



¡Fortaleciendo Capacidades!

**SUPERIOR TECNOLÓGICO DE TURISMO Y PATRIMONIO  
YAVIRAC**

**CARRERA DE TECNÓLOGO SUPERIOR EN DESARROLLO DE SOFTWARE  
LINKEAR**



**PROYECTO EMPRESARIAL  
DESARROLLO DE UNA PÁGINA WEB PARA SOCIALIZAR SOBRE LA  
INGENIERÍA SOCIAL**

**TÍTULO DEL PROYECTO:  
INGENIERÍA SOCIAL ¡NO TE CONFÍES!**

**GRUPO DE PROYECTO:**

BONILLA PILATASIG CAROLINA GISSELA (PRIMERO)

AGUIRRE DÍAZ CHRISTIAN KEVIN (PRIMERO)

GUALLI CHANGO DANIEL (SEGUNDO)

**TUTOR ACADÉMICO:** Ing. Geovanni Pazmiño

**TUTOR EMPRESARIAL:** Ing. Juan Carlos Hinojosa

**ASIGNATURA DE FASE PRÁCTICA:** FUNDAMENTOS DE PROGRAMACIÓN

– PROGRAMACIÓN ORIENTADA A OBJETOS.

**NIVEL(ES):** PRIMERO Y SEGUNDO



QUITO, 21 ABRIL 2022

## ÍNDICE

TÍTULO DEL PROYECTO .....	4
PLANIFICACIÓN Y CRONOGRAMA .....	10
OBJETIVOS .....	4
Objetivo General.....	4
Objetivos Específicos .....	4
INTRODUCCIÓN .....	4
Planteamiento del Problema .....	4
JUSTIFICACIÓN .....	5
INGENIERÍA SOCIAL (SEGURIDAD INFORMÁTICA) .....	5
TÉCNICAS Y TÉRMINOS .....	5
PRETEXTOS .....	6
REDES SOCIALES .....	6
PHISHING .....	7
VISHING.....	8
BAITING.....	8
QUID PRO QUO.....	8
ALCANCE DEL PROYECTO .....	8
METODOLOGÍA DE DESARROLLO DE SOFTWARE (SI APLICA) .....	9
Tipo de estudio .....	9
Modalidad de la investigación.....	9
Fuentes de información .....	9
MÉTODO DE INVESTIGACIÓN.....	9



**INSTRUMENTOS PARA LA RECOLECCIÓN DE LA INFORMACIÓN ..... 10**

Recolección de datos ..... 10

Procesamiento y análisis de datos ..... 10

**RESULTADOS ALCANZADOS ..... 10**

**CONCLUSIONES Y RECOMENDACIONES ..... 11**

CONCLUSIONES ..... 11

RECOMENDACIONES ..... 12

**REFERENCIAS ..... 12**

**ANEXOS ..... 12**



*¡Fortaleciendo Capacidades!*



## TÍTULO DEL PROYECTO

INGENIERÍA SOCIAL ¡NO TE CONFÍES!

## OBJETIVOS

### Objetivo General

Socializar el ataque cibernético de Ingeniería Social, sus métodos, causas y efectos, para su prevención, a través del desarrollo de un aplicativo web, que permita la cuantificación del nivel de conocimiento de este delito informático.

### Objetivos Específicos

- Prevenir a la sociedad sobre el ataque de Ingeniería Social mediante la difusión de información para la detección de dicho ataque.
- Desarrollar el aplicativo web para la divulgación de la metodología de causa y efecto de Ingeniería Social, para la autodefensa.
- Cuantificar el grado de los efectos que causa la Ingeniería Social en la integralidad de la víctima, a través de la realización de encuestas online mediante la interacción con los usuarios.

## INTRODUCCIÓN

### Planteamiento del Problema

El presente proyecto está enfocado en el estudio del ataque de Ingeniería Social, sus métodos, causas y efectos para evitar ser víctimas del mismo.

Es importante que la sociedad y empresas estén alertas con esta temática, teniendo en cuenta que, al implementar medidas de control estrictos, se puede evitar ser atacados por personas inescrupulosas que buscan beneficios ilegales apropiándose de los datos personales para ocasionar daños.

Por esta razón es importante que la sociedad se concientice y genere cultura, sobre el uso correcto que debe tener con la tecnología específicamente en la internet y redes sociales; de esta manera se logrará que la sociedad contribuya para apoyar, orientar, neutralizar y enfrentarse a éstos.



