**PRÁCTICA N°4**

**TEMA: “PREVENCIÓN DE ATAQUES DE INGENIERIA SOCIAL Y SEGURIDAD EN EL ACCESO”**

**1. OBJETIVOS**

1.1 Personalizar y configurar una simulación de ataque de phishing en un entorno controlado.

1.2 Implementar una campaña de concientización y entrenamiento para prevenir ataques de phishing.

1.3 Establecer factores adicionales de autenticación.

**5.INFORME**

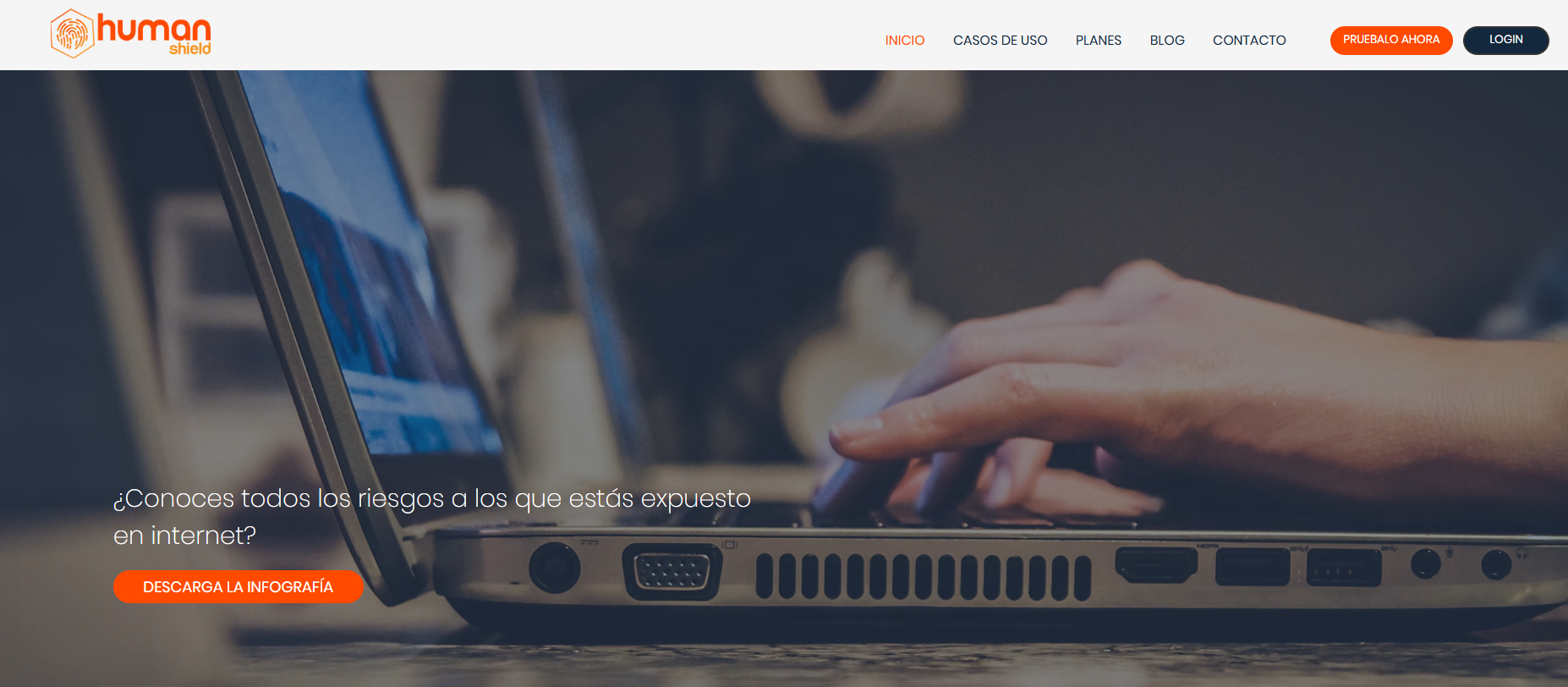
***5.1 ¿Cómo identificar la fiabilidad de un correo electrónico?***

* Verificar la autenticación del correo remitente
* Revisar que se encuentren bien redactados los correos sin faltas ortográficas o gramática grave.
* Identificar lo enlaces colocando el cursor sobre el enlace y ver si la URL es real.
* Solicitud de información confidencial.
* Firma del correo, como nombre del remitente, datos como teléfono y correo.
* Encabezado del correo , dirección ip.

