



CLAIN 2023 
XXVII Congreso Latinoamericano de
Auditoría Interna y Evaluación de Riesgos

Importancia de la Auditoría Interna en el apoyo al control de los riesgos emergentes

20
23

XXVII CONGRESO LATINOAMERICANO

**AUDITORÍA INTERNA
Y EVALUACIÓN DE RIESGOS**
LA ANTIGUA GUATEMALA, GUATEMALA



Conforme las empresas **aceleran su transformación digital** para mantenerse competitivas, en el entorno actual de innovaciones tecnológicas sin precedentes, **enfrentan riesgos que podrían afectar su continuidad.**

En ese nuevo contexto, la Auditoría Interna **es un pilar fundamental** que coadyuva a la **mejora en los procesos de gestión de riesgos y gobierno corporativo**, lo que requiere una **continua adaptación y preparación** que contribuyan en la **identificación de riesgos emergentes** y en **prácticas de auditoría interna más eficientes.**

Contenido



PANORAMA GLOBAL: INNOVACIÓN TECNOLÓGICA EN EL ÁMBITO FINANCIERO

1



RIESGOS EMERGENTES EN LAS INNOVACIONES TECNOLÓGICAS Y GESTIÓN DE LA CIBER RESILIENCIA

2



ROL DE LA AUDITORÍA INTERNA EN LA GESTIÓN DE RIESGOS EMERGENTES

3



Panorama global: Innovación tecnológica en el ámbito financiero



Tendencias tecnológicas financieras



Adecuación de los modelos de negocio



Tercerización de los servicios de TI



Tendencias tecnológicas financieras



Principales 10 tendencias tecnológicas bancarias en 2023



Fuente: StartUs Insight, febrero 2023

+26,000
fintechs operan internacionalmente

\$4 billones
valor estimado del e-commerce global

\$174 mil millones
Gasto esperado en ciberseguridad para 2024

30%
Clientes bancarios usaron al menos un servicio fintech

\$2 mil millones
Ingresos de la banca digital europea para 2026

Fuente: Zai

Panorama Fintech en Latinoamérica 2023

- ✓ Créditos
- ✓ Aceptación de pagos
- ✓ Gestión de patrimonio e inversiones
- ✓ Cripto y blockchain
- ✓ Soluciones business to business
- ✓ Insurtech
- ✓ Neobancos y billeteras
- ✓ Pagos transfronterizos
- ✓ Open banking
- ✓ Facilitadores de servicios

Fuente: Flagship Advisory Partners

Áreas de servicios de las 250 fintech más prometedoras del mundo en 2022

33 países
Procesamiento de pagos y redes (13 %), seguros (10 %), criptomonedas (10 %), core bancario e infraestructura (8 %)

Fuente: CB Insights

Impacto de las 10 principales tendencias tecnológicas bancarias

Inteligencia artificial



- Servicios bancarios
- Costos operativos
- Detección y fraude
- Aplicaciones AML y controles KYC
- Modelos de credit scoring
- Análisis de documentos
- Gestión del cumplimiento

23%

Open banking (API)

- Servicios financieros personalizados
- Acceso a datos financieros de clientes
- Cuentas bancarias en una sola plataforma
- Verificación del cliente
- Banca como servicio



19%

Banca hiper personalizada



- Banca omnicanal
- Herramientas de asesoría financiera

13%

Blockchain



- Transparencia y seguridad
- Automatización de transacciones
- Contratos inteligentes
- Pagos entre pares
- Finanzas descentralizadas

