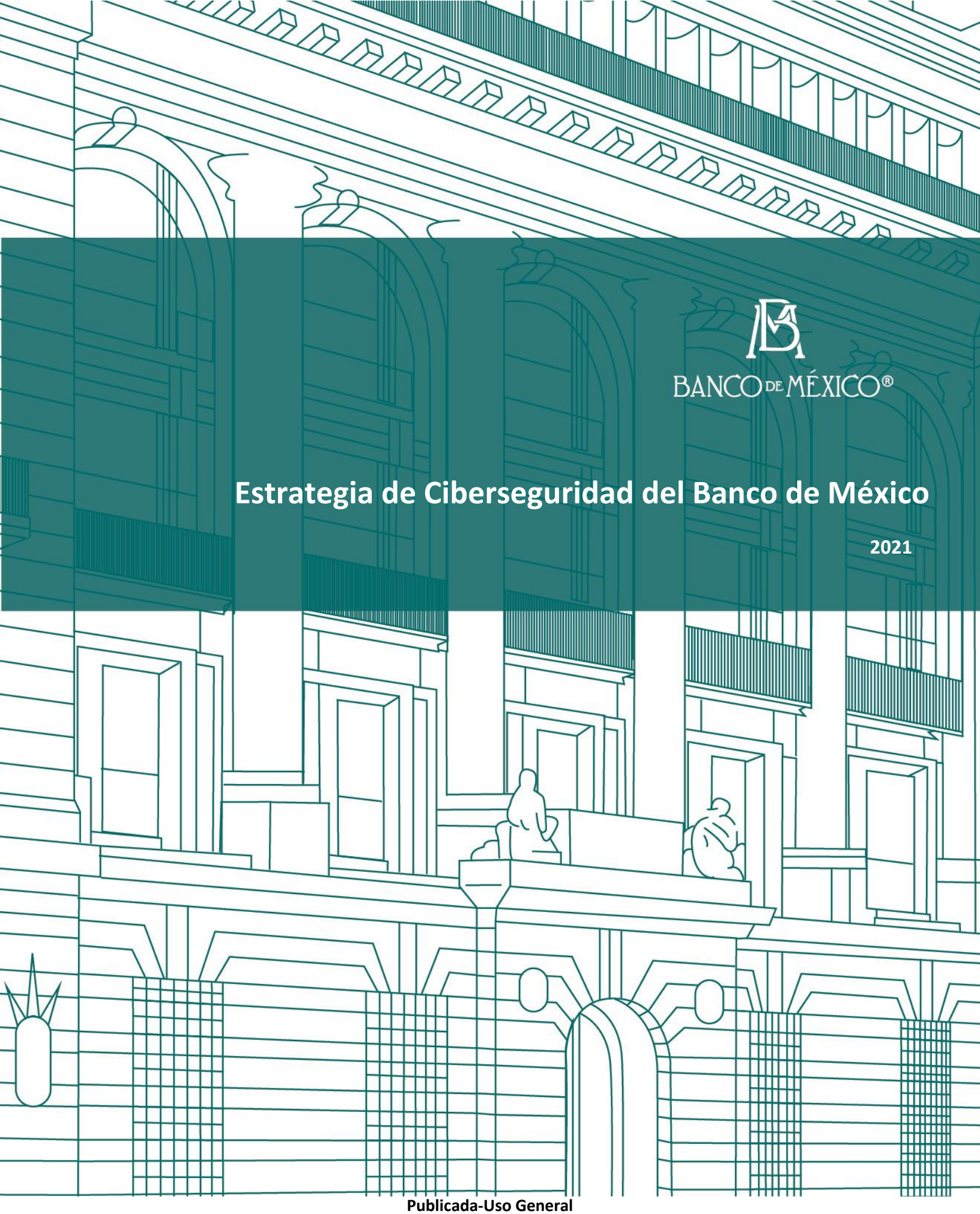

BANCO DE MÉXICO®

Estrategia de Ciberseguridad del Banco de México

2021

Antecedentes

Para el Banco de México la seguridad de la información siempre ha sido un tema importante y ha estado presente desde los inicios de la adopción de la tecnología de la información ensus procesos. En ese sentido, ha trabajado para preservar la confidencialidad, integridad ydisponibilidad de la información que maneja el Banco; incorporando diversos controles tecnológicos y administrativos, conforme a mejores prácticas y estándares internacionales con el fin de incrementar el nivel de protección de sus activos informáticos. Dichos estándares, además de lineamientos de organismos financieros internacionales, son el marco de referencia que ayuda a definir, en materia de seguridad de la información, la regulación que aplica a las Entidades Reguladas por el Banco.