## **JUSTIFICACIÓN**

Con el pasar del tiempo la tecnología y la internet han sido de gran importancia ya que gracias a sus múltiples avances ha logrado facilitar la vida de las personas respecto a la comunicación, relación, logro de información, enseñanza, aprendizaje, empleo entre otros, sin embargo, el uso incorrecto de la tecnología e internet por parte de las personas oportunistas trae consecuencias que afectan a las personas inocentes en este caso por medio de diferentes técnicas de Ingeniería Social atacando a las víctimas sin consideración alguna.

Por tal razón se hace importante el reconocimiento, primero; de que la información es el activo más importante que tiene una organización, junto con el recurso humano, y de que se le debe brindar la protección necesaria y pertinente para mantenerla resguardada de cualquier ataque. Y segundo, que como dicha información es tan importante, siempre va a existir quien la quiera obtener de forma no autorizada y en este sentido, se deben identificar cada una de las vulnerabilidades de los sistemas de seguridad.

Los resultados de esta información pueden ser útiles para que en el futuro se logre generar cultura y permitan resolver algunos de los problemas de Ingeniería Social.

## **INGENIERÍA SOCIAL (SEGURIDAD INFORMÁTICA)**

“La ingeniería social es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos. Es una técnica que pueden usar ciertas personas para obtener información, acceso o permisos en sistemas de información que les permitan realizar daños a la persona u organismo comprometidos” (WIKIPEDIA, 2016)

## **TÉCNICAS Y TÉRMINOS**

En la práctica, un ingeniero social usará comúnmente el teléfono o Internet para engañar a la gente, fingiendo ser, por ejemplo, un empleado de algún banco o alguna otra empresa, un compañero de trabajo, un técnico o un cliente. Vía Internet se usa, adicionalmente, el



envío de solicitudes de renovación de permisos de acceso a páginas web o correos electrónicos falsos que solicitan respuestas e incluso las famosas cadenas, llevando así a revelar sus credenciales de acceso o información sensible, confidencial o crítica.

Con este método, los ingenieros sociales aprovechan la tendencia natural de la gente a reaccionar de manera predecible en ciertas situaciones, –por ejemplo, proporcionando detalles financieros a un aparente funcionario de un banco– en lugar de tener que encontrar agujeros de seguridad en los sistemas informáticos.

La ingeniería Social está definida como un ataque basado en engañar a un usuario o administrador de un sitio en la internet, para poder ver la información que ellos quieren. Se hace para obtener acceso a sistemas o información útil.

Los objetivos de la ingeniería social son fraude, invasión de una red.

### **PRETEXTOS**

El pretexto es la creación de un escenario inventado para llevar a la víctima a revelar información personal o a actuar de una forma que sería poco común en circunstancias normales. Una mentira elaborada implica a menudo una investigación previa de la víctima para conseguir la información necesaria, y así llevar a cabo la suplantación (por ejemplo, la fecha de nacimiento, el número de la Seguridad Social, datos bancarios, etc.) y hacerle creer que es legítimo.

### **REDES SOCIALES**

Uno de los factores más peligrosos, es la creciente tendencia por parte de los usuarios, principalmente los más jóvenes, a colocar información personal y sensible en forma constante. Desde imágenes de toda su familia, los lugares que frecuentan, gustos personales y relaciones amorosas. Las redes sociales proveen de mucha información a un delincuente para que realice un ataque, como para robar tu identidad o en el menor de los casos ser convincente para tener empatía.



## PHISHING

Quizá el ataque más simple pero muy efectivo sea engañar a un usuario llevándolo a pensar que un administrador del sistema está solicitando una contraseña para varios propósitos legítimos. Los usuarios de sistemas de Internet frecuentemente reciben mensajes que solicitan contraseñas o información de tarjeta de crédito, con el motivo de "crear una cuenta", "reactivar una configuración", u otra operación benigna; a este tipo de ataques se los llama phishing (se pronuncia igual que fishing, pesca). Los usuarios de estos sistemas deberían ser advertidos temprana y frecuentemente para que no divulguen contraseñas u otra información sensible a personas que dicen ser administradores.

Otro ejemplo contemporáneo de un ataque de ingeniería social es el uso de archivos adjuntos en correos electrónicos, ofreciendo, por ejemplo, fotos "íntimas" de alguna persona famosa o algún programa "gratis" (a menudo aparentemente provenientes de alguna persona conocida) pero que ejecutan código malicioso (por ejemplo, usar la máquina de la víctima para enviar cantidades masivas de spam). Ahora, después de que los primeros correos electrónicos maliciosos llevaran a los proveedores de software a deshabilitar la ejecución automática de archivos adjuntos, los usuarios deben activar esos archivos de forma explícita para que ocurra una acción maliciosa. Muchos usuarios, sin embargo, abren casi ciegamente cualquier archivo adjunto recibido, concretando de esta forma el ataque.

