REVISTA ODIGOS

Período octubre 2021 - enero 2022
Vol. 2, Núm. 3
rodigos@uisrael.edu.ec
https://doi.org/10.35290/ro.v2n3.2021.493 • e-ISSN: 2697-3405

# Ingeniería social, un ejemplo práctico

*Fecha de recepción: 2021-07-05 • Fecha de aceptación: 2021-09-10 • Fecha de publicación: 2021-10-10*

**Juan Pablo Prado Díaz**
JPSystems, Ecuador
*Info.jpsystems@gmail.com*
*https://orcid.org/0000-0001-8268-4351*

**RESUMEN**

En la actualidad, las empresas han adoptado espacios de almacenamiento digitales, donde recopila uno de sus activos más valiosos, la información, la misma que puede constituir datos como estados financieros, cartera de clientes, datos que representa valor monetario, etc., esta puede ser codiciada por entidades mal intencionadas como puede ser empresas competidoras, ex empleados o también criminales informáticos, los cuales pueden utilizar estos datos como objeto de venta a la competencia, extorsión, manipulación, entre otros crímenes. Los delincuentes informáticos han empezado a robar y filtrar información mediante un conjunto de métodos y técnicas, la cual se denomina ingeniería social, la cual se enfoca en ataques a los empleados de una entidad. Es por esta razón que se ve necesario realizar campañas de concientización a todo el personal de una empresa, puesto que es uno de los vectores de riesgo informático que más ha sido explotado en la historia de la ciberseguridad. En el presente trabajo de investigación se propone una metodología para la generación y ejecución de campañas de ingeniería social, en el mismo se obtendrá como resultado una evaluación de vulnerabilidad a nivel del personal de determinada empresa, y se concluirá un grado de riesgo para la misma.

**PALABRAS CLAVE:** ingeniería social, ataque informático, seguridad informática, social hacking, ciberseguridad.

## ABSTRACT

Nowadays, companies have adopted digital storage spaces, where it collects one of its most valuable assets, the information, the same that can constitute data such as financial statements, customer portfolio, data that represents monetary value, etc., this can be coveted by malicious entities such as competing companies, former employees or also computer criminals, which can use this data as an object of sale to competitors, extortion, manipulation, among other crimes. Computer criminals have begun to steal and leak information through a set of methods and techniques, which is called social engineering, which focuses on attacks on employees of an entity. It is for this reason that it is necessary to carry out awareness campaigns to all the staff of a company, since it is one of the most exploited computer risk vectors in the history of cybersecurity. This research work proposes a methodology for the generation and execution of social engineering campaigns, which will result in a vulnerability assessment at the level of the personnel of a given company, and will conclude a degree of risk for it.


**KEYWORDS**: social engineering, social hacking, cyber attack, cybersecurity, computer security.

# Introducción

En las últimas décadas, dentro de las empresas y corporaciones (Navarrete, 2020), sean estas grandes o pequeñas, ha empezado a considerarse la información como el activo más estratégico de mayor valor. Si esta información es filtrada a individuos ajenos, a la empresa o que no estén autorizadas, y peor aún, que puedan llegar a realizar acciones delictivas con la anterior mencionada, se considera que estos datos confidenciales han sido expuestos, poniendo así en una posición vulnerable a la empresa como tal.

La seguridad informática, dentro de una empresa (Paredes et al., 2020), siempre busca las posibles vulnerabilidad y vectores de riesgo digitales que esta pudiera tener con el objetivo de evitar ataques y proteger el activo más valioso que es la información. La triada de la información se conforma en confidencialidad, integridad y disponibilidad (Casas, 2015).

El blog especializado en Sistemas de Gestión de Seguridad de la Información (2020), define estos pilares de la seguridad de la información como:

- **Confidencialidad:** el término tiene como finalidad el filtrado de información confidencial o de alto riesgo de una empresa sea esta por medio del mal uso o funcionalidad de sistemas informáticos o a su vez por medio de sus usuarios. La confidencialidad hace referencia a la necesidad de ocultar o mantener secreto sobre determinada información o recursos.
- **Integridad:** este punto tiene el objetivo evadir las modificaciones no autorizadas de la información sea por usuarios dentro y fuera de la empresa. Esta sólo se podrá modificar mediante autorización.
- **Disponibilidad:** finalmente, la información empresarial siempre debe estar dispuesta a sus usuarios autorizados cuando sea necesaria y respetando las condiciones de acceso de sistema.

El ser humano puede ser escéptico, suspicaz, inclusive llegar a ser nihilista, ante una persona desconocida o hecho del mismo proceder; sin embargo, esta desconfianza puede degradarse en el momento que el desconocido empiece a enfocarse o pretender tener las mismas relaciones intrapersonales como sentimientos, orientaciones, gusto, etc.

En una sociedad “bien vista”, comúnmente el ser humano tiende a entregar algo a cambio después de haber recibido otra cosa inicialmente, a manera de reciprocidad, dependiendo el caso y el escenario.

Como en toda entidad o empresa, siempre rige un organigrama institucional o escalafón en donde se especifica la clasificación entre empleados y directivos de una organización. La autoridad de un superior tiene el poder de designar tareas a sus empleados, desde las más sencillas de cumplir, hasta las más delicadas o laboriosas, desde las más acertadas a la función de cada colaborador, hasta las más raras.

La reacción del ser humano puede ser controlada si se la hace de manera acertada, una de las formas más seguras puede ser la urgencia y la presión a esta. Si un colaborador de una determinada empresa pide una tarea extraña o sospechosa a un compañero de trabajo, es muy probable que este no lo acepte o lo cuestione por tal requerimiento.

## Metodología

Dentro de la investigación se ha aplicado el método científico "deductivo", puesto que se iniciará de los principios de las técnicas de ingeniería social (confianza, compensación, poder, firmeza, celeridad y presión), para aplicarlos en a resoluciones de ataques informáticos.

La presente investigación se realizó con un caso de estudio, la empresa "OmniData" (nombre protegido) creada el 15 de diciembre del año 2000, se dedica a la compra y venta de equipos informáticos y de telecomunicaciones.

OmniData hace algunos años ha sido detectado por varios criminales informáticos, así mismo, ha sido objeto de varios ataques informáticos tales como *Phishing* (Jagatic et al., 2007)*, Vishing* (Jones et al., 2020), SPAM, intento de SCAM, ataques DDoS, etc.

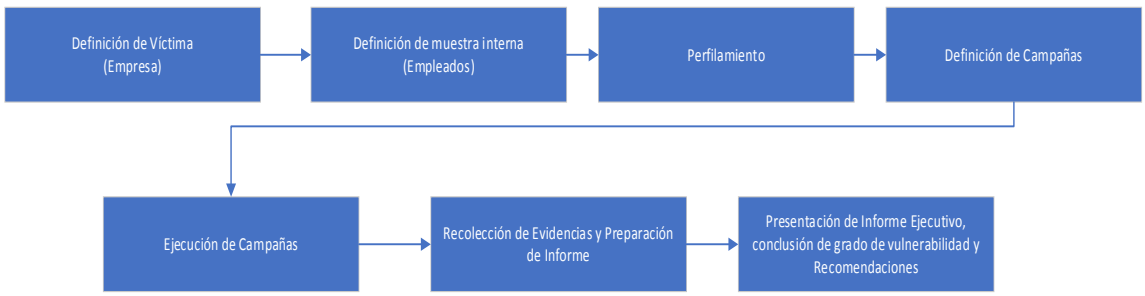
De esta manera, la gerencia general desea detectar todos los vectores de riesgo informático, principalmente en función al *social hackin*g que pueda tener la empresa y sus empleados, posteriormente se capacitará al personal necesario para evitar en un futuro más ataques de ingeniería social.

Dentro de la muestra se incluirá a todos los empleados de OmniData, clasificados por cada área, los mismos que serán: comercial, logística, tecnología, administrativo, gerencias y sub gerencias.

En relación a los marcos referenciales propuestos anteriormente, se define la siguiente metodología que se evidencia en la *Figura 1*.

**Figura 1**

*Metodología propuesta para el trabajo de investigación*



Como primer paso se procede con la definición de la víctima (selección de la empresa). Dentro del proceso de selección de la empresa objetivo a atacarla, se debe tomar en cuenta una previa recolección de información y análisis de la misma, de su giro de negocio, empleados, directivos, etc.

