

Informe Laboratorio 3

Sección x

Alumno x

e-mail: alumno.contacto@mail.udp.cl

Octubre de 2024

Índice

1. Descripción de actividades	2
2. Desarrollo de actividades según criterio de rúbrica	3
2.1. Identifica el algoritmo de hash utilizado al momento de registrarse en el sitio	3
2.2. Identifica el algoritmo de hash utilizado al momento de iniciar sesión	5
2.3. Genera el hash de la contraseña desde la consola del navegador	6
2.4. Intercepta el tráfico login con BurpSuite	7
2.5. Realiza el intento de login	8
2.6. Identifica las políticas de privacidad o seguridad	11
2.7. Demuestra 4 conclusiones sobre la seguridad	12

1. Descripción de actividades

Su objetivo será auditar la implementación de algoritmos hash aplicados a contraseñas en páginas web desde el lado del cliente, así como evaluar la efectividad de estas medidas contra ataques de tipo Pass the Hash (PtH). Para llevar a cabo esta auditoría, deberá registrarse en un sitio web y crear una cuenta, ingresando una contraseña específica para realizar las pruebas.

Al concluir la tarea, es importante que modifique su contraseña por una diferente para garantizar su seguridad.

Dado que la cantidad de sitios chilenos que utilizan hash es limitada, se permite realizar esta tarea en cualquier sitio web a nivel mundial. En este sentido, realice las siguientes actividades:

- Identificación del algoritmo de hash utilizado para las contraseñas al momento del registro en el sitio.
- Identificación del algoritmo de hash utilizado para las contraseñas al momento de iniciar sesión.
- Generación del hash de la contraseña desde la consola del navegador, partiendo de la contraseña en texto plano.
- Interceptación del tráfico de login utilizando BurpSuite desde su equipo.
- Realización de un intento de login, modificando una contraseña incorrecta por el hash obtenido en el punto anterior.
- Descripción de las políticas de privacidad o seguridad relacionadas con las contraseñas, incluyendo un enlace a las mismas.
- Cuatro conclusiones sobre la seguridad o vulnerabilidad de la implementación observada.

2. Desarrollo de actividades según criterio de rúbrica

2.1. Identifica el algoritmo de hash utilizado al momento de registrarse en el sitio

Primero, para el correcto proceder del siguiente laboratorio es pertinente la creación de un correo electrónico temporal que nos servirá para identificarnos en la web sin tener que poner en riesgo nuestros credenciales personales oficiales.

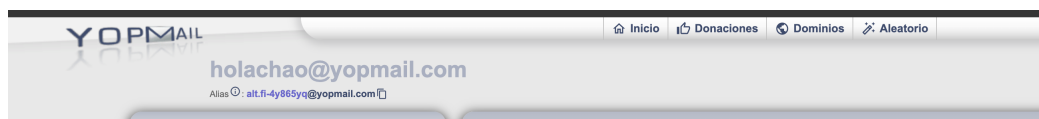


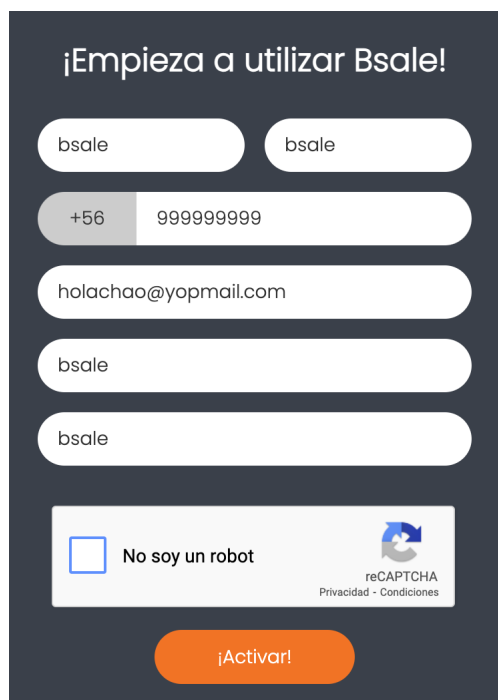
Figura 1: Correo temporal

Primero seleccionamos una pagina web (de carácter nacional ojalá) que tenga algún tipo de hash que podamos identificar. Dada una búsqueda provista en clases, se muestra a continuación un desarrollo de laboratorio con una página web llamada *www.bsale.cl*, que fue realmente seleccionada para demostrar vulnerabilidades en estos casos incluso de plataformas importantes que funcionan como sistema de ventas, control de inventario, control de ventas por internet, vale decir, monitoreo general de negocios desde su parte transaccional. En fin, como una plataforma de transacciones y generadora de documentos legales, resulta curioso haver este tipo de actividades.

