Cybersecurity

For Industrias Peñoles, information is an invaluable asset that must be protected, and all employees share the responsibility to safeguard it. With this in mind, we created a Cybersecurity Office in 2019, which establishes a model of cybersecurity governance that, besides being based on the **three lines of defense**, involves every level of our business. In 2023, we continued to strengthen cybersecurity in all of our business processes, aligned with our business strategies and mindful of our responsibility, as a compliance area, to safeguard digital security as a second line of defense in all of our technological processes.

Our cybersecurity governance initiatives continue to strengthen regulatory capacities for respecting the various laws governing the company and protecting information and technological assets at all levels of the organization. These initiatives encompass the three types of technology we work with: information technology, operating technology, and specialized technology.

We manage a **Cybersecurity Architecture Review Board** a multidisciplinary work team with decision-making capacity that contributes perspectives and analysis on technology projects and ensures that we meet international standards and internal guidelines, thus avoiding new cyberthreats. Based on its recommendations, we ensure that all technology projects are deployed in a secure manner and that we maintain the necessary level of protection for the entire organization. We are constantly on the alert for cybersecurity threats around us, and we analyze, identify, and remediate failures effectively through vulnerability management. We work as a team and in partnership with our technology areas to establish best security practices and standards for the evolution and technological innovation our business processes.

The **Access Identity Management Committee** a multidisciplinary team of representatives from the IT Department, functional leadership, and cybersecurity office, is responsible for overseeing compliance with policies and standards related to access control identities (IAM) to reduce the risks inherent to identities and access.

In the interest of full compliance with the Federal Law for the Protection of Personal Data in Possession of Private Parties, our Personal Data Management System has completed the second phase of its **audit** by the firm NYCE, and we now have certification for our business units.

We are in continuous communication and collaboration with Grupo BAL companies to share experiences, address challenges, and foster cybersecurity and risk culture (*see case study*). This is strengthened at all levels of the organization through various workshops; for example, IT Security workshop, simulation exercises at operational and executive levels, postings on news, and alerts to keep our people aware of the different threat environments that currently exist.

Public policy

Peñoles is dedicated to the pursuit of the common good. We work together with governments and participate responsibly in dialogues on public policy initiatives. In our due diligence process, we seek to understand and manage the risks involved in our business partners' public exposure. Our Code of Ethics and Conduct makes clear our stance on relations with political parties: we prohibit any direct or indirect contribution by or on behalf of the organization to political parties or campaigns or to any individual, corporation, association, organization, union, or any other type of public or private entity involved in political activities in Mexico or abroad.

For more information on how we manage relations with authorities, see the section on **Alliance for the Common Good**.

Case study - Código Hacker

For the third year in a row, we attended the Código Hacker cybersecurity congress, where, together with other Grupo Bal companies, we discussed topics such as security and trust in the cloud, artificial intelligence, cyber hygiene and personal safety, cyber resilience, and cybersecurity in collaborative environments. We also participated in a cyber-attack simulation, in which all members involved in IT issues participated.

Case study - Cybersecurity is our responsibility

We are continually raising awareness of the need to remain alert as we receive and consult information in a variety of media. With the slogan "Cybersecurity is our responsibility," we developed the following recommendations for staying secure in the face of cyber-attacks:

- **Be more alert,** Cybercriminals use certain types of news to create fake pages and links containing malicious software.
- **Promptly report,** any email, call or message you consider to be suspicious or of dubious origin.
- **Use corporate devices** to access the organization's services.
- **Use authorized media** for sharing sensitive or confidential information.
- **Use secure passwords** and do not share them with anyone.
- **Use only official sites** to consult information on the Internet.