Riesgo + Productividad

Exhibiciones ejecutivas y casos de uso de la industria con señales de mercado 2025-2026

IBM / Ponemon

$4.44M

Costo promedio global de la infracción (2025)

CrowdStrike

48 min

Tiempo promedio de irrupción (2025)

Google Mandiant

11 días

Tiempo medio de permanencia (2025)

Microsoft WorkLab

275

Interrupciones por día laboral (2025)

Preparado para: SEGA lanzamiento al mercado | Fecha: 2026-01-19 | Regiones: Centroamérica + México

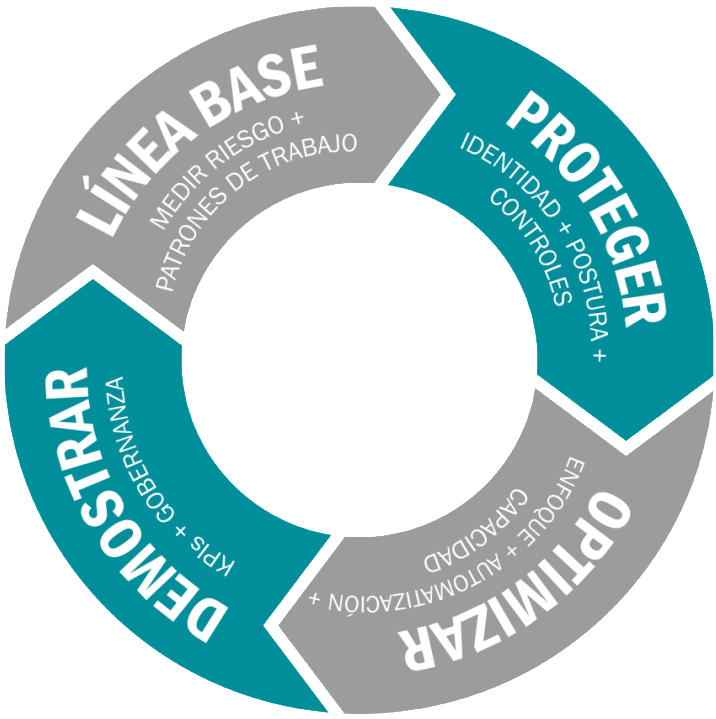
Señales del mercado 2025-2026 (por qué ahora)

- **Costo de la infracción:** $4.44M promedio (2025)
- **Velocidad de irrupción:** 48 min promedio, 51 seg más rápido (2025)
- **Tiempo de permanencia:** 11 días de media (2025)
- **Día laboral infinito:** 275 interrupciones/día (2025)
- **Riesgo macro:** IA + cadena de suministro + geopolítica (2026)

Prevenir Controles, identidad, postura	**Detectar** Señales, respuesta, evidencia
Habilitar Adopción, gobernanza	**Optimizar** Automatización, enfoque, capacidad

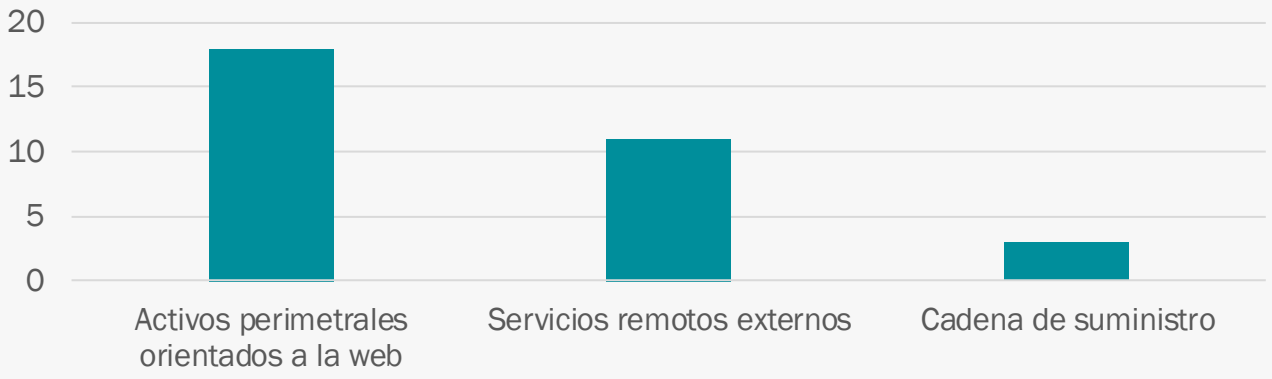
Madurez de la productividad

Volante de SEGA (simple y demostrable)



