factor remains the preferred vector of attack.
- 4 Credibility and reputation will always be affected (difficult to recover).
- 5 Having practice exercises optimizes the localization of vulnerabilities.



THANKS FOR YOUR ATTENTION!



MINISTERIO
DE INDUSTRIA
Y TURISMO



Oficina Española
de Patentes y Marcas

oepm.es