***5.2 Describir el paso a paso de la simulación del ataque de phishing.***

#### Implementación de la Campaña de concientización

1. Ingresar al enlace de la plataforma de Human Shield para realizar el registro del usuario y acceder a la herramienta (Figura 1).



*Figura 1: Plataforma Human Shield*

1. Una vez dentro de la plataforma se observa el dashboard con graficas sobre las campañas de concientización; en el lado izquierdo tenemos menú de opciones (Figura 2), para empezar con la personalización debemos contar con una lista de usuario o colaboradores a los que les emitiremos la campaña de concientización.

Una captura de pantalla de una red social

Descripción generada automáticamente

*Figura 2: Dashboard de Human Shield*

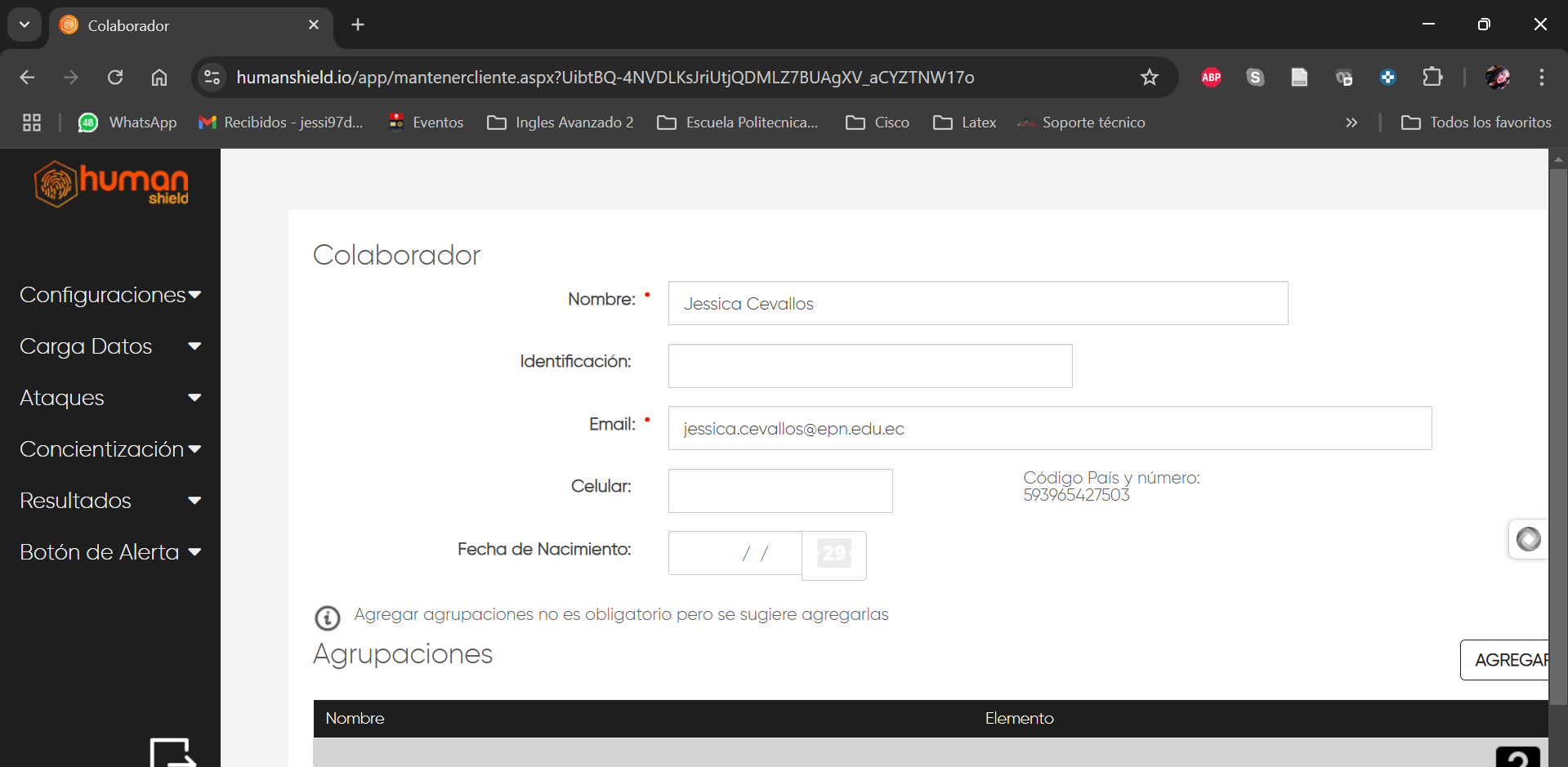
1. Ingresar en la opción de Carga de Datos > Colaboradores > Agregar usuarios tal como se presenta en la Figura 3, por lo que se necesita el nombre del usuario y el correo electrónico (Importante al hacer una prueba, solo se puede incluir usuarios de un solo dominio).

