# Ciberseguridad

Para Industrias Peñoles, la información es un activo valioso que debe protegerse y todo el personal comparte la responsabilidad de salvaguardarla. Para asegurar lo anterior, desde 2019 se creó la Oficina de Ciberseguridad, la cual establece el modelo de gobierno de ciberseguridad que, además de estar basado en las **tres líneas de defensa**, involucra a todos los niveles del negocio. Durante 2023 continuamos actualizando y fortaleciendo la ciberseguridad en todos los procesos de negocio, alineados a la estrategia, al ser, como área de cumplimiento, responsables de salvaguardar la seguridad digital como segunda línea de defensa en todos nuestros procesos tecnológicos.

Las iniciativas de gobierno de ciberseguridad continúan fortaleciendo las capacidades normativas para dar cumplimiento a las diferentes regulaciones a que está sujeta la organización y proteger la información y los activos tecnológicos en todos los niveles de la organización. De manera transversal, trabajamos con tres tipos de tecnologías: tecnologías de información (TI), tecnologías de operación (TO) y tecnologías especializadas (TE).

Gestionamos una **Mesa de Revisión de Arquitectura de Ciberseguridad** (MRA-C) integrada por un equipo de trabajo multidisciplinario con capacidad para tomar decisiones en la materia, que aporta sus diferentes puntos de vista en el análisis de los proyectos de tecnología y asegura que se cumplan los estándares internacionales y lineamientos internos, evitando así nuevas amenazas cibernéticas. A partir de sus recomendaciones, se verifica que cualquier proyecto de tecnología sea desplegado de manera segura, garantizando que la organización se mantenga en el nivel esperado de protección. Mantenemos una vigilancia continua de la ciberseguridad mediante un monitoreo constante de amenazas en el entorno, con el propósito de analizar, identificar y remediar fallas de manera eficaz a partir de nuestra gestión de vulnerabilidades. Trabajamos en equipo y colaboramos con nuestras áreas de tecnología para definir y establecer las mejores prácticas y estándares de seguridad para la evolución y la innovación tecnológica con la que operan los procesos de negocio.

De igual manera, contamos con un **Comité de Gestión de Identidad de Accesos** –equipo multidisciplinario conformado por la Subdirección de TI, líderes funcionales y la oficina de ciberseguridad– encargado de vigilar el cumplimiento de políticas y estándares relacionados con identidades de control de acceso (IAM) para reducir los riesgos inherentes a identidades y accesos.

Por otra parte, establecimos bases sólidas para el debido cumplimiento de la Ley Federal de Protección de Datos Personales en Posesión de Particulares (LFPDPPP). Llevamos a cabo la segunda fase de **auditoría** de nuestro Sistema de Gestión de Datos Personales con el despacho NYCE, con lo cual hoy contamos con la certificación en nuestras unidades de negocio.

Mantenemos comunicación y participación continuas con las empresas de Grupo BAL para compartir experiencias, resolver retos e incrementar la cultura de ciberseguridad y riesgos (*ver caso de estudio*) y la fortalecemos constantemente en todos los niveles de la organización mediante diferentes talleres. Ejemplos de lo anterior fueron el taller Seguridad Informática, ejercicios de simulación a niveles operativos y ejecutivos, publicaciones de noticias y alertas que nos permiten estar atentos a los diferentes entornos de amenazas que existen actualmente.

## Políticas públicas

En Peñoles buscamos el bien común, por lo cual colaboramos con los gobiernos y participamos responsablemente en el diálogo de las iniciativas de política pública. En nuestras debidas diligencias buscamos entender y gestionar los riesgos por exposición política de nuestros terceros. Además, nuestro Código de Ética y Conducta subraya nuestra postura ante las relaciones con partidos políticos de evitar que se realicen, en nombre de la organización, directa o indirectamente, aportaciones o donativos a partidos políticos, campañas electorales o a cualquier persona física o moral, asociación, organismo, sindicato o a cualquier otro tipo de entidad pública o privada, relacionados con actividades políticas, ya sea en México o en el extranjero.

Para más información sobre nuestra gestión de relaciones con autoridades, visita la sección **Alianza por el Bien Común**.

## Caso de estudio - Código Hacker

Por tercer año consecutivo participamos en el congreso de ciberseguridad Código Hacker, evento donde, en conjunto con más empresas de Grupo Bal, se abordaron temas como “Seguridad y confianza en la nube”, “Inteligencia artificial”, “Ciberhigiene y seguridad personal”, “Ciberresiliencia”, “Ciberseguridad en entornos colaborativos”; también participamos en un simulacro de ciberataque, en el que participaron todos los miembros relacionados con el tema de TI.

## Caso de estudio – “La ciberseguridad es nuestra responsabilidad”

Constantemente creamos conciencia sobre la necesidad de mantenernos alertas en los diferentes medios por los que recibimos y consultamos información, con el lema “La ciberseguridad es nuestra responsabilidad”, atentos a las siguientes recomendaciones para mantener la seguridad ante eventos de ciberataques:

- **Incrementa tu alerta,** los cibercriminales utilizan este tipo de noticias para crear páginas y ligas falsas que contienen softwares maliciosos.
- **Reporta oportunamente** cualquier correo electrónico, llamada o mensaje que se identifique como sospechoso o de dudosa procedencia.
- **Haz uso de los equipos corporativos** para acceder a los servicios de la organización.
- **Utiliza los medios autorizados** para compartir información sensible o confidencial.
- **Utiliza contraseñas seguras** y no las compartas con nadie.
- **Utiliza únicamente sitios oficiales** para consultar información en internet.