INFORMATION SECURITY

SASB FB-FR-230A.2, CG-MR-230A.1, CG-EC-230A.1

In 2023, the Technology team's priorities included:

- Modernizing technology and data systems to reduce technical debt.
- Strengthening our capabilities for business continuity and disaster recovery.

The Information Security strategy is based on the following ten pillars:

1. Cybersecurity: our focus is on protecting our entire technology ecosystem (hardware and software), every device, and our data.

2. Training and Awareness: we created an awareness program to help end users recognize potentially dangerous communications on our platforms. In addition, each of our associates is required to complete an annual information security training.

3. Data hijacking: we conducted a simulation of a ransomware attack to determine the strength and profile of our current tools, as well as our organization's response capability.

We had no ransomware attacks in 2023, thanks to our internal systems and layers of protection.

4. Security risk score: our enterprise information security capabilities are aligned with the National Institute of Standards and Technology (NIST). This allows us to identify risk and enables the ongoing protection of our technology assets and data.

5. Data Risks: data is one of our most important assets. Our information security experts are always working to detect potential risks and mitigate them.

6. Key security risks and incidents: we have a Security Operations Center that handles events that may occur within the Information Technology (IT) ecosystem. Our Incident Response team uses our processes to analyze and follow up on these incidents until they are solved.

7. User awareness program: we make sure that our suppliers and associates are aware of the potential threats in the digital ecosystem by running awareness and communication campaigns. This helps ensure that they don't misuse datain a way that might jeopardize the company, our associates, or our customers.

8. Vulnerability management: we are focused on preventing the persistence of security vulnerabilities that could be further capitalized on. Alerts areright away in order to prevent incidents.

9. Certificate management: our digital certificates make possible the secure transport for both internal and external applications.

10. Solution Security Plan (SSP) management: our review of security processes and architecture enables product owners to implement technology solutions that comply with privacy and information security controls