12%

Seguridad cibernética



8%

Tecnologías inmersivas



7%

Banca de las cosas

- Automatización de recopilación de datos en tiempo real
- Detección de fraudes



8%

Automatización de procesos bancarios



6%

Neobanca



3%

Computación cuántica



1%

Panorama global: Innovación tecnológica en el ámbito financiero



Tendencias tecnológicas financieras



Adecuación de los modelos de negocio



Tercerización de los servicios de TI



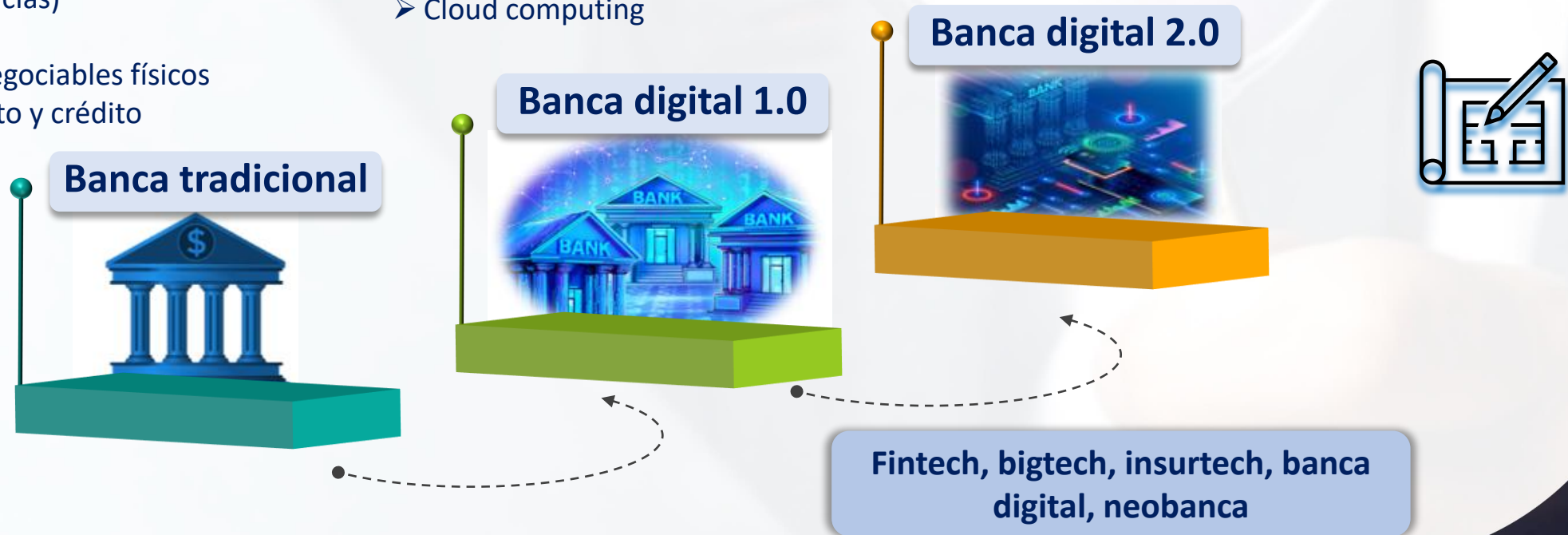
Adecuación de los modelos de negocio



- Productos y servicios cara a cara con el cliente (oficinas centrales, sucursales, agencias)
- ATM
- Instrumentos negociables físicos
- Tarjetas de débito y crédito

- Operaciones a través de redes sociales, banca móvil, en línea
- Plataformas y apps
- Pagos digitales
- Billeteras electrónicas
- Cloud computing

- Experiencia omnicanal
- IA
- Procesos automatizados y robotizados
- Blockchain
- IoT
- Banca abierta
- Biometría
- Realidad aumentada



Adecuación de los modelos de negocio en la banca local

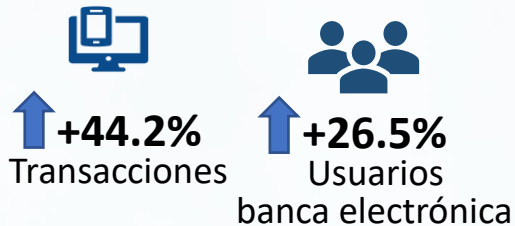


Condiciones en curso

Aumento en la transaccionalidad por canales electrónicos

% Transacciones		
2020	2021	2022
52.8%	60.1%	67.6%

2021-2022



2020-2022



Servicios de innovación



Remesas en línea y transferencias internacionales

Apps pago servicio de parqueo



Billeteras electrónicas



Apertura de cuentas de forma electrónica



Desafíos

Enfoques legales y regulatorios

Tecnologías disruptivas

Demandas y preferencias de nuevas generaciones

Cambios demográficos, socioeconómicos, ambientales

- Infraestructura financiera y tecnológica
- Protección al consumidor
- Capacidad financiera
- Datos y ciberseguridad

