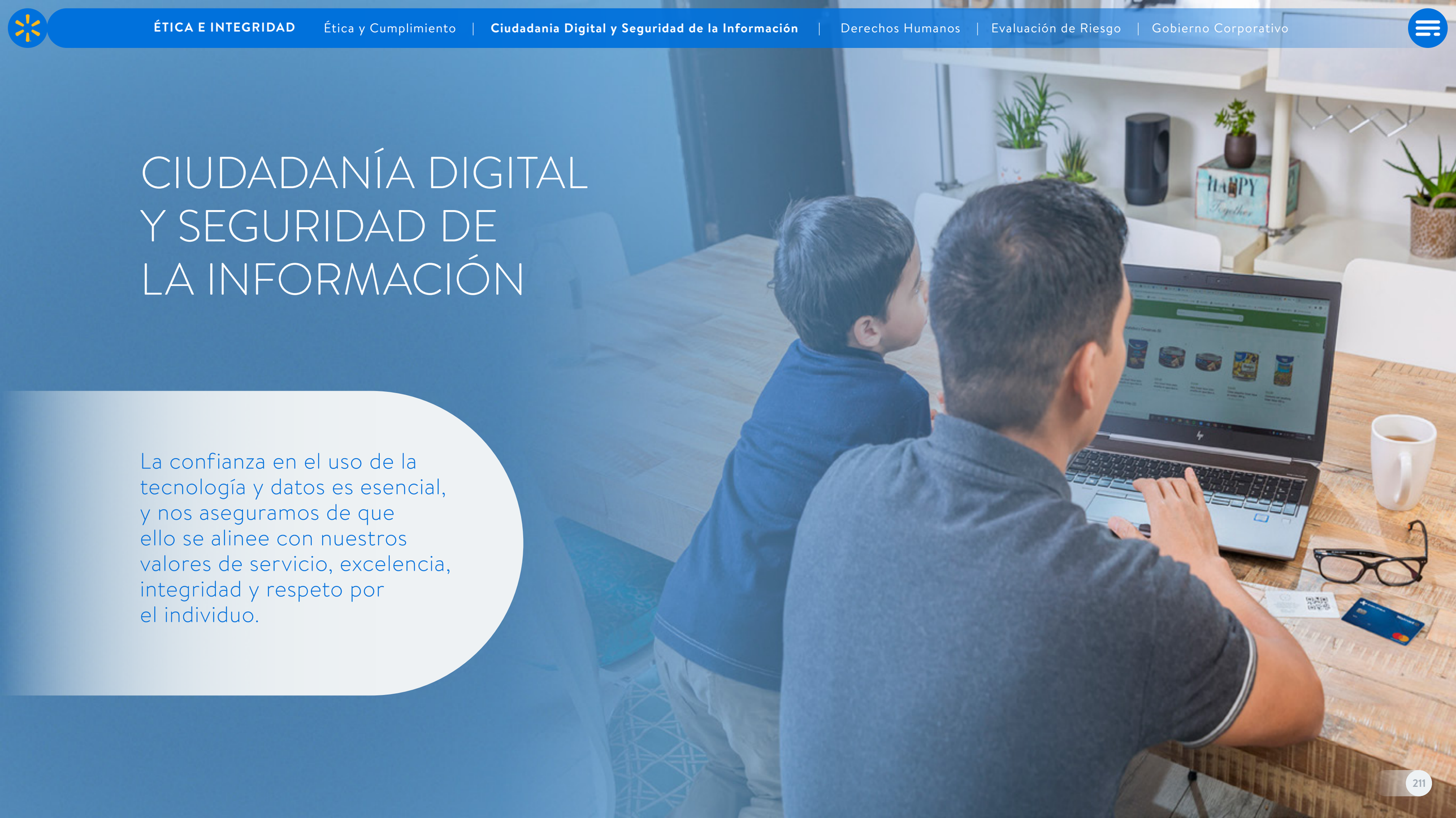
CIUDADANÍA DIGITAL Y SEGURIDAD DE LA INFORMACIÓN

La confianza en el uso de la tecnología y datos es esencial, y nos aseguramos de que ello se alinee con nuestros valores de servicio, excelencia, integridad y respeto por el individuo.



BUENOS CIUDADANOS DIGITALES

Nuestros compromisos de confianza digital proporcionan una base para que la compañía gane y mantenga la confianza del cliente en un mundo omnicanal, basado en datos y tecnología:

Servicio

Nuestro uso de la tecnología y los datos estará al servicio de las personas.

Excelencia

Nos esforzamos por alcanzar la excelencia en nuestra tecnología, haciéndola intuitiva, conveniente y segura.

Integridad

Usamos los datos de manera responsable, transparente y consciente.

Respeto

Nuestras prácticas de datos y tecnología tratan a las personas de manera justa, con dignidad y con estricto respeto a su privacidad.

Ponemos en práctica estos compromisos a través de cuatro áreas de enfoque:

Promoción de la imparcialidad

- A través de la guía del equipo global de Ciudadanía Digital, damos forma a las decisiones sobre el uso de las nuevas tecnologías, servicios y datos.

Protección de la privacidad

- Mantenemos políticas y controles con respecto al uso y el intercambio de información de clientes y asociados.

Gestión de datos, registros e información

- Apoyamos el uso de datos y tecnología, a través de políticas y procedimientos, capacitación de asociados, monitoreo y evaluación.