Captura de pantalla de un celular

Descripción generada automáticamente

*Figura 3: Agregar Usuarios*

1. Como se muestra en la Figura 4, los datos obligatorios son el correo institucional/corporativo y el nombre del usuario, ingresado los datos se coloca el botor agregar.



*Figura 4: Datos de los Usuarios*

1. Determinada el área o dedicación de los usuarios, se selecciona el tipo de amenaza que se va a enviar y el vector (es decir el medio por el que se va a enviar la amenaza) y la plantilla del correo electrónico, en este caso se toma la del CNE como se muestra en la Figura 5.

Interfaz de usuario gráfica

Descripción generada automáticamente

*Figura 5: Configuración tipo de ataque y medio de propagación*

1. En Ataque > Wizard

* Asignar el nombre del ataque Ejemplo: Prueba TIC
* Se procede a configurar, el dominio, nombre, email del remitente, según lo detalla la Figura 6.

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

*Figura 6: Configuración de Ataque*

1. Clic en Personalizar plantilla de correo (Figura 7), queda a disposición del estudiante la personalización en base al nombre y plantilla seleccionada.

Interfaz de usuario gráfica, Aplicación, Word

Descripción generada automáticamente

*Figura 7: Personalizar Plantilla*

1. En Ataque > Wizard > Desplegar Concientización Instantánea (sobre el ojo), tal como se observa en la Figura 8.

Editar el Logo del mensaje (mensaje se visualiza cuando hacen clic en el enlace), no olvide seleccionar la casilla.

Interfaz de usuario gráfica, Texto, Aplicación, Chat o mensaje de texto

Descripción generada automáticamente

*Figura 8: Configuración logo de concientización*

1. Dar clic desplegar concientización y seleccionar la campaña de concientización acorde al tipo de ataque emitido como se ilustra en la Figura 9. Ejemplo: Aprendamos sobre el Phishing y evitémoslo.

