Chief Information Security Officer (CISO) profile

Jesús Ricardo Medina Cantú currently acts as the Chief Information Security Officer (CISO) for GFNorte, a position he has held since 2018. He holds a Bachelor´s Degree in Administrative Informatics by the Autonomous University of Nuevo León and has a Master's Degree in Cybersecurity and ISA-PCI (Internal Security Advisor PCI-DSS).

Jesús joined GFNorte in August 2007 in the Electronic Banking area. In 2010, he started working within the Comptroller's Office in the Directorate of Control of Regulatory Provisions. In 2017 he became the SPEI Compliance Officer and since 2018 he has served as the CISO.

On November 27, 2018, the Mexican financial authorities issued regulatory provisions on information security to implement an internal control system of this matter in banks, as well as the obligation to have an Information Security Officer, known as CISO (Chief Information Security Officer).

The Mexican financial authority established that the CISO must report directly to the general director of the bank, in order to have independence from other areas, in the identification and reporting of information security risks.

The CISO has the following cybersecurity functions:

- Incident management and reporting to authorities
- Continuous evaluation of information security controls
- Monthly evaluation of safety indicators (KRI)
- Management of security alerts reported by financial sector participants in Mexico, as well as by relevant authorities.
- Responsible for regulatory compliance in payment systems (SPEI)
- Management of PCI-DSS certifications
- Identification of risks and follow-up to identified controls
- Reporting of risk situations to Council Support Committees (CAPS, CPR and integrity) and CEO
- Office of the Comptroller for the Protection of Personal Data

The CISO is responsible for supervising compliance with the cybersecurity strategy established in the PDSI and reports monthly to the CEO on the status of the projects contained in the Plan, as well as other relevant aspects such as alerts received from participants or authorities, training processes, results of technical evaluations of information security, and Cyber Risk indicators, among others.

In turn, the CISO reports various aspects of cybersecurity risk to the Audit Committee on its monthly sessions and in accordance with the corporate governance protocols related to internal control, this body through its President, reports to the Board of Directors.

The PDSI and its management before senior management and corporate governance, is established in the regulations of the Financial Group and is based on the Single Circular of Banks, regulation issued by the Mexican Authorities applicable to Financial Entities, for which it is in the public domain.

Likewise, it is reported that Banorte's Information Security Internal Control System has the following figures under the concept of the three lines of defense:

- At the first line of defense is the Information Security area, which has 212 people and considers processes such as: Government Security, Architecture and data protection, Operations (SOC), Cyber Crisis (intelligence and incident management), Application security and access control.
- On the second line is the CISO, which has 27 people who carry out annual compliance programs to assess the effectiveness of the technical security controls in the Bank's technological infrastructure, manage the annual PCI-DSS Certification process, assess the risk of the suppliers that are contracted establishing minimum incorporation requirements, and carries out all the reports of identified risks to the corporate governance bodies. In the second line there is also the IT Comptrollership area, which has 13 people who carry out operational and information security risk assessments, support monitoring of controls and implementation of internal policies.
- In the third line is the Internal Audit of Technology and Security, which has 23 elements dedicated to evaluating regulatory compliance based on its annual work program, which considers the review of critical suppliers, compliance with controls in payment systems, among others.