IT SECURITY / CYBERSECURITY

ARCACONTINENTAL

IT SECURITY / CYBERSECURITY

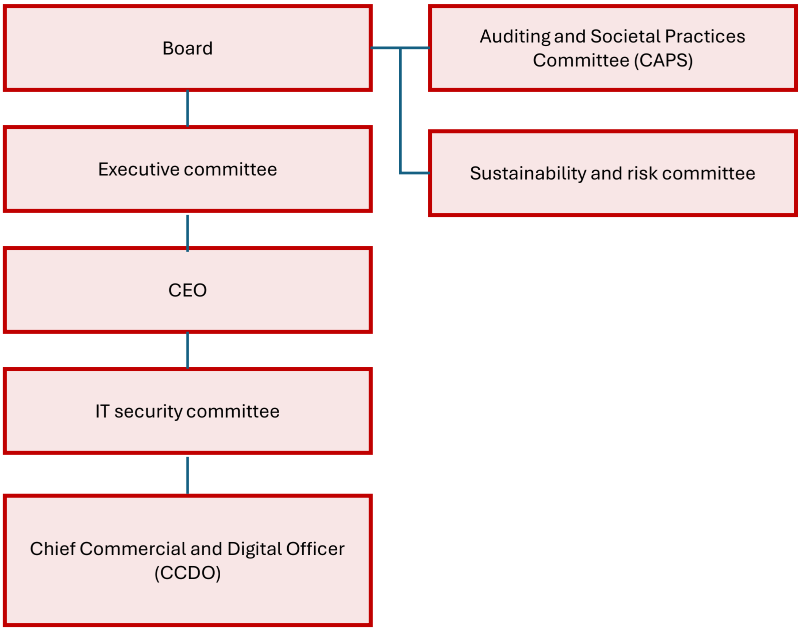
In today's rapidly digitizing world, where technological advancements such as cloud computing, online marketplaces, and digital payments have become the norm, Arca Continental recognizes the paramount importance of ensuring the utmost cybersecurity. As a leading bottling company, we understand that maintaining uninterrupted access to our network, IT systems, and sensitive data is crucial for the smooth functioning of our operations. Any disruptions or subpar performance in these areas can have severe repercussions, leading to increased costs and reputational risks for our organization. We are acutely aware of the risks associated with technical failures, human errors, malicious attacks, adverse weather events, natural disasters, and even potential terrorist threats. To mitigate these risks and ensure business continuity, we prioritize the implementation of comprehensive cybersecurity measures, including robust contingency plans.

Over the past decade, the alarming rise in information security breaches, some reaching unprecedented scales, has demonstrated the ever growing and evolving cyber threat landscape It has become evident that information security and cybersecurity have emerged as financially material issues that demand diligent management to safeguard our corporate value The multifaceted costs of cyberattacks can manifest in various ways, encompassing both internal operational expenses incurred in addressing cybercrime and incident prevention, as well as external consequences like the loss or theft of sensitive information, disruptions in our operations, potential fines and penalties, infrastructure damages, and even revenue losses due to customer attrition Therefore, ensuring the security and resilience of our networks and information systems is of utmost importance to Arca Continental as we strive to protect our customers, providers, collaborators and investors to maintain industry leadership, and drive sustainable growth in the dynamic bottling industry.

IT security Governance

Arca Continental places a strong emphasis on cybersecurity within our governance framework. We understand the critical importance of addressing cyber threats and ensuring the capability of our management team to effectively manage cyber-related issues. We foster a culture of continuous learning and development, equipping our board and senior executives with the necessary knowledge, leadership, and strategic skills to navigate the evolving cybersecurity landscape. By prioritizing cybersecurity throughout our organization, we strive to prevent IT system failures and major information security incidents, safeguarding our valuable assets and maintaining the trust of our stakeholders.

IT security Governance structure


Board
Auditing and Societal Practices Committee (CAPS)
Executive committee
Sustainability and risk committee
CEO
IT security committee
Chief Commercial and Digital Officer (CCDO)

Our comprehensive governance framework enables us to establish and maintain business continuity while effectively addressing cybersecurity challenges.

