



KIT DE CONCIENCIACIÓN

Manual de implantación



INSTITUTO NACIONAL DE
CIBERSEGURIDAD

SPANISH NATIONAL
CIBERSECURITY INSTITUTE

www.incibe.es


INSTITUTO NACIONAL DE CIBERSEGURIDAD

ÍNDICE



1. Introducción

pág. 08



2. Estructura de directorios

pág. 09



3. Planificación implantación del Kit

pág. 11



4. Ataque dirigido con Gophish

pág. 13

4.1. Despliegue del ataque

pág. 14

ÍNDICE



5. Ataque dirigido con ficheros maliciosos

pág. 15

5.1. Memorias USB infectadas

pág. 16

5.1.1. Preparación de las memorias USB

pág. 16

5.1.2. Preparación de la herramienta de seguimiento

pág. 21

5.1.3. Despliegue del ataque

pág. 24

5.2. Correo con enlace malicioso

pág. 25

5.2.1. Preparación de la herramienta de seguimiento

pág. 25

5.2.2. Despliegue del ataque

pág. 26

5.2.3. Seguimiento del alcance

pág. 31

5.2.4. Aviso informativo

pág. 31



6. Distribución de posters de presentación y trípticos

pág. 32



7. Proceso formativo

pág. 33

7.1. Temáticas tratadas

pág. 34

7.2. Recursos formativos incluidos en el kit

pág. 35

7.3. Distribución de los recursos formativos

pág. 36

7.3.1. Documento PDF explicativo

pág. 37

7.3.2. Posters

pág. 37

7.3.3. Consejos

pág. 38

7.3.4. Test de evaluación

pág. 38

ÍNDICE



8. Recordatorio ataques dirigidos

8.1. Ataque dirigido con Gophish

pág. 39

8.2. Ataque dirigido mediante enlace malicioso
en el correo

pág. 40

8.3. Ataque dirigido mediante USB

pág. 41

pág. 42



9. Valoración encuesta de satisfacción

pág. 49



10. Referencias

pág. 50

ÍNDICE DE FIGURAS



Ilustración 1: Fases del Kit de concienciación	pág. 08
Ilustración 2: Cronograma duración Kit	pág. 12
Ilustración 3: Ejemplos de estructura de directorios de la memoria USB	pág. 17
Ilustración 4: Editar fichero incibeweb.vbs con Bloc de notas	pág. 18
Ilustración 5: Código fuente del fichero incibeweb.vbs y valor editar posteriormente	pág. 19
Ilustración 6: Dirección IPv4 obtenida por consola	pág. 19
Ilustración 7: Valor editado con la nueva dirección IPv4	pág. 20
Ilustración 8: Firewall de Windows solicitando acceso a la herramienta de seguimiento	pág. 21
Ilustración 9: Herramienta de seguimiento ejecutándose	pág. 22
Ilustración 10: Resultados obtenidos por la herramienta de seguimiento	pág. 23
Ilustración 11: Ficheros ubicados en el mismo directorio para el ataque dirigido con enlace malicioso	pág. 25
Ilustración 12: Ejemplo de correo para el ataque dirigido con enlaces maliciosos	pág. 28
Ilustración 13: Añadir enlace en el correo	pág. 29
Ilustración 14: Enlace malicioso que apunta al fichero incibeweb.exe	pág. 30
Ilustración 15: Archivos necesarios para el ataque dirigido utilizando la herramienta WinRAR	pág. 43
Ilustración 16: Configuración de las opciones SFX avanzadas	pág. 44
Ilustración 17: Selecciones de ícono en las opciones SFX avanzadas	pág. 45
Ilustración 18: Editar nombre del archivo	pág. 46
Ilustración 19: Fichero .exe con ícono de PDF	pág. 46
Ilustración 20: Selección del carácter «U+202E» en la utilidad Mapa de caracteres	pág. 47
Ilustración 21: Modificación del nombre del archivo añadiendo «fdp» al final	pág. 48

ÍNDICE DE FIGURAS



Ilustración 22: Desplazar el cursor hasta el comienzo de «fdp» y pegar el carácter «U+202E»

pág. 48

Ilustración 23: Fichero con ícono de formato pdf y cuya extensión también parece pdf pero en realidad es .exe

pág. 48

ÍNDICE DE TABLAS



Tabla 1: Duración de las diferentes partes del Kit	pág. 11
Tabla 2: Duración y descripción ataque con dirigido con Gophish	pág. 13
Tabla 3: Duración y descripción ataque con dirigido con ficheros maliciosos	pág. 15
Tabla 4: Duración y descripción posters de presentación y trípticos	pág. 32
Tabla 5: Duración y descripción proceso formativo	pág. 33
Tabla 6: Duración y descripción recordatorio ataques dirigidos	pág. 39
Tabla 7: Duración y descripción recordatorio ataque dirigido con Gophish	pág. 40
Tabla 8: Duración y descripción recordatorio ataque dirigido con enlace malicioso	pág. 41
Tabla 9: Duración y descripción recordatorio ataque dirigido mediante USB	pág. 42



1.

INTRODUCCIÓN

El objetivo de este manual es orientar a las empresas en la correcta distribución y aplicación de los distintos materiales que conforman el «Kit de concienciación».

Mediante estos materiales, se podrán realizar campañas de concienciación sobre seguridad de la información en la empresa.

Cada sector industrial y cada empresa son diferentes, esto hace que sea complejo ofrecer unas reglas estrictas de implantación de esta herramienta. Por esta razón, en este manual se ofrecerán ideas y recomendaciones para la implantación y distribución de los contenidos del Kit.

La decisión final de cómo utilizar los materiales queda supeditada al criterio de la empresa que descarga el «Kit de concienciación».

Se proponen las siguientes fases:

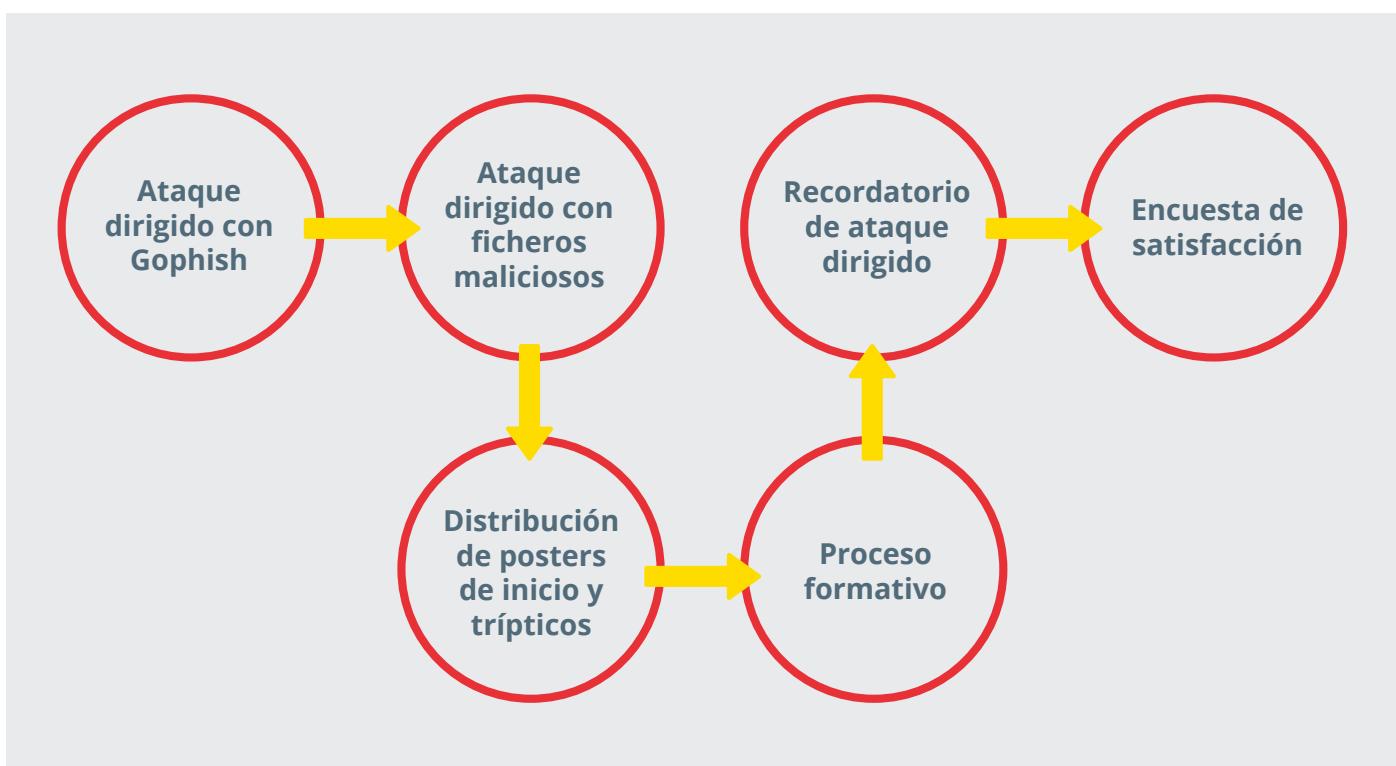


Ilustración 1. Fase del Kit de concienciación





2.

ESTRUCTURA DE DIRECTORIOS



El Kit de concienciación está compuesto por varios recursos ubicados en diferentes carpetas. A continuación se muestra la estructura básica por la que está formado.

- ▶ Kit_de_concienciacion.zip
 - » Ataques_dirigidos
 - Archivos_maliciosos.zip
 - Herramienta_seguimiento.zip
 - » Manual_Gophish
 - Manual_implantacion_Gophish.pdf
 - » Posters_presentacion
 - » Trípticos
 - » Recursos_formativos
 - 01_Informacion
 - 02_Informacion
 - 03_Informacion
 - 04_Fraudes_correo_electrónico
 - 05_Contraseñas
 - 06_Puesto_trabajo
 - 07_Puesto_trabajo
 - 08_BYOD_Teletrabajo
 - 09_Redes_sociales
 - » Encuenta_satisfaccion.pdf
 - » Manual_implantacion.pdf





2.

En la carpeta «Ataques_dirigidos» se encuentran dos ficheros comprimidos en formato ZIP con contraseña «INCIBE». En el primero de ellos están los archivos necesarios para llevar a cabo los ataques dirigidos. En el segundo archivo se encuentra la herramienta de seguimiento que servirá para llevar un registro del número de usuarios alcanzados en los ataques con este tipo de ficheros.

En la carpeta «Manual_Gophish» hay un archivo PDF que servirá como manual de implantación de la herramienta «Gophish», necesaria para llevar a cabo el primer ataque dirigido contra los empleados.

La carpeta «Posters_presentacion» está formada por dos posters que servirán para presentar el Kit de concienciación a los empleados.

En la carpeta «Trípticos» se encuentran los trípticos asociados al Kit con los principales consejos en ciberseguridad que deberán seguir los empleados. Todas las recomendaciones indicadas serán descritas de forma pormenorizada en los diferentes recursos formativos.

