mayavirtual

VULNERABILITY ASSESSMENT

Informe
Cyber Threat Discovery

Evaluación de seguridad y descubrimiento de amenazas sobre la infraestructura crítica de ACME Corporation S.A., realizada bajo un enfoque no intrusivo de solo lectura.

CLIENTE	FECHA DE EMISIÓN	VERSIÓN	CLASIFICACIÓN
ACME Corporation S.A.	9 de junio de 2026	1.0	Confidencial

SERVIDORES
3
Linux y Windows Server

BASES DE DATOS
2
Oracle y PostgreSQL

FIREWALL
1
Perímetro corporativo

Mayavirtual · Consultoría de Ciberseguridad
Guatemala · Servicio Cyber Threat Discovery · ctd@mayavirtual.net

Ref. CTD-2026-ACME-001
6 activos en alcance · 34 hallazgos

PARA DIRECCIÓN · NO TÉCNICO

01 Resumen ejecutivo

La evaluación realizada por Mayavirtual sobre los 6 activos críticos de **ACME Corporation S.A.** identificó un **nivel de riesgo global ALTO**. Se detectaron debilidades significativas en el endurecimiento (hardening) de servidores y bases de datos, reglas de firewall demasiado permisivas y controles de auditoría insuficientes. Aunque ningún hallazgo evidencia un compromiso activo, la combinación de **4 hallazgos críticos** con servicios expuestos eleva la probabilidad de un incidente si no se ejecuta el plan de remediación en los plazos sugeridos. La mayoría de los riesgos son corregibles con medidas de configuración de bajo costo y alto impacto («quick wins»).

NIVEL DE RIESGO GLOBAL

ALTO

Requiere acción priorizada en las próximas semanas.

Atención inmediata

PUNTUACIÓN DE RIESGO

72 /100

Índice ponderado por severidad y exposición de activos.

+18 vs. sector

TOTAL DE HALLAZGOS

34

4 críticos · 9 altos · 14 medios · 7 bajos.

13 priorizados

NIVEL DE HARDENING

58 %

Controles CIS aplicados sobre los activos evaluados.

Meta ≥ 85%

ACTIVOS EVALUADOS

6 /6

Cobertura completa del alcance contratado.

100% del alcance

CUMPLIMIENTO CIS

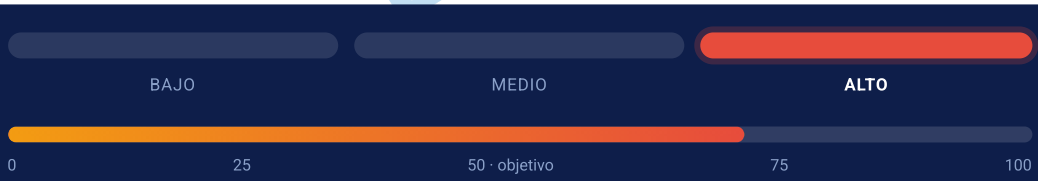
64 %

Conformidad frente a los benchmarks de referencia.

Brecha de 21 pts

SEMÁFORO DE RIESGO

ALTO

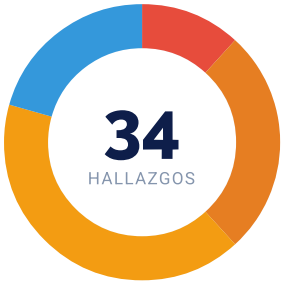


ESTADÍSTICA Y MÉTRICAS DE RIESGO

02 Riesgo cuantificable

Distribución de hallazgos por severidad

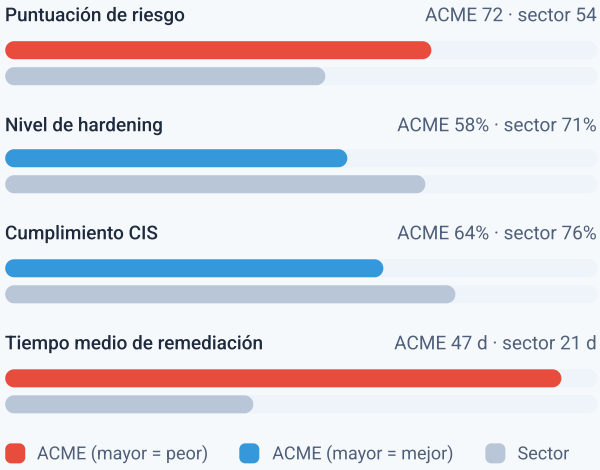
34 hallazgos totales · clasificación CVSS v3.1



