sia

An Indra company

Cybersecurity Solutions

Public Administrations

BEYOND CYBERSECURITY

The four forces of digital transformation

Digital transformation is driving the new economy. And it is governed by four great forces:

I. Digital interaction of people

II. Regulatory pressure

III. Evolution of Information Technologies

IV. Development of connected infrastructures and the development of the Internet of Things

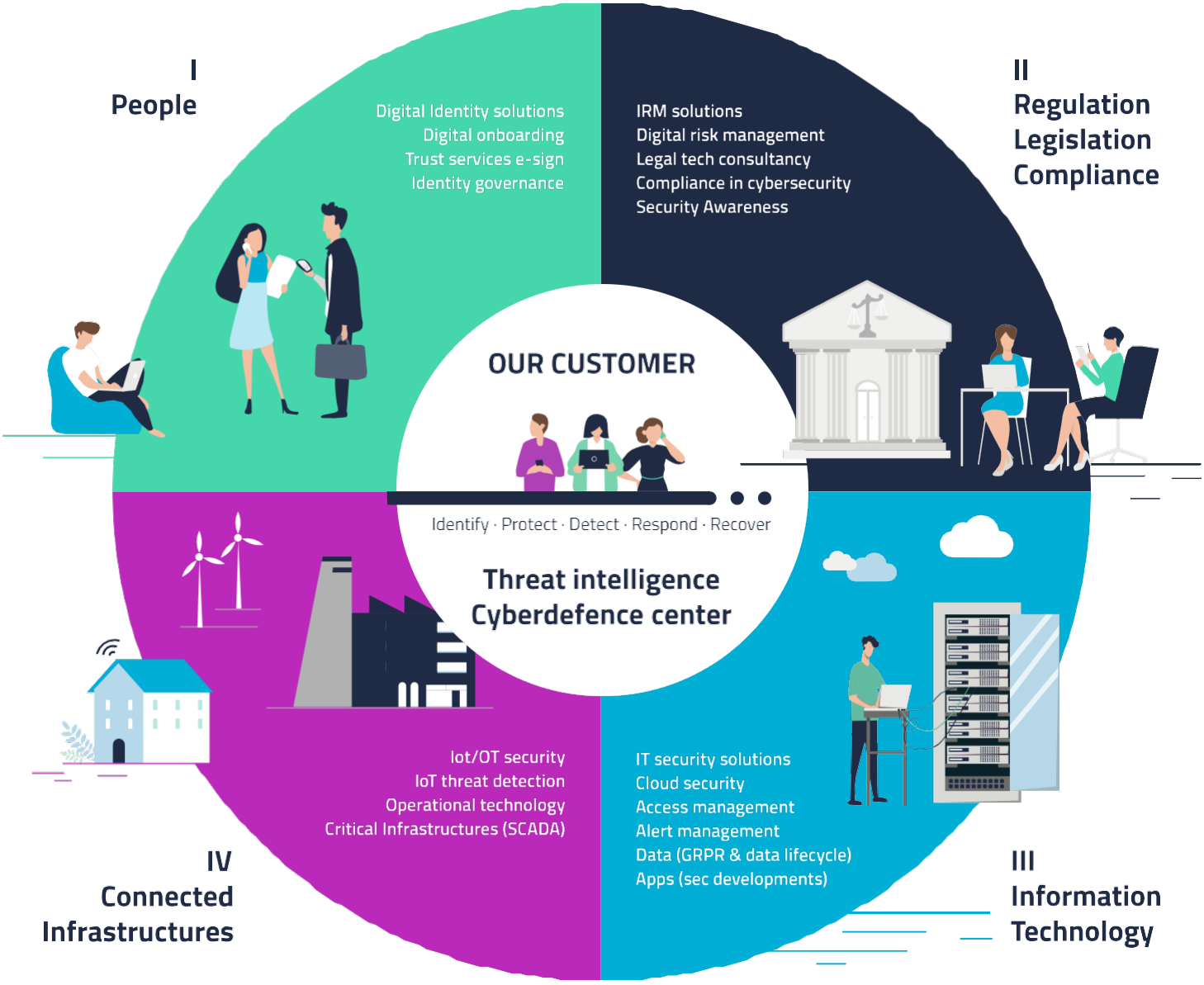
These four forces pose constant threats.

SIA, the cybersecurity company of the Indra group with more than 30 years of history, is leader in the market and has its mission to protect digital businesses by providing a response to these threats.

Our concept of cybersecurity goes further in scope and in the way we provide solutions.

Our solutions are integrated into Indra's portfolio, which allows us to offer greater capabilities and provide the necessary structure to successfully undertake the most ambitious projects.

These are the four driving forces:



SIA's 11 answers to the secure enabling of digital businesses

Ensuring regulatory compliance

The regulatory and legislative environment is complex and requires an expert level of knowledge.
The experience of our technical and legal specialists provides flexibility for adapting solutions to various industries and platforms.

