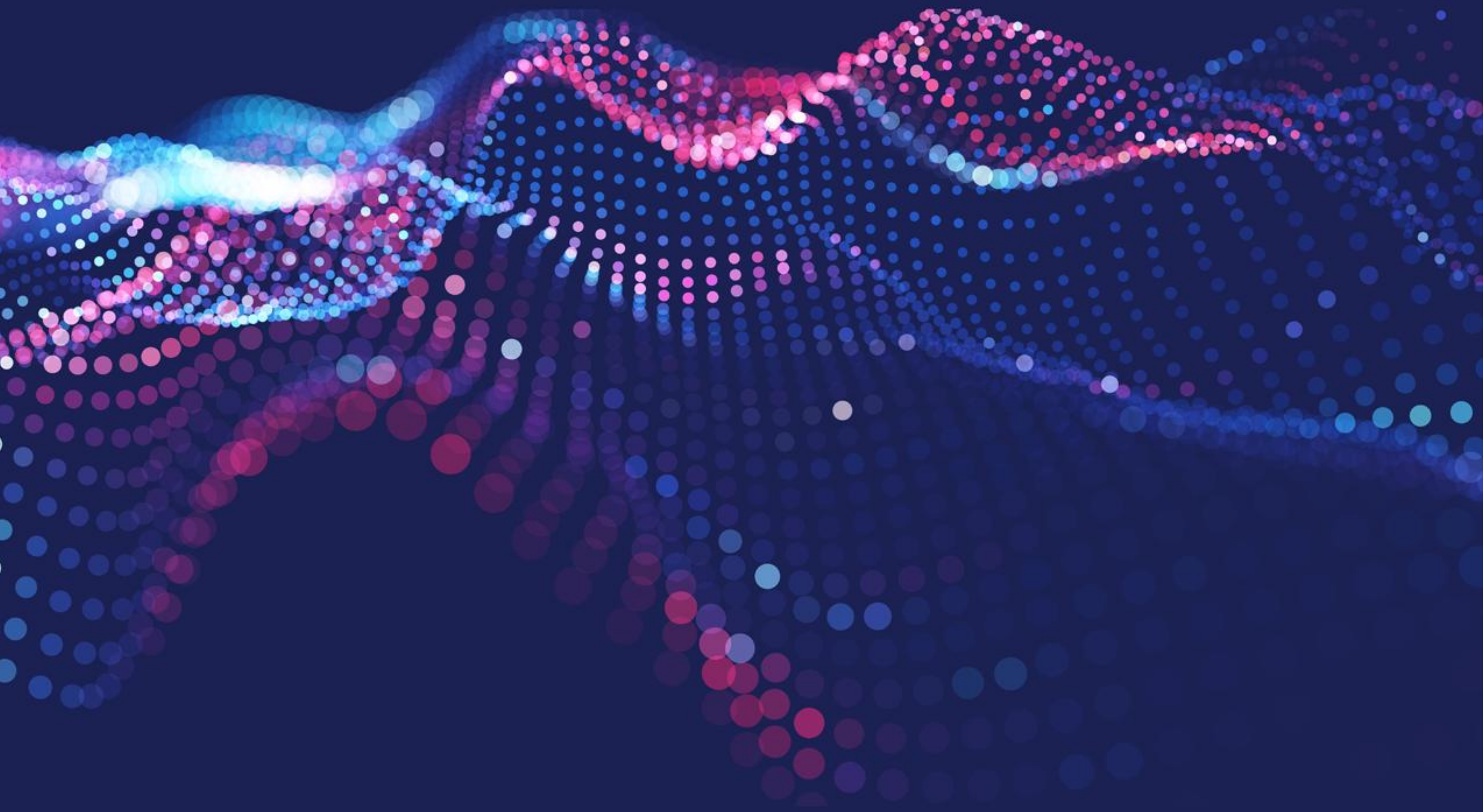
axtel

alestra

axnet | AXTEL NETWORKS

Tecnología
que conecta
tu vida



Public Position on Information Security

Information Security Criteria

We are a Mexican company with nearly 30 years of experience in Information and Communications Technology in Mexico. At Axtel, we offer a wide range of information security services and solutions based on current best practices in the market.