La ingeniería social también se aplica al acto de manipulación cara a cara para obtener acceso a los sistemas informáticos. Otro ejemplo es el conocimiento sobre la víctima, a través de la introducción de contraseñas habituales, lógicas típicas o conociendo su pasado y presente; respondiendo a la pregunta: ¿Qué contraseña introduciría yo si fuese la víctima?

La principal defensa contra la ingeniería social es educar y entrenar a los usuarios en el uso de políticas de seguridad y asegurarse de que estas sean seguidas.

Uno de los ingenieros sociales más famosos de los últimos tiempos es Kevin Mitnick.





## **VISHING**

El vishing consiste en realizar llamadas telefónicas encubiertas bajo encuestas con las que también se podría sacar información personal de forma que la víctima no sospeche.

Por este motivo debemos tener cuidado y no proporcionar información personal aunque se trate de nuestra compañía de móvil, electricidad o agua (entre otras), ya que podría ser un hacker que haya elegido casualmente la nuestra.

## **BAITING**

En este caso se utiliza un dispositivo de almacenamiento extraíble (CD, DVD, USB) infectado con un software malicioso, dejándolo en un lugar en el cual sea fácil de encontrar (por ejemplo, baños públicos, ascensores, aceras, etc.). Cuando la víctima encuentre dicho dispositivo y lo introduzca en su ordenador, el software se instalará y permitirá que el hacker obtenga todos los datos personales del usuario.<sup>3</sup>

## **QUID PRO QUO**

Quid pro quo significa "algo por algo". El atacante llama a números aleatorios en una empresa, alegando estar llamando de nuevo desde el soporte técnico. Esta persona informará a alguien de un problema legítimo y se ofrecerá a ayudarlo, durante el proceso conseguirá los datos de acceso y lanzará un malware.

En una encuesta de seguridad de la información de 2003, el 90% de los trabajadores de una oficina dieron a los atacantes lo que ellos afirmaban ser su contraseña en respuesta a una pregunta de la encuesta a cambio de una pluma. Estudios similares en años posteriores obtuvieron resultados similares utilizando chocolates y otros señuelos baratos, aunque no intentaron validar las contraseñas.

## **ALCANCE DEL PROYECTO**

En el presente proyecto nos enfocaremos en la creación de una página web “Ingeniería Social No Te Confíes” de bienvenida donde constará el nombre de la comunidad, lugar de ubicación, el contenido de la información y contactos, a su vez se diseñará un perfil virtual donde se detalla:

1. La creación de un usuario
2. Login





3. Proyecto

4. Encuesta y tabulación

La página web “Ingeniería Social No Te Confíes” se obtendrá los resultados de las encuestas para su proceso y de esta manera conseguir los niveles de percepción sobre este ataque.

## **METODOLOGÍA DE DESARROLLO DE SOFTWARE**

### **Tipo de estudio**

#### **Modalidad de la investigación**

La modalidad de la investigación que se aplico es de tipo descriptivo porque permite identificar las características de las variables y correlacionar los hechos o fenómenos a investigar.

El proyecto se realizará utilizando las Metodología Ágil SCRUM e Incremental, la cual tiene como objetivo un crecimiento progresivo de la funcionalidad del proyecto. Las tareas están divididas en interacciones específicas que no se repite las cuales se desarrolla en un lapso de tiempo y se analiza si se esta cumpliendo con el objetivo del proyecto.

#### **Fuentes de información**

**Primarias:** La información recopilada se obtuvo a partir de un estudio en el que se tomó una muestra de personas que se encuestó.

**Secundarias:** Además de las anteriores fuentes, se reunió información en páginas de Internet y en general toda la documentación necesaria para el desarrollo del proyecto.

## **MÉTODO DE INVESTIGACIÓN**

**Observación:** se aplicará este método para examinar los diferentes sucesos que ayudaran en el análisis del objeto de estudio.

**Inductivo:** se aplicará este método con el fin de analizar los acontecimientos particulares y llegar a conclusiones y requisitos.

**Deductivo:** este método se utilizará para el análisis de los sucesos generales para así llegar a realidades particulares.



