SUPERINTENDENCIA
DE BANCA, SEGUROS Y AFP

República del Perú

SUPERINTENDENCIA
DE BANCA, SEGUROS Y AFP
República del Perú

RESILIENCIA OPERACIONAL EN EL SISTEMA FINANCIERO PERUANO

Perspectivas del Riesgo Operacional en la era de la digitalización

Oscar Basso Winffel – Gerente de Riesgos

Setiembre 2025

Agenda

1. **La gestión del riesgo operacional en un contexto de cambios**
   ¿Cuál es la importancia en un contexto de digitalización?
2. **Importancia de los riesgos de servicios provistos por terceros**
   ¿Qué acciones está tomando la SBS?
3. **La resiliencia operativa frente a cambios imprevistos**
   ¿En un mundo como este, qué importancia tiene “la continuidad del negocio”?
4. **La gestión de la ciberseguridad en un entorno digital**
   ¿Cómo se adapta la industria a las nuevas técnicas de delito cibernético?

¿Ya estamos claros en lo que se se espera de los próximos años?

Las 10 principales predicciones estratégicas para 2024 y los próximos años

1. 2026: los "filtros de carisma" digital nos hacen parecer mejores
2. La productividad de la IA cambia el equilibrio geopolítico
3. El valor real de la neurodiversidad aumenta
4. Las operaciones con conciencia energética suponen una ventaja competitiva o un riesgo de fracaso
5. La IA generativa potencia la modernización de los sistemas heredados
6. El número de robots excede el número de trabajadores humanos
7. Los clientes máquina obligan a los CEO a adoptar nuevos canales
8. La información maliciosa es una amenaza con múltiples frentes
9. Los directores de seguridad de la información (CISO) ganan poder
10. Se forman sindicatos de personas contra las máquinas

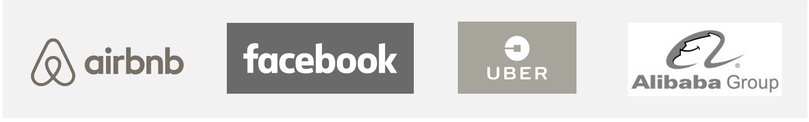
gartner.es

Fuente: Gartner

Gartner.

1

La gestión del riesgo operacional en un contexto de cambios



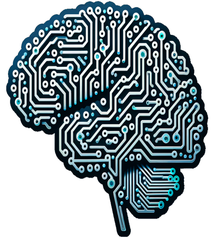
Un nuevo mundo de negocio

Uber	Compañía más grande de taxi.	**Vehículos: 0**
Facebook	Medio de comunicación más popular del mundo.	**Contenido propio: 0**
Alibaba	Comercio mayorista más grande del mundo.	**Inventario: 0**
Airbnb	Mayor proveedor de alojamiento del mundo.	**Inmuebles: 0**
Banca y Microfinanzas		**Agencias: 0**

Un nuevo mundo de negocio

Nuevas tecnologías disponibles: “facilitadoras”

- Nube
- Big data / data analytics
- Inteligencia artificial: bots, automations in finance
- Distributed ledger technology (blockchain, etc.)
- Mobile access y social media
- Identificación y contratación facial y digital



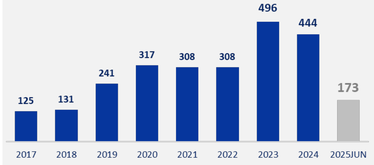
Contexto en el sistema financiero

Más presupuesto a iniciativas de innovación y transformación digital

Menos transacciones de clientes se realizan de manera física (por ventanilla))

Crece la demanda y la oferta de servicios financieros digitales

Nuevos productos/servicios y cambios importantes

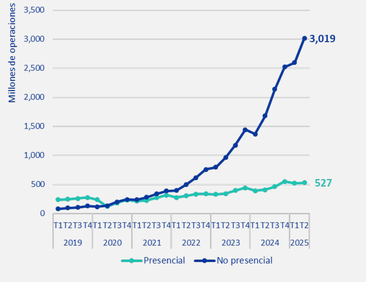


NPCI relacionados a transformación digital:

- Open Banking, uso de las API
- Migración a los servicios en nube
- Billeteras digitales e interoperabilidad
- Tarjetas y cuentas digitales
- *Onboarding* digital y biometría facial
- *Machine learning, Data lake, DataOps.*

Fuente: Elaboración propia.

