Universidad Diego Portales

CRIPTOGRAFÍA Y SEGURIDAD EN REDES

Tarea N°1

Autores:
Marcelo Luengo
Profesor:
Nicolás Boettcher

Fecha: Viernes 25 de junio

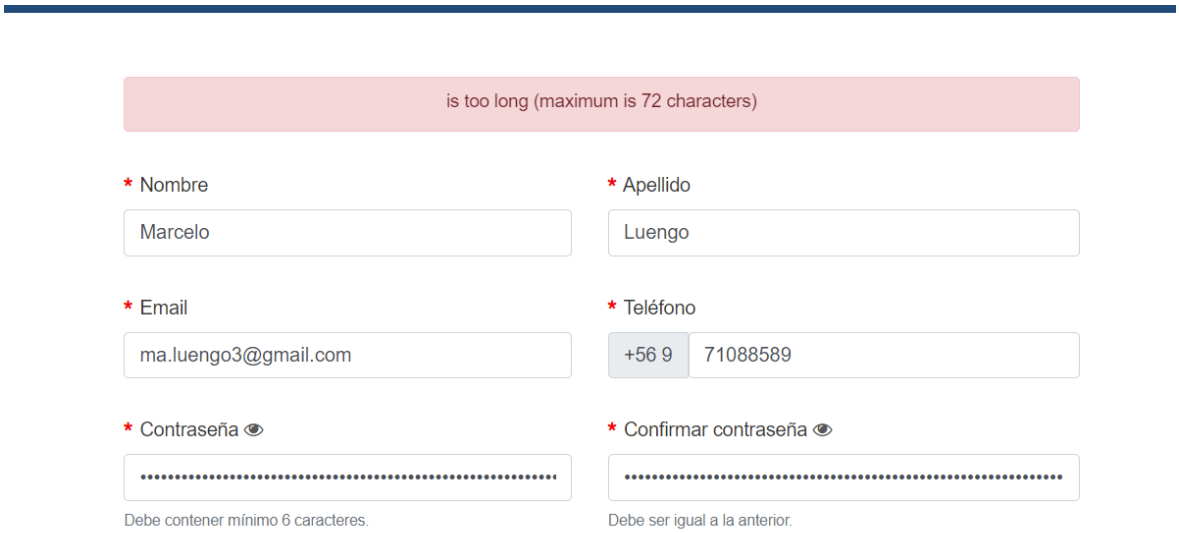
Índice

https://github.com/manfruta/Tarea1

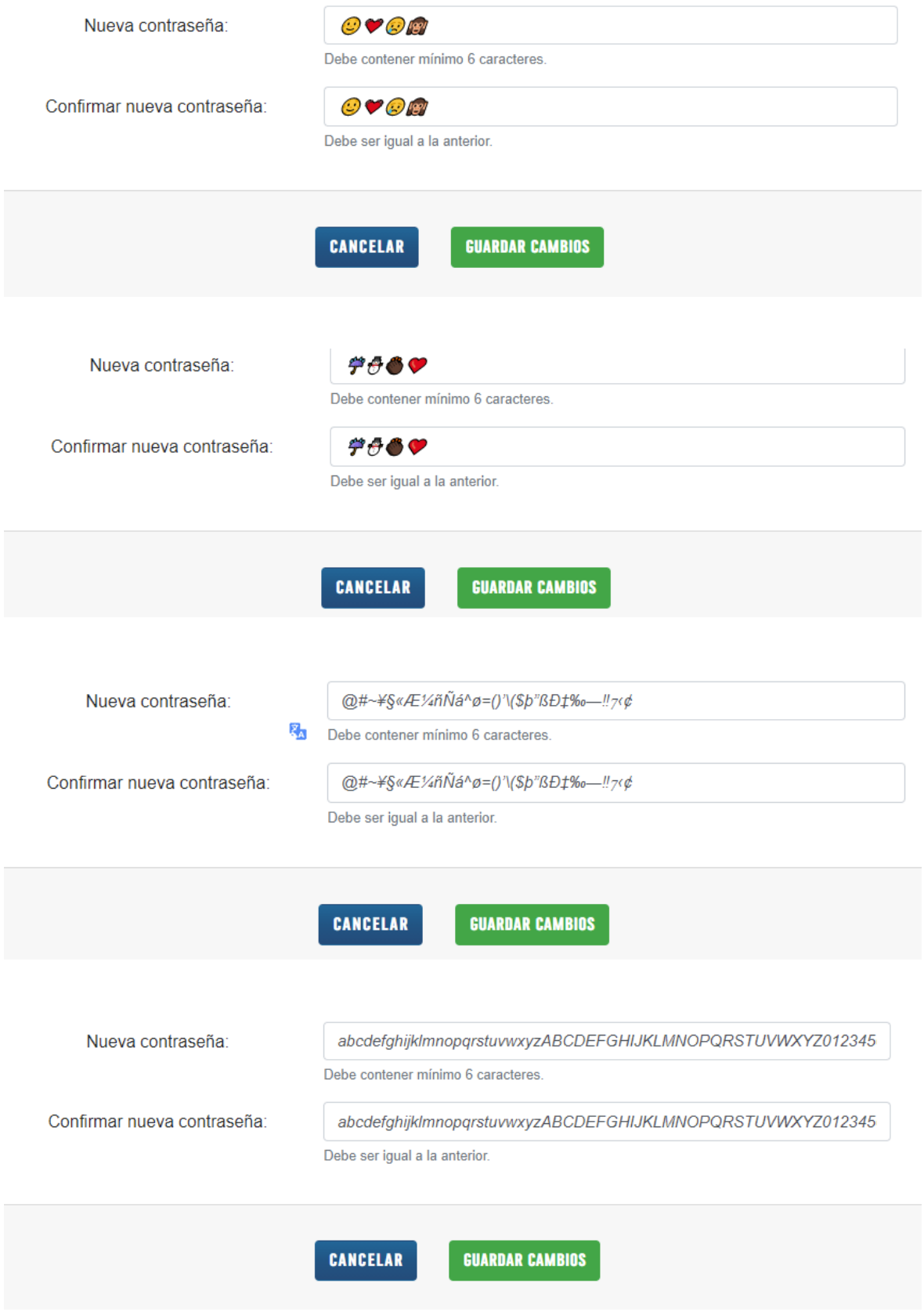
1. Pagina Chilena

1.1. ¿Cuál es el largo (L) mínimo y máximo de la contraseña a utilizar? ¿Cuál es la máxima base (W) que permite utilizar el sitio?