Por otra parte, el Banco de México ha adoptado procesos de gestión de vulnerabilidades y de incidentes y, cuando ha sido necesario, ha recurrido a servicios de evaluación de seguridad por parte de expertos. El Banco de México cuenta con personal altamente capacitado en seguridad informática, y con procesos robustos de protección y monitoreo desus sistemas e infraestructura.

El Banco de México parte del principio de que para mantener la confianza del público en elsistema financiero y en los sistemas de pagos, es crucial garantizar la seguridad de sus sistemas. Para tal efecto, el Banco es consciente de que es indispensable la participación activa y coordinada de las autoridades financieras, los Bancos y otras instituciones financieras, ya que en materia de ciberseguridad todos los jugadores son importantes.

Antes de 2016

En 2013, el Banco de México creó la Gerencia de Seguridad de Tecnologías de la Información como principal responsable de procurar la ciberseguridad en la Institución. La misión de esta área es asesorar, administrar y dirigir proyectos y actividades conforme la estrategia de protección informática institucional, para proporcionar servicios de seguridad tecnológica de vanguardia que permitan al Banco operar de manera confiable y oportuna. Esta gerencia cuenta con un equipo especializado que detecta y responde a incidentes de seguridad informática con un Centro de Reacción Temprana; también ha desplegado herramientas básicas de protección (antivirus, firewalls, detectores de intrusos, tokens de acceso, etc.), eimplementa controles sofisticados de seguridad.

Además de reforzar sus sistemas propios, desplegar mecanismos de defensa y establecer prácticas avanzadas de seguridad informática al interior; el Banco de México siempre ha estado pendiente y a la vanguardia de los desarrollos tecnológicos y protección del sistema financiero, en particular en lo referente a sistemas de pagos.

Desde su creación, el SPEI fue diseñado por Banco de México con elementos de protección robustos como uso de firmas electrónicas en todos sus intercambios de mensajes; plataformas de telecomunicaciones privadas y cifradas; y con mecanismos automatizados orientados a mantener la integridad de los datos intercambiados. Con apoyo de expertos internacionales, realiza revisiones de seguridad en el sistema SPEI. En términos regulatorios, exige a los participantes en el sistema que establezcan controles estrictos de seguridad, en su infraestructura y procesos, protegiendo principalmente al público usuario del sistema.

2016

A raíz de distintos incidentes internacionales de ciberseguridad en el sector financiero y el creciente número y sofisticación de los mismos, el Banco de México decidió hacer una revisión profunda de su estrategia de ciberseguridad que le permitiera identificar oportunidades de mejora y transformación.

Como primer paso, contrató a una consultora internacional para realizar una evaluación integral del estado de la ciberseguridad del Banco de México, la cual consideró aspectos tecnológicos, humanos y de procesos; a través de una metodología propia basada en estándares y prácticas internacionales, esta evaluación indicó que, si bien el Banco tenía unnivel razonable de seguridad, era importante robustecer dicho nivel dado su papel como institución estratégica y financiera.

2017-2020

En 2017, con el apoyo y acompañamiento de los consultores contratados, el Banco de México elaboró e inició un programa de reforzamiento de seguridad de su información, con líneas de acción que permiten reforzar la estrategia de ciberseguridad del Banco en 4 grandes pilares:

i. Proteger la información y sus procesos.
ii. Abordar el tema desde una perspectiva proactiva de defensa y prevención de riesgos.
iii. Enfocar la seguridad de la información a todo el ecosistema financiero que interactúan con Banco de México.
iv. Reforzar la gobernabilidad de la seguridad de la información, reorganizando áreas, dotando de recursos humanos, y diseñando políticas institucionales de ciberseguridad.

En 2018, se tuvieron avances en el programa de reforzamiento de la seguridad de la información del Banco de México. Los avances con base a los pilares fueron:

i. Se definieron mecanismosque atienden requerimientos de la Ley de Protección de Datos Personales y de la Ley de Transparencia.
ii. Se reforzaron áreas técnicas de seguridad informática; así como de los mecanismos de evaluación y protección de vulnerabilidades informáticas.
iii. Se elaboraron nuevos contratos y emitieron disposiciones para fortalecer la seguridad de la información de las conexiones de los intermediarios financieros a la Red Financiera a la infraestructura tecnológica y de comunicaciones del Banco. En estos se imponen requerimientos de seguridad de la información, a fin de cuidar la ciberseguridad del ecosistema. Asimismo, el Banco creó su Centro de Defensa de Ciberseguridad (CDC), que tiene como objetivo hacer frente a los incidentes de ciberseguridad que se presenten dentro y fuera del Banco.
iv. Con respecto a la gobernabilidad de la seguridad, la Junta de Gobierno del Banco de México autorizó, el 24 de abril de 2018, la creación de la Dirección de Ciberseguridad, la cual atiende responsabilidades para fortalecer la seguridad de la información al interior y hacia el sistema financiero.