Y en la carpeta «Recursos_formativos» se encuentran las 9 unidades temáticas que componen el Kit. Cada una de ellas cuenta con multitud de recursos entre los que se incluyen materiales gráficos y en formato texto.





3.

PLANIFICACIÓN IMPLANTACIÓN DEL KIT

Para una mejor comprensión sobre la correcta implantación del «Kit de concienciación» desarrollado por INCIBE, se ha elaborado una propuesta de planificación estándar a título orientativo, que servirá como estimación sobre los tiempos necesarios de implantación de cada una de las fases que lo componen. El periodo de duración del presente Kit está estimado en 11 meses y medio.



Las tareas incluidas en la siguiente tabla están ordenadas de manera cronológica.

Tarea	Duración
Ataque dirigido con Gophish	5 días laborables
Descanso entre ataques	5 días laborables
Ataque dirigido memoria USB	5 días laborables
Descanso entre ataques	5 días laborables
Ataque enlace malicioso correo	5 días laborables
Distribución posters presentación y trípticos	1 día laborable
Recurso formativo	9 meses
Ataque dirigido con Gophish	5 días laborables
Descanso entre ataques	5 días laborables
Ataque dirigido memoria USB	5 días laborables
Descanso entre ataques	5 días laborables
Ataque enlace malicioso correo	5 días laborables
Encuesta de satisfacción	1 día laborable

Tabla 1. Duración de las diferentes partes del Kit



3.

La siguiente imagen muestra un cronograma con el tiempo en semanas que ocupará toda la distribución del Kit.

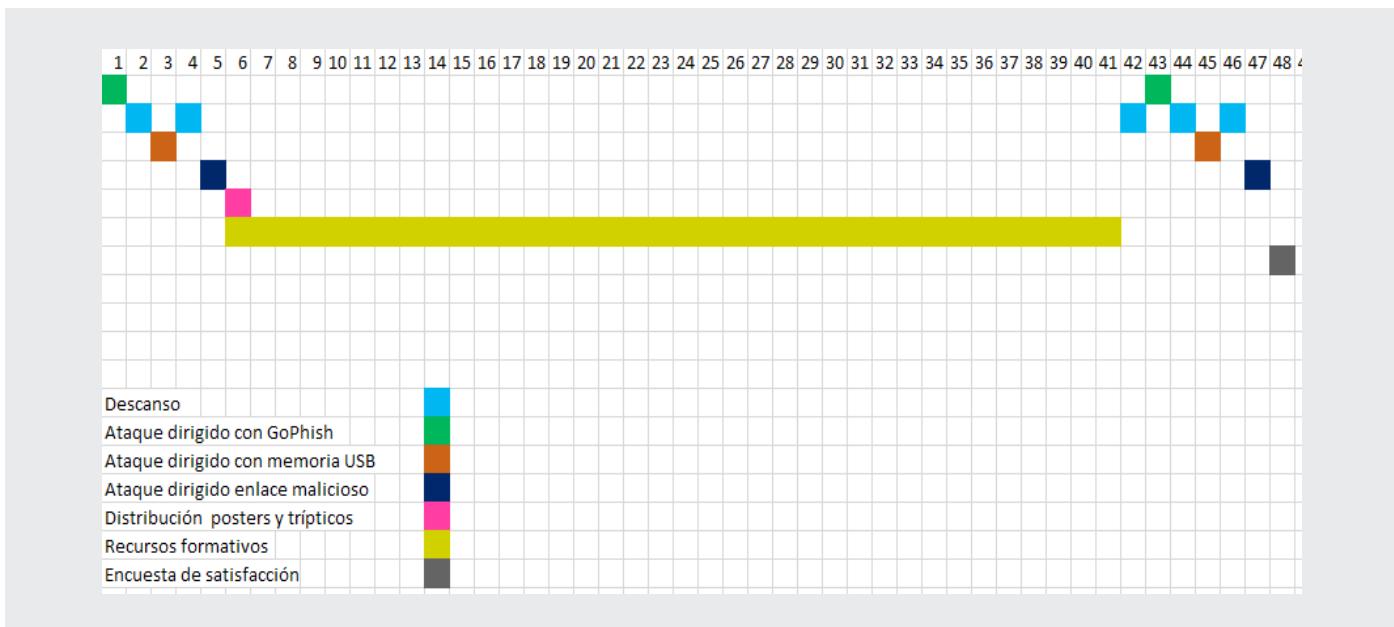


Ilustración 2. Cronograma duración del Kit

Es importante intentar que la preparación de los ataques dirigidos pase desapercibida para el mayor número de empleados posible y que solo unos pocos (los necesarios) sepan de su existencia. De esta forma se conseguirán obtener unos resultados más realistas que si los usuarios estuvieran alerta.

Además, para llevar a cabo la correcta implantación del Kit de concienciación se recomienda contar con ayuda de personal con conocimientos técnicos en informática y redes.

Los ataques dirigidos que se describen en los siguientes apartados están destinados contra usuarios con sistema operativo Windows, ya que es el S.O. más ampliamente utilizado en organizaciones de todo el mundo. En cuanto a los requisitos de la herramienta de seguimiento y *Gophish*, estos pueden ser ejecutados en sistemas operativos Windows, Linux o OSx.





4.

ATAQUE DIRIGIDO CON GOPHISH



Duración	5 días laborables
Descripción	Evaluación inicial del nivel de concienciación en seguridad

Tabla 2. Duración y descripción ataque con dirigido con Gophish

Para llevar a cabo este ataque con la herramienta *Gophish*, como con los siguientes ataques con ficheros maliciosos, se recomienda contar con personal especializado que tenga conocimientos en informática.

El primer tipo de ataque que se llevará a cabo contra los empleados es del tipo phishing. Este tipo de ataques es uno de los más comunes que llevan a cabo los ciberdelincuentes. El objetivo es suplantar a un servicio para obtener información confidencial relacionada con este. En el ataque que se llevará a cabo se capturará únicamente el usuario y la contraseña de acceso al servicio, pudiendo además ser capturada la contraseña parcialmente para no afectar a la privacidad del usuario.

El objetivo de este tipo de ataque es que los usuarios vean lo fácil que es ser engañados por un correo fraudulento y que se vea comprometida la información confidencial de la empresa o de sus servicios personales. Para llevar a cabo el ataque se ha de instalar y desplegar la herramienta *Gophish* (en la carpeta «Manual_Gophish» dentro del Kit se encuentra el documento «Manual_implantacion_Gophish.pdf» que explica paso a paso cómo llevar a cabo esta parte del Kit).





4.

4.1. Despliegue del ataque

El ataque dirigido con *Gophish* será el pistoletazo de salida a la implantación del Kit y tendrá una duración de 5 días laborables, pudiendo comenzar el día de la semana que mejor se adapte a la empresa. Para hacer que el ataque sea más efectivo, se recomienda hacerlo el día de la semana que generalmente se tenga más volumen de trabajo, ya que así será más efectivo.

Una vez se haya concluido con el primer ataque, se recomienda exportar los resultados y analizarlos para comprobar cuantos usuarios han «caído en la trampa». Además, servirá para comparar los resultados con el ataque que se realizará al concluir el periodo formativo. Una vez terminado este primer ataque, se debe establecer un tiempo de espera hasta el siguiente ataque dirigido con ficheros maliciosos, siendo lo recomendable una semana.





5.

ATAQUE DIRIGIDO CON FICHEROS MALICIOSOS



Duración	1 mes
Descripción	Evaluación inicial del nivel de concienciación en seguridad

Tabla 3. Duración y descripción ataque con dirigido con ficheros maliciosos

El objetivo de estos ataques dirigidos con ficheros maliciosos es concienciar a los empleados sobre lo fácil que es ejecutar *malware* en los dispositivos corporativos, también sobre la necesidad de ser precavidos a la hora de confiar en los archivos que ejecutan y los correos que reciben. Este será el segundo método empleado para «atacar» a los empleados de la empresa. Se recomienda desplegar como mínimo uno de los dos ataques dirigidos a continuación descritos.

Se plantean dos ataques dirigidos con vectores diferentes: por medio de una memoria USB y/o a través del correo electrónico.

Al igual que sucede con el ataque dirigido con *Gophish*, es importante que la preparación y el despliegue de estos ataques pasen lo más desapercibido posible dentro de la organización.





5.

5.1. Memorias USB infectadas

Una de las fuentes de infección en las organizaciones es a través de *malware* alojado en dispositivos de almacenamiento externos, usualmente memorias USB o pendrives. El ataque está basado en el despliegue de varias memorias USB «extraviadas» por la organización, las cuales contienen un archivo «malicioso» que, al ser ejecutado, muestran al usuario un portal web de INCIBE advirtiéndole del peligro que supone lo que acaba de hacer. En ella se indicarán los peligros de la acción que acaba de realizar y qué medidas deben seguirse para evitar el escenario de una posible infección en la red de la empresa. Es importante indicar que no será identificado ni utilizado ningún dato personal de los participantes en la prueba.

5.1.1. Preparación de las memorias USB

En primer lugar, es necesario adquirir las memorias USB donde se almacenará el fichero «infectado». Es recomendable que el fichero vaya acompañado de otro tipo de contenido totalmente inofensivo como, por ejemplo, un directorio llamado «Fotos» y otro «Trabajo» donde en cada uno de ellos haya ciertos ficheros genéricos, como imágenes descargadas de Internet, documentos PDF y/o documentos Excel o Word pero sin ser demasiados, ya que el objetivo es que se encuentre el fichero malicioso.

El Kit cuenta con 3 tipos de ficheros maliciosos, siendo el factor diferencial entre todos ellos la dificultad para su detección por parte de los usuarios ya que todos realizan la misma tarea, abrir la página web de INCIBE advirtiéndoles del peligro que acaban de correr. Estos ficheros maliciosos se encuentran en un archivo comprimido llamado «Ataques_dirigidos.zip» en la carpeta «Ataques_dirigidos». La clave con la que se encuentran protegidos es «INCIBE».



5.

A continuación se enumeran los ficheros maliciosos, están ordenados según la complejidad para su detección, siendo 1 el más bajo y 3 el más alto:

1. incibeweb.vbs

2. incibeweb.exe

3. incibeweb.doc

Dentro de la memoria USB se ubicará el fichero infectado, en una carpeta que llame la atención de las posibles víctimas o directamente en la raíz de la memoria como se muestra en los siguientes ejemplos.

