Ciberamenazas contra entornos empresariales

Una guía de aproximación para el empresario

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA TERCERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD
017
protege tu empresa

ÍNDICE

ÍNDICE

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE FIGURAS

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

1 INTRODUCCIÓN

¿Alguna vez te has preguntado qué sucedería si los ciberdelincuentes tuvieran acceso al correo electrónico corporativo, a la web de la empresa donde se promocionan los productos y servicios disponibles, o que simplemente toda la información de la empresa no pudiera ser accesible a causa de una infección por *malware*? La respuesta es simple, la capacidad de la empresa para continuar con su actividad y la confianza de los clientes se podría ver seriamente afectada, y por lo tanto su continuidad. Además, ciertos incidentes de seguridad, como aquellos que afectan a datos personales, podrían suponer consecuencias legales y sanciones por parte de las administraciones competentes.

Cualquier empresa, ya sea una gran corporación o una pequeña pyme, gestiona información de gran valor no solo para la propia empresa, sino también para los ciberdelincuentes. Además, no solamente la información es el objetivo de los ciberdelincuentes, los sistemas que la gestionan también son de su interés ya que pueden ser utilizados para perpetrar nuevos fraudes o simplemente para extorsionar a la empresa propietaria.

Por todo ello, **conocer las principales ciberamenazas que pueden afectar a las empresas se hace vital para poder identificarlas activamente y por lo tanto poder evitarlas.** La siguiente guía te mostrará de forma clara y con ejemplos las principales ciberamenazas, así como la vía de identificación y qué hacer en caso de ser víctima de una de ellas.

2 INGENIERÍA SOCIAL Y CORREO ELECTRÓNICO, BASE DE LA MAYORÍA DE INCIDENTES

La gran mayoría de incidentes de seguridad que afectan a las empresas tienen en común dos factores: el correo electrónico y comunicaciones que utilizan diferentes técnicas de ingeniería social. Aprender a identificar este tipo de comunicaciones fraudulentas será clave para reducir la posibilidad de sufrir un incidente de seguridad.

2.1. ¿Qué es la ingeniería social?

Películas y series televisivas generalmente muestran a los ciberdelincuentes como auténticos prodigios de la informática y la ciberseguridad, capaces de vulnerar cualquier sistema explotando sus vulnerabilidades. En este caso, la ficción supera claramente la realidad, en la mayoría de ocasiones **los ciberdelincuentes atacan al eslabón más importante en la cadena de la seguridad, los empleados.** Esto se debe a que los ataques basados en ingeniería social requieren mucho menos esfuerzo que otros tipos de ataques, y por lo tanto el beneficio es mayor.

La ingeniería social [REF - 1] **consiste en utilizar diferentes técnicas de manipulación psicológica** con el objetivo de conseguir que las potenciales víctimas revelen información confidencial, o realicen cualquier tipo de acción que pueda beneficiar al ciberdelincuente, como revelar información confidencial o instalar *software* malicioso.

Los ataques basados en ingeniería social se pueden categorizar en dos tipos diferentes en función del número de comunicaciones que debe realizar el ciberdelincuente hasta conseguir su objetivo:

- ***Hunting:*** mediante **una única comunicación** los ciberdelincuentes buscan obtener su propósito. Generalmente la técnica del *hunting* es utilizada en ataques de *phishing* o campañas de distribución de *malware*. Este tipo de campañas maliciosas son enviadas por los ciberdelincuentes de manera masiva, es decir, sin objetivos concretos.

2

- ***Farming:*** en este caso los ciberdelincuentes emplean **más de una comunicación** con la víctima hasta conseguir su objetivo. El *farming* comúnmente es utilizado en campañas de sextorsión, fraude del CEO o de RR.HH.

2.1.1. Fases de un ataque de ingeniería social

Todos los ataques basados en ingeniería social comparten ciertas características que hacen que el ciclo de vida sea similar **[REF - 2]** para todos ellos. Saber cuáles son puede marcar la diferencia a la hora de identificar uno de estos ataques. Pueden distinguirse cuatro fases:

"Todos los ataques basados en **ingeniería social** comparten ciertas características que hacen que el **ciclo de vida** sea similar para todos ellos."

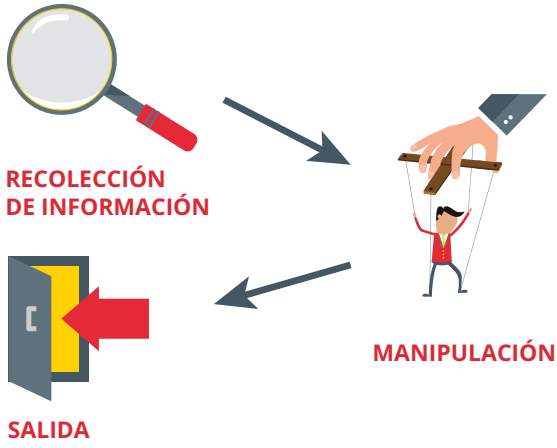


Ilustración 1 Fases de un ataque de ingeniería social

- **Recolección de información.** También conocida como fase de reconocimiento o *footprinting*, el ciberdelincuente recaba toda la información posible sobre las potenciales víctimas del fraude, como puede ser el correo electrónico, números de teléfono, nombres de dominio, etc.

- **Manipulación.** La manipulación psicológica es el punto clave en cualquier ataque de ingeniería social. Los ciberdelincuentes cuentan con muchas armas con las que manipular a la potencial víctima hasta conseguir sus objetivos como por ejemplo apelar a una supuesta urgencia o retirada de un servicio. Un tipo de manipulación llevada a cabo por los ciberdelincuentes consiste en establecer una relación de confianza mediante diferentes argucias, como nombres de dominio falsos o suplantando la identidad de una persona u organización de confianza.

- **Salida.** Fase final del ataque, una vez obtenido el objetivo el ciberdelincuente intentará hacer que el fraude no sea descubierto, ya que así el alcance será superior y por lo tanto tendrá un impacto mayor para la empresa.

2

En este vídeo **[REF - 3]** se muestra cómo un ataque basado en ingeniería social puede llegar a comprometer la seguridad de la empresa. El ataque en cuestión se realiza por medio de una llamada telefónica pero la base es la misma para cualquier ataque de ingeniería social.

2.2. El correo electrónico, principal medio de comunicación fraudulenta

Los ciberdelincuentes necesitan un medio de comunicación para propagar sus campañas fraudulentas, siendo el correo electrónico su preferido. Esto se debe principalmente a que **la gran mayoría de pymes y autónomos utilizan habitualmente el correo electrónico como herramienta de trabajo.** Esta frecuencia en su uso es lo que vuelve a esta herramienta peligrosa, ya que en muchas ocasiones las tareas se realizan de forma mecánica, lo que puede provocar infecciones por *malware* o accesos a páginas web fraudulentas.

Cuando se diseñó el correo electrónico no se establecieron medidas de seguridad, ya que no se pensaba que su uso se extendiera tanto. Esta falta de ciertas medidas de seguridad es aprovechada por los ciberdelincuentes para elaborar campañas de correos electrónicos fraudulentos más sofisticadas.

Algunas de las técnicas que usan los ciberdelincuentes para crear campañas maliciosas son:

- **Falsear la dirección del remitente (impersonalización).** En los correos electrónicos es posible **falsificar la dirección de correo electrónico del remitente, técnica a la que se denomina *email spoofing*** **[REF - 4]**. Al existir la posibilidad de falsificar la dirección del remitente, es posible hacerse pasar por una dirección de email legítima desde cualquier dominio web por otro que sirva para los propósitos de la campaña, como por ejemplo, el correo electrónico de un banco o cualquier, empresa, entidad u organización de confianza.

- ***Cybersquatting*** **[REF - 5]**. Esta técnica maliciosa es similar al *email spoofing*, ya que el propósito es suplantar el dominio web de una entidad reconocida. Pero al contrario que la técnica anterior, **el *cybersquatting* consiste en modificar ligeramente el nombre de dominio**, por ejemplo, el dominio «incibe.es» puede ser suplantado sustituyendo la segunda «i» por una «l», de tal manera que quedaría «inclbe.es». Si el usuario no es lo suficiente minucioso a la hora de inspeccionar dicha información, con total seguridad podrá ser engañado. El *cybersquatting* puede ser utilizado tanto para falsificar la dirección del remitente como los enlaces a páginas web que contengan los correos fraudulentos.

2

"Los **ataques de ingeniería social** pueden identificarse ya que generalmente todos ellos cuentan con **determinadas características.**"

» **Falsear enlaces.** Los correos fraudulentos suelen contener **enlaces falsificados que simulan enlazar a un sitio web legítimo cuando en realidad no es así.** Esta quizá sea la técnica más básica que pueden llevar a cabo los ciberdelincuentes, ya que es relativamente simple llevarla a cabo y obtiene grandes resultados.

» **Adjuntar documentos maliciosos.** En ocasiones las campañas maliciosas van acompañadas de adjuntos maliciosos que simulan ser ficheros legítimos, para ello pueden utilizar diferentes nombres de fichero que aparentan ser facturas, imágenes, documentación, etc. Otra técnica que utilizan es comprimir el archivo malicioso evitando que parezca *malware* cuando en realidad sí lo es. Además al comprimir los ficheros pueden pasar desapercibidos para los sistemas *antimalware*, lo que los vuelve aún más peligrosos. Habitualmente estas campañas hacen uso de las técnicas anteriores.

2.3. Pautas para identificar un ataque de ingeniería social

Los ataques de ingeniería social pueden identificarse ya que generalmente todos ellos cuentan con determinadas características **[REF - 6]**, que se explicarán a continuación:

» **Remitentes desconocidos**. Uno de los métodos más fiables y simples para comprobar si un correo puede ser legítimo o fraudulento, es analizar la dirección del remitente. En ocasiones, los ciberdelincuentes utilizan cuentas de correo que nada tienen que ver con la entidad a la que supuestamente representan, ya que trata de cuentas que han sido pirateadas o robadas previamente. Por ejemplo, recibir un correo de una supuesta entidad bancaria cuyo dominio web corresponde con cualquier otro tipo de empresa es una situación sospechosa, que indica un posible correo fraudulento. Cabe destacar que algunas organizaciones emplean para sus correos de promoción a empresas dedicadas al marketing por email, haciendo que la dirección del remitente y de la entidad a la que representa no correspondan, aunque estas comunicaciones suelen promocionar productos y servicios y no deberían solicitar accesos a áreas de administración.

2

- **Remitentes falseados.** Como se indicó en el apartado anterior, la dirección del remitente puede ser falseada suplantando a la entidad legítima. Comprobar si una dirección ha sido falseada es posible analizando las cabeceras del correo. Para ello tienes a tu disposición toda la información necesaria en el artículo ¿Dudas sobre la legitimidad de un correo? Aprende a identificarlos **[REF - 7]**. En otras ocasiones, el remitente del correo es falseado utilizando la técnica del *typosquatting* **[REF - 8]** y para evitarlo se debe comprobar minuciosamente el nombre de dominio ya que una simple letra podría ser el origen de un incidente de seguridad.

- **Comunicaciones impersonales.** En la mayoría de las ocasiones las comunicaciones fraudulentas recibidas por correo electrónico son impersonales, como por ejemplo «Estimado cliente, usuario, etc.». Las comunicaciones legítimas suelen ser personales, indicando el nombre de la persona o entidad a la que van dirigidas.

- **Adjuntos sospechosos.** Los ciberdelincuentes en ciertas ocasiones adjuntan en los correos ficheros maliciosos con los que infectar con *malware* los dispositivos de las víctimas. Se debe comprobar previamente la extensión del fichero adjunto, teniendo especial cuidado con las siguientes extensiones «.exe, .vbs, .msi, .vbs, .docm, .xlsm o .pptm». También se debe tener especial cuidado con los ficheros comprimidos que contengan un archivo con alguna de las extensiones anteriores.

- **Mala redacción.** Los ciberdelincuentes cada vez son más cuidadosos en la redacción de los correos, la presencia de faltas de ortografía y errores gramaticales se han vuelto más imperceptibles. La presencia de faltas de ortografía o errores gramaticales es un síntoma de comunicación fraudulenta, una entidad legítima suele cuidar mucho que las comunicaciones estén bien redactadas. A continuación se muestran dos correos fraudulentos, el primero muestra varios errores ortográficos algo que en la segunda muestra no se detecta.