El hash en si a trabajar en este informe es desde su diseño en web y en su apartado de “inicio de sesión”.

Ahora, y dicho lo anterior, primero hay que registrarnos en el sitio.

Existe un formulario pequeño simple a completar como primer acercamiento, y dado que no certifica con ningún otro servicio externo nombre, apellido, nombre de la empresa o incluso número telefónico de contacto, es muy sencillo de avanzar.



¡Empieza a utilizar Bsale!

bsale bsale

+56 999999999

holachao@yopmail.com

bsale

bsale

☐ No soy un robot reCAPTCHA Privacidad - Condiciones

¡Activar!

Figura 2: Formulario

Con nombre y apellido de “bsale”, a continuación un correo nos llega inmediatamente a nuestra casilla temporal junto con nuestro correo electrónico ingresado y una contraseña otorgada por ellos, que a todas luces aparenta ser algo generado de forma aleatoria.

¡Felicidades, ya puedes probar Bsale!

Hola, bsale

Durante los próximos 30 días podrás, de acuerdo a tus necesidades, probar nuestras funcionalidades. Recuerda que en esta versión no podrás emitir documentos tributarios válidos ante el SII.

Entra en Bsale y empieza a disfrutar de nuestra plataforma.

Estos son tus datos de acceso:

Correo electrónico:
holachao@yopmail.com

Clave:
qWo00SLvef

Figura 3: Correo ingresado y contraseña automática

2.2. Identifica el algoritmo de hash utilizado al momento de iniciar sesión

Ya teniendo acceso dado el previo paso de registro, iniciamos sesión usando otra contraseña para luego, en nuestra herramienta de desarrollador del mismo navegador, podamos identificar si nuestra contraseña se envía de forma hasheada y de qué tipo del mismo hacia sus registros.

Al momento de iniciar sesión con esta contraseña equívoca (“987654321”), identificamos el paquete “check_credentials” del apartado de network dentro del navegador, donde en su Payload tenemos el mail usado para ingresar sesión y la contraseña con efectivamente un hash aplicado.