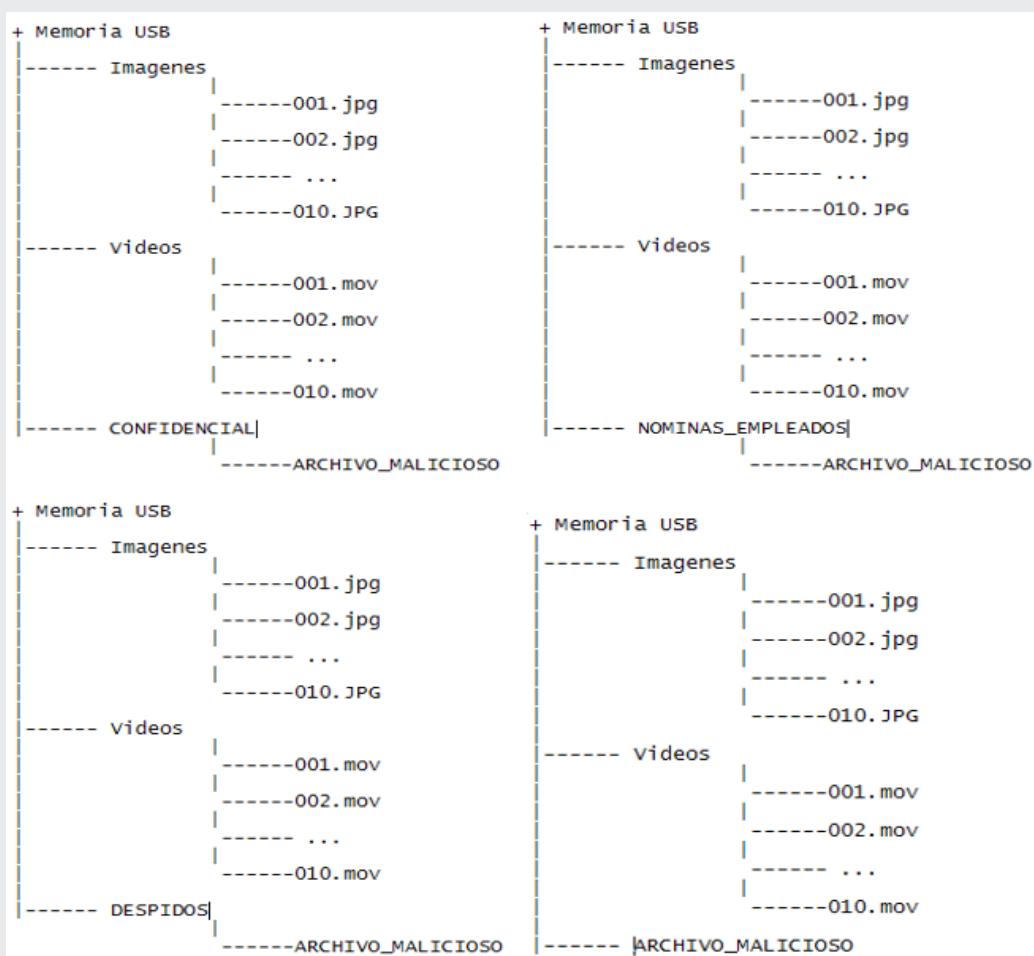


Ilustración 3. Ejemplos de estructura de directorios de la memoria USB



5.

Siguiendo alguna de las estructuras anteriores, o creando otra nueva que se adapte mejor a la organización, se ubicará el fichero infectado, en este caso se utilizará el archivo con nivel de dificultad sea 1 «incibeweb.vbs». Este es recomendable que sea renombrado por uno que llame la atención, como por ejemplo:

- ▶ CONFIDENCIAL.vbs
- ▶ MATERIAL_PRIVADO.vbs
- ▶ NOMINAS_MES.vbs
- ▶ LISTADO_DESPIDOS.vbs

Ya que el archivo malicioso debe realizar una conexión a la herramienta de seguimiento ubicada en la carpeta «Ataques_dirigidos», es necesario realizar una pequeña configuración del mismo porque cada empresa utilizará un rango diferente de direcciones IP locales diferentes. Para editar el archivo .vbs se debe pulsar el botón derecho del ratón y en el menú contextual, ir a la opción > Abrir con > Bloc de notas.

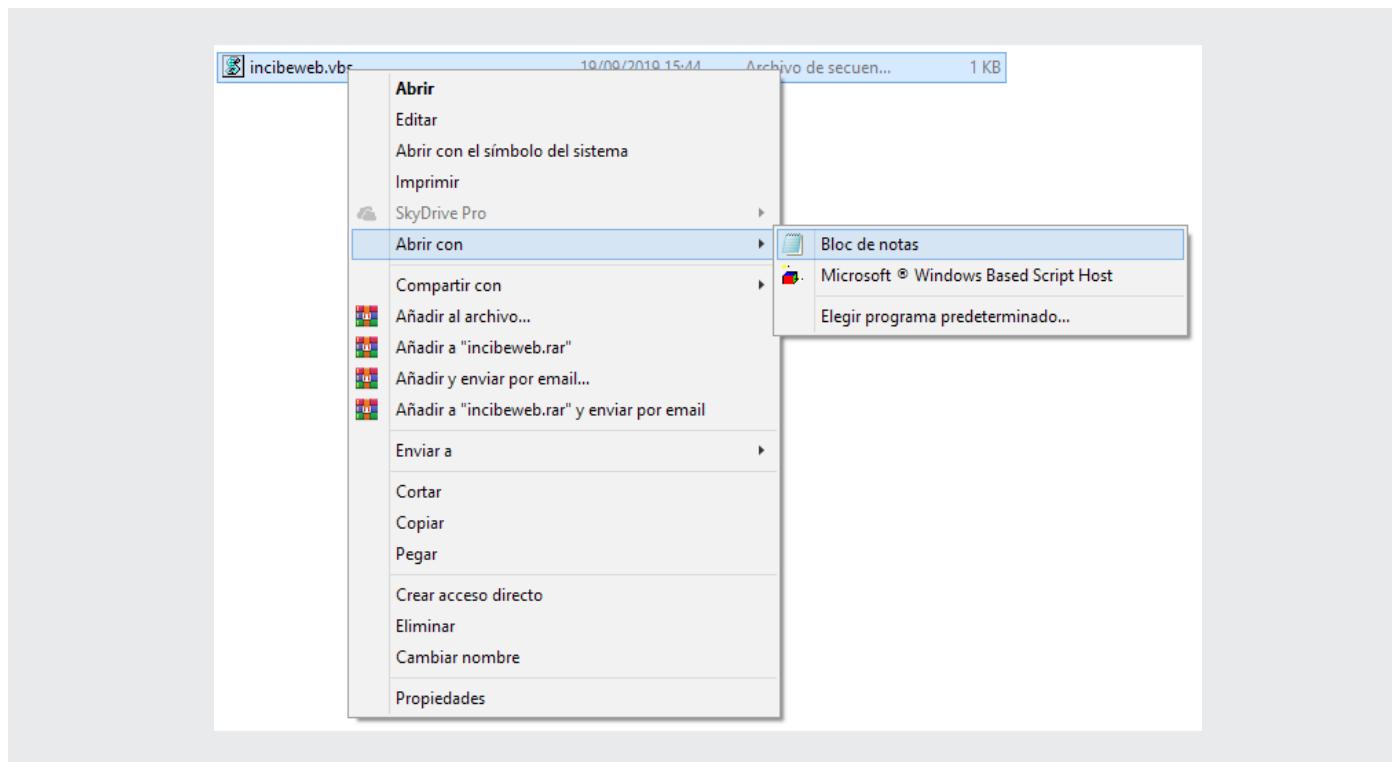


Ilustración 4. Editar fichero incibeweb.vbs con Bloc de notas



5.

De este modo se abrirá un Bloc de notas con el código fuente del archivo que deberá ser similar a la siguiente imagen:

```
Dim iURL
Dim objShell

iURL = "https://www.incibe.es/protege-tu-empresa/kit-concienciacion/ataque-simulado"

'*****La siguiente linea es donde hay que poner la direccion IP del equipo donde se ejecuta el servidor web del Kit

direccion_servidor_local = "http://200.100.45.88:9999"

' *****

set objShell = CreateObject("WScript.Shell")
objShell.run(iURL)

objShell.run(direccion_servidor_local)
```

Ilustración 5. Código fuente del fichero incibeweb.vbs y valor editar posteriormente

El siguiente paso es conocer cuál es la dirección IP del equipo donde se ejecutará la herramienta de seguimiento. Para que la herramienta de seguimiento funcione correctamente, el equipo que hará las veces de servidor debe tener acceso a la misma red que los equipos de los empleados. A modo de ejemplo, la dirección IP del servidor será la indicada en el apartado “Dirección IPv4”, tal y como se muestra en la siguiente imagen.

```
C:\Users\tecnico>ipconfig  
Configuración IP de Windows  
  
Adaptador de Ethernet Ethernet:  
  
    Sufijo DNS específico para la conexión . . . :  
    Vínculo dirección IPv6 local . . . . . : fe80::b21f:88ff:5d10:5dad%3  
    Dirección IPv4 . . . . . : 10.70.4.23  
    Máscara de subred . . . . . : 255.255.255.  
    Puerta de enlace predeterminada . . . . . : 10.70.4.1  
  
Adaptador de túnel isatap.<D0CB7F10-03AE-40B4-AC89-515596AA1B8C>:  
  
    Estado de los medios . . . . . : medios desconectados  
    Sufijo DNS específico para la conexión . . . :
```

Ilustración 6. Dirección IPv4 obtenida por con consola



5.

A continuación se sustituirá en el archivo .vbs con la nueva dirección IP, tal y como se muestra en la imagen:

```
Dim iURL
Dim objShell

iURL = "https://www.incibe.es/protege-tu-empresa/kit-concienciacion/ataque-
simulado"

'*****
'La siguiente linea es donde hay que poner la direccion IP del equipo donde se
ejecuta el servidor web del Kit

direccion_servidor_local = "http://10.70.4.23:9999"

'*****

set objShell = CreateObject("WScript.Shell")
objShell.run(iURL)

objShell.run(direccion_servidor_local)
```

Ilustración 7. Valor editado con la nueva dirección IPv

El puerto utilizado por la herramienta de seguimiento es el 9999, esto puede hacer que entre en conflicto con otra herramienta si está utilizando el mismo puerto. En ese caso se puede editar el puerto en escucha en el archivo «servidor.py» y ejecutarlo utilizando para ello el intérprete de **Python 3.8 [Ref. - 1]**.



5.

5.1.2. Preparación de la herramienta de seguimiento

El siguiente paso será activar la herramienta de seguimiento mediante la cual se puede obtener un listado de todos los equipos de la empresa que han ejecutado el fichero malicioso. El programa de seguimiento es un servidor web desarrollado en *Python* que registrará cada vez que se ejecuta un archivo malicioso de las memorias USB. Esta herramienta, y el equipo que la está ejecutando, deberán quedar en funcionamiento durante todo el tiempo que se esté realizando el ataque, es decir, 5 días laborables.

Para iniciar la herramienta de seguimiento hay que acceder a la carpeta «Ataques_dirigidos» y descomprimir el archivo «Herramienta_seguimiento.zip», cuya contraseña es «INCIBE». Una vez hecho, se ha de acceder a la carpeta «Servidor» y ejecutar el archivo «server.exe». Puede que el *firewall* del equipo donde se esté ejecutando requiera confirmación para permitir su correcto funcionamiento.

