REPORTE · 2026 · EDICIÓN I

Estado de la Seguridad M365 en México 2026

Un análisis operacional de los controles que fallan con más frecuencia en tenants Microsoft 365 del mercado mexicano, la brecha frente a la referencia de Microsoft Secure Score y el costo económico del incumplimiento.

Publicado por **simiriki** — Monterrey, N.L., México
Autor: Equipo de investigación de simiriki
Metodología: 192 reglas de detección aplicadas a Microsoft Graph y Azure ARM

Contenido

01	Resumen ejecutivo	3
02	Metodología y alcance	4
03	Los 10 hallazgos críticos más comunes	5
04	Brecha frente a Microsoft Secure Score	8
05	Costo económico del incumplimiento	9
06	Marco regulatorio mexicano (LFPDPPP · CNBV)	10
07	Benchmarks por tamaño de empresa	11
08	Roadmap de remediación priorizado	12
09	Sobre simiriki	13
10	Anexo: las 192 reglas de detección	14

01 · Resumen ejecutivo

El parque de tenants Microsoft 365 operando en México es una superficie crítica insuficientemente medida. La mayoría de las organizaciones —incluyendo firmas reguladas por la CNBV, despachos profesionales y manufactura orientada a exportación— desconoce cuántos de sus controles fundamentales están realmente activos. En ausencia de medición objetiva, las áreas de TI reportan “posture” con base en la configuración de referencia del fabricante, no en el comportamiento real del tenant.

The Mexican Microsoft 365 tenant fleet is a critical attack surface that is chronically under-measured. Most organizations —including CNBV-regulated firms, professional services and export-oriented manufacturing— do not know how many of their baseline controls are actually enforced.

Lo que este reporte documenta:

• Los controles específicos que con mayor frecuencia **aparentan estar activos y no lo están**.

• La **brecha real** frente a la referencia de Microsoft Secure Score.

• El **costo económico estimado** en MXN asociado a los hallazgos más comunes.

• Las **obligaciones regulatorias** vigentes para 2026 bajo LFPDPPP y, para firmas reguladas, CNBV.

• Un **roadmap de remediación priorizado** por impacto y esfuerzo.

192
controles de detección
detection rules

9
conectores activos
active connectors

48-72h
entrega estimada
estimated delivery

Todos los datos del presente reporte provienen de: (a) documentación pública de Microsoft sobre controles recomendados; (b) estadística pública de INEGI, Banxico y CONDUSEF sobre incidentes digitales; (c) publicaciones del INAI y Diario Oficial de la Federación sobre LFPDPPP; y (d) la taxonomía de detección de simiriki (192 reglas sobre Microsoft Graph y Azure Resource Manager). Donde el dato es una estimación o rango, se señala explícitamente.

02 · Metodología y alcance

Alcance técnico

El marco de análisis de simiriki evalúa un tenant Microsoft 365 contra **192 reglas de detección** con evaluadores reales —no scoring sintético. Cada regla consulta la API correspondiente (Microsoft Graph para identidad, correo, dispositivos y colaboración; Azure Resource Manager para red, infraestructura y cumplimiento) y emite un veredicto *passed*, *failed* o *needs_review*. Este reporte analiza específicamente los 56 controles con evaluador de verdad-en-datos (real verdict) y los contrasta con la recomendación oficial del fabricante.

Cobertura por dominio

Dominio	Reglas	Fuente primaria de datos
Identidad y acceso (IAM)	**42**	Microsoft Graph · AAD · Conditional Access
Correo y colaboración (EML/EXO)	**38**	Exchange Online · Graph Mail
Prevención de pérdida de datos (DLP)	**19**	Graph · Purview · SharePoint
Dispositivos (MDM/DEV)	**22**	Intune · Graph device compliance
Aplicaciones y desarrollo (APP/DEV)	**11**	Graph · App registrations
Auditoría y riesgo (AUD/RSK)	**14**	Unified Audit Log · Graph
Red, cómputo, bases (NET/CMP/DBS)	**28**	Azure Resource Manager
Gobierno y política (GOV)	**10**	Azure Policy · Defender for Cloud
Otros (PUR, PWR, TMS, OPS, SEN, AZR)	**8**	Graph · ARM · Sentinel

Fuente: taxonomía de detección de simiriki · lib/deepScan.ts (abril 2026).

Qué NO hace este reporte

No reportamos tenants específicos, no publicamos nombres de clientes, no generamos métricas promedio de “+N puntos de mejora” porque no tenemos aún una muestra lo suficientemente grande para respaldar una afirmación así. Lo que documentamos es: **los modos de falla más frecuentes que detectamos en el día a día**, y la brecha esperable contra la recomendación oficial de Microsoft.