Ciberseguridad y seguridad de la información

- Protegemos nuestra información e infraestructura digital de ataques cibernéticos mediante el cumplimiento de estándares internacionales, políticas de reporteo de incidentes, prácticas de escalamiento y pruebas de vulnerabilidad.

SEGURIDAD DE LA INFORMACIÓN

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

En 2023, las prioridades del equipo de Tecnología se enfocaron en:

- Modernizar las plataformas tecnológicas y de datos para reducir la deuda técnica.
- Fortalecer nuestro perfil de continuidad del negocio y recuperación ante desastres.

La estrategia de Seguridad de la Información se basó en los siguientes diez pilares:

1. Ciberseguridad: nuestro enfoque se centra en proteger todo nuestro ecosistema tecnológico *(hardware y software)*, cada dispositivo y nuestros datos.

2. Ingeniería social: desarrollamos un programa de concientización para que los usuarios finales pudieran identificar posibles mensajes dañinos en nuestras plataformas. Además, cada uno de nuestros asociados debe completar una capacitación anual en seguridad de la información.

3. Secuestro de datos: realizamos un ejercicio para simular un ataque de *ransomware*, lo que nos permitió identificar la fortaleza y el perfil de nuestras herramientas actuales y la capacidad de respuesta organizacional.

Gracias a nuestras herramientas internas y capas de protección, en 2023 no sufrimos ningún ataque de *ransomware.*

4. Puntuación de riesgos de seguridad: nuestras capacidades de seguridad de la información empresarial están alineadas con el Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés). Esto nos ayuda a identificar nuestro riesgo y permite la protección continua de nuestros activos y datos tecnológicos.

5. Riesgos de datos: los datos representan uno de nuestros activos más importantes. Nuestros equipos de seguridad de la información trabajan constantemente en identificar potenciales riesgos e implementar medidas de mitigación.

6. Riesgos e incidentes de seguridad clave: contamos con el Centro de Operaciones de Seguridad, que recibe los eventos del ecosistema de Tecnologías de la Información (TI) que puedan suscitarse. A través de nuestros procesos, el equipo de Respuesta a Incidentes los analiza y les da seguimiento hasta su cierre.

7. Programa de sensibilización del usuario: mediante campañas de sensibilización y comunicación, nos aseguramos de que nuestros asociados y proveedores conozcan los riesgos que pueden existir en el ecosistema digital, para evitar que, como usuarios de información, realicen alguna acción inapropiada con la misma, que pueda poner en riesgo a la compañía, a nuestros asociados o clientes.

8. Gestión de vulnerabilidades: actualmente, el enfoque radica en evitar la persistencia de vulnerabilidades de seguridad que podrían ser explotadas. Cualquier alerta es escalada inmediatamente para evitar incidentes.

9. Gestión de certificados: nuestros certificados digitales permiten el transporte seguro para aplicaciones internas y orientadas al Internet.

10. Gestión del SSP *(Solution Security Plan)*: nuestra revisión de procesos de seguridad y arquitectura permite a los propietarios de productos implementar soluciones tecnológicas que cumplan con los controles de privacidad y seguridad de la información.

Gobernanza de seguridad de la información

Nos enfocamos en robustecer y fortalecer nuestros planes de gestión de la información, para garantizar el manejo ético y seguro de esta. Nuestros Comités de Auditoría y Prácticas Societarias están involucrados en la estrategia de seguridad de la información. Los Comités se reúnen cada tres meses para revisar iniciativas, tendencias, riesgos y estrategias con el fin de mitigar potenciales daños a la información manejada por la compañía.

Las actividades gestionadas a través de nuestros diversos planes de acción en Seguridad de la Información son fundamentales, ya que impulsan un ecosistema operativo más seguro que protege la confiabilidad de nuestras aplicaciones y los datos que manejamos, tanto de la compañía como de nuestros grupos de interés.

Contamos con tres pilares que nos ayudan a ofrecer soluciones a los riesgos o críticas derivadas de las auditorías externas:

1. ARQUITECTURA DE RED DE TI:

Implementamos una arquitectura de red que busca reducir la vulnerabilidad de los datos sensibles de nuestros grupos de interés.

2. GESTIÓN DE ACCESO:

Realizamos informes periódicos de revisión de los usuarios de nuestras aplicaciones para identificar áreas de oportunidad o riesgos potenciales.

3. CONTROLES DE GESTIÓN DEL CAMBIO:

El proceso de gestión de cambios en México y Centroamérica sigue las prácticas y controles establecidos por nuestras políticas y estándares tecnológicos globales. Estos estándares se aplican a nuestras solicitudes, seguimiento y documentación de procesos y cambios dentro de nuestras herramientas comunes y globales.

Somos un referente mundial al tener un ecosistema tan grande y complejo frente a nuestros productos y servicios. Al manejar millones de transacciones por segundo, recibimos más de 1,500 millones de ciberataques por año. Por tanto, después de una contingencia que impacta nuestros pilares de continuidad en asociados, instalaciones, sistemas y terceros, activamos nuestros planes y controles para asegurar la continuidad del negocio y de nuestras actividades.

Durante el 2023 logramos el 20% de reducción de vulnerabilidades derivadas de pruebas de penetración a sistemas en comparación con el 2022.