GRUPO SEGA

Whitepaper estratégico ejecutivo · IA · Curva de Valor

Continuidad operativa en la era del riesgo digital

Cómo proteger identidad, datos, nube, endpoints y operaciones frente a amenazas modernas en Centroamérica.

Audiencia
CEO, COO, CFO, CIO, CISO, gerentes de TI y líderes de negocio.
Alcance
Guatemala, Honduras, El Salvador, Nicaragua, Costa Rica y Panamá.
Enfoque
60% ejecutivo / 40% técnico.
Tesis
La seguridad es una capacidad de continuidad operativa, no un gasto aislado de TI.

Dato de apertura

4.4M

Costo promedio global, en dólares, de una brecha de datos reportado por IBM en 2025.

Fuente: IBM Cost of a Data Breach Report 2025

Contenido

Una lectura ejecutiva para decidir dónde actuar primero.

01 · Resumen ejecutivo

La ciberseguridad ya no protege solamente sistemas. Protege la capacidad de operar.

La transformación digital expandió la superficie de ataque. Las empresas operan en múltiples nubes, conectan usuarios desde cualquier lugar, mueven datos entre aplicaciones SaaS y empiezan a incorporar IA en procesos críticos.

En ese entorno, la seguridad se convierte en una condición para sostener ingresos, continuidad, confianza y cumplimiento. La conversación ya no debe iniciar con herramientas, sino con riesgo: qué puede detener la operación, qué identidades abren puertas críticas, qué datos no pueden exponerse, qué infraestructura está mal configurada y qué controles necesita la IA antes de escalar.

Este whitepaper propone un marco de cinco capas para orientar decisiones ejecutivas: riesgo, identidad, datos, infraestructura e IA segura. El objetivo no es promover una pila tecnológica específica, sino construir una ruta práctica para reducir exposición, priorizar inversión y acelerar respuesta.

02 · Economía del riesgo digital

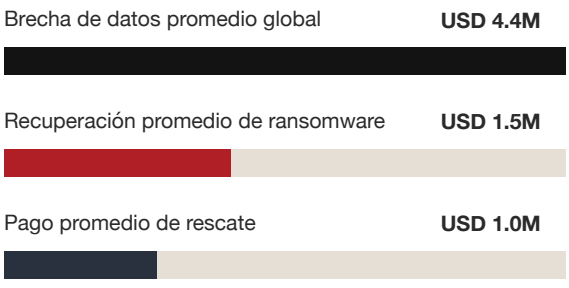
El valor de la seguridad se demuestra cuando traduce riesgo en impacto financiero, continuidad y velocidad de respuesta.

La ciberseguridad genera valor cuando reduce la probabilidad de interrupción, disminuye el costo de respuesta, protege ingresos, evita exposición de datos y acelera la recuperación.

El argumento ejecutivo no debe limitarse a “prevenir ataques”. Debe mostrar cómo la seguridad preserva la capacidad de operar bajo presión. Los datos recientes permiten construir una narrativa cuantitativa clara: una brecha de datos puede costar millones de dólares; el ransomware combina rescate, recuperación y disrupción; los ataques de identidad siguen explotando contraseñas débiles; y la IA en seguridad puede reducir costos y tiempos cuando se implementa con gobierno.

Costo financiero de eventos críticos

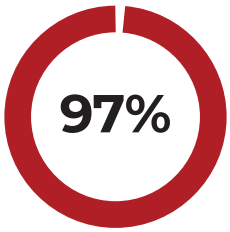
Comparación ejecutiva de referencias globales para dimensionar exposición económica.



Fuentes: IBM Cost of a Data Breach Report 2025; Sophos State of Ransomware2025.

Identidad: el punto de entrada más predecible

Microsoft reporta que 97% de los ataques de identidad observados fueron password spray, una técnica que explota contraseñas débileso o reutilizadas.



IMPLICACIÓNEJECUTIVA

La inversión en MFA resistente a phishing, passwordless, acceso condicional y gobierno de privilegios puede reducir una de las rutas de ataque más frecuentes y automatizables.

La identidad debe gestionarse como una capa de continuidad operativa: si una cuenta crítica cae, el impacto puede propagarse a datos, aplicaciones, nube y procesos centrales.

IA y automatización reducen costo y tiempo

IBM reporta que las organizaciones con uso extensivo de IA y automatización en seguridad tuvieron USD 1.9M menos en costos de brecha frente a organizaciones sin estas capacidades.

$1.9M

Ahorro promedio asociado al uso extensivo de IA y automatización en seguridad.