Operaciones del SF a través de canales de atención



Fuente: Elaboración propia con información provista ASBANC.

Se requiere una gestión de riesgos robusta para los riesgos emergentes internos y externos

El contexto regulatorio internacional se viene adaptando a los cambios, con una visión más enfocada de la gestión de los principales riesgos

Digital Operational Resilience Act **(DORA)**

1. Gestión de riesgos de TIC
2. Reporte de incidentes de TI
3. Pruebas de resiliencia digital
4. Gestión de riesgos de terceros de TIC
5. Intercambio de información

Revisions to the principles for the sound management of operational risk
(Comité de Supervisión Bancaria de Basilea)

"Recurrir a terceros puede ayudar a gestionar costos y mejorar servicios, pero también introduce riesgos que deben ser gestionados."

"El directorio y la alta gerencia son responsables de entender los riesgos operacionales asociados con los acuerdos de tercerización."

"Se deben desarrollar planes de contingencia viables para los servicios externalizados críticos."

"Los contratos y acuerdos de nivel de servicio deben ser exhaustivos, con clara asignación de responsabilidades entre el proveedor y el banco."

Principles for the sound management of third-party risk
(en consulta)

Logrando un balance

	Oportunidad	Riesgo
En el consumidor 	• Inclusión financiera • Servicios más personalizados • Menores costos de transacción • Servicios en menor tiempo	• Seguridad de la información • Protección de datos personales • Interrupción del servicio • Malas prácticas de mercado
En la entidad y el sistema 	• Procesos más eficientes y efectivos • Usos innovadores de la data para evaluación de crédito y estrategias de marketing • Impacto potencial en la estabilidad financiera • Desarrollo del mercado (competencia) • RegTech ➢ **Reducción de gastos operativos**	• Relevancia de riesgo de estrategia • Ataques a ciberseguridad • Riesgos de gestión de terceros • Riesgos de integridad financiera • Riesgos de compliance ➢ **Aumento de costos operacionales**

Cuadro elaborado en base al documento de Basilea: "Sound practices Implications of fintech developments for banks and bank supervisors"

2

Importancia de los riesgos de servicios provistos por terceros

Impulsadas por la digitalización las empresas requieren niveles de especialización que encuentran en terceros

Ello puede generar una mayor eficiencia y una mejor propuesta de valor, aunque también genera retos y riesgos importantes

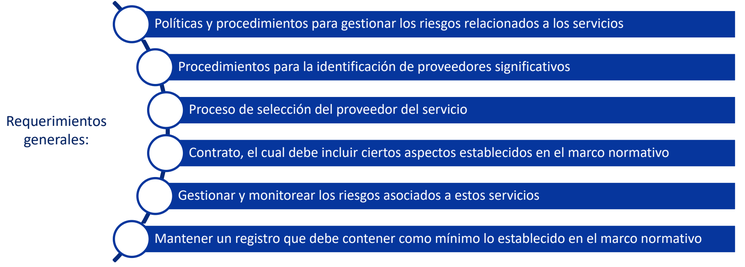
Principales beneficios

- Flexibilidad
- Escalabilidad
- Ahorro
- Eficiencia
- Especialización
- Innovación

Principales riesgos

- Operacional
- Estratégico
- De reputación
- De concentración
- De cumplimiento

La regulación establece requerimientos mínimos para fortalecer la gestión de los riesgos de terceros



La mayor dependencia de terceros genera múltiples retos, los cuales deben ser abordados con nuevas herramientas y estrategias

Retos identificados en la supervisión

- Heterogeneidad y volumen de los proveedores que dificulta su evaluación.
- Distinta aplicación de los criterios para evaluar a los terceros a lo largo de la empresa.
- Servicios complejos y especializados que dificultan la supervisión.
- Negociación de contratos con terceros con posición de dominio.
- Falta de alternativas ante falla de determinados servicios especializados.

