ZEROLYNX | OSANE CONSULTING
A ZEROLYNX COMPANY

CYBERSECURITY & INTELLIGENCE

Cybersecurity in the **Public** Sector

OVERVIEW

Public administrations constantly face fundamental challenges for the security and stability of the country. In the aftermath of the pandemic and in a global scenario of conflict, resilience is a key element for government entities to continue fulfilling their role as stewards of public welfare, protecting the data and essential services provided to citizens.

CHALLENGES

The country's cyber defense encompasses various challenges such as espionage, denial-of-service attacks against essential assets, or data exfiltration, all of which are critical issues for the commitment to national security. On the social front, the spread of fake news and disinformation pose notable threats that could undermine trust in institutions and social stability. Finally, in the realm of internal security, data theft, fraud, and disruption of supply chains are among the other major issues that could result in significant losses for our institutions.

SOLUTIONS

Public administrations are legally required to implement cybersecurity in line with their responsibilities. Zerolynx designs, implements, maintains, and operates comprehensive cybersecurity plans based on on the six areas of NIST (Govern, Identify, Protect, Detect, Respond, and Recover).

BENEFITS

Identification and Detection

Through our cyber intelligence and ethical hacking services, we offer a comprehensive solution, monitoring, detecting, and reporting various risks, such as exposed confidential data or severe vulnerabilities, ensuring the security of infrastructure and sensitive data.

Protection and Response

Our cybersecurity and DFIR (Digital Forensics and Incident Response) services safeguard your institution's attack surface, mitigate and respond to any threat, minimizing the impact on public services.

KEY FIGURES

- **40% of entities affected** by the Spanish National Security Framework still **do not meet the minimum requirements.**
- **Spain is the most cyber-attacked European country** and the **third globally**, behind the United States and Japan.
- **40% of identified attacks** on Spanish administrations were **successful**. **50% were directed at Local Entities**.

"Zerolynx, alongside the Spanish Home Office, ensured the security of the general elections on 23 June 2023. Thanks to the support of Zerolynx and other participating organizations, the elections were conducted without incidents, even though various malicious actors attempted attacks on other public and private infrastructures during the election day."

Francisco Alonso Batuecas
Head of the ICT Infrastructure and Security Area at the Spanish Home Office

TOP REFERENCES

MINISTERIO DEL INTERIOR · renfe · EUSKO JAURLARITZA GOBIERNO VASCO

ABOUT ZEROLYNX

European Cybersecurity and Intelligence Provider.
Global Top 100 Providers ranked 2023.

info@zerolynx.com
info@osaneconsulting.com

CYBERSECURITY MADE IN EUROPE