## **INSTRUMENTOS PARA LA RECOLECCIÓN DE LA INFORMACIÓN**

Las técnicas de investigación que se usó en este proyecto fue la técnica de la encuesta, la cual fue elaborada y aplicada satisfactoriamente. Esta encuesta conto con un cuestionario, el cual permitió identificar la inseguridad de la sociedad.

### **Recolección de datos**

La encuesta se aplicó en forma individual y virtual, a través de la web, logrando así la honestidad y veracidad en cada respuesta.

### **Procesamiento y análisis de datos**

Una vez recolectada la información, se ordenaron y analizaron las respuestas a través del método de porcentajes al cual se le genero su respectivo análisis estadístico, producto de la información obtenida por la aplicación de esta encuesta.

## **PLANIFICACIÓN Y CRONOGRAMA**

La planificación de tareas se realizó por medio de 5 semanas definidas de la siguiente manera: en la primera semana se llevó a cabo el plan de trabajo, el cual incluye: identificación del problema, objetivos, metodologías, tareas para alcanzar los objetivos descritos, para la segunda semana se realizó el diseño de la página de la cual desprende de tres fases:

1. Identificación del objetivo.
- 2.Reconocimiento del objetivo (qué, quién, como, etc.)
3. Diseñar la página

La tercera semana hace referencia a la ejecución correspondiente a la simulación del ataque informático de la técnica de Ingeniería Social, luego la cuarta semana realizo el análisis de la información obtenida y finalmente en la quinta semana se entregó el informe final con los resultados, conclusiones y recomendaciones sobre la investigación relacionada con las metodologías de la Ingeniería Social.



ACTIVIDADES	CRONOGRAMA	
	MARZO	ABRIL
1. Plan de trabajo	X	
2 y 3. Diseño de la página y ejecución	x	
4. Análisis de la información		x
5. Entrega del informe final		x

## RESULTADOS ALCANZADOS

1. Creación y desarrollo del CRUD de proyecto, para el registro del nombre, descripción, visión, misión, objetivos, causas y efectos.
2. Creación y desarrollo del CRUD del login-usuario, para el inicio de sesión: username, y password.
3. Creación y desarrollo del CRUD del registro usuario, para el registro del username, password, nombres, apellidos, cedula, celular, edad y ciudad.
4. Creación y desarrollo del CRUD de encuestas, para el registro de archivos referentes a la encuesta.

## CONCLUSIONES Y RECOMENDACIONES

### CONCLUSIONES

Con el desarrollo del presente trabajo se obtuvo:

- Identificar y diferenciar las técnicas de ingeniería social, así mismo las técnicas en función de la interacción que se tiene con la víctima.
- La ejecución de la encuesta donde se evidencio que las personas no son conscientes que pueden ser víctimas de Ingeniería Social, de igual forma existen vacíos y desconocimiento por parte de los encuestados sobre los tipos, técnicas, causas, consecuencias y peligros que abarca el tema.
- Brindar información con el fin de que las personas no sean víctimas de Ingeniería Social.



## RECOMENDACIONES

- Analizar con antivirus todos los correos que se reciban.
- No informar telefónicamente de las características técnicas de la red, ni nombre de personal a cargo, etc.
- Si tenemos un mensaje escrito o en las redes sociales debemos ignorarlo y borrarlo. Si el ataque se produce utilizando el nombre de algún conocido, debemos contactarnos con él y averiguar si la petición es cierta.
- Si tenemos una llamada telefónica se debe colgar inmediatamente, si el llamante, es persistente, es necesario pedirle un numero directo al que se le pueda llamar.

## REFERENCIAS

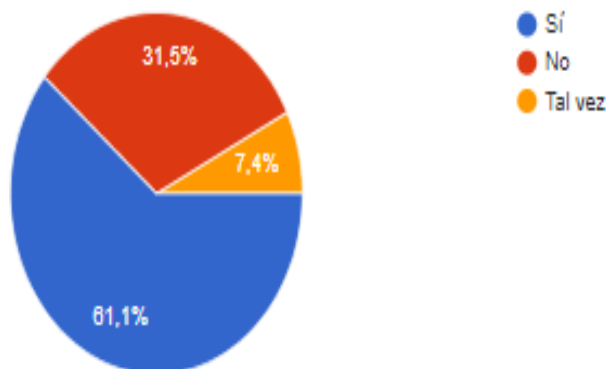
### Bibliografía

WIKIPEDIA. (16 de 02 de 2016). *WIKIPEDIA.COM*. Obtenido de [https://es.wikipedia.org/wiki/Ingenier%C3%ADa\\_social\\_\(seguridad\\_inform%C3%A1tica\)](https://es.wikipedia.org/wiki/Ingenier%C3%ADa_social_(seguridad_inform%C3%A1tica))