Preparing the business continuity plan

Attacks on our systems require the development of solid business continuity plans as a preventive measure. We can design these plans together with our experts, who will assist in incorporating the best practices in the industry

Implementing a Cybersecurity Plan

When defining a cybersecurity plan, it's common to start parallel projects given the urgency of the measures to be taken.
The scattering of assets and interaction between applications and users requires coordination: setting up a technical office is a good solution for this.

Promoting team awareness

Employees or collaborators can be inadvertent facilitators of threats to the organization. This is why training and awareness is important.
We work with several organizations in establishing these policies and tools, in combination with the more technical side.

Defining a solid security architecture

The plethora of manufacturers and the fragmentation of the cybersecurity market make it difficult to decide which solutions are best suited to your environment.
The inclusion of outside experts provides a different view and an opportunity for improvement.

Detecting and responding to threats

Threat management through the network of our cyberdefense centers (Madrid, Mexico, Bogotá) guarantees the protection of our clients.
Intelligence, detection and response services provide a comprehensive range of shared and in-home services

Managing digital identity

It's essential to control the rights to which services and profiles each person has.
Artificial intelligence in profiling processes - along with multiple-factor authentication and unified access (sign-on) solutions- in addition to the control of privileged accounts and data access, enable a complete governance identity program.

Promoting Digital Onboarding strategies

The growing number of digital clients requires a secure environment for their operations.
It's important to start integrating them ("Digital Onboarding") by taking advantage of identification technology and the use of biometric elements.

Securing digital signature processes

The digitalization of processes requires completing transactions with a digital signature in a flexible way.
A cloud solution makes integration with applications easier, ensuring archiving and retrieval.
All of this with the flexibility of customized and certified eIDAS development.

Controlling the risk of fraud

Detecting inappropriate client or employee behavior and actions is fundamental.
How? By implementing modular solutions for transactional and e-commerce processes. This is supplemented by expert agent control.

Managing digital risk

The progressive digitalization of organizations and its processes -enabling new businesses and channels- has exponentially increased the number of existing threats, thus introducing new risk vectors.
At SIA, we have the necessary skills to help organizations identify and manage digital risk in line with their business strategy.

SIA responds

These are our answers to...

The challenges of cybersecurity in the Public Administration Sector

"Spain Digital 2025" strategy

Reinforce cybersecurity based on three objectives:

1. Increase the cybersecurity capabilities of citizens and businesses
2. Foster the development of the entrepreneurial ecosystem in the cybersecurity sector
3. Boost Spain's international visibility regarding cybersecurity

Measures to be implemented in the area of cybersecurity:

1. 017 cybersecurity hotline to be offered by INCIBE
2. Strengthening cybersecurity for citizens, SMEs and professionals through awareness and training campaigns, creation and development of talent in cybersecurity, as well as hotlines for companies and professionals in this area
3. Promotion of the cybersecurity business ecosystem with the extension of current support processes and support to entrepreneurship
4. Promotion of Spain as an international hub in the field of cybersecurity
5. Deployment and operation of the cybersecurity operations center for the enhancement of cyber-incident prevention, monitoring and detection capabilities and the optimization of reaction and response capabilities to any cyber-attack

Key areas:

1. The extension of the security perimeter

All organizations have experienced a change in their security perimeter. The security devices that isolate each organization's data centers are no longer the ultimate secure barrier. The perimeter has expanded to the most vulnerable link in the chain: the public employee and the citizen. This fact will imply the incorporation of solutions oriented to manage any means of access to the administration's information systems (laptops, mobile phones, tablets, etc.), which must be managed in a secure way without violating the rights to privacy that are guaranteed by law. Solutions such as EMM (Enterprise Mobility Management) or EDR (Endpoint Detection and Response) as well as end identity management systems (CIAM) are likely to become a priority to ensure the security of data, administrators and public employees.

2. EU Directive

EU Directive 2018/1972 makes it mandatory for member states to deploy a Public Warning System (PWS) by June 2022. Organizations can take advantage of this system as an additional security mechanism to minimize the impact not only of natural disasters, terrorist attacks, or health emergencies, but also of security breaches in essential services that may cause risk or temporary unavailability.

3. The digital identity

There is need to revitalize the interaction between the administration and the administered, with the objective of standardizing the access mechanisms through the incorporation of more agile e-signature techniques—which include biometric technologies and personal accreditation when dealing with the administration.

4. The rise of cyber-resilience

The shift in the current paradigm—where investing in protection is essential to prevent attacks—must give way to the development of strategies to minimize impact and increase the resilience of public bodies. Focus must be placed on measures to recover services and infrastructures in the shortest time possible. Disaster recovery tools or distributed and protected cloud architectures, will take a leading role.

Where is the sector headed?

1. Secure digital transformation

The Spain Digital 2025 plan and the resources provided by the reconstruction funds will permit developing an ambitious digital transformation program for public administrations in the coming years. The incorporation of innovative solutions will facilitate the relationship with citizens and will boost the efficiency of public employees. This will require the incorporation of security related to it, such as digital identity governance, cyber-resilience, and biometrics, among others.