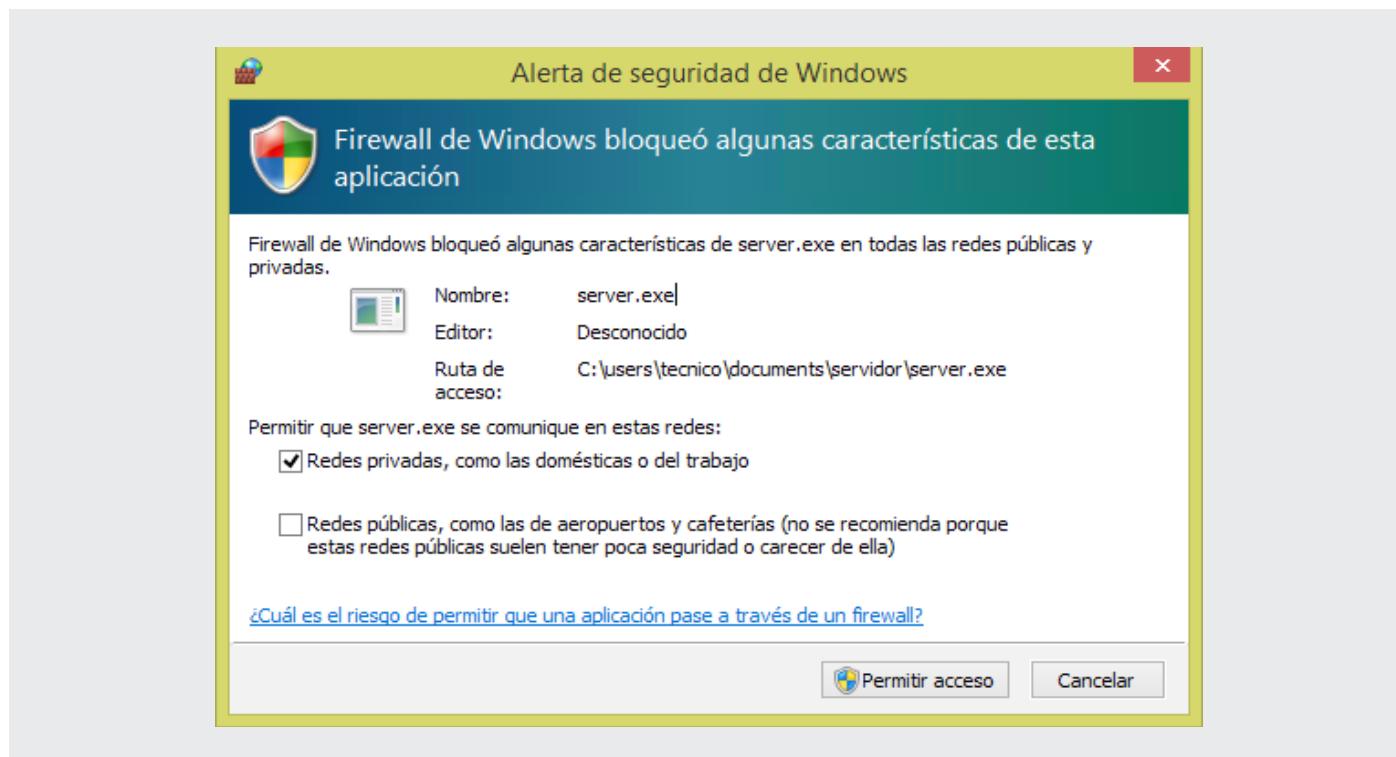


Ilustración 8. Firewall de Windows solicitando acceso a la herramienta de seguimiento



5.

Una vez se ha permitido su uso, se mostrará una ventana como la siguiente, donde se indica que el servidor está funcionando:

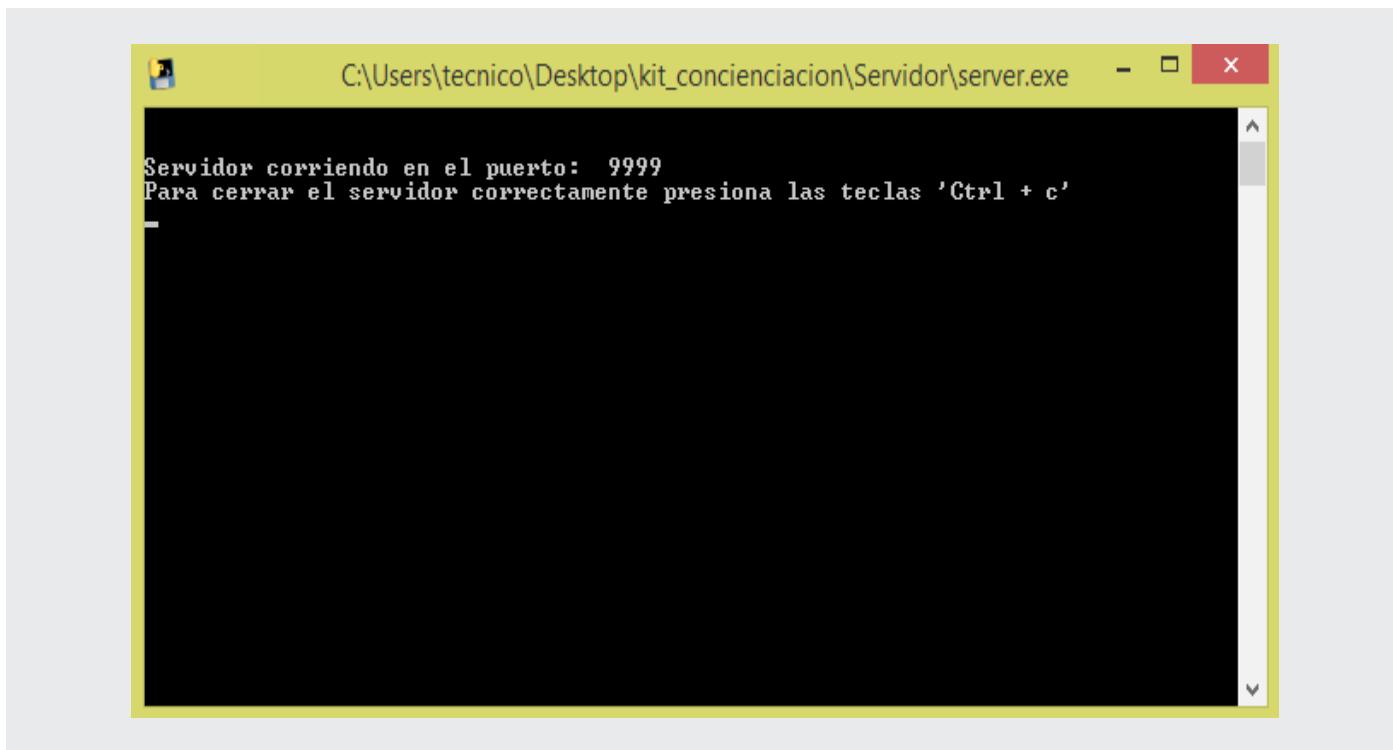


Ilustración 9. Herramienta de seguimiento ejecutándose



5.

Una vez que haya concluido el periodo de ataque, se cerrará el programa, presionando la combinación de teclas «Ctrl + c» y se habrá creado un archivo de texto llamado «Equipos_atacados.txt». Este archivo permanecerá en blanco hasta que no se cierre la herramienta de seguimiento. Dentro de este documento de texto se mostrará un listado con todas las direcciones IP de los equipos que han ejecutado el archivo malicioso de las memorias USB, cada dirección IP corresponde a un equipo diferente. El listado de equipos se mostrará de una manera similar a la siguiente imagen:



Ilustración 10. Resultados obtenidos por la herramienta de seguimiento

Una vez que se ha terminado, es recomendable mover este archivo a otra ubicación o renombrarlo ya que, en caso de volver a iniciar la herramienta de seguimiento, se sobrescribirá toda la información que contenga.

Para que el listado de equipos que han ejecutado el archivo malicioso no se vea alterado, es recomendable que todos los equipos de la organización tengan asignadas direcciones IP fijas y no dinámicas (DHCP). En caso de asignar las direcciones IP de forma fija, es recomendable elaborar un listado con la dirección IP que tiene asignada cada usuario.

En caso de no utilizar un equipo con sistema operativo Windows, o necesitar modificar el puerto a la escucha, se puede ejecutar la herramienta de seguimiento por medio del intérprete de **Python 3.8** y el archivo «server.py».



5.

5.1.3. Despliegue del ataque

El objetivo de esta prueba es que los empleados encuentren y ejecuten el archivo malicioso de la memoria USB. El número de memorias USB que desplegarán dependerá de lo grande que sea la organización y del número de empleados que esta tenga. Algunos lugares donde se pueden dejar son:

- ▶ sala de reuniones;
- ▶ ascensores;
- ▶ salas de descanso;
- ▶ garaje;
- ▶ entrada;
- ▶ servicios;
- ▶ pasillos;
- ▶ en los puestos de los empleados;
- ▶ en la impresora;
- ▶ máquina de café o agua;
- ▶ etc.

Es importante que el encargado de desplegar la memoria USB infectada no sea detectado durante el proceso. En el caso de que el empleado devuelva la memoria USB al departamento de informática o cualquier otro responsable, se le explicará la prueba y su finalidad, se le solicitará que no comente nada al resto de compañeros y se iniciará de nuevo el proceso, desplegando la memoria USB en otra ubicación. Es importante indicar al usuario lo correcto de su decisión de devolver el dispositivo sin haberlo usado



5.

5.2. Correo con enlace malicioso

Una de las principales fuentes de infección en las empresas sigue siendo a través de *malware* adjuntos a los correos electrónicos recibidos por los empleados, tanto al correo electrónico corporativo como al correo personal consultado desde Internet. Por esta razón, es muy importante concienciar a los usuarios de las consecuencias que puede tener para la organización el hecho de que descargue y ejecute en su equipo un adjunto infectado.

5.2.1 Preparación de las memorias USB

Al igual que en el ataque anterior basado en memorias USB con un archivo malicioso, este ataque también requiere iniciar la herramienta de seguimiento «server.exe» para comprobar cuantos usuarios son los que han ejecutado el adjunto malicioso. Para ello se seguirán los mismos pasos que en el apartado **5.1.2**.

El siguiente paso será seleccionar el archivo malicioso, en este caso se utilizará el archivo «incibeweb.exe». Al contrario que en el anterior ejemplo, no es necesario realizar ninguna modificación en el archivo malicioso. Este archivo se ubicará en la misma carpeta que está el programa de seguimiento «server.exe».

Nombre	Fecha de modifica...	Tipo	Tamaño
incibeweb.exe	02/10/2018 11:22	Aplicación	377 KB
server.exe	28/10/2019 17:33	Aplicación	4.308 KB
server.py	04/11/2019 9:19	Python File	2 KB

Ilustración 11. Ficheros ubicados en el mismo directorio para el ataque dirigido con enlace malicioso



5.