Board-level oversight:
The Auditing and Societal Practices Committee (CAPS) is in charge of supervising the cybersecurity strategies and processes. Their valuable insights and recommendations guide our decision making and help us ensure the integrity and resilience of our cybersecurity measures. The members of this committee are Sanjuana Herrera Galván, Ernesto López De Nigris and Armando Solbes Simón; who have held relevant positions in the financial, telecommunications, health and other sectors.

Executive Management Responsibility: Santiago José Herrera Varón

Chief Commercial and Digital Officer (CCDO), and the senior executive in charge of overseeing technology, systems, and information security with a primary focus on ensuring the quality of the cyber security security process

IT security Measures and Processes

At Arca Continental, we are committed to fostering a culture of information security and cybersecurity, integrating security principles and practices across all areas of our business W e are committed to fostering a culture of information security and cybersecurity, integrating security principles and practices across all areas of our business We firmly believe in the importance of equipping our employees with the necessary knowledge, skills, and credentials to ensure a secure work environment Just as drivers must possess a license to operate a vehicle, we require our employees to undergo rigorous IT security training and obtain relevant credentials before they can perform their roles This approach emphasizes our dedication to maintaining the highest standards of cybersecurity and safeguards our sensitive data and systems By prioritizing comprehensive training and compliance, we aim to create a collective responsibility towards protecting our valuable assets and maintaining the trust of our stakeholders

Our commitment to cybersecurity extends beyond governance and permeates throughout the organization To ensure that all employees understand the importance of cybersecurity and are equipped to identify and address potential threats, we have implemented several internal policies to ensure that all employees have clear guidelines and best practices to follow, promoting a secure work environment and safeguarding our sensitive data and systems conducted information security/cybersecurity awareness training, and established a clear escalation process for reporting any suspicious activities By emphasizing the significance of cybersecurity at all levels, we strive to create a collective responsibility towards protecting our valuable assets and maintaining the trust of our stakeholders.

The aforementioned internal policies clearly define the responsibilities of employees regarding cybersecurity, as well as the disciplinary measures that apply in the event of non-compliance.