2

Ilustración 2 Correo de tipo phishing con varios errores ortográficos y gramaticales

2

Illustración 3 Muestra de correo electrónico fraudulento sin errores ortográficos

2

- **Enlaces falseados.** Los correos electrónicos en ocasiones contienen enlaces que redirigen al usuario a una web fraudulenta, esos enlaces se pueden falsificar para que parezca que apuntan a una web legítima cuando en realidad no es así. Antes de acceder a un enlace, se debe verificar la web a la que redirige. Para ello, si se sitúa el ratón encima del vínculo se mostrará en la parte inferior de la pantalla el sitio al que realmente dirige. También se puede copiar el destino del enlace y pegarlo en un portapapeles para verificar el destino.

- **Firmas y otros elementos en la plantilla del correo.** Cuando se está acostumbrado a los correos de una entidad en concreto, es fácil identificar elementos comunes, como la firma de la parte inferior o el párrafo legal referente a la LOPDGDD «Ley orgánica de protección de datos y garantía de derechos digitales». Si esta firma o párrafo legal es diferente o directamente no está, podría ser un síntoma de que dicha comunicación probablemente sea fraudulenta.

3 PRINCIPALES FRAUDES Y AMENAZAS

Las ciberamenazas y fraudes que pueden afectar a empresas y autónomos son amplias, por ello conocer cuáles son, cómo identificarlas y qué hacer en caso de sufrir uno de estos incidentes de seguridad es muy importante para que la continuidad del negocio no se vea afectada. A lo largo de este punto mostramos los más relevantes y comunes.

Cuando se es víctima de cualquiera de los ataques que se enumeran a continuación, o cualquier otro tipo de fraude, es recomendable interponer una denuncia ante las Fuerzas y Cuerpos de Seguridad del Estado **[REF - 9]** (FCSE), aportando todas las pruebas disponibles **[REF - 10]**. También se puede reportar a INCIBE-CERT por medio del correo incidencias@incibe-cert.es para evitar que otros usuarios caigan en el fraude. Y ante cualquier duda, contactar con la Línea de Ayuda en Ciberseguridad de INCIBE, a través del número de marcación corta 017.

3.1. Fugas de información

Para la mayoría de empresas y autónomos la información que gestionan es uno de sus principales activos. Si por algún motivo esa información (datos personales, patentes, etc.) se filtrara o hiciera pública, las consecuencias para el negocio podrían tener un gran impacto.

3.1.1. ¿Qué es una fuga de información?

Una fuga de información o fuga de datos se produce cuando se pierde la confidencialidad de la información de la empresa. Dicha información solamente debería ser accesible el grupo de usuarios autorizado dentro de la organización. El problema se materializa cuando debido a un incidente de seguridad, dicha información es accesible por terceras personas no autorizadas.

3

Las fugas de información se pueden producir de dos formas diferentes **[REF - 11]**:

- **Involuntariamente.** Aunque la creencia popular supone que el motivo principal de las fugas de información está motivado por el acceso de un ciberdelincuente a la red de la empresa, en muchas ocasiones el origen de la fuga se produce de forma involuntaria y no intencionada por parte de los empleados. Algunas causas que pueden llevar a estas situaciones pasan, por ejemplo, por enviar un correo a múltiples destinatarios sin utilizar la función de copia oculta **[REF - 12]** (CCO) o perder un dispositivo móvil o de almacenamiento (USB o disco duro) con información confidencial o personal sin cifrar.

- **Deliberadamente.** En otras ocasiones, las fugas de información se producen de manera deliberada o intencionada por parte de un ciberdelincuente que ha conseguido acceso a alguno de los sistemas de la empresa, o también por lo que conocemos como "*insider* **[REF - 13]**". Esto es que un exempleado con acceso, o empleado descontento, por diferentes motivos, como vender la información, una patente, etc., o generar una pérdida de reputación a la empresa, realiza estas acciones.

3.1.2. Escenarios posibles

La información puede ser extraída de la empresa de multitud de formas diferentes, algunas de las más comunes son:

- **Dispositivos móviles y de almacenamiento externo.** Ordenadores portátiles, *smartphones*, *tablets*, discos duros externos o una simple memoria USB. Todos estos dispositivos pueden ser el origen de una fuga de información si son extraviados o robados y la información que contienen no se encuentra cifrada **[REF - 14]** mediante un algoritmo con una contraseña robusta.

- **El correo electrónico.** Desde ataques dirigidos basados en ingeniería social hasta fugas de información involuntaria causadas por la función de autocompletar el destinatario o la no utilización de la CCO. El correo electrónico es una de las herramientas más utilizada en entornos empresariales pero también puede ser el origen de una fuga de información.

- **Redes inalámbricas no confiables.** Las redes inalámbricas públicas o sin las suficientes medidas de seguridad pueden ser aprovechadas por ciberdelincuentes para robar la información que por ella se transmite.

- **Aplicaciones.** Ciertas herramientas, como las aplicaciones de almacenamiento en la nube o las herramientas colaborativas **[REF - 15]**, pueden ser el origen de un incidente. Si estas herramientas no son utilizadas adecuadamente, o se utilizan sin el consentimiento de la empresa, pueden suponer una fuga de información.

3

- **Redes sociales.** Publicar información confidencial, aunque sea involuntariamente, puede ser el origen de un incidente de seguridad si los ciberdelincuentes acceden a ella. Por ejemplo, publicar una imagen en la que se visualizan nombres de usuario o información confidencial.

- **Malware.** Troyanos, *spyware*, *keyloggers*, etc. La infección por cualquier tipo de *software* malicioso podría suponer que la información de la empresa se vea comprometida y caiga en manos de los ciberdelincuentes.

- **Credenciales de acceso inseguras.** Utilizar nombres de usuario por defecto y contraseñas débiles (fáciles de adivinar) o por defecto en los sistemas son un riesgo. Cuando se utilizan credenciales poco robustas, sin una longitud y tipo de caracteres apropiados, los ciberdelincuentes podrían llegar a descubrirlas fácilmente. De la misma forma, si se usan credenciales por defecto estas pueden encontrarse generalmente en los manuales publicados en Internet por el desarrollador.

3.1.3. ¿Qué hacer en caso de sufrir una fuga de información?

Las fugas de información deben gestionarse adecuadamente, **una gestión inadecuada puede magnificar el efecto negativo del incidente**. El plan que se propone a continuación ha sido obtenido de la guía "Cómo gestionar una fuga de información, una guía de aproximación al empresario **[REF - 16]**". La gravedad del incidente y el contexto en el que se produzca hace que los diferentes pasos se adapten al escenario específico.

Cuando una fuga de información afecta a datos personales[1] **[REF - 17]**, **la empresa está obligada a notificar el incidente a la Agencia Española de Protección de Datos, autoridades pertinentes u organismos equivalentes [REF - 18], y a las personas cuyos datos se hayan visto afectados** para que puedan tomar las medidas oportunas en un **plazo máximo de 72 horas** desde su conocimiento.

1 Toda información sobre una persona física identificada o identificable («el afectado»). Se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.

3

1 Fase inicial	» Detección del incidente » Alerta del incidente a nivel interno » Inicio del protocolo de gestión
2 Fase de lanzamiento	» Reunión del gabinete de crisis » Informe inicial de situación » Coordinación y primeras acciones
3 Fase de auditoría	» Auditoría interna y externa » Elaboración de informe preliminar
4 Fase de evaluación	» Reunión del gabinete de crisis » Presentación del informe de auditoría » Determinación de principales acciones » Tareas y planificación
5 Fase de mitigación	» Ejecución de todas las acciones del plan
6 Fase de seguimiento	» Valoración de los resultados del plan » Gestión de otras consecuencias » Auditoría completa » Aplicación de medidas y mejoras

Tabla 1 Resumen de acciones para gestionar una fuga de información

3.1.4. ¿Cómo reducir el riesgo?

Para prevenir las fugas de información, se deben aplicar medidas tanto a nivel organizativo, como técnico y legal. El conjunto de estas medidas reducirá la posibilidad de sufrir un incidente que afecte a la confidencialidad de la información.

» **Medidas organizativas.** Este tipo de medidas de seguridad afectan a la metodología de trabajo y organización con la que cuenta la empresa. Las más destacadas son:

- Definir una política de seguridad y procedimientos para todo el ciclo de vida de los datos **[REF - 19]**.
- Establecer un sistema de clasificación de la información **[REF - 20]**, para ligarlo a roles y niveles de acceso.
- Llevar a cabo acciones de formación y concienciación en ciberseguridad **[REF - 21]**.
- Implantar un sistema de gestión de seguridad de la información **[REF - 22]**.

3

» **Medidas técnicas.** Estas medidas tendrán como objetivo limitar los accesos no autorizados a la información, tanto por ciberdelincuentes como por los propios empleados, mediante una serie de herramientas *software*:

- Implantar un sistema de control de acceso e identidad **[REF - 23]**.
- Soluciones *anti-malware* **[REF - 24]** y anti-fraude, seguridad perimetral y protección de las telecomunicaciones.
- Control de contenidos, monitorización de tráfico y copias de seguridad **[REF - 25]**.
- Control de acceso a los recursos, actualizaciones de seguridad y parches.
- Implantar herramientas DLP **[REF - 26]** *(Data Loss Prevention).*

» **Medidas legales.** Las medidas legales servirán a la empresa para seguir la legislación vigente y poder tomar medidas contra empleados que filtren información deliberadamente:

- Establecer acuerdos de confidencialidad **[REF - 27]**.
- Solicitud de aceptación de la política de seguridad y de la de conformidad por parte de los empleados.
- Medidas relativas a la adecuación y cumplimiento de la legislación aplicable (LOPDGDD, LSSI, etc.).
- Cualquier otra medida de carácter disuasorio en base a la legislación vigente.

3.2. Ataques de tipo *phishing*

Los ataques de tipo *phishing* son el principal método utilizado por los ciberdelincuentes para robar información confidencial, como nombres de usuario y contraseñas o datos bancarios.

3.2.1. ¿Qué es un *phishing*?

Un *phishing* es un tipo de fraude cometido generalmente a través del correo electrónico, aunque pueden utilizar otros medios, como mensajes SMS (*smishing*), redes sociales, aplicaciones de mensajería instantánea o llamadas telefónicas (*vishing*), cuyo objetivo

3

principal es **robar información confidencial y credenciales de acceso.** Para lograr engañar a la víctima, los ciberdelincuentes suelen **suplantar la identidad de empresas y organizaciones reconocidas**, comúnmente aquellas de las que pretenden robar la información, como por ejemplo entidades bancarias, empresas del sector de la energía, de logística, etc.

Como técnica principal, los ciberdelincuentes suelen **falsear la dirección del remitente,** como ya se comentó en el apartado de ingeniería social, para que simule proceder de la entidad legítima cuando en realidad el mensaje procede de otra fuente. A esta técnica se la denomina *email spoofing* o suplantación de la dirección correo electrónico **[REF - 28]**.

Los ataques de tipo *phishing*, además del correo electrónico falso, **comúnmente, en el cuerpo del mensaje contienen un enlace que lleva a una página web fraudulenta** que tiene la misma estética que la página web legítima a la que intenta suplantar. En dicha web fraudulenta se solicita la información confidencial que se quiere sustraer, generalmente información personal, credenciales de acceso e información financiera. Para ofrecer más veracidad, **la web fraudulenta suele utilizar un nombre de dominio similar al legítimo**, siempre buscando como objetivo que las potenciales víctimas caigan en el engaño.

Una vez que la víctima del ataque ha facilitado toda la información que los ciberdelincuentes solicitan en la web fraudulenta, **el usuario suele ser redirigido a la página web legítima de la empresa suplantada con el fin de que el fraude pase el mayor tiempo desapercibido antes de que la víctima denuncie el hecho.**

3

En la sección "Avisos de seguridad" **[REF - 29]** se publican regularmente alertas de ciberseguridad entre las que se incluyen campañas de *phishing* **[REF - 30]**. Algunos ejemplos de comunicaciones fraudulentas de esta tipología son:

Ilustración 4 Campaña de correos fraudulentos solicitando el pago de un supuesto paquete

3

Ilustración 5 Campaña de phishing solicitando información confidencial alegando un supuesto fortalecimiento de la seguridad

3

Ilustración 6 Campaña de phishing por SMS

3

3.2.2. ¿Cómo identificar un ataque de *phishing* y poder prevenirlo?

Los ataques de tipo *phishing* suelen contener factores que facilitan su detección, y por lo tanto poder evitar ser víctima de este tipo de fraude. Los principales aspectos a analizar son:

Illustración 7 Ejemplo de correo electrónico fraudulento

» **Remitente**. Los correos de tipo *phishing* en ocasiones contienen **remitentes que no coinciden con la organización a la que supuestamente representan**, este es el primer indicador que ha de comprobarse. Por ejemplo, un correo que supuestamente procede de una entidad bancaria tendría un remitente cuyo dominio coincidiría con la entidad a la que representa, si dicho dominio no coincide es un síntoma de fraude.