Una vez que el atacante ha identificado, la empresa o entidad, donde quiere filtrar tanta información como requiera, deberá escoger a su víctima o grupo de objetivos para el ataque, sean por roles administrativos o cargos altos en el personal.

En relación al reconocimiento y recolección de información (*footprinting*) la base de todo ataque de ingeniería social (INCIBE, 2019) va de la mano del previo reconocimiento de la víctima, sea una persona, institución, empresa, etc.

Una vez realizado el proceso de perfilamiento del grupo de víctimas será más sencillo planificar los tipos de ataques que se van a realizar, a qué usuarios se los va a realizar, y el periodo de tiempo que se los va a evaluar y su persistencia.

Para la preparación del laboratorio de *hacking*, el atacante deberá proveerse de todas las herramientas necesarias para montar las campañas y poder lanzarlas, entre estas tendremos inicialmente la preparación y planificación de campañas de ataque para filtrado de información empresarial, Identificando y perfilando la o las victimas que serán objeto sea de análisis o explotación dentro de la empresa será adecuado planear los tipos de ataques a ser evaluados sobre ellos.

Cuando una empresa empieza a tener cierta cartera de clientes y así mismo pertenece a varias carteras de proveedores, es normal que sus empleados o usuarios empiecen a recibir correos de publicidad, ofertas, catálogos, promociones, liquidaciones, etc que pueden denominarse como spam.

A su vez, el *email spoofing* es la falsificación tanto de la dirección de correo electrónico, como de su dominio dentro del mismo.

Adicional al intento de manipulación del ser humano, para entregue información confidencial de la empresa, se propone técnicas (Cordero, 2018) de engaño para el filtrado de credenciales y evaluar el acceso a sistemas y redes de comunicaciones.

Las técnicas del engaño dentro de la ingeniería social (Lisa Institute, 2020) son consideradas muchas veces como un arte, donde si bien no existe un parámetro exacto o científico del ataque más indicado o adecuado para determinada víctima, dentro de escenarios corporativos y su respectiva infraestructura el ingeniero social se encontrarán aplicaciones y sistemas web los cuales podrían clonarse.

Para un ataque de simulación por infección de “Rubber Ducky”, el atacante debe engañar o convencer a la víctima de tal manera que esta conecte el medio electrónico por voluntad propia a su computador y este pueda hacer su trabajo con los *scripts* o acciones antes mencionadas.

- Soltar la unidad de almacenamiento en el suelo de la empresa.
- Puede ser muy útil persuadir a las víctimas con el hecho de brindar un regalo y que este contenga la memoria USB infectada.

El objetivo del ataque es que el ingeniero social pueda entrar físicamente a la empresa mediante algún motivo falso, usualmente se lo hace en nombre de una entidad tercera, al hacerlo este deberá emplear todas las técnicas (welivesecurity, 2014) necesarias para robar información confidencial.

Si bien es cierto que la planificación, organización y ejecución de un cronograma o de la manera de lanzar los ataques estarán en criterio del ingeniero social, se recomienda la siguiente plantilla que se muestra en la *Figura 2*.

**Figura 2**

*Plantilla de cronograma para campañas de IS*

| PLANTILLA PLAN DE CAMPAÑAS PARA ATAQUES DE ING. SOCIAL - EMPRESA X | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Semanas | Semana 1 | | | | | Semana 2 | | | | | Semana 3 | | | | | Semana 4 | | | | |
| Victimas / Días | Día 1 | Día 2 | Día 3 | Día 4 | Día 5 | Día 6 | Día 7 | Día 8 | Día 9 | Día 10 | Día 11 | Día 12 | Día 13 | Día 14 | Día 15 | Día 16 | Día 17 | Día 18 | Día 19 | Día 20 |
| Recepción | | | | | | | | | | | | | | | | | | | | |
| Empleado 1R | | | | | | | | | | | | | | | | | | X | | |
| Contabilidad | | | | | | | | | | | | | | | | | | | | |
| Empleado 1C | | | | | | | | X | | | | X | | | | | | | | |
| Empleado 2C | | | | | | | | | X | | | X | | | | | | | | |
| Empleado 3C | | | | | | X | | | | | | X | | | | | | | | |
| Tecnología | | | | | | | | | | | | | | | | | | | | |
| Empleado 1T | | X | | | | | | | | | | | | | | | | | | |
| Empleado 2T | | | | | X | | | | | | | | | | | | | | | |
| Seguridad | | | | | | | | | | | | | | | | | | | | |
| Empleado 1S | | | | | | | | | | | | X | | | | | | | | |
| Logística | | | | | | | | | | | | | | | | | | | | |
| Empleado 1L | | | X | | | | | | | | | | | | | | | | | |
| Cuentas Comerciales | | | | | | | | | | | | | | | | | | | | |
| Empleado 1C | | | | | | | | | | | | | | X | | | | | | |
| Corporativo | | | | | | | | | | | | | | | | | | | | |
| Empleado 1CC | | | | | | | | | | | | | | | | | | | | |
| Gerencia | | | | | | | | | | | | | | | | | | | | |
| Empleado 1G | | | | X | | | | | | | | | X | | | | | | | |
| Sub Gerencias | | | | | | | | | | | | | | | | | | | | |
| Empleado 1SG | | | | | | | X | | | | | | | | | | | | | |
| Limpieza | | | | | | | | | | | | | | | | | | | | |
| Empleado 1LZ | | | | | X | | | | | | | | | | | | | | | |
| Vectores de Ataque | Email Spoofing + Phishing Web | | | | | Smishing + Phishing Web | | | | | Rubber Ducky | | | | | Intrusión Física + Rubber Ducky | | | | |

En la parte de la ejecución, el atacante finalmente lanza las campañas ya realizadas y planificadas en contra de la víctima o grupo de individuos objetivos.

Toda la información documentada y recopilada resultado de los ataques informáticos serán reunidos, clasificados y analizados con el objetivo de identificar vulnerabilidades y vectores de ataque a la empresa

Una vez generado el informe, es responsabilidad del ingeniero social presentar a los directivos todo el proceso tomado en cada una de las fases analizadas en el presente trabajo de

investigación, de manera fácil y sencilla para el entendimiento de las personas ajenas al campo informático y de ciberseguridad (Alonso, 2020).

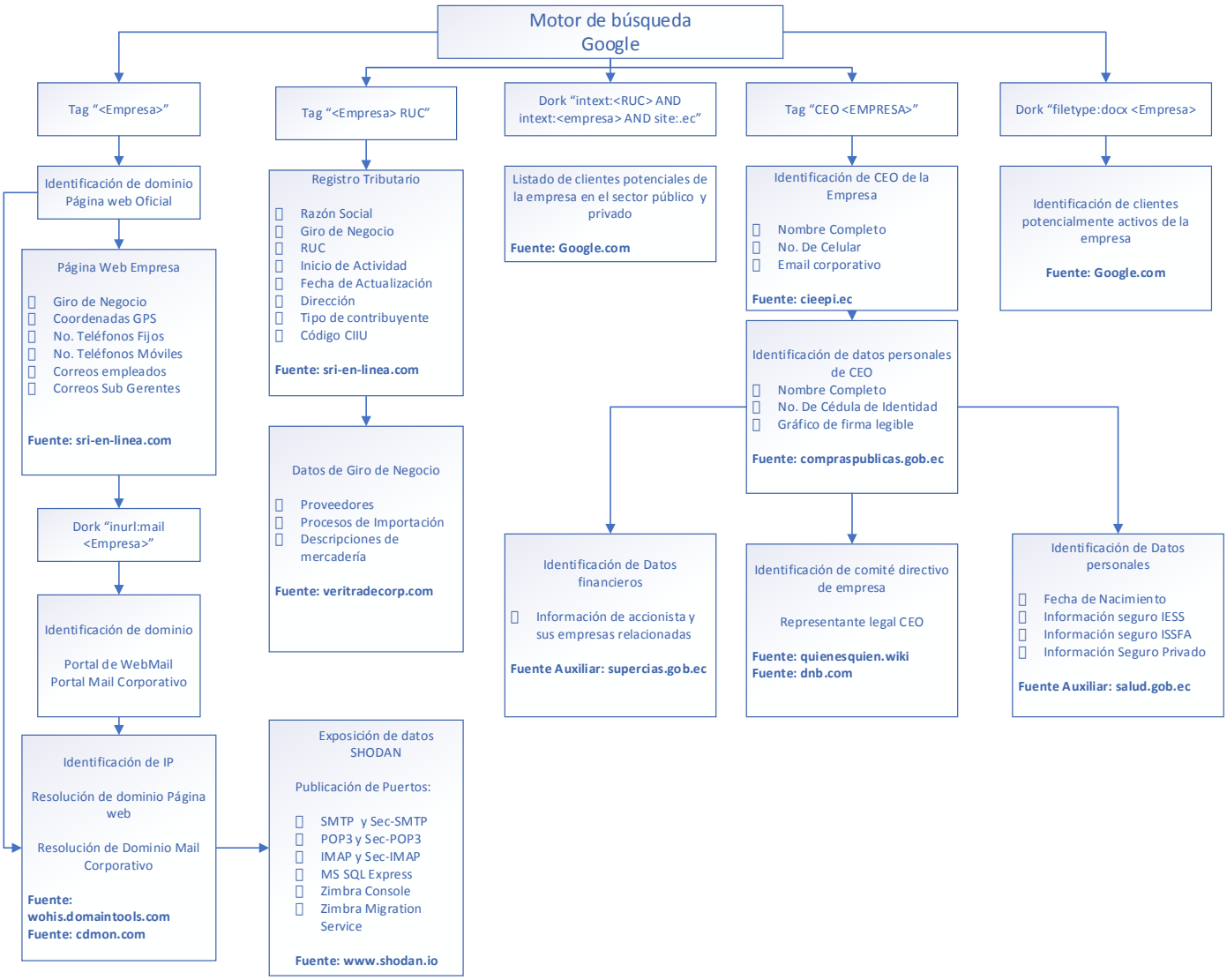
Los resultados anteriormente presentados también formarán parte de un informe ejecutivo, el cual será reflejado a la gerencia de la empresa, en el mismo que concluye el grado de vulnerabilidad informática que puede tener la empresa.

