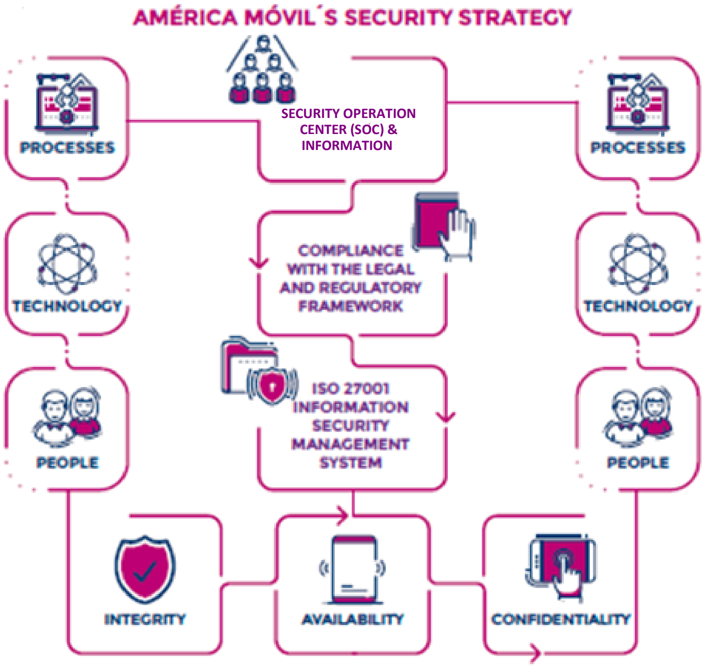
Information Security Strategy

The Technological evolution such as: IAAS (Infrastructure As A Service), IoT solutions and 5G, along with the expansion of digitization in all aspects of our daily lives has made cybersecurity a major concern for organizations, governments, and people in general. Cyberattacks and theft of sensitive information, as well as new and increasingly sophisticated types of cybercrime are relevant risks in all organizations worldwide that could lead to reputational damage in addition to financial impacts for both, companies, and their clients.

At América Móvil we offer cybersecurity connectivity solutions that not only make people feel safe when they use them, but also contribute to the overall information security of the communities where we operate.

América Móvil has an integrated security strategy that includes cybersecurity as well as data and communications privacy based on three main pillars:

- Integrity: Personal information must remain complete and accurate, for which we have established appropriate measures.
- Availability: Information must be available to its owners or authorized users at the precise moment they need it.
- Confidentiality: Personal data will be used exclusively by authorized personnel who have the necessary justification to use it.


AMÉRICA MÓVIL´S SECURITY STRATEGY
PROCESSES
SECURITY OPERATION CENTER (SOC) & INFORMATION
PROCESSES
TECHNOLOGY
COMPLIANCE WITH THE LEGAL AND REGULATORY FRAMEWORK
TECHNOLOGY
PEOPLE
ISO 27001 INFORMATION SECURITY MANAGEMENT SYSTEM
PEOPLE
INTEGRITY
AVAILABILITY
CONFIDENTIALITY

Through our Information Security Strategy, we manage and safeguard financial and confidential information efficiently, while minimizing risks of illegal or unauthorized access. We have developed policies and procedures supervised by the Information Security Officers and the Information Security Committees, both at the Corporate and subsidiary level, along with a Global Security Operations Center (SOC) managed by Scitum, a subsidiary of Telmex, that includes a cyber-intelligence team to identify threats.

The SOC fulfills the dual function of securing all our operations to provide confidence to customers about our services and solutions, in addition to delivering cybersecurity products and advisory services to our corporate clients to help them stay one step ahead of these challenges.

We have a General Information Security Policy, which provides guidelines for each operation to establish its local security framework, as well as to ensure effective communication of these policies to all employees.

The role of the Company´s personnel is key for the success of our Information Security Strategy. Therefore, regular training on our Information Security policies and procedures is essential. Also, we periodically implement awareness campaigns to remind our personnel the controls and best practices regarding consultation and access stored in the Company and its subsidiaries which is classified as sensitive in the operating processes that they carry out on daily basis.

In order to be updated in the latest trends, we organize the “América Móvil Cybersecurity Symposium” at least once a year in which we cover topics like information security trends, the Internet of Things, standards, challenges, opportunities, digital transformation, and access controls, among others.

We constantly evaluate and update our Information Security Strategy based on prevention, continuous improvement, and exchange of good practices among all the Group’s companies.

INFORMATION SECURITY GOVERNANCE

Our Chief Fixed Operations and Information Security Officer leads the Information Security efforts within the entire Company to ensure the correct implementation of our Strategy as well as ISO 27001 alignment across all operations.

We also have a Corporate Information Security Committee, which meets twice a month and supervises the implementation of América Móvil’s Information Security Strategy, with the following functions:

- Identifying the main risks for the business, focused on the operation and our services, as well as on the technological environment.
- Developing and managing the security strategy by creating and monitoring the Strategic Information Security Plan.
- Managing and allocating corporate and local budgets for information security.
- Determining priority actions in the face of current or future threats.

The new governance structure also allows for our subsidiaries' Information Security Teams and Scitum personnel to work closely at the incident detection level, also, we maintain our communication mechanism among operations to send alerts in a timely manner.

The local Information Security Officers are also responsible for:

- Adopting information security policies and procedures.
- Establishing strategies to comply with the guidelines that contribute to increasing the confidentiality, integrity, and availability of information resources.
- Implementing mechanisms that contribute to complying with best practices to protect information resources.
- Coordinating the evaluation and execution of projects that support activities related to Information Security.
- Supervising the communication and awareness campaigns.
- Analyzing incidents regarding security to determine solutions and preventive actions.
- Evaluating new and existing infrastructure that supports critical business processes.
- Coordinating the local Information Security Committee in each subsidiary.
- Supervising improvement measures of incidents reported by operations.
- Supporting other areas in the process of complying with information security guidelines.
- Coordinating and ensuring that all efforts, resources, tools, controls, and monitoring are consistent with confirming the availability, integrity, and confidentiality of the information.
- Informing the local CEO, the CISO and the Corporate Information Security Committee of any incident that could compromise critical information, as well as the potential impact and mitigation plans.

In addition, each subsidiary has its own local Information Security Committee. These interdisciplinary committees include employees from different areas (IT, engineering, finance, operation, maintenance, among others). Also, each operation has a "C" level executive responsible for reviewing the Cybersecurity Strategy. Each country determines a "Strategic Information Security Plan", which is updated annually or semi-annually.