Durante 2019 y 2020, el Banco incrementó su madurez de ciberseguridad en 10 dominios de seguridad de la información, a través del programa de reforzamiento de la seguridad, creando y formalizando documentos, normas, procesos o lineamientos a nivel institucional; y demostrando capacidad operativay tecnológica para apegarse a dicha normatividad, y estar en condiciones de extender su aplicación al resto de los procesos del Banco. Estos dominios son:

1) Gobernanza, Cumplimiento y Organización.
2) Protección de Datos.
3) Gestión de Riesgos de Seguridad.
4) Gestión de Identidad y Autenticación.
5) Respuesta a Incidentes.
6) Administración de Terceros y Proveedores.
7) Protección de Equipos de Punto Final.
8) Protección de Aplicaciones y Bases de Datos.
9) Protección de Redes y Centros de Datos.
10) Capacitación y Concientización en Seguridad.

Dentro de los resultados del programa de reforzamiento de la seguridad que fue concluido en Octubre 2020, el Banco logró mejorar: i) su postura en ciberseguridad al integrar la ciberseguridad y seguridad de la información como un tópico relevante en la organización, trascendiendo los componentes tecnológicos; ii) su capacidad de identificación, categorización, evaluación de riesgos a la información para protegerla, con base en su valor para la institución; iii) sus metodologías de mitigación y gestión de riesgos a la ciberseguridad; iv) sus capacidades de detección, análisis, contención, respuesta y

recuperación ante incidentes avanzados de seguridad de la información, y v) su colaboración y comunicación con otras autoridades ante incidentes de ciberseguridad que se presenten en el sistema financiero.

A finales de 2020, el Banco amplió las facultades de la Dirección de Ciberseguridad para que, adicional a sus funciones de política y estrategia, absorba funciones de seguimiento al cumplimiento de las normas y disposiciones internas y externas en materia ciberseguridad, así como de análisis de información de inteligencia en ciberseguridad y de coordinación de incidentes en ciberseguridad. Adicionalmente, la Dirección de Ciberseguridad se integró a la Dirección General de Contraloría y Administración de Riesgos con el objeto de integrar la gestión de riesgos en materia de ciberseguridad a los esquemas institucionales de gestión de riesgos.

El Banco con el objetivo de dar continuidad a los logros alcanzados, así como mantener y mejorar la madurez de la ciberseguridad de la institución de forma integral, definió un Programa de Reforzamiento Continuo de su ciberseguridad. Dentro de este programa se continuarán las acciones de fortalecimiento basados en los 10 dominios, se dará atención y seguimiento a las acciones derivadas de evaluaciones internas de riesgos, auditoría y control interno, así como las leyes aplicables al Banco, siempre en apego a estándares internacionales y mejores prácticas en materia de seguridad de la información.

El Programa de Reforzamiento Continuo consta de planes de implementación de controles de ciberseguridad en las diferentes áreas de la institución considerando el impacto en los procesos del Banco y la prioridad de atención de estos, basándose en las obligaciones internas y externas de la institución, así como en la mitigación de riesgos de seguridad referentes a amenazas que el Banco y el sistema financiero enfrentan en temas de ciberseguridad.

Finalmente, el Banco continuará fomentando la coordinación entre autoridades del sistema financiero y de seguridad nacional, para mejorar la atención de incidentes de ciberseguridad de forma oportuna y que contribuyan en la persecución de delitos. En el ámbito del fortalecimiento de los protocolos de respuesta a incidentes seguirá promoviendo ejercicios de ciberresiliencia entre este Banco Central y los participantes del sistema financiero. En el ámbito internacional, continuaremos participando en los grupos especializados en temas de ciberseguridad y ciberresiliencia que promueven las mejores prácticas en la materia, por ejemplo, el grupo de trabajo de ciberseguridad en Banco de Pagos Internacionales (BIS por sus siglas en inglés).

BANCO DE MÉXICO®

www.banxico.org.mx