Una vez realizada la conclusión en base a los resultados, la metodología recomendará un proceso de definición de mitigaciones, así como un plan de continuidad del negocio.

Par el presente caso se ha utilizado el siguiente flujo de proceso de adquisición de información, en conjunto la técnica ya conocida como "*Google Hacking*".

**Figura 3**

*Diagrama de flujo de trabajo de Google Hacking*



En la *Figura 3* se muestran todos los laboratorios realizados para localización de información empresarial, adicional, se identifica servidor de correos de la empresa (*Figura 4*):

Dork: inurl:mail <empresa>.com.ec URL: mail.<empresa>.com.ec

**Figura 4**

*Sitio de cliente web de correo electrónico de OmniData*


# Resultados

Para la preparación de las campañas de ataque, dentro del caso práctico se definen los siguientes escenarios.

Para lo cual se debe tomar en cuenta las siguientes herramientas:

- Sistema Operativo Kali Linux
- Máquina Virtual implementado en nube de Google Cloud

El objetivo será clonar el portal web (*Figura 5*) de ingreso al sistema de correo electrónico de OmniData, posteriormente clonar la página web y modificar su código fuente, tal que los campos de inicio de sesión sean intervenidos y al pulsar cualquier botón de “Ingresar”, capture la información ingresada en los cuadros de texto, está será almacenada en un archivo de texto plano que podrá ser visualizado después por el ingeniero social.

**Figura 5**

*Comparativa entre portal de correo electrónico original vs. clonada*

| Página Original | Página Clonada |
|---|---|
|  |  |



**Figura 6**

*Código PHP para capturar información de la página clonada*

```php
<?php

    $username = $_POST["username"];
    $password = $_POST["password"];

    $contenido="
                Usuario: $username
                Password: $password ";

    $archivo = fopen("$username.txt","w");
    fwrite($archivo,$contenido);

    header("Location: https://mail.[redacted].com.[redacted]");
?>
```

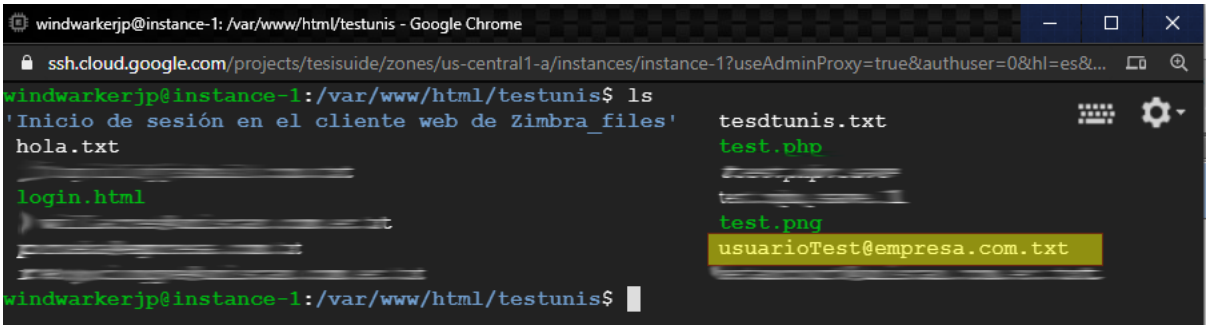
Como se puede apreciar en la *Figura 6*, el código es simple y no lleva más que unas cuantas líneas, solamente captura la información del campo "*username*" y "*password*" (*Figura 7*), a continuación, lo registra en un archivo de texto plano con el mismo nombre de usuario (*Figura 8*). Para completar el engaño, después de la acción del botón de inicio de sesión al presionar, el usuario será re direccionado a la página original del portal de correo.

**Figura 7**

*Prueba de ingreso de datos en portal de correo clonad*


**Figura 8**

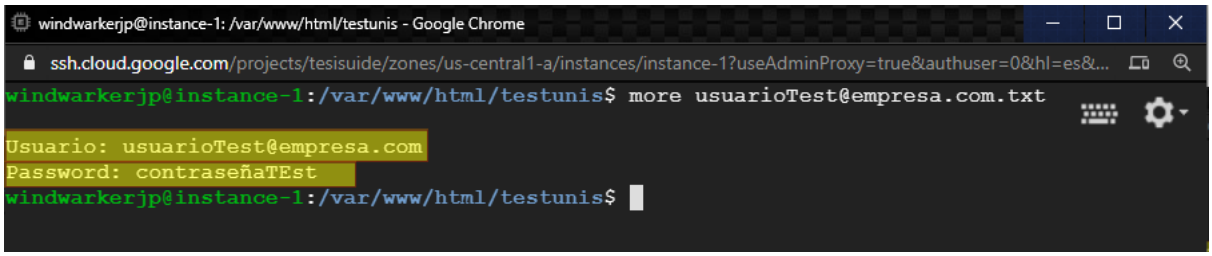
*Archivo generado por página web clonada*




Dentro del archivo de texto plano se encuentra la siguiente información que se muestra en la *Figura 9*:

**Figura 9**

*Contenido de archivo generado por página web clonada*



El sitio web será implementado y lanzado en la máquina virtual de *Google Cloud*, como se evidencia en las siguiente *Figuras 10* y *11*.