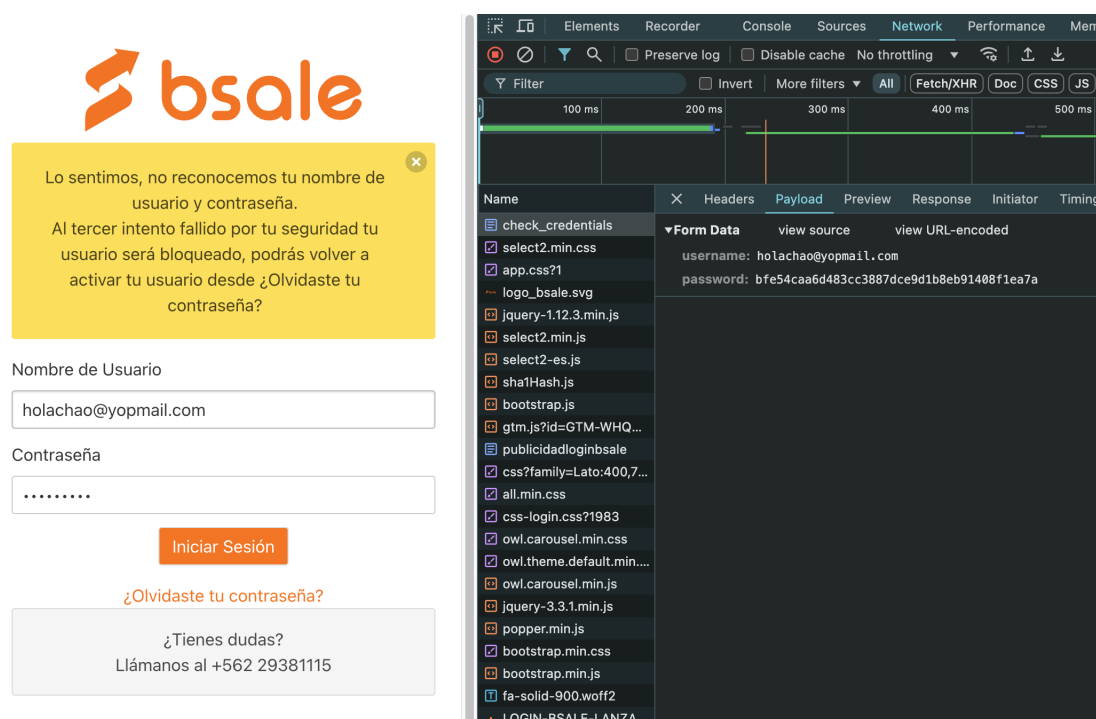


Figura 4: Identificación de Hash en plataforma BSale

Buscamos en google una página que nos pueda dar alguna señal o decir un poco más del tipo de hash que puede ser el usado para esta contraseña y nos encontramos con “tunnel-sup.com” y su apartado de “HashAnalyzer”.

En la siguiente imagen se presenta un pantallazo del hash contenido en el paquete enviado por la plataforma llamado “check_credentials” junto con la identificación de su hash respectivo.

Hash Analyzer

Tool to identify hash types. Enter a hash to be identified.

Hash:	bfe54caa6d483cc3887dce9d1b8eb91408f1ea7a
Salt:	Not Found
Hash type:	SHA1 (or SHA 128)
Bit length:	160
Character length:	40
Character type:	hexidecimal

Example Hash Inputs

Figura 5: Identificación de Hash

2.3. Genera el hash de la contraseña desde la consola del navegador

Desde la consola del navegador, como ya identificamos que el tipo de hash utilizado es SHA1, vamos a comprobar si usando la contraseña ingresada logramos identificar el mismo tipo de hash.



Figura 6: Contraseña con Hash efectivo

El resultado es satisfactorio dado que al ingresar la contraseña errónea “987654321” y al aplicarle el hash respectivo, efectivamente conseguimos exactamente el mismo resultado en comparación al anterior desprendido desde el Payload del paquete “check_credentials” previamente analizado.

2.4. Intercepta el tráfico login con BurpSuite

A continuación volvemos a interceptar el tráfico de login con mail temporal y contraseña errónea, pero esta vez usando BurpSuite como intermediario para luego realizar un intento de login siempre a partir desde la plataforma.

Primero, se realiza una toma del login con la contraseña errónea (“987654321” en este caso) para así entonces identificar (y así trabajar) con el respectivo paquete ya mencionado “check_credentials” desde el software como tal.

A continuación 2 figuras desprendidas del software:

2 DESARROLLO DE ACTIVIDADES SEGÚN CRITERIO DE RÚBRICA

Intercept on		Forward		Drop		Request to https:	
Time	Type	Direction	Host	Method	URL		
00:44:31 22 Oct 2024	HTTP	→ Request	www.googleadservices.com	GET	https://www.googleadservices.com/pagead		
00:44:32 22 Oct 2024	HTTP	→ Request	d.clarity.ms	POST	https://d.clarity.ms/collect		
00:44:32 22 Oct 2024	HTTP	→ Request	www.facebook.com	GET	https://www.facebook.com/tr/?id=1913041f		
00:44:32 22 Oct 2024	HTTP	→ Request	www.facebook.com	GET	https://www.facebook.com/privacy_sandbox		
00:44:32 22 Oct 2024	HTTP	→ Request	analytics.tiktok.com	POST	https://analytics.tiktok.com/api/v2/pixel		
00:44:32 22 Oct 2024	HTTP	→ Request	analytics.tiktok.com	POST	https://analytics.tiktok.com/api/v2/pixel/act		
00:44:32 22 Oct 2024	HTTP	→ Request	googleads.g.doubleclick.net	GET	https://googleads.g.doubleclick.net/pagead		
00:44:32 22 Oct 2024	HTTP	→ Request	td.doubleclick.net	GET	https://td.doubleclick.net/td/rul/959851608?		
00:44:32 22 Oct 2024	HTTP	→ Request	login.bsale.cl	POST	https://login.bsale.cl/check_credentials		
00:44:32 22 Oct 2024	HTTP	→ Request	google.com	POST	https://google.com/cdm/form-data/9598516		
00:44:32 22 Oct 2024	HTTP	→ Request	google.com	POST	https://google.com/pagead/form-data/9598516		
00:44:38 22 Oct 2024	HTTP	→ Request	d.clarity.ms	POST	https://d.clarity.ms/collect		
00:44:47 22 Oct 2024	HTTP	→ Request	d.clarity.ms	POST	https://d.clarity.ms/collect		
00:44:51 22 Oct 2024	HTTP	→ Request	www.googleadservices.com	GET	https://www.googleadservices.com/pagead		
00:44:53 22 Oct 2024	HTTP	→ Request	d.clarity.ms	POST	https://d.clarity.ms/collect		
00:44:57 22 Oct 2024	HTTP	→ Request	d.clarity.ms	POST	https://d.clarity.ms/collect		

