sia

An Indra company

Cybersecurity solutions

Energy

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

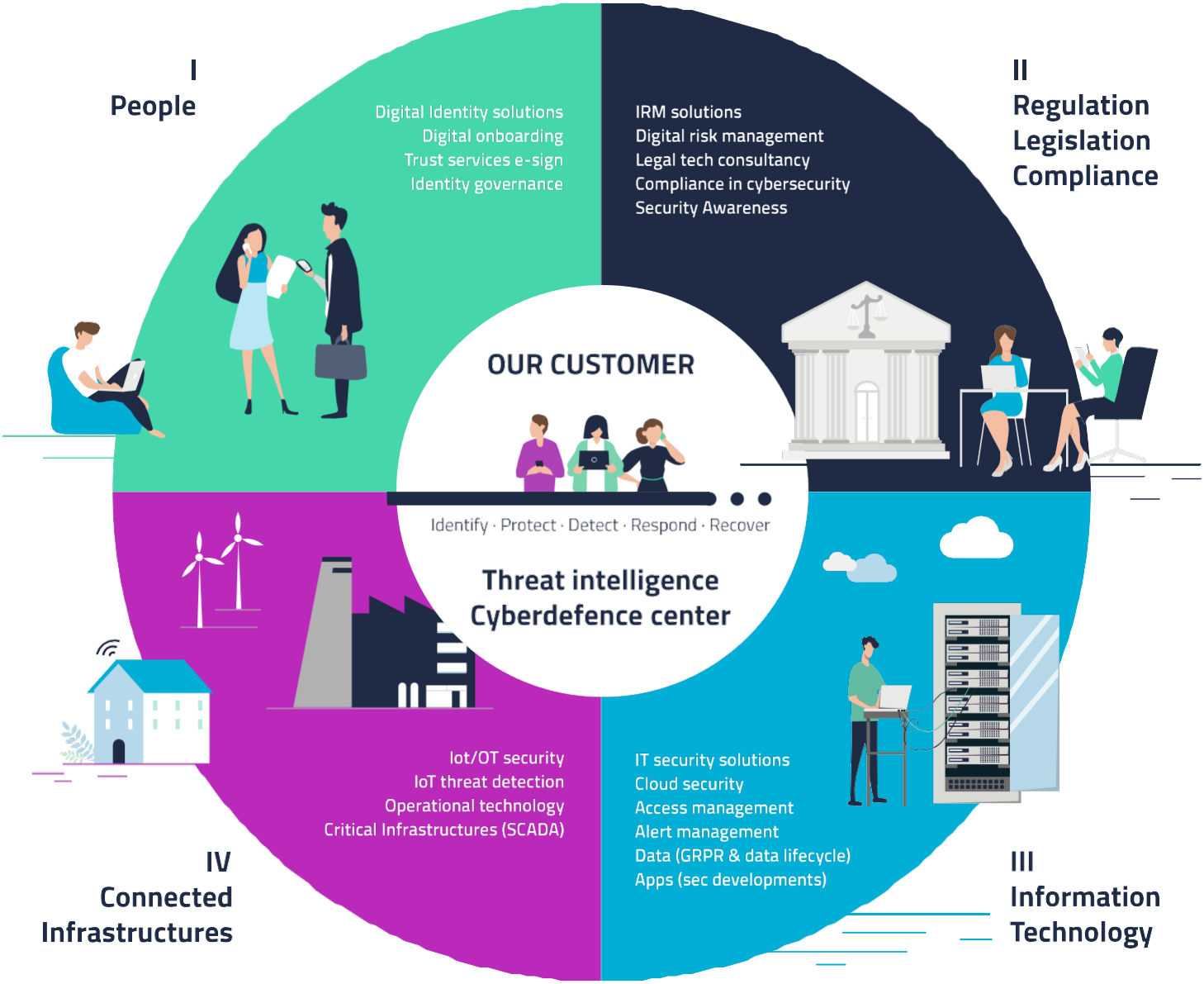
These four forces pose constant threats.

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

Assure regulatory compliance

The regulatory and legislative environment is complex and requires know-how.
The expertise of our technical and legal specialists provides flexibility to adapt solutions to different 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 thanks to our experts, who will facilitate the incorporation of industry best practices.

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.

Raise awareness among teams

Employees or collaborators can inadvertently expose the organization to threats, which is why training and awareness is so important.
We work alongside organizations to establish these policies and tools, aside from the more technical aspects.

Defining a solid security architecture

The large number of vendors and the fragmentation of the cybersecurity market makes it difficult to decide on the most suitable solutions for each environment.
The incorporation of external experts provides a different perspective and an opportunity for improvement.

Detect and respond to threats

Managing threats from of our network of cyber defense centers in Madrid, Mexico City and Bogota guarantees the protection of our clients.
Our intelligence, detection and response services provide a broad family of shared or in-house 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 facilitates integration with applications, ensuring the filing and retrieval of data. All this with the flexibility of a proprietary and eIDAS-certified development.