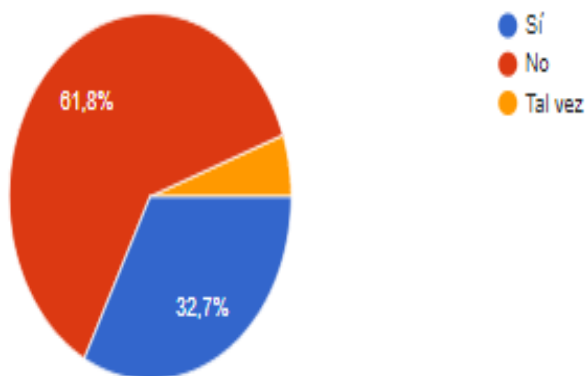
## ANEXOS

### ENCUESTA APLICADA

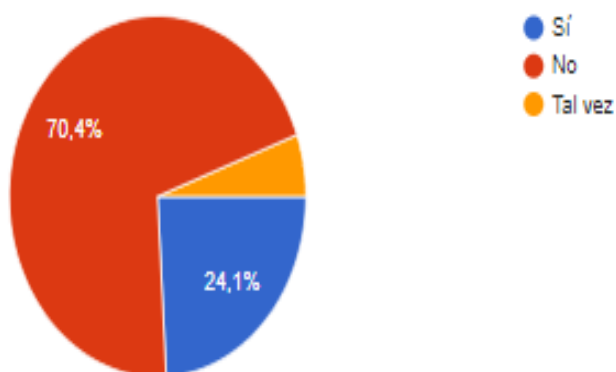
#### 1. ¿Alguna vez a escuchado hablar sobre los temas de Ciberseguridad?



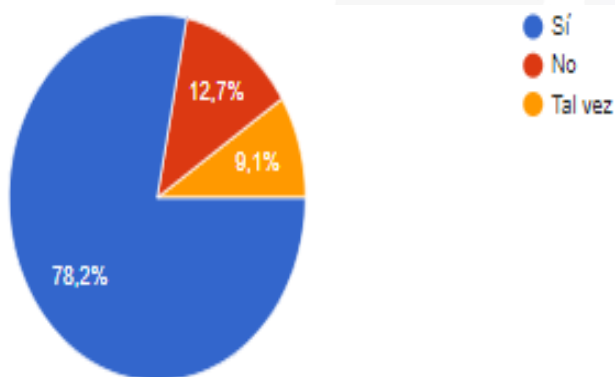
2. ¿Conoce sobre el tema de Ingeniería social?



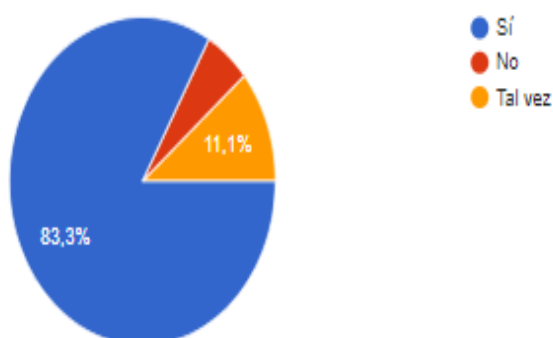
3. ¿Conoce sobre el tema de Phishing?



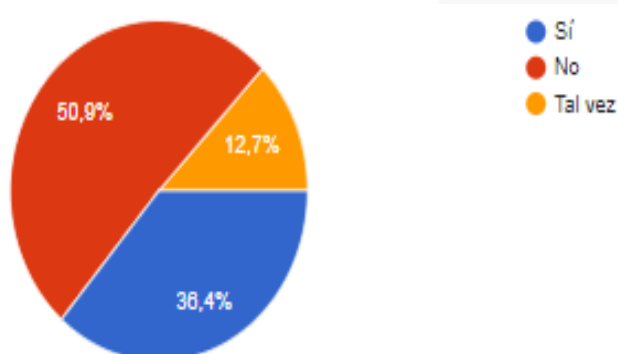
4. ¿Quisiera conocer más sobre los temas de Ciberseguridad (Ingeniería Social, Phishing)?