Expectativas sobre la gestión

- Gestionar los riesgos durante el ciclo de vida del servicio.
- Monitoreo eficaz de procesos y ANS.
- Comprender resiliencia de terceros en entornos operativos y financieros complejos, y planificar acorde a ello.
- Compartir mejores prácticas en el sector.
- **Desarrollar un modelo de gobernanza clara.**
- **Aplicar tecnologías que hagan eficiente los procesos.**

Responsabilidad de las tres líneas de defensa

IA

Gestión de Datos

Se espera una gestión más intensiva en los proveedores críticos, a través de una gestión del ciclo de vida del servicio

Fuente: BIS

Planificación: *Definir necesidad, objetivos y riesgos.*

Debida diligencia: *Evaluar antecedentes, capacidad operativa y de cumplimiento.*

Selección: *Comparar alternativas y elegir.*

Contratación: *Formalizar acuerdos y responsabilidades*

Monitoreo continuo: *Supervisar el desempeño, cumplimiento y riesgos.*

Terminación: *Cerrar la relación de manera ordenada, gestionar los riesgos de salida.*

3

La resiliencia operativa frente a cambios imprevistos

La creciente digitalización del sector financiero tiene un impacto en la capacidad de resiliencia operacional de las instituciones

Impactos positivos

- Reducción de la dependencia de la infraestructura física
- Automatización y eficiencia en la gestión de procesos críticos.
- Uso intensivo de analítica avanzada y monitoreo en tiempo real.
- Refuerzo de la resiliencia tecnológica basada en la desconcentración geográfica (almacenamiento en la nube).

Impactos negativos

- Surgimiento de nuevas vulnerabilidades (tercerización, BaaS, etc.)
- Mayor dependencia de terceros críticos (nube, procesamiento de datos, etc.)
- Complejidad creciente en la gestión de incidentes con rápida escalabilidad.
- Intensificación en la presión regulatoria y reputacional ante interrupciones.

La creciente digitalización fortalece la resiliencia mediante automatización, analítica avanzada y reducción de dependencias físicas, pero al mismo tiempo genera nuevas vulnerabilidades y dependencias críticas.

La proporción del tiempo de interrupción causado por fallas de componentes tecnológicos y de proveedores se ha incrementado

Fuente: Reporte CN-A

Fuente: Reporte CN-A

* Datos del año 2025 son con corte a junio

La SBS ha establecido nuevas disposiciones para la gestión de continuidad de canales digitales (Res. SBS N° 814-2025)

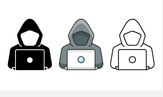
Entendimiento de la organización	• **Identificar** productos y servicios priorizados en canales digitales y **establecer un TOR** para c/u. • **Evaluar los riesgos de interrupción en canales digitales**, incluyendo la identificación de **componentes tecnológicos** que ante falla afectaría la continuidad de productos y servicios priorizados. • **Aprobación de las condiciones normales** de operación para cada producto y servicio priorizado por canal digital, por parte del Directorio o Comité de Riesgos.
Estrategias y planes	• **Implementar un sistema de monitoreo** del funcionamiento de canales digitales. • **Identificar / contar con canales o esquemas de atención alternativos**. • **Desarrollar protocolos para atender fallas tecnológicas** (plan de recuperación de servicios de TI) • **Desarrollar disposiciones para la comunicación oportuna** de incidentes o fallas significativas a grupos de interés (incluidos los usuarios) y canales alternativos disponibles.
Otras disposiciones	• **Realizar pruebas anuales** para verificar la efectividad de las estrategias definidas. • **Mantener un registro de eventos de interrupción** de productos y servicios priorizados ofrecidos a través de canales digitales ≥ 30 minutos

También ha establecido nuevas disposiciones para asegurar la entrega de servicios prioritarios a través de los principales canales digitales

