SEGURIDAD DE LA INFORMACIÓN

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

Creamos el programa de seguridad de la información para proporcionar a nuestro portafolio de marcas por todo el mundo, servicios de seguridad exhaustivos, rentables y basados en riesgo

Nos aseguramos de proteger la información y sistemas de información contra su acceso, uso, divulgación, alteración, modificación o destrucción no autorizados, proporcionando así confidencialidad, integridad y disponibilidad. Nuestro objetivo es mantener la seguridad de la información de la compañía a través de la mejor comprensión de este tema y las directivas por parte de los asociados y socios de negocio.

Asimismo, nos aseguramos de seguir las mejores prácticas para la identificación de riesgos, protección de información, detección de actividades sospechosas, así como estar preparados para la respuesta a incidentes a futuro.

Disponemos de políticas, normas, procedimientos y guías de la seguridad de la información con el fin de regular y concientizar a los asociados y proveedores sobre la importancia de la información y los recursos tecnológicos que utilizamos en la compañía. También impartimos capacitación a nuestros asociados para sensibilizarlos sobre la importancia de adoptar conductas alineadas a nuestras directivas de seguridad de la información.

Seguridad en cada transacción

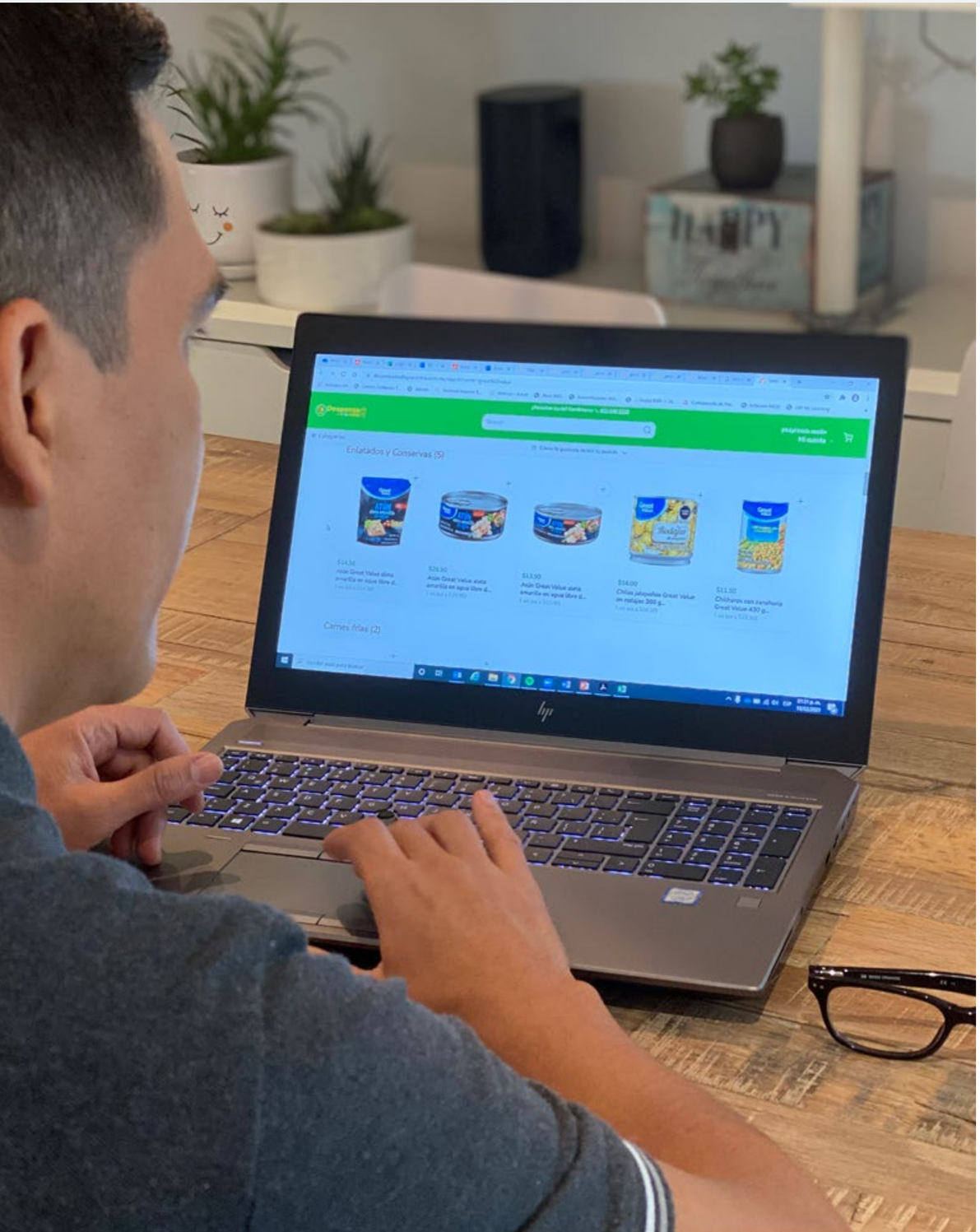
Identificamos y gestionamos vulnerabilidades presentes en los activos de información en la empresa, considerando elementos como: calendarización de análisis de vulnerabilidades, documentación de resultados y clasificación de vulnerabilidades basando su prioridad de atención en el riesgo que implican. Asimismo, proporcionamos los lineamientos para el diseño de planes de remediación de vulnerabilidades, los protocolos de pruebas de penetración para activos críticos y documentación de resultados de pruebas, solicitando la corrección de las oportunidades detectadas.