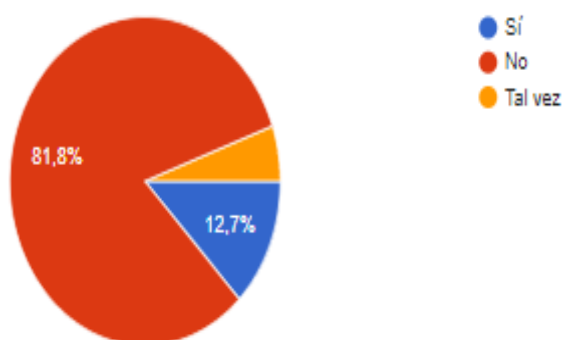
5. ¿Le gustaría que hubiese una comunidad de personas que compartan experiencias relacionadas a las estafas por medios tecnológicos e-mails, WhatsApp, publicidad en internet etc.?



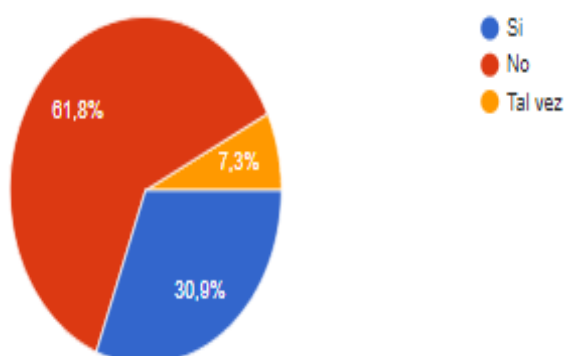
6. ¿Ha compartido cadenas de publicidad sobre empresas conocidas que supuestamente ofertan diferentes servicios como empleos o premios etc. Que se transmiten por medios tecnológicos: e-mails, WhatsApp, publicidad en internet etc.?



7. Conoce usted como evitar los ataques a través de la Ingeniería Social?



8. ¿Tiene algún conocido que haya sufrido una estafa por medios tecnológicos: e-mails, WhatsApp, publicidad en internet etc.? (Si su respuesta es SI describa su experiencia).



Describa su experiencia

22 respuestas

No

Llamó un supuesto familiar del extranjero a pedir dinero pero en realidad era un estafador

Ofrecieron un trabajo supuestamente de Amazon y le hackearon la cuenta

Saber más del tema

no conosco mucho sobre el tema de ciberseguridad

Robaron de su banco una cantidad de dinero a través de sus redes y su sistema operativo telefonico.

Por medio de las tarjetas de crédito tuvo un robo un familiar

Desearía conocer mas sobre el tema

Por llamada telefónica



Exelente

Muy buena nos ayuda a mejorar

No tengo mucha pero e visto muchos casos de robos x medio del celular

Primo sufrió robo cibernético

Por medio de una llamada informando que mi tío había y tenido un accidente y que le depositen a una cuenta para ayudarle pero era un estafador ya que mi tío estaba en su hogar

A un conocido le robaron mediante tarjetas

A mi tio le robaron 100\$ por llamada telefonica

Estafas por correo

Es algo muy penoso ver q hay personas sin escrúpulos q ganan dinero atravez de terceras personas

MUY BUENA!

