CYBERSECURITY PROGRAM AND STRATEGIC PLAN

Grupo Empresarial Argos

2025

Comprehensive Cybersecurity Program, Strategy and Management Model

1. Introduction

In an interconnected and digitalized world, cybersecurity has become a fundamental pillar for the success and sustainability of any organization. In the case of the Argos Business Group, which operates in more than 18 countries and spans 10 different industries, protecting information assets from cyber risks becomes even more crucial. This comprehensive cybersecurity program, strategy, and management model aim to provide a strategic vision and an organized articulation of the elements and measures necessary to protect our information assets in a highly digitalized and dispersed global environment.

2. Strategic Vision

The strategic vision of our cybersecurity strategy is to be a leader in protecting the information assets of the Argos Business Group, maintaining the trust and digital security of our customers and users. This will be achieved through the organized identification and coordination of cyber risks, the implementation of effective preventive and corrective measures, and the continuous strengthening of our cybersecurity capabilities.

3. Challenges and Questions

The development of the cybersecurity program and strategy seeks to address the following key challenges and questions, considering the complexity and operational dispersion of the Business Group:

Identification and Control of Critical Assets: How can critical information assets be identified, cataloged, and protected in a highly digitized and dispersed global environment, incorporating non-human identity management and quantum threat preparedness?

Risk Identification and Treatment: How can cybersecurity risks, including those powered by AI and quantum threats, be identified and prioritized, and treatment schemes be assigned that address operational dispersion, supplier interdependence, and the need for ethical AI governance?

Threat Prevention and Detection: What tools and strategies should be implemented to prevent and detect advanced AI-powered threats, such as deepfakes and non-malware attacks, while addressing systemic risks arising from the technological dispersion and interdependencies of the business group?

Business Continuity: How to define and implement a business continuity plan in the event of a cyberattack, considering the different industries and the lack of unity in risk response? How to design and implement a

business continuity plan that integrates resilience against advanced cyberattacks, such as ransomware targeting industrial systems and quantum threats, ensuring a unified response across a diverse business group?

Cybersecurity Culture and Ethical Awareness: How can we foster a cybersecurity culture that promotes ethical awareness and shared responsibility across all group companies, considering cultural and operational differences?

Organizational Coordination: How can we coordinate all areas of the group's various companies around cybersecurity, considering the definition of roles and responsibilities, fostering a culture of collaboration, integrating ethical AI governance, and preparing the organization for quantum and advanced threats under a single corporate framework?

4. Competitive Advantages of Cybersecurity

Implementing a solid cybersecurity strategy offers several competitive advantages for the Business Group, including:

Breakthrough into New Markets: Facilitates entry into international markets that require compliance with cybersecurity standards. Compliance with global cybersecurity standards (such as GDPR) facilitates entry into international markets. Offering services such as Zero Trust and quantum threat solutions (following NIST) attracts clients in regulated sectors such as healthcare and finance.

Increased Productivity: Limits the chances of successful attacks, reducing recovery time and minimizing economic and reputational losses.

Competitive Advantage: Ensures proper management of sensitive information, maintaining user preference and trust.

Improved Customer Service: Increases the efficiency and automation of solutions, improving customer satisfaction.

Efficient Resource Use: Enables the appropriate use of resources, avoiding additional costs and improving operational efficiency.

Leadership in Innovation: Positions the business group as a pioneer in the adoption of emerging technologies, such as ethical AI and post-quantum cryptography, enabling it to offer innovative services to external clients.

Ethical and Collaborative Culture: Promotes a cybersecurity culture with training that strengthens internal and external trust.

5. Scope of the Cybersecurity Management System

The scope of the Cybersecurity Management System covers the services provided to the companies in the business group, the Value Chain processes, and the enabling factors included:

Cement and concrete manufacturing:

- Industrial control systems (ICS) security: Protecting industrial control systems used in cement and concrete manufacturing against intrusions and cyberattacks.
- Supply Chain Security: Ensure the integrity and security of systems and data throughout the supply chain, from raw material procurement to product distribution.
- Intellectual Property Security: Protecting proprietary designs, processes, and technologies used in cement and concrete manufacturing from theft or tampering.
- Operational resilience: Implement measures to ensure operational continuity in the event of cyberattacks that could impact production and product delivery.

Generation, distribution and marketing of energy:

- Critical Infrastructure Protection: Ensure the protection of critical infrastructure assets, such as power plants, substations, and distribution networks, against cyberattacks that could disrupt energy supplies.
- Electrical system resilience: Implement measures to ensure the resilience of the electrical system to potential cyber threats, including the ability to respond and recover rapidly after an incident.
- Customer Data Security: Protecting sensitive customer information, such as billing and energy usage data, from unauthorized access and data theft.
- Regulatory Compliance: Meet energy sector-specific regulatory requirements regarding cybersecurity and data protection.

Administration of Road Concessions (Tolls) and Airports (Airports):

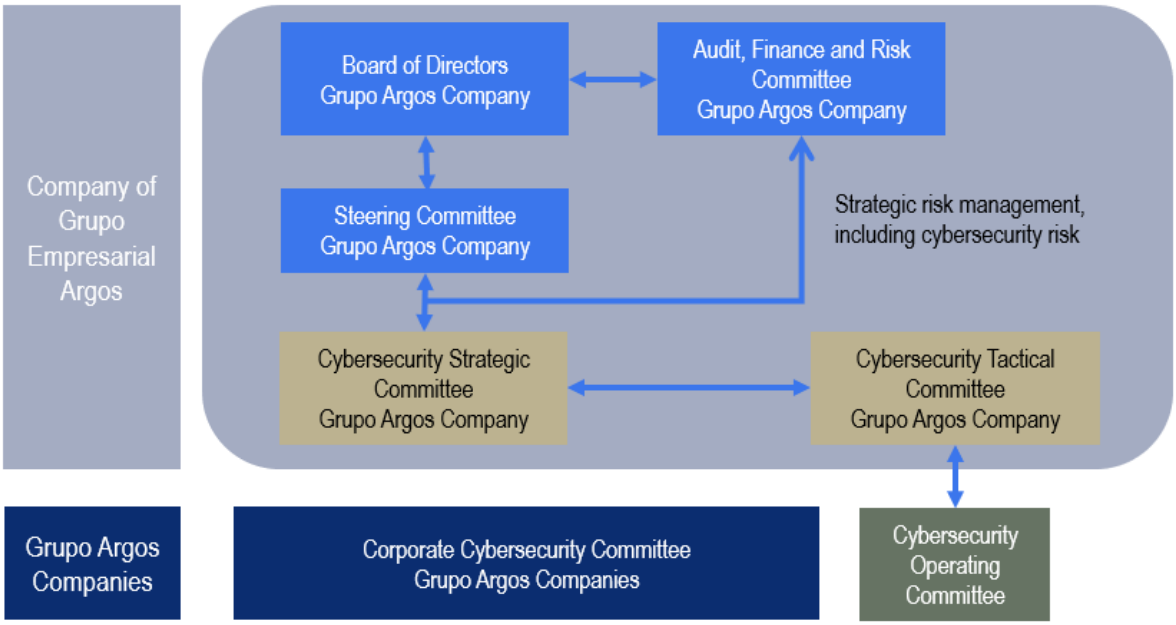
- Payment system security: Protect payment systems used at toll booths and airports against fraud and cyberattacks that could compromise users' financial information.
- Transportation Infrastructure Security: Ensure the integrity and availability of transportation infrastructure, including roads and airport facilities, against potential cyber threats that could impact public safety.
- Communications security: Protecting communications networks used for the management and operation of toll booths and airports against intrusions and unauthorized access.
- Crisis Management: Establish incident response plans and crisis management protocols to quickly address any disruptions or cyber incidents that may impact transportation operations.

Financial investments in infrastructure:

- Financial Transaction Security: Protecting sensitive financial transactions and data against fraud and cyberattacks that could compromise the integrity and confidentiality of information.
- Financial Risk Management: Identify and mitigate cyber risks that could affect the financial stability and reputation of infrastructure investments.
- Regulatory Compliance: Comply with financial sector-specific regulatory requirements regarding cybersecurity and the protection of customers' financial and personal data.
- Financial system resilience: Implement measures to ensure the resilience of the financial system to potential cyber threats, including the ability to recover after an incident.

6. Cybersecurity Governance and Responsibilities

Cybersecurity governance within the corporate group is based on clear support and backing from company management. This approach is realized through various key entities and roles that collaborate in comprehensive cybersecurity management.



Boards of Directors:

Boards of directors assume primary responsibility for the adoption and proper implementation of cybersecurity policies and standards. They also establish an organizational structure that provides guidance and direction for cybersecurity management. They allocate the necessary resources and provide effective leadership to mitigate digital risks within the organization.

