Contoso
CHILE SpA

INFORME MENSUAL

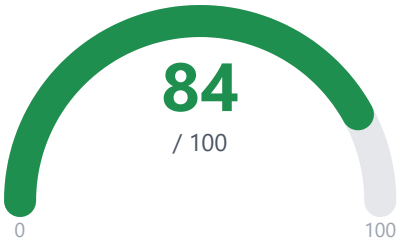
Estado de la Nube

Contoso Chile SpA

Agosto 2026

Datos recolectados el 17 de agosto de 2026

Resumen ejecutivo



Postura saludable, con oportunidades puntuales de mejora.

Puntaje por categoría

Análisis del consultor

- **MFA registrado sube de 46% a 94% en dos meses; ya no quedan administradores sin MFA.**
- **Las cuentas con rol de administrador global bajaron de 6 a 4 — menos superficie crítica expuesta.**
- **Quedan dos frentes abiertos — la política de autenticación heredada sigue en modo solo informe y DMARC continúa en `p=none`.**

El trabajo de los últimos dos meses se concentró en identidad, y el resultado se ve: el registro de MFA pasó de menos de la mitad de las cuentas a prácticamente toda la organización, y los tres administradores sin segundo factor que abrían el informe de hace dos meses ya no existen. Es el cambio de mayor impacto por unidad de esfuerzo que tenía este entorno, y está hecho.

Qué priorizar este mes

1. **Sacar de «solo informe» la política de autenticación heredada.** Está escrita y probada; mientras no se aplique, los protocolos antiguos siguen siendo un camino de entrada que el MFA recién implementado no cubre.
2. **Endurecer DMARC a `p=quarantine`.** SPF y DKIM ya están publicados y estables, que era el requisito previo. Mantener `p=none` significa que hoy cualquiera puede enviar correo a nombre del dominio sin consecuencias.
3. **Recuperar las 11 licencias E3 sin asignar** antes de la próxima renovación. Es la acción con retorno inmediato y sin riesgo operativo.

Sobre lo que este informe no evalúa

El inquilino no cuenta con licencias Entra ID P2, de modo que el módulo de riesgo de identidad aparece como no evaluado en el anexo. Eso significa «no se pudo determinar», no «sin cuentas en riesgo»: si la organización quiere visibilidad de credenciales filtradas y accesos anómalos, esa licencia es el requisito.

— Equipo de Consultoría TI, Servicio gestionado Microsoft 365

Principales hallazgos

Alto **[EXIT-002] Cuentas activas y licenciadas con inactividad prolongada** — 13 afectado(s)

Alto **[ALERT-001] Alertas de seguridad abiertas sin atender** — 5 afectado(s)

Alto **[CA-002] La autenticación heredada no está bloqueada** — 1 afectado(s)

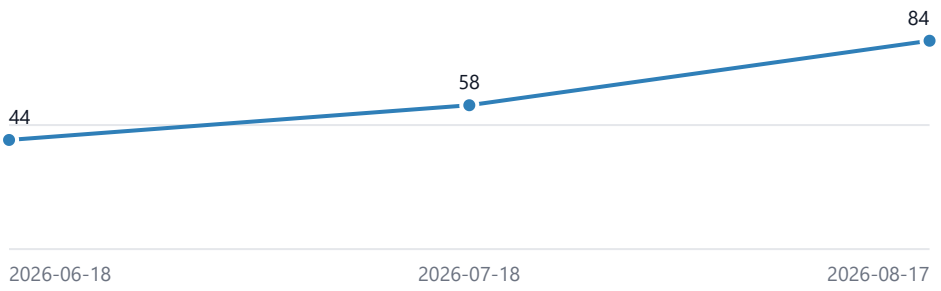
Medio **[PRIV-003] Alta concentración de roles privilegiados** — 18 afectado(s)

Medio **[STALE-001] Cuentas habilitadas sin actividad reciente** — 14 afectado(s)

