Certificación en Seguridad de la Información y Ciberseguridad
Certificación del Sistema de Gestión de Seguridad ISO 27001
Reporte de incidentes al CSIRT Gobierno 2022

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. Introducción

El Banco de la República procura: i) la seguridad de sus activos de información, ii) la ciberseguridad de las Tecnologías de Información y Comunicaciones (TIC) que soportan la infraestructura crítica del sector financiero y la operación de Banco, y iii) la ciberseguridad de los activos tangibles e intangibles que son vulnerables a través de las TIC.

Para el cumplimiento de dicha misión se han adoptado mejores prácticas y se ha establecido un Sistema de Gestión de Seguridad de la Información (SGSI), el cual está conformado por políticas, estándares (técnicos y generales de seguridad de la información), arquitectura computacional, procesos y procedimientos, estructura organizacional y mecanismos de verificación y control; y tiene como propósito garantizar que los riesgos de seguridad de la información y los riesgos de ciberseguridad sean conocidos, asumidos, gestionados y mitigados de forma documentada, sistemática, estructurada, repetible, eficiente y adaptable a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

Las Políticas de Seguridad de la Información y Ciberseguridad son elementos fundamentales dentro del SGSI puesto que contienen directrices que enmarcan la actuación de todos los empleados y contratistas del Banco de la República.

2. Objeto

Las Políticas de Seguridad de la Información y Ciberseguridad tienen por objetivo la protección de los activos estratégicos del Banco que dependen o usan las tecnologías de la información y las comunicaciones. Los objetivos específicos de esta política son:

1. Establecer directrices generales relacionadas con seguridad de la información y ciberseguridad.
2. Ser un medio de divulgación para comunicar los lineamientos establecidos por la Administración del Banco de la República respecto a la seguridad de la información y la ciberseguridad, generando cultura y compromiso en todos los niveles de la organización.
3. Establecer y comunicar la responsabilidad y autoridad sobre el manejo de la seguridad de la información y la ciberseguridad del Banco.
4. Orientar el debido cuidado y la debida diligencia en la gestión de la seguridad de la información y la ciberseguridad.
5. Establecer un orden y marco de actuación en temas de seguridad de la información y ciberseguridad, para todas las personas que presten sus servicios al Banco de la República.
6. Garantizar la confiabilidad, imagen y credibilidad del Banco de la República con sus empleados, clientes y con la sociedad en general.
7. Definir un lenguaje común sobre la seguridad de la información y la ciberseguridad dentro de la organización

3. Definiciones/Glosario

Para tales efectos se adoptan las siguientes definiciones:

- **Custodio**: Persona o el área responsable de proteger la información, de acuerdo con los lineamientos establecidos por el Generador (ver definición más adelante).
- **Estándar de seguridad de la información**: Conjunto de requisitos de obligatorio cumplimiento que especifica tecnologías, métodos y delimita las responsabilidades respecto de la seguridad de la información; así mismo establece pautas de acciones, según lo que les corresponda a las áreas en el ámbito de sus funciones.
- **Evidencia digital**: Información con valor probatorio generada, transmitida o almacenada en forma digital (generada por computador o generada por medio diferente y almacenado o transmitido por computador).
- **Generador o responsable**: Persona o área que crea la información.
- **Incidente de seguridad de la información**: Cualquier evento adverso que afecte o amenace los fundamentos de seguridad de la información (Confidencialidad, Integridad, Disponibilidad), de tal manera