Strategic Cybersecurity Committee:

This committee plays a key role in approving the organizational strategy for cybersecurity management. It also validates the cybersecurity policy and its guidelines, manages the risk map, and evaluates the effectiveness of the treatment measures adopted. It also oversees the adoption of recommendations issued by regulatory bodies and reports regularly to the board of directors and senior management.

Cybersecurity Tactical Committee:

The Tactical Committee is responsible for implementing the cybersecurity policy by proposing operational guidelines. It constantly monitors the cyber environment to identify risks and vulnerabilities, oversees the implementation of security measures, and designs penetration testing programs and cyberattack drills. It is also responsible for adjusting training and awareness programs, as well as communicating and reporting on the status of cybersecurity to senior management and other key members of the organization.

Owners and Custodians of Information and Cyber Assets:

Owners are responsible for the assigned assets, including their classification, control, and monitoring. Custodians ensure asset protection by enforcing the access restrictions and classifications established by the owners.

Control Areas (Technology, Risk, Audit):

These areas are responsible for managing and evaluating the measures adopted to mitigate cybersecurity risks from a technological, risk, and audit perspective.

Chief Information Security Officer (CISO):

Responsible for developing a comprehensive cybersecurity management model, framing the cybersecurity policy within this ecosystem. Their role focuses on managing risks associated with information security and cybersecurity, as well as designing and managing the Cybersecurity program to ensure internal control based on information technology and articulate business needs for a secure digital transformation, preserving the sustainability of the business group's organizations in the market. The role establishes the architectures and controls for processes, technologies, and people relevant to risk mitigation and the protection of information assets. This work is based on security practices, standards, and international regulations that govern the group's companies.

Users:

All employees, suppliers, contractors, and authorized third parties who use company information in the performance of their daily activities are considered users and play a crucial role in protecting the organization's assets.

7. Cybersecurity Policies and Guidelines

The corporate group's cybersecurity policies and guidelines represent management's commitment to protecting information and digital assets, as well as mitigating the risks associated with cyber threats. These guidelines are supported by internationally recognized standards and industry best practices, including ISO/IEC 27000 and the Center for Information Security (CIS) controls. See: Cybersecurity Policy

ISO/IEC 27000 Standard:

The ISO/IEC 27000 series of standards establishes a comprehensive framework for information security management, providing standards, guidelines, and best practices for implementing information security management systems (ISMS). The group's cybersecurity policy is based on the principles and requirements of ISO/IEC 27001, which establishes criteria for establishing, implementing, maintaining, and continually improving an ISMS based on a risk management approach.

CIS Controls (Center for Information Security):

CIS Controls are a set of information security best practices developed by the Center for Information Security. These controls provide a concise set of specific actions to improve an organization's cybersecurity. The corporate group's cybersecurity policy incorporates CIS controls as an integral part of its security approach, using these guidelines to define specific measures and management processes aligned with internationally recognized best practices.

Integration into Policies, Guidelines, and Annexes:

The business group's cybersecurity policies, guidelines, and annexes are based on the ISO/IEC 27000 standard and CIS controls, ensuring that they reflect the most rigorous and up-to-date cybersecurity standards. By integrating these references, the business group ensures that its policies and guidelines are aligned with industry best practices and current legal obligations, which contributes to strengthening the protection of its information and cyber assets against constantly evolving threats.

Cybersecurity Policy:

The Argos Business Group's cybersecurity policy is a high-level document that reflects senior management's commitment to information and operational security. This policy establishes the framework for action that guides the behavior of employees and third parties involved in the management of information and business-enabling technologies. Each company in the business group has its own cybersecurity policy, derived from the corporate policy, with the aim of establishing specific guidelines tailored to its operational and security needs.

The Argos Business Group's Cybersecurity Policy establishes guidelines and responsibilities to protect the company's information and cyber assets, guaranteeing their confidentiality, integrity, and availability, ensuring business sustainability and the safety of its people.

The objective of the policy is to establish frameworks and guidelines for the behavior of employees and third parties in the management of information and technologies, guaranteeing the company's cybersecurity. This policy applies to all company operations and is mandatory for all employees and third parties involved in information and operational technologies. The Argos Business Group is committed to complying with laws and regulations, managing risks, and adopting cybersecurity best practices to ensure business sustainability and personal safety. Employees and third parties must ensure that the policy is aligned with the company's objectives, actively support cybersecurity, and adopt a risk-management approach.

Information stored, created, or transmitted must be used exclusively for business purposes, and an up-to-date inventory of information assets must be maintained. Controls must be established to prevent the loss, damage, theft, or malfunction of information assets, ensuring their confidentiality, integrity, and availability.

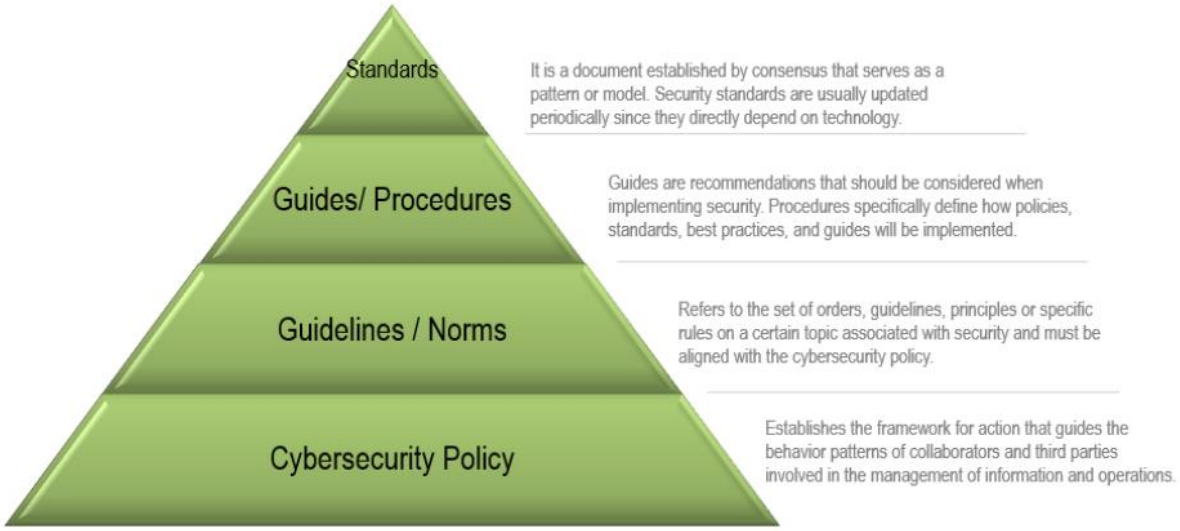
The Argos Business Group has defined an organizational structure with specific roles and responsibilities to ensure compliance with the cybersecurity policy. The policy must be reviewed annually or as needed and is approved by the Strategic Cybersecurity Committee.

Guidelines / Standards:

Cybersecurity guidelines and standards establish the set of orders, directives, principles, and specific rules that must be followed to ensure the security of information and operations. These guidelines are aligned with the corporate group's cybersecurity policy and ensure compliance with legal objectives and obligations. Each company in the group is committed to implementing these guidelines and standards consistently and effectively, adapting them to its specific operating context.

Technical Annexes/Guides:

The technical annexes/guides provide detailed and specific documentation in the form of guidelines, procedures, and standards for the implementation of cybersecurity policies. These documents address key aspects of information security, such as asset classification, operational security, secure use of IT resources, data protection, and more. Each technical annex/guide provides practical guidance to ensure the effective application of cybersecurity policies and guidelines in the different areas and processes of the group companies.



8. Cybersecurity Risk Management

Cybersecurity risk management is a fundamental component of the Business Group's information security strategy. It is based on a structured methodology that encompasses the identification, analysis, treatment, and continuous monitoring of risks related to digital security. This process is carried out in several stages:

Risk Identification: A thorough risk identification is carried out, considering the objective, scope, and context of the process or project. Threats, vulnerabilities, and potential consequences are identified using guiding questions such as: What do we want to protect? (asset), What should we protect it from? (threat), Why might the threat materialize? (vulnerability). This process is supported by tools such as interviews, document analysis, review of industry practices, and global trends. Risks are classified as internal events, controllable by the organization, and external events, beyond its direct control. This process follows a structured approach that includes: Identifying specific risks (Risk 1, Risk 2, ..., Risk N), defined as the effect of uncertainty on the achievement of cybersecurity objectives. For each risk, threats or causes (harmful actions with negative consequences) are identified, such as Threat 1, Threat 2, ..., Threat N. Associated vulnerabilities (weaknesses that facilitate the materialization of a threat) are determined, such as Vulnerability 1, Vulnerability 2, etc. Existing controls (Control 1, Control 2, ..., Control N) that mitigate the vulnerabilities are assessed.

