



Website Security Test

Estado de seguridad de los sitios web

División de Auditoría interna
Riesgo Tecnológico y Ciberseguridad
Chile

Fecha de realización: 2023-04-21

Tabla de contenidos

1	Introducción	2
2	Resumen General	3
3	Resumen por sitio web evaluado	4
3.1	www.u-cursos.cl	4
3.2	ucampus.uchile.cl	5
4	Resumen por Test	6
4.1	Revisión del código de estado HTTP	6
4.2	Revisión Métodos HTTP	7
4.3	Revisión Robots	8
4.4	Revisión Cookies	9
4.5	Revisión Cabeceras	10
4.6	Revisión Certificados	11
4.7	Revisión Cifrados y Protocolos	15
5	Anexos	17
5.1	Revisión del código de estado HTTP	17
5.2	Revisión Métodos HTTP	18
5.3	Revisión Robots	19
5.4	Revisión Cookies	20
5.5	Revisión Cabeceras	21
5.6	Revisión Certificados	22
5.7	Revisión Cifrados y Protocolos	23

1 Introducción

El presente informe muestra en detalle la evaluación del estado de seguridad perimetral de uno o varios sitios web expuestos a internet por parte de Banco Santander.

El objetivo de la revisión es dar a conocer las debilidades de seguridad detectada en los sitios web elegidos, aplicando un conjunto de pruebas de seguridad con el objetivo de analizar los riesgos expuestos que puedan afectar la confidencialidad y disponibilidad de la información accesible, tratada, almacenada y/o transmitida por estos activos.





La revisión se ha realizado siguiendo un enfoque de caja negra, es decir, sin disponer de información previa de los sistemas de información existentes y partiendo únicamente de la información relativa al alcance de la revisión (un sitio web específico).

Esto consiste en la realización de pruebas para cada sitio web, pruebas cuyo detalle está en su respectiva sección.

Las pruebas realizadas, como el cálculo de puntaje están acorde a lo que Banco Santander establece como estándar de seguridad.

La creación de este informe como también el cálculo de los ratings y puntajes están realizados de forma automática

A continuación se presenta la simbología presente en el informe la cual se usará para el puntaje de cada prueba a realizar y el rating total de la página;

-  Bueno
-  Aceptable
-  A mejorar
-  Insatisfactorio

A cada página web se le realizará un control con las siguientes pruebas;

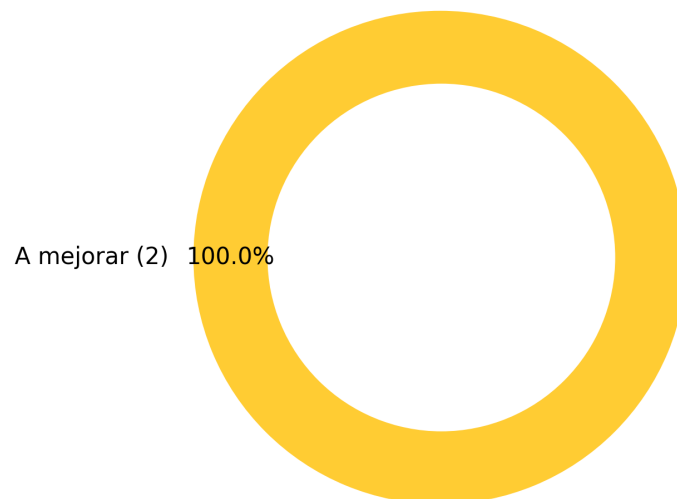
- Revisión del código de estado HTTP
- Revisión Métodos HTTP
- Revisión Robots
- Revisión Cookies
- Revisión Cabeceras
- Revisión Certificados
- Revisión Cifrados y Protocolos

2 Resumen General

A continuación se presenta la recopilación de los resultados obtenidos en la revisión de seguridad aplicada a los siguientes sitios web, a través de la asignación de un rating ponderado en base a las pruebas realizadas:

