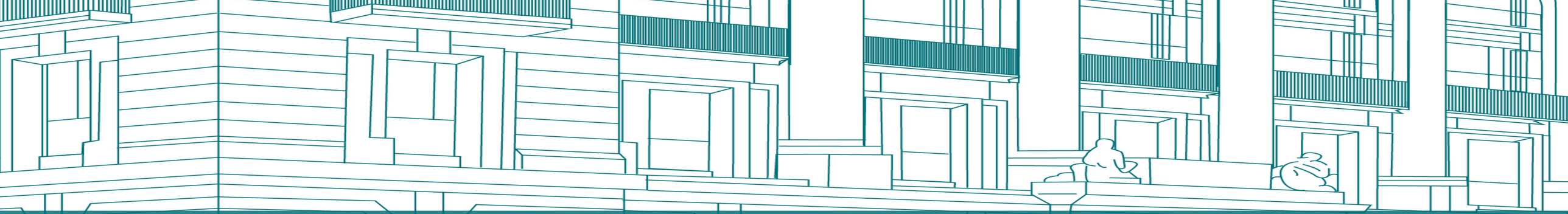


Estado: Final
Unidad Administrativa: DGEF - DISF
Fecha de última actualización: 14-Sep-2025

Consideraciones sobre el riesgo cibernético en la gestión de información financiera

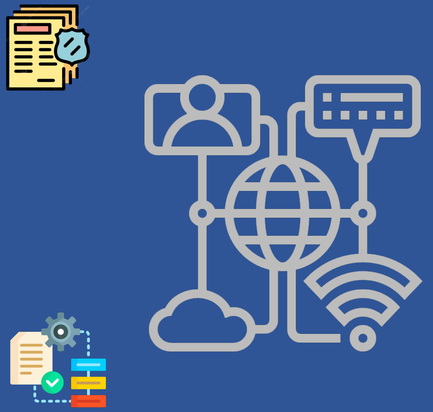
Juan Fernando Ávila Embriz

BANCO DE MÉXICO®

Las opiniones expresadas en esta presentación son responsabilidad exclusiva del autor, por lo que no necesariamente representan la postura del Banco de México ni de su Junta de Gobierno.

Agenda

- Antecedentes
- Proceso general de gestión de la información del sistema financiero
- Controles de seguridad de la información
- Controles de seguridad de la información para servicios de TI
- Plan Bienal de Ciberseguridad
- Controles prioritarios de Ciberseguridad
- Implementación de controles para el acopio, validación y carga de datos
  - ✓ Planeación y organización
  - ✓ Construcción y adquisición
  - ✓ Operación y soporte



Antecedentes

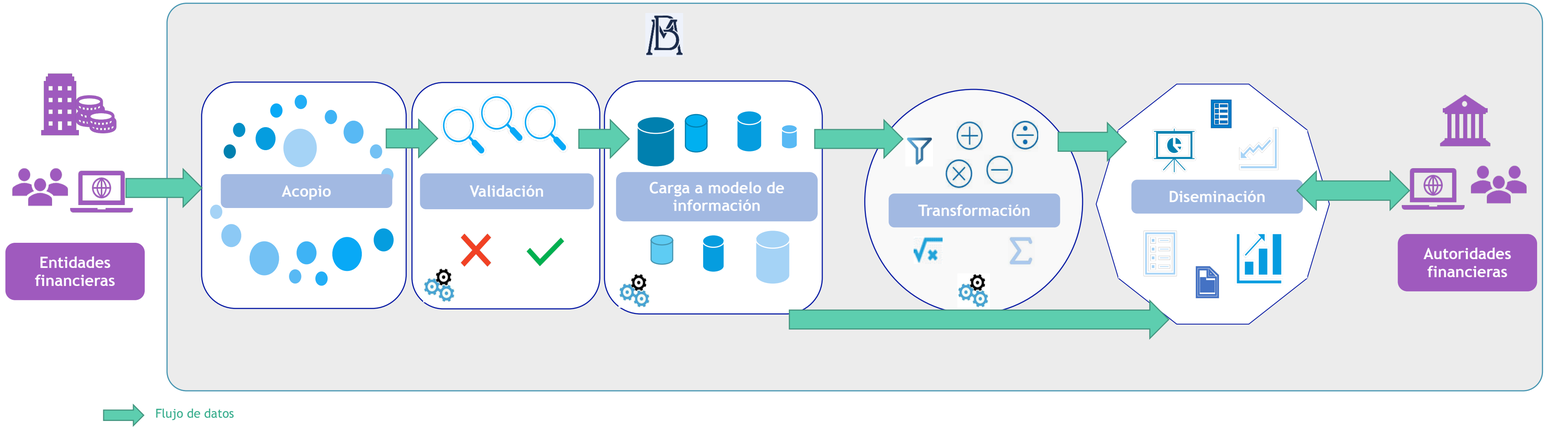
Desde 2017, el Banco de México inició un programa de reforzamiento de la seguridad de su información, que comenzó con un diagnóstico del grado de madurez en materia de ciberseguridad que tenía la institución. Con el diagnóstico obtenido, se instrumentaron políticas y lineamientos que sirven como referencia para fortalecer las capacidades de seguridad.