Controlling the risk of fraud

Detecting inappropriate client or employee behavior and actions is fundamental.
How? By implementing modular solutions for transactional or 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...

Cybersecurity challenges in the energy sector

The energy sector and, in particular, electricity and gas supply companies are particularly vulnerable to cyberattacks and their number has multiplied.

From our experience we can be sure that this increase in the number of attacks is due to:

1. Vulnerability is increasing due to the geographic dispersion of these types of companies
2. There are many interdependencies between physical devices and technology (OT)

SIA applies its experience in the world of cybersecurity to the particularities of this sector:

1. Using knowledge and technology to anticipate attacks and create robust security architectures
2. Creating a culture of awareness of cyberattacks because the employee is the first line of defense against them
3. Collaborating with the industry to address the convergence of physical and virtual devices

Cybersecurity must be considered throughout the entire value chain, from energy generation to transport and distribution through the network to the end user.

It must be considered that many of the legacy systems have been designed without cybersecurity in mind and that the complexity and number of interconnected systems makes management even more complex.

The most common crimes are data theft or hijacking, billing fraud and profit-seeking through ransomware.

Even sometimes the regulation itself does not take into account the interdependencies between OT and IT.

Distributed infrastructures add a lot of complexity, as there are many vulnerable points of generation such as solar farms that have not taken cybersecurity into account in cost-effectiveness studies.

Also to be considered is the complexity of devices such as wireless meters or electric vehicle charging stations that can be gateways to an attack that compromises the company's operation.

We contemplate the study of old systems maintained by organizations whose security protocols are non-existent or inadequate.

The processing of third party data is also important, such as power grid or compensation systems, as they can be the result of deliberate alteration, which can impact the operation by overloading the systems.

And it is also important to consider physical security, especially in remote wind farms and photovoltaic parks, where our parent company, Indra, plays a key role.

Therefore, SIA develops and implements prevention, detection and response plans.

The physical isolation of OT networks provides a false sense of security as they can be accessed by other means. Today, there is remote maintenance and occasional connections to uncontrolled systems.

In short, physical security and cybersecurity need to be integrated and should be a priority in the organization.

Cybersecurity practices being promoted in the industry

1. Definition and implementation of the risk management model in the supplier supply chain
2. Vulnerability management service
3. Implementation of a SOC (Security Operation Center) for industrial systems integrated with the IT SOC
4. Global implementation of DRP (Data Recovery Plan) projects based on business continuity plans
5. Assessment and Master Plan for industrial cybersecurity (OT - Operation Technology)

There is a clear trend towards the protection of OT environments —a pending task given we have moved to an interconnected model and are able to access the environments from the outside. The increase in attacks is again reflected in the introduction of vulnerability management services to handle the large amount of assets affected by them.

Cybersecurity practices that sector players have in mind

1. Implementation of a CSIRT in the OT area
2. Improved cyber intelligence services for threat detection and brand reputation
3. Review and update of the cybersecurity master plan for the next few years
4. Implementation of behavioral and anomaly analysis solutions (UEBA - User and Entity Behavior Analytics)
5. Upgrade to the new generation of cybersecurity infrastructure (EDR, CASB, DLP...)

There is a need to respond to attacks with a CSIRT, but in this case to operational environments.

On the other hand, there are companies in the sector that are thinking about the protection of communications in smart meter environments. In addition, there is a trend towards upgrading to the latest generation of cybersecurity technologies, such as information protection solutions.

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

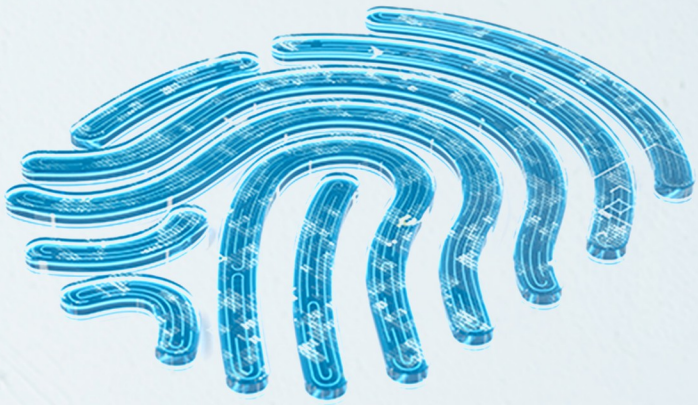
*Data obtained from SIA and Minsait's Ascendant report on Digital Maturity of Cybersecurity 2020-2021, based on personal interviews with leaders of a hundred large companies and organizations in Spain and the rest of Europe, as well as with some of the leading cybersecurity experts.

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

Energy



BEYOND CYBERSECURITY