Sitio Web	Rating
www.u-cursos.cl	●
ucampus.uchile.cl	●

En el siguiente gráfico se puede apreciar la distribución de los resultados obtenidos en base al nivel de seguridad que refleja el rating asignado a cada sitio web evaluado:



3 Resumen por sitio web evaluado

3.1 www.u-cursos.cl

A continuación se muestra un resumen del resultado obtenido en cada prueba realizada a este sitio web, lo cual sustenta el rating asignado:



Nombre del test	Criticidad	Puntaje
Revisión del código de estado HTTP	bajo	●
Revisión Métodos HTTP	bajo	●
Revisión Robots	bajo	●
Revisión Cookies	medio	●
Revisión Cabeceras	medio	●
Revisión Certificados	alto	●
Revisión Cifrados y Protocolos	alto	●

A continuación, se exponen las principales debilidades de seguridad localizadas en este sitio web:

Revisión Métodos HTTP

- Métodos HTTP inseguros habilitados: PUT, DELETE, OPTIONS, TRACE, PATCH, TRACK.

Revisión Cookies

- Las cookies: UCURSOS_SERVER, PHPSESSID, theme tienen problemas con la flag httponly

Revisión Cabeceras

- Las cabeceras: x-content-type-options, x-xss-protection y strict-transport-security están deshabilitadas

El resto de las pruebas han mostrado resultados satisfactorios

3.2 ucampus.uchile.cl

A continuación se muestra un resumen del resultado obtenido en cada prueba realizada a este sitio web, lo cual sustenta el rating asignado:



Nombre del test	Criticidad	Puntaje
Revisión del código de estado HTTP	bajo	●
Revisión Métodos HTTP	bajo	●
Revisión Robots	bajo	●
Revisión Cookies	medio	●
Revisión Cabeceras	medio	●
Revisión Certificados	alto	●
Revisión Cifrados y Protocolos	alto	●

A continuación, se exponen las principales debilidades de seguridad localizadas en este sitio web:

Revisión Métodos HTTP

- Métodos HTTP inseguros habilitados: PUT, DELETE, OPTIONS, TRACE, PATCH, TRACK.

Revisión Cookies

- La cookie: _LB tiene problemas con la flag httponly

Revisión Cabeceras

- Las cabeceras: x-content-type-options, x-xss-protection y strict-transport-security están deshabilitadas

El resto de las pruebas han mostrado resultados satisfactorios

4 Resumen por Test

4.1 Revisión del código de estado HTTP

Se evalúa la respuesta del servidor a la petición de un determinado sitio web, para verificar si la conexión se ha establecido de manera correcta o ha ocurrido algún error, a través de una codificación establecida. Para más información revisar el anexo de la sección

Resultados obtenidos:

Sitio web	Método de solicitud	Código de estado HTTP	Resultado
www.u-cursos.cl	GET	200	●
ucampus.uchile.cl	GET	200	●

Evaluación resultados





















- Verde: conexión exitosa al sitio web, ha resultado código de estado HTTP en el rango (200-299)
- Amarillo: Procesando conexión código de estado HTTP en el rango (100-199), conexión redirigida a otro sitio web códigos en el rango (300-399)
- Rojo: Conexión errónea al sitio web, por error de cliente con código de estado HTTP en el rango (400-499) o por error del servidor con código de estado HTTP en el rango (500-599)

4.2 Revisión Métodos HTTP

HTTP define un conjunto de métodos de petición para indicar la acción que se desea realizar en un recurso determinado.

Se procede a evaluar los métodos HTTP habilitados en cada sitio web, comprobando que no se permita el uso de métodos no recomendados o inseguros (Ej. PUT, DELETE, CONNECT, TRACE, OPTIONS).

