An Indra company

Cybersecurity solutions

Industry and Consumer Goods

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

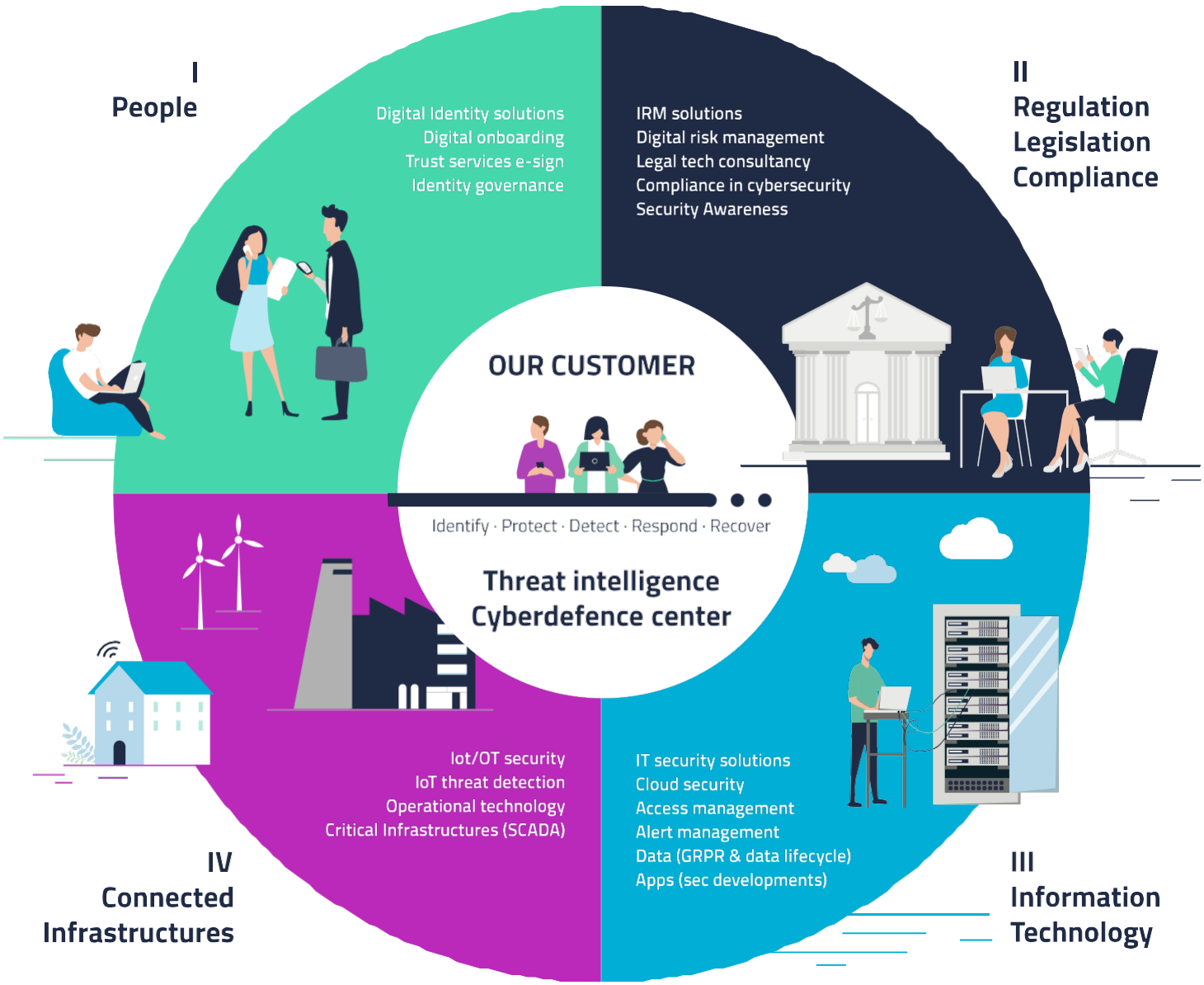
These four forces pose constant threats.

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...

Cybersecurity challenges in the industry sector

In an industry where cybersecurity was not a priority; the biggest challenge in the post COVID-19 era for manufacturing companies is the rapid adaptation to digital transformation.

Impact of COVID-19 on the sector

The pandemic has caused internal changes in companies in the industry sector such as remote working, the increase of online B2B or a greater focus on business continuity, to name but a few. In many cases, this has led to an acceleration of digitization processes and, as a consequence, the need to address cybersecurity issues.

Where is Industry heading?

Security partners

Obtaining specialized security profiles is becoming increasingly complex, leading companies to establish stable medium and long-term alliances with global security partners.

Digital signature

Digitization involves the conversion to electronic format of all data processed by the company. There is data, the content of which must be accredited, validated or authorized by persons through the use of digital signatures.

IT/OT convergence

Converging IT and OT infrastructures is the best option to be able to apply similar mechanisms for protection, monitoring, mitigation and response to cybersecurity incidents in both environments.