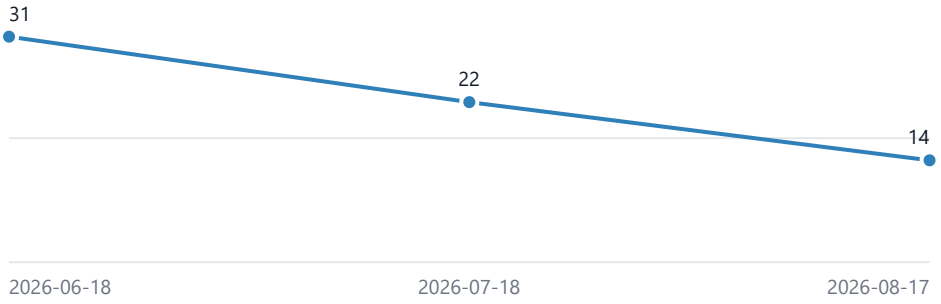
Evolución mensual

Comparado con el informe del **2026-07-18**. El puntaje general pasó de **58** a **84** (+26).

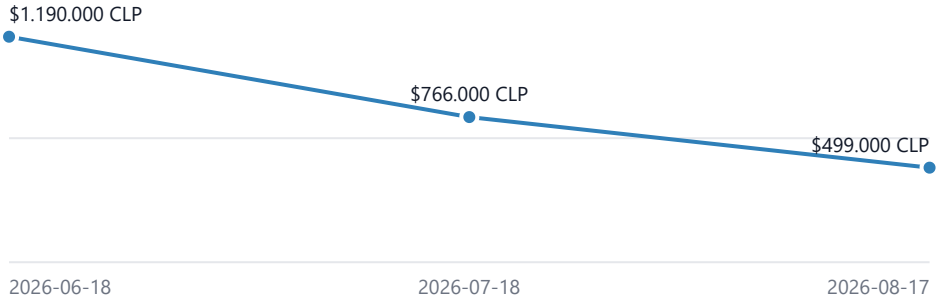
Puntaje general



Cuentas inactivas



Ahorro potencial mensual



Variación por categoría

Categoría	Anterior	Actual	Variación
Identidad	67	96	+29
Accesos	47	82	+35
Licenciamiento	84	84	0
Seguridad	32	67	+35
Operaciones	97	97	0

Resuelto desde el último informe

- **[CA-001] Sin controles de acceso condicional ni valores predeterminados** — Crítico (1 afectado(s) en el informe anterior)
- **[MFA-002] Administradores sin MFA registrado** — Crítico (1 afectado(s) en el informe anterior)
- **[PRIV-002] Miembros de roles privilegiados sin MFA registrado** — Crítico (1 afectado(s) en el informe anterior)
- **[PRIV-001] Demasiados Administradores Globales** — Alto (6 afectado(s) en el informe anterior)
- **[SEC-001] Puntaje de seguridad de Microsoft bajo** — Alto (1 afectado(s) en el informe anterior)
- **[SHARE-003] SharePoint acepta autenticación heredada** — Alto (1 afectado(s) en el informe anterior)
- **[MFA-001] Baja cobertura de MFA** — Medio (30 afectado(s) en el informe anterior)
- **[MAIL-004] Dominios sin firma DKIM** — Medio (1 afectado(s) en el informe anterior)

Nuevo este mes

- **[CA-002] La autenticación heredada no está bloqueada** — Alto (1 afectado(s))
- **[CA-004] Políticas de acceso condicional en modo solo informe** — Medio (1 afectado(s))

Hallazgos persistentes

Hallazgo	Severidad	Anterior	Actual	Variación	Salieron	Entraron
[EXIT-002] Cuentas activas y licenciadas con inactividad prolongada	Alto	20	13	-7	9	2
[ALERT-001] Alertas de seguridad abiertas sin atender	Alto	8	5	-3	7	4
[PRIV-003] Alta concentración de roles privilegiados	Medio	18	18	0	0	0
[STALE-001] Cuentas habilitadas sin actividad reciente	Medio	22	14	-8	10	2
[LIC-003] Licencias pagas sin actividad reciente	Medio	20	13	-7	9	2
[LIC-002] Licencias compradas sin asignar	Medio	16	11	-5	1	1
[SEC-002] Controles de seguridad recomendados sin aplicar	Medio	9	6	-3	3	0
[LIC-004] Licencias superpuestas en la misma cuenta	Medio	3	4	+1	0	1
[EXIT-001] Cuentas deshabilitadas con licencias asignadas	Medio	7	3	-4	4	0
[LIC-001] Licencias asignadas a cuentas deshabilitadas	Medio	7	3	-4	4	0
[MAIL-002] DMARC publicado pero sin aplicar (p=none)	Medio	1	1	0	0	0
[USE-002] OneDrive sin uso reciente	Bajo	31	24	-7	27	20
[USE-003] Baja adopción de Microsoft Teams	Bajo	33	22	-11	26	15
[USE-001] Buzones sin actividad reciente	Bajo	19	12	-7	17	10
[SHARE-004] Uso compartido externo sin restricción por dominio	Bajo	1	1	0	N/D	N/D

> "Salieron"/"Entraron" cuentan las cuentas u objetos que dejaron de estar o pasaron a estar afectados por cada hallazgo; N/D indica que el detalle por cuenta no está disponible para esa comparación.

