Certificación en Seguridad de la Información y Ciberseguridad (available in Spanish)
Certificación del Sistema de Gestión de Seguridad ISO 27001 (available in Spanish)
Reporte de incidentes al CSIRT Gobierno 2022 (available in Spanish)

La información a continuación es una extracción de la Circular Reglamentaria Interna Asunto 3 DG-T 10 Políticas de Seguridad de la Información y Ciberseguridad .

1. Introduction

Banco de la República (the Central Bank of Colombia) seeks to ensure: i) the security of its information assets, ii) the cybersecurity of the Information and Communications Technologies (ICT) that support the critical infrastructure of the financial sector and the Bank's operations, and iii) the cybersecurity of the tangible and intangible assets that are vulnerable through ICT.

To fulfill this mission, best practices have been adopted and an Information Security Management System (ISMS) has been established. This system is made up of policies, standards (technical and general information security standards), computer architecture, processes and procedures, organizational structure, and verification and control mechanisms. Its purpose is to ensure that information security risks and cybersecurity risks are known, assumed, managed, and mitigated in a documented, systematic, structured, repeatable, efficient, and adaptable manner to changes in risks, environment, and technologies.

The Information Security and Cybersecurity Policies are key elements in the ISMS since they contain guidelines that frame the actions of all employees and contractors of Banco de la República.

2. Purpose

The Information Security and Cybersecurity Policies aim at protecting the Bank's strategic assets that depend on or use the information and communications technologies. The specific objectives of this policy are:

1. To establish general guidelines related to information security and cybersecurity.
2. To be a means of dissemination to communicate the guidelines established by the Administration of *Banco de la República* regarding information security and cybersecurity, generating culture and commitment at all levels of the organization.
3. To establish and communicate the responsibility and authority over the Bank's information security and cybersecurity management.
4. To guide due care and due diligence in information security and cybersecurity management.
5. To establish an order and framework for action on information security and cybersecurity issues for all persons rendering services to Banco de la República.
6. To guarantee the reliability, image, and credibility of *Banco de la República* with its employees, customers, and society.
7. To define a common language on information security and cybersecurity within the organization.

3. Definitions/Glossary

For such purposes, the following definitions will apply:

- **Custodian:** The person or area responsible for protecting the information, in accordance with the guidelines established by the Creator (see definition below).
- **Information security standard:** A set of mandatory requirements that specifies technologies and methods and delimits responsibilities with respect to information security; it also establishes guidelines for actions, according to what corresponds to the areas within the scope of their functions.
- **Digital evidence**: Information with probative value generated, transmitted, or stored in digital form (computer-generated or generated by other means and stored or transmitted by computer).
- **Creator or person responsible**: Person or area that creates the information.
- **Information security incident**: Any adverse event that affects or threatens the fundamentals of information security (Confidentiality, Integrity, Availability), in such a way that it generates a negative impact on the information or the Bank.
- **Cybersecurity incident**: Any adverse event, real or suspected, that affects or threatens to affect the Bank's ICTs that support critical services provided to the financial system or the Bank's operation.
- **Corporate information**: Information that meets at least one of the following characteristics:
  - It is produced, sent, or received in the performance of a function, activity, service, or operation assigned to the Bank.
  - It serves as support or evidence of the rights, obligations, or liabilities of the Bank or third parties in

relation to the Bank.
    - Contains decisions, rules, or policies adopted or established by the Bank's competent authorities.
    - It is generated as a result of the interaction between the Bank and its customers, contractors, or users, which may be of interest to them or may have legal effects.
    - It is required in order to comply with any regulation or policy, to leave evidence and proof of the actions performed by the Bank's employees or by third parties rendering services to the Bank.
- **Individuals rendering services to the Bank**: Officers, employees, contractors, temporary employees, trainees, and other third parties rendering services to *Banco de la República*.
- **User**: The person or area that has been authorized by the Creator to have access to certain information.
- **Resilience**: The capacity to continue providing its missional functions in the event of critical adverse events against its information assets and technological platform.
- **Information Technology Resources**: Technological resources or support offered by the Bank to employees for the normal performance of their tasks (e.g., e-mail, Internet, telephones, personal computers, file servers, access accounts, etc.).
- **Information and Communication Technologies (ICT)**: Are the set of resources, tools, equipment, software, applications, networks, and media that allow the compilation, processing, storage, and transmission of information such as: voice, data, text, video, and images (Law 1341 of 2009, Article 6).
- **Critical Infrastructure**: Physical or virtual assets and systems that are vital to the nation, and therefore, their obstruction or destruction could result in adverse impacts on national cybersecurity, economic and social security, public health, or a combination of these issues.

