INFORMATION SECURITY

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

The information security program was created to provide our brand portfolio worldwide with comprehensive, profitable and risk-based security services

We guarantee protection for information and information systems against unauthorized access, use, dissemination, alteration, or destruction, thus providing confidentiality, safety, and availability. Our objective is to maintain company information safe through better understanding of this subject and guidelines by our associates and business partners.

We also ensure best practices are followed to identify risks, protect information, detect suspicious activities and to be prepared to respond to future incidents.

Our company has policies, standards, procedures and security for information, with the purpose of regulating and raising awareness among our associates and suppliers concerning the importance of the information and the technological resources used in the company. We also provide training for our associates so they may better understand the importance of adopting behaviors in line with our information security guidelines.

Security in every transaction

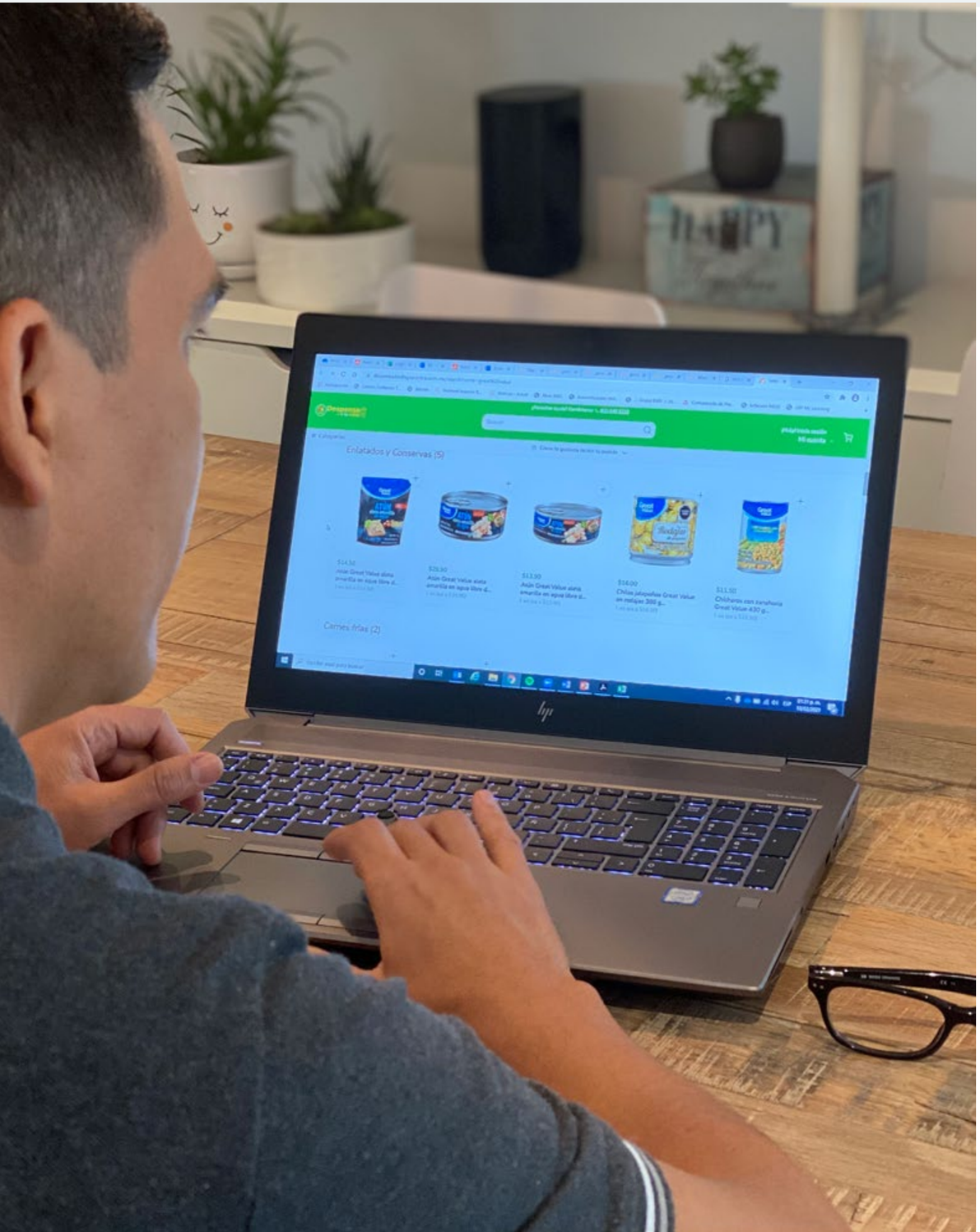
Vulnerabilities present in company information assets are identified and managed with the following elements in mind: vulnerability-analysis scheduling; results documenting; and results classifying, basing attention prioritization on the severity of the risk. Moreover, we provide the guidelines for designing vulnerability remediation plans; penetration-testing protocols for critical assets; and documentation of test results, requesting correction of opportunities detected.

Our Audit and Corporate Practices Committees are committed to the strategy of information security, thus making the review process a fundamental part of their activities. A review is conducted every four months of all mitigation initiatives, trends, risks, and strategies. Furthermore, each market where we operate has its own information security leader who is also part of the committee that reviews and defines the cybersecurity strategy.

Our ecosystem is complex, as we handle millions of transactions per second. Each year we receive upwards of 1.5 billion cyberattacks. Subsequently we have business continuity plans that allow us to establish controls to supply the tools and resources needed to perform our activities after any contingency jeopardizing operability by impacting the pillars of continuity: associates, facilities, systems, and third parties.

In 2020 we modernized our technological ecosystem and implemented safe and sustainable capabilities for the future. Our computer infrastructure and communications in stores, DCs and offices were improved. Similarly, we implemented proactive security monitoring and corrected access controls for key applications.

Insofar as fraud prevention, we doubled the number of audits as compared to 2019. Regarding security, requests for information on internal and outside reviews increased. In addition to the internal audit plan, compliance reviews took place for Sarbanes-Oxley, the Payment Card Industry and NIST Cybersecurity Framework..



DIGITAL CITIZENSHIP

Throughout 2020 we continued working on our new global area -Digital Citizenship. This area focuses on ensuring data management and technology based on our goal of being the most reliable omnichannel chain.

Digital Citizenship advises the company on matters related to privacy; the ethical use of data and governing the same; emerging technologies; cybersecurity; and record management. It is charged not only with the legality related to the use of data or technology in any specific manner, but also the effect of its use on our relationship of trust with our customers and stakeholders.