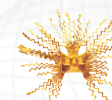


7

MANEJO INTEGRAL DE RIESGOS

- 7.1. Gestión de riesgos
- 7.2. Riesgos cibernéticos y resiliencia
- 7.3. Cultura organizacional y formación en ciberseguridad



Banco Central del Ecuador



7.1. Gestión de riesgos

La constante evolución del entorno financiero, tanto local como internacional, junto con el desarrollo de nuevas funciones institucionales orientadas a atender las crecientes necesidades de regulación bancaria, innovación e inclusión financiera, demandas de liquidez, y la incorporación de nuevas tecnologías de la información, han impulsado al BCE a rediseñar e implementar una estructura robusta capaz de identificar, medir, controlar y monitorear de manera efectiva los riesgos financieros, operativos y de seguridad de la información.

Este proceso de fortalecimiento de la gestión integral de riesgos dio inicio con los cambios estatutarios que facilitaron una visión unificada y la implementación de estrategias transversales. Esto ha garantizado un avance alineado al enfoque preventivo de riesgos, considerando los parámetros establecidos en los estándares internacionales y las tendencias vanguardistas adoptadas por otras entidades de la banca central.

Como parte del proceso de evolución y rediseño del enfoque de control interno, en 2024 se consolidaron esfuerzos interinstitucionales para aplicar mejores prácticas y fortalecer el monitoreo de los principales componentes —tanto monetarios como no monetarios— que respaldan la instrumentación de la política monetaria y refuerzan la sostenibilidad de la dolarización. Entre estos componentes se destacan: a) los activos financieros del BCE, b) el sistema de control interno, c) la seguridad de la información, y d) los mecanismos de control y prevención de lavado de activos y antisoborno.

Este proceso se materializa mediante el cumplimiento de la política de administración integral de riesgos, diseñada para garantizar una gestión estructurada y eficaz de los riesgos que enfrenta el BCE. Como parte de este esfuerzo, se consolidó el marco de gobierno corporativo, lo que ha permitido un monitoreo continuo de los diferentes riesgos a los que están expuestas las operaciones y actividades de la institución, que son documentados a través de informes y reportes periódicos presentados al Comité de Administración Integral de Riesgos y a la Junta de Política y Regulación Monetaria (JPRM). Estas acciones han fortalecido la capacidad institucional para anticipar, mitigar y responder a posibles contingencias, asegurando la estabilidad y seguridad de las operaciones del BCE.

En relación con los activos financieros del BCE, estos se encuentran sometidos a un monitoreo integral, alineado con los principios establecidos para el manejo de la información, el cumplimiento efectivo de las políticas y directrices emitidas, así como la constitución de provisiones que aseguren la adecuada razonabilidad de los estados financieros. En este marco, se realiza un seguimiento riguroso de las distintas exposiciones a riesgos, tales como riesgo de contraparte, de interés, de precio, de tipo de cambio y de liquidez, derivados de las operaciones previamente pactadas. Entre los aspectos supervisados



se incluyen la composición del portafolio, los límites y plazos de colocación, la exposición en monedas distintas al dólar, la duración y la estimación de la pérdida esperada condicional, entre otros.

En línea con la Política de Administración de los Activos Externos Disponibles para Inversión, se emitieron nuevos lineamientos de inversión y parámetros de riesgo, adaptados a la normativa vigente, con el objetivo de establecer restricciones preventivas que alineen los retornos con el presupuesto de riesgo aprobado. Asimismo, se definieron los criterios para la contratación de intermediarios financieros con los que opera el BCE, así como los parámetros mínimos para la selección de índices de referencia, garantizando el cumplimiento de los principios fundamentales de seguridad, liquidez y rentabilidad establecidos por la Ley.

En el marco de la Política para la Comercialización de Oro Adquirido por el Banco Central del Ecuador a los Mineros Artesanales y Pequeños Mineros y el Reglamento Interno para la Compra, Certificación o Venta de Oro No Monetario del Banco Central del Ecuador, durante 2024 se autorizó a 64 agentes económicos. Para ello, se ejecutaron procesos de validación, debida diligencia y verificación de requisitos, que incluyeron visitas in situ a los actores mineros que solicitaron su incorporación al programa.

7.2. Riesgos cibernéticos y resiliencia

Esta sección analiza las amenazas cibernéticas emergentes y expone las estrategias adoptadas por el BCE para fortalecer una ciberseguridad resiliente, en línea con los objetivos institucionales y las demandas de un entorno digital en permanente evolución.