4. General Information Security and Cybersecurity Policies

1. The Bank has an Information Security Management System (ISMS) that supports adequate risk management. This system will support the proper protection of information based on universally accepted principles of information security (Confidentiality, Integrity, Availability).
2. The Bank assesses the information in terms of security and determines the appropriate protection mechanisms accordingly.
3. From the initial stages of the projects, the Bank includes the evaluation of aspects related to security architecture and follows the guidelines established in this regard.
4. The Bank attends to incidents related to information security and cybersecurity.
5. The Bank implements mechanisms to monitor and promote the good use of technological resources.
6. The Bank implements access controls (physical and logical) so that corporate information is duly protected.
7. The Bank implements mechanisms and procedures to mitigate the risks associated with the management of information in the processes that support the operation of the business.
8. The Bank implements mechanisms and procedures to mitigate the risks associated with the management of the technological platform that supports the operation of the business.
9. The Bank implements a cybersecurity program aligned with best practices and the National Cybersecurity Policy. This program seeks to continuously improve its security posture and increase its resilience.

5. Information Security Certification

On 08 July 2022, the General Directorate for Technology Management obtained the ISO 27001-2013 certification for its information security management system, recognized by The Colombian Institute of Technical Standards and Certification (ICONTEC in Spanish)

- PDF Certificate
- Certificate transcript:
    - **Icontec certifica que el sistema de gestión de la organización:**
      Icontec certifies that the Organization Management System of:
      Banco de la República
      Carrera 7 # 14-78 Bogotá, D. C., Colombia

      Ha sido auditado y aprobado con respecto a los requisitos especificados en:
      Has been audited and approved based on the specified requirements of:
      ISO/IEC 27001:2013

      Este certificado es aplicable al siguiente alcance:
      This certificate is applicable to the following scope:

      La prestación de servicios de desarrollo e implantación de sistemas de información; servicios de implementación y operación de infraestructura informática y comunicaciones; servicios de seguridad informática, electrónica y mecánica; así como, los servicios y procesos de soporte, continuidad tecnológica, asesoría y apoyo complementarios que gestiona la Dirección General de Tecnología del

Banco de la República. Declaración de Aplicabilidad DSI-OD-60 2019 05.
The provision of development and implantation systems: services of development and operation of ICT infrastructure; security services in information, electronics, and mechanics; as well as services and processes of support, technological continuity, and complimentary advisory and assistance of de General Office of Technology Management of the Central bank of Colombia. Statement Applicability DSI-OD-60 2019 05.

Esta aprobación está sujeta a que el sistema de gestión se mantenga de acuerdo con los requisitos especificados, lo cual será verificado por ICONTEC.
This approval is subject to the maintenance of the management system according to the specified requirements, which will be verified by ICONTEC.

Certificado: SI003-1
Certificate:

Date Awarded: 29 August 2007
Expiration date of the previous cycle: 27 July 2022
Start date of current certification cycle: 08 July 2022
Expiration date of the current cycle: 27 July 2025
Recertification Audit Date: 23 May 2022
Revision date: 08 July 2022

6. Información sobre incidentes de seguridad digital

El Banco de la República se permite informar que "*en el periodo comprendido entre el día **1 de julio del 2022 y el día 30 de junio del 2023**, no se materializaron incidentes relevantes contra la plataforma de tecnología del Banco ni contra los datos que en ella residen. Particularmente, no se presentó ningún incidente relacionado con fuga de información que debiese informarse a la Superintendencia de Industria y Comercio relacionado con protección de datos personales. Tampoco se presentaron eventos de alto impacto (grave o muy grave) que debiesen informarse al CSIRT*."