Security in Edge Computing and Fog Computing

The security and privacy of IoT devices and their connection to cloud environments is increasingly in demand, with secure processes that ensure proper handling of data between devices and the cloud. Cloud-based signature solutions, biometrics, fraud controls and technologies for business data governance and protection.

What are the priorities of companies in the sector?

Successfully managed cybersecurity practices

1. Awareness campaigns to avoid phishing attacks
2. Implementation of behavioral analysis tools
3. Implementation of single sign-on - identity management
4. New perimeter protection for Zero Trust environments
5. Incident detection and response programs
6. Data encryption and tagging project

Cybersecurity practices being promoted in the industry

1. Implementation of DLP tools and data classification
2. Increase security measures in the cloud environment
3. Network segmentation
4. NAC (Network Access Control) project
5. Business continuity plans

With the arrival of the pandemic in 2020, companies are required to implement solutions focused on facilitating teleworking for their employees, with the need to add additional protective measures to ensure security. Because of this, it is essential to protect the new perimeter and, at the same time, to increase awareness and training of employees against attacks or possible intrusions.

Behavioral analysis is very important in the field of detection, an area still to be developed in many sectors.

Emphasis is placed on data protection, with the implementation of new tools for the prevention of data leakage —an area that is becoming increasingly important nowadays.

Work is also being carried out to develop and improve business continuity plans. Companies in the sector are aware of the importance of cybersecurity and are investing efforts in improving cloud protection strategy and network segmentation (IT/OT).

Cybersecurity practices that sector players have in mind

1. Improve security incident detection and monitoring capabilities
2. Implementation of the measures of the global cybersecurity master plan
3. Improve cloud protection
4. Convergence of IT / OT environments
5. DLP project implementation

Industrial companies are aware of the importance of cybersecurity and continue to invest efforts in improving security incident management, implementing specific tools such as SOCs or SIEMs.

Our answers to...

Cybersecurity challenges in the consumer sector

Retail identity management

The incorporation of identity management technologies, especially those based on biometric identification, as an opportunity to simplify and enrich customer communication.

Fraud management

The focus on fraud management has accompanied the radical growth of online transactions, both in e-commerce and more emerging models: *direct to consumer*.

Sustainability

In recent years, one of the most evident changes among consumers is the concern for more responsible consumption and companies are already looking for ways to adapt.

What are the priorities of companies in the sector?

Successfully managed cybersecurity practices

1. Outsourcing cybersecurity services
2. Employee awareness programs
3. Implementation of incident detection and response technologies
4. Endpoint protection
5. Electronic fraud management

Cybersecurity practices that are being promoted in the sector

1. Replicate the IT model in OT
2. Deployment of mobile device protection (EMM)
3. Development of cybersecurity policies for external suppliers
4. Improved mail protection
5. Implementation of the Privileged Account Management (PAM) project)

In the industry, identity management is being taken a step further, with initiatives to manage privileged user accounts. Some of the use cases that are

currently being promoted are those related to the convergence of IT - OT environments, trying to replicate the existing model in information systems to the OT environment. Companies in the sector are aware of the importance of cybersecurity and are investing efforts both in increasing protection through greater control with external providers, as well as in improving their security in mail and mobile devices (EMM).

Cybersecurity practices that sector players have in mind

1. Implementation of an IRM with DLP
2. Improve the software development cycle including *security by design*
3. Implementation of a SOC
4. Awareness programs at all levels
5. Identity management project

It is very important to create secure software development programs, as well as to include cybersecurity from the beginning of the projects. In the case of third-party development, we are already working on the development of policies that demand security requirements from suppliers.

As in other sectors, data protection is extremely important, through the implementation of advanced tools such as DLP or digital rights management tools. Likewise, within the projects to be developed in the short and medium term by companies in this sector, it is common to develop training and awareness plans for employees to minimize possible risks of intrusions or attacks in companies.

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

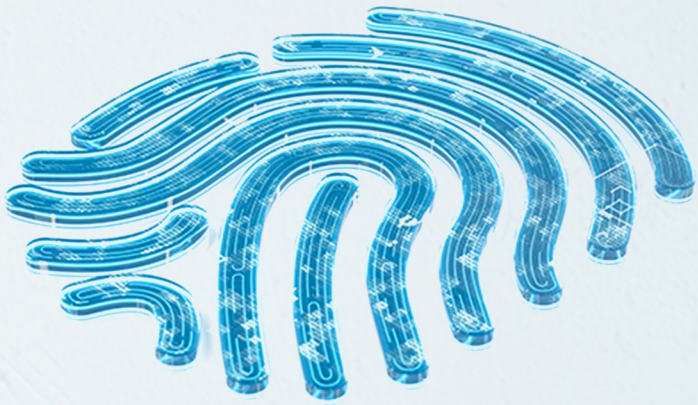
*Data obtained from SIA and Minsait's Ascendant report on Digital Maturity of Cybersecurity 2020-2021, based on personal interviews with leaders of a hundred large companies and organizations in Spain and the rest of Europe, as well as with some of the leading cybersecurity experts.

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

Industry and Consumer Goods



BEYOND CYBERSECURITY