Panorama global: Innovación tecnológica en el ámbito financiero



Tendencias tecnológicas financieras



Adecuación de los modelos de negocio



Tercerización de los servicios de TI



Tercerización de los servicios de tecnología de la información

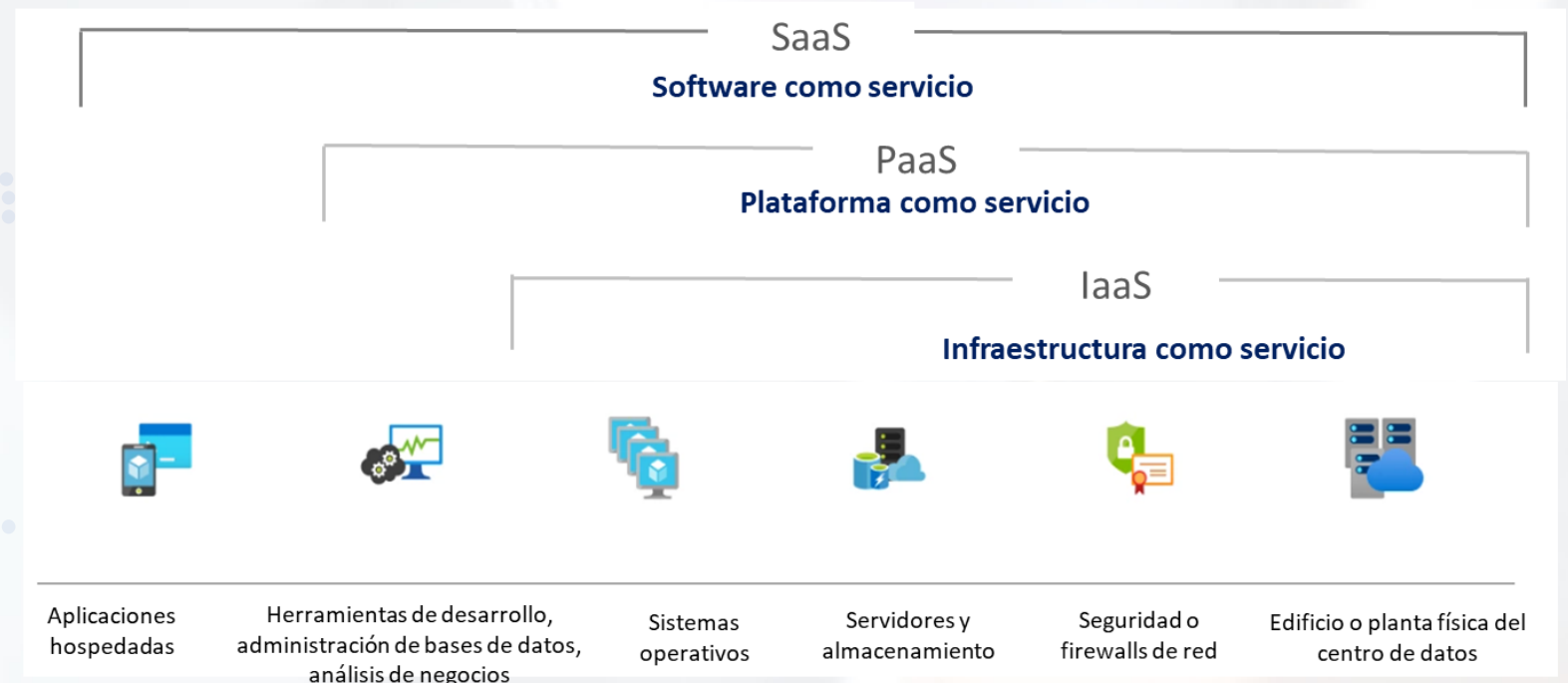


Principales tendencias en 2023

- 1 Tecnologías emergentes
- 2 Migración a la nube
- 3 Optimización de infraestructura
- 4 Ciberseguridad

Fuente: Jelvix

Procesamiento y almacenamiento en la nube



Fuente: Microsoft



Riesgos emergentes en las innovaciones y gestión de la ciber resiliencia



Intensificación de ciberataques a nivel global



Gestión de la ciber resiliencia y mejores prácticas

Intensificación de ciberataques a nivel global



600% Aumentó el cibercrimen debido a la pandemia

58% de los ataques cibernéticos a los estados se originaron en Rusia.