Nuestro Comité de Auditoría y Prácticas Societarias está comprometido con la estrategia de seguridad de la información, por lo que el proceso de revisión es parte fundamental de sus actividades. Cada cuatro meses se revisan iniciativas, tendencias, riesgos, y estrategias de mitigación. Adicionalmente, cada mercado en donde operamos cuenta con un líder de seguridad de la información que también es parte del comité que revisa y define la estrategia de ciberseguridad.

Nuestro ecosistema es complejo, ya que manejamos millones de transacciones por segundo. Cada año recibimos más de 1,500 millones de ciberataques. Es por ello que contamos con planes de continuidad del negocio que nos permiten establecer controles que brinden herramientas y recursos necesarios para ejecutar nuestras actividades después de una contingencia que comprometa la operatividad al impactar los pilares de la continuidad: asociados, instalaciones, sistemas y terceros.

En 2020 modernizamos nuestro ecosistema tecnológico e implementamos capacidades seguras y sostenibles para el futuro. Mejoramos la infraestructura de computación y comunicaciones en tiendas, centros de distribución y oficinas. De igual forma, implementamos un monitoreo proactivo de seguridad y corregimos controles de acceso para aplicaciones clave.

Con respecto a la prevención de fraudes, tuvimos el doble de auditorías que en 2019. En materia de seguridad, se incrementaron las solicitudes de información de revisiones internas y externas. Adicional al plan de auditoría interna, se atendieron revisiones de cumplimiento para *Sarbanes & Oxley, Payment Card Industry y NIST Cybersecurity Framework*.



CIUDADANÍA DIGITAL

En 2020 continuamos trabajando en nuestra nueva área global llamada Ciudadanía Digital. Esta área se centra en asegurar el manejo de datos y tecnología, basado en nuestro objetivo de ser la cadena omnicanal más confiable.

Ciudadanía Digital asesora a la compañía sobre cuestiones relacionadas con la privacidad, el uso ético de los datos y el gobierno de estos, las tecnologías emergentes, la ciberseguridad y la gestión de registros. Es responsable, no solo en materia legal sobre el uso de datos o tecnología de una manera particular, sino también sobre el efecto de su uso en nuestra relación de confianza con nuestros clientes y partes interesadas.