5.2.2. Despliegue del ataque

El envío de correos electrónicos se realizará a través de una cuenta de correo falsificada utilizando la herramienta *Gophish* de forma similar a como se realizó el ataque de *phishing* previo. Se comenzará creando el perfil de envío, todos los datos serán los mismos que en la campaña de *phishing* excepto el campo «From» o remitente, este deberá ir en consonancia con el tipo de correo que se pretenda enviar, por ejemplo:

- ▶ Si se va a hacer pasar el correo por uno perteneciente al departamento de informática, o de la empresa que se tenga contratado el soporte técnico, se usará como remitente la dirección de correo real o uno ficticio como **sistemas@empresa.es, dep-informatica@empresa.es**.
- ▶ Si se va hacer pasar el correo por el de un cliente o proveedor es recomendable que este comience por un nombre seguido de la empresa como **nombre.apellido@empresa.es**.

El siguiente paso será crear el correo que se enviará a los empleados, este irá en consonancia con el remitente elegido. Si se ha elegido como remitente el departamento de informática, el correo puede ser similar al siguiente, siempre teniendo en cuenta que hay crear la necesidad de ejecutar el archivo «malicioso»:

Asunto: Auditoría de Seguridad Interna

Buenos días, desde el Departamento de Informática os hacemos llegar este correo en relación con la Auditoría de Seguridad que se está llevando a cabo actualmente en la empresa. Uno de los procedimientos exige que se realicen ciertas comprobaciones en los equipos de usuario de la red interna.

Por ello, debes descargar y ejecutar un programa que analizará la seguridad del equipo. En el siguiente enlace está disponible para su descarga la herramienta de análisis.

Descargar programa

Gracias por vuestra colaboración. Departamento de Informática Empresa



5.

En caso de elegir como remitente un proveedor, se puede utilizar la siguiente plantilla:

Asunto: Factura devuelta

Buenos días, no hemos podido cobrar la última factura que tenemos a vuestra cargo. Por favor, comprobadla cuanto antes, ya que en caso de no proceder al pago, cancelaremos cualquier tipo de relación e interpondremos acciones legales.

Descargar factura

Esperamos recibir noticias.

Un saludo.

Y si se ha elegido un cliente se puede utilizar el siguiente gancho:

Asunto: Posible acuerdo comercial

Buenos días, me llamo XXXXXX y soy el gerente de una importante empresa de [PAÍS EXTRANJERO]. Estamos expandiendo nuestro negocio y creemos que su país y su empresa pueden ser una estupenda opción para generar nuevos y rentables ingresos.

Hemos desarrollado un dossier donde se detalla todo el plan de negocios que tenemos previsto llevar a cabo, lo hemos enviado a diferentes empresas ya que no podemos arriesgarnos a perder esta oportunidad de negocio y la que primero complete el formulario disponible en el siguiente enlace, será la elegida.

Descargar formulario

Esperamos su respuesta cuanto antes.

XXXXXXX

Todos estos correos deberán ir acompañados de logotipos genéricos y firmas, así como el típico texto referente a la protección de datos para dar más credibilidad al mismo.

El enlace deberá apuntar al archivo malicioso «incibeweb.exe» que se ha ubicado en la misma carpeta que el programa de seguimiento. Para ello, se ha de conocer primero la dirección IP del equipo que aloja el archivo malicioso tal y como muestra la Ilustración 5. Una vez se conoce la dirección del servidor habrá que crear el enlace con un texto similar a los que se muestran en los ejemplos. Para ello desde Gophish se ha de crear una nueva plantilla de correo siguiendo los pasos «Email Templates > New Template».



5.

Primero se elegirá el nombre de la plantilla, por ejemplo «Auditoría interna». A continuación el asunto o *Subject*, que siguiendo el primer ejemplo será «Auditoría de Seguridad Interna». Por último, hay que crear el cuerpo del correo, para ello se seleccionará el botón «HTML» y «Source», y se pegará el texto del correo dentro del editor.

The screenshot shows a 'New Template' dialog box. The 'Name' field contains 'Auditoría interna'. The 'Subject' field contains 'Auditoría de Seguridad Interna'. Below these fields is a rich text editor toolbar with tabs for 'Text' (selected) and 'HTML'. The editor's content area contains the following text:

Buenos días, Desde el Departamento de Informática os hacemos llegar este correo en relación con la Auditoría de Seguridad que se está llevando a cabo actualmente en la empresa. Uno de los procedimientos exige que se realicen ciertas comprobaciones en los equipos de usuario de la red interna.

Por ello, debes descargar y ejecutar un programa que analizará la seguridad del equipo, para ello debes descargar y ejecutar la herramienta de análisis disponible para su descarga en el enlace que encontrarás abajo.

[Descargar programa](#)

Gracias por vuestra colaboración. Departamento de Informática Empresa

Ilustración 12. Ejemplo de correo para el ataque dirigido con enlaces maliciosos



5.

A continuación hay que crear el enlace, para ello se selecciona el texto «Descargar programa» y el botón «Link» que se encuentra en el menú superior del editor de texto.

Buenos días, Desde el Departamento de Informática os hacemos llegar este correo en relación con la Auditoría de Seguridad que se está llevando a cabo actualmente en la empresa. Uno de los procedimientos exige que se realicen ciertas comprobaciones en los equipos de usuario de la red interna.

Por ello, debes descargar y ejecutar un programa que analizará la seguridad del equipo, para ello debes descargar y ejecutar la herramienta de análisis disponible para su descarga en el enlace que encontrarás abajo.

[Descargar programa](#)

Gracias por vuestra colaboración. Departamento de Informática Empresa

```
body p
```

Ilustración 13. Añadir enlace en el correo



5.

En el campo URL hay que poner la dirección IP del servidor, en este caso «10.70.4.23» seguido del puerto a escucha «9999» y el nombre del archivo malicioso. Quedaría de la siguiente manera:

- ▶ 10.70.4.23:9999/incibeweb.exe

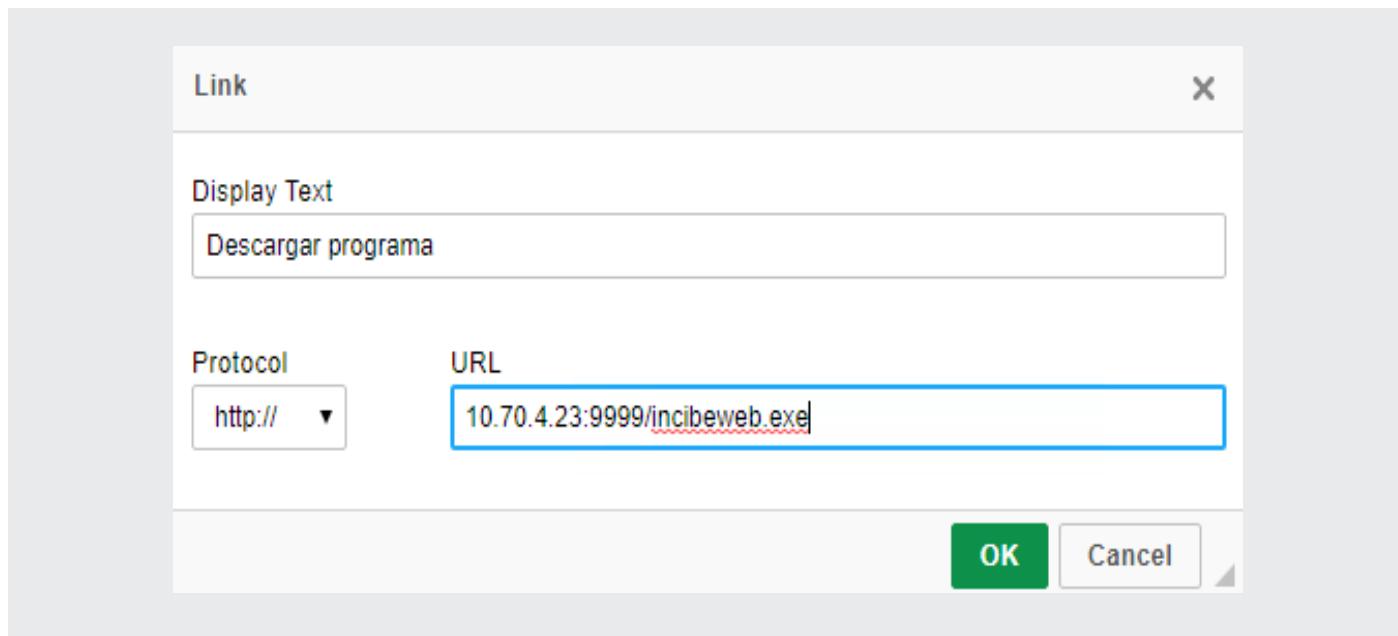


Ilustración 14. Enlace malicioso que apunta al fichero incibeweb.exe

A continuación se guardará la plantilla por medio del botón «Save Template».

El último paso será crear la campaña de envío siguiendo el mismo proceso que en el apartado anterior Ataque dirigido con *Gophish*. En el campo «Email Template» se elegirá el que se acaba de crear «Auditoría interna». En el resto de campos se pondrán los mismos que cuando se envió un phishing a los empleados, ya que, en este caso, algunos de ellos no tienen ninguna relevancia pero son obligatorios para poder crear la campaña.

El último paso será enviar la campaña por medio del botón «Launch Campaign».



5.

5.2.3. Seguimiento del alcance

Al igual que sucedía con el ataque por medio de memorias USB con ficheros maliciosos, este ataque tiene un periodo de duración de 5 días laborables, momento en el que se apagará el programa de seguimiento y se comprobará en el archivo "Equipos_atacados.txt" cuántos equipos han sido víctimas del engaño. Al igual que en el envío de correos de tipo phishing, es recomendable renombrar o cambiar de ubicación este archivo.

5.2.4. Aviso informativo

Una vez terminada la fase de ataques dirigidos, se deberá enviar un mensaje a los empleados informándoles del comienzo del programa de concienciación.

El mensaje puede ser similar al siguiente:

Asunto: Kit de sensibilización

Buenos días,

A pesar de los grandes avances tecnológicos de los últimos años y la aparición de dispositivos y entornos de seguridad más rápidos, eficientes y sofisticados, está demostrado que el principal elemento para garantizar la seguridad de una organización somos todos y cada uno de nosotros. Somos, sin lugar a dudas, el elemento más importante de la tradicional cadena de seguridad.

Por este motivo, hemos comenzado con un programa de concienciación en materia de ciberseguridad, que incorpora múltiples recursos que iremos viendo a lo largo de los próximos días.

Esta información es facilitada por INCIBE de forma absolutamente gratuita. INCIBE no se responsabiliza del uso que pueda hacerse de la misma. Hemos comenzando con la simulación de un ataque simulado, donde si habéis ejecutado el archivo habréis tomado conciencia de lo que ha ocurrido. Vamos a trabajar y a aprender todos los aspectos a tener en cuenta para prevenir este tipo de ataques.

Todo ello para mejorar nuestra seguridad desde el propio corazón de nuestra empresa: las personas.

Gracias por vuestra colaboración.

Departamento de Informática Empresa





6.