En otras ocasiones los ciberdelincuentes utilizan la **técnica *email spoofing***, que consiste en falsear el remitente haciendo que parezca proceder de la entidad

3

legitima cuando en realidad no es así. Para **comprobar si el remitente realmente es el que figura en el correo** se deben analizar las cabeceras del mismo, para ello puedes seguir las instrucciones facilitadas en el artículo ¿Dudas sobre la legitimidad de un correo? Aprende a identificarlos **[REF - 7]**.

» **Necesidad de llevar a cabo la petición de manera urgente.** La ingeniería social es el componente esencial en los correos electrónicos de tipo *phishing*. Los ciberdelincuentes suelen **alertar a las víctimas sobre situaciones negativas** a las que tendrán que hacer frente a no ser que sigan las instrucciones que facilitan, las cuales suelen ser acceder a una página web fraudulenta e introducir la información que solicitan, visualizar un archivo (malicioso), etc. Algunos de los ganchos más utilizados son la cancelación del servicio o cuenta, multas, sanciones por no acceder en tiempo y forma, etc. Son muchas las artimañas utilizadas cuyo fin es forzar al usuario a realizar una determinada acción a través de una coacción. Durante la pandemia sufrida por el COVID-19 los ciberdelincuentes se adaptaron para utilizar señuelos basados en esta temática y cualquier aspecto que pudiera englobarla, como los ERTE, ayudas gubernamentales, remedios milagrosos, posibles sanciones, e incluso multas de tráfico cuando comenzaba la movilidad entre comunidades. Todos ellos fueron recopilados por INCIBE bajo la etiqueta #CiberCOVID19 **[REF - 31]**.

» **Enlaces falseados.** Los enlaces ofuscados son una parte fundamental de este tipo de fraude. En la mayoría de las ocasiones es la vía esencial que utilizan los ciberdelincuentes para robar la información confidencial. **Los enlaces suelen aparentar que corresponden a la web legítima o sencillamente contienen un texto haciendo referencia a que sea seleccionado o *"clicado"***. Para comprobar a dónde apunta realmente el enlace, se puede situar el ratón encima y comprobar el cuadro de dialogo que figura en la parte inferior de la pantalla con la verdadera dirección. También se pueden utilizar herramientas online, como:

- Informe de transparencia de Google **[REF - 32]**
- *Free website security check & malware scanner* **[REF - 33]**
- Virustotal **[REF - 34]**
- URL haus **[REF -35]**

3

En otras ocasiones los enlaces pueden estar acortados, no siendo posible visualizar su destino si no se utilizan herramientas específicas como:

- Unshorten.It! **[REF - 36]**

Se ha de tener especial cuidado al acceder a enlaces en correos electrónicos, siendo preferible acceder introduciendo la dirección web directamente en el navegador o utilizando la aplicación oficial de la entidad. Las entidades legítimas, como las financieras, nunca solicitarán a los clientes credenciales de acceso en comunicaciones por correo electrónico.

- **Comunicaciones impersonales.** Las comunicaciones de entidades legítimas suelen referirse a su destinatario utilizando nombre y apellidos, por el contrario los ciberdelincuentes no suelen conocer esos datos personales por lo que las comunicaciones son impersonales. Recibir un mensaje procedente de una supuesta organización de la que se es cliente y que no contenga datos personales, como nombre y apellidos, es un síntoma de fraude.

- **Errores ortográficos y gramaticales.** Una auténtica comunicación de cualquier entidad no contendrá errores ortográficos o gramaticales, ya que la comunicación con sus clientes es un aspecto muy cuidado.

- **Firmas y estética del correo.** La estética y la firma del correo electrónico es otro factor a considerar. Cuando se está familiarizado con los correos de una determinada organización y una comunicación no sigue ese patrón, es un síntoma de fraude.

En caso de no haber detectado el ataque en la comunicación, es posible identificarlo por la web fraudulenta a la que redirige. Para ello lo principal es **analizar el nombre de dominio web y su certificado digital**, ya que estos son datos que no pueden ser falsificados fácilmente. Puedes aprender a identificar enlaces fraudulentos por medio del **recurso formativo 04 El correo electrónico, Principales fraudes y riesgos disponible en el Kit de concienciación [REF - 21]**.

3.2.3. ¿Qué hacer en caso de sufrir un ataque de *phishing*?

Cuando se es víctima de un ataque de *phishing*, lo principal, si se han introducido las credenciales en el sitio malicioso, es **modificar la contraseña de acceso del servicio suplantado y cualquier otro servicio en el que se utilicen las mismas credenciales**. También es importante **contactar con la entidad suplantada y con INCIBE-CERT [REF - 37]** para que esté informada de lo sucedido y pueda adoptar las medidas necesarias para proteger la información de sus clientes.

3

3.3. Fraude del CEO (*spear phishing*)

El fraude del CEO, *spear phishing* o BEC por sus siglas en inglés *Bussines Email Compromise*, consiste en una técnica llevada a cabo por los ciberdelincuentes para robar fondos de las empresas suplantando la identidad de un alto directivo.

3.3.1. ¿Qué es el fraude del CEO?

El fraude del CEO se trata de un ataque dirigido contra una víctima en concreto, de la cual se ha recopilado información previamente por distintos medios, como la página web corporativa, redes sociales "profesionales" o cualquier otro medio, cuyo objetivo es hacer que el ataque sea más creíble.

"El fraude del CEO, *spear phishing* o BEC por sus siglas en inglés *Business Email Compromise*, consiste en robar fondos de las empresas suplantando la identidad de un alto directivo "

En este fraude se atacan 2 objetivos de la misma organización: un alto directivo de la empresa y un empleado con capacidad para poder realizar transferencias bancarias. **Los ciberdelincuentes suplantan la identidad de un alto directivo y solicitan a un empleado, con capacidad de realizar transacciones financieras, una transferencia de dinero**, que generalmente suele ser de un monto importante, alegando cerrar una operación reseñable en la que se está trabajando. Las comunicaciones suelen producirse por medio del correo electrónico y utilizando direcciones falseadas, *email spoofing* o *typosquatting*, y la misma estética utilizada habitualmente, aunque a veces se usa la dirección legítima del directivo que previamente se ha comprometido. Esta técnica suele ser llevada a cabo por los ciberdelincuentes, coincidiendo con la ausencia del directivo suplantado de la sede, debido a viajes de negocio o cualquier otra eventualidad. Así se dificulta verificar la comunicación.

El empleado, al comprobar que la comunicación proviene de un alto directivo, no suele dudar de la solicitud y realiza la transferencia bancaria, produciéndose finalmente el fraude. En muchas ocasiones la solicitud de transferencia va acompañada de una **petición de urgencia y confidencialidad**, buscando como objetivo que el empleado no se comunique con otros compañeros y que el fraude se realice con la mayor brevedad posible.

3

Este tipo de ataques dirigidos suelen estar orientados a organizaciones de tamaño medio o grande, donde el rédito económico es mayor.

En el artículo del blog Historias reales: el fraude del CEO **[REF - 38]** se muestra el caso de una empresa que sufrió este tipo de ataque y las consecuencias que pudo llegar a tener para la organización en caso de haberse perpetrado.

A continuación se muestra el flujo de correos de uno de estos ataques, en el que se sigue la mecánica indicada en la Ilustración 1 Fases de un ataque de ingeniería social:

De: [redacted]
Enviado el: miércoles, 30 de septiembre
Para: [redacted]
Asunto: Confidencial

Hola [redacted],

Necesito tu ayuda para una operación financiera confidencial.

¿Puedo contar con tu discreción?

(Tenemos que hablar solamente por mail)

Cordialmente.

[redacted]

Ilustración 8 Correo inicial del ataque del fraude del CEO

De: [redacted]
Enviado el: miércoles, 30 de septiembre
Para: [redacted]
Asunto: RE: Confidencial

Por supuesto, [redacted]

Cuenta conmigo absolutamente.

Ya me indicarás.

Un abrazo.

[redacted]

Ilustración 9 Respuesta del empleado objetivo del ataque del fraude del CEO

3

De: [redacted]
Enviado el: miércoles, 30 de septiembre
Para: [redacted]
Asunto: RE: Confidencial

Perfecto [redacted].

Estamos en este momento efectuando una operación financiera en relación con la adquisición de una empresa.

En esta etapa, esta operación debe permanecer estrictamente confidencial, no debes hablar de esto con nadie de momento en la empresa ya sea por teléfono o de viva voz.

El anuncio de esta adquisición tendrá lugar el día 30 en nuestra instalaciones y en presencia de toda la administración implicada.

Serás mi contacto con el fin de finalizar la transacción, algo importantísimo para nuestra empresa.

¿Cuál es el saldo bancario actual?

Cordialmente.

[redacted]

Ilustración 10 Continuación del ataque del fraude del CEO.

En el fraude del CEO **[REF - 39]**, la comunicación terminaría ofreciendo información relativa al saldo disponible por parte de la empresa y solicitando una transferencia acorde al balance positivo, por parte del ciberdelincuente, a una cuenta controlada por él.

3.3.2. ¿Cómo identificar un ataque de fraude del CEO y poder prevenirlo?

Para poder identificar uno de estos fraudes, se deben seguir estos pasos:

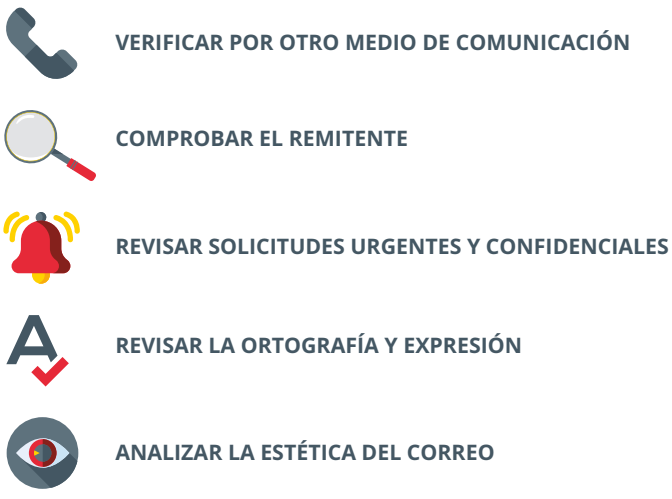


Ilustración 11 Pautas para identificar fraudes del CEO

3

- **Verificar por otro medio de comunicación.** Es recomendable no responder nunca al correo recibido y siempre verificar la solicitud por otro canal de comunicación, como puede ser un nuevo correo electrónico a otro empleado de la organización, una llamada por teléfono o a través de aplicaciones de mensajería instantánea, etc. Esta es la mejor opción para verificar de forma inequívoca si la comunicación es un fraude o es legítima. En algunas ocasiones los ciberdelincuentes utilizan tecnologías basadas en la inteligencia artificial para simular la voz del directivo **[REF - 40]** y así dotar de un extra a la comunicación fraudulenta.

  Un método utilizado en diferentes organizaciones para autorizar operaciones sensibles, como una importante transferencia bancaria, consiste en utilizar un código secreto que únicamente estará en posesión del personal autorizado a realizar transferencia y los altos directivos. De esta forma se podrá verificar si la comunicación es legítima o no. Este código es recomendable que sea renovado periódicamente.

- **Comprobar el remitente.** Este es el primer factor a analizar, un remitente cuyo nombre de dominio no coincida con el corporativo es un síntoma de fraude. En ocasiones los ciberdelincuentes pueden utilizar diferentes técnicas, como es el *cybersquatting*, para comprar dominios similares al de la empresa con el fin de engañar a los objetivos del ataque. También pueden utilizar la técnica del *email spoofing* por lo que conviene verificar la procedencia del correo en caso de tratarse de solicitudes inusuales o que impliquen cualquier tipo de transferencia bancaria.

- **Revisar solicitudes urgentes y confidenciales.** Cualquier solicitud que provenga de un alto directivo, que vaya acompañada de urgencia y confidencialidad, debe poner en alerta a los empleados, ya que puede tratarse de un intento de fraude.

- **Revisar la ortografía y expresión.** En ocasiones los correos recibidos contienen faltas de ortografía o expresiones poco comunes o inusuales, como las generadas por traductores automáticos.

- **Analizar la estética del correo.** Generalmente los correos de una organización en concreto siempre utilizan la misma estética, como sellos, logotipos, información legal, etc. Cuando uno de estos elementos difiere de los habituales, es un síntoma de correo fraudulento salvo que se haya comprometido la cuenta de correo del directivo suplantado.

3

3.3.3. ¿Qué hacer en caso de sufrir un ataque de fraude del CEO?