**Figura 10**

*Prueba de página web clonada publicada en Internet*

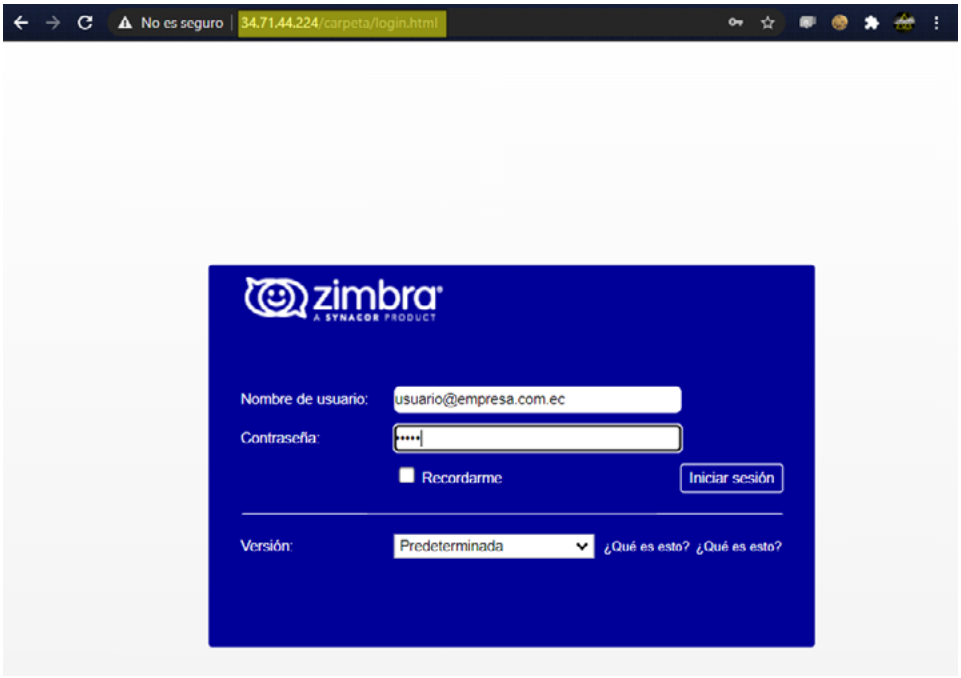
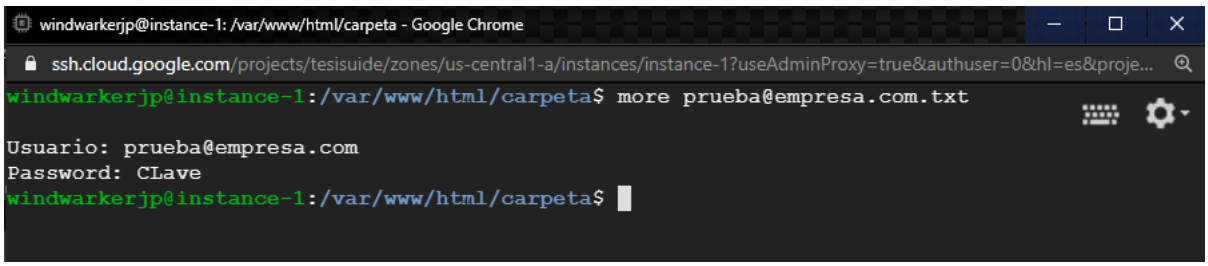



**Figura 11**

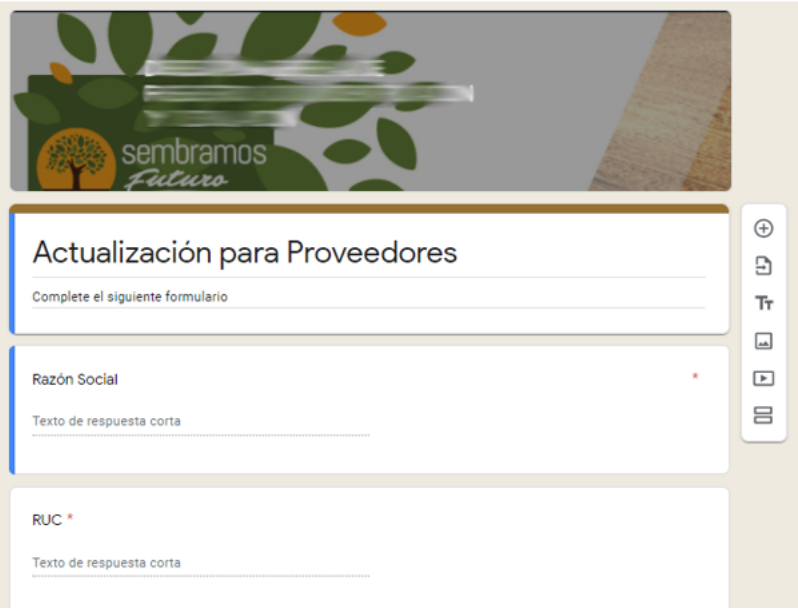
*Archivo generado por la página web de prueba*




Muchas empresas o entidades solicitan información de tendencias de compra y preferencias de productos a través de formularios, como puede ser Google Forms, Survey Monkey, entre otros; sin embargo, no se considera adecuado o formal que una institución pública lo haga, por este motivo, se define lanzar una petición de información empresarial por medio de un formulario no oficial, en este caso será Google Forms, y la entidad remitente será una entidad pública del Ecuador, como se puede observar en la *Figura 12*.

**Figura 12**

*Página de Google Forms para captura de datos de proveedores*




### 3.1 Implementación de plataforma de GoPhish

Para el proceso de clonación se utilizará un servidor de correo electrónico Zimbra, el cual será objeto de cambios de remitente. GoPhish (s.f) es una plataforma para la creación, planificación y ejecución de ataques de ingeniería social en base de ataques de *phishing*. Para el caso práctico se implementan plantillas de correo para los siguientes escenarios:

- Inicio de sesión en portal web del cliente de correo electrónico para validar mejores del sistema del mismo. En el link del portal web de cliente de correo se enmascara el enlace original del sitio clonado preparado anteriormente.
- Actualización de datos corporativos de la empresa para la entidad del Registro Civil del Ecuador con el objetivo de calificarse como proveedores.

Para el presente caso práctico se utilizará el módulo de creación de Usuarios y Grupos de GoPhish para generar grupos de víctimas por departamento corporativo.

### 3.2 Preparación para ataque mediante Rubber Ducky

Se implementó un ataque de captura de información mediante una simulación de Rubber Ducky (Cannoles, 2017). Para este tipo de ataque se tendrá como objetivo robar información del computador de la víctima, en este caso uno de los empleados de OmniData, mediante un virus de autoría propia en lenguaje C# (*Figura 13*).

**Figura 13**

*Método constructor de la clase*

```
public Form1()
{
    InitializeComponent();
    this.FormBorderStyle = System.Windows.Forms.FormBorderStyle.None;
    this.ShowInTaskbar = false;
    this.Load += new EventHandler(Form1_Load);

}
```

Una vez compilado y generado el ejecutable de la aplicación se procede a probarla en la misma computadora (*Figura 14 y Figura 15*).

**Figura 14**

*Pruebas del aplicativo Rubber Ducky*

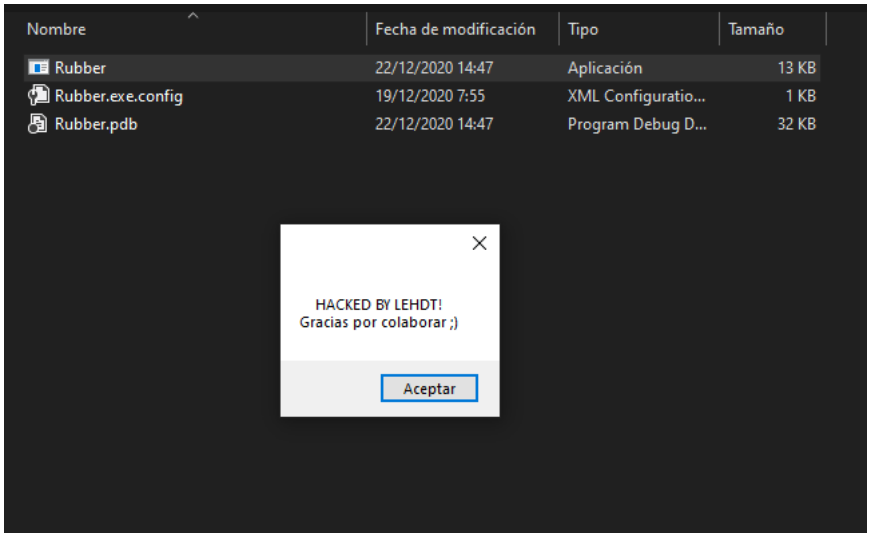
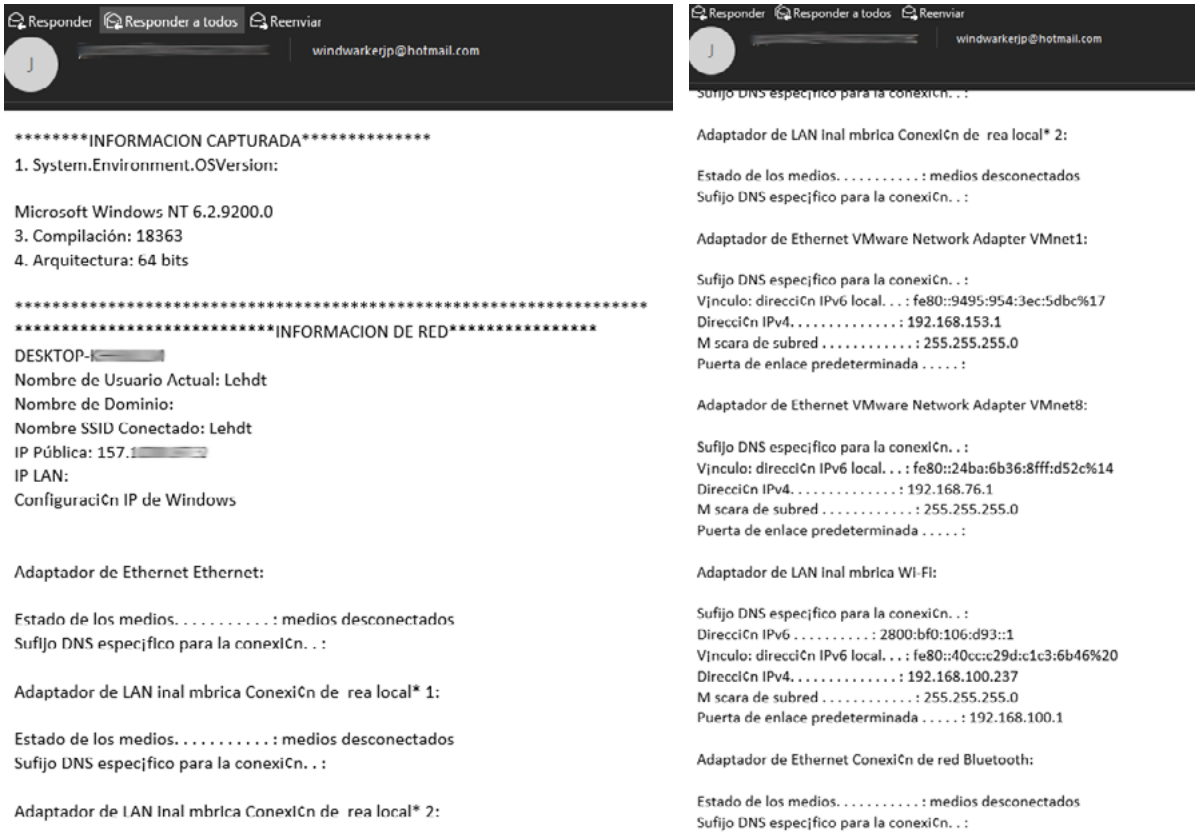