DISTRIBUCIÓN DE POSTERS DE PRESENTACIÓN Y TRÍPTICOS



Duración	1 día
Descripción	Comienzo de la fase de concienciación en ciberseguridad

Tabla 4. Duración y descripción posters de presentación y trípticos

Después de haber realizado los ataques dirigidos incluidos en el «Kit de concienciación» y de dejar un tiempo indicado para que los usuarios hayan tenido la oportunidad de «enfrentarse» a dichas pruebas, se recomienda distribuir los posters de inicio y trípticos del Kit. Deberán ser impresos y colocados en lugares visibles donde el empleado los pueda leer tranquilamente (el ascensor, la sala de café, salas de reuniones, etc.)





7.

PROCESO FORMATIVO



Duración	1 recurso formativo por mes. Total 9 meses
Descripción	Distribución de los recursos formativos en ciberseguridad

Tabla 5. Duración y descripción proceso formativo

El siguiente paso es distribuir de forma organizada y espaciada los recursos formativos. En el Kit, se incluyen 9 recursos formativos distribuidos en 6 temáticas distintas. Cada uno de los recursos formativos se empleará para transmitir información útil sobre seguridad de la información y consejos o buenas prácticas a la hora de manejar información corporativa.





7.

7.1. Temáticas tratadas

Las 6 temáticas tratadas se distribuyen en 9 recursos formativos:

- ▶ La información
 - 1. La información. El activo imprescindible de tu organización
 - 2. La información. Clasificación, cifrado y metadatos
 - 3. La información. *Backups*, borrado y tipos de almacenamiento
- ▶ El correo electrónico
 - 4. El correo electrónico. Principales fraudes y riesgos
- ▶ Contraseñas
 - 5. Contraseñas. Y medidas complementarias
- ▶ El puesto de trabajo
 - 6. El puesto de trabajo. Medidas de protección I
 - 7. El puesto de trabajo. Medidas de protección II
- ▶ BYOD y teletrabajo
 - 8. Dispositivos móviles y teletrabajo. Riesgos y protección
- ▶ Redes sociales
 - 9. Redes sociales. Medidas de seguridad para los perfiles de empresa



7.

7.2. Recursos formativos incluidos con el Kit

Para cada uno de los 9 recursos formativos se incluyen los siguientes materiales:

- ▶ **Presentación PowerPoint:** útil sobre todo en caso de que se realice un curso de formación en el que un formador explique a los empleados la problemática y cómo evitarla. Las presentaciones en PowerPoint incluyen los principales conceptos a asimilar de la píldora, redactados de forma esquemática y con notas para ayudar al formador a desarrollar la ponencia.
- ▶ **Documento PDF explicativo:** desarrollo de los conceptos a asimilar, redactados de manera explicativa y detallada, junto con ejemplos y buenas prácticas.
- ▶ **Test de evaluación:** pruebas tipo test sobre cada recurso formativo que servirán para evaluar los conocimientos asimilados.
- ▶ **Posters:** imágenes diseñadas para ser impresas y ubicadas en diferentes estancias de la organización cuyo contenido visual y mensaje servirán para concienciar sobre cada recurso formativo.
- ▶ **Consejos:** imágenes que contienen distintos mensajes, concebidas para ser distribuidas por medio del correo electrónico corporativo o la intranet. Cada recurso formativo consta de dos consejos diferentes.





7.

7.3. Distribución de los recursos formativos

Los recursos formativos de cada unidad temática se distribuirán siguiendo esta estructura:

- ▶ Día 1:
 - » Distribución de posters.
 - » Distribución de un documento PDF explicativo.
 - » Distribución del primer consejo.
 - » Presentación del recurso formativo «opcional».
- ▶ Día 15:
 - » Distribución del primer consejo.
- ▶ Día 20:
 - » Distribución del test de evaluación.

La distribución de los materiales es recomendable que se realice por recurso formativo y a continuación se explica cómo hacerlo.

A la hora de distribuir los diferentes materiales, se puede hacer de diferentes formas:

- ▶ mediante un correo electrónico con el material adjunto;
- ▶ habilitar un directorio compartido al que accedan los empleados y sean ellos los que se descarguen el material;
- ▶ publicarlo en la intranet corporativa;
- ▶ publicarlo en algún servicio de almacenamiento en la nube;
- ▶ etc.

Si la empresa ha podido organizar jornadas de formación, es recomendable que el responsable de realizar la ponencia utilice la presentación en PowerPoint disponible para cada unidad. Cada diapositiva cuenta con notas para ayudar al ponente a llevar a cabo la presentación, además de que es un documento totalmente editable.



7.

Independientemente de si ha habido presentación del recurso formativo por medio de un ponente o no, la distribución de los materiales se realizará atendiendo a la siguiente estructura:

7.3.1. Documento PDF explicativo

El primer documento que se facilitará a los empleados será el PDF que contiene toda la información sobre el recurso formativo, explicada de forma sencilla para que cualquiera, independientemente de sus conocimientos en ciberseguridad, pueda entenderla. Este documento deberá ser leído y comprendido por los empleados a lo largo del mes que durará el recurso formativo en cuestión.

7.3.2. Posters

Los posters son documentos cuyo fin es que sean impresos y ubicados en diferentes sitios de la organización, como ascensores, pasillos, sala de descanso, etc., donde los empleados puedan verlos y asimilar el mensaje que quieren transmitir. Cada unidad temática está compuesta por dos posters distintos, aunque en algunos casos hay una tercera versión en horizontal de uno de ellos, para que se escoja la que más guste.

Los posters serán puestos en los lugares elegidos al comienzo del recurso formativo. Al terminar el recurso formativo, es recomendable que sean retirados y puestos los del recurso formativo siguiente.

Una vez se haya terminado el proceso de formación, los posters pueden ser rotados para que los miembros de la empresa no se olviden de aplicar ciberseguridad en su día a día.



7.

7.3.3. Consejos

Cada recurso formativo está asociado a dos consejos, estos son imágenes que se pueden publicar en el blog interno, en la intranet, pueden ser enviadas por correo electrónico, etc. Al tratarse de dos consejos por cada recurso formativo, el primero de ellos será entregado nada más comenzar la unidad y el segundo será facilitado transcurrida la mitad de la formación.

7.3.4. Test de evaluación

A lo largo de la última semana de cada recurso formativo, se facilitará a los empleados un test de evaluación que deberán responder y entregar al responsable del Kit antes de que se haya comenzado con el nuevo recurso formativo.

Este test será calificado pudiendo entregar a los empleados los resultados del mismo si el responsable lo cree conveniente. Este test servirá para determinar si los conocimientos han sido asimilados por los empleados o no, pudiendo incidir sobre algún punto en particular no comprendido o si algún miembro de la empresa no ha obtenido un resultado aceptable.



8.

RECORDATORIO ATAQUES DIRIGIDOS



Duración	6 semanas
Descripción	Evaluación final del nivel de concienciación en seguridad

Tabla 6. Duración y descripción recordatorio ataques dirigidos

Una vez se han completado todos los recursos formativos, es recomendable realizar una nueva tanda de ataques dirigidos. Estos nuevos ataques serán más difíciles de detectar que los realizados en primera instancia, de esta forma los empleados podrán aplicar gran parte de los conocimientos aprendidos durante el transcurso de la formación. Además, el responsable del implantar el Kit tendrá otro punto de referencia para valorar si los miembros de la organización han mejorado en ciberseguridad.





8.

8.1. Ataque dirigido con Gophish

Duración	2 semanas
Descripción	Evaluación final sobre detección de correos electrónicos fraudulentos de tipo phishing

Tabla 7. Duración y descripción recordatorio ataque dirigido con Gophish

Se realizará una nueva campaña de correos electrónicos fraudulentos de tipo phishing con *Gophish*, utilizando como objetivo un servicio alternativo al elegido en el ataque inicial.





8.

8.2. Ataque dirigido mediante enlace malicioso en el correo

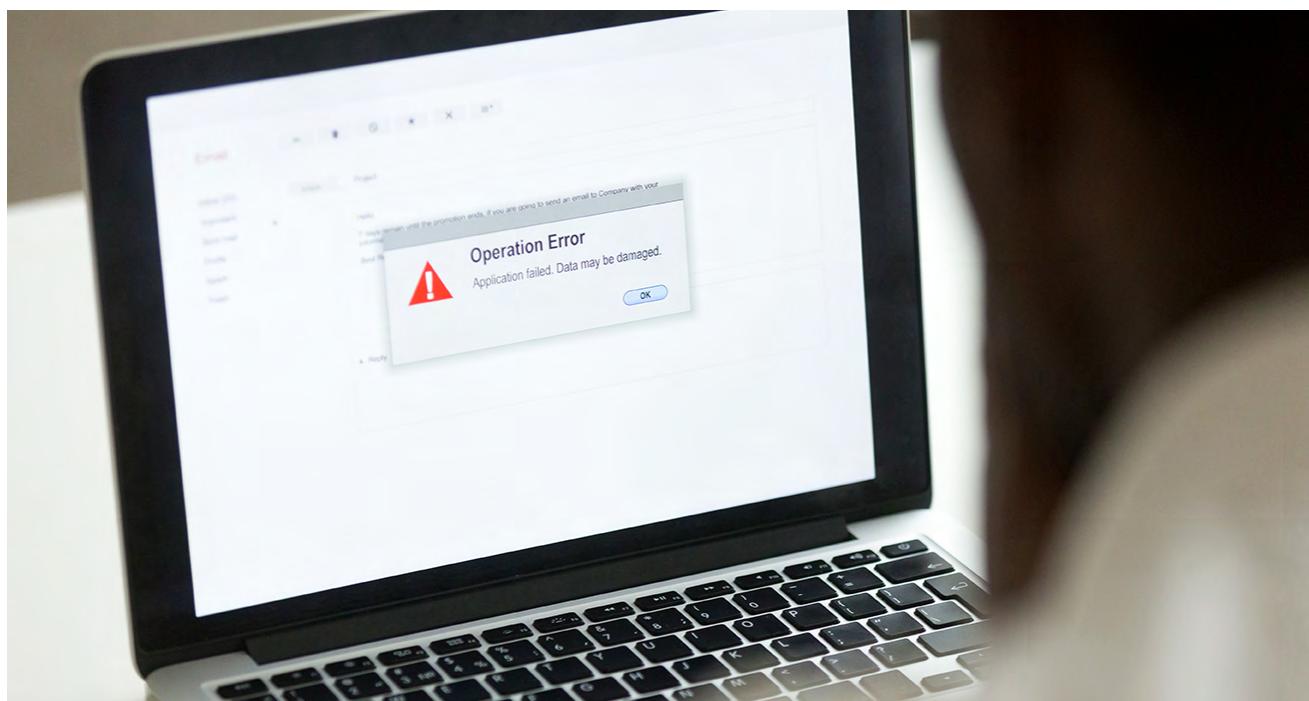
Duración	2 semanas
Descripción	Evaluación final sobre detección de correos electrónicos fraudulentos con adjuntos maliciosos

Tabla 8. Duración y descripción recordatorio ataque dirigido con enlace malicioso

Se realizará una nueva campaña de ataque mediante un enlace malicioso en correo electrónico como se describió en el apartado 3.

Esta vez se utilizará el siguiente fichero malicioso:

- ▶ Incibeweb.doc





8.