7.2.1. Panorama global de amenazas cibernéticas

En un entorno global cada vez más digitalizado e interconectado, las amenazas cibernéticas han experimentado un notable incremento en términos de frecuencia, sofisticación y alcance, impactando de manera particular a las instituciones financieras. Incidentes como los ataques de *ransomware*, las intrusiones en sistemas de pagos y las acciones de espionaje corporativo han evidenciado que incluso las infraestructuras tecnológicamente más avanzadas pueden ser comprometidas. Ejemplos como el ciberataque al Banco Central de Bangladesh —ocurrido el 4 de febrero de 2016, en el que actores maliciosos lograron transferir fraudulentamente 81 millones de dólares desde las reservas del país a cuentas en Filipinas y Sri Lanka—, y las vulnerabilidades detectadas en la red SWIFT —la plataforma global que soporta transferencias financieras entre más de 11.000 instituciones en más de 200 países— han demostrado que los riesgos cibernéticos no solo se limitan a ataques

Presentación

Entorno económico
internacional

Situación
macroeconómica del
Ecuador

Operaciones del Banco
Central del Ecuador

Servicios de la Banca
Central

Museo de la Moneda y
Biblioteca Económica

La investigación y el
enverdecimiento del
Banco Central del
Ecuador

Manejo integral de
riesgos

Resoluciones de la
Junta de Política y
Regulación monetaria



**Banco Central
del Ecuador**

directos, sino también a debilidades en los entornos locales de los participantes y ponen de relieve la urgencia de adoptar un enfoque integral de ciberseguridad, que abarque mecanismos efectivos de prevención, detección, respuesta y recuperación. Este enfoque resulta esencial para garantizar la continuidad operativa, preservar la confidencialidad, integridad y disponibilidad de la información, así como mantener la confianza de los múltiples actores interconectados con el Banco Central del Ecuador.

En esta línea, durante 2024, el Banco Central del Ecuador fortaleció su estrategia de ciberseguridad implementando diversas acciones de carácter preventivo y formativo. Estas iniciativas respondieron a la necesidad de consolidar una cultura organizacional orientada a la seguridad y mitigar los riesgos asociados al factor humano y cibernético, uno de los vectores más recurrentes en incidentes de ciberseguridad.

7.2.2. Gobernanza y marcos normativos

La gobernanza en seguridad de la información constituye una base esencial para el fortalecimiento institucional, especialmente en entidades públicas y de la banca central, que gestionan información crítica y de alto valor estratégico. En este contexto, el Esquema Gubernamental de Seguridad de la Información (EGSI versión 3.0), publicado mediante el Acuerdo No. MINTEL-MINTEL-2024-0003 del 1 de marzo de 2024, establece un marco técnico estructurado y sistemático para proteger los activos de información del sector público ecuatoriano. Este esquema establece directrices claras para la gestión de la seguridad de la información, mediante un sistema que permite identificar, evaluar y mitigar los riesgos, definir políticas y procedimientos, y fomentar una cultura organizacional orientada a la seguridad. El EGSI versión 3.0 está alineado con estándares internacionales ampliamente reconocidos, tales como la ISO/IEC 27001:2022 (Gestión de la Seguridad de la Información, Ciberseguridad y Protección de la Privacidad), la ISO/IEC 27002:2022 (Controles de Seguridad de la Información) y la ISO/IEC 27005:2022 (Gestión de Riesgos de Seguridad de la Información).

Siguiendo los lineamientos del Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL), el BCE ha avanzado en la implementación del EGSI versión 3.0, aplicando de forma progresiva los principios de la norma ISO/IEC 27001 a los procesos definidos en su alcance institucional. Esta implementación gradual refleja una visión estratégica de madurez organizacional, en la que se prioriza la integración transversal de la seguridad de la información como un eje habilitador de la misión institucional.

Un hito relevante en este proceso fue la emisión de la Resolución Nro. JPRM-2024-005-A, del 8 de marzo de 2024, mediante la cual la Junta de Política y Regulación Monetaria aprobó el Estatuto Orgánico de Gestión Organizacional por



Procesos del Banco Central del Ecuador. En este documento, se crea y se establece formalmente a la Subgerencia de Seguridad de la Información, antes Unidad de Seguridad de la Información, consolidando su rol estratégico en la estructura organizacional del BCE.