**Figura 15**

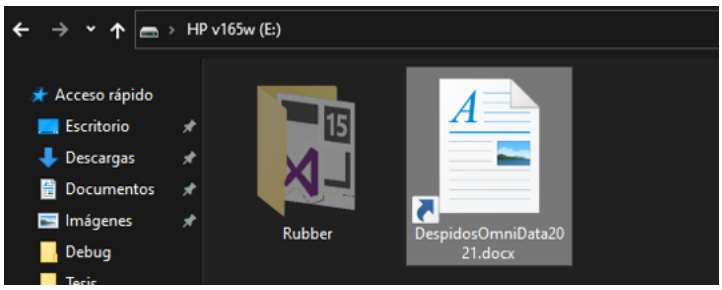
*Resultado de pruebas de aplicación Ruber Ducky*




Para el caso práctico se ha optado por disfrazar el archivo por documentos, sean estos de textos o multimedia con el objetivo de engañar al la víctima y mediante algún pretexto ella misma ejecute el archivo con el código malicioso. Uno de tantos ejemplos que podemos implementar podría ser como el que se ve en la *Figura 16*.

**Figura 16**

*Aplicativo Rubber Ducky ejecutable y enmascarado*



### 3.3 Preparación para ataque de Vishing

Para el caso práctico se tendrá el escenario donde un agente de cuentas de seguro social llamará a la empresa a pedir información de correos electrónicos y convencer a una de las víctimas de llenar un formulario, donde se capturará cierta información de la empresa. Para lo cual se necesitará preparar la información que se observa en las *Figura 17*, *18 y 19*.

**Figura 17**

*Plantilla de remitente falso para ataque Vishing*

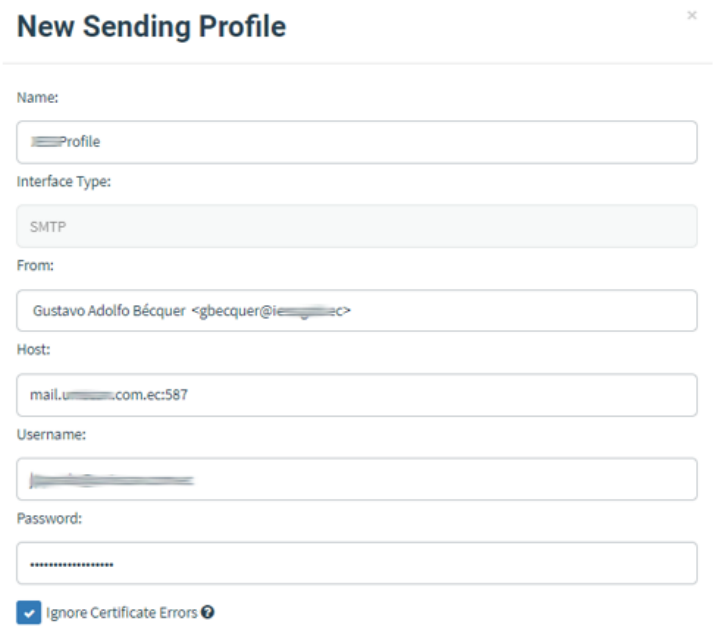


**Figura 18**

*Plantilla de remitente falso para ataque Vishing*

Estimado Usuario Afiliado / Empleador del [redacted].

Con el objetivo de mantener los datos de nuestros usuarios y empleadores afiliados el Instituto Ecuatoriano [redacted] invita a Ud. a llenar el siguiente formulario de datos básicos empresarial.

URL: Enlace a Formulario

Agradeciendo su valioso tiempo, me subscribo.

Atte.

---

Gustavo Adolfo Becquer.
Ejecutivo de Cuentas
[redacted]
Dirección: Av. 10 de Agosto y bogota esquina.
Teléfono: (02) 234-5678
Celular: (09)-967-6543

**Figura 19**

*Formulario de Google para captura de datos en ataque Vishing*


## 3.4 Preparación para el escenario de ataque de intrusión física + infección por USB

**(Ruber Ducky)**

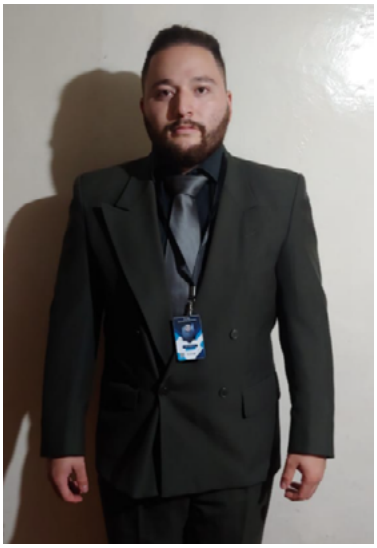
Se trata de que el ingeniero social o una persona contratada por él, visité a la empresa de manera física, se anuncie y pueda ingresar con algún pretexto o situación falsa. Tomando en cuenta los procesos operativos de la empresa, todo cliente nuevo debe calificarse como tal, entregando ciertos documentos, y es por esta razón que el intruso intentará ingresar a las instalaciones de OmniData. Si el ambiente se torna adecuado, el intruso entrará en el tema de calificación de cliente corporativo, probablemente tendrá que llenar un formulario, así como entregar documentación, es aquí donde el atacante pide de favor ejecutar y/o imprimir un documento que tiene almacenado en un dispositivo USB, el cual tendrá un documento de texto *.docx, el cual “contiene” toda la documentación necesaria para la calificación.

Este archivo está disfrazado con la aplicación desarrollada para el ataque de infección por USB. El infiltrado pedirá de favor que la víctima ejecute el documento falso, si tiene éxito, él rápidamente pretenderá atender una llamada de urgencia y escapará por sus propios métodos de las instalaciones de OmniData. Si todo el proceso tiene éxito, la información de esa computadora será capturada y enviada al correo electrónico del ingeniero social. Para el efecto se considera que el intruso deberá tener ciertas características:

- Se definirá una empresa falsa para el infiltrado. Para el efecto, se ha buscado empresas por medio del servicio electrónico de rentas internas, se ha escogido la empresa con la razón social y actividad económica más adecuada para el caso. Se decide hacerlo de esta manera, pues si OmniData requiere evaluar una identificación de empresa (RUC), como proceso de calificación de cliente, podrá hacerlo sin problemas.
- Deberá presentarse con ropa formal, como se muestra en la *Figura 20*.

