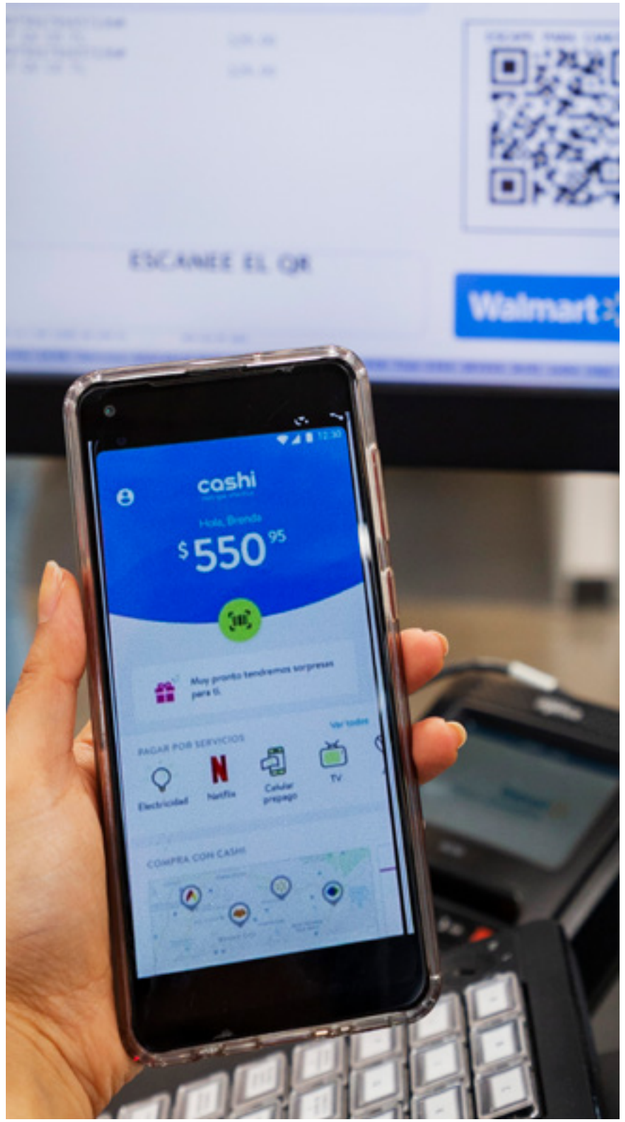
INFORMATION SECURITY

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

For us, information security in Mexico and Central America is as important as our business strategy

We know the scope involved in processing data from our customers, suppliers and associates. Our objective is to maintain information security by fully understanding information shared by our associates, business partners and relevant Tribe leads. To achieve this, we have information security policies, standards, procedures and guidelines that seek to regulate and raise awareness among associates and suppliers about the importance of safeguarding information and the use of technological resources used by our company. We also train our associates to make them aware of the importance of adopting behaviors aligned with our information security guidelines.



Thanks to our comprehensive, cost-effective and risk-based security services, we are able to provide a reliable and solid service. To do this, we ensure that information and information systems are protected against unauthorized access, use, disclosure, alteration, modification or destruction.

Our purpose is to provide greater confidentiality, integrity and availability for our customers every day

In addition, we ensure that we follow best practices to identify risks, detect suspicious activities and anticipate potential incidents. We also identify and manage vulnerabilities present in the company's information assets, considering elements such as: vulnerability analysis scheduling, results documentation and vulnerability classification, prioritizing their attention according the risk involved.

On the other hand, we provide guidelines for the design of vulnerability remediation plans, penetration testing protocols for critical assets and documentation of test results, requesting the correction of detected opportunities.

Information Security Governance

The Audit and Corporate Practices Committees are involved in the information security strategy. The Committees meet every three months to review initiatives, trends, risks and strategies with the aim of mitigating potential damage to the information handled by the company.

Additionally, in each market where we operate, we have an information security leader who is part of the Audit and Corporate Practices Committees. This allows us to define and review the best cybersecurity strategy for each specific case, according to its context and needs.

Our vast and complex ecosystem of products and services positions us as a global reference point. As we handle millions of transactions per second, we receive more than 1.5 billion cyber-attacks per year. Therefore, after a contingency that impacts our continuity pillars in matters related to associates, facilities, systems and third parties, we activate our plans and controls to ensure the continuity of the business and our activities.

RESULTS
During 2022 we achieved

88% reduction in vulnerabilities derived from system penetration testing compared to 2021. We also obtained the PCI Security Standards certification with no findings noted.

We improved our NIST CSF (National Institute of Standards and Technology Cyber Security Framework) maturity level from **3.83 to 4.0, the highest rating of this framework.**

In line with Infosec International, we are working to consolidate our response and prevention protocols to improve the way we react in the event of a ransomware attack.

In terms of security, there was an increase in the number of requests for information from internal and external reviews. We receive audits from both the Internal Audit team and external entities in the financial sector to demonstrate compliance in correspondent banking services, as well as with external auditors from NIST, Sarbanes & Oxley and PCI (Payment Card Industry).

P. 171