Esta jerarquización refuerza el compromiso de la alta dirección con la seguridad de la información institucional y permite una gestión más eficaz y transversal de los riesgos cibernéticos, en línea con marcos de gobernanza modernos y resilientes. Su misión es:

Gestionar la seguridad de la información mediante la definición de estrategias, políticas, normas o controles en concordancia con la normativa nacional y las mejores prácticas internacionales, a fin de preservar la confidencialidad, integridad y disponibilidad de la información y contribuir al cumplimiento de la misión y objetivos estratégicos del Banco Central del Ecuador.

Figura 227. Sistema de gestión de seguridad de la información



Fuente: Banco Central del Ecuador



7.2.3. Gestión de riesgos y resiliencia cibernética

La gestión de riesgos cibernéticos se ha consolidado como un componente esencial dentro de la gobernanza institucional, especialmente en entornos altamente digitalizados, donde la disponibilidad, integridad y confidencialidad de la información constituyen pilares fundamentales.

En este contexto, la resiliencia cibernética se define como la capacidad de una organización para anticipar, resistir, adaptarse y recuperarse frente a incidentes de ciberseguridad. Esta capacidad no solo depende de controles tecnológicos robustos, sino también de estructuras de gobernanza eficaces, marcos normativos adecuados y una cultura organizacional comprometida con la seguridad de la información. La resiliencia implica, además, estar preparados para mantener operaciones críticas ante interrupciones, así como asegurar la continuidad de los servicios esenciales frente a ataques cibernéticos deliberados o fallos sistémicos.

El BCE ha avanzado significativamente en esta dirección mediante la adopción de prácticas internacionales en la gestión del riesgo cibernético, la implementación de planes de continuidad del negocio y recuperación ante desastres, así como la evaluación periódica de vulnerabilidades. Asimismo, el desarrollo de pruebas de respuesta ante incidentes y ejercicios de simulación ha contribuido a fortalecer su capacidad institucional para enfrentar escenarios adversos, minimizando tanto el impacto operacional como el reputacional.

7.3. Cultura organizacional y formación en ciberseguridad

En un entorno donde las amenazas cibernéticas evolucionan constantemente, la tecnología por sí sola no es suficiente para proteger los activos institucionales. La cultura organizacional en ciberseguridad emerge como un factor crítico para fortalecer la postura de defensa de la banca central, promoviendo conductas seguras, actitudes proactivas y una comprensión compartida sobre los riesgos asociados al uso de la información y los sistemas digitales.

El Banco Central del Ecuador ha reconocido que la protección de la información debe ser una responsabilidad compartida por todos los niveles de la organización. En ese sentido, durante 2024, se ha liderado diversas iniciativas enfocadas en la formación y concienciación de los colaboradores para la protección de la información. Estas acciones han incluido el envío sistemático de mensajes de concienciación por correo electrónico, la ejecución del plan anual de sensibilización, capacitaciones presenciales especializadas y simulacros de ciberataques de *phishing*. Estas actividades no solo han buscado