El largo mínimo de caracteres soportados en la password al momento de registrarse es de 6.
El largo máximo de caracteres soportados en la password al momento de registrarse es de 72.



Se probo con todas las bases y todas son reconocidas en la pagina, probando con la primera y cambiando la clave para las demas, aceptando todas


Nueva contraseña:
Debe contener mínimo 6 caracteres.
Confirmar nueva contraseña:
Debe ser igual a la anterior.
CANCELAR
GUARDAR CAMBIOS
Nueva contraseña:
Debe contener mínimo 6 caracteres.
Confirmar nueva contraseña:
Debe ser igual a la anterior.
CANCELAR
GUARDAR CAMBIOS
Nueva contraseña:
@#~¥§«Æ¼ñÑá^ø=()'\($þ"ßÐ‡‰—‼ㄱ‹¢
Debe contener mínimo 6 caracteres.
Confirmar nueva contraseña:
@#~¥§«Æ¼ñÑá^ø=()'\($þ"ßÐ‡‰—‼ㄱ‹¢
Debe ser igual a la anterior.
CANCELAR
GUARDAR CAMBIOS
Nueva contraseña:
abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ012345
Debe contener mínimo 6 caracteres.
Confirmar nueva contraseña:
abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ012345
Debe ser igual a la anterior.
CANCELAR
GUARDAR CAMBIOS

1.2. El largo mínimo/máximo está restringido desde el cliente? En caso de ser así, intente deshabilitar el límite de la password y verifique si el server permite registrarse con una password de un mayor tamaño. En caso de no poder, indique porqué no lo logró.

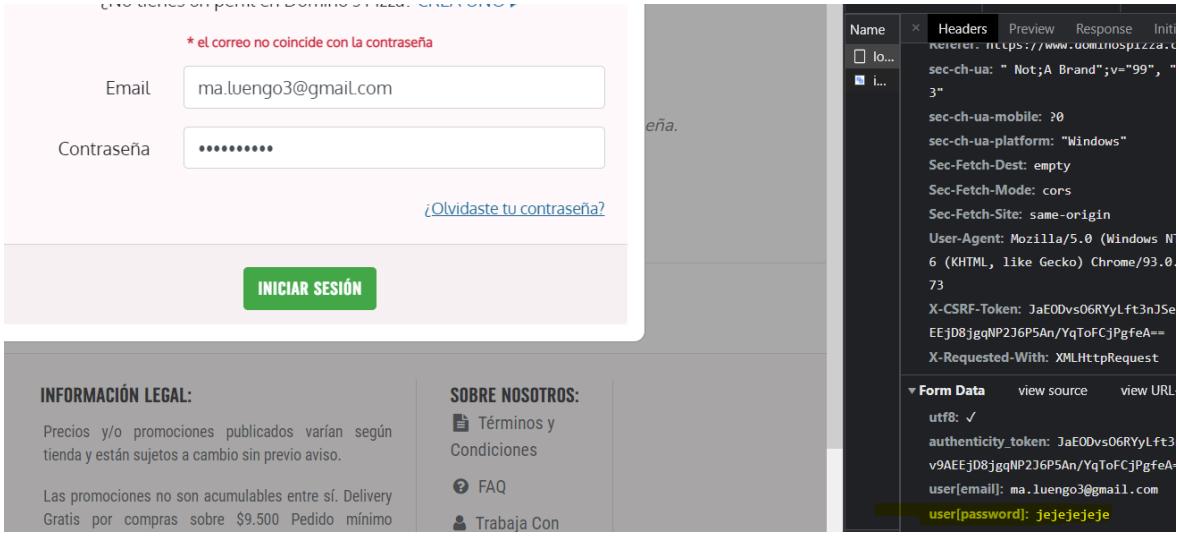
El largo si están restringidos, no deja cambiar nada. No se puede dashabilitar ya que las verificaciones de la contraseña están siendo directamente validadas por el backend, el fronted(Javascript)solo valida que la contraseña no sea nula.

1.3. ¿Existe comprobación de robustez de la pass al momento de registrarse? En caso de ser así, intente deshabilitar esta opción y verifique si el server acepta el uso de contraseñas débiles. En caso de no poder, indique porqué no lo logró.

No existe comprobación de robustez ya que acepta contraseñas débiles se muestra en la imagen a continuación.

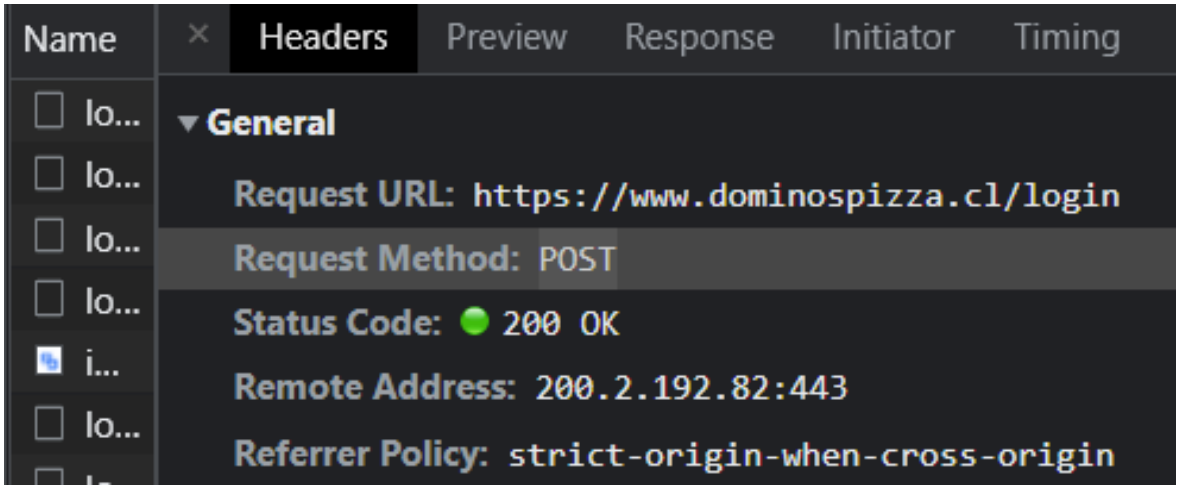
1.4. ¿Se transmite la contraseña en texto plano?

Si se transmite la contraseña en texto plano.



1.5. ¿En qué variable se transmite al server el user y password? (Variable utilizada en GET o POST, no en el HTML)

El user y el pass se transmiten al server en variable POST.



1.6. ¿Qué información se solicita para restablecer la contraseña?

La información que se solicita para restablecer la contraseña es solo el correo.