Axtel's senior management is committed to promoting and continuously improving its Information Security Management System, which is considered one of the best mechanisms for protecting the organization's information. That is why it has established security governance with clear roles and responsibilities, led by the Information Security Committee (ISC).

Our Information Security Management System is governed by a Policy and Objectives aligned with the business strategy, and to comply with these, a Work Program is established which guarantees the security of personnel, information, facilities, and the environment.

The Information Security Program coordinates a series of business-aligned efforts capable of managing security internally, incorporating best security practices into the business strategy to ensure the continuity of our services and processes, managing the risks of our services, and fostering a culture of protecting our own and third-party information among our employees. This has allowed us to offer services that exceed standards, with security controls in place from design through the entire service lifecycle.

Information Security Committee

The Information Security Committee (ISC) is the body that governs Security Management. It is made up of an Executive Committee involving the main areas of the value chain, as well as other areas on demand, if required.

Some of the CSI's responsibilities include ensuring compliance with Information Security regulations and strategies, providing business knowledge to protect the confidentiality, integrity, and availability of the company's critical information, ensuring that its work teams are aware of information security threats, consciously managing risks, agreeing on strategies, and ensuring legal and regulatory compliance applicable to Axtel.

Our Staff

At Axtel, our staff is trained and certified by international organizations to meet the needs of our customers.

In addition, we continuously educate our staff on various information security issues, considering their role and functions within the company.

We have security controls associated with the employee life cycle. All our employees adhere to the Code of Ethics, Conflict of Interest Policy, and Confidentiality Policy.

Privacy

Axtel respects the right to privacy and protects the personal data of our employees, customers, and suppliers, for whom it acts as data controller, including sensitive personal data. Therefore, your information is duly protected by administrative, technical, and physical security measures, preventing possible damage, loss, alteration, or unauthorized access, thus complying with the applicable regulatory and legal framework.

Axtel Certifications

At Axtel, we are constantly updating our information security standards and best practices. As a result, we have obtained and maintained internationally recognized certifications, adhere to best practices, and preserve the security of our assets.

Below are some of the certifications we have obtained and best practices we follow:

ISO 27001

International standard that enables the assurance of confidentiality, integrity, and availability of information.

ISO 31000

International standard that provides guidelines and principles for managing risk in organizations.

ISO 22301

International standard that enables business continuity to be ensured in the event of a disruptive event.

FIRST

International forum that facilitates incident response and interaction between Incident Response Teams.

PCI DSS

Security standards that include a set of requirements to protect cardholder data.

SSAE 18

Standard that allows for the certification of the design and effectiveness of general security, IT, and OT controls.

Best practices

NIST

Standards and best practices for managing cybersecurity risks.

ITIL

Best practices for managing information technology services, technology development, and operations.

COSO

Best practices for IT processes and applications that support the organization's financial statements.

Other certifications

ISO 9001

International standard aimed at managing and improving the quality of processes, products, and services.

ISO 20000

International standard focused on IT service management that defines a set of processes for delivering effective service.

Information Security Processes

At Axtel, one of our main concerns is our security and that of our customers. Therefore, to maintain control and ensure confidentiality, integrity, and availability of information, we have the following processes in place:

Risk management

It is carried out with the aim of identifying, managing, and making decisions based on potential risks and opportunities that support Axtel's objectives. Once identified, risks are managed in accordance with the Risk Treatment Plan. Always seeking to improve our services, we are aligned with best practices in risk management and certified in ISO 31000.

Physical and environmental security

We have physical and environmental security controls in place at our facilities where information is processed.