Figura 7: Paquete check_credentials asociado a método post, en request

```
Request
Pretty Raw Hex
1 POST /check_credentials HTTP/2
2 Host: login.bsale.cl
3 Cookie: _fbp=fb.1.1729568498187.115419469386339540; _gid=GA1.2.1996115916.1729568498; _tt_enable_cookie=1; _t1
4 1kjdhYi7C2%7CfQ8%7C0%7C1756; _ga=GA1.1.42761577.1729568498; _ga_DB7P1FRXT9=GS1.1.1729581902.2.1.1729581911.5:
5 8b226820902711efb0cd795ffb0d9e0a; _uetvid=8b2264d0902711efa7a86941e9070bb1; _clsk=txz9o9%7C1729581911933%7C3%;
6 1.1.1787376960.1729568498.933970969.1729581958.1729581979
7 Content-Length: 81
8 Cache-Control: max-age=0
9 Sec-Ch-Ua: "Not;A=Brand";v="24", "Chromium";v="128"
10 Sec-Ch-Ua-Mobile: ?0
11 Sec-Ch-Ua-Platform: "macOS"
12 Accept-Language: es-419,es;q=0.9
13 Upgrade-Insecure-Requests: 1
14 Origin: https://login.bsale.cl
15 Content-Type: application/x-www-form-urlencoded
16 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/128.0.661:
17 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,appl:
18 Sec-Fetch-Site: same-origin
19 Sec-Fetch-Mode: navigate
20 Sec-Fetch-User: ?1
21 Sec-Fetch-Dest: document
22 Referer:
23 https://login.bsale.cl/?_gl=1*4u27ay*_gcl_au*MTc4NzM3Njk2MC4xNzI5NTY4NDk4LjIwNDA5MDk1NzEuMTcyOTU2ODUzNi4xNzI5M
RXT9*MTcyOTU4MTkwM14yLjEuMTcyOTU4MTkw0S41My4wLjE2NTkzNjE5OTM.
20 Accept-Encoding: gzip, deflate, br
21 Priority: u=0, i
22
23 username=holachao%40yopmail.com&password=bfe54caa6d483cc3887dce9d1b8eb91408f1ea7a
```

Figura 8: Payload con hash de contraseña errónea

2.5. Realiza el intento de login

Teniendo esto, se intenta intercambiar el hash del paquete (el “erróneo”) con el de la contraseña funcional usando la función “Intruder” de BurpSuite agregándolo a su lista de contraseñas a probar en “Payload Settings”.

Payload settings [Simple list]

This payload type lets you configure a simple list of strings that are use

Paste a5e799a1018d027a6092220017f6ffd6743fdc5a

Load ...

Remove

Clear

Deduplicate

Add

Add from list ... [Pro version only]

Figura 9: Intruder ad-portas de probarse con hash de contraseña correcta

Y es apartir de este punto, si hemos hecho todo correctamente, es que confirmaremos si nuestro ataque Pass The Hash funciona o no....lamentablemente no tuvimos éxito.

5. Intruder attack of https://login.bsale.cl

Attack Save ?