1.7. ¿Cómo opera el servicio de restablecer contraseña? (se envía la existente, se crea una temporal o el usuario resetea la antigua por una nueva)

El servicio al restablecer la contraseña se envía un correo con un link.

1.8. ¿En el proceso de reseteo se expone información privada del usuario? ¿La información expuesta está completa o de forma parcial (n***@gmail.com)?

En el proceso de reseteo se expone información privada del usuario como el correo electrónico y la información es expuesta de forma completa.

1.9. En caso de generar una password temporal. ¿Qué patrón tiene la nueva contraseña al resetearla? Automatice 10 reseteos de la contraseña (utilizando el proceso c) para obtener el patrón de las nuevas contraseñas, representado por una expresión regular. La extracción de las contraseñas nuevas que le lleguen al correo electrónico o celular, lo puede hacer de forma manual.

No genera password temporal, ya que envía un link para cambiar la contraseña.

1.10. ¿El sitio recuerda contraseñas antiguas? ¿Cuántas? ¿Es posible eliminar esas passwords de la memoria del server (se pueden sobrescribir)?

No recuerda contraseñas ya que al cambiar la contraseña por la misma, si lo permite.No es posible eliminar esas password ya que no las guarda.

1.11. ¿Las políticas del usuario obligan a entregar información verdadera? Verifique si el sitio obliga a ingresar su segundo apellido. En caso de ser así, ¿Qué podría hacer un usuario que solo tenga uno, sin tener que falsificar sus datos?

No, ya que al ingresar información al azar, mas que nada en nombre y apellido, la cuenta se crea igual. La pagina solo pide el primer apellido.

1.12. ¿El sitio es susceptible a ataques por fuerza bruta? ¿Cómo lo evita? Pruebe automatizando 100 accesos (recuerde que su cuenta se podría inhabilitar o bloquear, por lo que deberá realizar este proceso al final y no a última hora)

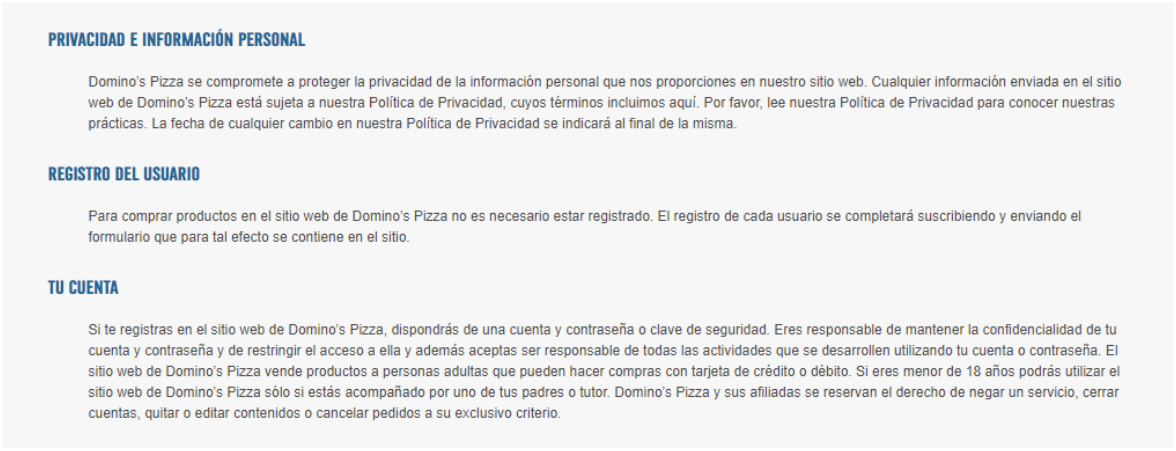
El sitio si es susceptible a ataques por fuerza bruta, no lo evita de ninguna forma y tampoco se bloquea la cuenta. Se hizo la automatización de los 100 accesos donde el código a ocupar se encuentra en el github.

1.13. ¿Existe la opción de eliminar su cuenta? En caso de ser así, ¿Queda algún indicio de la existencia de su cuenta?

No existe la opción de eliminar la cuenta.

1.14. ¿Los resultados obtenidos se condicen con las políticas de privacidad y seguridad del sitio?

La mayoria de los resultados coinciden, menos la seguridad, ya que al aceptar fuerza bruta, contraseñas poco seguras, no bloquear cuentas.La pagina no respeta sus políticas de seguridad



PRIVACIDAD E INFORMACIÓN PERSONAL

Domino's Pizza se compromete a proteger la privacidad de la información personal que nos proporciones en nuestro sitio web. Cualquier información enviada en el sitio web de Domino's Pizza está sujeta a nuestra Política de Privacidad, cuyos términos incluimos aquí. Por favor, lee nuestra Política de Privacidad para conocer nuestras prácticas. La fecha de cualquier cambio en nuestra Política de Privacidad se indicará al final de la misma.

REGISTRO DEL USUARIO

Para comprar productos en el sitio web de Domino's Pizza no es necesario estar registrado. El registro de cada usuario se completará suscribiendo y enviando el formulario que para tal efecto se contiene en el sitio.

TU CUENTA

Si te registras en el sitio web de Domino's Pizza, dispondrás de una cuenta y contraseña o clave de seguridad. Eres responsable de mantener la confidencialidad de tu cuenta y contraseña y de restringir el acceso a ella y además aceptas ser responsable de todas las actividades que se desarrollen utilizando tu cuenta o contraseña. El sitio web de Domino's Pizza vende productos a personas adultas que pueden hacer compras con tarjeta de crédito o débito. Si eres menor de 18 años podrás utilizar el sitio web de Domino's Pizza sólo si estás acompañado por uno de tus padres o tutor. Domino's Pizza y sus afiliadas se reservan el derecho de negar un servicio, cerrar cuentas, quitar o editar contenidos o cancelar pedidos a su exclusivo criterio.