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

*Figura 9: Selección de la concientización adecuado*

1. Dar clic en siguiente y seleccionar a los usuarios que se emitirá el correo, como se muestra en la Figura 10.

Interfaz de usuario gráfica, Aplicación, Teams

Descripción generada automáticamente

*Figura 10: Selección de Usuarios*

1. En la Figura 11, se selecciona la actividad a realizar, en este caso se coloca ejecutar.

Interfaz de usuario gráfica, Aplicación, Sitio web

Descripción generada automáticamente

*Figura 11: Actividades a realizar*

1. La disposición mostrada en la Figura 12 resalta, Ejecución del Ataque y Confirmar

Captura de pantalla de un celular

Descripción generada automáticamente

*Figura 12: Listado de Ataques Ejecutados*

1. El correo ejecutado se muestra en la Figura 13 de la siguiente manera.

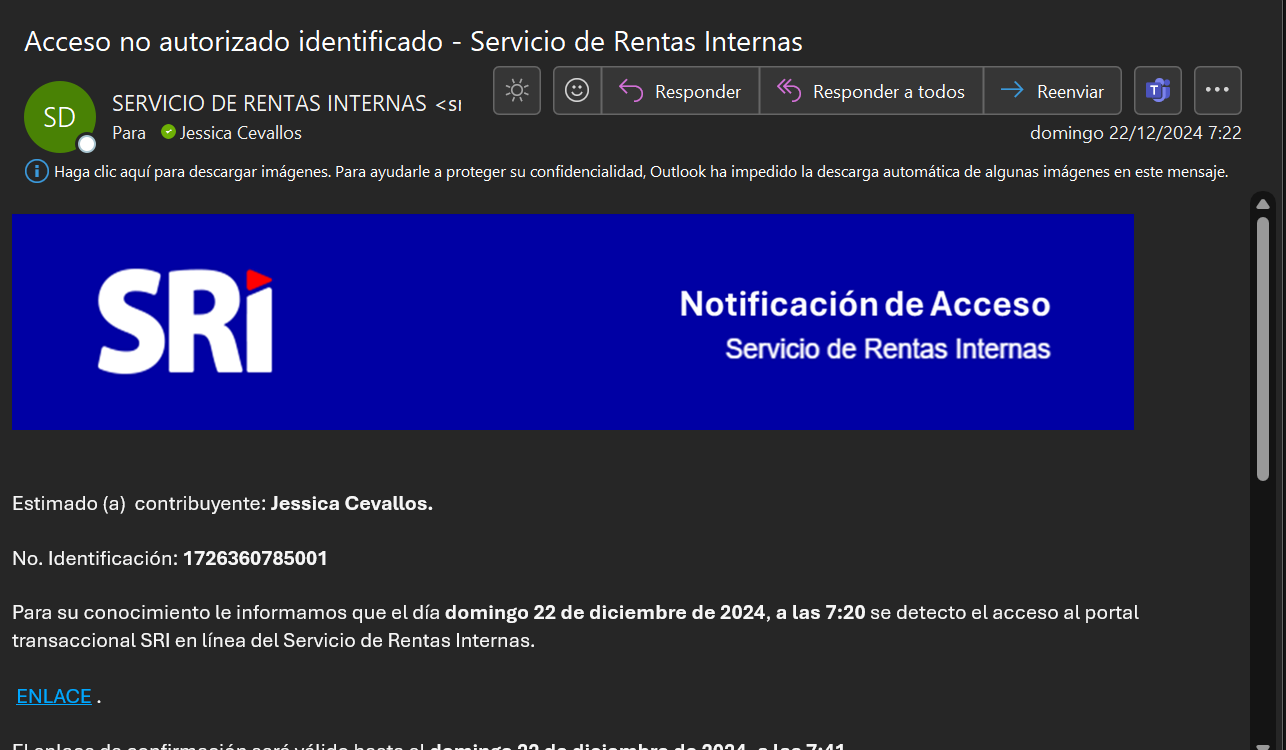


Figura 13: Correo Electrónico emitido

***5.3 Que hacer en el caso de ser infectado por un ataque de phishing.***

En el caso de que sea un dispositivo que pertenezca a una organización se debe informar al departamento encargado de la seguridad, para que ellos continúen con el protocolo de contingencia que deben tener.

Si se dieron información confidencial de acceso como usuario y contraseñas cambiar las contraseñas y monitorear la actividad de las cuentas, realizar un escaneo al dispositivo para identificar el ataque y mitigar el riesgo de impacto.