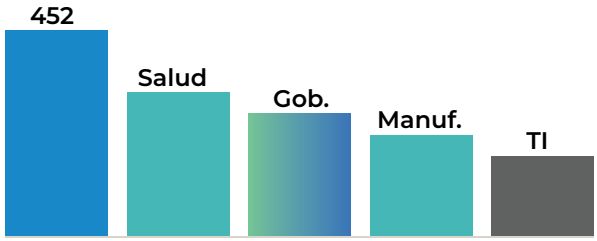
80

Días menos en el ciclo de brecha reportados por IBM para organizaciones con IA y automatización extensiva.

La oportunidad no está en "usar IA" de forma genérica, sino en acelerar triage, correlación, investigación, priorización y respuesta sin perder trazabilidad ni control.

Ransomware regional: presión creciente en LAC

Recorded Future registró 452 incidentes de ransomware que afectaron a América Latina y el Caribe en 2025.



Nota: las barras sectoriales son cualitativas para representar exposición relativa; el dato cuantitativo citado es el total regional.

Cadena de valor de la inversión en seguridad

El valor no aparece en una sola métrica. Se acumula cuando la organización reduce exposición, limita movimiento lateral, protege datos, acelera respuesta y mejora recuperación.

01 ↓
Exposición

Menos credenciales vulnerables, accesos excesivos y configuraciones débiles.

02 ↑
Visibilidad

Mayor cobertura sobre identidad, datos, endpoint, SaaS y nube.

03 ↓
Tiempo

Menor tiempo de detección, investigación, contención y recuperación.

04 ↓
Costo

Menor costo de brecha, menor interrupción y menor esfuerzo manual.

05 ↑
Confianza

Mayor resiliencia, cumplimiento y capacidad de operar bajo presión.

El riesgo moderno no entra por una sola puerta.

Ransomware, phishing avanzado, infostealers, abuso de identidad, configuraciones cloud débiles y shadow AI forman una cadena de riesgo, no eventos separados.

El atacante moderno rara vez empieza con un ataque sofisticado visible. Con frecuencia comienza por mapear activos expuestos, comprar credenciales, probar contraseñas reutilizadas, abusar de accesos remotos o explotar vulnerabilidades conocidas que no fueron corregidas a tiempo.

La pregunta ejecutiva no es "¿tenemos herramientas de seguridad?", sino "¿sabemos qué puede detener la operación y qué tan rápido podemos contenerlo?".

VECTOR	QUÉ BUSCA EL ATACANTE	IMPLICACIÓN EJECUTIVA
Credenciales comprometidas	Acceder como usuario legítimo y moverse lateralmente.	La identidad debe tratarse como control de riesgo de negocio.
Ransomware y extorsión	Cifrar, exfiltrar y presionar con interrupción o exposición pública.	Continuidad, backups, respuesta y comunicación de crisis son capacidades críticas.
Datos sensibles	Extraer información con valor financiero, regulatorio o reputacional.	Sin clasificación y DLP, la organización no sabe qué está realmente protegiendo.
Nube y endpoints	Explotar configuraciones débiles, permisos excesivos o dispositivos vulnerables.	La seguridad debe operar con visibilidad unificada y gestión continua de exposición.
IA no gobernada	Exponer datos, automatizar fraude o comprometer modelos y aplicaciones.	La IA requiere controles de acceso, política, auditoría y monitoreo desde el diseño.

GRUPO SEGA

04 · Identidad

La identidad es el nuevo perímetro operativo.

En un modelo híbrido, el control más importante no es dónde está el usuario, sino quién es, desde qué dispositivo accede, a qué recurso entra y bajo qué nivel de riesgo.

La dependencia de contraseñas sigue siendo una de las fragilidades más explotables. Los ataques de password spray son efectivos porque combinan automatización, credenciales reutilizadas y controles de acceso insuficientes. Por eso, Zero Trust no debe presentarse como una filosofía abstracta, sino como un conjunto concreto de decisiones: verificar explícitamente, conceder mínimo privilegio y asumir compromiso.

CONTROL	DECISIÓN EJECUTIVA	RESULTADO ESPERADO
MFA moderna	Priorizar usuarios privilegiados y aplicaciones críticas.	Reducir exposición a robo de credenciales y password spray.
Passwordless	Reducir dependencia de contraseñas en escenarios de alto riesgo.	Menor fricción y menor superficie de ataque.
Acceso condicional	Aplicar políticas según usuario, dispositivo, ubicación y sensibilidad.	Control dinámico sin bloquear productividad legítima.
PAM / PIM	Limitar privilegios permanentes.	Menor impacto ante compromiso de una cuenta crítica.

