sia

An Indra company

Cybersecurity solutions

Financial Services and Insurance

BEYOND CYBERSECURITY

The four driving forces of digital transformation

Digital transformation is driving the new economy, and it is governed by four great driving 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

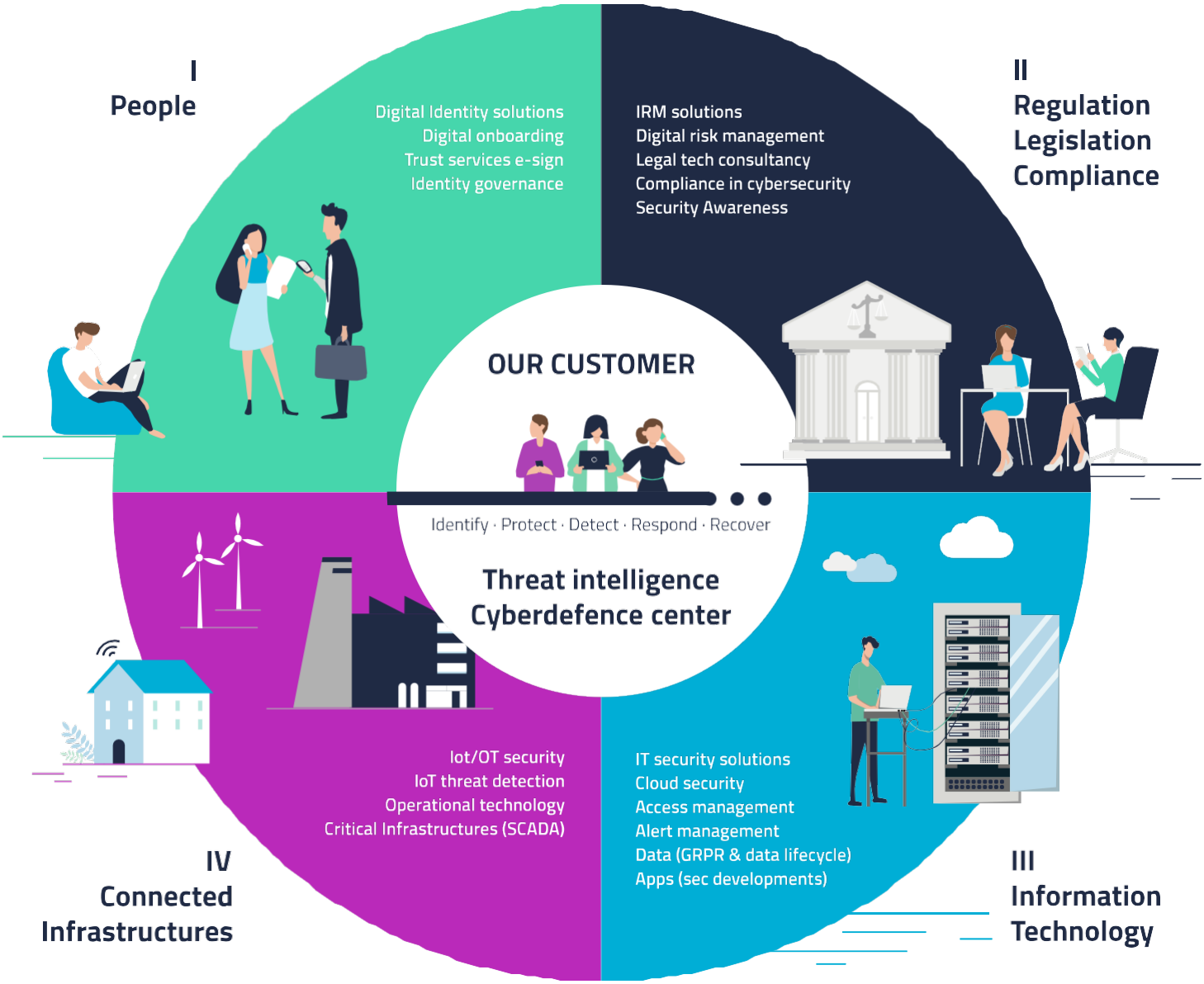
These four forces pose constant threats.

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. You 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

t'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 digitization 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 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 cybersecurity challenges in the Banking sector

Where is the sector headed?

Digital sales channels

Banks are expected to reduce their branch network by 25% and focus more on the use of digital channels. Customers, including those over 65, show an increasing preference for conducting their daily transactions through digital means, in alignment with those of younger customers. Therefore, cybersecurity budgets will increase with the expansion of digital channels.

Emergence of new players

Other operators (large technology companies) offer financial products in addition to their own business. They are trying to replace the role of banks, despite the strict regulations that prevent them from acting as full-service banking institutions.

Cryptocurrencies

Banks are already exploring the cryptocurrency market, seeking to provide it with the same security and trust as the classic monetary system. It should be noted here that there are already banks that have started to accept cryptocurrency as an exchange instrument.

Reorientation of income

There is a fall in income due to falling interest rates. Accordingly, banks are looking for other options, such as increasing commissions to non-engaged customers, new commissions, increasing activity in companies, offering new products related to insurance, funds and savings plans, and even divestments in non-strategic assets and businesses.

What are the priorities of companies in the sector?

Successfully-managed cybersecurity practices in industry

1. Adequate incident response strategy
2. Awareness programs at all levels of the organization
3. Fraud prevention programs
4. Data Leakage Prevention Project (DLP)
5. Implementation of managed SOC services
6. Implementation of EDR solutions

Due to the large number of attacks occurring in recent years, the most common use cases successfully implemented are those related to incident response.