8.3. Ataque dirigido mediante USB

Duración	2 semanas
Descripción	Evaluación final sobre dispositivos de almacenamiento externo

Tabla 9. Duración y descripción recordatorio ataque dirigido mediante USB

Se realizará una nueva campaña de ataque mediante memorias USB con ficheros maliciosos, como se describió en el apartado 3.

Esta vez se puede utilizar el mismo archivo «incibeweb.vbs» que en el primer ataque o se pueden realizar varias modificaciones para hacerlo más difícil de detectar.



8.

Para modificar el archivo y que este sea más difícil de detectar por los empleados, se seguirán los siguientes pasos:

- ▶ Lo primero será seleccionar el archivo y editar la dirección IP por la del equipo que hará de servidor tal y como se mostró en el primer ataque.
- ▶ El siguiente paso consistirá en modificar el ícono para que simule ser un archivo pdf. Para ello se requiere tener instalada la herramienta WinRAR **[Ref. - 2]** y seguir los siguientes pasos:
 - » Seleccionar el archivo «incibeweb.vbs» y la imagen «marioneta.jpg», disponibles en el archivo Archivos_maliciosos.zip» presentes en el directorio «Ataques_dirigidos» del Kit y seleccionar el botón secundario del ratón y «Añadir al archivo...»

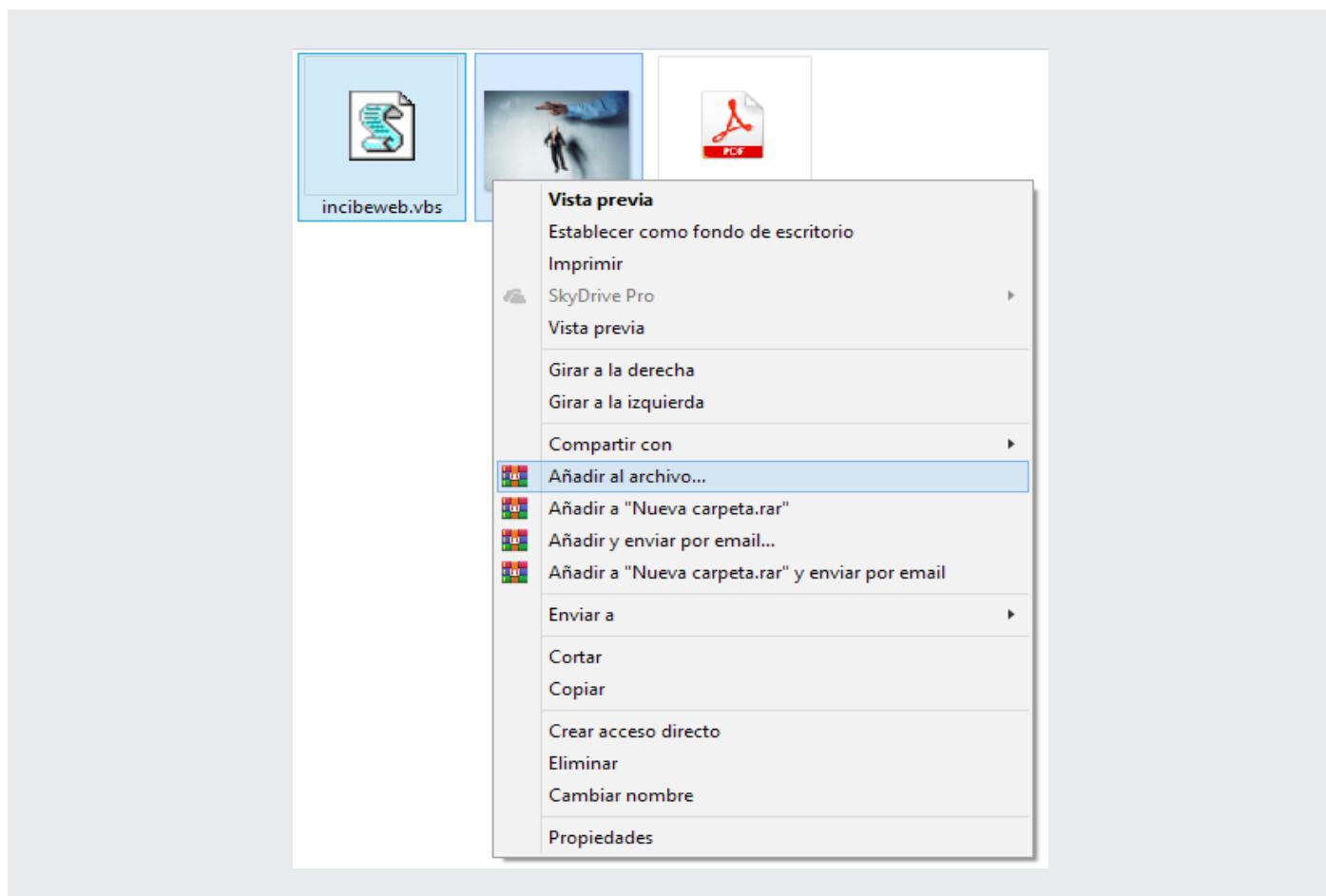


Ilustración 15. Archivos necesarios para el ataque dirigido utilizando la herramienta WinRAR



8.

- » En la pestaña «General» se seleccionará la opción «Crear un archivo autoextraible».
- » En la pestaña «Avanzado» se seleccionará el botón «Autoextraible...».
 - En la ventana que se abre llamada «Opciones SFX avanzadas» y en la pestaña «Instalación» se deben indicar los nombre de los dos archivos anteriormente seleccionados tal y como muestra la imagen:

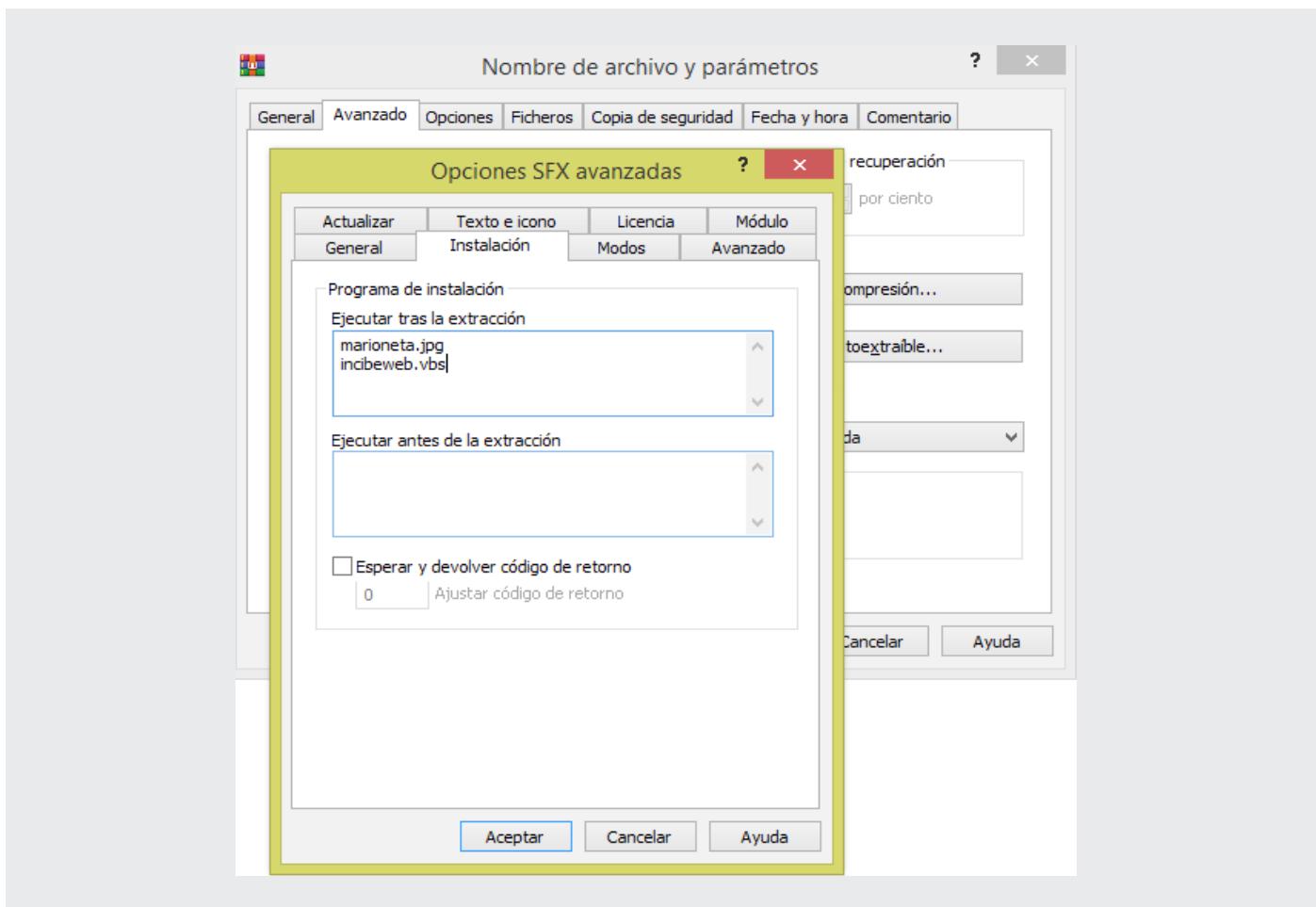


Ilustración 16. Configuración de las opciones SFX avanzadas



8.

- A continuación, en la pestaña «Modos», se marcará la opción «Ocultar todo».
- En la pestaña «Texto e icono» se seleccionará en la opción «Cargar ícono desde fichero» el archivo llamado «pdf.ico» también disponible en el archivo «Archivos_maliciosos.zip».