05 · Datos

No se puede proteger lo que no se ha clasificado.

Los datos definen el impacto de un incidente. Un ataque sobre un equipo aislado no tiene la misma gravedad que una fuga de información financiera, expedientes de clientes, propiedad intelectual, credenciales o documentación regulada.

Por eso, la seguridad de datos debe pasar de controles manuales y reactivos a descubrimiento, clasificación, etiquetado, DLP y monitoreo de riesgo interno.

La gobernanza de datos convierte la seguridad en una conversación de prioridades: qué información es crítica, quién puede verla, cómo se comparte y qué ocurre si se expone.

Capacidades mínimas

Inventario de repositorios, clasificación automática, etiquetas de sensibilidad, prevención de fuga, auditoría de accesos y monitoreo de comportamiento anómalo.

Riesgo a evitar

Controles de perímetro fuertes, pero datos sensibles sin clasificación, compartidos en exceso o cargados en herramientas externas sin gobierno.

06 · Infraestructura híbrida

El workplace moderno exige una defensa integrada.

La empresa ya no opera en un único centro de datos. Opera en endpoints, redes remotas, aplicaciones SaaS, nubes públicas, entornos híbridos y dispositivos móviles. Esta fragmentación puede generar puntos ciegos, duplicación de herramientas y alertas desconectadas.

La respuesta debe evolucionar hacia XDR, gestión moderna de endpoints, postura cloud, priorización de vulnerabilidades y automatización de respuesta. La meta no es producir más alertas; es reducir tiempo de detección, tiempo de contención y exposición acumulada.

CAPA	PROBLEMA FRECUENTE	ENFOQUE RECOMENDADO
Endpoint	Dispositivos sin postura consistente o fuera de control operativo.	Gestión moderna, EDR/XDR y políticas de cumplimiento.
Cloud	Permisos excesivos, configuraciones débiles y APIs expuestas.	Posture management, seguridad de workloads e identidad cloud.
Aplicaciones SaaS	Accesos no monitoreados y compartición excesiva de información.	CASB, DLP, gobierno de aplicaciones y monitoreo de actividad.
Operaciones	Alertas aisladas sin correlación ni playbooks.	XDR, SIEM, automatización y respuesta coordinada.

07 · IA segura

La IA acelera la defensa, pero también amplifica el riesgo.

El dilema no es adoptar o no adoptar IA. Es adoptarla con controles proporcionales a su acceso, autonomía y exposición de datos.

En seguridad, la IA puede ayudar a resumir incidentes, priorizar alertas, enriquecer investigaciones, asistir a analistas, automatizar playbooks y reducir tiempos de respuesta. Pero la IA también introduce riesgos de shadow AI, fuga de información, prompts con datos sensibles, accesos excesivos y modelos o aplicaciones sin control suficiente.

IA como acelerador defensivo

El valor operativo está en reducir carga manual y acelerar análisis, no en reemplazar el criterio del equipo de seguridad.

$1.9M Ahorro promedio asociado al uso extensivo de IA y automatización en seguridad.

80 Días menos en el ciclo de brecha reportados por IBM para organizaciones con IA y automatización extensiva.

IA como superficie emergente

Sin gobierno, la IA puede convertirse en un nuevo canal de exposición de datos, accesos y decisiones.

13% de organizaciones reportaron brechas de modelos o aplicaciones de IA, según IBM.

