

EscanearVulnerabilidades

Informe de Seguridad Web

URL https://banco.santander.cl/personas
Dominio banco.santander.cl
Fecha 14 de julio de 2026 a las 17:26

Checks 9 pruebas
Hallazgos 44 totales
Problemas 8 detectados

C

67/100

puntos de seguridad



RESUMEN EJECUTIVO

El análisis de seguridad técnica realizado sobre el sitio web ha arrojado una puntuación de 67/100, lo que equivale a una nota C. Durante la evaluación se ejecutaron 9 checks pasivos, resultando en 6 verificaciones satisfactorias, 1 advertencia y 2 fallos críticos en la configuración del servidor. El portal demuestra una gestión correcta de su certificado digital, pero presenta carencias severas en la implementación de cabeceras de seguridad y en la redirección forzada de tráfico cifrado. Debido a la ausencia de políticas para mitigar ataques de inyección y suplantación, se concluye que el sitio es actualmente vulnerable ante amenazas comunes de la web.

Resumen de Riesgos



Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 59 dias
Cabeceras de Seguridad	20	FALLO	Solo 1/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	0	FALLO	No hay redireccion HTTP a HTTPS
Deteccion CMS	100	OK	No se detecto un CMS conocido
Version CMS Expuesta	100	OK	No se detecto version de CMS expuesta
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	60	AVISO	Falta sitemap.xml
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 59 dias

- INFO Certificado valido
El certificado SSL es valido y de confianza
- INFO Dias hasta expiracion
59 dias restantes (expira: 2026-09-11T23:59:59.000Z)
- INFO Fecha de emision
Emitido desde: 2025-09-11T00:00:00.000Z
- INFO Puerto 443
Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 20/100

Estado: FALLO

Solo 1/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

- ALTO Content-Security-Policy
Falta — Previene XSS y ataques de inyeccion de contenido

- ALTO

X-Frame-Options
Falta — Protege contra clickjacking
- INFO

Strict-Transport-Security
Presente: max-age=2628000 ; includeSubDomains
- MEDIO

X-Content-Type-Options
Falta — Evita MIME-type sniffing
- MEDIO

Referrer-Policy
Falta — Controla la informacion de referer enviada
- MEDIO

Permissions-Policy
Falta — Restringe APIs del navegador (camara, micro, etc.)

Redireccion HTTPS — 0/100

Estado: FALLO

No hay redireccion HTTP a HTTPS

- ALTO

HTTP !' HTTPS redireccion
HTTP 403 — No dirige a HTTPS
- INFO

HSTS (Strict-Transport-Security)
HSTS activo: max-age=2628000 ; includeSubDomains
- BAJO

HSTS includeSubDomains
HSTS cubre subdominios
- MEDIO

HSTS max-age
max-age=2628000 (30 dias) — Recomendado minimo 180 dias
- INFO

Respuesta HTTPS
HTTPS responde con status 403

Deteccion CMS — 100/100

Estado: OK

No se detecto un CMS conocido

- INFO

WordPress
No detectado
- INFO

Joomla
No detectado
- INFO

Drupal
No detectado
- INFO

Magento
No detectado
- INFO

Shopify
No detectado
- INFO

PrestaShop
No detectado
- INFO

Wix
No detectado
- INFO

Squarespace
No detectado

Version CMS Expuesta — 100/100

Estado: OK

No se detecto version de CMS expuesta

- INFO

Archivo /readme.html
No accesible (correcto)
- INFO

Archivo /README.txt
No accesible (correcto)
- INFO

Version CMS
No se detecta ninguna version expuesta

Seguridad de Cookies — 100/100

Estado: OK

No se encontraron cookies

● INFO **Cookies detectadas**
El sitio no establece cookies en la respuesta inicial

Contenido Mixto — 100/100

Estado: OK
No se detecto contenido mixto

● INFO **Contenido mixto**
Todos los recursos se cargan por HTTPS

Robots.txt y Sitemap — 60/100

Estado: AVISO
Falta sitemap.xml

- INFO **robots.txt**
Presente (24 bytes)
- INFO **Reglas robots.txt**
0 Disallow, 1 Allow
- BAJO **sitemap.xml**
No encontrado (HTTP 403)
- BAJO **security.txt**
No encontrado — Recomendado para política de divulgacion

Puertos Abiertos — 100/100

Estado: OK
2 puerto(s) abierto(s), todos esperados

- INFO **Puerto 21 (FTP)**
Cerrado — Transferencia de archivos sin cifrar
- INFO **Puerto 22 (SSH)**
Cerrado — Acceso remoto seguro
- INFO **Puerto 23 (Telnet)**
Cerrado — Acceso remoto sin cifrar
- INFO **Puerto 25 (SMTP)**
Cerrado — Envio de correo
- INFO **Puerto 80 (HTTP)**
Abierto (esperado) — Servidor web
- INFO **Puerto 443 (HTTPS)**
Abierto (esperado) — Servidor web seguro
- INFO **Puerto 3306 (MySQL)**
Cerrado — Base de datos MySQL expuesta
- INFO **Puerto 3389 (RDP)**
Cerrado — Escritorio remoto Windows
- INFO **Puerto 5432 (PostgreSQL)**
Cerrado — Base de datos PostgreSQL expuesta
- INFO **Puerto 6379 (Redis)**
Cerrado — Cache Redis sin autenticacion por defecto
- INFO **Puerto 8080 (HTTP-Alt)**
Cerrado — Servidor web alternativo / proxy
- INFO **Puerto 27017 (MongoDB)**
Cerrado — Base de datos MongoDB expuesta

Analisis de Seguridad

VULNERABILIDADES DETECTADAS

[HIGH] Content-Security-Policy: La ausencia de esta política permite la ejecución de scripts maliciosos y ataques de inyección de contenido (XSS).
[HIGH] X-Frame-Options: Al no estar configurada, el sitio permite que su contenido sea cargado en marcos externos, facilitando ataques de clickjacking.
[HIGH] Redirección HTTP a HTTPS: El servidor responde con errores 403 y no redirige automáticamente las conexiones inseguras hacia el protocolo cifrado.
[MEDIUM] X-Content-Type-Options: La falta de esta cabecera deja a los usuarios expuestos a ataques de MIME-type sniffing por parte del navegador.

[MEDIUM] Referrer-Policy: No se controla la información de procedencia enviada a otros dominios, lo que podría filtrar rutas internas de navegación.

[MEDIUM] Permissions-Policy: No se restringen las capacidades del navegador, permitiendo potencialmente el acceso a hardware o APIs sin restricciones de seguridad.

[MEDIUM] HSTS (HTTP Strict Transport Security): El parámetro max-age está configurado en solo 30 días, un tiempo inferior al estándar recomendado de 180 días.

[LOW] sitemap.xml: El archivo de mapa del sitio no fue encontrado, lo que dificulta la auditoría completa de los recursos públicos disponibles.