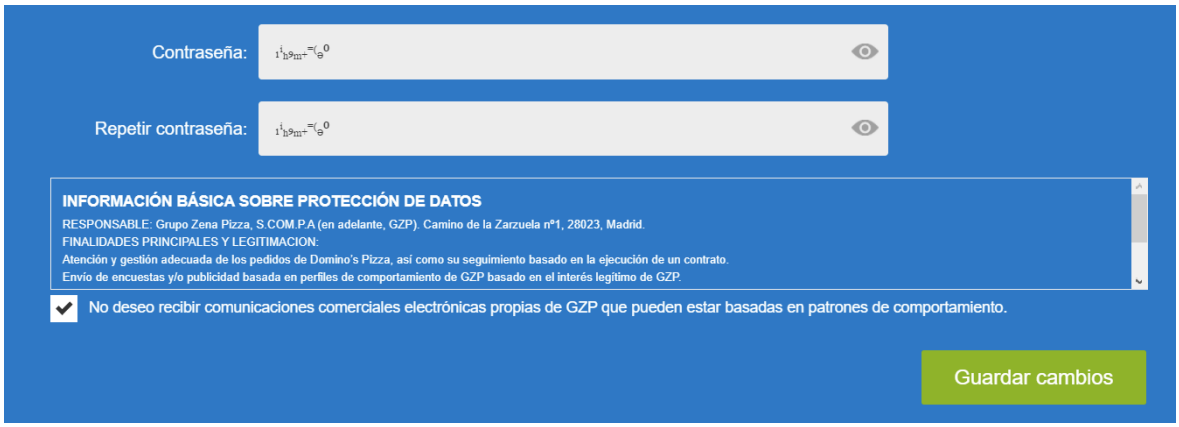
2. Pagina Europea

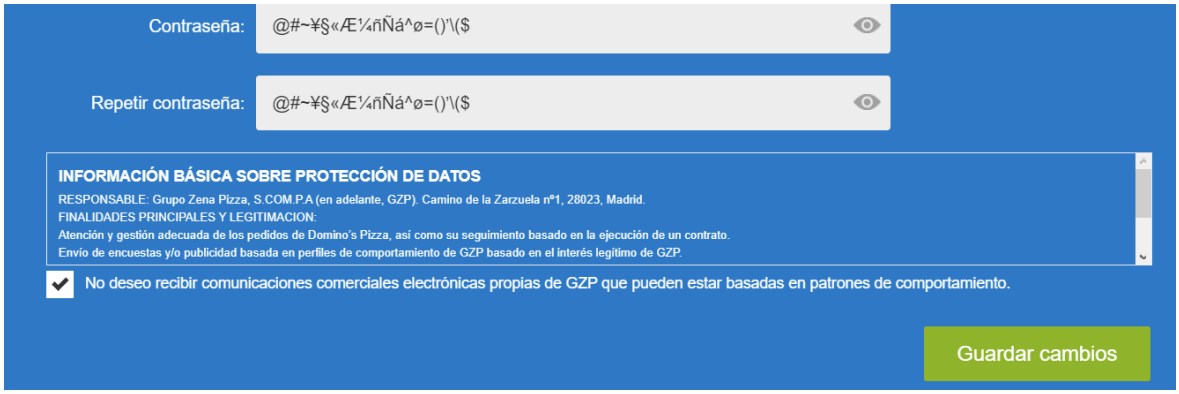
2.1. ¿Cuál es el largo (L) mínimo y máximo de la contraseña a utilizar? ¿Cuál es la máxima base (W) que permite utilizar el sitio?

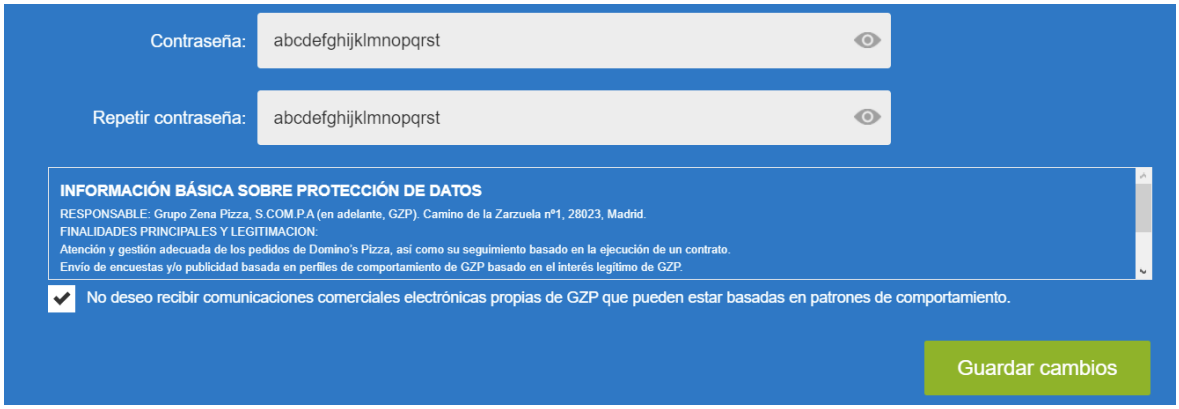
El largo mínimo de caracteres soportados en la password al momento de registrarse es de 8.

El largo máximo de caracteres soportados en la password al momento de registrarse es de 20, destacando que la pagina no lo dice, pero de todas formas acepta 20 caracteres.

Se probo con las 6 bases y acepta todas menos el alfabeto arabico.

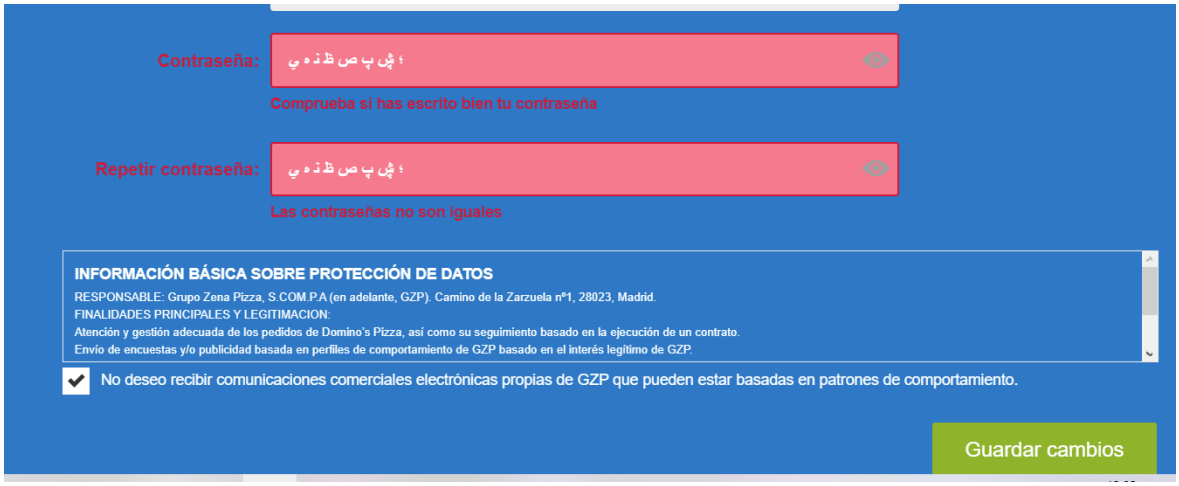





Contraseña:
abcdefghijklmnopqrst
Repetir contraseña:
abcdefghijklmnopqrst
INFORMACIÓN BÁSICA SOBRE PROTECCIÓN DE DATOS
RESPONSABLE: Grupo Zena Pizza, S.COM.P.A (en adelante, GZP). Camino de la Zarzuela nº1, 28023, Madrid.
FINALIDADES PRINCIPALES Y LEGITIMACION:
Atención y gestión adecuada de los pedidos de Domino's Pizza, así como su seguimiento basado en la ejecución de un contrato.
Envío de encuestas y/o publicidad basada en perfiles de comportamiento de GZP basado en el interés legítimo de GZP.
No deseo recibir comunicaciones comerciales electrónicas propias de GZP que pueden estar basadas en patrones de comportamiento.
Guardar cambios