03 · Los 10 hallazgos críticos más comunes

Cada hallazgo corresponde a una regla específica de la taxonomía de simiriki, con nombre técnico, evaluador real contra Graph o ARM, y la acción de remediación priorizada. El orden refleja frecuencia observada y severidad agregada, no alfabético.

IAM-001 CRÍTICO

MFA obligatoria no aplicada al 100% de usuarios privilegiados

El tenant tiene MFA habilitada pero no aplicada por Conditional Access sobre roles privilegiados (Global Admin, Exchange Admin, Privileged Role Admin). La exclusión se da por cuentas break-glass mal configuradas o políticas heredadas con excepciones residuales.

IAM-002 CRÍTICO

Conditional Access con brechas en sign-in risk y user risk

Las políticas existen pero no cubren los dos gatillos más relevantes: riesgo de inicio de sesión y riesgo de usuario. Sin esto, Identity Protection detecta pero no bloquea.

IAM-008 CRÍTICO

Autenticación heredada (legacy auth) no bloqueada

Protocolos legacy (IMAP, POP3, SMTP básico, autenticación básica de Exchange) siguen abiertos para compatibilidad con impresoras, escáneres o ERPs antiguos. Cada puerto abierto es un bypass de MFA.

EML-001 ALTO

Registro SPF ausente o demasiado permisivo

SPF no publicado o terminado en ~all en vez de -all. Habilita spoofing del dominio principal de correo. Observado con frecuencia en dominios corporativos que usan múltiples proveedores de correo transaccional.

EML-003 ALTO

DMARC en política p=none

El registro existe pero no rechaza ni pone en cuarentena. Esto significa que el atacante puede suplantar el dominio sin consecuencias. DMARC en p=none es equivalente a no tener DMARC.

EML-004 ALTO

Reenvío automático de buzón habilitado

Usuarios individuales pueden configurar forwarding a direcciones externas. Es el vector clásico de exfiltración post-compromiso de credenciales.

DLP-003 ALTO

Compartición externa sin restricción en SharePoint/OneDrive

Sites con “Anyone with the link” habilitado a nivel tenant. Documentos sensibles —nóminas, contratos, propiedad intelectual— quedan accesibles sin autenticación.

IAM-006 MEDIO

Política de contraseñas débil o no enforced

Configuración permite contraseñas de 8 caracteres sin complejidad obligatoria, o la política existe en directorio pero no se aplica a cuentas sincronizadas desde AD on-prem.

IAM-003 MEDIO

Cuentas de invitado (B2B) sin expiración ni revisión

Guests creados para proyectos temporales permanecen en el tenant meses o años después. Muchos de ellos con roles de “Member” en Teams sensibles.

DKIM / EML-002 MEDIO

DKIM no firmado o clave rotada incorrectamente

Al menos una selectora de DKIM está inactiva, o el dominio carece del registro. Impacta entregabilidad y, combinado con SPF/DMARC débiles, abre vía de spoofing.

04 · Brecha frente a Microsoft Secure Score

Microsoft Secure Score asigna puntos por control configurado. Es útil como referencia del fabricante, pero con dos limitaciones conocidas: (a) es estático —se actualiza a intervalos, no en tiempo real— y (b) no distingue entre “control configurado” y “control efectivamente aplicado a la población correcta”. Una política de Conditional Access puede sumar puntos sin estar aplicándose a los usuarios privilegiados.

Lo que simiriki agrega

La taxonomía de 192 reglas —de las cuales 56 tienen evaluadores reales que miden comportamiento observado— se ejecuta contra los datos reales del tenant y emite veredicto verificable. En los controles con evaluador real, nunca devuelve *passed* falso. Si los datos disponibles no permiten concluir, el veredicto es *needs_review* y se indica exactamente qué evidencia adicional se requiere.

Interpretación honesta

Los dos instrumentos son complementarios. Microsoft Secure Score responde *¿qué recomendaciones he adoptado?*. El marco de simiriki responde *¿están esas recomendaciones realmente aplicadas a quien deben, hoy?*.

05 · Costo económico del incumplimiento

Tres componentes componen el costo esperado de un incidente de seguridad derivado de los hallazgos anteriores: (1) sanciones administrativas; (2) costo operativo de contención, forense y recuperación; y (3) costo de oportunidad por interrupción y daño reputacional.

Concepto	Rango estimado (MXN)	Fuente / referencia
Sanción LFPDPPP por incumplimiento grave	$194,450 – $31,112,000	Art. 64 LFPDPPP · UMA 2026
Multa CNBV instituciones financieras	Variable · hasta 30,000 UMAs	LRAF / Disposiciones generales
Honorarios de respuesta a incidente (forense + legal)	$180,000 – $1,200,000	Rango típico en el mercado mexicano
Costo de downtime por día (PyME / Mid-Market)	$50,000 – $800,000	Estimación basada en encuestas INEGI
Notificación a titulares afectados	Variable	Depende de número de titulares · INAI

Los rangos son estimaciones. Fuentes primarias: Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), CNBV, INAI, Diario Oficial de la Federación. No se aplican a todas las organizaciones por igual.

