



Empresa Ejemplo, S.A. de C.V.

DOMINIO

empresa-ejemplo.example

FECHA

Octubre 2026

REFERENCIA

NG-EJEMPLO-001

ALCANCE

Revisión externa autorizada, sin exploits. Auditoría cloud de solo lectura (en este ejemplo, AWS; también Azure, Google Cloud y Oracle Cloud según el proyecto).

1. Resumen ejecutivo

2

Críticos

5

Altos

8

Medios

100%

Con evidencia

La superficie externa de Empresa Ejemplo tiene dos hallazgos críticos que conviene atender esta semana: credenciales de empleados en un corpus de brechas y un

bucket de respaldos con lectura pública. Ambos se verificaron con evidencia y ninguno requiere explotar nada para confirmarse.

Detrás de ellos hay cinco hallazgos altos, la mayoría de configuración cloud y TLS, y ocho medios que mejoran la postura general sin urgencia inmediata.

Qué atender primero

ESTA SEMANA

Rotar credenciales filtradas y cerrar el acceso público del bucket (NG-01, NG-02).

30 DÍAS

Reducir permisos del rol de despliegue, retirar TLS antiguo y proteger el panel de administración (NG-03 a NG-07).

90 DÍAS

Higiene de DNS, cabeceras y cifrado en reposo (NG-08 a NG-15).

2. Alcance y metodología

Revisión externa autorizada por escrito. Fuentes: registros públicos de certificados, motores de infraestructura expuesta, corpus de brechas y enumeración activa.

Auditoría cloud con acceso de solo lectura acordado en el alcance (en este ejemplo, AWS).

Cada hallazgo se prueba antes de anotarse. El reporte distingue lo verificado de lo observado y de los indicios.

Niveles de validación

Verificado Se comprobó con evidencia reproducible.

Observado Se observó la señal; falta confirmar impacto con una prueba autenticada.

Indicio Señal débil; se lista aparte y no cuenta como hallazgo.

3. Hallazgos

ID	HALLAZGO	SEVERIDAD	FUENTE	EVIDENCIA	ESTADO
NG - 01	Credenciales filtradas (info-stealer)	CRIT	Brechas	registro verificado	Verificado
NG - 02	Bucket de respaldos con lectura pública	CRIT	Cloud AWS	listado público	Verificado
NG - 03	IAM con privilegio excesivo	HIGH	AWS	IAM policy	Verificado
NG - 04	TLS con protocolo obsoleto	HIGH	Handshake	TLS version	Verificado
NG - 05	Panel de administración expuesto sin MFA visible	HIGH	Hosts vivos	status 200 + login	Observado
NG - 06	Clave de acceso de servicio sin rotar en más de un año	HIGH	AWS	credential report	Verificado
NG - 07	Certificado próximo a vencer en servicio crítico	HIGH	Handshake	fecha de expiración	Verificado
NG - 08	Subdominio de desarrollo expuesto	MED	Hosts vivos	status 200	Verificado
NG - 09	SPF en softfail, no hardfail	MED	DNS	dig TXT	Verificado
NG - 10	DMARC en modo monitoreo (p=none)	MED	DNS	dig TXT	Verificado

ID	HALLAZGO	SEVERIDAD	FUENTE	EVIDENCIA	ESTADO
NG - 11	Cabeceras de seguridad ausentes (HSTS, CSP)	MED	Handshake	HTTP headers	Verificado
NG - 12	Versión del servidor visible en el banner	MED	Hosts vivos	HTTP banner	Observado
NG - 13	Registros DNS huérfanos	MED	DNS	CNAME sin destino	Verificado
NG - 14	Puerto de administración abierto a un rango amplio	MED	AWS	security group	Verificado
NG - 15	Dos volúmenes sin cifrado en reposo	MED	AWS	EBS config	Verificado

Hallazgos desarrollados

NG-01

CRIT

Credenciales filtradas (infostealer)

IMPACTO

Con credenciales válidas de un empleado, un atacante puede entrar a servicios sin pasar por ninguna defensa de red.

RECOMENDACIÓN

- Rotar la contraseña de las cuentas afectadas y revocar sesiones activas.
- Activar MFA en todos los servicios donde esa cuenta tenga acceso.
- Revisar el equipo del usuario: el origen suele ser un infostealer en el endpoint.