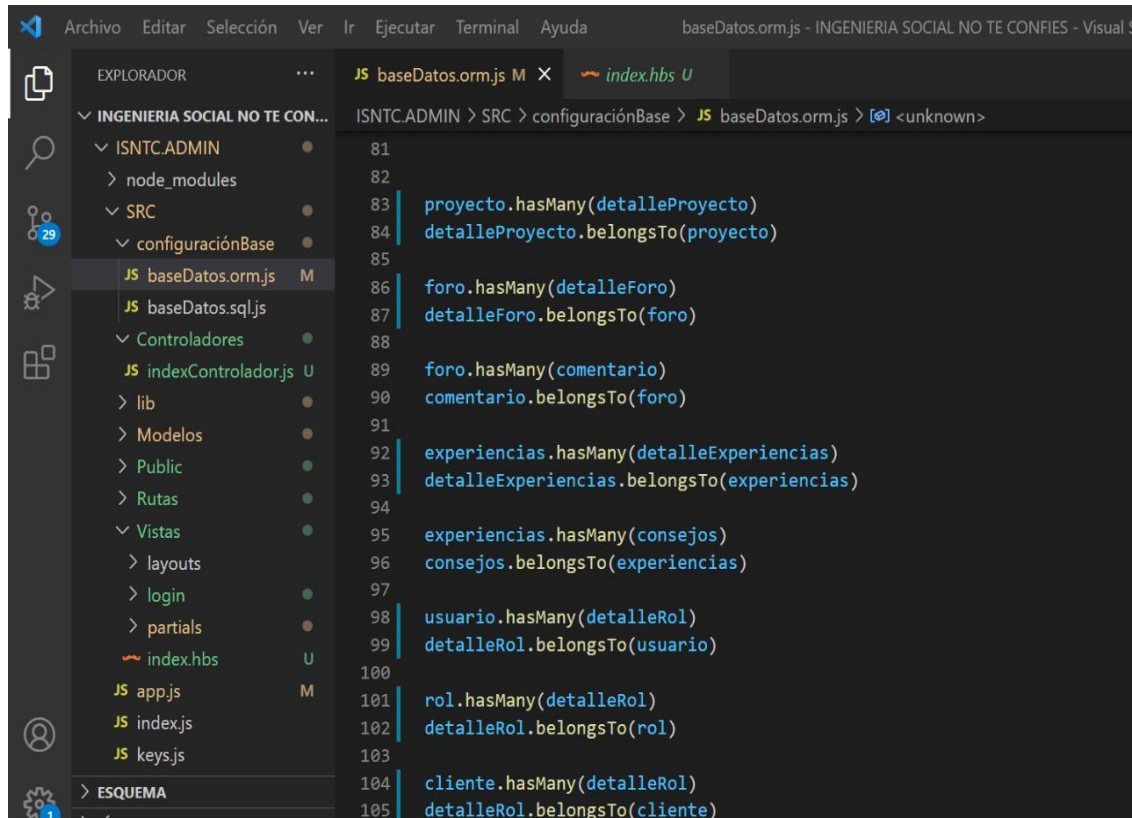
Ninguna

excelente formulario

Una vez aplicada la respectiva encuesta obtuvimos un porcentaje del 74,8% a favor para poder realizar el proyecto y a su la vez brindar ayuda a la comunidad por medio de la página web a desarrollarse.

**Link de la página creada:**  
<https://github.com/CHRISTIANAGUIRRE16/INGENIERIA-SOCIAL-NO-TE-CONFIES.git>





Archivo Editar Selección Ver Ir Ejecutar Terminal Ayuda baseDatos.orm.js - INGENIERIA SOCIAL NO TE CONFIES - Visual Studio Code