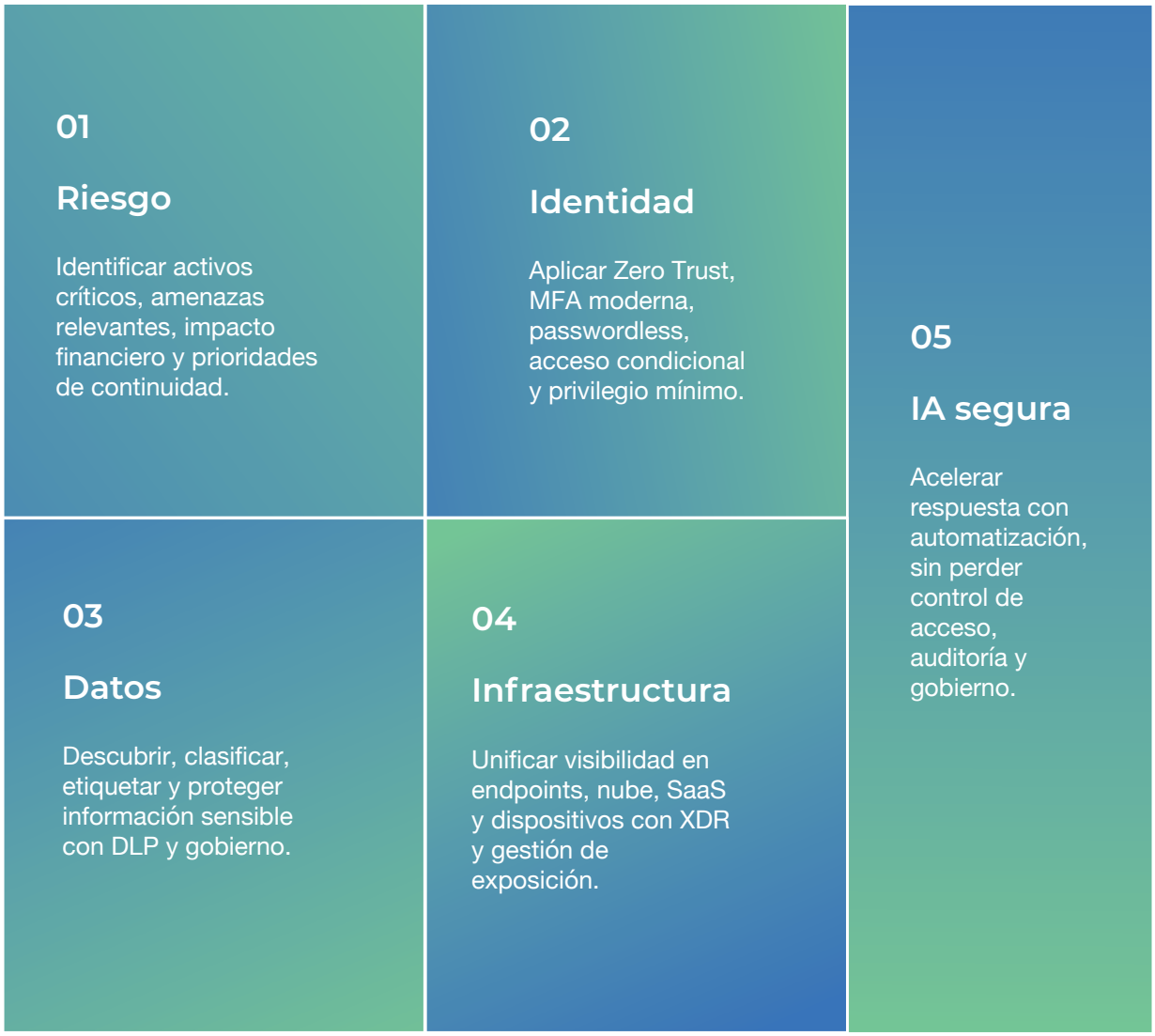
97% de esas organizaciones no tenían controles adecuados de acceso a IA.

Fuente: IBM Cost of a Data Breach Report 2025.

08 · Framework recomendado

Modelo de cinco capas para resiliencia digital.

El marco conecta la narrativa de riesgo con decisiones ejecutables: entender exposición, controlar acceso, proteger datos, asegurar infraestructura y operar defensa aumentada con IA.