Crítico	4	12%
Alto	9	26%
Medio	14	41%
Bajo	7	21%

Comparativa contra benchmark del sector

ACME vs. promedio del sector financiero/servicios (LATAM)



Riesgo por activo

Puntuación ponderada (0–100) y severidad máxima detectada por cada activo en alcance

ACTIVO	TIPO	HALLAZGOS	SCORE DE RIESGO	SEVERIDAD MÁX.
App Server Linux SRV-LNX-01 · 10.20.4.11	Servidor	8	81	Crítico
Base de datos Oracle DB-ORA-01 · 10.20.4.31	Base de datos	6	78	Crítico
Windows Server 2019 SRV-WIN-02 · 10.20.4.12	Servidor	7	74	Alto
Firewall perimetral FW-PERIM-01 · 10.20.0.1	Firewall	5	70	Alto
DB / App host Linux SRV-LNX-03 · 10.20.4.13	Servidor	5	66	Alto
Base de datos PostgreSQL DB-PG-02 · 10.20.4.32	Base de datos	3	49	Medio

PÉRDIDA POTENCIAL ESTIMADA

Q. 1.85 M

Exposición financiera ante un escenario de explotación de los hallazgos críticos.

ESTIMACIÓN

VENTANA DE EXPOSICIÓN

47 días

Antigüedad media de las vulnerabilidades críticas sin mitigar. ESTIMACIÓN

ACTIVOS EN RIESGO ALTO/CRÍTICO

5 de 6

83% del alcance presenta al menos un hallazgo de severidad alta o crítica.

Las cifras económicas y temporales son estimaciones ilustrativas calculadas con modelos de exposición simplificados; no constituyen una valoración actuarial ni una garantía de pérdida.

PARTE TÉCNICA · 6 HALLAZGOS REPRESENTATIVOS

03 Hallazgos técnicos detallados

Se presentan los hallazgos de mayor relevancia detectados durante la evaluación. Cada ficha incluye su clasificación de severidad, vector CVSS, activo afectado, evidencia técnica y recomendación de remediación.

CTD-001 SSH con cifrado débil y acceso directo de root habilitado

Crítico **8.6** CVSS

ACTIVO AFECTADO	CATEGORÍA	VECTOR
SRV-LNX-01 · 10.20.4.11	CIS 5.2 · CWE-326	AV:N/AC:L/PR:N/UI:N

DESCRIPCIÓN TÉCNICA

El servicio **OpenSSH** del servidor permite el inicio de sesión directo como **root** y acepta algoritmos de cifrado e intercambio de claves obsoletos (CBC, `diffie-hellman-group1`). Esta combinación facilita ataques de fuerza bruta sobre la cuenta privilegiada y deja el canal expuesto a degradación criptográfica.

EVIDENCIA

```
# /etc/ssh/sshd_config (extracto)
PermitRootLogin yes
Ciphers aes128-cbc,3des-cbc,aes256-cbc
KexAlgorithms diffie-hellman-group1-sha1
PasswordAuthentication yes

$ ssh -Q cipher root@10.20.4.11
# >> servidor negocia 3des-cbc (débil)
```

IMPACTO

Un atacante con acceso a la red podría comprometer la cuenta root mediante fuerza bruta o interceptar la sesión, obteniendo control total del servidor de aplicaciones y pivotando hacia las bases de datos.

RECOMENDACIÓN DE REMEDIACIÓN

- Establecer **PermitRootLogin no** y administrar mediante usuarios con sudo.
- Restringir a cifrados AEAD modernos (`chacha20-poly1305`, `aes256-gcm`) y KEX `curve25519`.
- Migrar a autenticación por clave pública y deshabilitar contraseñas.

CTD-002 Oracle con cuentas por defecto y privilegios excesivos

Crítico **9.1** CVSS

ACTIVO AFECTADO	CATEGORÍA	VECTOR
DB-ORA-01 · 10.20.4.31	CIS DB · CWE-1188	AV:N/AC:L/PR:L/UI:N

DESCRIPCIÓN TÉCNICA

La instancia **Oracle Database** conserva cuentas predeterminadas activas con contraseñas conocidas y otorga el rol DBA a usuarios de aplicación. Existe además el privilegio PUBLIC sobre paquetes sensibles, ampliando innecesariamente la superficie de ataque.

EVIDENCIA

```
SQL> SELECT username, account_status FROM dba_users
       WHERE username IN ('SCOTT','DBSNMP','OUTLN');
USERNAME     ACCOUNT_STATUS
SCOTT        OPEN      -- pass por defecto: tiger
DBSNMP       OPEN
SQL> SELECT grantee FROM dba_role_privs WHERE granted_role='DBA';
APP_USER     -- rol DBA sobre cuenta de aplicación
```

IMPACTO

Acceso no autorizado a datos sensibles, escalada a administrador de base de datos y posible ejecución de código en el host. Riesgo directo de exfiltración masiva de información de clientes.