98% de los delitos cibernéticos se basan en la ingeniería social

1,270,883 ataques de phishing en el 3T de 2022, el peor trimestre observado por APWG. **23.2%** de los cuales fueron contra el sector financiero

61% Subieron los ataques de phishing de marzo a octubre 2022

82% en ataques de phishing y robo de credenciales. La causa principal: el elemento humano



Segunda industria objetivo en 2022: **servicios financieros**

38% aumentó de ciberataques en todo el mundo, por semana en redes corporativas, en 2022

1% del PIB mundial Costo equivalente del cibercrimen

255 millones incidentes de phishing en 2022

US\$10.5 trillones anuales

Costo estimado de los delitos cibernéticos para 2025

US\$2.5 millones Promedio del costo de un ataque de malware a una empresa (incluido el tiempo para resolverlo)

US\$6 trillones

Costo anual mundial estimado del delito cibernético

US\$12.3 millones

costaron, **11,395** incidentes en el 1S de 2022, con un aumento de ataques de phishing del **48%**

150 millones

de ataques de phishing se bloquean diariamente



Estadísticas de ciberataques a bancos a nivel local



2020 - 2022

↑ +161%

ciberataques de 2020 a 2022

212 millones

Ciberataques en 2022

↑ +5.0%

Ciberataques 2021 vrs. 2022

Incidentes a mayo 2023

+1,000

Sitios de suplantación identificados

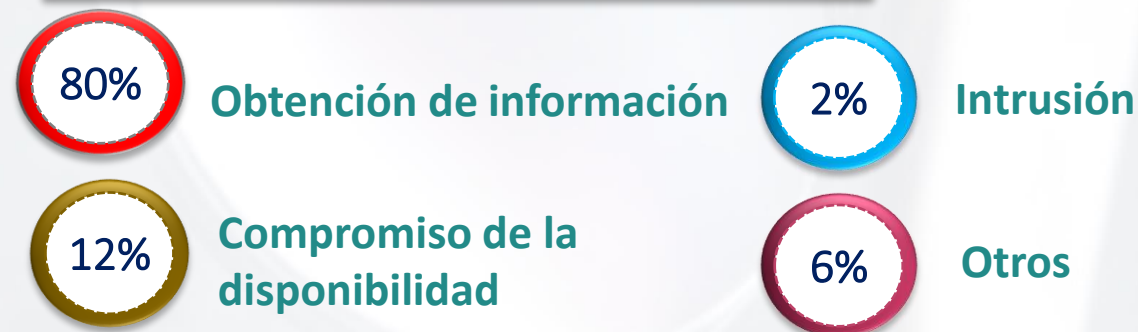
+245,000

clientes afectados

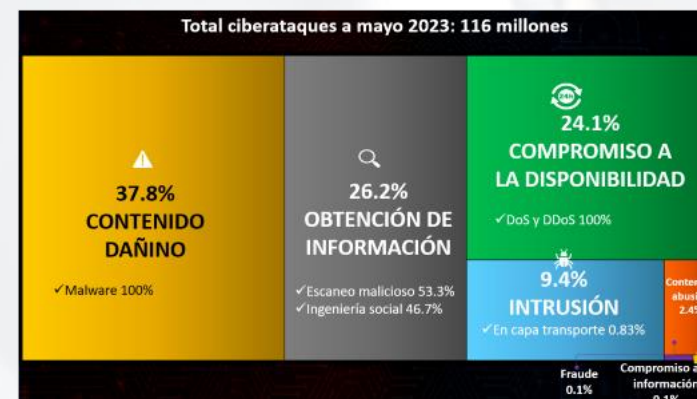


Fuente: Información remitida por las entidades bancarias.

