PUBLIC REPORT
2023 SUSTAINABILITY ACTIONS: CYBERSECURITY

Governance

Regarding cybersecurity management at Grupo México, the Audit and Corporate Practices Committee of the Board of Directors is responsible for overseeing the group's cybersecurity strategy. The Committee has appointed Director Fernando Ruiz to report cybersecurity performance to the Board of Directors. Progress in the cybersecurity plan of the three divisions is reviewed quarterly, while the implementation of the strategy and organizational priorities are reviewed semiannually.

At the executive level, the Chief Information Security Officer (CISO) is responsible for monitoring the implementation of the strategy and overseeing the group's cybersecurity action plans. Each of our divisions has Information Security Directors who report the implementation of the cybersecurity strategy and performance to the CISO on a quarterly basis.

Information Security Culture

At Grupo México, we have a General Policy of Information Security that standardizes expectations in this area with an institutional approach. Additionally, each of our divisions has its own information security policy, which has been published and disseminated internally to all personnel through their respective intranet portals and institutional email campaigns.

In all three divisions of the group, information security training is conducted via the Knowb4 platform for all employees, including training courses and virtual workshops. These workshops also cover the main risks employees may face and the processes they should follow in case of suspicious events. The platform also includes phishing tests conducted at least twice a year, and employees who fail the test are scheduled for additional training.

The training is mandatory and is part of the performance evaluation, with meticulous follow-up, and directors are informed accordingly.

In 2024, we will continue with the training plan based on the results of phishing tests, differentiating those with negative results to strengthen awareness.

All employees have access to procedures that describe the process they should follow if they identify any suspicious event. Each division of the group has institutional email accounts managed by the respective Information Security departments. These email accounts have been disseminated internally so that employees can report any suspicious event or request priority assistance.

If any person within the organization, due to carelessness or negligence, endangers information or access to systems, they will be sanctioned according to the severity of the infraction, up to and including dismissal if warranted.

Information Security Risk Management

Within the organization, we have Risk Management processes and committees that identify essential risks for the company, with cybersecurity established as one of the most important risks. This methodology is based on ISO 27000 and COBIT.

Additionally, once the risks are identified, our control framework is based on the Center for Internet Security (CIS), which includes 18 specific control topics and 153 subtopics that are internally monitored. Progress is presented to the Audit and Corporate Practices Committee every three months. Furthermore, an external review of the controls is conducted by a top-tier independent company, which prepares a report on the maturity of the cybersecurity function.

Seventy percent of our infrastructure is hosted in top-tier data centers with the required global certifications.

Business Continuity Management

We have a Disaster Recovery Plan (DRP) and business continuity plans for IT infrastructure in the operations of our three divisions in Mexico, Peru, and the United States, aimed at ensuring the continuity of our activities in the event of any incident.

In case of incidents, we have "Information Security Incident Management Procedures" based on the National Institute of Standards and Technology (NIST) cybersecurity framework and controlled through our CIS reference framework.

All three divisions have an external Security Operations Center (SOC) with top-tier companies supporting the monitoring of our servers, applications, and user devices to detect any incidents, providing the first response to them.

Our procedures cover all phases of the incident response process, including detection and analysis, containment and intelligence development, eradication and remediation, recovery, and post-incident activities. Evaluations include essential qualitative and quantitative factors to determine the relative importance of information security and cybersecurity incidents. We conduct response drills at least once a year, continuously updating our business continuity plan and Information Security Incident Management Procedure.

During 2022/2023, vulnerability assessments were conducted. Two of the divisions use the TENABLE system for continuous vulnerability analysis, while one division receives this service from the SOC company. Additionally, at least twice a year, external companies conduct penetration tests and simulated hacks on all our systems to verify that vulnerabilities have been addressed and to identify any new ones.

Cybersecurity Incidents

No significant cybersecurity incidents occurred in 2023 at Grupo México.

Indicators	2023
Number of Information Security Breaches	0
Number of Customers and Employees Affected by Security Breaches	0