En caso de sufrir un incidente de este tipo se recomienda interponer una denuncia ante las Fuerzas y Cuerpos de Seguridad del Estado **[REF - 9]**, aportando todas las pruebas posibles. También es recomendable ponerse en contacto con la entidad bancaria informándoles de lo sucedido ya que puede darse la situación de que sea posible cancelar la transferencia.

3.4. Fraude de RR.HH.

El fraude de RR.HH. **[REF - 41]** utiliza técnicas similares al fraude del CEO pero en esta ocasión las víctimas son el personal de recursos humanos de la empresa y un empleado al que suplantan su identidad.

3.4.1. ¿Qué es el fraude de RR.HH?

En la comunicación, **el ciberdelincuente se hace pasar por un empleado de la empresa y solicita que el siguiente ingreso correspondiente a su nómina se realice a un nuevo número de cuenta** controlado por el estafador.
Para perpetrar el ataque, los ciberdelincuentes han realizado un estudio previo de la empresa víctima, identificando a los empleados del departamento de RR.HH., los empleados con los que cuenta la empresa, la entidad financiera con la que trabaja y las cuentas de correo electrónico utilizadas. Al igual que otros tipos de fraudes, para dotar de más veracidad a la comunicación fraudulenta, los ciberdelincuentes utilizan técnicas de *email spoofing* o *cybersquatting*.

Ilustración 12 Correo de tipo fraude de RR.HH.

> "En caso de sufrir un incidente de este tipo se recomienda interponer **una denuncia ante las Fuerzas y Cuerpos de Seguridad del Estado"**

3

La sextorsión es un tipo de estafa en la que los ciberdelincuentes informan a la víctima por correo electrónico de que ha sido grabada en **situaciones comprometedoras, que serán difundidas entre sus contactos de correo electrónico y redes sociales** a no ser que realice un pago a modo de rescate.

3.4.2. ¿Cómo identificar un ataque de fraude de RR.HH. y poder prevenirlo?

Las pautas para identificar este tipo de estafa son similares al fraude del CEO, siendo la principal diferencia la solicitud de cambio de cuenta bancaria por un empleado de la organización. **Ante cualquier correo que parezca proceder de un empleado de la empresa, se debe verificar dicha solicitud mediante otro medio de comunicación, como una llamada telefónica o presencialmente**, así se podrá verificar sin ninguna duda si el cambio de cuenta bancaria es legítimo o no.

3.4.3. ¿Qué hacer en caso de sufrir un ataque de fraude de RR.HH?

Es recomendable interponer una denuncia ante las Fuerzas y Cuerpos de Seguridad del Estado **[REF - 9]**, aportando todas las pruebas posibles y contactar con la entidad bancaria para que estén al tanto de lo sucedido. También se debe cambiar el número de cuenta fraudulento por el legítimo, en caso de que se haya modificado.

3.5. Sextorsión

La sextorsión es un tipo de estafa en la que los ciberdelincuentes informan a la víctima por correo electrónico de que ha sido grabada en situaciones comprometedoras, que serán difundidas entre sus contactos de correo electrónico y redes sociales a no ser que realice un pago a modo de rescate.

3.5.1. ¿Qué es la sextorsión?

Las campañas fraudulentas de sextorsión suelen contener mensajes bastante elaborados en los que se informa al usuario de que su dispositivo ha sido comprometido o hackeado. Durante ese supuesto periodo de hackeo, el ciberdelincuente ha conseguido acceder a la cámara, micrófono, pantalla y la lista de contactos. El ciberdelincuente asegura tener un video privado comprometedor, que difundirá entre los contactos de la víctima a no ser que realice un pago en criptomonedas **[REF - 42]** en un periodo de tiempo determinado.

3

Para dotar de más veracidad a **la comunicación, el correo suele simular proceder de la dirección de la víctima** (*email spoofing*), al igual que en otras comunicaciones fraudulentas, cuando en realidad el correo no procede de ahí. Para dotar de más veracidad al fraude, los ciberdelincuentes pueden indicar en la comunicación la contraseña de algún servicio que se ha filtrado previamente y cuyo descifrado ha sido posible.

Los siguientes ejemplos muestran comunicaciones de sextorsión.

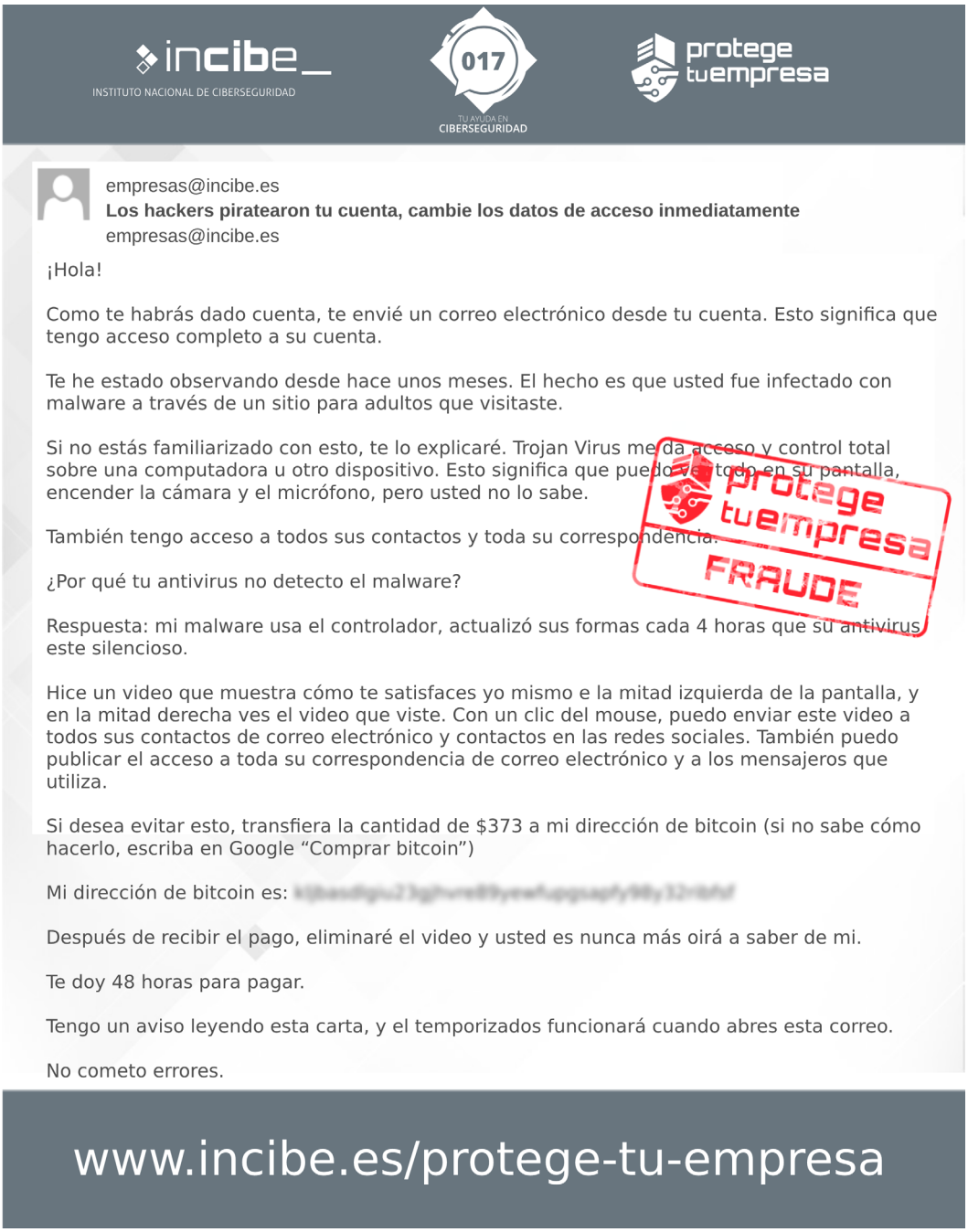


Ilustración 13 Correo electrónico de sextorsión

3

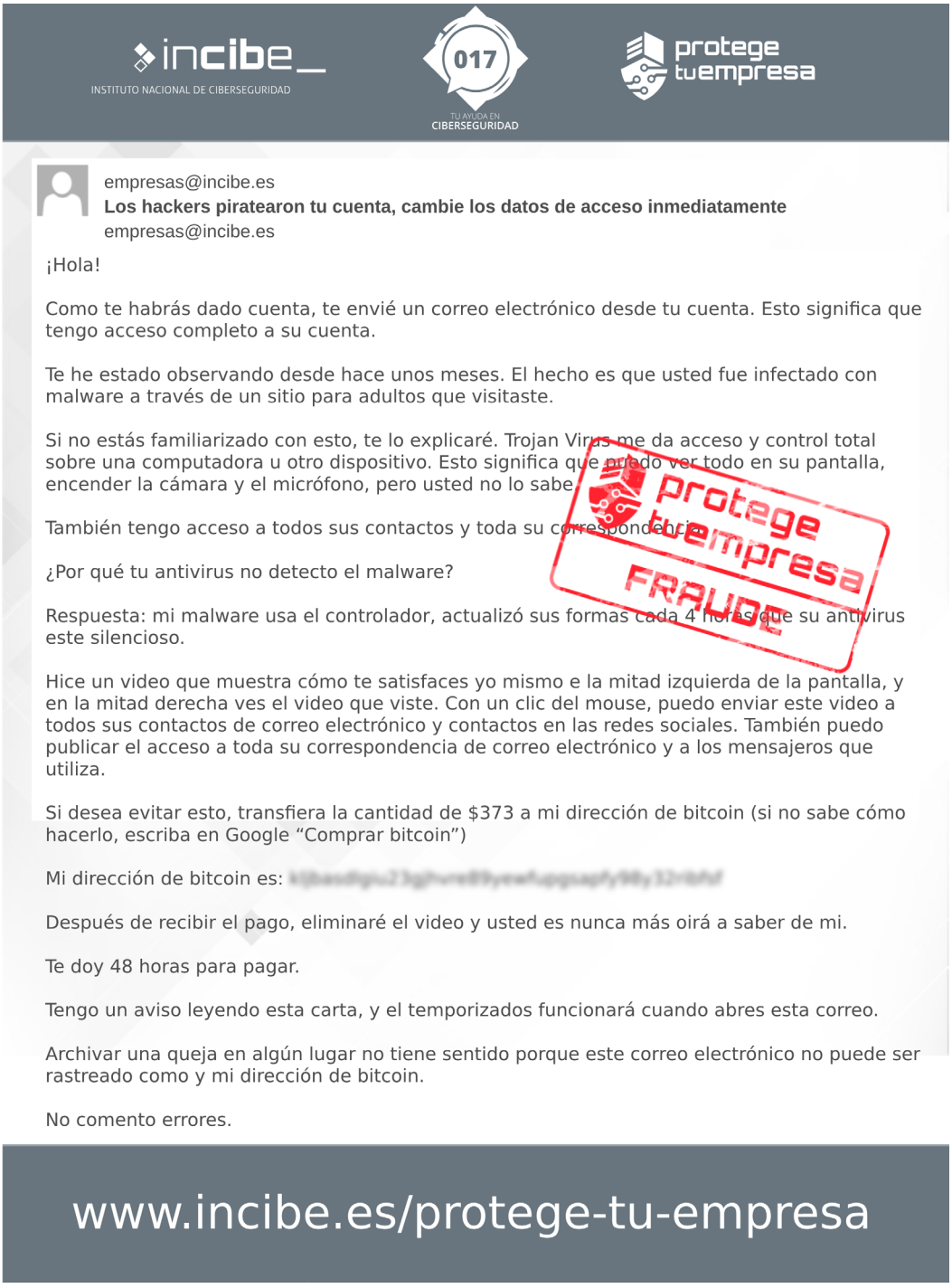


Ilustración 14 Segunda muestra de sextorsión

3.5.2. ¿Cómo identificar un ataque de sextorsión y poder prevenirlo?

Los ataques de sextorsión son fácilmente identificables ya que todos cuentan con características en común:

- **Los correos simulan proceder de la cuenta de la víctima,** lo que en realidad no es así. El correo procede de otra cuenta de correo pero la dirección del remitente está falsificada. También pueden indicar la contraseña de algún servicio asociado a la cuenta de la víctima, que se ha filtrado previamente y ha sido posible su descifrado.

- **Asunto alarmante que informa sobre que la cuenta o dispositivo ha sido comprometido.** Como técnica de ingeniería social los ciberdelincuentes informan de que han comprometido la cuenta o el dispositivo, cuando en realidad no es así.