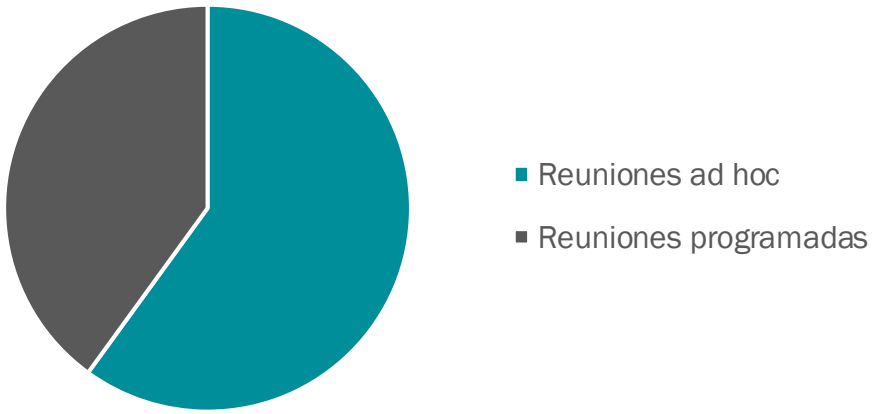
Exhibiciones ejecutivas (menos texto, más señal)

Exhibición 2: Dónde comienzan los ataques (huella de exposición, 2025) *Cuota de compromisos de IR (porcentaje)*



Fuente: Informe de defensa digital de Microsoft 2025 (compromisos de respuesta a incidentes)

Exhibición 3: Las reuniones son cada vez más “ad hoc” (2025)



Interrupciones/día	Promedio entre pings	Las ediciones de PPT duran 10 minutos	Chat fuera de horario interanual
275	**2 minutos**	**+122%**	**+15%**

Fuente: Índice de tendencias laborales de Microsoft / WorkLab (telemetría y encuesta de 2025)

Casos de uso (página 1 de 2)

Banca
CISO + COO (Crítico para operaciones)

Puntos de dolor
- Intrusión basada en credenciales
- Brechas en evidencia de auditoría
- Sobrecarga de tickets

Palancas de SEGA
- Endurecimiento de identidad y acceso
- Detección y respuesta de amenazas
- Analítica de patrones de trabajo

KPIs para demostrar Impacto
- Reducción de MTTR (Tiempo Medio de Respuesta)
- Cobertura de acceso privilegiado
- Aumento del tiempo de enfoque

Seguros
(Director de Ops + Cumplimiento)

Puntos de dolor
- Exposición de PII (Datos Personales) vía email/archivos,
- Riesgo de acceso de terceros
- Deriva de SLA

Palancas de SEGA
- Políticas de protección de datos
- Gobernanza de acceso
- Capacidad y balanceo de carga

KPIs para demostrar Impacto
- Reducción de tiempo de ciclo
- Reducción de re-trabajo
- Reducción de excepciones de política

Retail
(CIO + Líder de eCom)

Puntos de dolor
- Incidentes de disponibilidad
- Cuentas compartidas
- Sobrecarga en picos

Palancas de SEGA
- Monitoreo + respuesta
- Acceso Zero Trust
- Automatización de ops + enfoque

KPIs para demostrar Impacto
- Reducción de minutos de inactividad
- Reducción de tasa de incidentes
- Reducción de pedidos pendientes (backlog)

Distribución
Ops + Finanzas

Puntos de dolor
- Exposición de dispositivos de campo
- Errores en facturas
- Conciliaciones manuales

Palancas de SEGA
- Endpoints seguros
- Automatización de flujos de trabajo
- Línea base de productividad por rol

KPIs para demostrar Impacto
- Reducción de errores
- Cierre de ciclo más rápido
- Horas ahorradas

Manufactura
(IT de Planta + Mantenimiento)

Puntos de dolor
- Impacto de ransomware
- Ventanas de parches
- Mantenimiento reactivo

Palancas de SEGA
- Segmentación + controles
- Contención rápida
- Analítica de trabajo estándar

KPIs para demostrar Impacto
- Reducción de paradas
- Reducción de tasa de fallas en cambios
- Reducción de tiempo de entrega

Gobierno
(Director de Servicios Digitales)

Puntos de dolor
- Exposición de datos sensibles
- Presión de auditoría
- Fragmentación de procesos

Palancas de SEGA
- Controles listos para evidencia
- Gobernanza de identidad
- Rediseño de procesos + productividad

KPIs para demostrar Impacto
- Aumento de SLA
- Mejora de postura de cumplimiento
- Reducción de rezago

Casos de uso (página 1 de 2)

BPO / SSC
(Operaciones + RRHH)

Puntos de dolor
- Riesgo en el manejo de PII (Información de Identificación Personal)
- Alta rotación
- Variación de calidad

Palancas de SEGA
- Controles de acceso
- Analítica de comportamiento
- Perspectivas de coaching

KPIs para demostrar Impacto
- AHT (Tiempo Promedio de Operación) abajo
- QA (Control de Calidad) arriba
- Riesgo de deserción reducido

Cuidado de la Salud
(Administración + IT)

Puntos de dolor
- Riesgo de acceso a EHR (Expediente Clínico Electrónico)
- Exposición de proveedores
- Personal sobrecargado

Palancas de SEGA
- Identidad y pistas de auditoría
- Gobernanza de datos
- Analítica de carga de trabajo.

KPIs para demostrar Impacto
- Tiempo de admisión abajo
- Carga fuera de horario abajo
- Anomalías de acceso abajo.