Results Positions Payloads Resource pool Settings

Intruder attack results filter: Showing all items

Request	Payload	Status code	Response r...	Error	Timeout	Length	Comment
0		200	179			7566	
1	a5e799a1018d027a6092220017f...	200	187			7566	

Request Response

Pretty Raw Hex

```

16 Sec-Fetch-Mode: navigate
17 Sec-Fetch-User: ?1
18 Sec-Fetch-Dest: document
19 Referer:
https://login.bsale.cl/?_gl=1*4u27ay*_gcl_au*MTc4NzM3Njk2MC4xNzI5NTY4NDk4LjIwNDA5MDk1NzEuMTcyOTU2ODUzNi4xNzI5NTY4Njcy*_ga*NDI3NjE1NzcuMTcyOTU2ODQ5OA.**_ga_DB7P1FRXT9*MTcyOTU4MTkwMi4yLjEuMTcyOTU4MTkw0S41My4wLjE2NTkzNjE5OTM.
20 Accept-Encoding: gzip, deflate, br
21 Priority: u=0, i
22 Connection: keep-alive
23
24 username=holachao%40yopmail.com&password=a5e799a1018d027a6092220017f6ffd6743fdc5a

```

0 highlights

Finished

Figura 10: Request - correcto y sin éxito

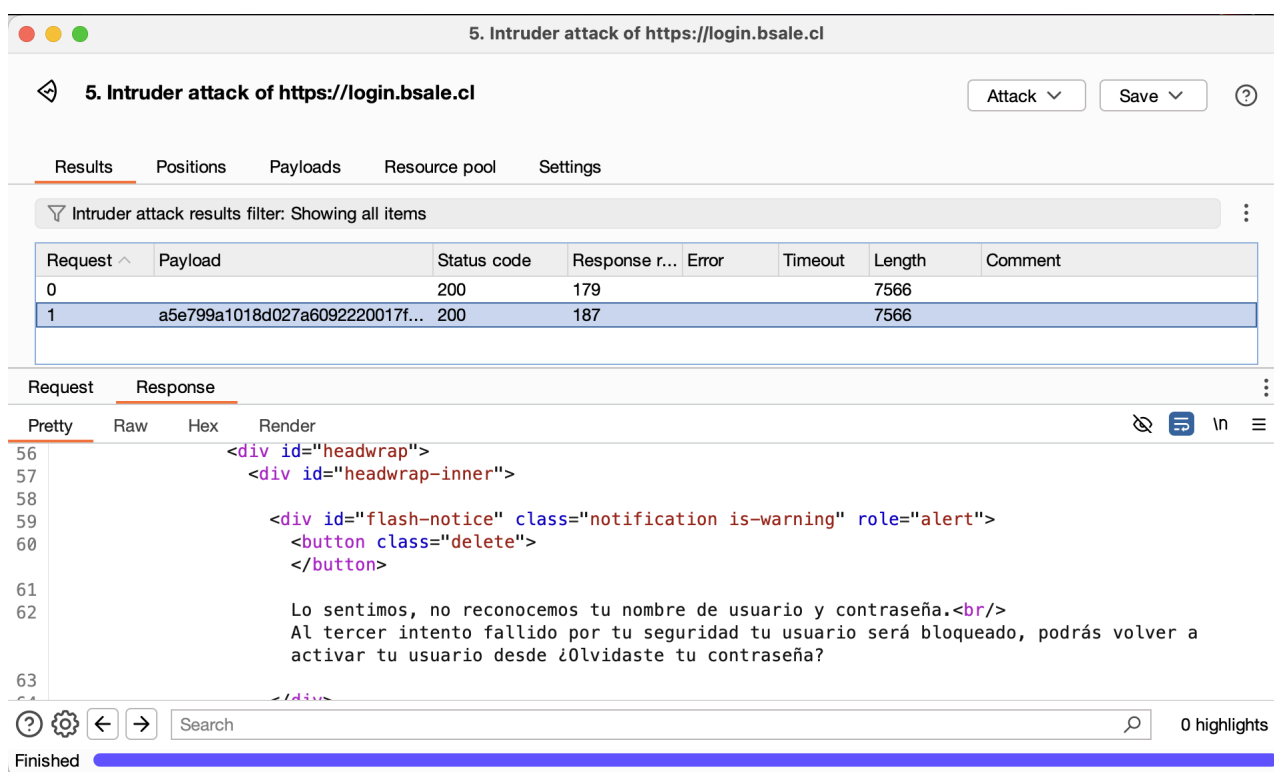


Figura 11: Request - BSale sin identificar mail ni contraseña