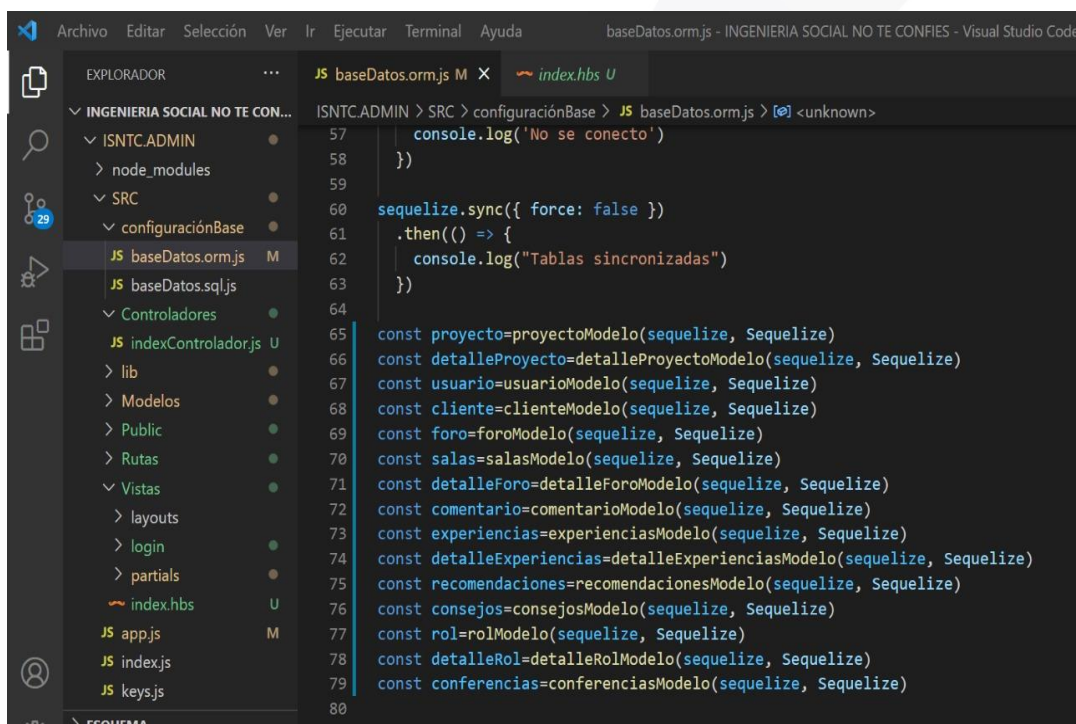
EXPLORADOR

- INGENIERIA SOCIAL NO TE CON...
- ISNTC.ADMIN
  - node\_modules
  - SRC
    - configuraciónBase
      - baseDatos.orm.js M
      - baseDatos.sql.js
      - Controladores
      - indexControlador.js U
      - lib
      - Modelos
      - Public
      - Rutas
      - Vistas
      - layouts
      - login
      - partials
      - index.hbs U
      - app.js M
      - index.js
      - keys.js
- ESQUEMA

ISNTC.ADMIN > SRC > configuraciónBase > JS baseDatos.orm.js > [?] <unknown>

```

81
82
83 proyecto.hasMany(detalleProyecto)
84 detalleProyecto.belongsTo(proyecto)
85
86 foro.hasMany(detalleForo)
87 detalleForo.belongsTo(foros)
88
89 foro.hasMany(comentario)
90 comentario.belongsTo(foros)
91
92 experiencias.hasMany(detalleExperiencias)
93 detalleExperiencias.belongsTo(experiencias)
94
95 experiencias.hasMany(consejos)
96 consejos.belongsTo(experiencias)
97
98 usuario.hasMany(detalleRol)
99 detalleRol.belongsTo(usuario)
100
101 rol.hasMany(detalleRol)
102 detalleRol.belongsTo(rol)
103
104 cliente.hasMany(detalleRol)
105 detalleRol.belongsTo(cliente)
  
```



Archivo Editar Selección Ver Ir Ejecutar Terminal Ayuda baseDatos.orm.js - INGENIERIA SOCIAL NO TE CONFIES - Visual Studio Code

EXPLORADOR

- INGENIERIA SOCIAL NO TE CON...
- ISNTC.ADMIN
  - node\_modules
  - SRC
    - configuraciónBase
      - baseDatos.orm.js M
      - baseDatos.sql.js
      - Controladores
      - indexControlador.js U
      - lib
      - Modelos
      - Public
      - Rutas
      - Vistas
      - layouts
      - login
      - partials
      - index.hbs U
      - app.js M
      - index.js
      - keys.js
  - ESQUEMA


ISNTC.ADMIN > SRC > configuraciónBase > JS baseDatos.orm.js > [?] <unknown>

```

57 console.log('No se conecto')
58 })
59
60 sequelize.sync({ force: false })
61 .then(() => {
62   console.log("Tablas sincronizadas")
63 })
64
65 const proyecto=proyectoModelo(sequelize, Sequelize)
66 const detalleProyecto=detalleProyectoModelo(sequelize, Sequelize)
67 const usuario=usuarioModelo(sequelize, Sequelize)
68 const cliente=clienteModelo(sequelize, Sequelize)
69 const foro=foroModelo(sequelize, Sequelize)
70 const salas=salasModelo(sequelize, Sequelize)
71 const detalleForo=detalleForoModelo(sequelize, Sequelize)
72 const comentario=comentarioModelo(sequelize, Sequelize)
73 const experiencias=experienciasModelo(sequelize, Sequelize)
74 const detalleExperiencias=detalleExperienciasModelo(sequelize, Sequelize)
75 const recomendaciones=recomendacionesModelo(sequelize, Sequelize)
76 const consejos=consejosModelo(sequelize, Sequelize)
77 const rol=rolModelo(sequelize, Sequelize)
78 const detalleRol=detalleRolModelo(sequelize, Sequelize)
79 const conferencias=conferenciasModelo(sequelize, Sequelize)
80
  
```



```
module.exports = {  
  proyecto,  
  detalleProyecto,  
  usuario,  
  cliente,  
  foro,  
  detalleForo,  
  comentario,  
  experiencias,  
  detalleExperiencias,  
  recomendaciones,  
  consejos,  
  rol,  
  detalleRol,  
  conferencias,  
  salas,  
}
```

 **"EL ARTE DE HACKEAR HUMANOS"**


INICIAR SESIÓN

Ingresar usuario

Ingresar contraseña

[INGRESAR](#)

[REGISTRARSE](#)



 **"EL ARTE DE HACKEAR HUMANOS"**

REGISTRO

Ingresar nombres

Ingresar email

Ingresar usuario

Ingresar contraseña

[REGISTRARSE](#)