EVIDENCIA

```
corpus: breach-corpus (registro de infostealer)
cuenta : a***@empresa-ejemplo.example
fecha  : coincide con la ventana de infección reportada
contraseña: [censurada en este reporte]
```

VALIDACIÓN

Verificado: el registro del corpus coincide en dominio y fecha. No se probó acceso a ningún servicio.

Bucket de respaldos con lectura pública

IMPACTO

Los respaldos pueden contener datos de clientes y secretos de aplicación. Cualquier persona en Internet puede listarlos y descargarlos.

RECOMENDACIÓN

- Bloquear el acceso público a nivel de cuenta (S3 Block Public Access).
- Revisar los registros de acceso para saber si hubo descargas ajenas.
- Rotar cualquier secreto que haya vivido en esos respaldos.

EVIDENCIA

```
$ curl -s https://respaldos-ejemplo.s3.amazonaws.com/ | head
<ListBucketResult>
  <Name>respaldos-ejemplo</Name>
  <Contents><Key>db/2026-09-30.sql.gz</Key>...
(listado público; no se descargó ningún objeto)
```

VALIDACIÓN

Verificado: el listado es visible sin autenticación. No se descargó contenido.

NG-03

HIGH

IAM con privilegio excesivo

IMPACTO

Un rol con permisos de administrador amplía el daño de cualquier credencial comprometida: el atacante hereda el control de la cuenta.

RECOMENDACIÓN

- Reemplazar la política por permisos mínimos para el despliegue.
- Separar el rol de despliegue del de ejecución.
- Activar alertas de uso inusual del rol.

EVIDENCIA

```
{
  "RoleName": "app-deploy",
  "Statement": [{ "Effect": "Allow", "Action": "*", "Resource": "*" }]
}
```

VALIDACIÓN

Verificado: revisión de la política con acceso de solo lectura acordado en el alcance.

NG-04

HIGH

TLS con protocolo obsoleto

IMPACTO

Los protocolos TLS antiguos tienen debilidades conocidas y pueden incumplir requisitos de cumplimiento.

RECOMENDACIÓN

- Deshabilitar TLS 1.0 y 1.1; permitir solo TLS 1.2 y 1.3.
- Verificar que ningún cliente legítimo dependa del protocolo antiguo.

EVIDENCIA

```
$ openssl s_client -connect portal.empresa-ejemplo.example:443 -tls1
Protocol  : TLSv1
Cipher    : ECDHE-RSA-AES256-SHA
Verify return code: 0 (ok)
```

VALIDACIÓN

Verificado: el servidor aceptó el handshake con TLS 1.0.

NG-09

MED

SPF en softfail, no hardfail

IMPACTO

Con SPF en softfail, un correo falsificado con el dominio puede llegar a la bandeja de entrada.

RECOMENDACIÓN

- Pasar SPF a -all cuando DMARC esté en cuarentena o rechazo.
- Publicar DKIM para todos los remitentes legítimos.

EVIDENCIA

```
$ dig +short TXT empresa-ejemplo.example  
"v=spf1 include:_spf.proveedor.example ~all"
```

VALIDACIÓN

Verificado: el registro DNS público lo confirma.

4. Plan de remediación

Orden sugerido según severidad real y esfuerzo. Las fechas se acuerdan en la llamada de cierre.

ESTA SEMANA

NG-01 Credenciales filtradas (infostealer)

NG-02 Bucket de respaldos con lectura pública

30 DÍAS

- NG-03 IAM con privilegio excesivo
- NG-04 TLS con protocolo obsoleto
- NG-05 Panel de administración expuesto sin MFA visible
- NG-06 Clave de acceso de servicio sin rotar en más de un año
- NG-07 Certificado próximo a vencer en servicio crítico

90 DÍAS

- NG-08 Subdominio de desarrollo expuesto
- NG-09 SPF en softfail, no hardfail
- NG-10 DMARC en modo monitoreo (p=none)
- NG-11 Cabeceras de seguridad ausentes (HSTS, CSP)
- NG-12 Versión del servidor visible en el banner
- NG-13 Registros DNS huérfanos
- NG-14 Puerto de administración abierto a un rango amplio
- NG-15 Dos volúmenes sin cifrado en reposo

5. Notas

Este documento es un ejemplo con datos ficticios: dominio, direcciones, cuentas y resultados no corresponden a ninguna empresa real.

Un reporte real incluye la evidencia completa de cada hallazgo, la remediación detallada y una sesión de resultados. El alcance y los entregables se definen en la propuesta.