**Figura 20**

*Sujeto utilizado para ataque de intrusión física*



Deberá portar su credencial y gafete corporativo, para lo cual se ha diseñado e impreso una identificación falsa por medio de una impresora Zebra de credenciales (*Figura 21*).

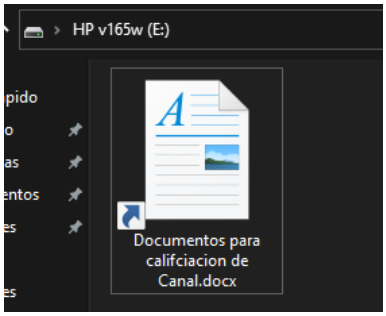
**Figura 21**

*Proceso de manufactura de credenciales falsas para infiltrado*

- Finalmente, se debe prepara la memoria USB infectada con el siguiente archivo enmascarado, esta memoria debe portar el infiltrado, entregar a la víctima y convencerla de ejecutar el archivo a continuación (*Figura 22*).

**Figura 22**

*Aplicativo Rubber Ducky enmascarado para ataque de Intrusión Física*




### 3.5 Definición de cronograma de lanzamiento de campañas

Cada semana se ha dividido de la siguiente manera:

- **Semana 1:** ataque email *spoofing* y *Phishing* web
- **Semana 2:** ataque email *spoofing* + *Vishing* + *Phishing* por google forms

- **Semana 3:** ataque por infección de memoria USB (Simulación de Rubber Ducky)
- **Semana 4:** intrusión física + infección por USB

En la siguiente *Figura 23* se evidencia de mejor manera:

**Figura 23**

*Cronograma de lanzamiento de Campañas de Ataques de Ing. Social para OmniData*

| CRONOGRAMA PARA LANZAMIENTO DE CAMPAÑAS DE ATAQUES DE ING. SOCIAL PARA OMNIDATA | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Semanas** | **Semana 1** | | | | | **Semana 2** | | | | | **Semana 3** | | | | | **Semana 4** | | | | |
| **Victimas / Días** | **Día 1** | **Día 2** | **Día 3** | **Día 4** | **Día 5** | **Día 6** | **Día 7** | **Día 8** | **Día 9** | **Día 10** | **Día 11** | **Día 12** | **Día 13** | **Día 14** | **Día 15** | **Día 16** | **Día 17** | **Día 18** | **Día 19** | **Día 20** |
| **Comercial** | | | | | | | | | | | | | | | | | | | | |
| Vendedor 1 | X | | | | | | | | | | | X | | | | | | | | X |
| Vendedor 2 | X | | | | | | | | | | | X | | | | | | | | X |
| Vendedor 3 | X | | | | | | | | | | | | X | | | | | | | |
| **Administración** | | | | | | | | | | | | | | | | | | | | |
| Administrativo 1 | | X | | | | | | | | | | X | | | | | | | | |
| Administrativo 2 | | X | | | | | | | | | | X | | | | | | | | |
| Administrativo 3 | | X | | | | | | | | | | X | | | | | | | | |
| **Tecnología** | | | | | | | | | | | | | | | | | | | | |
| Técnico 1 | | | X | | | | | | | | | X | | | | | X | | | |
| Técnico 2 | | | X | | | | | | | | | X | | | | | X | | | |
| Técnico 3 | | | X | | | | | | | | | X | | | | | X | | | |
| Técnico 4 | | | X | | | | | | | | | X | | | | | X | | | |
| **Recepción** | | | | | | | | | | | | | | | | | | | | |
| Recepcionista 1 | | | | X | | | | | | X | | X | | | | | | | | |
| Recepcionista 2 | | | | X | | | | | | X | | X | | | | | | | | |
| **Gerentes** | | | | | | | | | | | | | | | | | | | | |
| Gerente General | | | | | X | | | | | | | X | | | | | | | | |
| Sub Gerente 1 | | | | | X | | X | | | | | X | | | | | | | | |
| Sub Gerente 2 | | | | | X | | | | | | | X | | | | | | | | |
| Sub Gerente 3 | | | | | X | | | | | | | X | | | | | | | | |
| **Vectores de Ataque** | Email Spoofing + Phishing Web | | | | | Email Spoofing + Vishing + Phishing Google Forms | | | | | Ataque de Infección USB (Rubber Ducky) | | | | | Intrusión Física + Rubber Ducky / Intrusión Wifi por Evil Twin | | | | |

### Lanzamiento de ataque email *Spoofing* + *Phishing* web (Semana 1)

El objetivo de esta campaña es enviar a todas las víctimas de la empresa en el periodo de 1 semana un correo electrónico por parte del departamento de IT (*email Spoofing*), para la validación de sus credenciales en el sistema cliente de correo electrónico corporativo (*web Phishing*). Para lo cual se planificará en los siguientes grupos de usuarios.

- **Departamento comercial:** Día 1
- **Departamento administrativo:** Día 2
- **Departamento de IT:** Día 3
- **Recepción:** Día 4
- **Gerente y sub gerentes:** Día 5.

### Lanzamiento de ataque + *Vishing* + *Phishing Google Forms* (Semana 2)

En este ataque se define contratar una persona tercera por parte del ingeniero social se hará pasar por una institución pública, este realizará una llamada telefónica a la empresa (*Vishing*), el atacante tratará de ganarse la confianza de la víctima, con el fin de obtener su correo electrónico corporativo para enviar un formulario proveniente de la misma institución pública (*email spoofing*), acto seguido el operador falso debe conseguir que el usuario afectado llene un formulario falso con ciertos datos corporativos (*Phishing mediante Google Forms).*

### Ataque de intrusión mediante simulación de USB infectado (Rubber Ducky) (Semana 3)

El objetivo en el presente ataque será de convencer o engañar a la víctima de conectar un dispositivo de almacenamiento USB infectado con la aplicación desarrollada (*Figura 24*) y disfrazada de documento de texto, temas ya explicados en el apartado de planificación de campañas.

**Figura 24**

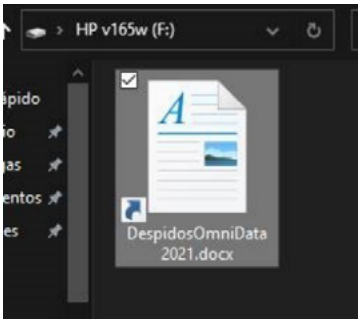
*Memorias USB HP de 8GB*


### Escenario 1 – Dispositivo USB abandonado – Día 12

Se colocan los dispositivos USB abandonados en varios lugares de las instalaciones de la empresa y se espera a los resultados. Adicional, se disfraza el archivo infectado de la siguiente manera como se ve en la *Figura 25*.

**Figura 25**

*Aplicativo Rubber Ducky enmascarado para ataque de Infección USB*



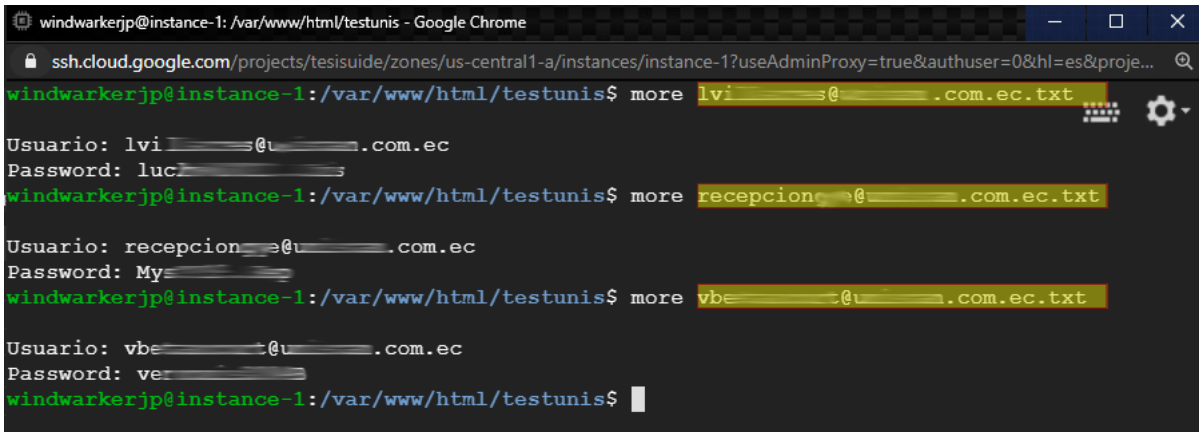

Una vez abandonado los dispositivos, el ingeniero social queda a la espera, si al correo llega la información de la víctima (tal como se desarrolló el aplicativo), la campaña será exitosa.