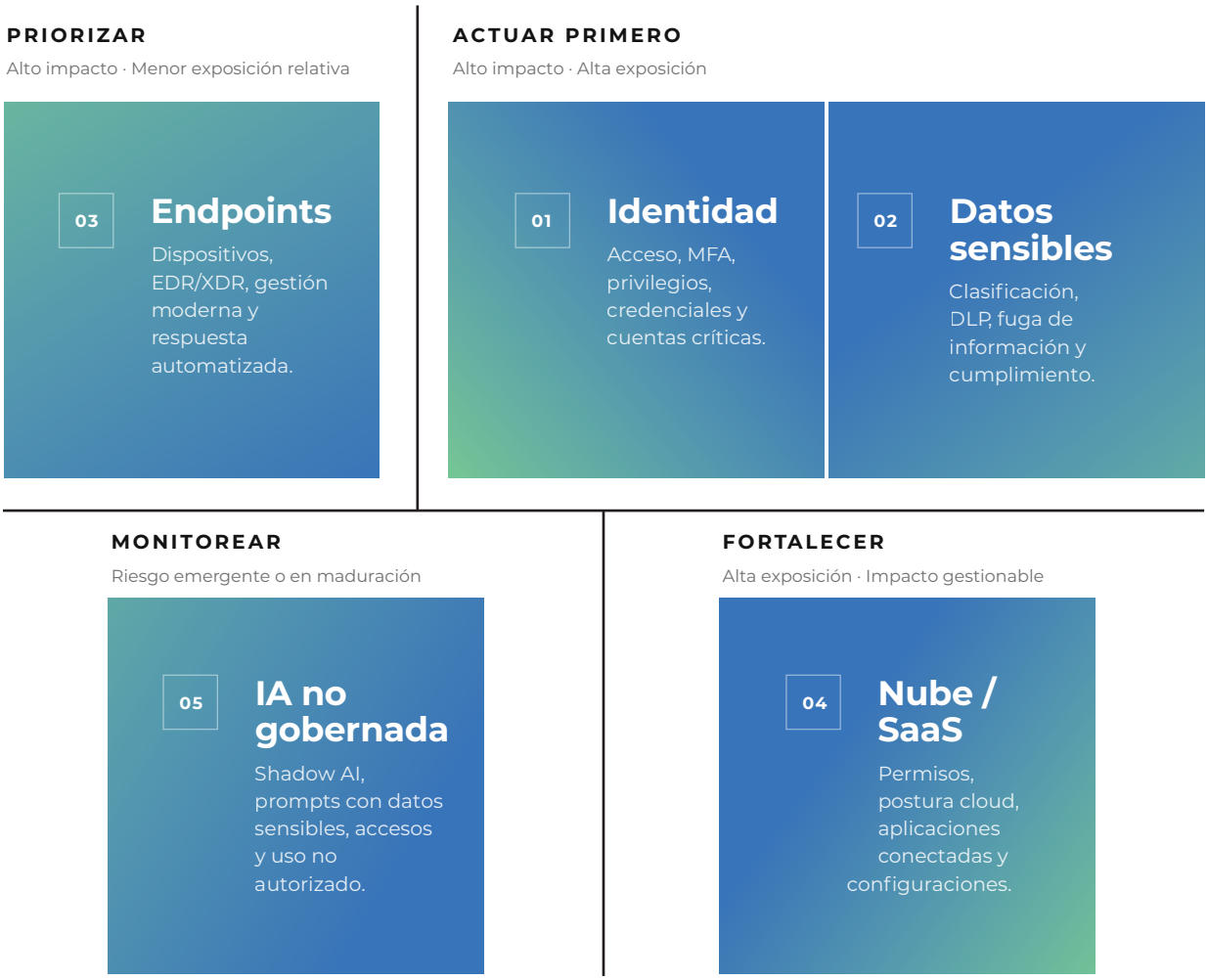


09 · Mapa ejecutivo de exposición

Priorizar no es elegir herramientas. Es decidir qué riesgo reducir primero.

El mapa de exposición organiza los dominios críticos según dos criterios ejecutivos: impacto potencial en el negocio y nivel de exposición actual.

La lectura es simple: los dominios ubicados en “Actuar primero” combinan alta exposición y alto impacto sobre continuidad operativa, cumplimiento, reputación y pérdida financiera.



Exposición actual

Lectura ejecutiva

Identidad y datos sensibles deben tratarse como las dos prioridades iniciales porque concentran exposición, impacto financiero y capacidad de propagación del incidente.

Decisión recomendada

Iniciar con controles de acceso, privilegios, clasificación de información y visibilidad integrada antes de escalar automatización o IA defensiva.

Prioridades derivadas del mapa

PRIORIDAD	DOMINIO	POR QUÉ IMPORTA	PRIMERA ACCIÓN RECOMENDADA
1	**Identidad**	Es la ruta más directa para comprometer aplicaciones, datos y privilegios.	Activar MFA resistente a phishing, acceso condicional y revisión de privilegios.
2	**Datos sensibles**	Define el impacto regulatorio, reputacional y financiero de una brecha.	Inventariar, clasificar y etiquetar información crítica.
3	**Endpoints**	Siguen siendo punto frecuente de entrada, propagación y persistencia.	Consolidar gestión moderna, EDR/XDR y respuesta automatizada.
4	**Nube / SaaS**	La operación digital depende de configuraciones, permisos e integraciones seguras.	Evaluar postura cloud, permisos excesivos y aplicaciones conectadas.
5	**IA no gobernada**	Es un riesgo emergente que puede amplificar fuga de datos y accesos indebidos.	Definir política de uso, controles de acceso y monitoreo de herramientas IA.