Risk Analysis and Assessment: This stage aims to determine the level of risk exposure, considering the probability of occurrence and the potential impact. Existing controls are identified, and their effectiveness in mitigating risks is assessed by asking the question: What is currently being done to reduce the risk? The level of risk is calculated by assessing how the consequences affect the entity (impact) and the likelihood of

occurrence (probability). Risks are rated according to their level of exposure and located on a risk map, which facilitates the prioritization of actions.

Risk Treatment: After analyzing risk exposure, action plans are defined to mitigate critical, high, or moderate risks. Different treatment options are evaluated, such as avoiding, mitigating, transferring, or retaining the risk, based on cost/benefit criteria and expected mitigation.

Monitoring: Continuous monitoring and reporting mechanisms are established for effective risk management. The implementation of action plans is monitored, and risk analyses are periodically reviewed to ensure their validity. The risk report is consolidated to inform relevant stakeholders within the organization.

Exposure level = probability x impact

Probability						
	5. Very high	5	10	20	40	80
	4. High	4	8	16	32	64
	3. Moderate	3	6	12	24	48
	2. Low	2	4	8	16	32
	1. Very low	1	2	4	8	16
● Low ● Moderate ● High ● Critical		1.Minor	2.Under	4.Important	8.Major	16.Significant
		Impact				

The risk map is divided into four risk zones: low, moderate, high, and critical.

Cybersecurity Risks Identified

Specific risks in the field of cybersecurity are assessed and managed according to established methodology. Some of these risks include:

Loss of Confidentiality and Unauthorized Disclosure of Information: This can be caused by industrial espionage, information leakage or theft, or loss of equipment.

Unauthorized Alteration and Modification of Information or Systems: The integrity of information can be compromised by the introduction of malware, viruses, or ransomware.

Loss, Destruction, or Unavailability of Information: Data may be at risk of loss, destruction, or unavailability when needed.

Noncompliance with Standards and/or Regulations: Improper handling of information can lead to noncompliance with standards or regulations, especially those related to data privacy.

CyberRisk: The unavailability, interruption, or damage to information and operational systems due to cyber threats represents a significant risk.

Deception of Systems and People: Emerging technologies such as data poisoning and deepfakes can be used maliciously to deceive information systems and people.

Vulnerabilities in Provider Technology Services: Vulnerabilities in technology services provided by third parties that make up a company's supply chain can expose the organization to security risks.

9. Cybersecurity Management System (Framework)

The Business Group's cybersecurity management system is based on recognized frameworks such as NIST, COBIT, and ISO 27000, as well as industry-specific standards, including NERC CIP (energy), ISA99 (manufacturing), RAC 160 (aeronautics), and financial regulations such as GDPR and SEC. This system integrates cybersecurity best practices, aligning with each company's corporate governance, business strategies, risk management, and the requirements of strategic partners in each sector. This program integrates cybersecurity best practices and draws on each company's corporate governance, business strategies, and risk management, as well as the specific guidelines of its strategic partners in each industrial sector. By 2025, the system adopts a Zero Trust approach to unify controls in hybrid environments, incorporates ethical AI governance to protect against threats such as data poisoning and deepfakes, and prepares the infrastructure for quantum computing with post-quantum cryptography. This allows the group to offer cybersecurity services to third parties, strengthening its competitive position.

In the financial investment sector, regulations such as the GDPR (General Data Protection Regulation) in Europe and specific SEC (Securities and Exchange Commission) regulations in the United States apply. In the energy sector, regulations such as the NERC CIP (Standards for Critical Infrastructure Protection) and energy market-specific regulations are followed in each country where the business group operates, reinforcing the protection of OT systems against attacks seeking physical damage. In manufacturing, ISA99 standards and solutions for mapping IoT/OT devices are implemented, mitigating risks in the supply chain. In road and airport concessions, data security and privacy regulations established by government agencies such as the OAS (Organization of American States) and aviation control agencies such as the FAA (Federal Aviation Administration) are followed. This comprehensive approach ensures that the cybersecurity management program is aligned with industry-specific standards and regulations, ensuring adequate protection of information assets and mitigation of cyber risks across all of the Group's operations.

The cybersecurity management system is based on a PDCA continuous improvement cycle in each of its 7 functions:

Governance: Strengthening cybersecurity governance to identify, assess, and reduce cybersecurity risk. This includes defining strategic and tactical management committees and developing cybersecurity policies.

Identification: Identifying critical information assets, assessing threats, and reassessing cyber risk.

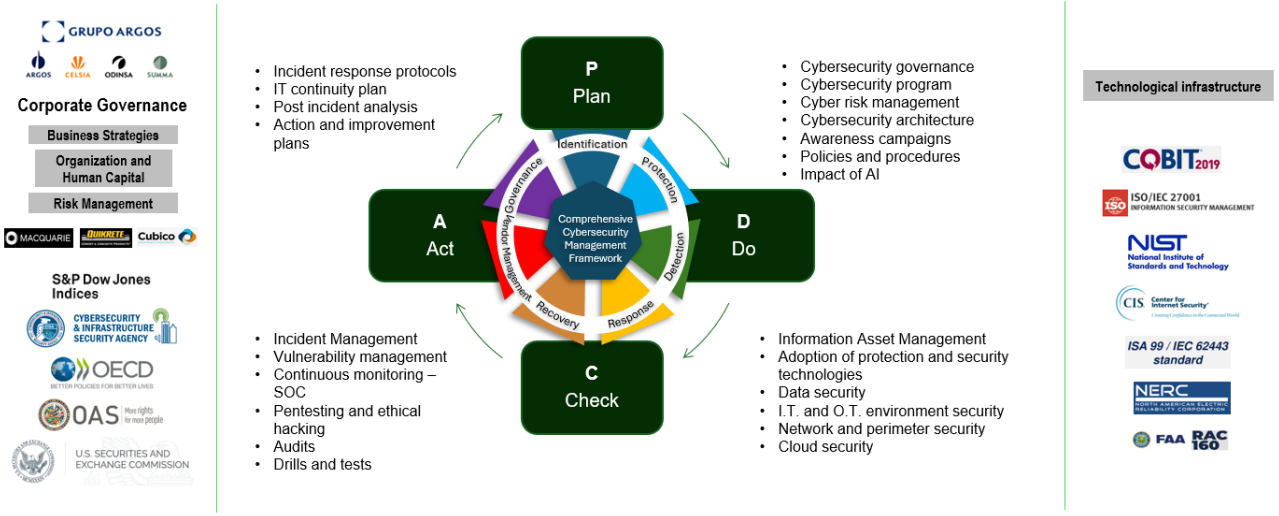
Protection: Developing capabilities to protect information assets against cyber threats. This includes adopting preventive technologies and measures.

Detection: Implementing tools and processes for the early detection of cyber threats and malicious activities.

Response: Developing security incident response plans to respond promptly and effectively to cyberattacks.

Recovery: Planning for business continuity and information recovery in the event of a cyberattack.

Third-Party Management: Integrating cybersecurity policies and controls into the supply chain and collaborating with third-party providers.



10. Cybersecurity Strategy

1. Perspectives

To adapt to emerging trends and challenges in cybersecurity, our strategy considers the following key perspectives:

Artificial Intelligence and Machine Learning: Increased use of these technologies is expected to identify and detect threats more quickly and accurately. Leveraging AI and machine learning to improve detection and response to advanced threats, such as deepfakes and AI-driven phishing, and integrating ethical AI governance to prevent risks such as data poisoning and algorithmic biases, allows the group to offer AI-based managed cybersecurity services to external clients.

Privacy Protection: A renewed focus on data privacy protection and control over personal information, strengthening data privacy through Zero Trust frameworks that ensure continuous authentication and granular controls, complying with global regulations (GDPR), and implementing identity management solutions to protect sensitive data in hybrid environments, positions the group as a trusted provider of privacy services to third parties. Internet of Things (IoT): Security in IoT and OT environments has become a key priority given the increase in connected devices and their exposure to cyberattacks. Protecting these assets is critical to prevent security breaches and physical damage, especially in sectors such as manufacturing and energy. This requires mapping and monitoring devices in dispersed environments, as well as offering specialized IoT/OT security services that ensure visibility, control, and effective response to threats.

Ransomware: Ransomware remains one of the most critical threats, especially in its double and triple extortion variants, which combine encryption, theft, and data disclosure. The cybersecurity strategy must focus on prevention and effective response, including capabilities to detect attacks targeting OT environments that eliminate forensic traces. Strengthening defenses, maintaining secure backups, and having robust response plans are essential to mitigate the impact of these increasingly sophisticated attacks.