RECOMENDACIÓN DE REMEDIACIÓN

- Bloquear o eliminar cuentas por defecto (SCOTT, DBSNMP, etc.) y rotar credenciales.
- Aplicar mínimo privilegio: revocar DBA de cuentas de aplicación y crear roles específicos.
- Revocar grants PUBLIC sobre paquetes UTL_* y habilitar auditoría unificada.

PARTE TÉCNICA · CONTINUACIÓN

03 Hallazgos técnicos detallados

CTD-003 Firewall con reglas «any-any» heredadas

Alto 7.5 CVSS

ACTIVO AFECTADO	CATEGORÍA	VECTOR
FW-PERIM-01 · 10.20.0.1	CIS FW · CWE-284	AV:N/AC:L/PR:N/UI:N

DESCRIPCIÓN TÉCNICA

El firewall perimetral mantiene **reglas permisivas heredadas** que autorizan tráfico any → any en varios puertos, sin registro asociado. La política carece de una regla final de denegación explícita, por lo que el orden de evaluación deja servicios internos accesibles desde redes no confiables.

EVIDENCIA

```
# Política de firewall (extracto exportado)
id   src        dst        service   action  log
142  any        any        tcp/3389  accept   off
143  any        10.20.4.0  any       accept   off
198  any        any        any       accept   off   # regla heredada 2019
# >> ausencia de regla final 'deny any-any'
```

IMPACTO

Exposición de RDP y servicios internos a Internet, facilitando reconocimiento y explotación. La falta de logging impide la detección y el análisis forense de un eventual incidente.

RECOMENDACIÓN DE REMEDIACIÓN

- Eliminar reglas any-any heredadas y aplicar mínimo privilegio por servicio y origen.
- Añadir regla final explícita deny any-any con registro activado.
- Habilitar logging en todas las reglas y revisar la base trimestralmente.

CTD-004 Ausencia de parches críticos en Windows Server

Alto 8.1 CVSS

ACTIVO AFECTADO	CATEGORÍA	VECTOR
SRV-WIN-02 · 10.20.4.12	CIS 1.x · CWE-1104	AV:N/AC:H/PR:N/UI:N

DESCRIPCIÓN TÉCNICA

El servidor **Windows Server 2019** presenta un retraso de parches superior a 90 días, con boletines de seguridad críticos pendientes y el servicio SMBv1 aún habilitado. Esto lo hace vulnerable a familias de exploits ampliamente difundidas.

EVIDENCIA

```
PS> Get-HotFix | Sort InstalledOn -Desc | Select -First 1
InstalledOn : 2026-03-04   # > 90 días sin parches
PS> Get-WindowsOptionalFeature -Online -FeatureName SMB1Protocol
State : Enabled
# Boletines críticos pendientes: 7
```

IMPACTO

Ejecución remota de código y propagación lateral tipo gusano a través de SMBv1. Un único host sin parchear puede comprometer todo el segmento de servidores.

RECOMENDACIÓN DE REMEDIACIÓN

- Aplicar los parches críticos pendientes y establecer una ventana mensual de actualización.
- Deshabilitar SMBv1 en todo el parque.
- Implementar gestión centralizada de parches (WSUS/Intune) con SLA de 15 días para críticos.

PARTE TÉCNICA · CONTINUACIÓN

03 Hallazgos técnicos detallados

CTD-005 Políticas de contraseñas deficientes en el dominio

Medio 5.8 CVSS

ACTIVO AFECTADO	CATEGORÍA	VECTOR
Dominio AD · ACME.LOCAL	CIS 1.1 · CWE-521	AV:N/AC:L/PR:L/UI:N

DESCRIPCIÓN TÉCNICA

La política de contraseñas del dominio permite **longitud mínima de 6 caracteres**, sin bloqueo por intentos fallidos ni complejidad obligatoria. No existe verificación contra diccionarios de contraseñas comprometidas.

EVIDENCIA

```
PS> Get-ADDefaultDomainPasswordPolicy
MinPasswordLength      : 6
ComplexityEnabled      : False
LockoutThreshold       : 0   # sin bloqueo
MaxPasswordAge         : 0.00:00:00
```

IMPACTO

Mayor probabilidad de éxito en ataques de fuerza bruta y password spraying contra cuentas de usuario y servicio, sin bloqueo que los frene.