Para ello, se adoptaron los estándares internacionales del National Institute of Standards and Technology (NIST), los cuales se adecuaron a la institución mediante la definición de controles de seguridad de la información y controles prioritarios de ciberseguridad.

A partir de los controles de ciberseguridad, desde 2021 se definen planes de trabajo bienales que permiten cerrar las brechas identificadas a partir del diagnóstico obtenido, así como elementos emergentes.

Proceso general de gestión de la información del sistema financiero

- La operación del Banco de México se define a partir de procesos. La Dirección de Información del Sistema Financiero (DISF), adscrita a la Dirección General de Estabilidad Financiera (DGEF), tiene entre sus responsabilidades el proceso de Acopiar, Validar, Transformar y Diseminar información financiera.
- La información financiera es requerida a los diferentes participantes del sistema financiero mediante ***Formularios,*** los cuales son enviados al Banco de México por medio de sistemas desarrollados internamente, los cuales cumplen con altos estándares de seguridad.
- Una vez que la información llega al Banco de México, es validada y, de ser necesario, transformada para ponerla a disposición de las áreas que lo requieran por sus funciones, así como a otras autoridades financieras.



Modelo de Información del sistema financiero

Datos acopiados directamente por Banco de México

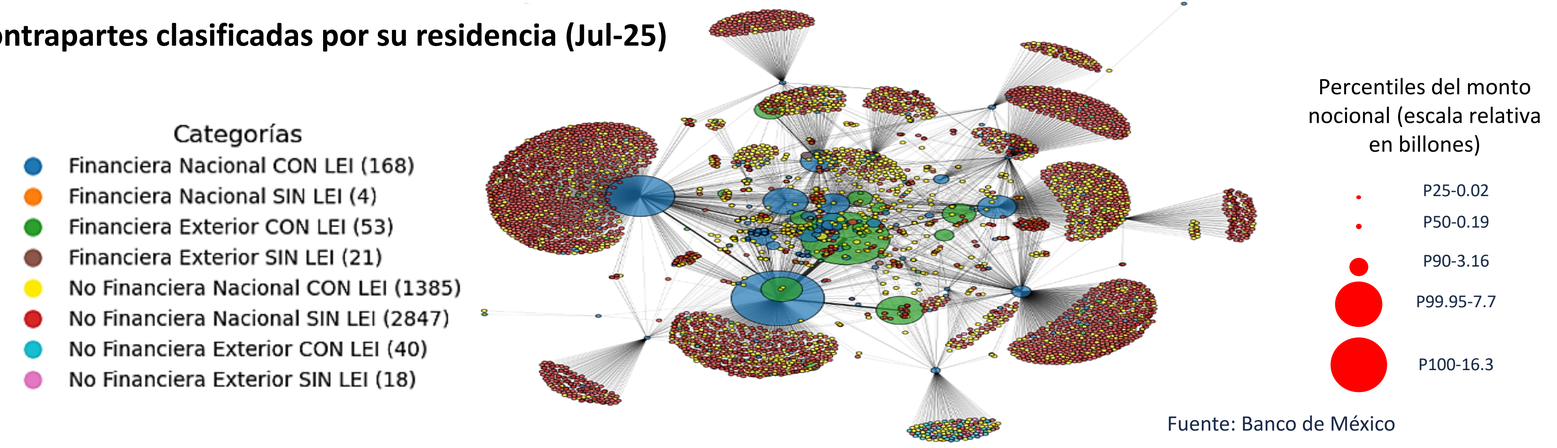
Datos acopiados por otras entidades, como autoridades regulatorias, contrapartes centrales, entre otros.