- En el correo se informa de que el **dispositivo ha sido infectado por *malware* y ahora está bajo el control de ciberdelincuente**. También se informa de que ha realizado una **grabación comprometida de la víctima** y que no será difundida a cambio de un **rescate pagado en criptomonedas. Dicha grabación tampoco existe, es solamente una técnica de ingeniería social para forzar a la víctima a pagar.**

3.5.3. ¿Qué hacer en caso de sufrir un ataque de sextorsión?

En caso de recibir uno correo de sextorsión, **se debe hacer caso omiso a sus demandas y nunca pagar el rescate. Ni el dispositivo está infectado con *malware*, ni se ha realizado ninguna grabación comprometida**. Se debe eliminar de la bandeja de correo para evitar equivocaciones y notificar la incidencia a INCIBE-CERT para que puedan tomar las acciones necesarias para mitigar la campaña maliciosa.

3

"Para proteger la web corporativa, se debe contar con una **política de seguridad adecuada**"

3.6. Ataques contra la página web corporativa

La página web de la empresa es un activo importante, los ciberdelincuentes buscarán atacarla por diversos motivos, como es hacerse con información confidencial, utilizarla para perpetrar nuevos ataques o simplemente para dañar la imagen de la organización.

3.6.1. ¿Qué es un ataque contra la página web corporativa?

La página web corporativa es el escaparate de la empresa hacia Internet, permitiendo ofrecer servicios y productos de manera global. Disponer de un portal web funcional, seguro y que cumpla las necesidades de los trabajadores y clientes es imprescindible para las organizaciones.

Las páginas web de las empresas son un objetivo de los ciberdelincuentes, desde aquellos cuyo único objetivo es vulnerar su seguridad, como entretenimiento, hasta aquellos que buscan un beneficio económico. Los incidentes de seguridad cuyo origen está en la página web de la empresa se producen principalmente por los siguientes motivos:

- **Vulnerabilidades no parcheadas.** Una vulnerabilidad consiste en un fallo o deficiencia en un *software* que puede permitir a un usuario no legítimo, como un ciberdelincuente, llevar a cabo acciones no autorizadas, como robar información. Las páginas web, como cualquier otra clase de *software*, pueden contar con vulnerabilidades. Si estas no son parcheadas, podrían llegar a ser explotadas por los ciberdelincuentes en su propio beneficio.

- **Malas configuraciones.** Aplicar malas configuraciones a la página web, como permitir contraseñas simples, no aplicar sistemas de verificación tipo *captcha* **[REF - 43]**, o mostrar más información que la estrictamente necesaria cuando se produce un error, puede suponer también el origen de un incidente de seguridad.

3

- **Errores de diseño.** Cuando un portal web no está diseñado siguiendo unos estándares de seguridad, como es el elaborado por la Fundación OWASP **[REF - 44]**, puede que contenga errores de diseño, los cuales pueden ser explotados por los ciberdelincuentes.

Los incidentes de seguridad provocados por alguna de las razones anteriores pueden derivar en diversas situaciones que pueden comprometer la seguridad y privacidad de la empresa y de sus clientes:

- **Fugas de información.** Un incidente que afecte a la página web corporativa puede ser el origen de una fuga de información **[REF - 16]** ya que los ciberdelincuentes pueden llegar a exfiltrar tanto información confidencial de la empresa como de su personal y clientes.

- **Denegaciones de servicio.** Una denegación de servicio **[REF - 45]** o DoS, por sus siglas en inglés (*Denial of Service*), se entiende como un conjunto de técnicas que tienen por objetivo dejar un servidor inoperativo. Este tipo de ataques provocan que tanto clientes como trabajadores no puedan interactuar con la página web de forma normal, lo que provocaría una pérdida de rendimiento y reputación.

- **Como origen de otro incidente de seguridad.** Cuando un ciberdelincuente vulnera la seguridad de la página web corporativa, puede llegar a comprometer otros sistemas de la organización, como el correo electrónico, dispositivos como ordenadores o aparatos IoT (*Internet of Things*), llevar a cabo ataques de tipo *ransomware*, etc.

- ***Defacement*** **[REF - 46]** Este tipo de ataque consiste en cambiar la apariencia de la página web corporativa por otra a elección del ciberdelincuente como reivindicación política, alardear o simplemente dañar la reputación de la organización.

- **Como herramienta para atacar a otros usuarios.** Una técnica muy utilizada por los ciberdelincuentes es vulnerar la seguridad de páginas web legítimas, y utilizarlas como trampolín para perpetrar otros fraudes, como puede ser distribuir *malware* o alojar una campaña de *phishing*.

3

3.6.2. ¿Cómo evitar los ataques contra la página web corporativa?

Para proteger la web **[REF - 47]** corporativa reduciendo el riesgo de que los ciberdelincuentes puedan vulnerar su seguridad y comprometer la privacidad y seguridad de la empresa, se debe contar con una política de seguridad **[REF - 48]** adecuada. Esta política debe contemplar los siguientes puntos:

- **Certificado SSL.** Un certificado SSL **[REF - 49]** o también conocido como certificado web sirve para proteger las comunicaciones que se establecen entre la página web corporativa y el dispositivo del usuario, evitando que los ciberdelincuentes puedan robar la información en tránsito, como por ejemplo, nombres de usuario y contraseñas. Los certificados SSL también sirven para **identificar la web de forma inequívoca** generando así confianza entre los clientes. Además, muchos navegadores marcan los sitios web sin certificado SSL, cifrado anticuado **[REF - 50]**, estar firmado por una entidad no reconocida o que cuenten con un certificado caducado como sitios inseguros, por lo que siempre es recomendable tener uno instalado.

- **Actualizaciones de seguridad.** La gran mayoría de páginas web están diseñadas usando gestores de contenido o CMS por sus siglas en inglés (*Content Management System*). Dichos CMS publican regularmente actualizaciones de seguridad que corrigen las vulnerabilidades descubiertas, además de dotar de nuevas características al gestor. Siempre se debe contar con la última versión disponible del CMS, además también se debe tener actualizado el resto de componentes que conforman el gestor, como son los *plugins* y temas utilizados. Si cuentas con Wordpress como gestor de contenidos, puedes seguir las recomendaciones de seguridad disponibles en los artículos y en nuestra sección de avisos:

  - Medidas de seguridad avanzadas en WordPress I **[REF - 51]**
  - Medidas de seguridad avanzadas en WordPress II **[REF - 52]**
  - Gestor de contenidos **[REF - 53]**

- **Contraseñas robustas.** La contraseña junto con el nombre de usuario conforma en la mayoría de los casos la única puerta de entrada al área de administración o *backend*. Es importante que las contraseñas de acceso sean lo más robustas posibles **[REF - 54]**, para ello deben contar con mayúsculas, minúsculas, números y símbolos, y con una longitud mínima de 8 caracteres, siempre teniendo en cuenta que cuantos más caracteres mejor. Para que los usuarios no hagan uso de credenciales de acceso

3

débiles, es recomendable establecer mecanismos que no permitan utilizar contraseñas sin unos mínimos de seguridad. Para dotar de un extra de seguridad a la página web, se puede establecer un mecanismo por el que, ante determinados intentos erróneos de acceso, se inhabilite al usuario asociado durante un determinado tiempo, que se incrementará exponencialmente si continúan los intentos fallidos. Además, se puede habilitar un doble factor de autenticación de tal forma que además de estar en conocimiento de usuario y contraseña, sea necesario un tercer factor que solamente deberá conocer el usuario legítimo, como puede ser una clave OTP (*One Time Password*) o cualquier otro sistema.

- **Copias de seguridad.** Las copias de seguridad **[REF - 26]** son fundamentales en cualquier entorno corporativo y la página web de la empresa no es una excepción. Se deben realizar copias periódicas y almacenarlas en un entorno seguro, además se debe comprobar que es posible su restauración.

- **Sistemas captcha.** Estos sistemas impiden que los *bot* **[REF - 43]** o programas automatizados puedan interactuar con determinadas partes de la web, como el área de comentarios o la página de inicio de sesión.

- **Gestión de registros (*logging*).** Un sistema de gestión de registros **[REF - 55]** o *logs* guarda los eventos más importantes que se producen en la página web. Así, en caso de incidente de seguridad, se podrá investigar lo sucedido para mitigar el incidente y tomar las medidas necesarias para que no vuelva a suceder.

- **Entornos de producción y prueba.** Cuando se aplica una actualización de seguridad o cualquier otro cambio relevante en la web, es recomendable realizarlo previamente en un entorno controlado. Así, en caso de desastre, la página web de la empresa no se verá afectada. Por ello es importante disponer de dos entornos bien diferenciados: un entorno de pruebas o pre-producción y la página web funcional y pública o producción.

- **Metodología de desarrollo seguro.** Cuando se solicita un desarrollo específico, la empresa contratada debe utilizar una metodología de desarrollo seguro, como la elaborada por la Fundación OWASP **[REF - 44]**. Este tipo de metodologías establecen unos requisitos de seguridad que debe cumplir el *software* que se desarrolle para reducir la posibilidad de sufrir un incidente de seguridad.

3

- **Monitorización de tráfico.** Monitorizar el tráfico servirá para identificar posibles indicios de ciberataque. Existen determinadas herramientas, como los sistemas de detección de intrusos o IDS o los WAF (*Web Application Firewall* **[REF - 56]**), cuya instalación reducirá y evitará una gran variedad de ataques.

- **Sistemas de respaldo.** Los sistemas de respaldo permiten seguir ofreciendo el servicio web a los clientes y trabajadores en caso de incidente de seguridad o fallo del sistema. El sistema de respaldo estará ubicado en un servidor independiente que será activado cuando el servidor principal no pueda ofrecer el servicio.

- **Auditoría técnica periódica.** Antes de publicar la web es recomendable que sea analizada por personal técnico especializado en busca de vulnerabilidades o malas configuraciones que pueda poner en riesgo la seguridad del sistema.

- **Proveedor de seguridad externo.** Escoger un proveedor de seguridad **[REF - 57]** dotará de un extra de seguridad a la web y permitirá reducir las consecuencias en caso de sufrir un incidente de seguridad.

- **Pagos online seguros.** En caso de que la página web permita a los clientes comprar online, se deben implementar métodos seguros, como los TPV virtuales cuyas comunicaciones viajen cifradas o contratar una entidad intermediadora reconocida, como PayPal o Google.

- **Cumplimiento legal y normativo.** Para evitar sanciones por incumplimiento normativo, la página web corporativa debe cumplir con la legalidad vigente. Para ello debe tratar los datos personales de acuerdo a la Ley Orgánica de Protección de Datos y Garantía de Derechos Digitales o LOPDGDD **[REF - 58]**, la Ley de Servicios de la Sociedad de la Información o LSSI **[REF - 59]** y la Ley de Propiedad Intelectual o LPI **[REF - 60]**. Además deberá cumplir cualquier otro tipo de normativa vigente que pueda afectar a la actividad de la empresa.

3.6.3. ¿Qué hacer en caso de sufrir un ataque contra la web corporativa?

Los incidentes que afectan a la página web corporativa pueden llegar a tener graves consecuencias para la continuidad de la empresa, como ya se indicó en el apartado ¿Qué es un ataque contra la página web corporativa?. Cuando la página web de la empresa sufre un ataque se deben llevar a cabo una serie de pasos que mitiguen las consecuencias **[REF - 61]** del mismo y que la actividad pueda ser restaurada en el menor tiempo posible:

3

Ilustración 15 Pasos para recuperar la actividad después de sufrir un incidente de seguridad

- **Evaluar el incidente.** En primera instancia se debe hacer una evaluación previa del incidente, identificando a grandes rasgos el alcance y tipología del mismo, para ello los sistemas de *logs*, IDS, etc. serán de gran ayuda.

- **Comunicación del incidente.** Solamente deben tener conocimiento del incidente aquellas personas o departamentos que puedan ser de ayuda. Este será el momento de contactar con proveedores de servicio o soporte técnico, además es recomendable interponer una denuncia ante las Fuerzas y Cuerpos de Seguridad del Estado **[REF - 9]**. También se deberá notificar a la Agencia Española de Protección de Datos **[REF - 62]**, en caso de que se hayan visto comprometidos datos personales, y con INCIBE-CERT, a través del servicio de respuesta a incidentes **[REF - 63]**.

- **Contención de daños y minimización de los riesgos.** Una actuación rápida y eficaz puede reducir las consecuencias de un incidente de forma considerable. Se deberá desconectar el servidor web afectado de la red y determinar la vía de entrada de los ciberdelincuentes al entorno corporativo. Además es recomendable clonar los discos de los dispositivos afectados para que puedan ser analizados posteriormente.