En las figuras anteriores, 10 y 11, queda en evidencia cómo es que el ataque a pesar de haber sido bien ejecutado y bien puesto el valor del hash correcto en el lugar, la pagina de BSale no llevó a cabo la solicitud completa. La imagen 11 incluso mas que el error, nos deja en claro una potencial solución de quizás cambiar la contraseña e intentarlo nuevamente.

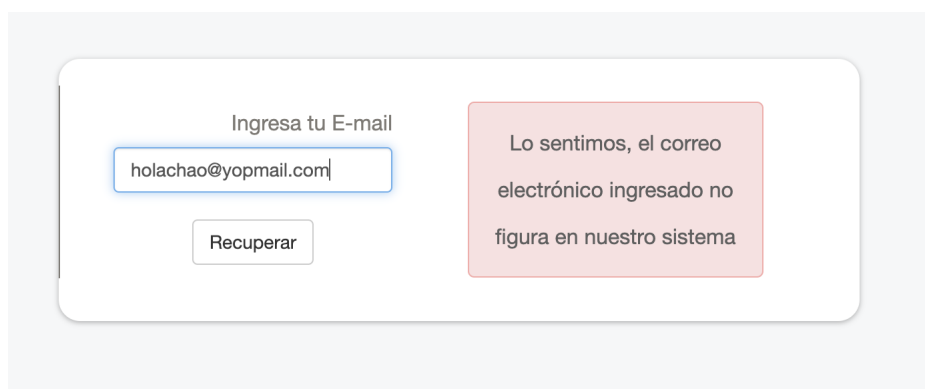


Figura 12: Correo no en sistema

Es difícil saber realmente que es lo que pasó dentro del sistema de BSale para que el ataque no tuviera éxito, es más, para que ni siquiera el mail estuviese ingresado siendo que fue creado hace no tanto tiempo atrás.

A simple vista podría parecer un ambiente muy seguro pero realmente si pudimos llegar tan lejos para incluso identificar un hash de una pagina de transacciones sin siquiera con uso de algún tipo de salt para despistar ni en correo electrónico ni contraseña, quizás es indicador que se podría hacer un poco más para encriptar datos en general.

2.6. Identifica las políticas de privacidad o seguridad

La pagina oficial, “bsale.cl”, tiene abajo - de toda la página - un pequeño menú donde uno de los apartados es de “Politica de Privacidad”, más es un documento simple y sin entrar tanto en detalle.

