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.