Cloud Cybersecurity: Cloud cybersecurity is essential given the growing adoption of hybrid environments. It is key to develop robust solutions that protect data and services, integrating detection tools to mitigate misconfigurations and API attacks. The implementation of models such as Zero Trust Network Access (ZTNA) strengthens access control and segmentation. Furthermore, the group seeks to position itself as a provider of cloud security services to third parties, leveraging its expertise and market demand.

Threats to Artificial Intelligence: Protecting AI systems becomes crucial in the face of emerging threats such as prompt injection and data poisoning, which seek to manipulate machine learning models. It is essential to implement ethical audits, strict access controls, and data validation mechanisms to safeguard the integrity of these systems. Cybersecurity must adapt to ensure that AI operates safely, reliably, and in line with company objectives.

Quantum Computing Readiness: Preparing for the era of quantum computing requires prioritizing the transition to post-quantum cryptography (PQC) to protect sensitive data from future attacks. Following NIST guidelines and the DHS's 2030 deadlines for critical systems, it is vital to begin evaluating and adopting quantum-resistant algorithms, thus ensuring the long-term resilience of strategic information.

Resilience Against Industrial Systems (OT) Threats: Protect OT systems against attacks that seek physical damage, such as those identified by the SANS Institute, using segmentation and real-time monitoring. This allows the group to offer OT security solutions to external industries, such as energy and manufacturing, diversifying its portfolio.

2. Premises for the Construction of the Strategy

The main focus of the current cybersecurity strategy is to build a resilient and ethical Zero Trust-based cybersecurity ecosystem, integrating AI governance, quantum computing readiness, and third-party ecosystem security to protect the business group's global operations and position it as a leading provider of cybersecurity services in external markets. This approach responds to advanced threats, such as the 1,000% increase in AI-driven phishing, deepfakes, attacks on OT systems seeking physical damage, and the need to protect the supply chain with Software Bill of Materials (SBOM).

The strengthening of the management system promotes an ethical culture through training on emerging threats and AI audits. The new premise regarding the third-party ecosystem ensures secure collaboration with suppliers and partners through Zero Trust controls and global threat intelligence, mitigating risks in dispersed environments. This strategy not only protects the group's global operations but also consolidates it as a leader in cybersecurity, capable of expanding services to external clients, with or without equity participation, in an increasingly demanding market.

3. Cybersecurity Strategy

The Business Group's cybersecurity strategy is based on the overriding purpose of maintaining the digital trust and security of our customers and users, with the specific objective of protecting the organization's critical assets and data against cyber threats. It is based on a comprehensive strategy that encompasses risk reduction, resilience, collaboration and awareness, as well as the implementation of cyber defense measures. It is supported by recognized frameworks and draws on corporate governance, business strategies, and governing and oversight agencies to ensure digital trust and security within the organization.

This strategy is structured around five fundamental pillars:

Pillar 1: Risk Reduction

This pillar focuses on strengthening cybersecurity governance to identify, assess, and reduce cybersecurity risk. Strong risk identification capabilities are established, and cybersecurity governance is consolidated through the definition of strategic and tactical management committees. Cybersecurity policies are also established to frame the organization's posture for protecting information assets. This pillar includes the identification of information and cyber assets, threat assessment, and cyber risk reassessment.

This pillar includes:

Strengthening cybersecurity governance to identify, assess, and reduce risk.

Establishing strategic and tactical management committees.

Developing cybersecurity policies that define companies' stance on protecting information assets.

Implementing an ethical AI governance framework to audit models and prevent risks such as data poisoning, bias, or any other threat to information.

Conducting cryptographic inventories to identify systems vulnerable to quantum threats.

Pillar 2: Resilience

Resilience refers to an organization's ability to respond in a timely and effective manner to cyberattacks and ensure operational continuity. This pillar develops security incident response plans and continuity plans that enable the organization to quickly respond to and recover from cyberattacks.

This pillar includes:

Development of capabilities to respond to and ensure operational continuity in the face of cyberattacks, including the design of continuity plans that integrate IT and OT for attacks on critical infrastructure.

Development of security incident response plans and continuity plans.

Pillar 3: Collaboration and Awareness

This pillar focuses on fostering a cybersecurity culture and promoting collaboration among various stakeholders, both internal and external. Effective communication channels are established and cybersecurity education is promoted. Awareness and collaboration are essential to strengthening defenses and addressing cyber threats together.

This pillar includes:

Promoting a cybersecurity culture and collaboration among various stakeholders, both internal and external, including training programs on deepfakes, AI phishing, and the ethical use of AI, tailored to the group's industries.

Integrating threat simulations (phishing, OT attacks) to reinforce awareness among employees and partners.

Implementing effective communication channels and cybersecurity education programs.

Pillar 4: Cyber Defense

The cyber defense pillar focuses on adopting cybersecurity protection technologies and tools, including machine learning and artificial intelligence (AI) capabilities, to effectively address emerging threats. Generative AI has played a crucial role, not only in the hands of cybercriminals but also in accelerating the detection of cyberattacks globally. The usefulness of AI in analyzing large volumes of data and improving threat detection is highlighted. In a geopolitical context, cyberwarfare and hacktivism are increasingly relevant, making it necessary to have preventive, detective, and corrective policies, as well as updated cybersecurity tools.

This pillar includes:

Adoption of cybersecurity protection technologies, including machine learning and AI capabilities to address emerging threats.

Implementation of preventive, detective, and corrective actions and policies to protect IT systems and data.

Pillar 5: Strategic Integration of the Third-Party Ecosystem and Disruptive Technologies

Ensure the security, interoperability, and resilience of the business group's third-party ecosystem (suppliers, strategic partners, supply chains) while leading the adoption of disruptive technologies, positioning the business group as a global innovator.

This pillar includes:

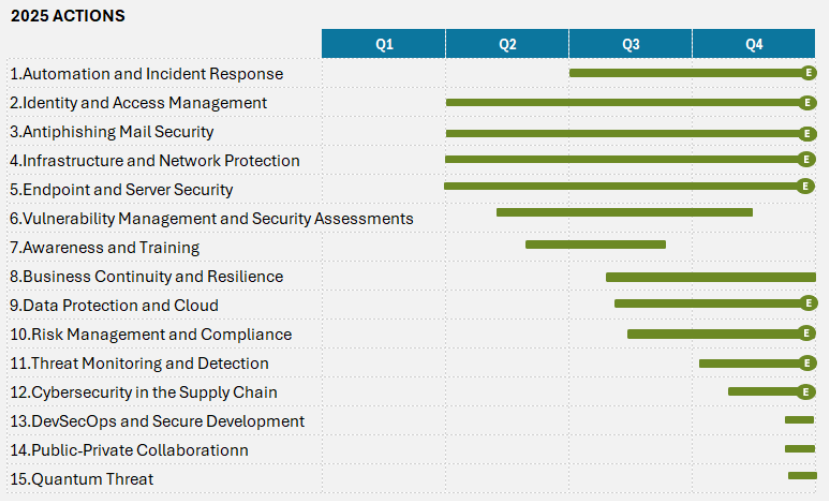
Strengthening third-party security by mitigating risks in manufacturing and energy.

Integrating threat intelligence to monitor actors on the dark web, ensuring the trust of partners and investors.

Preparing infrastructure for quantum computing.

Aligning with regulations (NERC CIP, ISA99, GDPR, FAA) to ensure interoperability with external partners.

Offering ecosystem auditing services and security solutions.



11. Cybersecurity Architecture and Controls

Cybersecurity Architecture is defined as a set of representations that describe the function, structure, and interrelationship of security components within our Information Technology and Operations environment. Our architecture is based on fundamental principles. First, we apply the concept of Security by Design, ensuring that information protection is aligned with business objectives and considering the interconnectivity and interoperability of systems. Likewise, we implement Least Privilege Authorization, ensuring that people, systems, applications, and processes have access only to the information necessary to fulfill their functions, establishing a default state of no access. We seek standardization of our security components to reduce the complexity and cost of security, guaranteeing uniform processes and facilitating automation. In addition, we implement the principle of Defense in Depth, which consists of ensuring integrated protection and activating controls at all layers of the system. This principle, detailed later in this document, is fundamental to guaranteeing robust security that is adaptable to different threats. We consider system redundancy to mitigate potential security breaches and ensure business continuity. We strive to achieve user acceptance by ensuring that our security measures are psychologically acceptable. Additionally, we apply the Identity Principle, ensuring that all

security components have a unique identifier. Finally, we effectively manage risks to reduce information exposure and maximize the performance of our Information and Operational Technologies.

The principle of defense in depth is a fundamental cybersecurity strategy that seeks to provide a series of overlapping and complementary layers of security to protect the business group's information assets and systems. This strategy is based on the idea that if one layer of security fails or is breached, additional layers are in place to prevent, detect, or mitigate potential attacks or intrusions.