Frecuencia	Microdatos										Otra información	
Diario	Mercado cambiario (1)	Derivados (4)	Títulos (reportos/compra-venta/préstamos) y tenencias (3)	Operaciones interbancarias (2)	Depósitos a plazo (2)	Operaciones transfronterizas (1)	Cheques y transferencias	Operaciones con tarjetas de crédito y débito	Calificaciones, precios y factores de riesgo	Portafolios de fondos de pensiones y fondos de inversión	Contrapartes (1)	LEI
Semanal	Derivados (1)			Facilidades de liquidez (1)			Información de fondeo (1)				Cajeros, sucursales y bóvedas (1)	Cuotas y tasas de descuento (1)
Mensual	Tenencia de acciones (1)	Derivados (5)	Certificados de depósito (1)	Cuentas de fondos de pago electrónico (2)	Títulos (reportos/compra-venta/préstamos) y tenencias (3)	Facilidades de liquidez (1)	Créditos hipotecarios (1)	Créditos cartera comercial (1)	Buró de crédito (empresas) (2)			
Bimestral	Crédito revolvente (tarjetas de crédito) (1)					Crédito no revolvente (6)					Catálogo de clientes (1)	
Trimestral	Garantías de liquidez (cada 4 meses) (1)					Buró de crédito (2)					Avalúos de viviendas	
Semestral	Cuentas individuales de los fondos de pensiones (principales características)											

Importancia de la información financiera en la toma de decisiones

Red de entidades de banca comercial con el total de sus contrapartes clasificadas por su residencia (Jul-25)

- Como ejemplo de la riqueza de la información del modelo, contar con microdatos sobre las transacciones de derivados permite identificar riesgos potenciales de concentración en el mercado.
- La gráfica presenta la red de exposiciones, clasificando a los nodos según su sector. El tamaño de los nodos se escala de acuerdo al monto nocional vigente.



Fuente: Banco de México

Controles de seguridad de la información

- Desde 2017, en la definición de los planes de reforzamiento de la seguridad, se planteó una serie de ***Políticas y Lineamientos de Seguridad de la Información***, en la que se detallan los dominios de seguridad de la información.
- Dichos dominios incluyen las siguientes dimensiones:

Dimensión de estrategia de implementación de dominios	
PL.01 GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	PL.07 SEGURIDAD DE EQUIPOS DE USO PERSONAL
PL.02 GESTIÓN DE ACTIVOS DE INFORMACIÓN	PL.08 SEGURIDAD DE LAS SOLUCIONES DE TECNOLOGÍAS DE LA INFORMACIÓN
PL.03 GESTIÓN DE VULNERABILIDADES	PL.09 SEGURIDAD DE CENTROS DE CÓMPUTO Y TELECOMUNICACIONES
PL.04 GESTIÓN DE IDENTIDADES, AUTORIZACIONES Y ACCESOS	PL.10 CONCIENTIZACIÓN Y CAPACITACIÓN
PL.05 GESTIÓN DE INCIDENTES, RESILIENCIA Y PRUEBAS DE SEGURIDAD	PL.11 GESTIÓN DE LA CONFIGURACIÓN
PL.06 GESTIÓN DE TERCEROS	

Controles de seguridad de la información

En el 2019 se definió una serie de controles de seguridad de la información basados en el estándar NIST 800-53, revisión 4. Estos controles tienen como objetivo **proteger la Confidencialidad, Integridad y Disponibilidad de la Información**, a través del cumplimiento de los dominios establecidos.

En 2023, estos controles fueron actualizados a partir de la versión estándar NIST 800-53 revisión 5 de 2020.

Internamente el Banco de México aplica pruebas de estos controles de seguridad de la información a los servicios de TI que soportan los procesos de la institución.