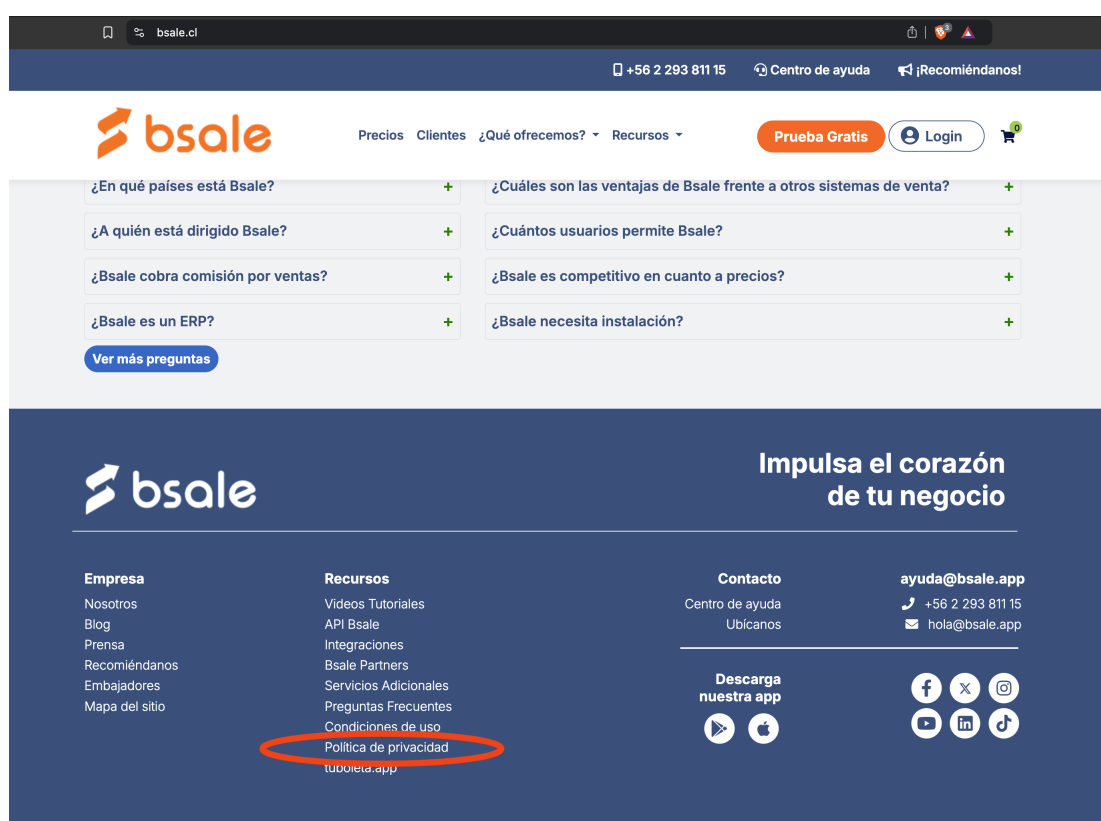


Figura 13: Apartado menú inferior

Se pueden consultar en el link <https://www.bsale.cl/sheet/politica-privacidad>, pero las políticas de privacidad de Bsale se ajustan de Protección de la Vida Privada, limitando el tratamiento de datos personales a lo estrictamente necesario para sus actividades comerciales y cumpliendo con la normativa chilena. El consentimiento informado es un eje fundamental en el tratamiento de datos, aunque también se permite el uso de datos de fuentes públicas sin necesidad de autorización previa.

Además, se contempla la transferencia de datos a terceros, como empresas de marketing, para actividades comerciales, lo que puede aumentar el riesgo de exposición. Bsale asegura

adoptar medidas de seguridad adecuadas para proteger los datos personales, pero aclara que no puede garantizar una seguridad perfecta en internet y, por lo tanto, no se responsabiliza por accesos no autorizados o interceptaciones ilegales, lo que implica un reconocimiento de los riesgos inherentes al entorno digital.

2.7. Demuestra 4 conclusiones sobre la seguridad

1. La falta de uso de hashes para proteger contraseñas e identificadores personales es un punto débil que comparte Bsale con algunas empresas grandes y chicas que no priorizan o no invierten en la implementación de tecnologías de seguridad modernas. Hoy por hoy se están implementando medidas como autenticación multifactor para evitar este tipo de cosas, mas no en todas las empresas hay preocupación de modernizar su seguridad digital.
2. Similar a muchas otras empresas, Bsale afirma implementar medidas de seguridad para proteger los datos, pero admite que **la seguridad perfecta no existe en el entorno digital**. Este reconocimiento es frecuente en las políticas de privacidad de muchas empresas (y de diversos tamaños), reflejando una realidad en la que las empresas saben que las vulnerabilidades externas, como ataques de terceros, siguen siendo una amenaza, particularmente cuando no se usan tecnologías de cifrado o hash.
3. Es común entre muchos tipos de empresas permitir la transferencia de datos personales a terceros, como proveedores de marketing o análisis. Esto expone a los datos a riesgos adicionales, ya que no siempre se tiene control completo sobre cómo esos terceros protegen la información, especialmente si no se utilizan medidas de seguridad robustas como el hashing, ya comprobado en este laboratorio.
4. Es probable que los usuarios, cada vez más conscientes de las prácticas de seguridad digital, pueden desconfiar de empresas que no utilizan mecanismos de protección como el hashing para sus contraseñas e identificadores el día de mañana; y la falta de tales medidas puede afectar negativamente la percepción de seguridad y la reputación de la empresa, llevando a una posible pérdida de clientes que valoran la protección de sus datos personales.