Instead of relying solely on a single security measure, multiple layers of security are implemented with different approaches and controls, significantly increasing the robustness of the security system. Some of the security layers that can be implemented as part of defense in depth include:

Network perimeter: We use firewalls, intrusion prevention systems (IPS), intrusion detection systems (IDS), and other security devices to protect the network perimeter and control incoming and outgoing traffic. Identities, Authentication, and Access Control: Measures such as strong passwords, multi-factor authentication (MFA), role-based access controls (RBAC), and access policies are implemented to ensure that only authorized users have access to systems and data. In addition, we focus on identity management, which encompasses the centralized and secure administration of users' digital identities, including the creation, modification, deactivation, and deletion of user accounts in a timely and controlled manner. Through a comprehensive approach to identity security, we strengthen our ability to protect our information assets and prevent unauthorized access to our systems and sensitive data.

Endpoint security: Security measures are implemented on endpoint devices, such as computers and mobile devices, to protect them against threats such as malware, ransomware, and phishing attacks.

Application security: Application development security controls, such as penetration testing, static and dynamic code analysis, and web application firewalls (WAFs), are implemented to protect applications from vulnerabilities and attacks.

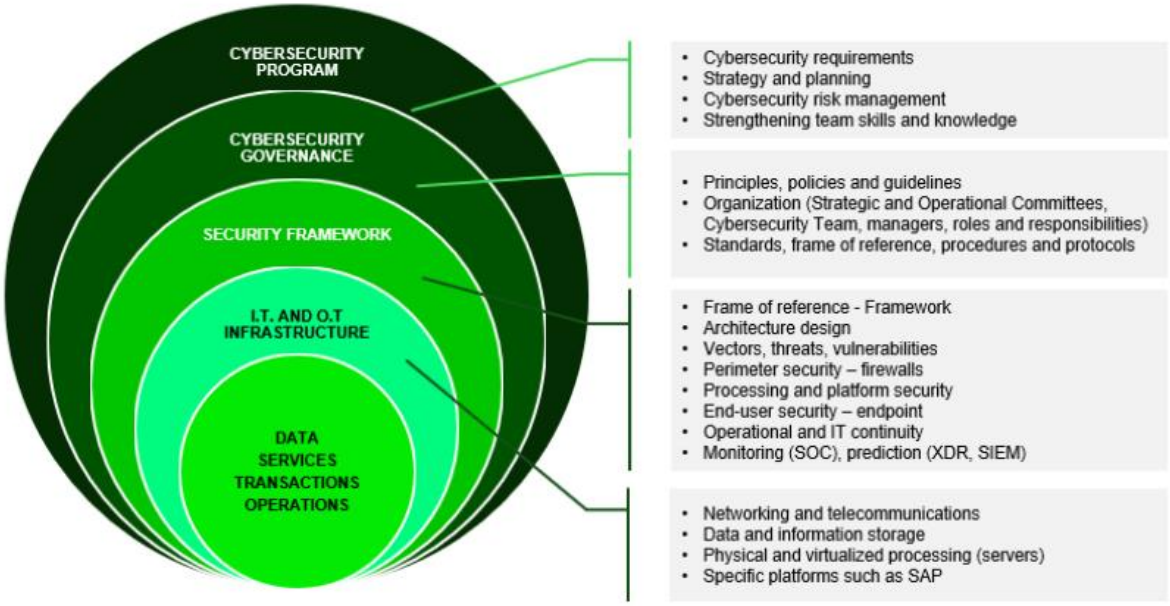
Data security: Encryption measures, both in transit and at rest, are implemented to protect data confidentiality and integrity. Data loss prevention (DLP) controls and backup and recovery mechanisms are also implemented to ensure data availability.

Cloud security: Specific security measures are implemented to protect data and systems residing in public, private, or hybrid cloud environments. This includes the use of cloud security services, such as web application firewalls (WAFs), policy-based access controls, data encryption, and continuous cloud security monitoring. Industrial Systems Security (OT): We ensure the integrity and availability of industrial and operational systems (OT) by implementing specific security controls, such as network segmentation, critical asset monitoring, and regular security updates.

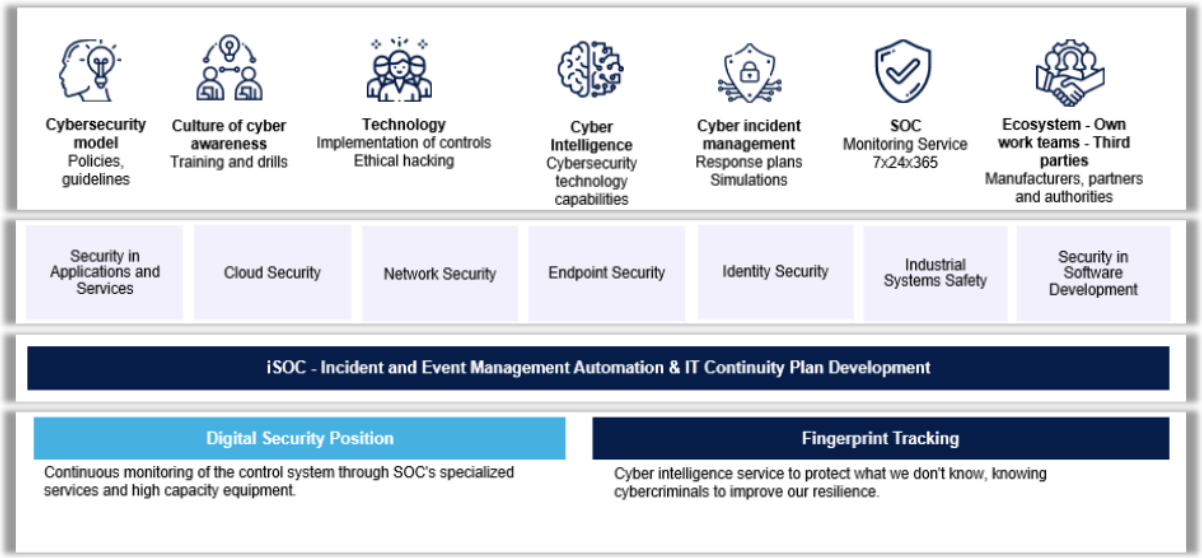
Software Development Security: We integrate security measures throughout the software development lifecycle, including penetration testing, static and dynamic code analysis, and security training for developers, to prevent vulnerabilities and ensure application security.

Intrusion Detection and Response: We use tools and systems to monitor and detect malicious or suspicious activity on the network and systems. This may include intrusion detection systems (IDS), security information and event monitoring (SIEM), and user and entity behavior analytics (UEBA).

Awareness and Training: We conduct cybersecurity awareness and training programs to educate employees on security best practices and promote a culture of security within the organization.



By implementing defense in depth in all of these areas, we strengthen our cybersecurity posture and significantly reduce the likelihood of successful attacks. Each layer of security contributes to the overall protection of information assets and systems, creating a more resilient security environment that is adaptable to ever-evolving threats.



12. Vulnerability Management Lifecycle

Vulnerability management is an essential component of the Business Group's cybersecurity program, designed to mitigate risks arising from security breaches in technological platforms. This process begins with the identification of vulnerabilities through an agnostic and multidimensional approach, which considers human resources, automated scans, technical audits, and specialized tools. The objective is to understand the real risks affecting critical assets and offer effective solutions to address them, with a scope that covers all of the group's technological systems. The process begins with the identification of the systems to be assessed and culminates with the confirmed remediation of the vulnerabilities and the issuance of the closure report. See: Vulnerability Management Procedure.

Guidelines

The procedure establishes guidelines that allow for the ongoing detection, evaluation, and treatment of security weaknesses in technological assets. Management begins with the reporting of critical assets by the Infrastructure area, followed by sampling and inclusion in the scanning tool. Tests are performed continuously for systems with installed agents and monthly for all other systems. The results are managed by the Cybersecurity team, in collaboration with the Security Operations Center (SOC), without affecting the operation of business processes. Detected vulnerabilities are classified according to their criticality (critical, high, medium, low), which determines the maximum recommended time for treatment, ranging from one month for critical vulnerabilities to six months for low-level vulnerabilities.

The established remediation timeframes vary depending on the criticality of the finding. Critical vulnerabilities must have compensating controls in place within the first seven days and be fully closed within one month. High-level vulnerabilities have a timeframe of two months, medium vulnerabilities three months, and low vulnerabilities six months. Exceptions to these deadlines can only be approved by the CISO, considering factors such as the asset's level of exposure, its strategic value, and its history as a target of attacks.

Roles and Responsibilities

The process has a clear distribution of responsibilities. The Cybersecurity Specialist is responsible for documenting, analyzing, and implementing improvements in the vulnerability lifecycle. The Cybersecurity Manager leads the implementation of technical controls and ensures policy compliance, in addition to generating the required reports and metrics. The CISO, for his part, is responsible for making strategic decisions, such as approving exceptions and choosing tools. Network, infrastructure, application, and user IT specialists are responsible for applying patches, managing configurations, and providing risk acceptance support when certain vulnerabilities cannot be mitigated.