As a result, banks have defined threat response strategies that have proven to be effective. In this area, there are banks that have implemented managed SOC services and on-site detection and response solutions. Data protection and fraud prevention are very important areas in this sector. Several banking institutions have already implemented data leakage prevention Solutions through DLP (Data Loss Prevention) projects as well as specific anti-fraud tools.

Cybersecurity practices being promoted in the industry

1. Monitoring based on the MITRE ATT&CK
2. Digital Fraud
3. SSDLC (Software Development Lifecycle)
4. Network segmentation

Companies in the sector are aware of the importance of cybersecurity, which is why some are already working on advanced solutions to improve monitoring based on the MITRE ATT&CK framework.

Some banking institutions are investing efforts in incorporating security into software development, with security by design and security by default measures.

Cybersecurity practices that sector players have in mind

1. Artificial Intelligence Solutions for incident response
2. Privileged Access Management (PAM)
3. Network segmentation
4. Identity management project

As in most sectors, it is important to implement projects with organizational components, such as identity life cycle management and, in particular, the management of privileged user accounts.

Companies in the sector are planning to invest their efforts in incident detection and response, with more advanced artificial intelligence solutions.

Cybersecurity practices that have been more difficult to implement in the sector

1. Security by design
2. IRM project implementation
3. Improved approach to complex projects such as identity management
4. Implementation of a cybersecurity dashboard

All failed data projects focus on the implementation of data exploitation technologies and tolos. Institutions fail due to insufficient management of the integration of these technologies in the bank.

Answers for...

The cybersecurity challenges in the Insurance sector

Where is the insurance sector headed?

Digital sales channels

Not only does the industry need to increase, adapt and improve its channels to offer remote customer services, but the information needs to be available to all channels.

New paradigm

The new life cycle of households will bring a new paradigm for the insurance mix, in a time of consolidation of the hyper-connected customer, who is beginning to demand distinctive experiences and the use digital channels (with the necessary implementation of the corresponding protection measures).

What are the priorities of companies in the sector?

Successfully-managed cybersecurity practices in industry

1. Defining cybersecurity controls
2. Development of employee awareness and training plans
3. Deployment and implementation of the SOC
4. Adaptation to the NIST framework

The most common practices that have been successfully introduced are those related to incident detection and monitoring, as well as implementing a culture of cybersecurity within the organization through training and awareness-raising plans. These two points are highly valued by insurers, as there is an increase in the number of attacks in the sector.

The fact that some success stories are based on the incorporation of cybersecurity in the development of new projects reveals that there is still some way to go in this process.

Cybersecurity practices being promoted in the industry

1. Identity management projects
2. Evolution of the security model to the cloud
3. Fraud detection technologies
4. Equip the organisation with technology to ensure recovery from ransomware
5. Implementation of technology for the detection of anomalous behavior (UEBA)

Among the use cases that are being promoted today, those that stand out are related to the detection of anomalous behavior patterns within the organization and the implementation of new technologies for recovering from attacks. Companies in the sector are aware of the importance of cybersecurity and are reinforcing their technological tools to prevent and detect fraud, which is so prevalent in the insurance sector.

Similarly, due to the increase in the amount of data being stored in the cloud, greater security in cloud environments is becoming a priority.

Cybersecurity practices that sector players have in mind

1. Awareness plans to implement cybersecurity in projects from the design stage onwards
2. Deployment of EDR (Endpoint Detection Response) Solutions
3. Identity life cycle governance
4. Implementation of Threat Hunting practices
5. Equip the organization with information leakage detection capabilities

For insurance companies, emphasis is placed on the need to involve cybersecurity teams in all projects, engaging them from the outset. Implementing workplace solutions and more advanced threat hunting practices are being promoted in the area of incident detection and response.

Data protection is high on the agenda of companies in the sector, studying tools to detect information leaks such as DLP (Data Loss Prevention).

Cybersecurity practices that are most complex to implement in the sector

1. Navigation proxy implementation project
2. Evolution of the identity management platform
3. Vulnerability Management

Identity management has proven to be a very necessary project but, at the same time, complex when it comes to its implementation, since it requires not only the implementation of technology but also modifications at an organizational level. Vulnerability management, in some cases, has been identified as a complicated issue given the difficulty in prioritizing the remediation of vulnerabilities caused by factors such as lack of personnel, lack of time, excessive bureaucracy between departments, etc. Any assets with vulnerabilities must be identified and, above all, their impact must be quantified so that they can be successfully managed.

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

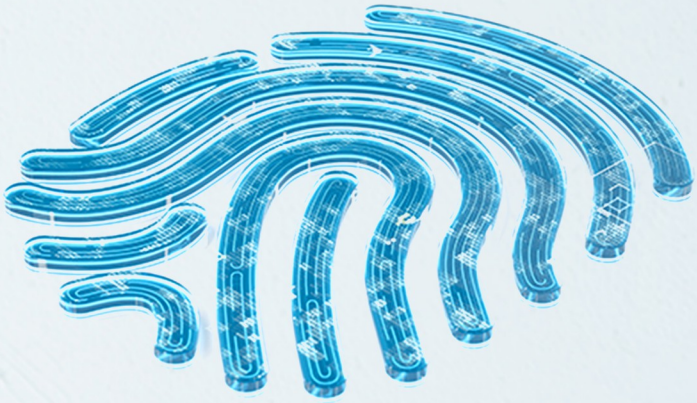
*Data obtained from SIA and Minsait's Ascendant report on Digital Maturity of Cybersecurity 2020-2021, based on personal interviews with leaders of a hundred large companies and organizations in Spain and the rest of Europe, as well as with some of the leading cybersecurity experts.

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

Financial Services and Insurance



BEYOND CYBERSECURITY