Hallazgos por categoría

Accesos (82/100)

Alto **[EXIT-002] Cuentas activas y licenciadas con inactividad prolongada**

13 cuenta(s) habilitada(s) y licenciada(s) no registran actividad en los últimos 90 días.

Por qué importa: A diferencia de una cuenta deshabilitada, esta conserva acceso activo — es el patrón más probable de un ex-empleado no dado de baja a tiempo.

Impacto de negocio: Riesgo de acceso indebido a datos corporativos, además del costo de la licencia.

Recomendación: Confirmar con RR.HH. o el área responsable si la persona sigue activa; si no, deshabilitar la cuenta y liberar sus licencias. Solución rápida

Afectados (13): cristobal.martinez@contoso.example, constanza.flores@contoso.example, felipe.perez@contoso.example, isidora.contreras@contoso.example, fernanda.hernandez@contoso.example, catalina.gutierrez@contoso.example, isidora.morales@contoso.example, antonia.munoz@contoso.example, benjamin.gutierrez@contoso.example, antonia.tapia@contoso.example · confianza: high

Listado completo en `anexo_hallazgos.csv` (hallazgo EXIT-002).

Medio **[PRIV-003] Alta concentración de roles privilegiados**

18 cuentas (13% del total) tienen al menos un rol de directorio asignado.

Por qué importa: Un porcentaje alto de cuentas con privilegios eleva el impacto potencial de cualquier compromiso individual.

Impacto de negocio: Mayor superficie de ataque administrativa.

Recomendación: Auditar las asignaciones de rol y aplicar el principio de menor privilegio; preferir roles con alcance acotado sobre roles amplios. Proyecto

Afectados (18): cristobal.martinez@contoso.example, catalina.castillo@contoso.example, nicolas.gonzalez@contoso.example, maria.martinez@contoso.example, cristobal.silva@contoso.example, fernanda.hernandez@contoso.example, fernanda.diaz@contoso.example, agustin.diaz@contoso.example, isidora.araya@contoso.example, valentina.flores@contoso.example · confianza: medium

Listado completo en `anexo_hallazgos.csv` (hallazgo PRIV-003).

Medio **[EXIT-001] Cuentas deshabilitadas con licencias asignadas**

3 cuenta(s) deshabilitada(s) conservan una o más licencias asignadas.

Por qué importa: Suele indicar ex-empleados cuyo proceso de baja quedó incompleto: la cuenta se deshabilitó pero nunca se liberaron sus licencias.

Impacto de negocio: Costo mensual recurrente por licencias no utilizadas.

Recomendación: Completar el proceso de baja: remover licencias y, si corresponde, eliminar la cuenta según la política de retención. Solución rápida

Afectados (3): francisca.gutierrez@contoso.example, matias.araya@contoso.example, matias.gonzalez@contoso.example · confianza: high

Identidad (96/100)

Medio **[STALE-001] Cuentas habilitadas sin actividad reciente**

14 cuenta(s) habilitada(s) no registran inicio de sesión en los últimos 90 días.

Por qué importa: Las cuentas habilitadas sin uso son una superficie de ataque innecesaria: cualquier credencial comprometida en una cuenta inactiva pasa desapercibida más tiempo.

Impacto de negocio: Riesgo de acceso no autorizado no detectado, además del costo de licencias asociadas (ver sección de licenciamiento).

Recomendación: Revisar y deshabilitar las cuentas sin actividad, o confirmar con el área correspondiente si siguen siendo necesarias. Solución rápida

Afectados (14): cristobal.martinez@contoso.example, constanza.flores@contoso.example, felipe.perez@contoso.example, isidora.contreras@contoso.example, fernanda.hernandez@contoso.example, catalina.gutierrez@contoso.example, isidora.morales@contoso.example, antonia.munoz@contoso.example, benjamin.gutierrez@contoso.example, antonia.tapia@contoso.example · confianza: high

Listado completo en `anexo_hallazgos.csv` (hallazgo STALE-001).