Incident Management

At Axtel, we manage incidents to prevent, respond to, and/or restore any interruption of services and/or processes as quickly as possible, seeking to address incidents quickly and effectively. We have an Incident Response Team that adheres to international best practices from organizations such as FIRST, NIST, and ENISA to track and resolve security incidents from detection to resolution, documentation, and closure.

Vulnerability Management

Vulnerability management allows us to identify, assess, remedy, and verify that the various vulnerabilities in our information systems have been mitigated in a timely manner.

Audits and reviews

Audits are carried out to review compliance with security controls and ensure their effectiveness. These audits are carried out both internally, ensuring compliance with our controls, and externally, obtaining new certificates and maintaining existing ones. Likewise, the Security team performs Penetration Tests (Pentests) on our information systems with the aim of identifying vulnerabilities that an attacker could exploit to implement measures to prevent our assets from being compromised.

Training and awareness

One of the main risk factors in a company is human error. Because of this, at Axtel we are committed to maintaining behaviors that strengthen a culture of digital hygiene, which is why we conduct employee behavior analyses. In addition, we strive to stay constantly up to date on security issues through a Training and Awareness Program that seeks to raise awareness of topics of interest and threats to offer reliable and secure services to our customers.

Business Continuity and Resilience

Business continuity is a priority for Axtel, as we understand the importance and impact of our services on our customers and the community. That is why our Information Security Committee meets regularly, including business continuity and resilience issues on its agenda, as well as key indicators for adapting strategies that enable timely decisions to be made in order to be prepared for disruptive events. It also considers a robust governance model in each business unit that is responsible for managing continuity through various assessments, work programs, drills, periodic tests, and effectiveness indicators.

Our resilience allows us to anticipate and be prepared for events of any kind (natural disasters, health, technological failures, etc.) that could put our personnel and operations at risk. Always seeking to improve our services, we are aligned with best practices and, as a result, we have achieved ISO 22301 certification for our Business Continuity Management System.

Change Control

We have adequate change control in our information systems, which allows us to track activities and ensure the integrity of information.

Patch management

We have an adequate patch management strategy, carrying out the entire life cycle from asset identification to validation and deployment. We are staying up to date to protect our information assets from potential risks.

Identities and access

Identities and access aim to record and manage users' logical access, as well as their permissions to Axtel's information systems, ensuring that access privileges are granted in accordance with the policies established by the company.

Laws and regulations

At Axtel, we identify and comply with applicable laws and regulations as a company, such as the Federal Law on Protection of Personal Data Held by Private Parties, the Federal Telecommunications and Broadcasting Law, the Federal Law on Protection of Industrial Property, and the Federal Copyright Law, as well as applicable laws and regulations as a service provider, including those related to the National Banking and Securities Commission (CNBV), the Federal Commission for the Protection against Sanitary Risks (COFEPRIS), the Federal Civil Aviation Agency (AFAC), and international rules such as the General Data Protection Regulation (GDPR), among others.

Security architecture

Design the structure of information security controls that must be in place before changes or additions are made to our service infrastructure.

Cyber Defense Operations Center

The Cyber Defense Operations Center is responsible for monitoring our clients' infrastructure and safeguarding information assets. Within our CDC, security controls are designed, developed, and implemented to mitigate risks to assets, with specialized attention from security experts 24/7, allowing us to prioritize risks, analyze, and respond more quickly to address requirements and control cybersecurity incidents before they can cause significant damage.

Thanks to our CDC, our clients can focus their efforts on their core business, with the peace of mind that their assets are protected and constantly updated, in accordance with international information security standards and best practices.

Collaboration

We collaborate with various authorities, organizations, and stakeholders, including the following:

UNAM CERT

POLICÍA FEDERAL

FGR

CNBV
COMISION NACIONAL BANCARIA Y DE VALORES

IMPI
INSTITUTO MEXICANO DE LA PROPIEDAD INDUSTRIAL

ift
INSTITUTO FEDERAL DE TELECOMUNICACIONES

FIRST
Improving Security Together

Cybersecurity Business Line
Information Security Department