DIGITAL CITIZENSHIP AND INFORMATION SECURITY

Trust in the use of technology and data is critical, consistent with our values of service, excellence, integrity, and respect for the individual.

DIGITAL CITIZENSHIP

Our digital trust commitments provide a foundation for the company to earn and maintain customer trust in an omnichannel, data-driven, technology-driven world:

Service

Our use of technology and data will focus on serving people.

Excellence

We strive for excellence in our technology, making it intuitive, convenient and safe.

Integrity

We use data in a responsible, transparent, and conscious way.

Respect

Our data and technology practices treat people fairly, with dignity, and with a strong regard for their privacy.

We implement these commitments through four main areas:

Promoting fairness

- We shape decisions about the use of new technologies, services, and data under the leadership of our global Digital Citizenship team.

Protecting privacy

- We have policies and controls in place for the use and exchange of customer and associate information.

Managing data, records, and information

- We facilitate the use of data and technology through policies and procedures, associate training, and monitoring and evaluation.

Cybersecurity and information security

- We protect our information and digital infrastructure from cyber-attacks by adhering to international standards, implementing incident reporting policies, executing escalation procedures, and conducting vulnerability testing.

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

Information Security Governance

To guarantee ethical and secure information management, we concentrate on bolstering and solidifying our information management strategies. Our Audit and Corporate Practices Committees are involved in our information security strategy. The Committees meet on a quarterly basis to review initiatives, trends, risks and strategies to reduce potential damage to the information handled by the company.

Activities managed through our different Information security action plans are fundamental, as they drive a more secure operating ecosystem that protects the reliability of our applications and the data we handle, both from the company and our stakeholders.

Our ability to respond to risks or criticism resulting from external audits is supported by three pillars:

1. IT NETWORK ARCHITECTURE:

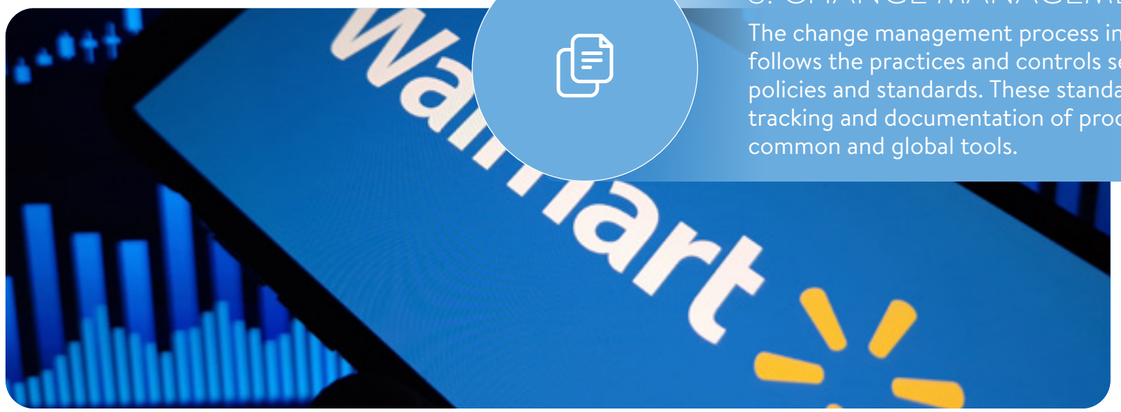
We put in place a network architecture that seeks to reduce the vulnerability of our stakeholders' sensitive data.

2. ACCESS MANAGEMENT:

We undertake regular user review reports on our applications to identify any room for improvement or potential risk.

3. CHANGE MANAGEMENT CONTROLS:

The change management process in Mexico and Central America follows the practices and controls set forth in our global technology policies and standards. These standards are applicable to requests, tracking and documentation of processes and changes within our common and global tools.



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.

During 2023 we achieved 20% reduction in vulnerabilities derived from system penetration testing compared to 2022.