

axtel

**Tecnología
que conecta
tu vida**

alestra*

axnet | AXTEL
NETWORKS

**Postura Pública
de Seguridad de
Información**

Criterios de Seguridad de la Información

Somos una empresa mexicana con casi 30 años de experiencia en Tecnologías de Información y Comunicaciones en México. En Axtel contamos con un amplio portafolio de servicios y soluciones de seguridad de información, basado en las mejores prácticas actuales de la especialidad en el mercado.

La Dirección General de Axtel está comprometida con el fomento y mejora continua de su Sistema de Gestión de Seguridad de Información, el cual se considera como uno de los mejores mecanismos para proteger la información de la organización, es por eso, que ha establecido una gobernabilidad de seguridad con roles y responsabilidades claros, encabezada por el Comité de Seguridad de la Información (CSI).

Nuestro Sistema de Gestión de Seguridad de Información está gobernado por una Política y Objetivos alineados a la estrategia del negocio, y para cumplir con estos se establece un Programa de trabajo el cual permite garantizar la seguridad del personal, la información, las instalaciones, así como el medio ambiente.

El Programa de Seguridad de Información coordina una serie de esfuerzos alineados al negocio capaz de gestionar internamente la seguridad, incorporando a la estrategia del negocio las mejores prácticas de seguridad, para asegurar la continuidad de nuestros servicios y procesos, administrando los riesgos de nuestros servicios, fomentando en nuestros colaboradores la cultura de protección de la información propia y de terceros. Esto nos ha permitido ofrecer servicios que exceden los estándares, contando con controles de seguridad desde su diseño y en todo el ciclo de vida de los servicios.

Comité de Seguridad de Información

El Comité de Seguridad de Información (CSI) es el órgano que rige el Gobierno de Seguridad. Está conformado por un Comité Ejecutivo dentro del cual están involucradas las principales áreas de la cadena de valor, así como, en caso de requerirse algunas otras áreas bajo demanda.

Entre algunas de las responsabilidades del CSI se encuentran el asegurar el apego a la normativa y a las estrategias de Seguridad de Información, proveer el conocimiento del Negocio para proteger la Confidencialidad, Integridad y Disponibilidad de la Información crítica de la empresa, asegurar que sus equipos de trabajo se encuentren concientizados acerca de las amenazas de Seguridad de Información, administrar de forma consciente los riesgos, acordar estrategias, así como asegurar el cumplimiento legal y regulatorio aplicable a Axtel.

Nuestro personal

En Axtel nuestro personal está capacitado y cuenta con certificaciones avaladas por organismos internacionales para atender las necesidades de nuestros clientes.

Adicional, concientizamos a nuestro personal de manera continua en diversos temas de Seguridad de Información, tomando en cuenta su rol y funciones dentro de la empresa.

Contamos con controles de seguridad asociados al ciclo de vida del colaborador. Todos nuestros colaboradores se apegan al Código de Ética, Reglamento de Conflicto de intereses y Confidencialidad.

Privacidad

Axtel respeta el derecho a la privacidad y protege los datos personales de nuestros colaboradores, clientes y proveedores, de los que funge como encargado, incluyendo los datos personales sensibles; por tanto, su información se encuentra debidamente protegida tomando medidas de seguridad administrativas, técnicas y físicas, previniendo posibles daños, pérdidas, alteración o acceso no autorizado, cumpliendo así con el marco normativo y legal aplicable.

Certificaciones de Axtel

En Axtel estamos en constante actualización en normas y mejores prácticas de Seguridad de Información, por ello hemos logrado obtener y mantener certificaciones reconocidas a nivel internacional, mantenemos el apego a las mejores prácticas, y preservamos la seguridad de nuestros activos.

A continuación, algunas de las certificaciones obtenidas y mejores prácticas:

ISO 27001

Norma internacional que permite el aseguramiento de la confidencialidad, integridad y disponibilidad de la información.