Principales ciberataques 2022



A mayo 2023



Total ciberataques a mayo 2023: 116 millones



37.8%

CONTENIDO DAÑINO

✓ Malware 100%



26.2%

OBTENCIÓN DE INFORMACIÓN

✓ Escaneo malicioso 53.3%
✓ Ingeniería social 46.7%



24.1%

COMPROMISO A LA DISPONIBILIDAD

✓ DoS y DDoS 100%



9.4%

INTRUSIÓN

✓ En capa transporte 0.83%

Contenido abusivo
2.4%

Fraude
0.1%

Compromiso a la información
0.1%

Riesgos emergentes en las innovaciones y gestión de la ciber resiliencia



Intensificación de ciberataques a nivel global



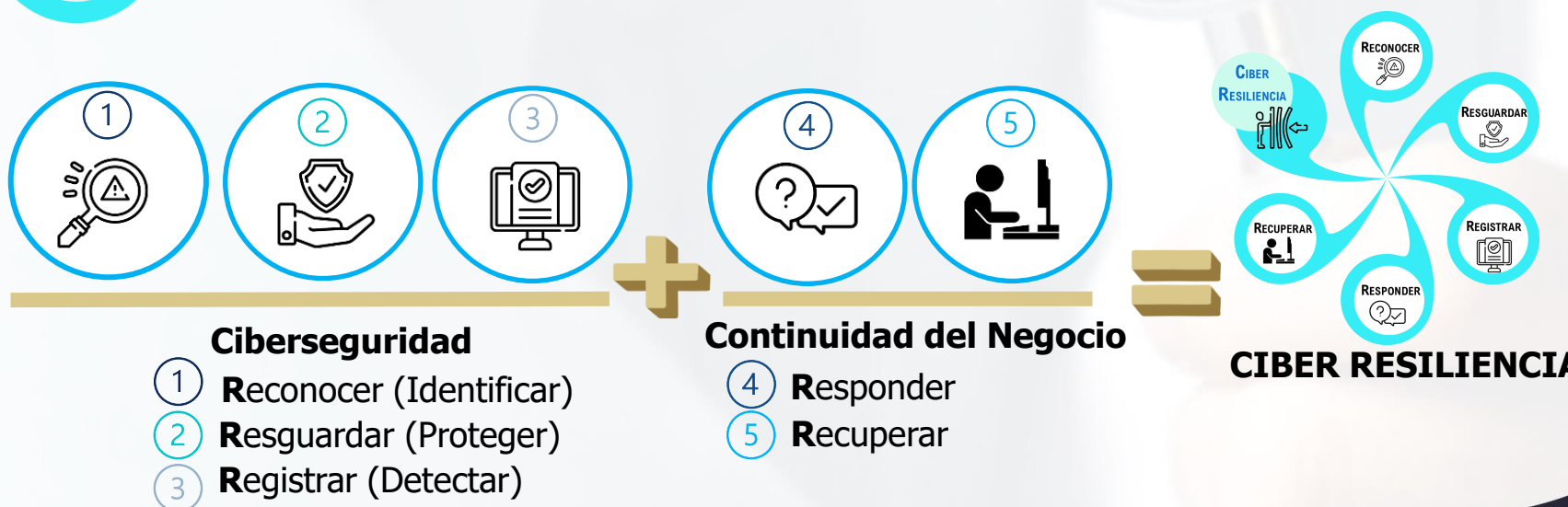
Gestión de la ciber resiliencia y mejores prácticas

Gestión de la ciber resiliencia y mejores prácticas a nivel internacional



Es la habilidad de una organización para adaptarse a las condiciones cambiantes, aprovechando sus capacidades digitales para prepararse, resistir y recuperarse rápidamente ante una interrupción o incidente de ciberseguridad, mientras se crece y se capitalizan las condiciones cambiadas.

Adaptación propia – CISA – RSA - ISO 22316



Gestión de la ciber resiliencia y mejores prácticas a nivel internacional



Marcos de Referencia y Mejores Prácticas



BASILEA

Principios de Riesgo Operacional
P10. Tecnología de la información y comunicaciones
Principios de resiliencia operacional



Reglamento de Resiliencia Operacional Digital



Estándar de seguridad de datos para tarjetas de pago



Riesgo Cibernético en la banca central – Encuesta 2021



Gestión de riesgos de la banca central, Fintech y Ciberseguridad – Documentos de trabajo -



Fortalecimiento de la regulación local



Organización para la administración del riesgo tecnológico




Oficial de seguridad de la información -CISO- coordina el cumplimiento de políticas, procedimientos y mecanismos de seguridad de la información y ciberseguridad y gestiona los incidentes de seguridad de la información.


Centro de Operaciones de Seguridad -SOC- monitorea y defiende la infraestructura tecnológica de una organización.