Licenciamiento (84/100)

Medio **[LIC-003] Licencias pagas sin actividad reciente**

13 cuenta(s) habilitada(s) con licencia paga no registran actividad en ningún servicio de Microsoft 365 en los últimos 90 días.

Por qué importa: Una licencia asignada a una cuenta que no usa ningún servicio es gasto puro: no aporta valor y se factura mes a mes hasta que alguien la retira o reasigna.

Impacto de negocio: Ahorro potencial estimado de $216.000 CLP al mes al retirar o reasignar estas licencias.

Recomendación: Revisar estas cuentas: retirar la licencia de las que ya no la necesitan o reasignarla a personal activo antes de comprar puestos adicionales. Solución rápida

Afectados (13): cristobal.martinez@contoso.example — Office 365 E3, Office 365 E1, constanza.flores@contoso.example — Office 365 E3, felipe.perez@contoso.example — Office 365 E3, isidora.contreras@contoso.example — Office 365 E3, fernanda.hernandez@contoso.example — Office 365 E1, catalina.gutierrez@contoso.example — Office 365 E3, isidora.morales@contoso.example — Office 365 E1, antonia.munoz@contoso.example — Office 365 E3, benjamin.gutierrez@contoso.example — Office 365 E1, antonia.tapia@contoso.example — Office 365 E3 · confianza: high

Listado completo en `anexo_hallazgos.csv` (hallazgo LIC-003).

Medio **[LIC-002] Licencias compradas sin asignar**

11 puesto(s) comprado(s) en 1 SKU(s) no están asignados a ningún usuario.

Por qué importa: Los puestos comprados y no asignados representan gasto sin retorno inmediato.

Impacto de negocio: Ahorro potencial estimado de $231.000 CLP al mes. Costo mensual por licencias adquiridas y no utilizadas.

Recomendación: Reasignar los puestos disponibles o reducir la cantidad comprada en la próxima renovación. Solución rápida

Afectados (11): ENTERPRISEPACK (11 sin asignar) · confianza: high

Medio **[LIC-004] Licencias superpuestas en la misma cuenta**

4 cuenta(s) tienen asignadas dos o más licencias cuyo alcance se solapa (por ejemplo E1 y E3); la de menor nivel es redundante.

Por qué importa: Cuando una cuenta tiene una licencia superior, la licencia inferior del mismo grupo no agrega funcionalidad y se está pagando por duplicado.

Impacto de negocio: Ahorro potencial estimado de $32.000 CLP al mes al retirar las licencias de menor nivel redundantes.

Recomendación: Retirar la licencia de menor nivel de cada cuenta afectada, conservando únicamente la de mayor alcance. Solución rápida

Afectados (4): ignacio.hernandez@contoso.example — redundante: Office 365 E1, vicente.lopez@contoso.example — redundante: Office 365 E1, cristobal.martinez@contoso.example — redundante: Office 365 E1, maria.rojas@contoso.example — redundante: Office 365 E1 · confianza: high

Medio **[LIC-001] Licencias asignadas a cuentas deshabilitadas**

3 licencia(s) siguen asignadas a 3 cuenta(s) deshabilitada(s).

Por qué importa: Las licencias no se liberan automáticamente al deshabilitar una cuenta; siguen facturándose hasta que alguien las retira.

Impacto de negocio: Ahorro potencial estimado de $20.000 CLP al mes. Costo mensual recurrente por licencias no utilizadas.

Recomendación: Retirar las licencias asignadas a cuentas deshabilitadas o eliminarlas si ya no se requieren, según política de retención. Solución rápida

Afectados (3): francisca.gutierrez@contoso.example, matias.araya@contoso.example, matias.gonzalez@contoso.example · confianza: high

Operaciones (97/100)

Bajo **[USE-002] OneDrive sin uso reciente**

24 cuenta(s) de OneDrive no registran actividad de archivos en los últimos 90 días.

Por qué importa: El almacenamiento de OneDrive sin uso suele corresponder a cuentas abandonadas; también puede haber datos de personal que salió que nadie está gestionando.