ISO 31000

Norma internacional que ofrece las directrices y principios para gestionar el riesgo de las organizaciones.

ISO 22301

Norma internacional que permite el aseguramiento de la Continuidad de Negocio en caso de presentarse un evento disruptivo.

FIRST

Foro internacional que facilita la respuesta a incidentes, así como la interacción entre Equipos de Respuesta a Incidentes.

PCI DSS

Normas de seguridad que incluyen un conjunto de requerimientos para proteger los datos de tarjeta habiente.

SSAE 18

Norma que permite atestar el diseño y efectividad de los controles generales de seguridad, TI y OT.

Mejores Prácticas

NIST

Estándares y mejores prácticas para administrar los riesgos relacionados a ciberseguridad.

ITIL

Mejores prácticas para la gestión de servicios de tecnologías de la información, desarrollo de tecnologías y sus operaciones.

COSO

Mejores prácticas acerca de los procesos y aplicaciones de TI que soportan los estados financieros de la organización.

Otras Certificaciones

ISO 9001

Norma internacional orientada a la gestión y mejora de la calidad de los procesos, productos y servicios,

ISO 20000

Norma internacional orientada a la gestión de servicios TI y define un conjunto de procesos para ofrecer un servicio efectivo.

Procesos y Controles de Seguridad de Información

En Axtel una de nuestras principales preocupaciones es nuestra seguridad y la de nuestros clientes, por ello con el objetivo de mantener los controles y asegurar la Confidencialidad, Integridad y Disponibilidad de la información, contamos con los siguientes procesos:

Administración de riesgos

Se lleva a cabo con el objetivo de identificar, administrar y tomar decisiones basadas en riesgos y oportunidades potenciales que apoyen a los objetivos de Axtel. Una vez identificados los riesgos son gestionados conforme al Plan de Tratamiento de Riesgos. Buscando siempre la mejora en nuestros servicios, nos encontramos alineados a las mejores prácticas en riesgos y certificados en ISO 31000.



Seguridad física y ambiental

Contamos con controles de seguridad física y ambiental dentro de nuestras instalaciones donde se procesa la información



Gestión de incidentes



En Axtel gestionamos los incidentes para prevenir, responder y/o restaurar lo más pronto posible cualquier interrupción de los servicios y/o procesos, buscando atender los incidentes de forma rápida y efectiva. Contamos con un Equipo de Respuesta a Incidentes el cual se apega a mejores prácticas internacionales de organismos como FIRST, NIST y ENISA para dar seguimiento y solución a incidentes de seguridad desde la etapa de detección hasta la resolución, documentación y cierre.

Administración de vulnerabilidades

La administración de vulnerabilidades nos permite identificar, evaluar, remediar y verificar que las diferentes vulnerabilidades de nuestros sistemas de información hayan sido mitigadas de forma oportuna.



Auditorías y revisiones

Se llevan a cabo auditorías en las que se revisa el cumplimiento de los controles de seguridad para garantizar su efectividad. Dichas auditorías se llevan a cabo tanto de manera interna, asegurando el cumplimiento de nuestros controles y, en consecuencia, auditorías externas, obteniendo nuevos certificados y manteniendo los actuales.



Así mismo, el equipo de Seguridad realiza Pruebas de Penetración (Pentest) hacia nuestros sistemas de información con el objetivo de identificar vulnerabilidades que un atacante pudiera explotar con la finalidad de implementar medidas evitando que nuestros activos se vean comprometidos.

Capacitación y concientización

Uno de los principales factores de riesgo en una empresa es el error humano, debido a esto, en Axtel nos preocupamos por mantener comportamientos que fortalezcan una Cultura de Higiene Digital, por lo que contamos con análisis de comportamiento de los colaboradores. Adicional, buscamos mantenernos actualizados constantemente en temas de seguridad, mediante un Programa de Capacitación y Concientización que busca dar a conocer temas de interés y concientizar sobre las amenazas, para ofrecer servicios confiables y seguros al cliente.