ID	Familia	No. de Líneas Base 2023
AC	Control de Acceso	19
AT	Concientización y Capacitación	4
AU	Auditoría y Rendición de Cuentas	12
CA	Valoración, Autorización y Monitorización	8
CM	Gestión de la Configuración	12
CP	Planeación de Contingencias	9
IA	Identificación y Autenticación	10
IR	Respuesta a Incidentes	8
MA	Mantenimiento	6
MP	Protección de Medios	7
PE	Protección Física y Ambiental	17
PL	Planeación	6
PS	Seguridad de Personal	9
RA	Evaluación de Riesgos	6
SA	Adquisición de Sistemas y Servicios	12
SC	Protección de Sistemas y Comunicaciones	19
SI	Integridad de los Sistemas y la Información	12
SR	Gestión de Riesgos de la Cadena de Suministro	8

Plan Bienal de ciberseguridad

A principios de 2021, el Banco de México incorporó a su Programa de Reforzamiento Continuo de Ciberseguridad, la instrumentación de planes bienales de 14 Controles Prioritarios (CP) de ciberseguridad.

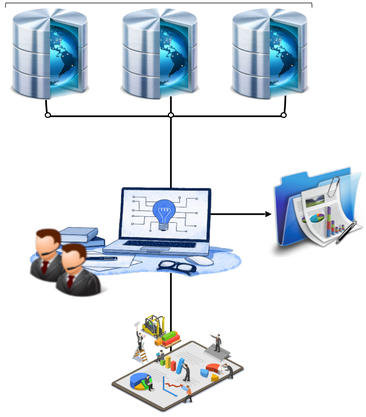
En dicho plan, se han venido cubriendo brechas en un proceso de mejora continua.

La DISF ha enfocado sus esfuerzos en la atención de dichas brechas, principalmente para su proceso de gestión de la información del sistema financiero.

A lo largo de casi cuatro años, ha instrumentado más de 200 acciones de mejora para el cumplimiento de los CP establecidos.

Controles prioritarios de ciberseguridad (CP)

ID	Nombre del control prioritario de ciberseguridad
CP01	Inventario de activos tecnológicos
CP02	Identificación, categorización y evaluación de riesgos de los activos de información
CP03	Uso de herramienta de Data Loss Prevention
CP04	Padrón de proveedores críticos
CP05	Gestión de vulnerabilidades
CP06	Atención de evaluaciones de seguridad de la información
CP07	Gestión de incidentes



ID	Nombre del control prioritario de ciberseguridad
CP08	Planeación de la capacidad
CP09	Ciclo de vida de desarrollo seguro de soluciones tecnológicas
CP10	Gestión integral de identidades y accesos
CP11	Documentación y plan individual de ciberseguridad
CP12a	Monitorización de la operación y sistemas
CP12b	Provisión de servicios externos
CP13	Gestión de terceros
CP14	Gestión del cifrado de información

Implementación y ejecución de controles en la Provisión de servicios de TI

Los controles de seguridad en los sistemas de información se implementan en todos los grupos de procesos de la gestión de TI, que incluye la operación de los procesos que soportan:

Planeación y organización

- Políticas y procedimientos de ciberseguridad
- Concientización y capacitación de ciberseguridad

Construcción o adquisición

- Desarrollo seguro, pruebas de evaluación de seguridad y gestión de vulnerabilidades
- Incorporación de clausulas de seguridad de información en contratos y supervisión de personal externo

Operación y soporte

- Controles de acceso del servicios de TI y políticas de contraseñas
- Monitoreo de incidentes de seguridad e identificación de vulnerabilidades de componentes
- Planes de contingencia y de respuesta a incidentes

Implementación y ejecución de controles en la Provisión de servicios de TI

Planeación y organización de servicios de TI

PL.10 Concientización y capacitación

AT-02 Capacitación sobre concientización de la seguridad y privacidad

PL.01 Gestión de la seguridad de la información

PL-10 Selección línea base controles

PL.01 Gestión de la seguridad de la información

PL-01 Política y procedimientos de planificación de seguridad

Procesos operativos que implementan controles de ciberseguridad transversales

PL.02 Gestión de activos de información

RA-02 Categorización de seguridad

Implementación y ejecución de controles en la Provisión de servicios de TI

Procesos operativos que implementan controles de ciberseguridad transversales

Planeación y organización de servicios de TI

Procesos operativos que se generaron o mejoraron a partir del inicio de los Programas de reforzamiento continuo de la Ciberseguridad para establecerse como buenas practicas cotidianas y recurrentes bien definidas y en ejecución:

- **Actualización periódica de contraseñas** de cuentas de usuario, cuentas de servicio o cuentas de administración usadas en todos los niveles de servicios de TI.
- **Revisión periódica de privilegios de acceso** de los usuarios de los servicios TI, que permite la depuración de privilegios por desvinculación de personas con sus entidades o cambios no notificados de sus funciones.
- **Categorización de activos de información** que se usan o generan en los procesos para establecer su clasificación de acceso (Público, Uso General o Uso Limitado), y para facilitar la aplicación de políticas de DLP o la disponibilidad para efectos de solicitudes de transparencia.