2. Security Operations Center

As defined in Axis 4 of the Spain Digital 2025 plan, an essential element in the administration's strategy will be the development and strengthening of the SOC of the General State Administration. The aim will be to coordinate the response to incidents, unify the management of security alerts, intelligence information on threats and, finally, contribute to minimizing the impact of potential attacks aimed at the public administration.

3. Cloud infrastructure protection

The sector is firmly committed to cloud solutions, and some organizations have already completed this process. Cloud-based email protection, CASB solutions, and Zero Trust as an alternative to traditional architectures will become a trend in the short and medium term.

The priorities of Public Administrations

Success stories:

1. Implementation of a multi-factor authentication (MFA) system
2. Mainstream the management of both corporate and personal mobile devices (EMM)
3. Hiring of SOC services with EDR and SIEM, etc.
4. Protection of the corporate email in cloud infrastructure
5. National Security Framework certification

Due to the exceptional situation caused by COVID-19, the various administrations have made it a priority to guarantee a secure remote working. Projects for implementing multi-factor authentication or adaptive authentication based on access risk have become, by far, the most in-demand and successfully implemented this year, along with secure management of mobile devices using EMM solutions.

The evolution of SIEM towards greater added-value services has also been successfully carried out in different organizations, incorporating and monitoring the information sourced from EDR systems.

Mail protection in cloud infrastructures is another of the projects that can be considered a success case, as is the growing need for the administration to lead by example and not be satisfied with the obligatory compliance with the ENS, taking the next step and developing their IT to meet certification requirements.

Investment:

1. Implementation of DLP projects
2. Identity governance (privileged accounts)
3. Technical Security Office to ensure the secure development life cycle
4. Outsourcing of the DPO service and Security Office
5. Improve recovery capabilities with continuity plans and tools to increase the resilience of organizations

Public bodies have outsourced a large part of the administration and management of their IT infrastructure to different trusted providers, but need to retain control over privileged accounts. The agencies that have not already launched it are planning to tackle PAM (Privileged Access Management) projects in the short term. The mechanisms for the prevention of information leakage (DLP - Data Loss Prevention), the introduction of secure development techniques in app-development departments (SecDevOps)—as well as the incorporation of specialized tools to strengthen their business continuity plans—will make up a large part of the strategy of public bodies in an effort to minimize the loss of confidential information and avoid damaging their corporate image.

Lastly, Public Administrations without sufficient means to maintain an in-house security department are choosing to outsource their DPO (Data Protection Officer) and security office services.

Cybersecurity practices that sector players have in mind

1. Identity governance (privileged accounts)
2. Use of Artificial Intelligence for the detection of anomalous behaviors
3. Evolution of the protection of corporate cloud services (CASB, email protection, sandboxing...)
4. Ethical hacking campaigns involving deception techniques
5. Information security awareness campaigns (phishing prevention, good practices... etc.)

PAM solutions will be part of the identity governance strategy in public organizations, along with next-generation SIEMs.

The need to apply techniques to protect cloud environments such as CASB solutions (Cloud Access Security Broker) will play an essential role in the short-term strategies of public institutions.

The incorporation of deception techniques to obtain information on how the institutions could be attacked, and the improvement of the security measures of the environment, are already beginning to be included in different technical requirements. They are part of the counter-intelligence work, which is incorporated in the current tenders for ethical hacking.

SIA is the ideal technology partner to successfully undertake these tasks. We are SIA. Beyond Cybersecurity.

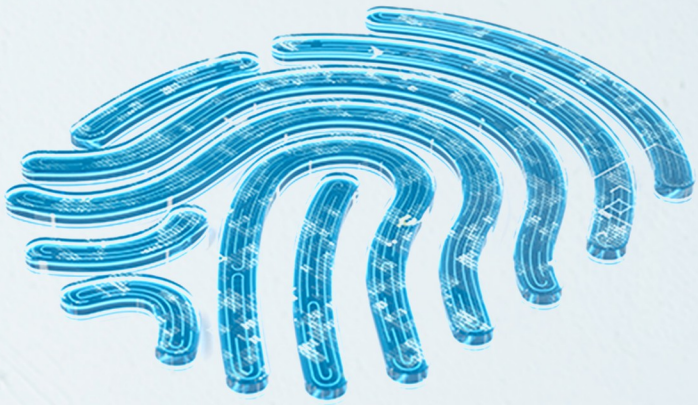
*Data obtained from SIA and Minsait's Ascendant report on Digital Maturity of Cybersecurity 2020-2021, based on personal interviews with leaders of a hundred large companies and organizations in Spain and the rest of Europe, as well as with some of the leading cybersecurity experts.

SIA would like to invite you to see the full report in a meeting with our team of specialists, which is very useful as a roadmap for improvement in this area. Please contact us: siainfo@sia.es

An Indra company

Cybersecurity Solutions

Public Administrations



BEYOND CYBERSECURITY