3

» **Identificar la gravedad del incidente.** En este paso se debe identificar los sistemas, equipos e información afectados por el incidente. Esto permitirá determinar qué activos de la empresa se han visto afectados y por lo tanto se podrá tomar las acciones que se consideren oportunas. Las principales consideraciones a analizar son:

- Determinar la tipología del ataque, como por ejemplo un *defacement*, *ransomware*, fuga de información, alojamiento de *malware* o un *phishing*, etc.

- Punto de origen o vector de ataque utilizado para atacar. Esto puede ser desde aprovecharse de vulnerabilidades no parcheadas hasta un ataque de *phishing*.

- Ataque dirigido o aleatorio. Los incidentes provocados por situaciones relacionadas con comunicaciones genéricas e impersonales, o debidos a vulnerabilidades no parcheadas, es muy probable que sean ataques aleatorios. Por el contrario, si el ataque cuenta con información personal de la víctima o sobre el *software* utilizado, es muy posible que sea dirigido.

- Determinar activos atacados. En base a todas las variables anteriores se identificarán los activos que han podido verse afectados.

» **Protección de las pruebas.** Gestionar las copias adecuadamente es vital en caso de interponer una denuncia ante las FCSE. Es importante recopilar todas las pruebas posibles realizando copias completas del sistema y los activos que aloja antes de llevar a cabo cualquier otra acción sobre el dispositivo en cuestión. Es recomendable realizar copias exactas de los discos y pruebas que se deben analizar. Además, se debe indicar quién hizo las copias, cuándo se realizaron y quién ha tenido acceso a ellas.

» **Notificación a organismos externos.** En caso de que el incidente se haya producido de manera intencionada es recomendable interponer una denuncia ante las FCSE aportando todas las pruebas posibles. Además, es recomendable notificar el incidente a INCIBE-CERT **[REF - 63]** como centro de respuesta a incidentes de seguridad de referencia para los ciudadanos y entidades de derecho privado en España.

» **Recuperación de sistemas.** Es hora de reinstalar los equipos afectados y restaurar las copias de seguridad en caso de existir.

» **Lecciones aprendidas.** Tomar las medidas oportunas para reducir el riesgo de que se produzca de nuevo un incidente de seguridad similar.

3

3.7. *Ransomware*

¿Qué sucedería si toda la información de tu empresa fuera inaccesible? Seguramente, la actividad diaria se vería seriamente afectada, llegando incluso a detenerse. Además, si no se cuenta con copias de seguridad funcionales, este hecho se agravaría. Estas son las consecuencias que puede sufrir una empresa ante una infección por *ransomware*.

3.7.1. ¿Qué es un ataque de *ransomware*?

"El ***ransomware*** es un tipo de ***malware* o *software* malicioso** que afecta a la información contenida en los diferentes dispositivos, impidiendo su acceso, generalmente cifrándola y solicitando un **rescate económico a los afectados"**

El *ransomware* es un tipo de *malware* o *software* malicioso que afecta a la información contenida en los diferentes dispositivos impidiendo su acceso, generalmente cifrándola y solicitando un rescate económico a los afectados a cambio de poder recuperar su acceso. En muchos casos, los ataques de *ransomware* no solamente afectan al dispositivo origen de la infección, sino que se propaga por otros dispositivos a los que tenga acceso, como unidades de red o información almacenada en la nube.

Las infecciones por *ransomware* se producen principalmente por dos vías diferentes:

- **Campañas de *malware* a través del correo electrónico.** Los ciberdelincuentes suelen enviar correos electrónicos fraudulentos donde se distribuye el *malware*. Dicho *software* malicioso puede estar adjunto en el propio correo electrónico o vinculado a un enlace que se encuentra dentro del propio correo. Para dotar de más credibilidad a los correos, los ciberdelincuentes suelen utilizar diferentes técnicas de ingeniería social con las que forzar a las potenciales víctimas a descargar y ejecutar el *malware*.

- **Vulnerabilidades o configuraciones de seguridad deficientes.** Los ciberdelincuentes también pueden infectar los dispositivos sin interacción de las potenciales víctimas. Para ello se valen de vulnerabilidades no parcheadas o configuraciones de seguridad deficientes, como por ejemplo, en los escritorios remotos **[REF - 64]**.

3

A continuación se muestra un ejemplo de correo malicioso que distribuye *malware*, como puede ser un *ransomware*:

Ilustración 16 Correo electrónico malicioso que distribuye malware por medio de un enlace malicioso

3.7.2. ¿Cómo evitar un ataque de *ransomware*?

Para evitar ser víctima de un *ransomware* es importante seguir estos consejos:

- **Precaución con adjuntos en correo electrónico y enlaces a páginas externas.** Se deben seguir las mismas recomendaciones que en las campañas de *phishing*, y en caso de duda, nunca se descargará el fichero adjunto ni se accederá al enlace que figura en el correo. El objetivo final de los ciberdelincuentes es que la potencial víctima descargue y ejecute el *malware*. Por ello, siempre se deben analizar con el antivirus del equipo o con cualquier otra herramienta en línea los archivos adjuntos o que provengan de una web externa; y ante la menor duda, nunca se deben abrir. Algunas extensiones de ficheros que nunca deben ejecutarse salvo que se conozcan los orígenes son:

  - .exe
  - .msi

3

- .vbs
- Archivos ofimáticos con macros como:
  - .docm
  - .xlsm
  - .pptm
  - .doc
  - .xls
  - .ppt
  - .docx
  - .xlsx
  - .pptx
- Y cualquier archivo comprimido que contenga alguna de estas extensiones.

» ***Software* actualizado y configuraciones de seguridad robustas.** Todo el *software* de la empresa, tanto en los diferentes dispositivos como aquellos servicios que son accesibles desde Internet, deben estar siempre actualizados a la última versión disponible. Entre los errores de configuración que destacan como origen de un incidente de tipo *ransomware* se encuentra la utilización de credenciales de acceso débiles. Para evitar esta problemática siempre se deben utilizar contraseñas robustas y evitar utilizar nombres de usuario comunes o genéricos, como administrador, nombre de la empresa, etc.

» **Herramientas *antiransomware*.** Existen herramientas específicas que evitan o reducen las consecuencias de un incidente de seguridad de tipo *ransomware* que monitorizan la red y los dispositivos empresariales deteniendo y bloqueando los procesos de cifrado.

3.7.3. ¿Qué hacer en caso de sufrir un ataque de *ransomware*?

En caso de sufrir un incidente **[REF - 65]** de este tipo se deben seguir una serie de pasos para minimizar las consecuencias del mismo:

3

Ilustración 17 Pasos para aislar un incidente de seguridad de tipo ransomware

- **Aislar el equipo o equipos infectados de la red** principal de la organización tan pronto como sea posible. Así se evitará que la infección pueda afectar a otros dispositivos o servicios de la empresa.

- **Clonar los discos de los dispositivos infectados.** Así se podrá mantener el disco en su estado original e intentar recuperar los datos sobre la copia. Es posible que no exista un método de recuperación actualmente pero en un futuro sí que exista.

- **Desinfectar los dispositivos afectados y el disco clonado** para intentar recuperar los archivos cifrados. Para ello, es recomendable analizar todos los equipos de la empresa con un *antimalware* en busca del *software* malicioso que provocó la infección de la información de la empresa.

- **Intentar recuperar los archivos cifrados** en el disco clonado previamente desinfectado. En la sección Ayuda *Ransomware* **[REF - 65]** dispones de las indicaciones necesarias para restaurar la actividad de tu empresa. Además, puedes comprobar si existe una solución que permite el descifrado. **El proyecto de la EUROPOL denominado** *No More Ransom* **[REF - 66]** cuenta con diferentes herramientas de descifrado que permiten recuperar la información inaccesible en muchas ocasiones.

  En caso de disponer de una copia de seguridad se debe restaurar utilizando la más reciente y libre de modificaciones maliciosas. Siempre se debe contar con una política de copias de seguridad **[REF - 67]** en la que se realice copias periódicas y se compruebe que es posible recuperar

3

"El **fraude del falso soporte de Microsoft**, es una llamada de un supuesto técnico de Microsoft avisando sobre múltiples **errores de seguridad** detectados en los dispositivos de la empresa"

la información. En la copia de seguridad que se restaure se debe comprobar el acceso a la información y que esta no se ha visto afectada por la infección por *ransomware*.

En caso de no disponer de copia de seguridad ni de solución, en el proyecto *No More Ransom* los sistemas operativos Windows cuentan con un **sistema de seguridad denominado *shadow copy* o *snapshot***, que mantiene copias de versiones anteriores de ficheros. Hay que localizar una copia previa a la infección y restaurarla. Es probable que se hayan perdido datos, pero se podrá continuar con la actividad.

- Finalmente, **utilizar un disco nuevo o formateado**, así como una **instalación en limpio del sistema operativo, y restaurar la copia de seguridad más reciente** anterior a la infección.

Además, es recomendable interponer una denuncia ante las Fuerzas y Cuerpos de Seguridad del Estado **[REF - 9]** aportando toda la información disponible. También se puede poner el incidente en conocimiento de INCIBE-CERT **[REF - 63]** y de la AEPD **[REF - 62]** en caso de que se vean afectados datos personales.

3.8. Fraude del falso soporte de Microsoft

Una llamada de un supuesto técnico de Microsoft avisando sobre múltiples errores de seguridad detectados en los dispositivos de la empresa. Este es el comienzo de un fraude que podría saquear las cuentas e información estratégica y confidencial de la empresa.

3.8.1. ¿Qué es el fraude del falso soporte de Microsoft?

Se trata de un fraude donde **el estafador suplanta la identidad de un técnico de Microsoft [REF - 68] con el pretexto de solucionar ciertos problemas técnicos en el equipo**, siendo su objetivo real comprometer la seguridad y privacidad del dispositivo afectado y, por lo tanto, de la propia empresa.

Los ciberdelincuentes contactan con la víctima mediante dos vías diferentes:

3

- **Llamada directa a un teléfono de la empresa.** Los ciberdelincuentes contactan directamente con un empleado de la empresa haciéndose pasar por técnico de soporte de Microsoft. En la llamada informan que los dispositivos de la empresa están en peligro y deben llevarse a cabo acciones de inmediato para garantizar la seguridad de la empresa.

- **Página de error fraudulenta (*adware*).** Los ciberdelincuentes crean páginas falsas de error donde se indica al usuario que su equipo está en riesgo y debe ponerse en contacto con ellos para solucionar los problemas. En la página se muestra un número de teléfono al que llamar y donde supuestamente ayudarán a solucionar los fallos.

Una vez se establece la comunicación telefónica, generalmente en inglés, aunque también pueden dirigirse en español, los ciberdelincuentes suelen proporcionar una serie de datos técnicos para dar más credibilidad al fraude. Una de las técnicas utilizadas por los ciberdelincuentes para generar una sensación de alerta es indicar al usuario que ejecute el visor de eventos de Windows, donde se puede visualizar toda la actividad que ocurre en el dispositivo, como notificaciones simples y mensajes de error que se registran en el sistema.

El siguiente paso es indicar a la víctima que debe **instalar un *software* de acceso remoto** para poder solucionar los problemas. Este tipo de herramientas permiten el control de un ordenador o un móvil a distancia. Esta herramienta permitirá acceder al ciberdelincuente al equipo y tomar el control del mismo, con el consiguiente **riesgo para la privacidad y seguridad de la empresa.**

En una variante de este fraude **los ciberdelincuentes solicitarán el pago de una cantidad determinada de dinero a cambio de solucionar los supuestos problemas de seguridad.** Además, permitir el acceso remoto puede tener otras consecuencias para la empresa, como:

- **Fugas de información.** Al permitir el acceso de los ciberdelincuentes al dispositivo corporativo, estos pueden acceder a información confidencial e incluso a datos privados de clientes.

- **Robo de credenciales de acceso e información bancaria.** Los dispositivos pueden almacenar nombres de usuario y contraseñas de acceso, particularmente en los navegadores web **[REF - 69]**, a diferentes servicios de la empresa que pueden ser robados. También pueden robar información bancaria en caso de que se encuentre almacenada en el dispositivo.

3

» **Instalación de *malware*.** En algunos casos pueden instalar *software* malicioso que puede provocar diferentes situaciones de riesgo, como fugas de información o acceso remoto al dispositivo, utilizarlo para perpetrar otros tipos de fraude o incluso impedir el acceso a la información que contiene por medio de un *ransomware*.

Durante la pandemia provocada por el COVID-19 los ciberdelincuentes que utilizan este tipo de argucias para comprometer la ciberseguridad de las empresas cambiaron de técnica; y como sucede con otros tipos de fraude, comenzaron a utilizar como gancho cualquier situación relacionada con el COVID-19.