### 3.6 Resultados del ataque de email *Spoofing* + *Phishing* web

Tal como se puede ver en la *Figura 26*, el portal web logra capturar 3 cuentas de usuarios los mismos que se almacenan en sus archivos *.txt.

**Figura 26**

*Contenido de los archivos con la información capturada*




Considerando las evidencias antes previstas, se concluye que el ataque de Email *Spoofing* web + *Phishing* web fue un éxito, afectando los siguientes departamentos

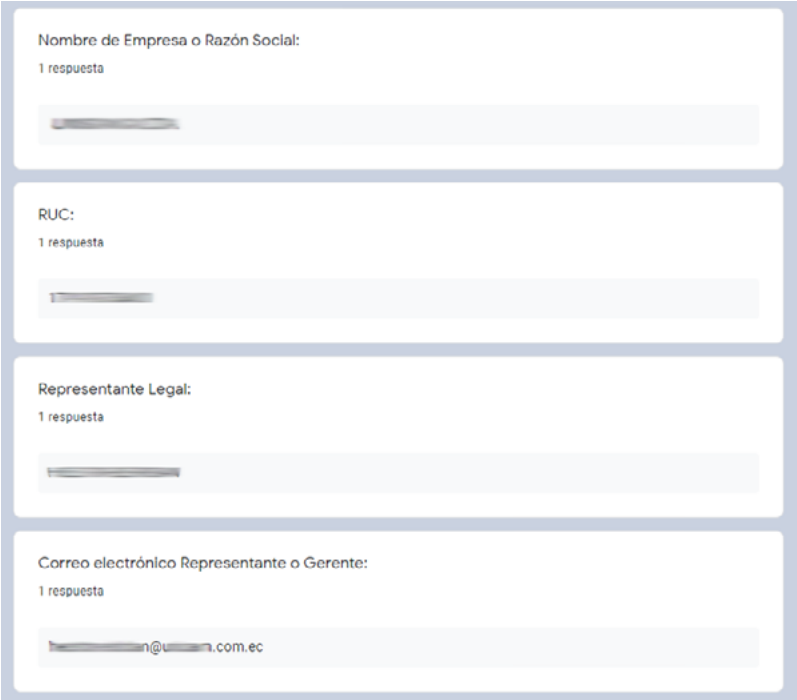
- **Departamento de TI**: 1 víctima
- **Gerente Administrativo:** 1 Victima
- **Recepción** 1 Victima

### 3.7 Resultados del ataque de Email Spoofing + Vishing + Google Forms

Una vez finalizazada la llamada telefónica, el ingeniero social reporta que el ataque fue exitoso y el resultado se visualiza en el formulario de Google, como se ve en la *Figura 27*.

**Figura 27**

*Resultado del ataque de Vishing*



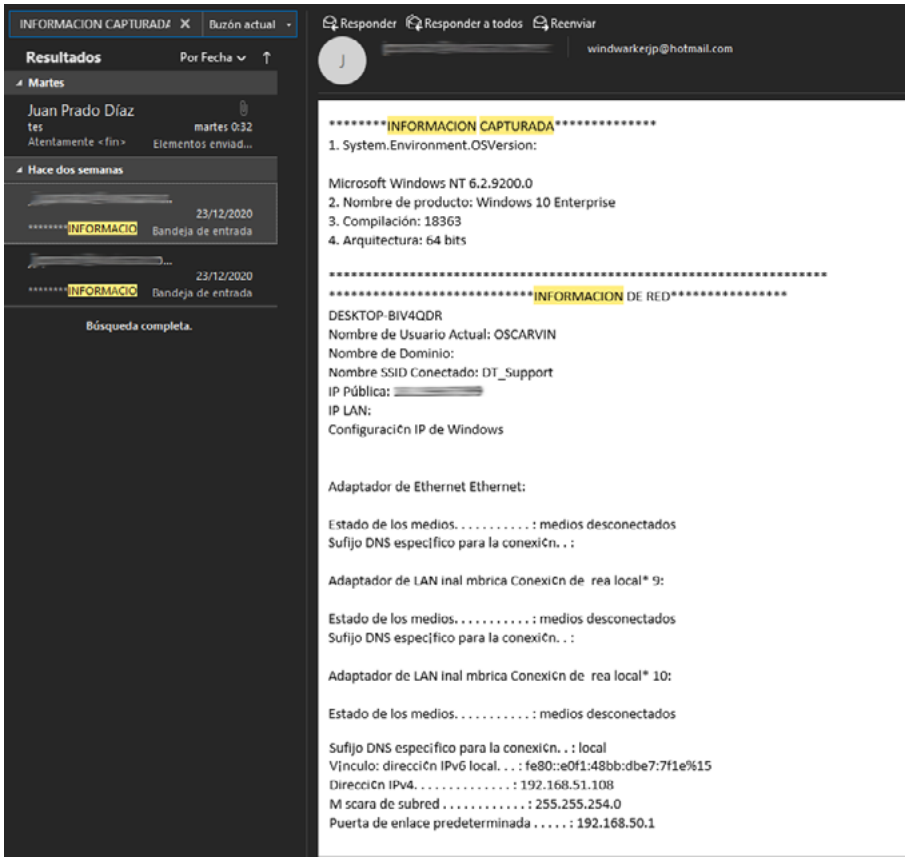

En consecuencia, se concluye que el ataque tuvo éxito, afectando a los siguientes usuarios: recepción (1 víctima).

### 3.8 Resultados del ataque de infección por USB (Rubber Ducky)

En el presente apartado se reunén los resultados pertencientes a la semana 3. Considerando la función del aplicativo creado, el cual debe enviar la información de sus víctimas al correo electrónico del ingeniero social, se evidencia el siguientes resultados que se observan en la *Figura 28*.

**Figura 28**

*Correos electrónicos resultantes del ataque por infección de USB*




Por consiguiente, se concluye que el ataque de infección por UBS (Rubber Ducky), tuvo éxito, afectando a los siguientes usuarios:

- **Departamento de técnología:** 1 víctima
- **Departamento de ventas:** 1 víctima

### 3.9 Resultados del ataque de intrusión física + infección por USB (Rubber Ducky)

La víctima al insertar la memoria en su computador y ejecuta el archivo dentro de él, se inicia el proceso de captura y enviado de información personal del dispositivo del usuario afectado: Comercial (1 victima).

**Figura 29**

*Correo electrónico resultante del ataque de intrusión física*


**Figura 30**

*Cronograma de lanzamiento de Campañas de Ataques de Ing. Social para OmniData*

| RESULTADO DE CAMPAÑAS EJECUTADAS DE ING. SOCIAL PARA OMNIDATA | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Semanas** | **Semana 1** | | | | | **Semana 2** | | | | | **Semana 3** | | | | | **Semana 4** | | | | |
| **Víctimas / Días** | **Día 1** | **Día 2** | **Día 3** | **Día 4** | **Día 5** | **Día 6** | **Día 7** | **Día 8** | **Día 9** | **Día 10** | **Día 11** | **Día 12** | **Día 13** | **Día 14** | **Día 15** | **Día 16** | **Día 17** | **Día 18** | **Día 19** | **Día 20** |
| **Comercial** | | | | | | | | | | | | | | | | | | | | |
| Vendedor 1 | X | | | | | | | | | | | X | | | | | | | | X |
| Vendedor 2 | X | | | | | | | | | | | X | | | | | | | | X |
| Vendedor 3 | X | | | | | | | | | | | | X | | | | | | | |
| **Administración** | | | | | | | | | | | | | | | | | | | | |
| Administrativo 1 | | X | | | | | | | | | | X | | | | | | | | |
| Administrativo 2 | | X | | | | | | | | | | X | | | | | | | | |
| Administrativo 3 | | X | | | | | | | | | | X | | | | | | | | |
| **Tecnología** | | | | | | | | | | | | | | | | | | | | |
| Técnico 1 | | | X | | | | | | | | | X | | | | | X | | | |
| Técnico 2 | | | X | | | | | | | | | X | | | | | X | | | |
| Técnico 3 | | | X | | | | | | | | | X | | | | | X | | | |
| Técnico 4 | | | X | | | | | | | | | X | | | | | X | | | |
| **Recepción** | | | | | | | | | | | | | | | | | | | | |
| Recepcionista 1 | | | | X | | | | | | | | X | | | | | | | | |
| Recepcionista 2 | | | | X | | | | | | X | | X | | | | | | | | |
| **Gerentes** | | | | | | | | | | | | | | | | | | | | |
| Gerente General | | | | | X | | | | | | | X | | | | | | | | |
| Sub Gerente 1 | | | | | X | | X | | | | | X | | | | | | | | |
| Sub Gerente 2 | | | | | X | | | | | | | X | | | | | | | | |
| Sub Gerente 3 | | | | | X | | | | | | | X | | | | | | | | |
| **Vectores de Ataque** | Email Spoofing + Phishing Web | | | | | Email Spoofing + Vishing + Phishing Google Forms | | | | | Ataque de Infección USB (Rubber Ducky) | | | | | Ataque de Intrusión WiFi Evil Twin | | | | |