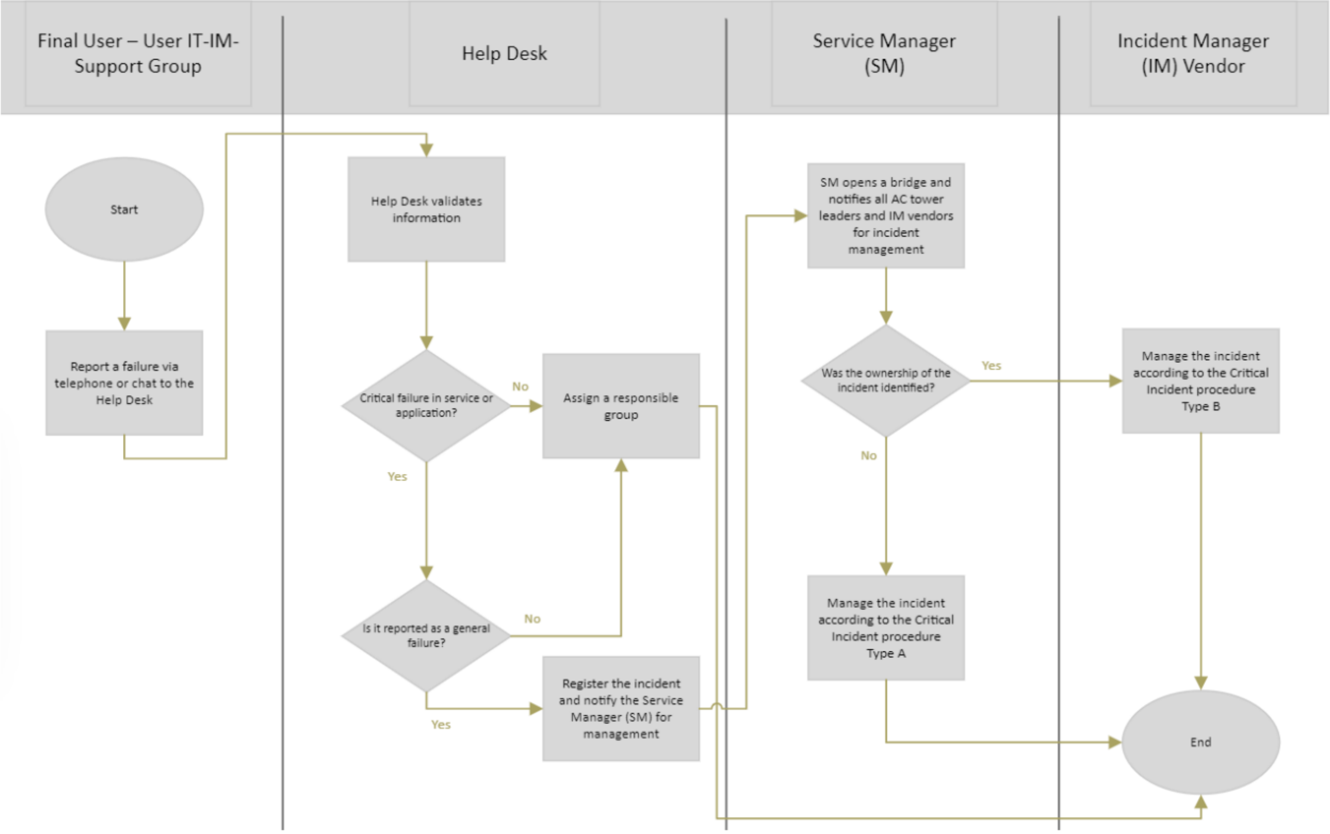
IT security training

Arca Continental is committed to enhancing the knowledge and skills of its employees in the realm of IT security We provide comprehensive training programs that equip them with the necessary tools and awareness to effectively mitigate risks and contribute to a secure operating environment In addition to annual training initiatives, we ensure that IT security training is reinforced during the onboarding process for new employees This ensures that from their very first days with the company, all individuals are equipped with the latest information and best practices to uphold our stringent security standards By consistently emphasizing the importance of IT security training, we foster a culture of vigilance and preparedness throughout our organization.

Cybersecurity awareness/training program	Program results
All users with access to IT resources must take an annual training course on topics related to good Information Security practices.	In the 2022 - 2023 cycle of training, there was more than 90% compliance.
All users who fall for a Phishing simulation must take an additional course related to the subject.	100% of the users who have fallen for the simulations take a training course.
AC Cybersecurity Week	Annual event. In 2023, there were conferences with various topics related to Information Security and Protection. In 2023, more than 8,000 employees participated

IT security risk process

At Arca Continental, we have implemented a well-defined escalation process that empowers employees to report any suspicious incidents or concerns they may encounter, ensuring prompt and effective response measures are taken to address potential cybersecurity threats.


Final User – User IT-IM-Support Group
Help Desk
Service Manager (SM)
Incident Manager (IM) Vendor
Start
Report a failure via telephone or chat to the Help Desk
Help Desk validates information
Critical failure in service or application?
No
Yes
Assign a responsible group
Is it reported as a general failure?
No
Yes
Register the incident and notify the Service Manager (SM) for management
SM opens a bridge and notifies all AC tower leaders and IM vendors for incident management
Was the ownership of the incident identified?
Yes
No
Manage the incident according to the Critical Incident procedure Type A
Manage the incident according to the Critical Incident procedure Type B
End

At Arca Continental, we make continuous efforts to mitigate risks associated with cybersecurity During 2023, we did not detected any security breaches Our philosophy revolves around proactively mitigating the risks involved in this realm, with the understanding that it requires daily diligence, as the risk always remains We remain committed to safeguarding our valuable assets through ongoing vigilance and proactive measures

Incident Response

We have a Disaster Recovery Plan (DRP) and we test it at least once per year. Additionally, we conduct anual Table Top exercises to assess our capacity to respond to disasters and cybersecurity incidents.

External Vulnerability Analysis

We conduct a monthly analysis of vulnerabilities, through an expert third party, and additionally we use BAS tools to continuously perform tests. We conduct at least 2 penetration tests per year (Black Box and White Box).