Impacto de negocio: Baja adopción de OneDrive y posibles datos huérfanos sin respaldo de gobierno.

Recomendación: Confirmar si estas cuentas siguen siendo necesarias; preservar o transferir los datos relevantes y liberar el resto. Proyecto

Afectados (24): catalina.castillo@contoso.example, javiera.sepulveda@contoso.example, javiera.lopez@contoso.example, maria.martinez@contoso.example, matias.tapia@contoso.example, isidora.rodriguez@contoso.example, martina.rojas@contoso.example, antonia.sepulveda@contoso.example, matias.munoz@contoso.example, josefa.reyes@contoso.example · confianza: high

Listado completo en `anexo_hallazgos.csv` (hallazgo USE-002).

Bajo **[USE-003] Baja adopción de Microsoft Teams**

22 usuario(s) con licencia de Teams no registran actividad en Teams en los últimos 90 días.

Por qué importa: Una licencia de Teams sin uso es capacidad de colaboración pagada que no se está aprovechando; suele deberse a falta de habilitación o de capacitación, no de necesidad.

Impacto de negocio: Retorno bajo sobre la inversión en licenciamiento y una oportunidad de mejora de productividad sin costo de licencia adicional.

Recomendación: Impulsar la adopción de Teams (capacitación, casos de uso internos) o revisar si estos usuarios requieren la licencia. Proyecto

Afectados (22): vicente.lopez@contoso.example, maria.rojas@contoso.example, javiera.lopez@contoso.example, isidora.araya@contoso.example, martina.rojas@contoso.example, vicente.gonzalez@contoso.example, isidora.perez@contoso.example, valentina.flores@contoso.example, catalina.perez@contoso.example, ignacio.lopez@contoso.example · confianza: high

Listado completo en `anexo_hallazgos.csv` (hallazgo USE-003).

Bajo **[USE-001] Buzones sin actividad reciente**

12 buzón(es) no registran actividad de correo en los últimos 90 días.

Por qué importa: Un buzón sin actividad suele indicar una cuenta que ya no se usa (personal que salió, o una licencia que podría reasignarse) o un buzón de recurso que conviene documentar.

Impacto de negocio: Posible licencia de Exchange pagándose sin uso; además, cada buzón activo es superficie de ataque adicional.

Recomendación: Revisar los buzones inactivos: convertir en compartidos, archivar o retirar la licencia según corresponda. Solución rápida

Afectados (12): vicente.lopez@contoso.example, martina.castillo@contoso.example, josefa.reyes@contoso.example, constanza.torres@contoso.example, isidora.morales@contoso.example, vicente.hernandez@contoso.example, cristobal.fuentes@contoso.example, benjamin.gutierrez@contoso.example, matias.sepulveda@contoso.example, diego.rojas@contoso.example · confianza: high

Listado completo en `anexo_hallazgos.csv` (hallazgo USE-001).

Seguridad (67/100)

Alto **[ALERT-001] Alertas de seguridad abiertas sin atender**

5 alerta(s) de Microsoft Defender siguen abiertas (estado nuevo o en curso), de las cuales 1 son de severidad alta o crítica.

Por qué importa: Una alerta abierta es una detección que el entorno ya hizo y que nadie revisó ni cerró. La inversión en detección solo se convierte en protección cuando alguien responde: sin ese paso, el atacante y el sistema de seguridad conviven.

Impacto de negocio: Incidentes potencialmente en curso, detectados y no atendidos — el peor escenario en una revisión posterior a una brecha o ante un seguro.

Recomendación: Definir un responsable y una cadencia de revisión de alertas (al menos semanal), partiendo por las de severidad alta, y cerrar cada alerta como resuelta o falso positivo. Solución rápida

Afectados (5): Suspicious inbox forwarding rule created — severidad critical (microsoftDefenderForOffice365), Sign-in from an anonymous IP address — severidad medium (microsoftDefenderForIdentity), Impossible travel activity — severidad low (microsoftDefenderForCloudApps), Email reported by user as phish — severidad medium (microsoftDefenderForOffice365), Malicious URL clicked in email — severidad low (microsoftDefenderForOffice365) · confianza: high

Alto **[CA-002] La autenticación heredada no está bloqueada**

Ninguna política de acceso condicional activa bloquea los protocolos de autenticación heredada (IMAP, POP, SMTP, ActiveSync antiguo).