Contraseña:
Repetir contraseña:
INFORMACIÓN BÁSICA SOBRE PROTECCIÓN DE DATOS
RESPONSABLE: Grupo Zena Pizza, S.COM.P.A (en adelante, GZP). Camino de la Zarzuela nº1, 28023, Madrid.
FINALIDADES PRINCIPALES Y LEGITIMACION:
Atención y gestión adecuada de los pedidos de Domino's Pizza, así como su seguimiento basado en la ejecución de un contrato.
Envío de encuestas y/o publicidad basada en perfiles de comportamiento de GZP basado en el interés legítimo de GZP.
No deseo recibir comunicaciones comerciales electrónicas propias de GZP que pueden estar basadas en patrones de comportamiento.
Guardar cambios


Contraseña:
Repetir contraseña:
INFORMACIÓN BÁSICA SOBRE PROTECCIÓN DE DATOS
RESPONSABLE: Grupo Zena Pizza, S.COM.P.A (en adelante, GZP). Camino de la Zarzuela nº1, 28023, Madrid.
FINALIDADES PRINCIPALES Y LEGITIMACION:
Atención y gestión adecuada de los pedidos de Domino's Pizza, así como su seguimiento basado en la ejecución de un contrato.
Envío de encuestas y/o publicidad basada en perfiles de comportamiento de GZP basado en el interés legítimo de GZP.
No deseo recibir comunicaciones comerciales electrónicas propias de GZP que pueden estar basadas en patrones de comportamiento.
Guardar cambios

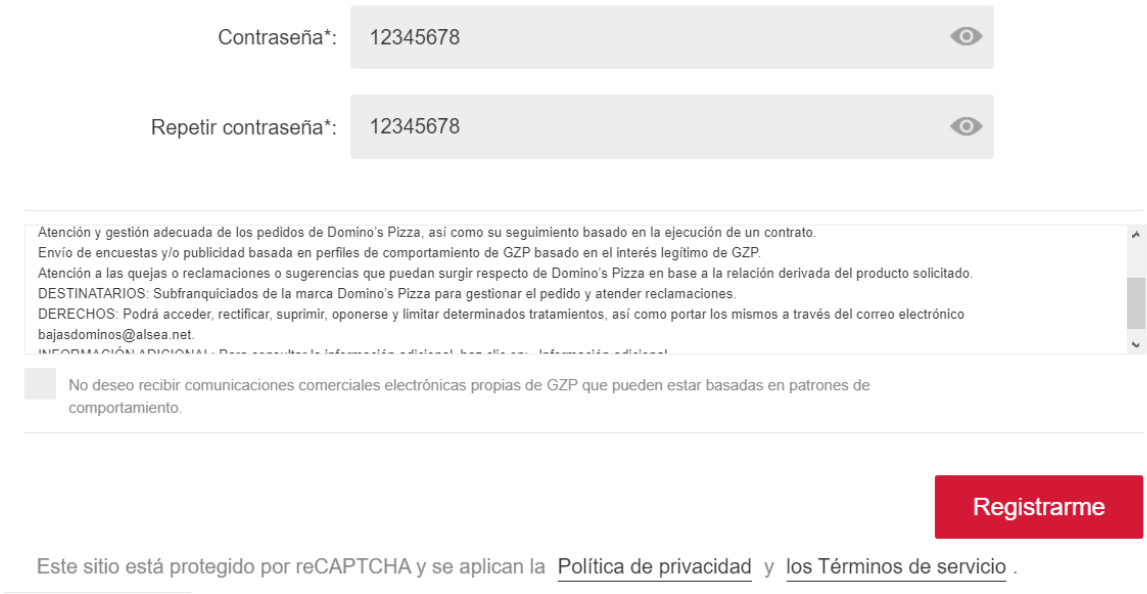


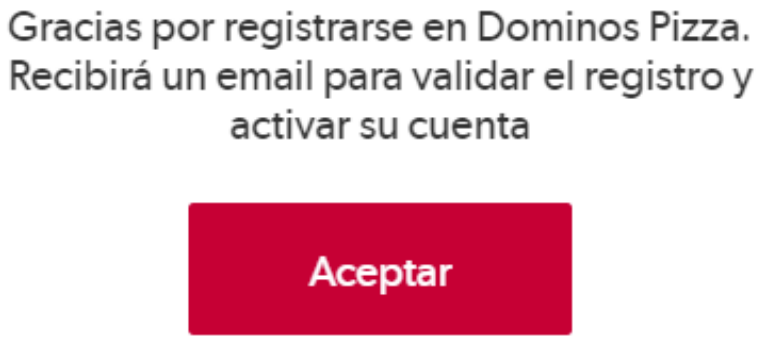
2.2. El largo mínimo/máximo está restringido desde el cliente? En caso de ser así, intente deshabilitar el límite de la password y verifique si el server permite registrarse con una password de un mayor tamaño. En caso de no poder, indique porqué no lo logró.

El largo si están restringidos, no deja cambiar nada. Al igual que en la pagina chilena, no puede dashabilitar ya que las verificaciones de la contraseña están siendo directamente validadas por el backend, el fronted(Javascript)solo valida que la contraseña no sea nula.

2.3. ¿Existe comprobación de robustez de la pass al momento de registrarse? En caso de ser así, intente deshabilitar esta opción y verifique si el server acepta el uso de contraseñas débiles. En caso de no poder, indique porqué no lo logró.