3.8.2. ¿Cómo evitar el fraude del falso soporte de Microsoft?

Evitar este tipo de fraude es relativamente sencillo, ya que como indica Microsoft **[REF - 70]**, desde la compañía no realizan proactivamente comunicaciones por correo electrónico o telefónicas que no hayan sido solicitas previamente. **El soporte técnico de Microsoft solamente se pone en contacto con los usuarios que lo han solicitado previamente.**

Ante cualquier llamada de un técnico o mensaje de un supuesto técnico de Microsoft que no se ha solicitado previamente, se debe **colgar inmediatamente** sin facilitar ningún tipo de información. **Además, nunca se debe llamar a un supuesto técnico de Microsoft si aparece un mensaje de alerta al navegar por Internet.**

3.8.3. ¿Qué hacer en caso de sufrir un fraude del falso soporte de Microsoft?

En caso de sufrir un fraude de este tipo, tal y como indican desde la Unidad de Crímenes Digitales de Microsoft **[REF - 71]**, los ciberdelincuentes podrían realizar varias acciones maliciosas. Por ello, se deben llevar a cabo varias acciones para salvaguardar la seguridad de la empresa y la información que gestiona:

Ilustración 18 Acciones a seguir en caso de sufrir un incidente de falso soporte de Microsoft

3

"El ***malware* vía correo electrónico** es una de las principales formas que tienen los ciberdelincuentes para infectar los dispositivos de las víctimas"

- En el caso de haber realizado operaciones financieras desde el dispositivo o compras de productos o servicios por Internet, se debe **contactar con la entidad bancaria**, ya que se han podido hacer con las claves de acceso. Además, se deben **cambiar las credenciales de acceso de todos los servicios desde los que se haya accedido con el equipo afectado**.

- **Desinstalar cualquier *software***, como el que permite el acceso remoto, que se haya instalado en un periodo de tiempo posterior a la llamada del falso soporte técnico.

- **Analizar el equipo con una herramienta antimalware**, ya que los ciberdelincuentes han podido instalar *software* malicioso. Si se ha sufrido una **infección por *ransomware*** se deben seguir las recomendaciones indicadas en el apartado ¿Qué hacer en caso de sufrir un ataque de *ransomware*?

- **Reportar el incidente** a las Fuerzas y Cuerpos de Seguridad del Estado, INCIBE-CERT **[REF - 9]** y Microsoft **[REF - 72]**.

3.9. Campañas de correos electrónicos con *malware*

El *malware* vía correo electrónico es una de las principales formas que tienen los ciberdelincuentes para infectar los dispositivos de las víctimas. Un simple correo que aparenta ser una factura, un justificante de compra o cualquier otro señuelo, podría suponer el inicio de una infección que ponga en riesgo la seguridad de la organización.

3.9.1. ¿Qué son las campañas de correos electrónicos con *malware*?

Las campañas de correos electrónicos para distribuir *malware* son una de las principales vías de infección que utilizan los ciberdelincuentes para comprometer los dispositivos de las víctimas. Los correos enviados, al igual que sucede en las campañas de *phishing*, utilizan técnicas de ingeniería social con las que forzar a la potencial víctima a descargar y ejecutar el archivo malicioso que comprometerá el sistema.

3

En las campañas de *malware* el archivo malicioso se distribuye de dos formas diferentes:

- **Como fichero adjunto en los correos.** Una de las vías utilizada es adjuntar el *malware* a los propios correos. Para dotar de más credibilidad al fichero adjunto suelen utilizar nombres que no alerten al usuario.

- **Mediante enlace web.** Esta es otra de las vías utilizadas, para ello añaden un enlace a una página web externa desde donde la víctima descargará el *software* malicioso. El enlace suele estar ofuscado u oculto para no alertar a los destinatarios del correo sobre el fraude. Pueden utilizar enlaces en formato texto, pero también podrían usar imágenes que simulan ser archivos adjuntos, como por ejemplo, el icono de un archivo PDF.

Las campañas de correos electrónicos fraudulentos pueden distribuir varios tipos de *malware*, como son *keyloggers* (*software* malicioso que registra las pulsaciones que se realizan en el teclado, realiza capturas de pantalla, etc.), RAT (*Remote Access Tool* **[REF - 73]**) o incluso *ransomware*.

A continuación se muestran correos electrónicos fraudulentos cuyo objetivo es difundir *malware*:

Ilustración 19 Campaña de malware por correo electrónico simulando un proceso extrajudicial

3

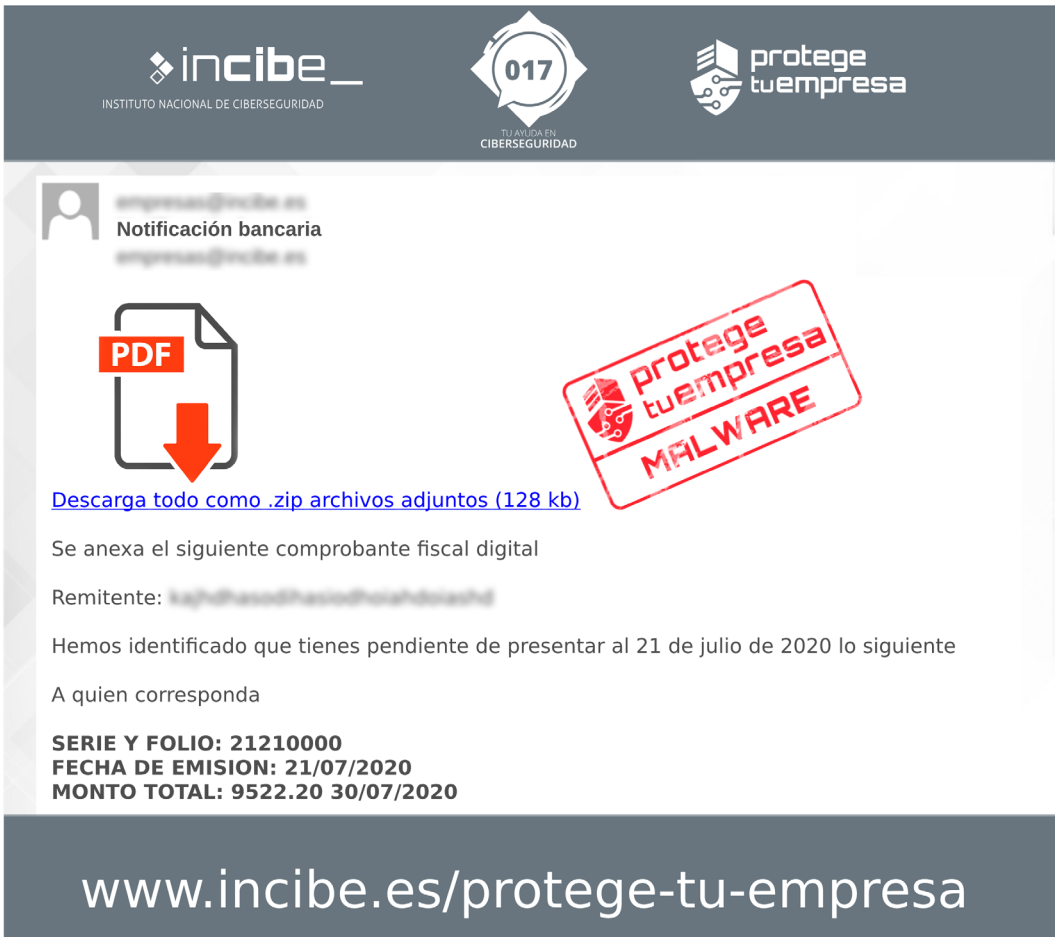


Ilustración 20 Campaña de malware simulando una notificación bancaria

Ilustración 21 Campaña de malware adjunto en el correo utilizando falsos presupuesto en Excel

3

3.9.2. ¿Cómo evitar las campañas de correos electrónicos con *malware*?

Cualquier fichero recibido en el correo electrónico, bien sea adjunto en el email o descargado mediante el enlace a una página web externa, debe tratarse con precaución, ya que podría contener *malware*. Es recomendable analizarlo siempre con el antivirus instalado en el dispositivo o con herramientas en línea para el análisis de *malware*, como Virustotal **[REF - 74]**, MetaDefender **[REF - 75]** o Jotti's **[REF - 76]**; y en **caso de contener indicios de software malicioso, nunca debe ejecutarse.**

Los siguientes tipos de archivos jamás deben ejecutarse, a no ser que se conozca su origen legítimo:

- .exe
- .msi
- .vbs
- .js

Además, **los ciberdelincuentes suelen utilizar archivos de Microsoft Office**, ya que son ficheros muy utilizados en entornos empresariales. Las siguientes extensiones de archivos Office tampoco deben ejecutarse en el dispositivo a no ser que se conozca su origen legítimo, ya que contienen macros. Las **macros** son programas diseñados con el lenguaje *Visual Basic for Applications* (VBA) que permiten automatizar tareas, pero también pueden ser **utilizadas con fines maliciosos para infectar dispositivos con *malware*.**

- .xls
- .xlsx
- .xlsm
- .doc
- .docx
- .docm
- .ppt
- .pptx
- .pptm

Además, los ciberdelincuentes pueden ocultar las macros en ficheros Microsoft Office cuya extensión no termina en ("m"). Por ello, en caso de ejecutar uno de estos archivos, **nunca se debe habilitar la edición o el contenido** por medio del botón superior, como se muestra en las siguientes imágenes.