Por qué importa: Los protocolos heredados no soportan MFA: un atacante que los use elude por completo cualquier exigencia de segundo factor. Son la vía preferida en los ataques de rociado de contraseñas.

Impacto de negocio: El MFA del inquilino puede ser sorteado en la práctica, anulando la inversión en control de identidad.

Recomendación: Crear una política de acceso condicional que bloquee los clientes de autenticación heredada para todos los usuarios, con un período previo en modo solo informe para detectar aplicaciones antiguas. Solución rápida

Afectados (1): — · confianza: high

Medio **[SEC-002] Controles de seguridad recomendados sin aplicar**

6 control(es) recomendado(s) por Microsoft no están aplicados; completarlos sumaría hasta 175 puntos. Los de mayor impacto son: Desplegar Defender for Endpoint en los equipos (+40); Bloquear la autenticación heredada (sin MFA posible) (+30); Política de acceso ante inicios de sesión de riesgo (+30); Política de acceso ante usuarios en riesgo (+30); Activar roles privilegiados solo cuando se necesiten (PIM) (+25).

Por qué importa: Cada control pendiente es una recomendación concreta de Microsoft basada en la configuración real del inquilino, no en un estándar genérico — y la mayoría no requiere licencias adicionales.

Impacto de negocio: Riesgo evitable con configuración ya disponible: el costo de aplicarlos es tiempo de administración, no inversión.

Recomendación: Priorizar los controles listados por puntaje ganado y planificar su aplicación; los de identidad (MFA, autenticación heredada) primero. Proyecto

Afectados (6): Desplegar Defender for Endpoint en los equipos (+40 pts), Bloquear la autenticación heredada (sin MFA posible) (+30 pts), Política de acceso ante inicios de sesión de riesgo (+30 pts), Política de acceso ante usuarios en riesgo (+30 pts), Activar roles privilegiados solo cuando se necesiten (PIM) (+25 pts) · confianza: high

Listado completo en `anexo_hallazgos.csv` (hallazgo SEC-002).

Medio **[CA-004] Políticas de acceso condicional en modo solo informe**

1 política(s) de acceso condicional están en modo solo informe: registran lo que harían, pero no bloquean nada.

Por qué importa: El modo solo informe existe para probar una política antes de aplicarla. Una política que lleva meses ahí da una falsa sensación de protección: aparece en la consola como configurada, y no protege.

Impacto de negocio: Controles que la organización cree tener y no tiene.

Recomendación: Revisar el registro de cada política en modo solo informe y activarla, o eliminarla si ya no aplica.
Solución rápida

Afectados (1): Bloquear autenticación heredada · confianza: high

Medio **[MAIL-002] DMARC publicado pero sin aplicar (p=none)**

1 dominio(s) publican DMARC con la política `p=none`, que solo pide informes y no instruye rechazar ni poner en cuarentena el correo suplantado.

Por qué importa: `p=none` es la etapa de observación de DMARC, no su objetivo: mientras siga ahí, el correo que suplanta al dominio se entrega igual. Es la diferencia entre tener la alarma instalada y tenerla conectada.

Impacto de negocio: Fraude por suplantación: facturas con datos bancarios alterados, instrucciones de pago falsas a nombre de un ejecutivo, y daño reputacional ante clientes que reciben correo fraudulento desde el dominio de la empresa.

Recomendación: Revisar los informes DMARC recibidos, corregir los emisores legítimos que no pasen, y endurecer la política a `p=quarantine` y luego `p=reject`. Proyecto

Afectados (1): contoso.example · confianza: high

Bajo **[SHARE-004] Uso compartido externo sin restricción por dominio**

El uso compartido externo está habilitado (Solo invitados que ya existen en el directorio) sin una lista de dominios permitidos o bloqueados.

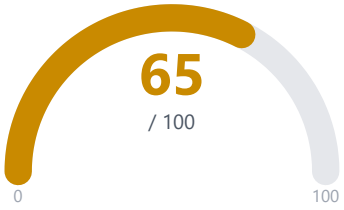
Por qué importa: Una lista de dominios permitidos limita el uso compartido a los socios reales del negocio, y convierte un error de tipeo en la dirección de un invitado en un rechazo en vez de en una filtración.