Process Flow and Findings Management

The operational process flow begins with the verification of the technological assets to be scanned, their correct configuration in the scanning tool, and the execution of the test. Once the results are obtained, a detailed analysis is performed to classify the findings and validate whether immediate action is required. In critical cases, the change process is activated to apply emergency patches. For less critical vulnerabilities, a vulnerability matrix is documented and then disseminated to the responsible teams. These teams must implement corrective actions, which are managed and validated by the vulnerability lifecycle work cell.

The process also includes the management of findings from Ethical Hacking (ETH) tests, which allow for a more in-depth identification of exploitable weaknesses. These findings are analyzed to determine whether they require immediate action, and if so, the corresponding emergency change is managed. In all cases, the recommendations are rigorously followed up until the gaps are confirmed to be closed. Finally, detailed reports are prepared with the results of each exercise, which serve as evidence for the responsible areas and as input for future audits.

The process includes supporting documentation such as flowcharts and a baseline of critical assets. Key concepts for understanding the process are also addressed, such as vulnerability, risk, scanning, critical assets, and ethical hacking tests. These elements allow for a shared understanding among the stakeholders involved and strengthen process governance.

13. Business Continuity Management

Business continuity management is a strategic pillar that strengthens the Business Group's resilience, providing a solid framework based on policies, guidelines, impact analyses, strategies, procedures, and well-defined roles. This program prepares the organization to face disruptions—such as technical failures or cyberattacks—emergencies affecting physical facilities, and crises with a high reputational impact, ensuring the continuous operation of critical processes in Manufacturing, Energy, Concessions, and Financial Investments. Beyond protecting the group's interests, this initiative fosters a culture of preparedness and response among employees, enhances the institutional reputation, and positions the group as a competitive leader, capable of offering continuity solutions to third parties in a global environment.

The continuity model is structured around three key pillars: disruptions (technical failures, human errors, or malicious acts, including attacks on operating systems), emergencies (events that compromise the physical infrastructure), and crises (prolonged scenarios with reputational repercussions). This approach, supported by international standards and emerging technologies such as advanced cryptography, ensures that the group not only overcomes disruptions but also transforms them into opportunities, integrating cybersecurity as an essential component of its strategy.

The core purpose of the program is to establish a strategic and operational framework that guarantees the continuity of the Business Group's business in the face of disruptive events, aligning with recognized global standards. This framework seeks to prevent, contain, and efficiently recover operations, protecting the confidentiality, integrity, and availability of information. In 2025, the program focuses on anticipating emerging threats such as attacks on critical systems and advanced technological risks, while strengthening the group's ability to offer continuity services to external clients, consolidating its leadership in regulated sectors such as Energy and Concessions.

The program covers all the Business Group's companies, their critical processes, technology services, physical and digital infrastructure, collaborators, and strategic third parties, including suppliers and partners in Manufacturing, Energy, Concessions, and Financial Investments. In 2025, its scope extends to external ecosystems, supporting business expansion with managed cybersecurity solutions.

Key Program Components

The program is based on three interdependent components that ensure a comprehensive response. Prevention protects life, well-being, and critical resources, reducing the likelihood of disruptions through predictive controls and third-party audits. Containment enables a rapid and effective response to incidents, minimizing impacts with comprehensive plans for technological and operational systems. Recovery restores critical processes based on business impact analysis (BIA) and metrics such as recovery time (RTO) and recovery point (RPO), integrating

advanced solutions to address technological threats, and offering recovery services to third parties such as airports or power plants.

Continuity Governance

The program establishes a clear, strategic organizational structure. The Boards of Directors and the Audit, Finance, and Risk Committees lead approval, oversight, and monitoring, ensuring alignment with corporate objectives. The presidents of the business group's companies and Steering Committees drive implementation and report on progress, while the Integrated Risk Management Area designs policies and leads the strategy. The Risk and Technology Areas of the subsidiaries execute operational tactics, and Process Owners and Risk Managers identify risks and promote a culture of continuity. Internal Audit evaluates effectiveness, and all employees apply the protocols, supporting the expansion of continuity services to third parties.

Related Response Plans

Business continuity is articulated through comprehensive plans that ensure an adaptive response. SUMMA's Emergency Plans address physical emergencies at administrative headquarters, protecting critical infrastructure. The Crisis Management Plan (CMP) equips the Crisis Management Committee (CMC) with tools to manage high-impact scenarios, adapting to events such as prolonged cyberattacks. The Technology Recovery Plan (DRP) restores critical technology platforms with advanced simulations and solutions, while Critical Process Recovery Procedures (BCP) restore essential operations in Manufacturing, Energy, and Concessions, providing services to third parties such as airports.

Integration with Cybersecurity

The Continuity Program is strategically integrated with the Cybersecurity Program, recognizing that incidents such as ransomware, intrusions, or attacks on operating systems are primary causes of disruptions. The Cybersecurity Incident Response Procedure, supported by predictive technologies and segmentation, ensures threat detection, analysis, containment, and eradication, facilitating the secure restoration of technological services. This coordination ensures a rapid response to cyberattacks, immediately activates recovery plans (DRP, BCP, PMC), and aligns the Crisis Committee for escalated incidents, prioritizing critical processes defined in the BIA.

Control and Approval Officers

The program involves the Boards of Directors, Audit, Finance, and Risk Committees, company Presidents, Risk and Technology Departments, Risk Managers, Internal Audit Departments, and all employees, who play an active role in its implementation and promotion, as well as external clients who access related services.

The Boards of Directors approve the program, while the Audit, Finance, and Risk Committees oversee its execution and progress, ensuring alignment with regulations and strategic objectives, including preparation for global markets.

14. Data Protection and Encryption

The main objective of this section is to establish robust technical criteria for the encryption of information, both in transit and at rest, aligned with the Business Group's data classification. This approach protects the confidentiality, integrity, and availability of information, strengthening security and cybersecurity in a global and dispersed environment. In 2025, the program prioritizes anticipating emerging risks, such as quantum threats and advanced attacks, ensuring the protection of critical data in Manufacturing, Energy, Concessions, and Financial Investments, while complying with regulations such as NERC CIP, GDPR, FAA, and ISA99.

Strategic Approach

Data protection and encryption are essential to ensure strong authentication mechanisms, non-repudiation, and the security of corporate information and identities against cyber threats. This comprehensive approach minimizes risks associated with confidential information leaks, protecting the sensitive data of the group and its strategic partners across all industries. To this end, advanced protocols such as TLS (Transport Layer Security) and IPSec (Internet Protocol Security) are implemented, ensuring secure data transport on internal and external networks, including internet connections. These protocols are used to protect confidential information, such as financial data or critical infrastructure, from unauthorized access.

The encryption complies with international standards, such as those established by NIST in the FIPS standard, ensuring that the algorithms and modules used are resistant to brute-force attacks, even by actors with significant computational power. This applies to both low-privilege user and administrator passwords, protecting critical systems in the Energy and Manufacturing sectors. Furthermore, preparation for disruptive technologies is prioritized through the adoption of post-quantum cryptography (PQC), ensuring that the group's systems are ready to withstand future quantum threats, especially in regulated sectors such as Financial Investments.

Key Activities

To ensure effective protection, the program establishes specific activities. Critical cryptographic vulnerabilities, such as those that could compromise large-scale systems, were remediated within a maximum of 60 days of identification, implementing preventive and detective controls if full remediation is not immediately feasible. Encryption keys are stored centrally and securely for up to five years from their last use, facilitating corporate, legal, or judicial investigations, a key aspect for Concessions and Financial Investments.

Confidential information at rest is protected through physical storage in secure locations, such as safes, or through encryption with keys separate from the encrypted data, ensuring its integrity across all group companies. Furthermore, a detailed and separate log of encrypted data is maintained, allowing investigators to validate that the lost information was protected at the time of the incident, a crucial requirement for compliance with regulations such as the GDPR. The implemented authentication mechanisms are robust, resisting attacks such as keylogging, replay, session hijacking, and brute force, utilizing digital certificates, one-time passwords, multi-factor authentication, and symmetric and asymmetric encryption, which reinforces identity protection across all sectors.

Management and Review

Session encryption using protocols such as TLS or IPSec does not require additional hardware-level protection, except in scenarios where a compromise represents a catastrophic risk, such as transactional operations in Financial Investments. However, encryption protocols, algorithms, and modules are reviewed annually, validating exceptions to the security policy to maintain their effectiveness against new threats. Likewise, security controls applied to encryption and data protection are evaluated annually, identifying and correcting potential operational flaws, a process that ensures alignment with international standards and industry regulations.