- **Evaluaciones periódicas de seguridad** para detección de vulnerabilidades con pruebas de Pentest, Red Team o Revisión especializada de código, y cumplimiento de controles.
- **Identificación y gestión de vulnerabilidades,** adicionalmente a las evaluaciones de seguridad se realiza un seguimiento del estado que guardan muchas de las librerías y software usados en los servicios de TI y se realiza una gestión para evaluar el riesgo e implementar las acciones de mitigación de las vulnerabilidades identificadas.
- **Registro y actualización de inventario de activos tecnológicos** para la identificación de los activos tecnológicos usados en los servicios de TI y sus relaciones, la evaluación del impacto de su afectación a la información o servicios asociados en caso de cambios o daño.
- **Gestión de incidentes de seguridad y continuidad operativa** para el seguimiento de los incidentes de seguridad identificados, interna o externamente, de acuerdo con lineamientos que facilitan la comunicación con las áreas involucradas y así, atender de forma eficiente todas las etapas de continuidad operativa de los procesos, y, en su caso, detonar los planes de contingencia necesarios.

Acopio, validación y carga de datos

Proceso de Desarrollo de Sistemas

- Análisis de necesidades del Modelo operativo
- Diseño de solución y servicios
- Construcción de solución
- Pruebas de servicios construidos
- Despliegue de aplicaciones y servicios

Prácticas de Desarrollo seguro

PL.08 Seguridad de las soluciones de TI
SI-10 Validación de información de entrada

PL.08 Seguridad de las soluciones de TI
SI-11 Manejo de errores

PL.08 Seguridad de las soluciones de TI
SI-03 Protección contra código malicioso

PL.02 Gestión de activos de información
RA-02 Categorización de seguridad

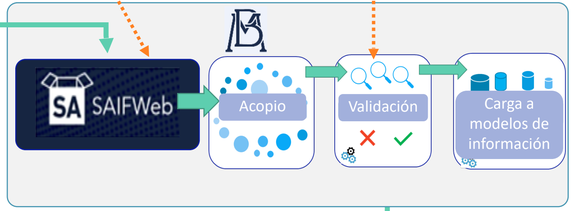
Proceso de Configuración de Procesos de acopio y validación

- Identificación y análisis de necesidades de información
- Diseño conceptual del proceso
- Análisis de especificaciones de proceso
- Diseño de proceso
- Configuración del proceso
- Pruebas de operación del proceso
- Liberación del proceso

Sistema de acopio para que las entidades financieras cumplan con la entrega de sus requerimientos de información

Construcción o adquisición de servicios de TI

55 formularios o procesos de acopio y validación de datos automatizados y configurados en sistema de acopio.



Acopio, validación y carga de datos

Operación y soporte de servicios de TI

Acreditación de usuarios del sistema de acopio

Acreditación de Representantes legales de entidad

Validación de pruebas de identidad con poderes

Incorporación de usuarios del sistema de acopio

Asignación de permisos a formularios de datos

Se cuenta con 3,200 usuarios registrados con diferentes roles de 250 entidades del sistema financiero