Nota: este mapa es un marco cualitativo de priorización. Debe ajustarse con datos reales del assessment de cada organización.

La madurez de seguridad cambia el costo probable de un incidente.

El mismo ataque puede producir impactos muy distintos según la preparación de la organización.

Este modelo no pretende estimar un ROI universal. Su función es ayudar al comité ejecutivo a comparar escenarios: una organización reactiva paga más en interrupción, esfuerzo manual y recuperación; una organización con controles integrados reduce superficie, acelera contención y preserva continuidad.

ESCENARIO	CARACTERÍSTICAS	IMPACTO ESPERADO	PRIORIDAD EJECUTIVA
Reactivo Herramientas aisladas	MFA parcial, baja clasificación de datos, visibilidad fragmentada, respuesta manual.	Mayor tiempo de contención, mayor costo de recuperación y mayor exposición reputacional.	Diagnóstico urgente de activos, identidades críticas y datos sensibles.
Controlado Controles básicos integrados	MFA priorizada, acceso condicional, EDR/XDR, backups probados y playbooks iniciales.	Menor probabilidad de propagación y mejor capacidad de recuperación.	Consolidar visibilidad y gobierno de datos.
Resiliente Seguridad como capacidad operativa	Zero Trust, clasificación extendida, XDR/SIEM, automatización, gobierno de IA y métricas ejecutivas.	Menor exposición acumulada, menor tiempo de respuesta y mejor continuidad.	Optimización continua y simulacros ejecutivos.

11 · Recomendaciones ejecutivas

Qué deberían priorizar los líderes en 2026.

- **Tratar la ciberseguridad como continuidad operativa.** El lenguaje del comité debe conectar riesgo con ingresos, operación, cumplimiento y confianza.
- **Reducir dependencia de contraseñas.** MFA moderna, passwordless y acceso condicional deben avanzar primero en identidades críticas.
- **Clasificar datos antes de escalar controles.** La seguridad de información empieza por saber qué datos existen y quién puede acceder.
- **Unificar visibilidad**. XDR, SIEM y postura cloud deben reducir puntos ciegos, no multiplicar alertas desconectadas.
- **Gobernar IA desde el diseño.** Toda adopción de IA debe incluir política, controles de acceso, monitoreo y auditoría.
- **Medir exposición, no actividad.** El comité necesita indicadores de riesgo, no solamente volumen de alertas o proyectos ejecutados.

Conclusión ejecutiva

El valor de la ciberseguridad está en reducir el costo de la incertidumbre.

Las empresas no invierten en seguridad para acumular controles. Invierten para operar con menos exposición, responder con más velocidad y sostener confianza cuando el entorno digital se vuelve más hostil.

La evidencia muestra que el costo de una brecha puede ser material, que el ransomware sigue afectando la región, que la identidad continúa siendo una puerta de entrada crítica y que la IA puede reducir costos y tiempos sólo cuando se adopta con gobierno.

La decisión ejecutiva no es si la seguridad importa, sino qué riesgos deben reducirse primero y qué capacidades deben institucionalizarse. La organización que avance hacia una arquitectura integrada de riesgo, identidad, datos, infraestructura e IA segura estará mejor preparada para proteger continuidad operativa, cumplimiento y confianza digital.

Próximo paso recomendado

Realizar un assessment ejecutivo de seguridad y continuidad digital para identificar brechas críticas, priorizar controles, estimar exposición operativa y definir las capacidades prioritarias de mitigación.

Fuentes y notas

Referencias utilizadas

1. Presentación interna “Protegiendo el Futuro Digital: Continuidad Operativa a través de la Seguridad”, SEGA 2026.
2. IBM, Cost of a Data Breach Report 2025. Datos usados: costo promedio global de brecha, brechas relacionadas con IA, controles de acceso de IA, shadow AI, ahorro por IA y automatización.
3. Microsoft, Digital Defense Report 2025. Dato usado: 97% de ataques de identidad observados fueron password spray.
4. Sophos, The State of Ransomware 2025. Datos usados: pago promedio de rescate, costo promedio de recuperación, vulnerabilidades explotadas y falta de habilidades.
5. Recorded Future / Insikt Group, Latin America and the Caribbean Cybercrime Landscape. Dato usado: 452 incidentes de ransomware en LAC en 2025.

Nota editorial: las cifras deben revalidarse antes de publicación final, especialmente si el documento será distribuido comercialmente en 2026 o usado por país/industria específica.