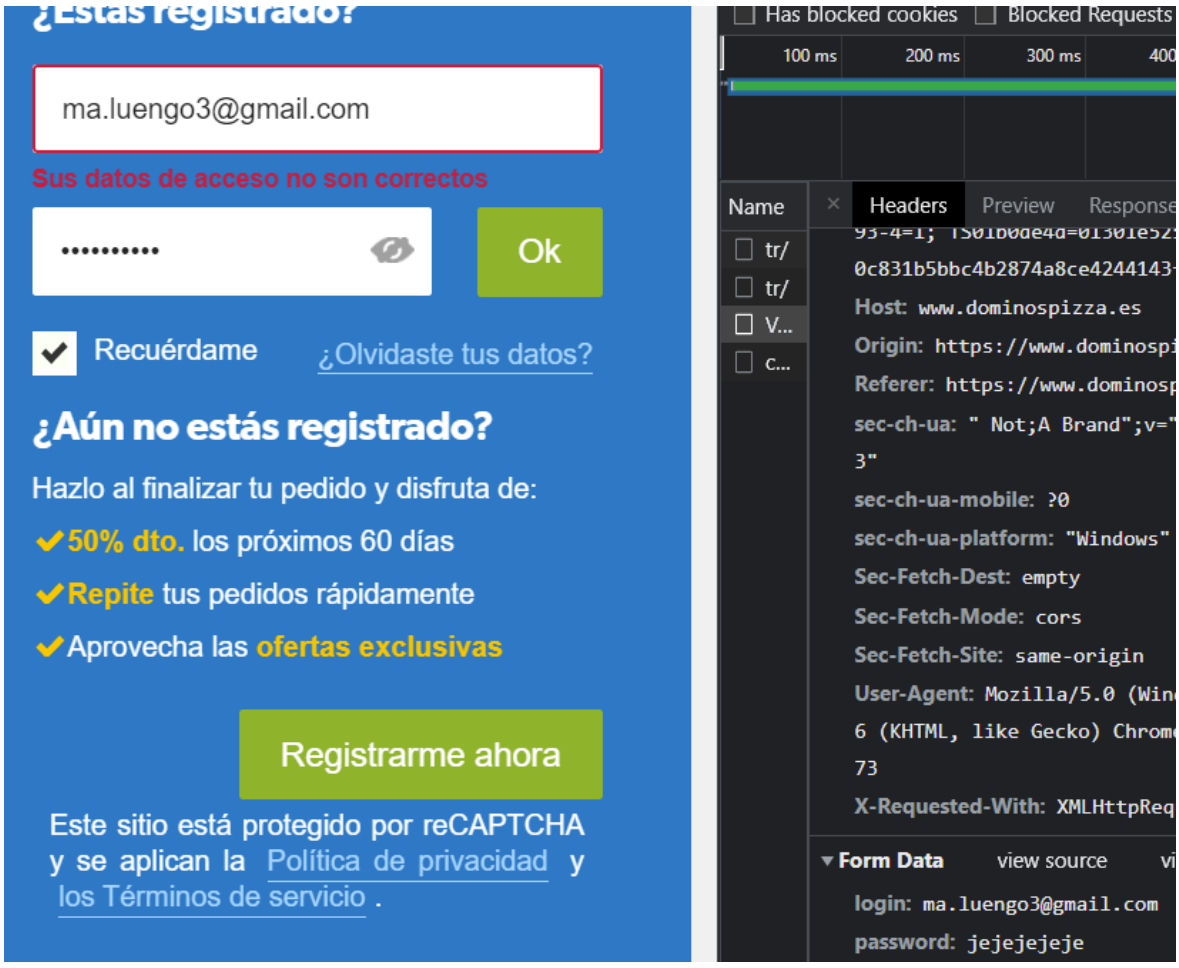
No existe comprobación de robustez ya que acepta contraseñas débiles como se muestra en las imágenes a continuación.





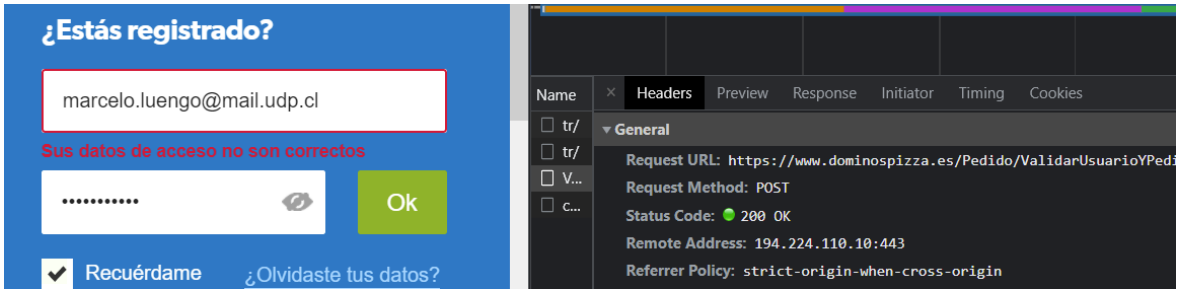
2.4. ¿Se transmite la contraseña en texto plano?

Si se transmite la contraseña en texto plano.



2.5. ¿En qué variable se transmite al server el user y password? (Variable utilizada en GET o POST, no en el HTML)

El user y pass se transmiten en variable post.



2.6. ¿Qué información se solicita para restablecer la contraseña?

La información que se solicita para restablecer la contraseña es solo el correo.

2.7. ¿Cómo opera el servicio de restablecer contraseña? (se envía la existente, se crea una temporal o el usuario resetea la antigua por una nueva)

El servicio al restablecer la contraseña se envía un link al correo.

2.8. ¿En el proceso de reseteo se expone información privada del usuario? ¿La información expuesta está completa o de forma parcial (n***@gmail.com)?

En el proceso de reseteo se expone informacion privada del usuario como el correo electronico y la información es expuesta de forma completa.

2.9. En caso de generar una password temporal. ¿Qué patrón tiene la nueva contraseña al resetearla? Automatice 10 reseteos de la contraseña (utilizando el proceso c) para obtener el patrón de las nuevas contraseñas, representado por una expresión regular. La extracción de las contraseñas nuevas que le lleguen al correo electrónico o celular, lo puede hacer de forma manual.