A continuación se muestran los resultados obtenidos, primeramente se muestra la página junto con el resultado general obtenido y luego se listan los métodos HTTP “HABILITADOS” en cada sitio web con su respectiva recomendación, para más información revisar el anexo de la sección.

www.u-cursos.cl	
GET	
POST	
HEAD	
PUT	
DELETE	
OPTIONS	
TRACE	
PATCH	
TRACK	
ucampus.uchile.cl	
GET	
POST	
HEAD	
PUT	
DELETE	
OPTIONS	
TRACE	
PATCH	
TRACK	

Evaluación resultados

- Verde: El sitio web no tiene habilitados métodos HTTP inseguros
- Rojo: El sitio web tiene habilitado al menos un método HTTP considerado inseguro
- Métodos HTTP no recomendados o inseguros: PUT, DELETE, CONNECT, TRACE y OPTIONS

4.3 Revisión Robots

Los navegadores de internet cuentan con unas máquinas o robots (archivo /robots.txt) que rastrean la web para clasificar e indexar la mayor cantidad de información posible a sus bases de datos.

En esta sección se comprueba que el archivo robots.txt expuesto para determinado sitio web tenga acceso controlado a los archivos de imagen, páginas web y directorios asociados.

A continuación se muestran los resultados, para más información revisar el anexo de la sección.

Nombre de la página	Habilitado	Datos	Resultado
www.u-cursos.cl	True	User-agent: *; disallows (6);	●
ucampus.uchile.cl	True	User-agent: *; disallows (6);	●

Evaluación resultados

- Verde: No se obtuvo acceso a la ruta ../robots.txt de este sitio web, o se tiene acceso validando restricciones al acceso de indexación de rastreadores en navegadores (por ejemplo: Validar que User-agent: * tenga una lista de sentencias "Disallow" definida).
- Rojo: Se tiene acceso a la ruta ../robots.txt de este sitio web sin restricciones al acceso de indexación de directorios y páginas por parte de rastreadores en navegadores (por ejemplo: Validar que User-agent: * tiene la sentencia "Allow: /" definida).

4.4 Revisión Cookies

Verificar que las cookies son generadas con determinadas flags que incrementen la seguridad de las sesiones.

A continuación se muestran los resultados, para más información revisar el anexo de la sección.

www.u-cursos.cl	Secure	HttpOnly	Resultado
UCURSOS_SERVER	False	False	●
PHPSESSID	True	False	●
theme	False	False	●
General:			●

ucampus.uchile.cl	Secure	HttpOnly	Resultado
_LB	False	False	●
_fcfm	True	True	●
General:			●

Evaluación resultados

- Verde: en la prueba por cookie es necesario que secure y httponly tengan el valor True
- Rojo: en la prueba por cookie, al menos un valor es False
- Para la prueba general del sitio web se calcula el promedio de los resultados de sus respectivas cookies

4.5 Revisión Cabeceras

En esta sección se revisan cuatro cabeceras en donde se busca:

Comprobar que el sitio web dispone de protección contra clickjacking, evitando así que se cargue el sitio en un frame remoto y minimizando, por tanto, un posible ataque de phishing.

Analizar que se han implantado protecciones contra ataques del tipo cross site scripting.

Verificar que existen medidas para evitar ataques del tipo ssl-stripping en un ámbito de “man in the middle”, garantizando así uso de http strict transport security y forzando a que todas las comunicaciones sean transmitidas por un canal seguro.

A continuación se muestran los resultados, para más información revisar el anexo de la sección.

www.u-cursos.cl	Datos	Resultado
x-content-type-options	None	●
x-frame-options	SAMEORIGIN	●
x-xss-protection	None	●
strict-transport-security	None	●
General:		●

ucampus.uchile.cl	Datos	Resultado
x-content-type-options	None	●
x-frame-options	SAMEORIGIN	●
x-xss-protection	None	●
strict-transport-security	None	●
General:		●