Impact and Value

This strategic approach to data protection and encryption strengthens the Business Group's resilience against cyber threats, protecting critical assets and ensuring the trust of customers and partners. By integrating advanced technologies such as PQC and robust authentication mechanisms, the program not only complies with strict regulations but also positions the group as a cybersecurity leader, capable of offering data protection services to third parties, such as airports or financial partners, generating commercial value in a competitive market.

15. Classification of Information

The Business Group defines the criteria and corporate methodology for the inventory, classification, and labeling of its information assets, consolidating them as a strategic pillar of comprehensive asset management, in strict alignment with cybersecurity policies. This approach ensures that information receives the appropriate level of protection based on its value and criticality, strengthening security in Manufacturing, Energy, Concessions, and Financial Investments, and complying with regulations such as NERC CIP, GDPR, FAA, and ISA99, while protecting against emerging risks in a global environment.

Definition and Scope of Business Information

Business information comprises all data owned or maintained by the Business Group, related to its business activity. This includes knowledge, trade secrets, strategic, economic, tax, administrative, and operational information, as well as information protected by intellectual property or specific legal regimes. By 2025, the program recognizes the importance of protecting data in a context of increasing interconnectedness and advanced threats, such as unauthorized access to critical systems or breaches of personal data, ensuring confidentiality, integrity, and availability across all of the Group's industries.

Classification of Business Information

Business information is classified according to its level of access and use, prioritizing its protection. Restricted access information includes confidential data, trade secrets, data protected by intellectual property, confidential information, information related to contracting processes, organizational information, personal data, and information about third parties in custody. For example, confidential information—such as financial or tax data—can only be accessed by authorized shareholders and executives, in compliance with the Commercial Code, while trade secrets, such as non-patentable strategic knowledge, require high-level security measures, including access and modification logs. Information protected by intellectual property, such as distinctive signs or internally developed software, is restricted to authorized business uses, with the Communications Department overseeing exceptions.

Confidential information includes data on clients, suppliers, and strategic projects, while personal data is governed by Law 1581 of 2012, ensuring its protection across all group companies. On the other hand, publicly accessible information is divided into internal public information, which can be shared between departments for operational purposes, and external public information, such as the mission, vision, corporate values, or data registered in the business registry, always subject to the restrictions defined by the group. Critical cyber assets, such as those that use routable protocols or are externally accessible, are also classified as restricted, guaranteeing additional controls to protect critical infrastructure in Energy and Manufacturing.

Information Asset Inventory

The information asset inventory is a structured process that identifies and documents each asset with key characteristics: name, description, owner, associated area, presence of personal data, container (physical or electronic), custodian, classification, and criticality. For example, an asset may include customer databases stored in SharePoint or external servers, with a defined owner who establishes the necessary controls. If the asset contains personal data, it is registered in accordance with Law 1581 of 2012, detailing its purpose, owners, and security measures. This inventory, reviewed annually, ensures accurate and up-to-date management, protecting data across all the group's industries.

Classification and Criticality

Asset classification is based on the security pillars of confidentiality, integrity, and availability, aligned with standards such as ISO 27001. Confidentiality is categorized into high (reserved or secret), medium (confidential),

and low (internal or public) levels, defining who can access the information and under what conditions. Integrity assesses the impact of unauthorized modifications, classifying assets as high, medium, or low based on operational or economic consequences. Availability measures the acceptable downtime, prioritizing assets that, if not accessible within one day, generate significant impacts. Criticality combines these criteria, identifying high-priority assets (for example, with high confidentiality) to assign them stricter controls, ensuring the protection of strategic data in Financial Investments and Concessions.

Tagging and Handling

Asset tagging is based on confidentiality, applying rigorous guidelines. Confidential, secret, or confidential information requires encryption for transmission and storage, visible labels (digital or printed), and secure, locked storage to prevent unauthorized access. For destruction, secure erasure techniques are used, and printed documents are transported in sealed envelopes. Tag nomenclature follows the ID-Confidentiality-Availability-Integrity format, facilitating identification, such as “0001-MC-A-M” for an asset with medium confidentiality, high integrity, and medium availability. This process ensures that sensitive data across all industries is protected and handled appropriately.

Repositories and Storage

The program recommends secure tools for storing information. OneDrive is used for internal or confidential data that employees need to share, enabling secure collaboration. Collaboration tools facilitate the sharing of public or internal information in meetings, while SharePoint stores confidential or secret data common to processes, such as contracts or indicators. High-critical information, such as board minutes or personnel databases, is stored in business applications or restricted SharePoint sites. The use of portable hard drives is prohibited for corporate documents, minimizing the risk of information leakage.

Management Procedure

The inventory, classification, and labeling procedure consists of four stages. During the definition process, a responsible team in each company identifies the assets to be inventoried, working with process owners to validate them annually. The review verifies the assets' relevance and adjusts their classification in response to organizational changes, new processes, or system migrations. The update incorporates these changes into the inventory, and publication ensures that the document is classified as "Confidential," with restricted access to modifications. The classification is shared with custodians to apply the necessary controls. This procedure strengthens data management within the group, ensuring its security and regulatory compliance.

Impact and Value

Information classification aims to ensure secure data management, protecting critical assets and minimizing the risk of unauthorized disclosure. By implementing a structured approach, the cybersecurity program ensures regulatory compliance, strengthens customer and partner trust, and enables business opportunities, such as offering data management services to third parties, consolidating its competitive advantage.

16. Cybersecurity Awareness

The accelerated digital transformation driven by the pandemic has exposed organizations to new cyber threats, especially those based on social engineering. Attackers no longer rely exclusively on technical vulnerabilities, but instead exploit human error through techniques such as phishing, manipulation, or deception. In this context, employees and contractors become the first line of defense. Therefore, it is essential to establish a structured culture and awareness strategy that educates, sensitizes, and empowers staff against emerging digital risks. This strategy must go beyond simple training and seek a sustained change in behavior toward a conscious and preventative attitude. See: Security Culture and Awareness Program.

Purpose and Objective of the Awareness Program

The culture and awareness program aims to tangibly improve the organization's security posture by prioritizing human risk management. It seeks to develop a collective awareness that promotes security self-control, operational discipline, and the commitment of each employee to protecting digital assets. Its objectives include protecting information from internal and external threats, improving incident response capacity, strengthening organizational resilience, and creating a network of human sensors that can detect and report incidents before they escalate. It also seeks to establish clear metrics to measure the program's effectiveness and ensure ongoing support from the organization's leaders.

Justification and Strategic Importance

Technical controls, although crucial, are insufficient against attack vectors focused on human behavior. Everyday actions such as opening suspicious emails, using unknown USB devices, or interacting with links on social media represent gaps that can be exploited by attackers. Employees' lack of adherence to security policies represents a significant risk. Therefore, ongoing awareness and training are positioned as the best preventive response to close these gaps and strengthen the organization's collective defense.

The program applies to all employees, contractors, and third parties with access to the organization's systems, data, or networks. The IT Security team is responsible for leading the program's execution and sustainability, with support from Human Talent and process leaders. Their tasks include identifying target audiences, designing content, planning campaigns, selecting media outlets, and evaluating impact. All of this is implemented under an annual plan that maintains the program's continuity, adaptability, and effectiveness.

Audiences and Segmentation

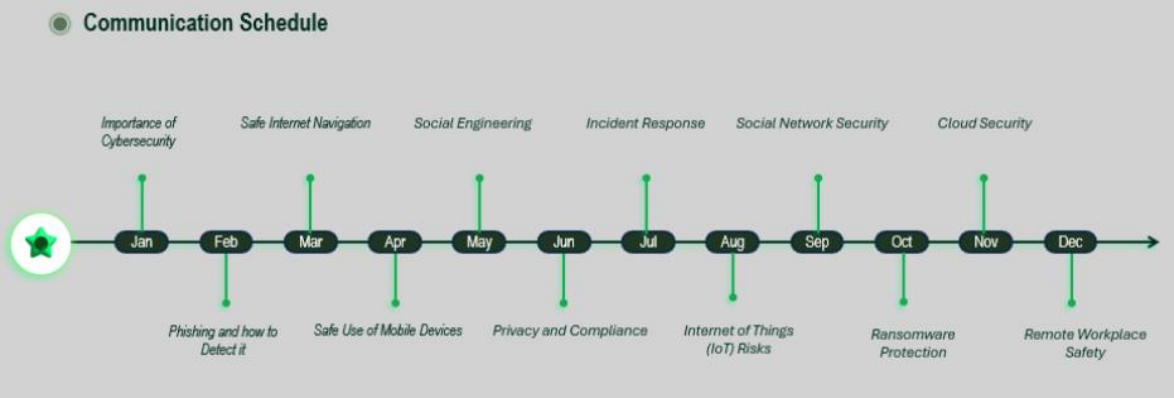
The program recognizes that not all audiences require the same type of training. Therefore, it segments its campaigns into three main groups: general staff (employees and contractors), privileged users (such as system