que genere un impacto negativo sobre la información o el Banco.
- **Incidente de ciberseguridad**: Es cualquier evento adverso, real o sospechoso, que afecte o amenace con afectar las TIC del Banco que soportan servicios críticos prestados al sistema financiero o la operación del Banco.
- **Información corporativa**: Aquella que cumple con al menos una de las siguientes características:
  - (i) Se produce, envía o recibe en desarrollo de una función, actividad, servicio u operación, asignada al Banco.
  - (ii) Sirve de sustento o prueba de derechos, obligaciones o responsabilidades a cargo del Banco o de terceros en relación con el mismo.
  - (iii) Aquella en la que constan las decisiones, normas o políticas tomadas o establecidas por las instancias competentes del Banco.
  - (iv) Se genera como resultado de la interacción entre el Banco y sus clientes, contratistas, o usuarios, que puede ser de interés para éstos o puede generar efectos jurídicos.
  - (v) Se requiere con el fin de dar cumplimiento a alguna norma o política, dejar evidencia y prueba de las actuaciones realizadas por los empleados del Banco o por terceros que le prestan servicios.
- **Personas que prestan servicios al Banco** : Comprende funcionarios, empleados, contratistas, empleados temporales, estudiantes en práctica y otros terceros que prestan servicios al Banco de la República.
- **Usuario**: Es aquella persona o área que ha sido autorizada por el Generador para tener acceso a cierta información.
- **Resiliencia**: Capacidad de continuar prestando sus funciones misionales ante la materialización de eventos adversos críticos contra sus activos de información y plataforma tecnológica.
- **Recursos de tecnología de información**: Recursos o apoyos tecnológicos ofrecidos por el Banco a los empleados para el normal desempeño de sus funciones (ej.: correo, Internet, teléfonos, computadores personales, servidores de archivo, cuentas de acceso, etc.).
- **Las tecnologías de la información y las comunicaciones (TIC)** : Son el conjunto de recursos, herramientas, equipos, programas informáticos, aplicaciones, redes y medios; que permiten la compilación, procesamiento, almacenamiento, transmisión de información como: voz, datos, texto, video e imágenes (Ley 1341 de 2009 Art. 6).
- **Infraestructura crítica**: Activos y sistemas, físicos o virtuales, que son tan vitales para la nación que la obstrucción o destrucción de estos activos y sistemas, podría ocasionar impactos adversos en la ciberseguridad nacional, en la seguridad económica y social, en la salud pública, o en una combinación de estos asuntos.

4. Políticas generales de seguridad de la información y ciberseguridad

1. El Banco cuenta con un Sistema de Gestión de la Seguridad de la Información (SGSI) que apoya una adecuada gestión de riesgos. Dicho Sistema soportará la debida protección de la información a partir de principios universalmente aceptados de seguridad de la información (Confidencialidad, Integridad, Disponibilidad).
2. El Banco valora la información desde el punto de vista de seguridad y acorde a ello determina los mecanismos de protección adecuados.
3. El Banco desde las etapas iniciales de los proyectos, incluye la evaluación de aspectos relacionados con la arquitectura de seguridad y sigue los lineamientos establecidos al respecto.
4. El Banco atiende los incidentes relacionados con la seguridad de la información y ciberseguridad.
5. El Banco implementa mecanismos para vigilar y promover el buen de los recursos tecnológicos.
6. El Banco implementa controles de acceso (físico y lógico) para que la información corporativa se encuentre debidamente protegida.
7. El Banco implementa mecanismos y procedimientos para mitigar los riesgos asociados a la gestión de la información en los procesos que soportan la operación del negocio.
8. El Banco implementa mecanismos y procedimientos para mitigar los riesgos asociados a la administración a la administración de la plataforma tecnológica que soporta la operación del negocio.
9. El Banco implementa un programa de ciberseguridad alineado con mejores prácticas y la Política Nacional de Ciberseguridad. Dicho programa busca el mejoramiento continuo de su postura de seguridad y aumentar su resiliencia.

5. Certificación en seguridad de la información

En el año 2022-07-08 la Dirección General de Tecnología obtuvo la certificación ISO 27001- 2013 para su sistema de gestión en seguridad de la información, reconocida por Icontec.

- Certificado en PDF
- Transcripción del certificado:
  - **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 the 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:

Fecha de Otorgamiento: 2007-08-29
Fecha de Vencimiento del Ciclo Previo: 2022-07-27
Fecha de Inicio del ciclo actual de certificación: 2022-07-08
Fecha de Vencimiento ciclo actual: 2025-07-27
Fecha de Auditoria de Recertificación: 2022-05-23
Fecha de Revisión: 2022-07-08

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 2023 y el día 30 de junio del 2024,*** *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*."