Impacto de negocio: Contenido compartible hacia cualquier dominio, incluidos correos personales de empleados y competidores.

Recomendación: Definir una lista de dominios permitidos con los socios y clientes con los que efectivamente se colabora. Proyecto

Afectados (1): — · confianza: medium

Postura de seguridad



Puntaje de seguridad de Microsoft

320 / 495 puntos

El promedio de organizaciones comparables es **47%**.

Controles pendientes de mayor impacto

Control recomendado	Puntos	Servicio
Desplegar Defender for Endpoint en los equipos	+40	Defender
Bloquear la autenticación heredada (sin MFA posible)	+30	AzureAD
Política de acceso ante inicios de sesión de riesgo	+30	AzureAD
Política de acceso ante usuarios en riesgo	+30	AzureAD
Activar roles privilegiados solo cuando se necesiten (PIM)	+25	AzureAD

Control de acceso

- Políticas de acceso condicional activas: **1** (además 1 en modo solo informe, que no bloquean nada)
- Valores predeterminados de seguridad: **deshabilitados**

Uso compartido externo

Nivel configurado en SharePoint y OneDrive: **Solo invitados que ya existen en el directorio**

Autenticación de correo por dominio

Dominio	SPF	DKIM	DMARC
contoso.example	Sí	Sí	p=none (solo monitoreo)

Detección y respuesta

- Alertas de Defender abiertas: **5** (1 de severidad alta o crítica)

Licenciamiento y costos

AHORRO POTENCIAL ESTIMADO

$499.000 CLP / mes

sumando todos los hallazgos de licenciamiento (LIC-*): licencias en cuentas deshabilitadas, puestos sin asignar, licencias sin actividad y superpuestas

Utilización por SKU

Licencia	Compradas	Asignadas	Utilización
Office 365 E3	95	84	88%
Exchange Online (Plan 1)	13	13	100%
Office 365 E1	39	39	100%

Tabla de remediación priorizada

Prioridad	ID	Hallazgo	Severidad	Esfuerzo	Afectados
1	EXIT-002	Cuentas activas y licenciadas con inactividad prolongada	Alto	Solución rápida	13
2	ALERT-001	Alertas de seguridad abiertas sin atender	Alto	Solución rápida	5
3	CA-002	La autenticación heredada no está bloqueada	Alto	Solución rápida	1
4	PRIV-003	Alta concentración de roles privilegiados	Medio	Proyecto	18
5	STALE-001	Cuentas habilitadas sin actividad reciente	Medio	Solución rápida	14
6	LIC-003	Licencias pagas sin actividad reciente	Medio	Solución rápida	13
7	LIC-002	Licencias compradas sin asignar	Medio	Solución rápida	11
8	SEC-002	Controles de seguridad recomendados sin aplicar	Medio	Proyecto	6
9	LIC-004	Licencias superpuestas en la misma cuenta	Medio	Solución rápida	4
10	EXIT-001	Cuentas deshabilitadas con licencias asignadas	Medio	Solución rápida	3
11	LIC-001	Licencias asignadas a cuentas deshabilitadas	Medio	Solución rápida	3
12	CA-004	Políticas de acceso condicional en modo solo informe	Medio	Solución rápida	1
13	MAIL-002	DMARC publicado pero sin aplicar (p=none)	Medio	Proyecto	1
14	USE-002	OneDrive sin uso reciente	Bajo	Proyecto	24
15	USE-003	Baja adopción de Microsoft Teams	Bajo	Proyecto	22
16	USE-001	Buzones sin actividad reciente	Bajo	Solución rápida	12
17	SHARE-004	Uso compartido externo sin restricción por dominio	Bajo	Proyecto	1

Anexo metodológico

Datos recolectados

Fuente	Estado	Registros	API
organization	Correcto	1	v1.0
users	Correcto	142	v1.0
subscribed_skus	Correcto	4	v1.0
user_registration_details	Correcto	142	v1.0
directory_roles	Correcto	5	v1.0
report_settings	Correcto	1	v1.0
office365_active_users	Correcto	132	v1.0
mailbox_usage	Correcto	132	v1.0
onedrive_usage	Correcto	119	v1.0
teams_user_activity	Correcto	119	v1.0
secure_score	Correcto	1	v1.0
secure_score_control_profiles	Correcto	20	v1.0
conditional_access_policies	Correcto	2	v1.0
security_defaults	Correcto	1	v1.0
sharepoint_settings	Correcto	1	v1.0
security_alerts	Correcto	8	v1.0
dns_domains	Correcto	1	dns
risky_users	Permiso denegado	0	v1.0

Módulos no evaluados

identity_risk: No evaluado — permiso faltante: risky_users

Listado completo de afectados

Cada hallazgo muestra hasta 10 cuentas u objetos en el cuerpo de este informe. El listado completo de cada hallazgo está en `anexo_hallazgos.csv`, junto a este archivo.