Authorized User

Entidades financieras

SAIFWeb

Acopio

Validación

Carga a modelos de información

PL.04 Gestión de identidades, autorizaciones y accesos

AC -02Administración de cuentas

PL.04 Gestión de identidades, autorizaciones y accesos

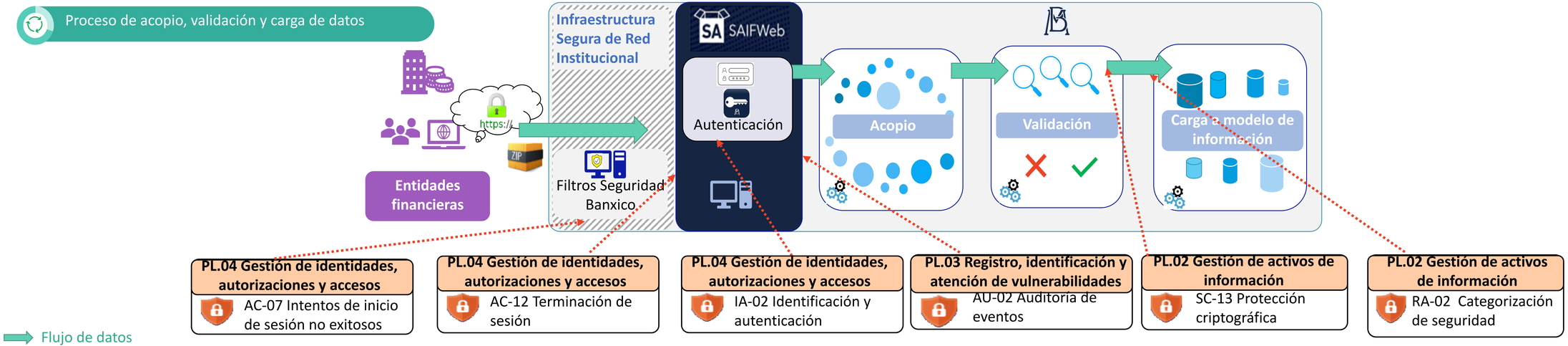
IA-12 Prueba de identidad

PL.02 Gestión de activos de información

RA-02 Categorización de seguridad

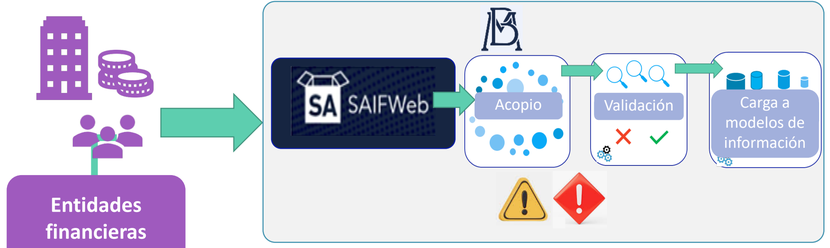
Acopio, validación y carga de datos

Operación y soporte de servicios de TI



Acopio, validación y carga de datos

Operación y soporte de servicios de TI



Entidades financieras

PL.04 Gestión de identidades, autorizaciones y accesos

IA-02 Identificación y autenticación

PORTAL DE SERVICIOS

Proceso de gestión de solicitudes de servicio o reporte de incidentes

Categorización de solicitud → Revisión en Línea frontal → Solución de grupo especializado → Notificación de solución → Confirmación de solución

Autoservicios

PL.02 Gestión de activos de información

RA-02 Categorización de seguridad

10,000 casos de soporte a incidentes y **3,500** solicitudes de servicio atendidos por año.

PL.05 Gestión de incidentes, resiliencia y pruebas de seguridad

IR-08 Plan de respuesta a incidentes de seguridad

Gestión de incidentes de seguridad

Inteligencia Artificial y los retos de la ciberseguridad

Implementación de herramientas de IA

Modelos de Aprendizaje Asistido y otras soluciones

Modelos de Lenguaje Extendido (*Large Language Models*)

Mayor productividad

Retos ante la IA

Confidencialidad de la información al utilizar soluciones basadas en la nube

La complejidad de las herramientas puede dificultar el entendimiento e identificación de posibles riesgos de seguridad

Los ciberataques habilitados por IA pueden afectar infraestructuras financieras críticas, causando disrupciones masivas

Conclusiones

El Banco de México adoptó un enfoque integral y proactivo, combinando normatividad, controles técnicos, capacitación, coordinación y colaboración institucional para robustecer la ciberseguridad dentro de la institución.

La Dirección de Información del Sistema Financiero (DISF) ha aplicado cabalmente el enfoque del Banco, cerrando las brechas identificadas en la línea base del diagnóstico inicial.

Actualmente la DISF mantiene en sus sistemas y procesos, un elevado nivel de seguridad que le permite garantizar el buen funcionamiento de sus procesos y el adecuado resguardo de la información que administra.