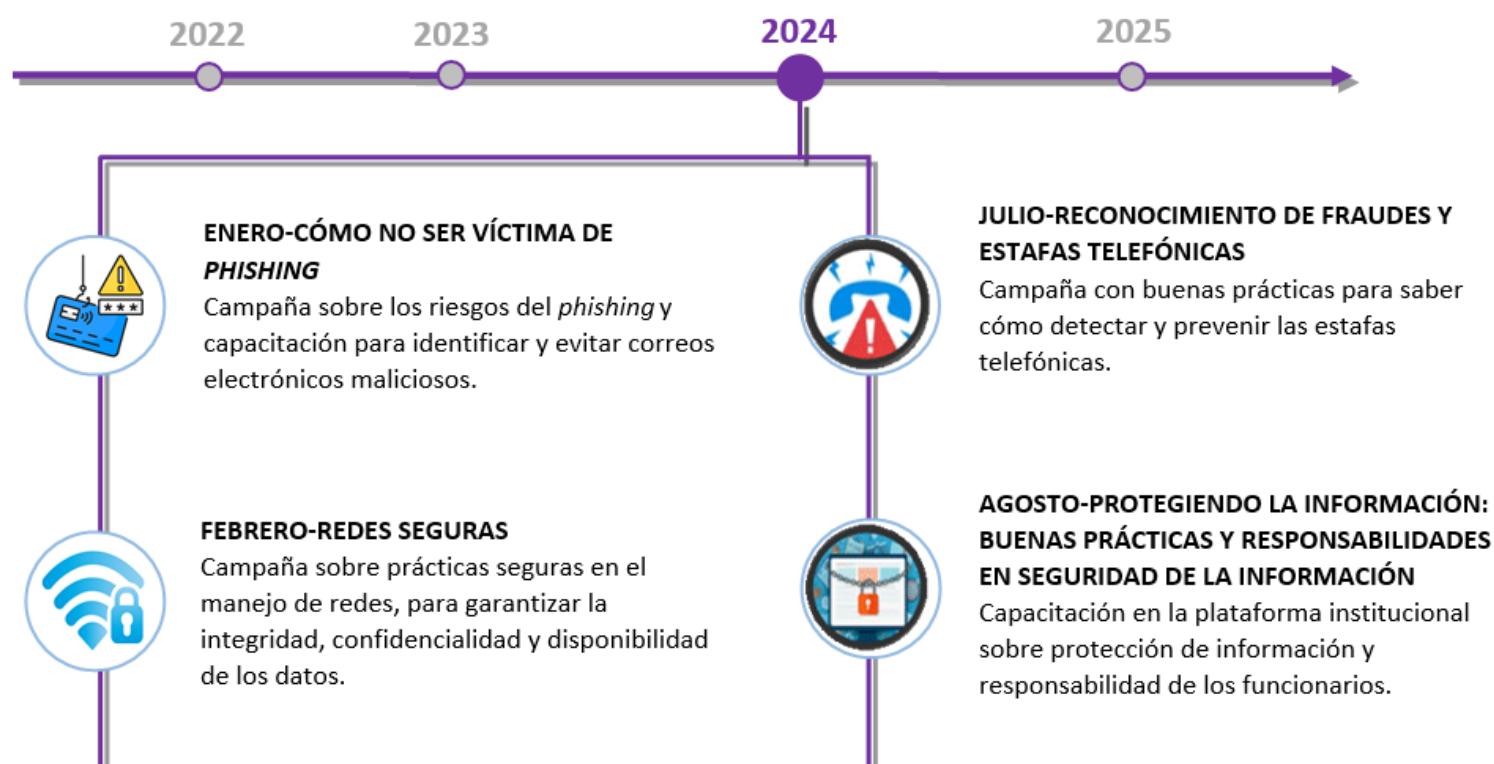


educar, sino también medir el nivel de exposición al riesgo humano y fortalecer los mecanismos de respuesta frente a posibles incidentes.

La cultura de seguridad se construye a través de la repetición, la claridad en los mensajes y la coherencia institucional. Por ello, los contenidos de las campañas del BCE han estado alineados con los objetivos estratégicos de la entidad y las buenas prácticas nacionales e internacionales. Además, se ha promovido un lenguaje accesible y contextualizado, adaptado al rol de cada grupo de interés dentro de la organización.

Con el fin de evidenciar los avances alcanzados durante 2024, a continuación, se detallan las principales actividades desarrolladas mensualmente, en el marco del fortalecimiento de la cultura organizacional y la gestión integral de la ciberseguridad:

Figura 228. Cultura organizacional y gestión integral de la ciberseguridad





MARZO-DATOS SEGUROS

Campaña con información sobre medidas para mantener datos seguros, prevenir accesos no autorizados y salvaguardar su privacidad.



ABRIL-MANTÉN TU ESCRITORIO LIMPIO Y SEGURO

Campaña con recomendaciones para mantener el espacio de trabajo ordenado, minimizando riesgos de pérdida, robo, alteración o divulgación de información.



MAYO-FUGA DE INFORMACIÓN

Campaña con recomendaciones para prevenir la pérdida de datos mediante controles como la clasificación adecuada, cifrado y copias de seguridad.



JUNIO-TELETRABAJO: ¡MANTENTE SEGURO EN LÍNEA!

Campaña orientada en proteger la información institucional, creando contraseñas seguras, usando adecuadamente la VPN y el correo institucional.



SEPTIEMBRE-PHISHING-EVITAR ENLACES Y ARCHIVOS SOSPECHOSOS

Campaña con recomendación sobre buenas prácticas para evitar ser víctima de *phishing* no abrir archivos ni hacer clic en enlaces sospechosos.



OCTUBRE-SEGURIDAD EN DISPOSITIVOS MÓVILES

Campaña con buenas prácticas para prevenir proteger la red institucional y dar cumplimiento normativo.



NOVIEMBRE-USO SEGURO DE REDES SOCIALES

Campaña sobre el uso seguro de las redes sociales, con el fin proteger la información y reputación institucional.



DICIEMBRE-PROTECCIÓN CONTRA RANSOMWARE

Campaña con recomendaciones para prevenir ser víctimas de este tipo de *malware* y cómo actuar en caso de sospechar que el equipo ha sido infectado.

Fuente: Banco Central del Ecuador