Continuidad de Negocio y Resiliencia

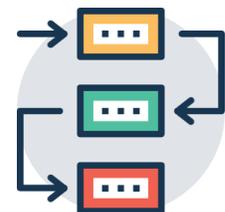
Para Axtel la Continuidad de Negocio es prioridad, pues entendemos la importancia y el impacto de nuestros servicios hacia los clientes y la comunidad, por ello que nuestro Comité de Seguridad de Información sesiona periódicamente, incluyendo en su agenda los temas de Continuidad de Negocio y Resiliencia, así como los indicadores clave para adecuar estrategias que permitan tomar decisiones oportunas para estar preparados ante eventos disruptivos. Asimismo, considera un modelo robusto de gobernabilidad en cada unidad de negocio que se encarga de gestionar la Continuidad a través de diferentes evaluaciones, programas de trabajo, simulacros y pruebas periódicas e indicadores de efectividad.



Nuestra resiliencia nos permite anticiparnos y estar preparados ante eventos de cualquier tipo (desastres naturales, salud, fallas tecnológicas, etc.) que puedan poner en riesgo a nuestro personal y nuestras operaciones. Buscando siempre la mejora en nuestros servicios, estamos alineados a las mejores prácticas y gracias a esto hemos logrado certificar nuestro Sistema de Gestión de Continuidad de Negocio en ISO 22301.

Control de cambios

Contamos con un adecuado control de cambios en los sistemas de información lo que nos permite llevar a cabo una trazabilidad de las actividades que se realizan, así como asegurar la integridad de la información.



Gestión de parches

Tenemos una estrategia adecuada para la gestión de parches, llevando a cabo el ciclo de vida desde la identificación de los activos hasta la validación y despliegue. Nos mantenemos actualizados para proteger nuestros activos de información de riesgos potenciales.



Identidades y accesos

Identidades y accesos tiene como objetivo registrar y administrar los accesos lógicos de los usuarios, así como sus permisos a los sistemas de información de Axtel, asegurando que los privilegios de acceso se otorguen de acuerdo con las políticas establecidas en la empresa.



Leyes y regulaciones

En Axtel identificamos y damos cumplimiento a las leyes y regulaciones aplicables como empresa, por ejemplo, la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, Ley Federal de Telecomunicaciones y Radiodifusión, Ley Federal de Protección a la Propiedad Industrial y Ley Federal de Derechos de Autor, así como también las leyes y regulaciones aplicables como proveedor de servicios, incluyendo las relacionadas con la Comisión Nacional Bancaria y de Valores (CNBV), Comisión Federal de la Protección contra Registros Sanitarios (COFEPRIS), la Agencia Federal de Aviación Civil (AFAC) y reglas internacionales como el General Data Protection Regulation (GDPR), entre otras.



Arquitecturas de seguridad

Diseña la estructura de los controles de seguridad de información que tiene que haber ante cambios o introducción en la infraestructura de nuestros servicios.



Centro de Operaciones de Ciberdefensa

El Centro de Operaciones de Ciberdefensa es el encargado de monitorear la infraestructura de nuestros clientes y salvaguardar los activos de información. Dentro de nuestro CDC se diseñan, desarrollan e implementan controles de seguridad para mitigar los riesgos en los activos, con atención

especializada de expertos en seguridad 24x7, lo cual nos permite priorizar riesgos, detectar, analizar y responder de manera más rápida para atender requerimientos y controlar incidentes de ciberseguridad, previo a que puedan causar un daño significativo.

Gracias al CDC nuestros clientes pueden enfocar sus esfuerzos en el core de su empresa, con la tranquilidad de que sus activos se encuentran protegidos y en constante actualización, bajo las normas y mejores prácticas internacionales de Seguridad de Información.

Colaboración

Colaboramos con diversas autoridades, organizaciones y partes interesadas como las siguientes:



Línea de Negocio Ciberseguridad
Dirección de Seguridad de Información