Metodología de licenciamiento y uso

Los hallazgos de uso (`USE-*`) y de licencias sin actividad (`LIC-003`) se basan en los informes de uso de Microsoft 365 (ventana de 30 días). Una cuenta se considera inactiva cuando no registra actividad en el servicio dentro del umbral de antigüedad configurado. La cuantificación de costos usa la tabla de precios del perfil del inquilino; un SKU sin precio configurado se reporta en cantidad de puestos pero sin cifra monetaria.

Metodología de seguridad

Los hallazgos de seguridad combinan cuatro fuentes: el Puntaje de seguridad de Microsoft y su catálogo de controles (`SEC-*`), las políticas de acceso condicional y los valores predeterminados de seguridad (`CA-*`), la configuración de uso compartido de

SharePoint/OneDrive (`SHARE-*`) y consultas DNS públicas sobre los dominios verificados del inquilino (`MAIL-*`). Los hallazgos `RISK-*` provienen de Entra ID Protection, que **requiere licencias Entra ID P2**: en inquilinos sin esa licencia el módulo aparece como no evaluado más arriba, lo que significa «no se pudo determinar», nunca «sin cuentas en riesgo».

Cómo se calculan las tendencias

La sección «Evolución mensual» compara los hallazgos de este informe con los del informe anterior por su identificador estable (p. ej. `MFA-001`). Un hallazgo se considera **resuelto** solo si su módulo fue evaluado en ambos informes y ya no aparece, y **nuevo** solo si su módulo también fue evaluado en el informe anterior; los módulos omitidos en cualquiera de los dos informes, o incorporados/retirados del análisis entre ambos, se excluyen de la comparación y se declaran como notas de comparabilidad. El movimiento de cuentas dentro de un hallazgo persistente se calcula comparando las listas de cuentas afectadas: una cuenta renombrada aparece como una salida y una entrada (limitación conocida). Los meses sin dato para una métrica se muestran como huecos en las líneas de tendencia, nunca como cero. La sección solo se incluye cuando existe al menos un informe anterior evaluado.

Análisis del consultor

Cuando el resumen ejecutivo incluye un apartado «Análisis del consultor», ese texto está **redactado por el consultor**, no generado por el motor: es su lectura del mes y su criterio de priorización. Todo lo demás en este informe —hallazgos, puntajes, tendencias y cifras— se deriva automáticamente de los datos recolectados.

Versión del informe

Motor de evaluación	El Guardián 0.8.0
Plantilla del informe	1.1
Fecha de generación	2026-08-17T12:02:54.018317-04:00

El motor determina *qué* se evalúa y con qué criterios; la plantilla determina *cómo* se presenta. Dos informes con el mismo par de versiones son comparables página por página.

Limitaciones conocidas

Solo se evalúa la configuración a nivel de inquilino: los hallazgos de uso compartido (`SHARE-*`) reflejan la configuración global de SharePoint/OneDrive, no las excepciones por sitio ni los enlaces ya compartidos. Un inquilino correctamente configurado hoy puede seguir teniendo enlaces públicos creados antes del cambio.

La política de acceso condicional se evalúa por su definición, no por su efecto: se analiza qué exige cada política activa, no a cuántos inicios de sesión reales se aplicó. Las exclusiones de usuarios o grupos dentro de cada política no se descuentan del análisis.

MFA registrado no equivale a MFA exigido: los hallazgos de MFA (`MFA-001` / `MFA-002`) se basan en `isMfaRegistered`, que indica si la cuenta tiene registrado un método de autenticación fuerte — no si ese método es efectivamente exigido al iniciar sesión. Una cuenta puede tener un método registrado y aun así no tener MFA exigido (por ejemplo, sin una política de acceso condicional que lo requiera); estas cuentas no aparecen como afectadas en estos hallazgos.