Evaluación resultados

- Se busca que x-frame-options tenga como valor deny o sameorigin para obtener verde, de otra forma obtiene rojo
- Se busca que x-content-type-options tenga como valor nosniff para obtener verde, de otra forma obtiene rojo
- Se busca que x-xss-protection tenga valor 1 para obtener verde, de otra forma obtendrá rojo
- Se busca que strict transport security tenga como valor max-age mínimo 31536000 para obtener verde, de otra forma obtiene rojo
- Para la prueba general del sitio web, se calcula el promedio de los resultados de las cuatro cabeceras anteriores

4.6 Revisión Certificados

En esta parte se verifica la integridad de los certificados

Evaluación resultados

- Para obtener verde en el certificado basta que este esté vigente y use la encriptación adecuada, en caso contrario obtiene rojo

4.6.1 www.u-cursos.cl

Número de certificados: 3
General: ●

Certificado #1 ●

common name	CN=*.u-cursos.cl	
valid from	2022-09-20	✓
valid to	2023-10-04	✓
key name	_RSAPublicKey	
key curve	None	
issuer	CN=Sectigo RSA Domain Validation Secure Server CA,O=Sectigo Limited,L=Salford,ST=Greater Manchester,C=GB	
signature algorithm	sha256WithRSAEncryption	✓

Certificado #2 ●

common name	CN=Sectigo RSA Domain Validation Secure Server CA,O=Sectigo Limited,L=Salford,ST=Greater Manchester,C=GB	
valid from	2018-11-02	✓
valid to	2030-12-31	✓
key name	_RSAPublicKey	
key curve	None	
issuer	CN=USERTrust RSA Certification Authority,O=The USERTRUST Network,L=Jersey City,ST=New Jersey,C=US	
signature algorithm	sha384WithRSAEncryption	✓

Certificado #3

common name	CN=USERTrust RSA Certification Authority,O=The USERTRUST Network,L=Jersey City,ST=New Jersey,C=US	
valid from	2019-03-12	✓
valid to	2028-12-31	✓
key name	_RSAPublicKey	
key curve	None	
issuer	CN=AAA Certificate Services,O=Comodo CA Limited,L=Salford,ST=Greater Manchester,C=GB	
signature algorithm	sha384WithRSAEncryption	✓

4.6.2 ucampus.uchile.cl

Número de certificados: 3

General: ●

Certificado #1



common name	CN=ucampus.uchile.cl	
valid from	2022-09-20	✓
valid to	2023-10-04	✓
key name	_RSAPublicKey	
key curve	None	
issuer	CN=Sectigo RSA Domain Validation Secure Server CA,O=Sectigo Limited,L=Salford,ST=Greater Manchester,C=GB	
signature algorithm	sha256WithRSAEncryption	✓

Certificado #2



common name	CN=Sectigo RSA Domain Validation Secure Server CA,O=Sectigo Limited,L=Salford,ST=Greater Manchester,C=GB	
valid from	2018-11-02	✓
valid to	2030-12-31	✓
key name	_RSAPublicKey	
key curve	None	
issuer	CN=USERTrust RSA Certification Authority,O=The USERTRUST Network,L=Jersey City,ST=New Jersey,C=US	
signature algorithm	sha384WithRSAEncryption	✓

Certificado #3

common name	CN=USERTrust RSA Certification Authority,O=The USERTRUST Network,L=Jersey City,ST=New Jersey,C=US	
valid from	2019-03-12	✓
valid to	2028-12-31	✓
key name	_RSAPublicKey	
key curve	None	
issuer	CN=AAA Certificate Services,O=Comodo CA Limited,L=Salford,ST=Greater Manchester,C=GB	
signature algorithm	sha384WithRSAEncryption	✓

4.7 Revisión Cifrados y Protocolos

(no sale en el excel, A.5 puede ser?)