RECOMENDACIÓN DE REMEDIACIÓN

- Exigir longitud mínima de 14 caracteres y umbral de bloqueo de 5 intentos.
- Habilitar verificación contra listas de contraseñas filtradas y MFA para acceso remoto.

CTD-006 Ausencia de logging y auditoría centralizada

Medio 6.2 CVSS

ACTIVO AFECTADO	CATEGORÍA	VECTOR
Múltiples activos	CIS 8.x · CWE-778	AV:N/AC:L/PR:L/UI:N

DESCRIPCIÓN TÉCNICA

No existe un repositorio centralizado de registros (SIEM/syslog). Los eventos de seguridad se almacenan localmente, con rotación agresiva y sin correlación, lo que impide la detección temprana y el análisis forense.

EVIDENCIA

```
$ grep -i "remote" /etc/rsyslog.conf
# >> sin destino remoto configurado (*. @siem)
$ auditctl -l
No rules
# Windows: reenvío de eventos (WEF) no configurado
```

IMPACTO

Incapacidad de detectar actividad maliciosa en curso y pérdida de evidencia ante un incidente, prolongando el tiempo de detección y respuesta.

RECOMENDACIÓN DE REMEDIACIÓN

- Desplegar recolección centralizada (syslog remoto / Windows Event Forwarding) hacia un SIEM.
- Definir reglas de auditoría (`auditd`, políticas avanzadas de Windows) y retención mínima de 12 meses.

ACCIONES PRIORIZADAS

04 Plan de remediación priorizado

REF.	ACCIÓN DE REMEDIACIÓN	PRIORIDAD	ESFUERZO	RESPONSABLE SUGERIDO
CTD-002	Bloquear cuentas Oracle por defecto y revocar privilegios DBA excesivos	P1 · Crítica	●○○ Bajo · 1–2 d	DBA / Administrador Oracle
CTD-001	Endurecer SSH: deshabilitar root, cifrados modernos, claves públicas	P1 · Crítica	●○○ Bajo · 1 d	Administrador de sistemas Linux
CTD-004	Aplicar parches críticos de Windows y deshabilitar SMBv1	P2 · Alta	●●○ Medio · 3–5 d	Equipo de infraestructura Windows
CTD-003	Depurar reglas any-any del firewall y activar logging	P2 · Alta	●●○ Medio · 3–5 d	Equipo de redes / seguridad perimetral
CTD-005	Reforzar política de contraseñas del dominio y habilitar MFA	P3 · Media	●●○ Medio · 4 d	Administrador de Active Directory
CTD-006	Implementar logging centralizado (SIEM) y reglas de auditoría	P4 · Programada	●●● Alto · 3–4 sem	SOC Mayavirtual + TI ACME

✓ Quick wins (0–2 semanas)

Alto impacto y bajo esfuerzo · ejecutar de inmediato

- **CTD-001 · CTD-002** — endurecimiento de SSH y limpieza de cuentas Oracle, solo configuración.
- Deshabilitar **SMBv1** y servicios heredados innecesarios.
- Activar **logging** en reglas de firewall existentes.

→ Mejoras a mediano plazo (1–3 meses)

Requieren proyecto, presupuesto o cambio de proceso

- Despliegue de **SIEM** y correlación centralizada (CTD-006).
- Programa formal de **gestión de parches** con SLA por severidad.
- Revisión periódica de **reglas de firewall** y línea base CIS automatizada.

ESTÁNDARES Y ENFOQUE

05 Metodología y alcance

La evaluación se ejecutó bajo un **enfoque no intrusivo de solo lectura**, sin explotación activa ni impacto sobre la disponibilidad de los sistemas en producción, alineada con los siguientes marcos de referencia.

CIS Benchmarks

Líneas base de endurecimiento para Linux, Windows, Oracle y firewall.

NIST SP 800-115

Guía técnica para evaluaciones de seguridad de la información.

ISO/IEC 27001

Marco de controles de gestión de seguridad de la información.

1. **Reconocimiento** — Inventario y delimitación del alcance contratado.
2. **Enumeración** — Identificación de servicios y configuración expuesta.
3. **Análisis** — Contraste contra líneas base CIS y CVSS v3.1.
4. **Validación** — Verificación manual y descarte de falsos positivos.
5. **Reporte** — Priorización de riesgos y plan de remediación.

! Documento de ejemplo · aviso legal

Este es un documento de muestra con datos 100% ficticios. ACME Corporation S.A. es una empresa imaginaria; los activos, direcciones IP, hallazgos, puntuaciones y cifras económicas fueron inventados con fines ilustrativos y no representan ningún sistema, organización o evaluación real.

ELABORADO POR

Equipo Cyber Threat Discovery · Mayavirtual

mayavirtual