06 · Marco regulatorio mexicano

LFPDPPP (2010, vigente)

Los Arts. 19 y 20 obligan a los responsables a establecer y mantener medidas de seguridad administrativas, físicas y técnicas para la protección de los datos personales. El INAI ha sostenido que la omisión demostrable (p. ej. falta de MFA en sistemas con datos personales) configura incumplimiento sancionable.

CNBV · Circular Única de Bancos y actualizaciones 2026

Para instituciones financieras reguladas, la CNBV mantiene disposiciones específicas de ciberseguridad (continuidad operativa, gestión de incidentes y reportes obligatorios). El plazo de notificación de incidentes y los requerimientos de bitácora auditable son los puntos que con más frecuencia incumplen tenants no preparados.

Iniciativas 2026

Durante 2026 están en discusión reformas en materia de ciberseguridad sectorial (sector financiero, telecomunicaciones y salud). Este reporte se actualizará cuando las reformas entren en vigor.

07 · Benchmarks por tamaño de empresa

Tamaño	Empleados	Prioridad 1	Prioridad 2	Prioridad 3
Pequeña	10–50	MFA + CA base	SPF / DMARC	Backup M365
Mediana	51–250	MFA privilegiados	DLP básico	Audit log 365d
Mid-Market	251–1,000	Defender P2	Sentinel piloto	Identity Protection
Enterprise	1,000+	Zero Trust completo	Sentinel + SOC	Purview + DLP avanzado

08 · Roadmap de remediación priorizado

Orden recomendado para organizaciones que inician el trayecto. Cada etapa asume que la anterior está consolidada.

Semana 1-2 · Tapar hemorragias

Bloquear autenticación heredada · Aplicar MFA a roles privilegiados · Publicar SPF, DKIM y DMARC con política mínima de cuarentena · Desactivar reenvío automático externo.

Semana 3-6 · Base de Conditional Access

Políticas cubriendo: sign-in risk, user risk, ubicaciones, dispositivos no compliant. Excepciones documentadas y con revisión trimestral.

Mes 2-3 · DLP + Purview

Etiquetado de sensibilidad básico · Políticas DLP sobre correo y SharePoint · Limitación de compartición externa.

Mes 3-4 · Monitoreo activo

Sentinel en modo pilot o Defender XDR según pila disponible · Incorporación de logs críticos · Reglas de detección base.

Mes 4-6 · Gobierno y postura

Azure Policy · revisiones de acceso · auditoría trimestral · plan formal de respuesta a incidentes alineado a CNBV/LFPDPPP.

09 · Sobre simiriki

simiriki es una consultora de **operational infrastructure** con sede en Monterrey, N.L., México. Definimos esta categoría como la capa ejecutiva entre las políticas corporativas, las plataformas de nube y el comportamiento real del tenant. No vendemos SaaS —vendemos ingeniería aplicada para cerrar la brecha entre lo que la dirección cree que está funcionando y lo que en realidad está ocurriendo en la infraestructura.

Cómo operamos

Escaneo gratuito	OAuth a M365, 192 reglas, entrega de reporte preliminar en minutos. Sin compromiso, sin tarjeta de crédito.
Auditoría ($19,900 MXN)	Reporte técnico completo con plan de remediación priorizado, sesión de revisión de 30 minutos, entrega estimada 48-72h, garantía de satisfacción a 7 días.
S.O.S. Retainer ($50,000 MXN/mes)	Monitoreo continuo + remediación gestionada. Reporte mensual ejecutivo. Ingeniero dedicado.
Enterprise / Sentinel + Defender XDR	Implementaciones hechas a la medida para mid-market y arriba. Cotizamos por escenario.

Agenda un escaneo gratuito

simiriki.com/scan — conecta tu tenant con OAuth de Microsoft (permisos read-only) y recibe tu reporte preliminar en minutos. Si prefieres que hablemos primero: **reportes@simiriki.com**.

10 · Anexo: las 192 reglas

Inventario resumido de la taxonomía. El catálogo completo con IDs, descripciones y remediación recomendada se publica en **simiriki.com/deepscan/catalogo** (acceso gratuito).

Prefijo	Dominio	Reglas
IAM-	Identidad y acceso	42
EML- / EXO-	Correo y colaboración	38
DLP-	Prevención de pérdida de datos	19
MDM- / DEV-	Dispositivos y desarrollo	33
AUD- / RSK-	Auditoría y riesgo	14
NET- / CMP- / DBS-	Red, cómputo, bases	28
GOV-	Gobierno y política	10
AZR- / SEN- / OPS- / PUR- / PWR- / TMS-	Plataforma y operación	8
Total		**192**