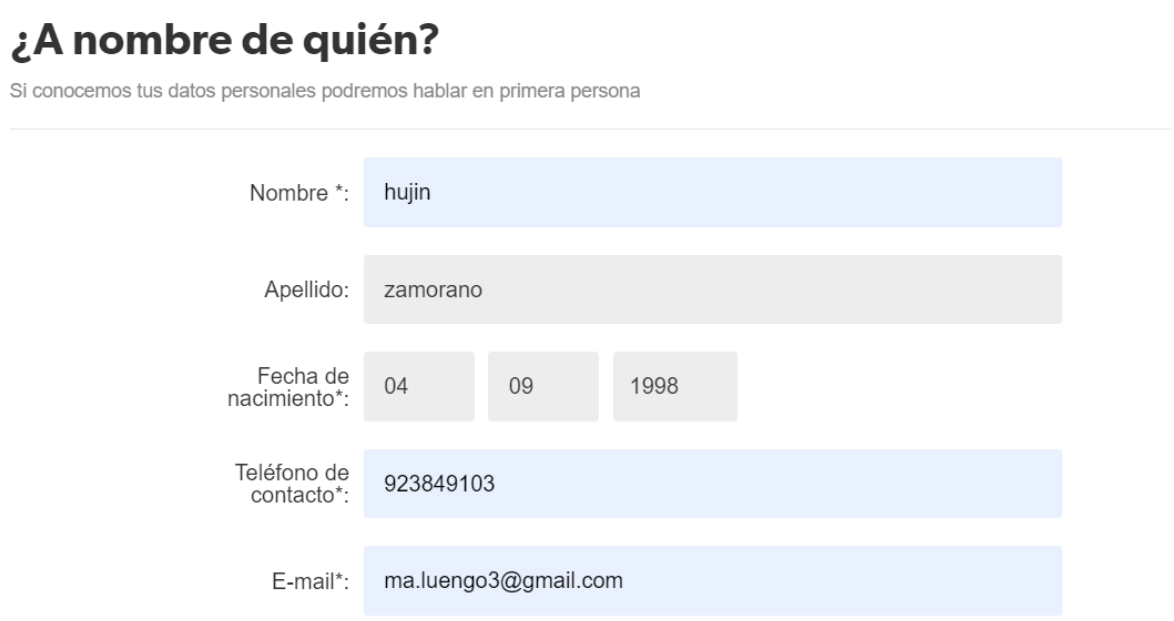
No genera password temporal, ya que envía un link para cambiar la contraseña.

2.10. ¿El sitio recuerda contraseñas antiguas? ¿Cuántas? ¿Es posible eliminar esas passwords de la memoria del server (se pueden sobrescribir)?

No recuerda contraseñas ya que al cambiar la contraseña por la misma contraseña si lo permite.No es posible eliminar esas password ya que no las guarda.

2.11. ¿Las políticas del usuario obligan a entregar información verdadera? Verifique si el sitio obliga a ingresar su segundo apellido. En caso de ser así, ¿Qué podría hacer un usuario que solo tenga uno, sin tener que falsificar sus datos?

No, ya que al ingresar información al azar, mas que nada en nombre y apellido, la cuenta se crea igual. La pagina solo pide el primer apellido.

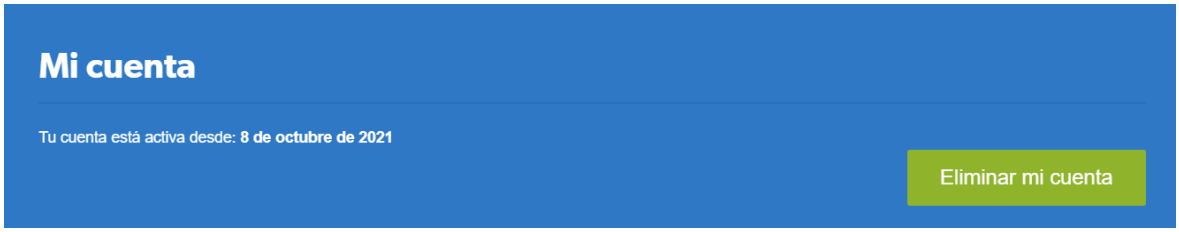


2.12. ¿El sitio es susceptible a ataques por fuerza bruta? ¿Cómo lo evita? Pruebe automatizando 100 accesos (recuerde que su cuenta se podría inhabilitar o bloquear, por lo que deberá realizar este proceso al final y no a última hora)

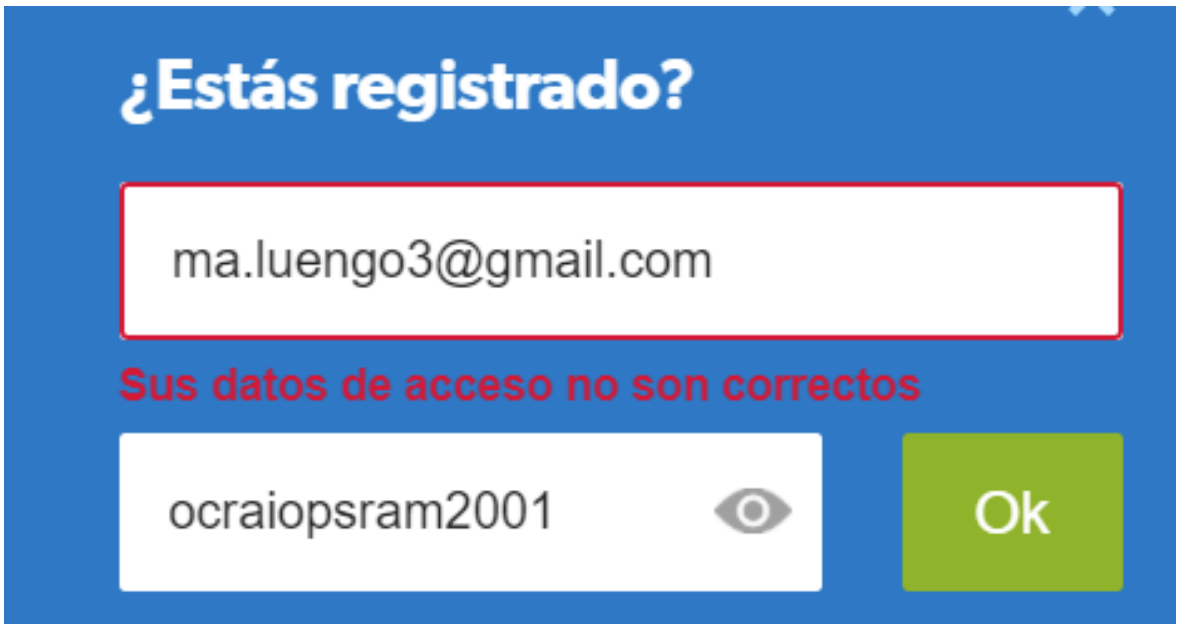
El sitio si es susceptible a ataques por fuerza bruta, no lo evita de ninguna forma y tampoco se bloquea la cuenta. Se hizo la automatización de los 100 accesos donde el código a ocupar se encuentra en el github.

2.13. ¿Existe la opción de eliminar su cuenta? En caso de ser así, ¿Queda algún indicio de la existencia de su cuenta?