Una vez finalizada la campaña y obtenido las evidencias de cada uno de los resultados, departamentos y usuarios afectados, estos también se reflejan en el plan de trabajo anteriormente mencionado (*Figura 30*) en donde se puede describir con la siguiente leyenda:

- x Ataque exitoso planificado / Usuario afectado
- Ataque exitoso no planificado / Usuario afectado
- x Usuarios no afectados

**Tabla 1**

*Datos relevantes por usuario de resultados de las Campañas de Ing. Social*

| Datos relevantes por usuario | |
|---|---|
| Total, de ataques enviados | 40 |
| Total, de tipos de ataque exitosos | 6 |
| Total, de tipos de ataque fallidos | 0 |
| Total, de usuarios afectados | 8 |
| Total, de usuarios Invictos | 8 |
| Total, muestra | 16 |

Para el caso práctico se propone un informe ejecutivo que consta de los siguientes ítems:

- Portada
- Introducción, donde se presenta una breve descripción del proceso y resultados.
- Objetivos
- Metodología
- Cronograma de Trabajo
- Ejecución de metodología
- Evidencias encontradas por Perfilamiento de Empresa y Empleados.
- Evidencias encontradas las campañas ejecutadas.
- Resultados de la tabulación
- Identificación de vulnerabilidades de la empresa en el ámbito de ingeniería social.
- Conclusión y recomendaciones finales

En este apartado el ingeniero social definirá un grado de riesgo y dentro del mismo calificará a la empresa en función a los ataques realizados y vulnerabilidades encontradas, como se ve en la *Tabla 2*.

**Tabla 2**

*Tabla de calificación de grado de riesgo para OmniData*

| No. | Tipo de Ataque Nativo | Grado de Riesgo | | |
|---|---|---|---|---|
| | | **BAJO** | **MEDIO** | **ALTO** |
| 1 | EMAIL SPOOFING | | | X |
| 2 | PHISHING | | X | |
| 3 | VISHING | | | X |
| 4 | INFECCIÓN POR USB (RUBBER DUCKY) | | X | |
| 5 | INTRUSIÓN WIFI (EVIL TWIN) | X | | |
| 6 | INTRUSIÓN FÍSICA | | | X |
| | **TOTAL** | **1** | **2** | **3** |

# Conclusiones

Se ha logrado generar una guía metodológica aplicada, la cual tenga la capacidad de poder planificar una serie de ataques informáticos en torno a técnicas de ingeniería social en una empresa previamente perfilada.

En el transcurso del mismo se ha identificado varios pasos importantes dentro del proceso de la guía metodológica, tales como son el perfilamiento previo de la empresa, así como la planificación de campañas de ingeniería social.

Se logra identificar en las implementaciones de cada ataque la importancia de generar un ambiente de confianza con la víctima, así como de cumplir el concepto de celeridad, con el objetivo de no dar oportunidad al usuario afectado sospechar que está en un ambiente de ataque informático.

Así mismo, se logra comprobar la vulnerabilidad de una empresa en base a la planificación y ejecución de campañas de ataque informático e ingeniería social.

Se diagnóstica las vulnerabilidades de la empresa en el caso práctico, calificándola con un grado de riesgo alto a la misma, para la cual también se realizan las respectivas recomendaciones para evitar que su información sea vulnerada.

Se diagnostica de manera evidente que el personal de la empresa dentro del caso práctico es un vector de vulnerabilidad dentro de la empresa, la cual es susceptible a ataques tanto *Phishing, Spoofing, Vishing*, entre otros vistos dentro del presente caso práctico.

Como parte de las recomendaciones, dependiendo la campaña ejecutada, las víctimas pueden descubrir o sospechar que están sufriendo un ataque informático, es recomendable que el ingeniero social este en constante monitoreo de las posibles reacciones de la víctima y pueda actuar de manera apropiada en caso de generarse una emergencia.

Es importante que las empresas que son evaluadas bajo este concepto de campañas de ingeniería social tengan un plan de concientización, el mismo que puede ser implementado como parte del plan de mitigaciones de ciberseguridad de una empresa.

En la implementación de cada ataque el ingeniero social debe tener siempre en cuenta el marco teórico del trabajo de investigación donde recomienda siempre ganar la confianza de la víctima, la compensación, el poder, la firmeza y la celeridad en todo escenario que se vaya a crear, sea este por medio digital, telefónico, físico, etc.

# Referencias


Alonso, R. (10 de diciembre de 2020). Timo del CEO: el ciberataque con el que se roban millones haciendo una sola llamada. *ABC Redes* https://www.abc.es/tecnologia/redes/abci-timo-ciberataque-roban-millones-haciendo-sola-llamada-202012090135_noticia.html

Cannoles, B., & Ghafarian, A. (2017). Hacking Experiment by Using USB Rubber Ducky Scripting. *Journal of Systemics*, *15*(2), 6671. http://www.iiisci.org/journal/sci/FullText.asp?var=&id=ZA340MX17

Casas, P. (19 noviembre de 2015). El triángulo de la seguridad. *Universidad Nacional Autónoma de México*. http://blogs.acatlan.unam.mx/lasc/2015/11/19/el-triangulo-de-la-seguridad/

Cordero, W. (2018). *Implementación de técnicas de ingeniería social en la Institución Técnica de Panqueba*. [Tesis de especialización, Universidad Nacional Abierta y a Distancia] Repositorio UNAD. https://repository.unad.edu.co/handle/10596/22690

Gophish. (s.f). Open-Source Phishing Framework. https://getgophish.com/

INCIBE. (05 de septiembre de 2019). Ingeniería social: técnicas utilizadas por los ciberdelincuentes y cómo protegerse*. Instituto Nacional de Ciberseguridad.* https://www.incibe.es/protege-tu-empresa/blog/ingenieria-social-tecnicas-utilizadas-los-ciberdelincuentes-y-protegerse

Jagatic, T. N., Johnson, N. A., Jakobsson, M., & Menczer, F. (2007). Social phishing. *Communications of the ACM*, *50*(10), 94-100. https://doi.org/10.1145/1290958.1290968

Jones, K. S., Armstrong, M. E., Tornblad, M. K., & Namin, A. S. (2020). How social engineers use persuasion principles during vishing attacks. *Information & Computer Security*. https://www.emerald.com/insight/content/doi/10.1108/ICS-07-2020-0113/full/html

Lisa Institute. (08 de mayo de 2020). Guía Práctica contra la Ingeniería Social. https://www.lisainstitute.com/blogs/blog/guia-practica-ingenieria-social

Navarrete, J. (14 de septiembre de 2020). ECUADOR EN RIESGO – CIBERATAQUES. *BDO Ecuador*. https://www.bdo.ec/es-ec/noticias/2020/ecuador-en-riesgo-ciberataques

Paredes, A. R. Z., Quevedo, I. M. S., & Chalacán, L. J. M. (2020). Seguridad informática en las PyMES de la ciudad de Quevedo. *Journal of business and entrepreneurial studie*, *4*(2). https://doi.org/10.37956/jbes.v4i2.97

SGSI. (01 de febrero de 2018). Los tres pilares de la seguridad de la información: confidencialidad, integridad y disponibilidad. *Blog especializado en Sistemas de Gestión de Seguridad de la Información*. https://www.pmg-ssi.com/2018/02/confidencialidad-integridad-y-disponibilidad/

welivesecurity. (21 de mayo de 2014). Las técnicas de Ingeniería Social evolucionaron, ¡presta atención!. https://www.welivesecurity.com/la-es/2014/05/21/tecnicas-ingenieria-social-evolucionaron-presta-atencion/