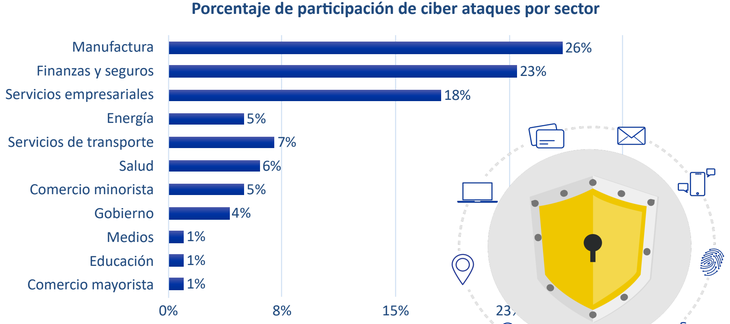
Alcance	Empresas con los canales digitales: **banca por internet, aplicativo móvil o billeteras digitales** *(principales canales digitales)*; a través de los que ofrezcan servicios de **transferencias, pagos interoperables, pago de planillas** o **a proveedores** *(servicios prioritarios).*
Reportes CD	• Para comunicar condiciones normales de productos y servicios, y canales alternativos. • Deben ser aprobados por Directorio o Comité de Riesgos. • **Remisión anual a SBS**. **Modificaciones** deben reportarse en un máximo **7 días**.
TOR y eventos de interrupción	• Servicios prioritarios en principales canales digitales deben: ○ Considerar un **TOR ≤ 3 horas** en **empresas sistémicas** y **≤ 5 horas** en **otras empresas.** ○ **No deben interrumpirse** entre 06:00 am y 10:00 pm, por **periodos mayores a los antes mencionados** en un **día**, de forma continua como acumulada. • Deben **ejecutar pruebas anuales para verificar** cumplimiento de **TOR**. Informes de resultados deben ser remitidos como parte del IG-ROp.
Estrategias de continuidad	Deben contemplar desarrollo de **procedimientos** que, en caso de interrupciones, permitan **continuar ofreciendo servicios prioritarios**; y/o **permitir** a usuarios **disponer** de sus depósitos a través de otros canales.

4

La gestión de la ciberseguridad en un entorno digital



Aun siendo altamente regulado y supervisado, el sector financiero experimenta permanentemente ciberincidentes

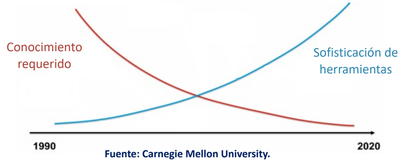


Fuente: IBM X-Force 2025 Threat Intelligence Index

Aun siendo altamente regulado y supervisado, el sector financiero experimenta permanentemente ciberincidentes

Las ciberamenzas son un riesgo emergente en el entorno digital que afecta a las entidades financieras como a los usuarios finales

Los ciberdelincuentes requieren de menos conocimiento y disponen de herramientas más sofisticadas



Fuente: Carnegie Mellon University.

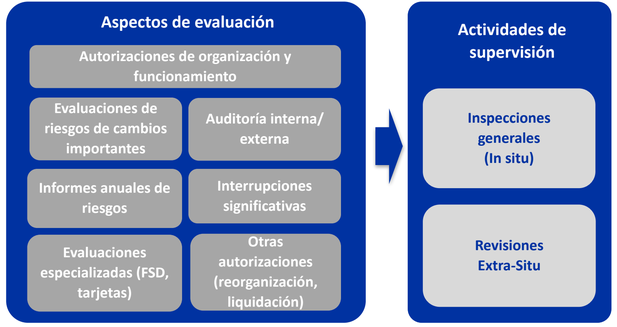
Afectan a entidades y clientes	• Los ciberataques no solo afectan la infraestructura de las instituciones financieras, Derivan en fraudes directos contra los usuarios (robo de credenciales, estafas en canales digitales).
Generan desconfianza	• Cada incidente visible genera desconfianza en los servicios financieros digitales, lo que puede frenar la adopción de banca electrónica, pagos móviles y nuevas soluciones fintech.
Presentan una mayor sofisticación	• Las amenazas evolucionan hacia phishing, smishing y fraudes en comercio electrónico, aprovechando la falta de educación digital de los usuarios, y bajas medidas de control en las instituciones financieras.

Organismos internacionales relevantes para la ciberseguridad en el sistema financiero