Equipo de Respuesta a Incidentes de Seguridad Informática -CSIRT responde a los incidentes.

Aspectos fortalecidos para la Admón. del Riesgo Tecnológico (2020-2021)

 **Organización para la gestión**

 **Plan de recuperación ante desastres y plan de pruebas**

 **Ciberseguridad**

 **Procesamiento y almacenamiento**

 **Contratación de servicios con terceros**



Elementos que se consideran en la supervisión del riesgo tecnológico



Gestión de riesgos

Gobierno corporativo



Supervisión del rol de la AI

Examina la efectividad de la administración integral de riesgos, del sistema de control interno y del gobierno corporativo, para agregar valor y mejorar las operaciones de la entidad.

Garantiza que los controles internos existentes son adecuados para mitigar los riesgos y que los procesos de gobierno son eficaces y eficientes.

Evalúa el cumplimiento de los objetivos, políticas y procedimientos aplicados en la gestión, el control y el gobierno.



CISO



SOC



CSIRT

Rol de la Auditoría Interna en la gestión de riesgos emergentes



Consideraciones regulatorias en el ámbito del sector financiero local

Consideraciones regulatorias en el ámbito del sector financiero local

Funciones a cargo de la Auditoría Interna:

- ✓ Evaluar, entre otros, la idoneidad y efectividad de las políticas y procedimientos de gobierno corporativo y del sistema de control interno.
- ✓ Velar por la eficacia de procesos de gestión integral de riesgos.
- ✓ Agregar valor
- ✓ Contribuir a la mejora en el desempeño de las entidades.



Enfoque en riesgos de la Auditoría Interna

Auditoría Interna con enfoque en riesgos

4 ejes prioritarios de auditoría interna en el sector bancario:

1. Identificar, seleccionar y evaluar los riesgos más significativos
2. Definir los
3. Procesos (política de riesgos, gobierno y control)
4. Calidad de sistemas de información que apoyan la gestión de riesgos

Acciones con agilidad:

- Mejorar en los procesos de gobierno, control y gestión de riesgos
- Tener de disposición inteligencia y reportes.

Tecnologías de apoyo

Tendencias en tecnologías de apoyo a la Auditoría Interna

Tecnología	Beneficios que ofrece	Procesos que soporta
Inteligencia Artificial (IA)	Automatización de procesos	Identificación de datos
Big Data	Análisis de grandes volúmenes de datos	Validación
Cloud Computing	Acceso remoto y escalabilidad	Control de flujo de trabajo
Blockchain	Seguridad y transparencia	Procesamiento de transacciones
IoT (Internet of Things)	Conectividad de dispositivos	Monitoreo de activos
Robótica (RPA)	Automatización de tareas repetitivas	Revisión de datos

Consideraciones regulatorias en el ámbito del sector financiero local



Funciones a cargo de la Auditoría Interna:

- Evaluar, entre otras, la idoneidad y efectividad de las políticas y procedimientos de gobierno corporativo y del sistema de control interno.
- Velar por la eficacia de procesos de gestión integral de riesgos.