En esta prueba se verifican que los protocolos usados sean los correctos por temas de seguridad y que los suites sean seguros

Evaluación resultados

- el protocolo obtendra color verde si cumple con lo recomendado, de otra forma obtendra rojo
- el suite obtendra color verde si cumple con los parámetros de seguridad sugeridos, de otra forma obtiene rojo

4.7.1 www.u-cursos.cl

General: ●

Protocolos detectados

TLS 1.2	4/156	uso recomendado
---------	-------	-----------------

Cipher suites

TLS 1.2

TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	●
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	●
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	●
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	●

4.7.2 ucampus.uchile.cl

General: ●

Protocolos detectados

TLS 1.2	4/156	uso recomendado
----------------	-------	------------------------

Cipher suites

TLS 1.2

TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	●
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	●
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	●
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	●

5 Anexos

Pendiente.

5.1 Revisión del código de estado HTTP

Guía breve:

- Códigos informativos (100-199): El servidor reconoce la petición iniciada por el buscador y está siendo procesada.
- Códigos de éxito (200-299): la solicitud ha sido recibida, entendida o procesada por el buscador.
- Códigos de redirección (300-399): un nuevo destino ha sido sustituido para la fuente solicitada.
- Códigos de error de cliente (400-499): el sitio web no ha sido alcanzado, la página no está disponible o ha ocurrido un problema técnico con la solicitud.
- Códigos de error del servidor (500-599): la solicitud ha sido aceptada, pero debido a un error con el servidor, no se ha podido completar la petición.

5.2 Revisión Métodos HTTP

Explicación de los métodos HTTP:

- GET: El método más común en la navegación web. Devuelve un código de respuesta y las cabeceras asociadas. Incluye el documento solicitado (habitualmente una página) en el cuerpo del mensaje.
- HEAD: Idéntico al anterior, con la salvedad de que no devuelve el documento en el cuerpo de la respuesta. Se utiliza para extraer información sobre el documento solicitado o comprobar si existe sin necesidad de enviar y recibir el documento como tal.
- POST: Pensado para publicar la información contenida en el cuerpo de la petición en el recurso donde se envía esa petición. La información que se publica y la forma de hacerlo depende completamente del servidor y el recurso. Hoy, el uso que se le da a este método es el de paso de parámetros de cliente a servidor (en muchas ocasiones para ficheros). La respuesta por parte del servidor es la misma que para una petición GET.
- TRACE: Implementa la función de eco para los mensajes HTTP. El servidor responde en el cuerpo del mensaje con la misma petición que el cliente ha realizado. Se utiliza para comprobar que las peticiones son recibidas correctamente. Su finalidad es la de depuración.
- OPTIONS: Este método presenta las opciones que el recurso o servidor dispone o requiere. De esto se puede obtener información como por ejemplo los métodos permitidos (en la cabecera ALLOW).
- CONNECT: Utilizado para crear la comunicación con un proxy HTTP (SSL).
- PUT: Mediante este método es posible almacenar el documento que se envía como cuerpo de la petición en el propio servidor (físicamente en disco). Si el recurso al que se hace referencia en la petición no existe se creará y si existe se sobrescribirá.
- DELETE: Al igual que el método PUT, este verbo afecta directamente al recurso al que se hace la petición. Tiene la capacidad de eliminar el elemento y dejar al servidor sin ese recurso.

Riesgos de los métodos inseguros:

- PUT: Permite interactuar directamente con recursos legítimos del sistema, en específico para crearlos (por ejemplo una web shell para controlar el servidor, o fichero modificado para conseguir desfigurar alguna web legítima).
- DELETE: Permite interactuar directamente con recursos legítimos del sistema, en específico para eliminar archivos o activos de, por ejemplo, una compañía.
- TRACE: Este método devuelve como cuerpo las cabeceras de la petición del cliente, incluyendo la cabecera Cookie que (según entornos) puede resultar crítica si existe una sesión establecida con el servidor. La combinación de este Método HTTP con un fallo Cross Site Scripting en la aplicación web puede acabar en un robo de sesión de usuario, incluso si las Cookies han sido establecidas como HttpOnly. Este ataque es conocido como «Cross Site Tracing» o XST.