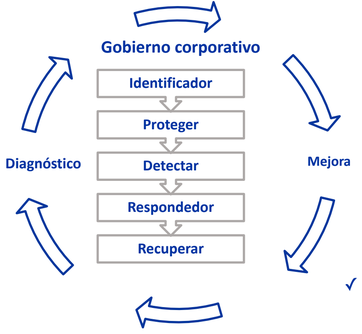
Organismo	Rol en la Ciberseguridad Financiera
BIS (Banco de Pagos Internacionales) – Comité de Supervisión Bancaria de Basilea (BCBS)	Principios para la resiliencia operativa.
FSB (Financial Stability Board)	Recomendaciones sobre ciberseguridad y gestión de riesgos.
IOSCO (Organización Internacional de Comisiones de Valores)	Establece estándares de ciberresiliencia para mercados de valores.
IAIS (Asociación Internacional de Supervisores de Seguros)	Promueve estándares de ciberseguridad para supervisores de seguros.
OCDE (Organización para la Cooperación y el Desarrollo Económicos)	Publica directrices sobre seguridad digital y protección de infraestructuras críticas.
IMF (Fondo Monetario Internacional)	Evalúa riesgos cibernéticos en el sistema financiero global y asesora a países sobre políticas de resiliencia.
ISO (Organización Internacional de Normalización)	Desarrolla normas internacionales de ciberseguridad y relacionados.
ENISA (Agencia de Ciberseguridad de la Unión Europea)	Proporciona guías y buenas prácticas para sectores críticos, incluyendo el financiero.
NIST (Instituto Nacional de Estándares y Tecnología - EE.UU.)	Publica un marco de ciberseguridad ampliamente adoptado como referencia global.

La Regulación de SI y ciberseguridad requiere que las empresas cuenten con un entorno seguro y confiable (Res. SBS N° 504-2021)

Macroproceso de supervisión de ciberseguridad



A partir de este año se realizan verificaciones in-situ a los programas de ciberseguridad en las principales entidades financieras



Reporte incidentes significativos de ciberseguridad

Análisis forense para determinar las causas y gestionar dichos incidentes

Lineamientos para compartir información

- ✓ Seleccionar un marco de referencia
- ✓ **Alcance**
- ✓ **Priorización**
- ✓ **Proporcional**

Además, la seguridad de la información y la ciberseguridad requieren un abordaje en múltiples frentes

Supervisión

- Equipo especializado en la supervisión de ciberseguridad
- Supervisión continua de la ciberseguridad:
  - Vulnerabilidades en el perímetro externo
  - Vulnerabilidades en aplicaciones móviles
  - Factores de autenticación seguros

Desarrollo de Capacidades

- Implementación de un laboratorio para pruebas seguridad (Apoyo de la UIT)
- Herramientas que permiten visualizar el nivel de seguridad de servicios expuestos a internet.
- Herramientas que permiten obtener información local e internacional sobre ciberamenazas.

Cooperación

- Asistencia técnica del Fondo Monetario Internacional
- Asistencia técnica de la Unión Internacional de Telecomunicaciones (UIT)

Principales autoridades del sector financiero

- Instituciones financieras
- Seguros
- Empresas Administradoras de Pensiones(AFP)

- Sistemas de pago
- Instituciones Financieras que Operan en el Sistema de Pagos

- Bolsa de valores
- Cavali
- Agentes de bolsa

Otras autoridades

- Autoridad Nacional de Protección de Datos Personales (MINJUSDH)
- Organismo Supervisor de la Inversión Privada en Telecomunicaciones (OSIPTEL)
- Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (INDECOPI)
- Centro Nacional de Confianza Digital de la Presidencia del Consejo de Ministros (PCM)
- Ministerio del Interior (MININTER)

La SBS está fomentando una estrategia de ciberseguridad específica para sector financiero.

Estrategia nacional de ciberseguridad para el sector financiero

Conclusiones

- El entorno actual es propicio para desarrollar nuevos negocios digitales, pero ello implica la aparición de riesgos que deben ser abordados con nuevas herramientas y con la misma agilidad.
- Hoy en día, la gestión de riesgos de terceros se ha convertido en una tarea más compleja, pero necesaria, que puede beneficiarse de la aplicación de nuevas tecnologías.
- Los cambios regulatorios relacionados a la resiliencia operativa responden a un entorno de mayor riesgo, y una presión creciente del público por servicios siempre disponibles.
- La ciberseguridad requiere adaptabilidad continua y coordinación entre todos los actores del ecosistema financiero para lograr una respuesta efectiva.

BANKING IS NECESSARY

BANKS ARE NOT.

(1994)

Bill Gates

SUPERINTENDENCIA
DE BANCA, SEGUROS Y AFP
República del Perú

Gracias

Los Laureles 214,
San Isidro, Lima – Perú
Central telefónica: (01) 630-9000
www.sbs.gob.pe