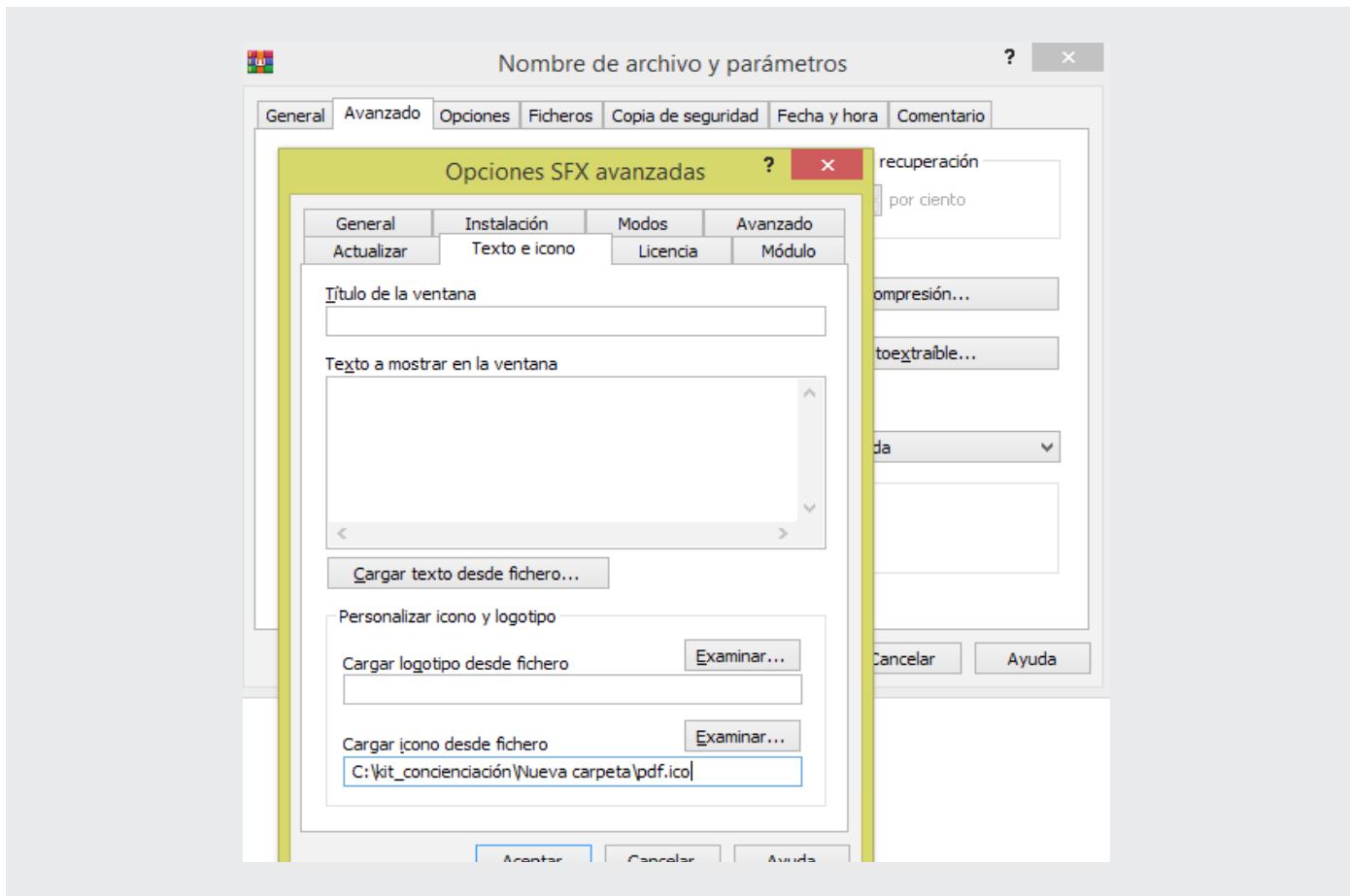


Ilustración 17. Selecciones de ícono en las opciones SFX avanzadas



8.

- » A continuación se seleccionará el botón «Aceptar».
- » Por último se debe modificar el nombre al archivo utilizando uno que sirva de gancho, como por ejemplo «factura» y otra vez «Aceptar».

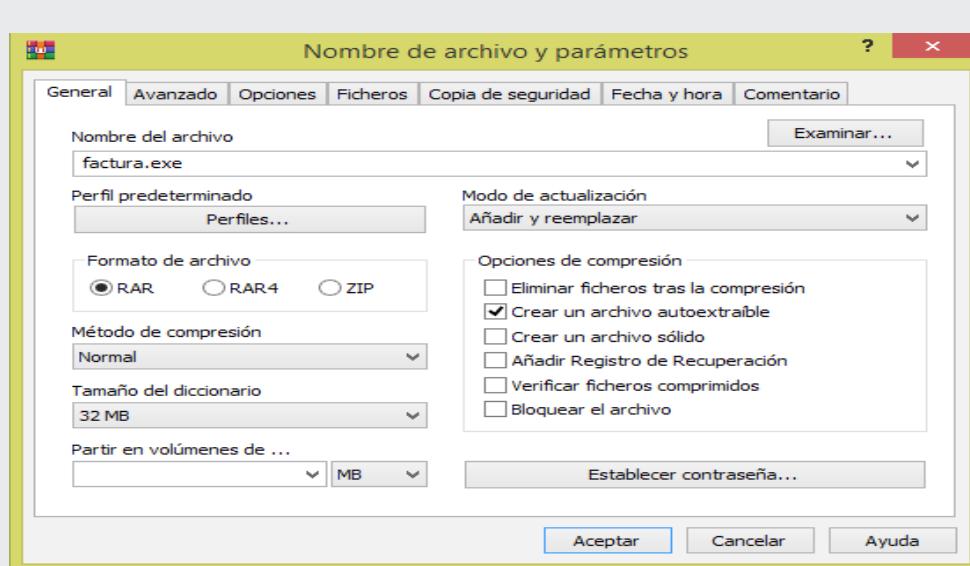


Ilustración 18. Editar nombre del archivo

- » El resultado deberá ser un archivo cuyo icono simula ser un PDF pero cuya extensión es .exe.



Ilustración 19. Fichero .exe con icono de PDF



8.

- El siguiente paso será ofuscar su extensión para que simule ser un archivo pdf. Para ello se seguirán los siguientes pasos:

- » Se abrirá la herramienta que incorporan los sistemas operativos Windows, denominada «Mapa de caracteres», disponible en la siguiente ruta:
 - » C:\Windows\system32\charmap.exe
 - » El siguiente paso consistirá en seleccionar el carácter «U+202E: Reemplazar de derecha a izquierda». Una vez se ha encontrado, se presionará el botón «Seleccionar» y a continuación el botón «Copiar».

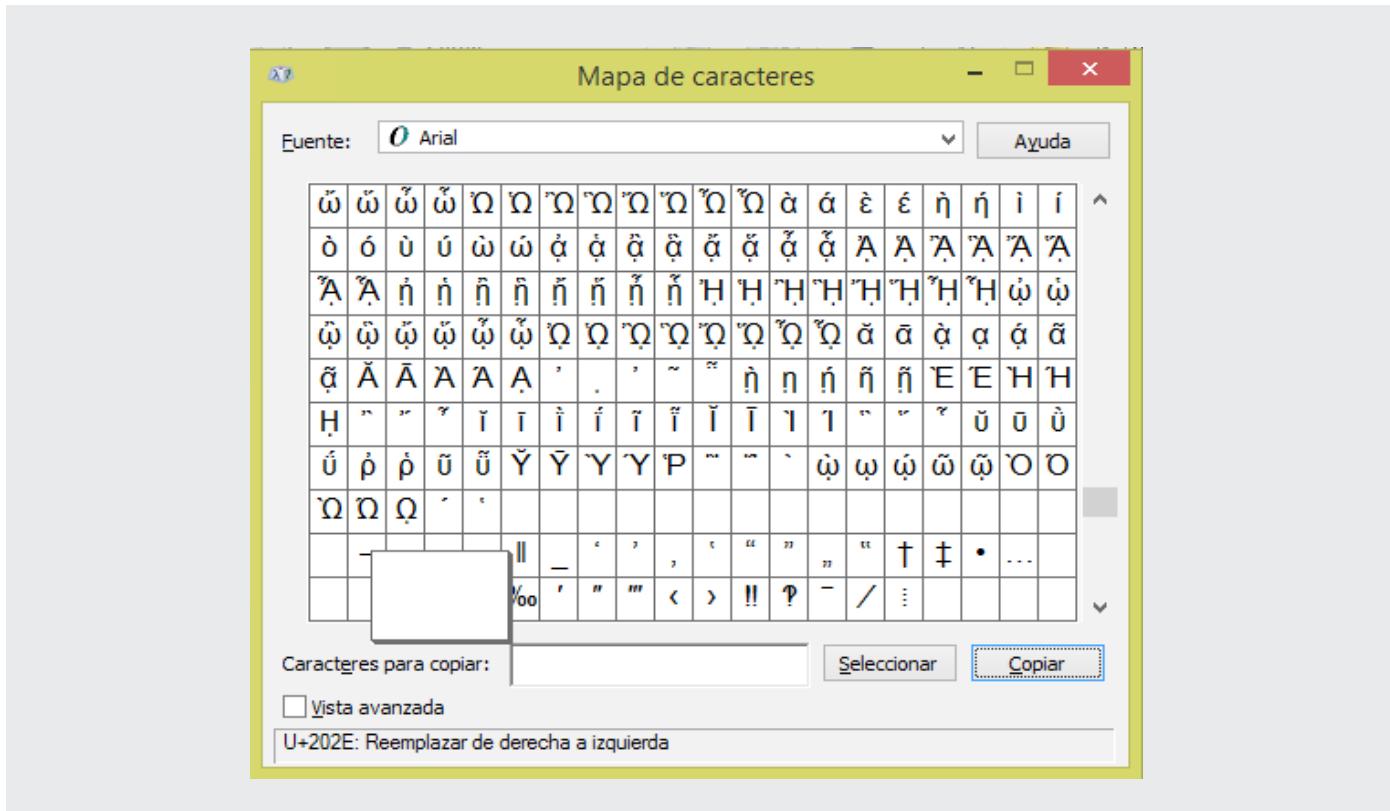


Ilustración 20. Selección del carácter «U+202E» en la utilidad Mapa de caracteres



8.

- » Una vez copiado, se seleccionará el archivo que se acaba de crear y mediante el botón secundario del ratón se cambiará el nombre al mismo, añadiendo al final de este «fdp» tal y como muestra la imagen.

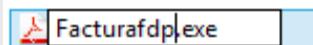


Ilustración 21. Modificación del nombre del archivo añadiendo «fdp» al final

- » Y por último se situará el cursor por delante de la «f» y a continuación se utilizará el atajo de teclado pegar «Ctrl + v».



Ilustración 22. Desplazar el cursor hasta el comienzo de «fdp» y pegar el carácter «U+202E»

- » Quedando el archivo tal y como se muestra en la imagen.



Ilustración 23. Fichero con ícono de formato .pdf y cuya extensión también parece .pdf pero en realidad es .exe



9.

VALORACIÓN, ENCUESTA DE SATISFACCIÓN



Una vez se haya implantado el «Kit de concienciación», la empresa puede hacernos llegar su experiencia y opinión sobre el proceso de implantación y su utilidad en materia de concienciación de la seguridad de la información.

Invirtiendo cinco minutos en cumplimentar dicha encuesta y enviándola a INCIBE, conseguimos una retroalimentación de información continua y una base sobre la que mejorar nuestro Kit.

La encuesta consta de varios aspectos a evaluar, con un valor del 1 al 5, donde el 5 se corresponde con la mejor valoración.





REFERENCIAS

- 1.** Python - <https://www.python.org/downloads/>
- 2.** WinRAR - <https://www.winrar.es/>
- 3.** INCIBE - Protege tu empresa - Herramientas - Servicio AntiRansomware - <https://www.incibe.es/protege-tu-empresa/herramientas/servicio-antiransomware>



KIT DE CONCIENCIACIÓN

Manual de implantación



INSTITUTO NACIONAL DE
CIBERSEGURIDAD

SPANISH NATIONAL
CIBERSECURITY INSTITUTE

www.incibe.es


INSTITUTO NACIONAL DE CIBERSEGURIDAD