5.3 Revisión Robots

Explicación de los resultados:

- User-agent: indica el nombre del cliente automático, denominado “rastreador de buscador”, al que se aplica la regla. El asterisco (*) se aplica a todos los rastreadores, excepto a los de AdsBot, que deben nombrarse explícitamente.
- Allow: indica los directorios o las páginas del dominio raíz que el user-agent que se haya especificado en el grupo debe rastrear.

5.4 Revisión Cookies

Explicación de los resultados:

- HTTPOnly: El uso de la flag HttpOnly cuando se genera una cookie ayuda a mitigar el riesgo de script del lado del cliente que accede a la cookie protegida (si el navegador lo soporta), puesto que, no revela la cookie a un tercero y solo puede ser accesible a través del protocolo HTTP.
- Secure: El uso de la flag Secure indica que esta cookie sólo se tiene que enviar a través de una comunicación segura y encriptada, como puede ser una conexión SSL (HTTPS), garantizando así, la integridad, confidencialidad y autenticación.

5.5 Revisión Cabeceras

Cabecera X-Frame-Options:

- Puede ser usado para indicar si debería permitírsele a un navegador renderizar una página de un <frame>, <iframe>, <embed> u <object>.
- Las páginas web pueden usarlo para evitar ataques de clickjacking, asegurándose de que su contenido no es embebido en otros sitios.
- DENY: La página no puede ser mostrada en un marco, independiente del sitio que esté intentándolo.
- SAMEORIGIN: La página solo puede ser mostrada en un marco del mismo origen que dicha página.
- ClickJacking, también conocido como “ataque de compensación de UI”, es cuando un atacante usa varias capas transparentes u opacas para engañar a un usuario para que haga clic en un botón o enlace en otra página cuando intenta hacer clic en la página del nivel superior. Por lo tanto el atacante está secuestrando los clics destinados a su página y enrutando a otra página, muy probablemente propiedad e otra aplicación, dominio o ambos.

Cabecera X-Content-Type-Options:

- Es un marcador utilizado por el servidor para indicar que los tipos MIME (Multipurpose Internet Mail Extensions; indican la naturaleza y el formato de un documento, archivo o variedad de bytes) anunciados en los encabezados Content-Type no se deben cambiar ni seguir, de esta forma se permite desactivar el MIME type sniffing.

Cabecera X-XSS-Protection:

- Es una característica de internet explorer, chrome y safari que impide la carga de una página cuando detecta ataques del tipo Cross-Site-Scripting (XSS).

Cabecera Strict-Transport-Security:

- Característica de seguridad que permite a un sitio web indicar a los navegadores que sólo se debe comunicar con HTTPS en lugar de usar HTTP.

5.6 Revisión Certificados

Pendiente.

5.7 Revisión Cifrados y Protocolos

Protocolo

- Proporcionan conexiones seguras, permitiendo que dos partes se comuniquen con privacidad, integridad de datos, identificación y autenticación utilizando certificados digitales.
- Estos son: SSL y TLS

Algoritmo de intercambio de claves

- Empleado para compartir las claves simétricas con las que se cifrarán las comunicaciones.
- Estos son: DH, DHE, ECDH, ECDHE, RSA y DSA

Firma digital

- Verifica las identidades tanto del cliente, como del servidor durante la sesión.
- Estos son: RSA, ECDSA, DSS, AES, RC2, RC4, RC5, DES, 3DES y BlowFish

Modo de cifrado

- Especifica el modo de cifrado de bloques que se utilizará para el cifrado.
- Estos son: CBC, GCM, EAX, CCM, ECB, PCBC, CFB, OFB y CTR

Hash

- Algoritmo de cifrado irreversible que verifica la integridad de los mensajes.
- Estos son: SHA-1, SHA-256, SHA-384, AEAD, HMAC, MD2, MD4 y MD5