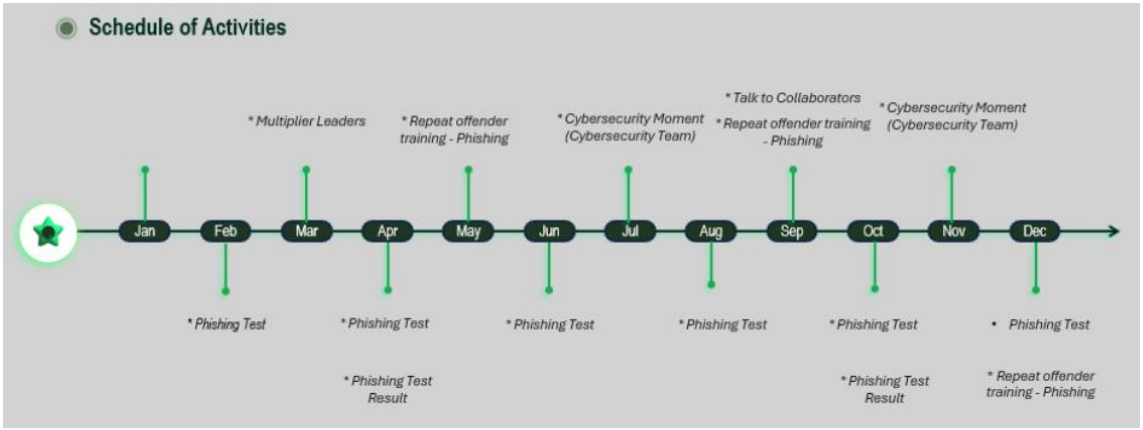
administrators), and executives (such as vice presidents or managers). Each group receives content tailored to their risk level, access type, and strategic role within the organization, using methods such as visual campaigns, targeted training, and self-learning platforms.

Human Risks to be Mitigated

The human risks addressed by the program include the loss or disclosure of information, unauthorized data alteration, malware infection, and unintentional human error such as incorrect information submission. Risk is defined as the combination of the probability of occurrence and the impact of the incident, and can originate from both negligence and deliberate attacks. The campaigns seek to reduce these risks through awareness and the modification of insecure behaviors.

The topics addressed are selected based on their relevance and applicability to all levels of the organization. They include password management, malicious email detection, safe use of social media, personal data protection (Law 1581), incident response, and best practices during travel or remote work. Specific technical topics for privileged users, such as secure development, cloud security, and asset management, are also included.



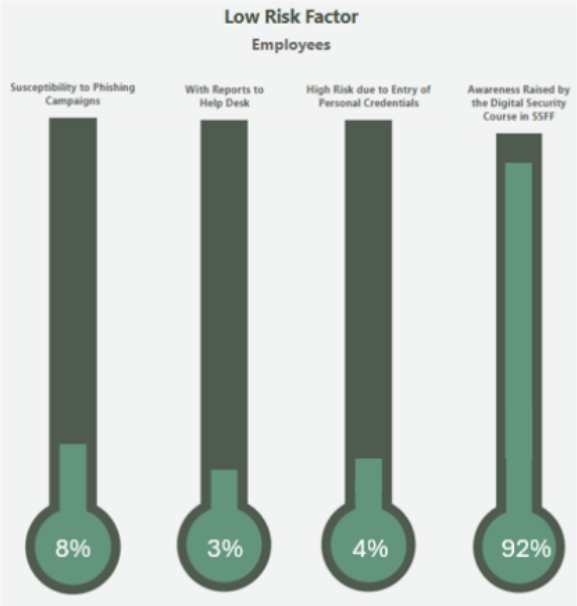


Communication Techniques and Dissemination Channels

To ensure effective coverage, the program utilizes multiple communication channels: physical speakers, intranet, email, wallpapers, e-learning modules, and internal social media. Key messages are also reinforced through targeted sessions and visual materials that aim to maintain constant attention on risks and best practices.

Evaluation, Metrics, and Success Indicators

Program effectiveness is measured through simulated phishing campaigns, cultural surveys, lost device reports, and threat behavior analysis. Metrics are divided into three types: compliance (what is done), impact (behavior changes), and strategic (incident reduction). These metrics allow managers to make informed decisions, identify areas for improvement, and report progress to senior management.



The program is formalized each year in a detailed plan that includes specific objectives, activities by target group, campaign schedule, evaluation techniques, and corrective actions. This document guides ongoing implementation and maintains an improvement cycle that ensures the program's maturity over time.

The program is aligned with international standards such as ISO/IEC 27001 and SOC 2, meeting the training requirements for information security system management. Mandatory training includes general security, ISMS, and secure development, and its periodic implementation supports compliance controls for audits and certifications.

17. Cybersecurity Program Audit

Cybersecurity auditing is a critical function within the comprehensive technological and digital risk management model. Its purpose is to independently and systematically assess the effectiveness of implemented controls, the level of process maturity, and the degree of compliance with regulatory frameworks, internal policies, and international standards. In addition to enabling retrospective evaluation, this activity acts as a continuous improvement mechanism, promotes the early detection of weaknesses, and strengthens the defense posture against emerging threats. The audit process should not be understood solely as a regulatory or administrative requirement, but as a strategic enabler to ensure the organization's cyber resilience, operational efficiency, and digital trust.

The main objective of this chapter is to establish how the cybersecurity capabilities deployed in the organization are reviewed, validated, and strengthened through periodic audits. These audits are conducted in close coordination with internal and external audit departments, ensuring their alignment with corporate risks, strategic priorities, and management frameworks such as NIST CSF, ISO/IEC 27001, and COBIT. These audits ensure that controls do not exist solely on paper but are effective, measurable, and properly integrated into business processes.

Plans

During the year, an audit plan was structured that covers multiple dimensions of the digital and technological environment. These audits were designed with a risk-based approach and cover both technical and strategic aspects. The most relevant projects include audits with Ethical Hacking on critical platforms, a review of the organizational cyber resilience level with the support of specialized consultants, and the validation of digital transformation initiatives. Audits aimed at reviewing the overall cybersecurity strategy and the controls implemented by strategic suppliers have also been prioritized as part of a more robust approach to supply chain risk management.

Scope of the Audits

The scope of these audits is broad and covers essential elements of corporate cybersecurity. First, governance is analyzed, i.e., the existence and implementation of policies, strategic plans, defined roles, and appropriate oversight mechanisms. Second, technical aspects are assessed, such as penetration testing (Ethical Hacking), configuration reviews, vulnerability scans, and compliance analysis against recognized security benchmarks such as those of the Center for Internet Security (CIS). Another essential component is organizational resilience, measured through the maturity of business continuity plans (BCP), disaster recovery plans (DRP), and crisis management plans (PMC), all of which are assessed not only in terms of their documentation but also in terms of their applicability and practical testing. Likewise, controls applicable to third parties and strategic suppliers are reviewed, incorporating on-site visits and analysis of contractual compliance with security clauses. Finally, the

integration of cybersecurity into innovation and digital transformation initiatives is considered, ensuring that the principles of "security by design" are present from the early stages of the project lifecycle.

Integration with the Business Continuity Program

A fundamental aspect of this audit approach is its integration with the Business Continuity Program. These reviews identify synergies and dependencies between the cybersecurity incident response procedure, operational continuity plans, technological disaster recovery plans, and institutional crisis management plans. This integration is critical to ensuring that, in the event of a disruptive event—such as a cyberattack, massive data loss, or a disruption to the digital supply chain—the organization's response is swift, coordinated, and effective. The audits verify whether the scenarios contemplated in the BCPs and DRPs include cyber incidents, whether specific drills for ransomware attacks or information exfiltration have been conducted, and whether there is clear traceability of responsibilities during crisis management.

As a result of these exercises, recommendations and improvement plans are generated, prioritized according to their level of criticality and the inherent risk they represent for the organization. These action plans include corrective and compensatory measures and are managed using GRC (Governance, Risk, and Compliance) tools with structured follow-up by the Cybersecurity Committee. Furthermore, progress and relevant findings are presented to the Risk and Audit Committees, thus ensuring visibility and oversight at the highest level. The benefits of this process include the timely correction of technical or regulatory deviations, the strengthening of key controls, improved protection against emerging threats, and increased maturity in digital asset governance.

Finally, lessons learned are documented and transferred to the responsible teams, not only to resolve immediate findings but also to prevent their recurrence. This practice has led to concrete improvements such as policy updates, the integration of recurring findings into annual training plans, the automation of critical findings follow-up, and the periodic review of the organization's maturity based on models such as the NIST CSF Tiers or the CMMI.