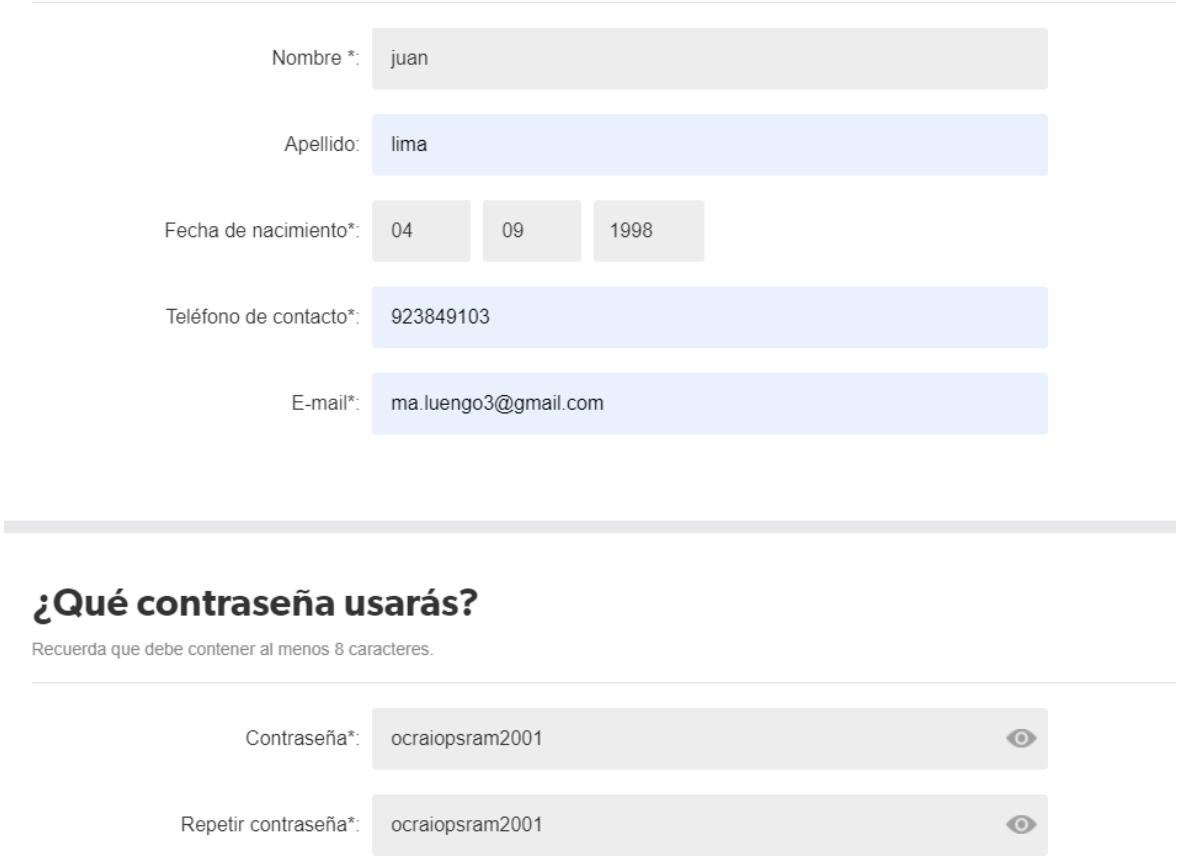
Si existe la opción de eliminar la cuenta.



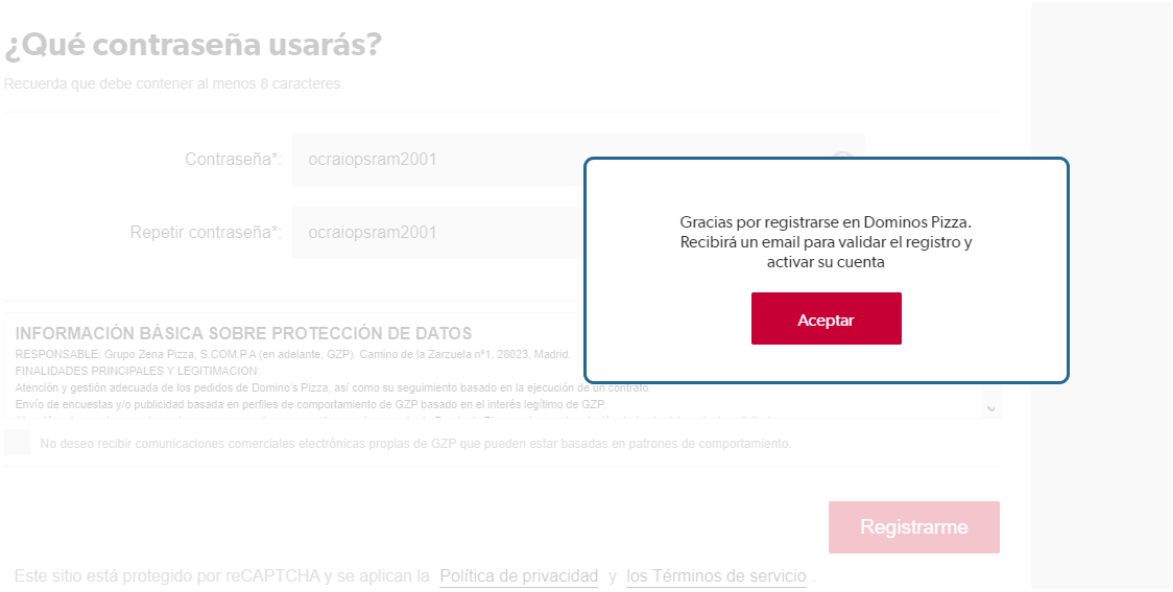
para verificar los indicios lo primero es intentar ingresar con la cuenta ya eliminada, lo que no nos deja por lo tanto la cuenta si fue eliminada



Se llega a la conclusión de que no quedan indicios de la cuenta eliminada, ya que nos deja crear un cuenta con los mismos datos.



Por consiguiente crearemos un cuenta con los mismos datos eliminados.



2.14. ¿Los resultados obtenidos se condicen con las políticas de privacidad y seguridad del sitio?

Los resultados obtenidos si coinciden en su mayoría pero presentan algunas incoherencias al momento de dejar todo el cargo de los datos a Grupo Zena Pizza, S.COM.P.A (en adelante, GZP), dejando a ellos al cuidado de los datos.Cuando según los estudios realizadosal igual que en la pagina chilena, la seguridad no corresponde a sus politicas de seguridad, ya que al aceptar fuerza bruta, contraseñas poco seguras, no bloquear cuentas, etc, la hace poco segura.