- ✓ Agregar valor
- ✓ Coadyuvar a la mejora en el desempeño de las entidades

Auditoría Interna con enfoque en riesgos



Resiliente

Digital

Ágil

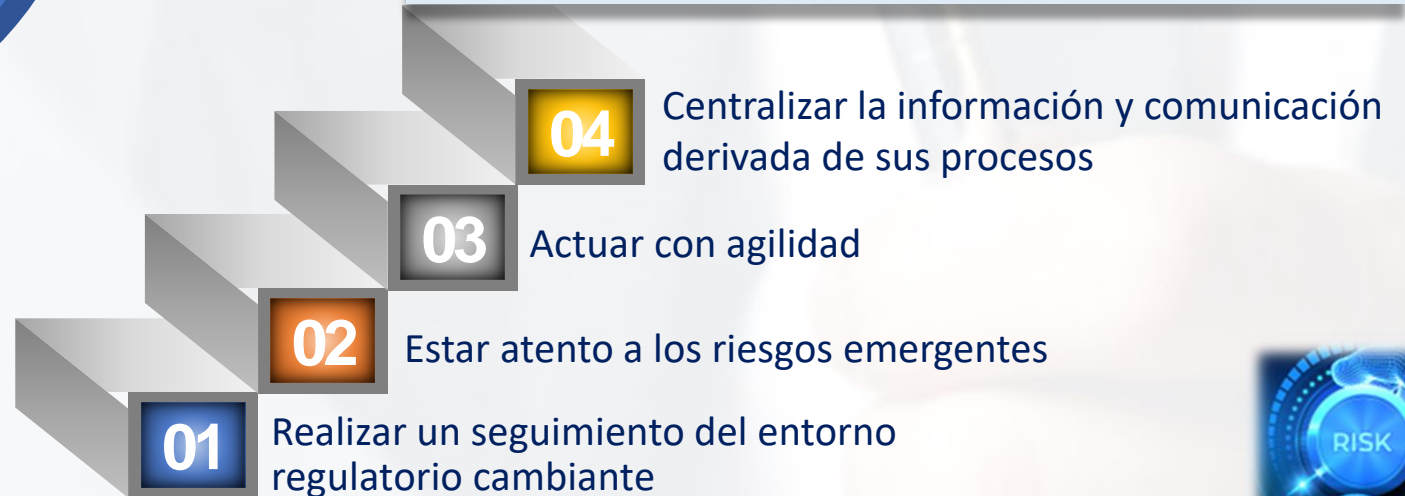
- ✓ Con base a riesgos para determinar prioridades
- ✓ Recursos (cantidad y experiencia) adecuados
- ✓ Visión prospectiva



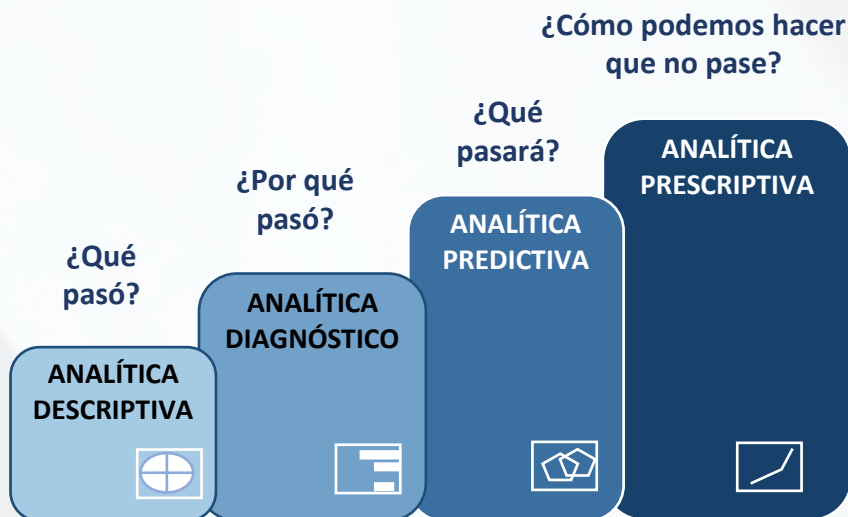
- ✓ Mejoras en los procesos de gobierno, control y gestión de riesgos
- ✓ Toma de decisiones estratégicas y operativas

- ✓ Identificación, alineación y evaluación de los riesgos más significativos
- ✓ Evaluación de:
 - Procesos (gestión de riesgos, gobierno y control)
 - Calidad del sistema de resiliencia operativa y gestión de crisis
 - Plan de continuidad de negocio y recuperación ante desastres
- ✓ Inclusión de riesgos emergentes y amenazas clave

4 mejores prácticas de auditoría interna en el sector bancario



Tendencias en tecnologías de apoyo a la Auditoría Interna



Tecnología para una arquitectura de Big data	Procesos que apoyan
Interfaz de programación de aplicaciones (API)	Recopilación de datos
Automatización robótica de procesos (RPA)	Validación
Lago de datos	Gestión de datos no estructurados
Computación en la nube	Procesamiento y almacenamiento
Tableros dinámicos (dashboard)	Visualización e interacción
Machine learning (ML), procesamiento natural del lenguaje (NLP), análisis visual	Análisis de datos





"Las especies que sobreviven no son las más fuertes, ni las más rápidas, ni las más inteligentes; sino aquellas que se adaptan mejor al cambio".

Charles Darwin



¡Muchas gracias!