Educación
Director IT

Puntos de dolor
- Compromiso de cuentas
- Baja capacidad de IT
- Sombra IT

Palancas de SEGA
- MFA resistente a phishing
- Postura del dispositivo
- Automatización de autoservicio

KPIs para demostrar Impacto
- Incidentes abajo
- Tickets por usuario abajo
- Tiempo de reparación abajo

Hospitalidad
GM + Finanzas

Puntos de dolor
- Fraude y contracargos
- Picos estacionales
- Informes manuales.

Palancas de SEGA
- Monitoreo de fraude
- Productividad basada en roles
- Informes automatizados.

KPIs para demostrar Impacto
- Pérdidas abajo
- Cierres más rápidos
- Fuga de ingresos reducida

Servicios Profesionales
Socio Director

Puntos de dolor
- Riesgo de fuga de IP (Propiedad Intelectual
- Cambio de contexto (context switching)
- Puntos ciegos de utilización

Palancas de SEGA
- DLP y gobernanza de acceso
- Protección del tiempo de enfoque
- Pronóstico de capacidad.

KPIs para demostrar Impacto
- Utilización arriba
- Re-trabajo abajo
- Horas fuera de jornada reducidas

Tecnología / SaaS
CTO + SecOps

Puntos de dolor
- Exposición de la cadena de suministro
- Dispersión de privilegios
- Presión de lanzamientos

Palancas de SEGA
- Postura de CI/CD segura
- Gestión de acceso privilegiado
- Automatización para tareas tediosas

KPIs para demostrar Impacto
- Tasa de fallas en cambios abajo
- Tiempo medio de detección abajo
- Agotamiento por tareas manuales abajo

Plan de implementación (Primero el POC/ Prueba de Concepto)

Día 0-3	Día 4-15	Día 16-45	Día 46-90
Línea base	**POC**	**Escalar**	**Operar**
Desplegar sensores, definir roles y KPIs	Demostrar controles de riesgo + ganancias de productividad	Expandir a equipos y procesos prioritarios	Cadencia de gobernanza, automatización, tableros

Tablero de KPIs (lo que medimos desde el Día 1):

Riesgo: Cobertura de MFA, control de acceso privilegiado, eventos de anomalías, tiempo de contención.

Ops: Tickets por usuario, MTTR, tasa de fallas en cambios, minutos de inactividad.

Personas: Interrupciones/día, tiempo de enfoque, carga fuera de horario, principales fuentes de distracción.

Valor: Horas ahorradas, costos evitados, preparación de evidencia de cumplimiento.

Fuentes (Fuentes actualizadas 2025-2026)

- Microsoft Digital Defense Report 2025 (Microsoft).
- Microsoft Work Trend Index / WorkLab (2025): "Infinite workday" productivity telemetry.
- CrowdStrike 2025 Global Threat Report (breakout time, malware-free detections).
- Google Mandiant M-Trends 2025 (median dwell time, initial vectors).
- Verizon 2025 DBIR (third-party involvement, vulnerability exploitation trends).
- IBM Cost of a Data Breach Report 2025 (global average breach cost).
- World Economic Forum: Global Cybersecurity Outlook 2026 (AI, geopolitics, supply chain risk context).
- ENISA Threat Landscape 2025 (EU incident analysis and trends).

Prevenir • Detectar • Habilitar • Optimizar

Ejemplos concretos para operacionalizar Riesgo + Productividad (Guía operativa SEGA)

Prevenir

Detener las vías comunes)

- MFA resistente al phishing (FIDO2/passkeys) para usuarios privilegiados y de alto riesgo.
- Establecimiento de línea base de postura (Secure Score / cumplimiento de dispositivos) + sprints de endurecimiento rápido.
- Mínimo privilegio con PIM/JIT + políticas de acceso condicional por rol.

Detectar

Encontrar + contener rápido (medible)

- Triaje de alertas con modelo de severidad + ruta de escalación 24/7.
- SLA de contención (ej., severidad alta: triaje <15m, contención <60m).
- Telemetría unificada (punto final, identidad, nube) -> libros de jugadas para ataques repetidos.

Habilitar

Gobernar la capa de colaboración

- Gobernanza de M365: políticas de compartición externa por grupo/sitio, predeterminado = compartir lo mínimo.
- Protección de datos: etiquetas de sensibilidad + DLP para datos personales/financieros.
- Retención y eDiscovery: políticas defendibles para auditorías e incidentes.

Optimizar

Aumentar la capacidad (sin agotamiento)

- Automatización: triaje de tickets, aprobaciones, informes (Power Platform / RPA).
- Reducción de interrupciones: higiene de reuniones, política de notificaciones, bloques de enfoque.
- Tableros de operaciones: capacidad, carga y puntos críticos de desperdicio -> cadencia de ejecución semanal.

Ejemplos reales de la Industria (lo que se vé en la práctica):

Banca Prevenir: PIM para roles de administrador; Detectar: alertas de identidad enrutadas.

Retail Habilitar: endurecer la compartición externa para proveedores; Detectar: endpoint.

BPO/SSC Optimizar: triaje automático de tickets + sugerencias de conocimiento; Prevenir.

Manufactura Detectar: aislar endpoints comprometidos rápido; Habilitar: retención.
+1