3

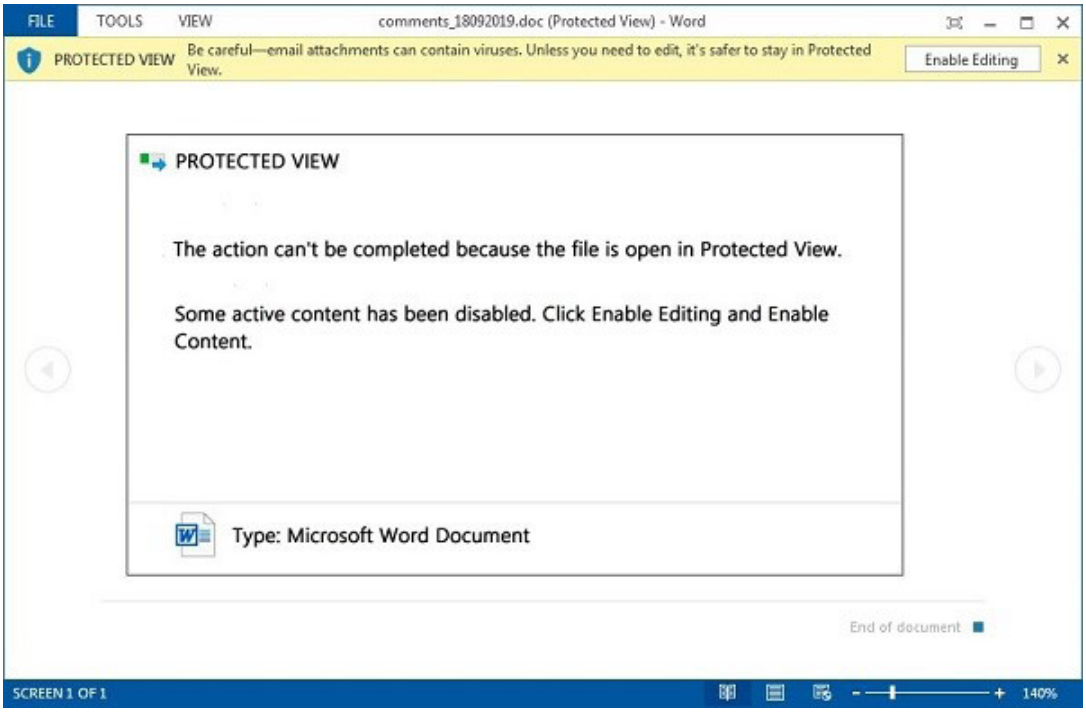


Ilustración 22 Documento de Microsoft Office protegido

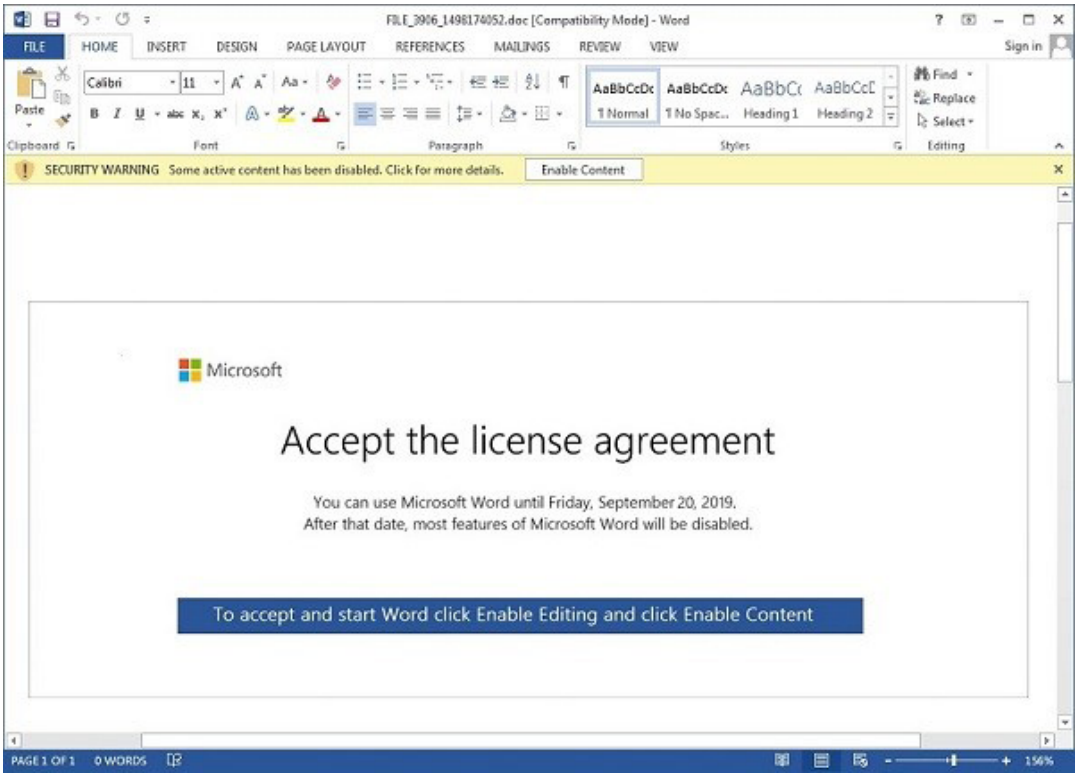


Ilustración 23 Alerta de seguridad, documento Microsoft Office protegido

3

Otro tipo de archivos cuyo uso no es muy común en campañas de *malware*, pero que pueden poner en riesgo la seguridad de la empresa, son los **ficheros PDF**. En este tipo de ficheros el riesgo está asociado a utilizar un visor de PDF desactualizado y que presente vulnerabilidades no parcheadas. Para evitar este vector de ataque se debe mantener el **visor de PDF actualizado a la última versión disponible.**

Es muy habitual en las campañas de *malware* que los **ficheros maliciosos se encuentren comprimidos**, esto tiene como objetivo dificultar la tarea de los antivirus y ofuscar su objetivo de cara a las potenciales víctimas. Si dentro de estos ficheros comprimidos se encuentra algún archivo como los descritos anteriormente, se debe tratar siguiendo las mismas recomendaciones de seguridad que si no estuviera comprimido.

3.9.3. ¿Qué hacer en caso de sufrir una infección por *malware*?

Cuando la empresa sufre una infección por *malware* se deben seguir una serie de pasos para volver a recuperar la actividad empresarial. Puedes obtener más información en los siguientes artículos:

- Primeros pasos en la respuesta a incidentes **[REF - 77]**.
- Respuesta a incidentes: tomando evidencias y recuperando la actividad **[REF - 78]**.
- Respuesta incidentes: ya he restaurado los sistemas, ¿y ahora qué? **[REF - 61]**.

Además, en caso de que se viera afectada información personal se deberá notificar a la Agencia Española de Protección de Datos (AEPD) en un plazo inferior a 72 horas. Puedes obtener más información sobre cómo notificar brechas de seguridad a la AEPD en la siguiente guía:

- Guía para la gestión y notificación de brechas de seguridad **[REF - 79]**.

Por último, es recomendable interponer una denuncia ante las Fuerzas y Cuerpos de Seguridad del Estado **[REF - 9]**, aportando todas las pruebas posibles, y ante el servicio de respuesta a incidentes que ofrece INCIBE-CERT **[REF - 63]**.

3.10. Ataques de denegación de servicio

Al igual que los ataques de tipo *ransomware*, que impiden el acceso a la información de la empresa, los ataques de denegación de servicio impiden el correcto funcionamiento de los servicios que ofrece la empresa tanto a empleados como a clientes.

3

3.10.1. ¿Qué son los ataques de denegación de servicio?

Los ataques de denegación de servicio, o DoS por sus siglas en inglés (*Denial of Service*), tienen como objetivo **degradar la calidad de un servicio; por ejemplo, la página web corporativa, hasta dejarlo en un estado no funcional**. Para conseguirlo los ciberdelincuentes saturan los recursos del sistema que aloja el servicio a interrumpir, enviándoles una avalancha de peticiones que no son capaces de atender.

Los ataques DoS generalmente son llevados a cabo cuando el servicio a atacar cuenta con algún tipo de vulnerabilidad, que es aprovechada por el ciberedelincuente para comprometer la calidad del servicio.

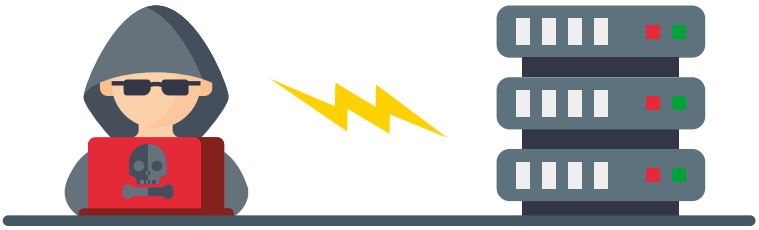


Ilustración 24 Diagrama ataque DoS

Una variante de los ataques DoS es la denegación de servicio distribuido o DDoS por sus siglas en inglés (*Distributed Denial of Service*). Los ataques **DDoS utilizan un elevado número de dispositivos atacantes**, al contrario que el ataque DoS, que puede ser llevado a cabo por un único dispositivo atacante. Los ataques DDoS generalmente son llevados a cabo por *bots*, dispositivos infectados cuyo propietario muchas veces desconoce que sus dispositivos forman parte de esta *botnet* **[REF - 80]**.

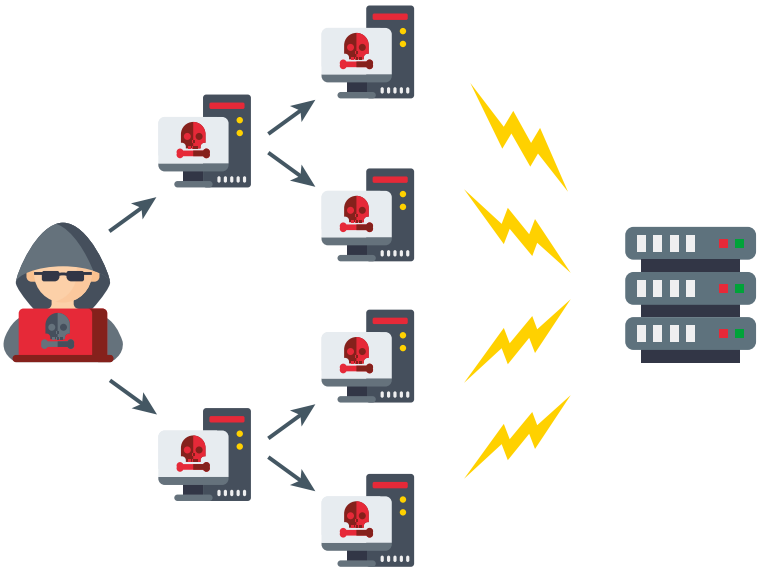


Ilustración 25 Diagrama ataque DDoS

3

En algunas ocasiones, como en la campaña "Oleada de correos fraudulentos que amenazan con 'hackear' tu empresa" **[REF - 81]**, los ciberdelincuentes tratan de extorsionar a las víctimas indicando que van a lanzar un ataque de denegación de servicio contra los servicios corporativos. En realidad ese ataque no será lanzado, únicamente juegan con el miedo que provocan las ciberamenazas con cierta repercusión, como fue *WannaCry* **[REF - 82]**, para que las víctimas paguen el dinero solicitado.

3.10.2. ¿Cómo evitar los ataques de denegación de servicio?

En muchas ocasiones solamente se es consciente de que se está sufriendo un ataque de denegación de servicio cuando se está siendo atacado. Por ello, **implementar medidas preventivas será imprescindible** para proteger los servicios de la empresa.

Cuando el **servicio accesible desde Internet se encuentra dentro de la red interna** de la empresa es necesario aplicar las siguientes medidas:

- **Ubicar el servidor web en una zona desmilitarizada.** También conocida como DMZ **[REF - 83]**, evita que en caso de intrusión el ciberdelincuente pueda acceder a la red interna de la empresa donde se encuentran alojados recursos críticos para esta, como el servidor de ficheros, y evitar la degradación de los mismos.

- **Implementar sistemas de detección y prevención de intrusiones (IDS/IPS).** Este tipo de sistemas monitorizan las conexiones que se establecen a los servicios corporativos alertando, detectando y evitando los accesos no autorizados, e incluso bloqueando direcciones IP que están llevando a cabo un ataque DDoS.

- ***Software* de protección.** Implementar un *software* de protección con funcionalidad mixta, como un UTM **[REF - 84]**, permite gestionar de manera unificada la mayoría de ciberamenazas que pueden afectar a una empresa.

- **Contratar un proveedor de seguridad externo.** Cuando se ofrece un servicio de alta disponibilidad se puede contratar los servicios de un proveedor de seguridad externo **[REF - 57]**, que actuará como intermediario entre el servidor web y los usuarios, reduciendo las consecuencias de sufrir uno de estos incidentes.

Si el **servicio se encuentra alojado en un proveedor externo de *hosting* es recomendable informarse sobre las medidas de seguridad que**

3

ha implementado, debiendo ser similares a las indicadas anteriormente. Algunos proveedores de *hosting* ofrecen estas medidas de seguridad desde el panel de administración. Es recomendable:

- Verificar quién será el encargado de su configuración y administración. **Ofrecer el mayor ancho de banda posible**, tanto si el servicio se encuentra alojado en la red corporativa como si se encuentra en un proveedor externo. Así se podrán gestionar mejor los picos de tráfico que causan las denegaciones de servicio. Disponer del mismo servicio duplicado en otro servidor y que, en función del número de peticiones, se distribuya entre uno u otro. A estas técnicas se las denomina **redundancia y balanceo de carga** respectivamente. Esta medida reduce los riesgos de sufrir un ataque de denegación de servicio, ya que al disponer de más un servidor se reducirá la posibilidad de que se detenga debido a la sobrecarga. Además, ofrece otros beneficios como la tolerancia a los fallos ya que si un servidor se detiene el otro seguirá dando servicio. Disponer de **soluciones de seguridad basados en la nube**, como los WAF que ofrecen diferentes proveedores, pueden ser de gran ayuda a la hora de prevenir y mitigar las consecuencias de un ataque de denegación de servicio. Los WAF **[REF - 85]** actúan como intermediarios entre el servicio web y los usuarios, interponiéndose también a ciberdelincuentes y a los *bots*. Por último, se ha de tener todo el **sistema actualizado a la última versión disponible**, tanto el *software* ejecutado por el servidor como por los componentes que dotan de seguridad al servicio.

3.10.3. ¿Qué hacer en caso de un ataque de denegación de servicio?

Pese a que se implementen medidas de prevención siempre existe la posibilidad de sufrir un ataque DoS o DDoS. Por ello, se pueden seguir las siguientes recomendaciones cuando se es víctima de uno de estos ataques:

Ilustración 26 Fases para mitigar un incidente de seguridad de denegación de servicio

3

"El ***adware*** es una de las vías utilizadas por los ciberdelincuentes para **obtener beneficios de forma lícita"**

- **Preparación previa al ataque.** En esta fase se deben elaborar los procedimientos técnicos y organizativos que servirán para mitigar las consecuencias de uno de estos ataques.
- **Fase de identificación de actividad anómala.** Se monitorizarán los indicadores que revelan uno de estos ataques, como pueden ser herramientas específicas, ancho de banda, uso de CPU, etc.
- **Identificar el vector de ataque.** Para ello, hay que recopilar y clasificar la información relevante como direcciones IP de origen y destino, protocolo y puerto utilizado etc.
- **Fase de rastreo.** Hay que identificar los puntos de ingreso en la red corporativa para mitigar el ataque de manera eficiente. Para ello, hay que rastrear los flujos de ataque desde las secciones atacadas en la red corporativa hasta los dispositivos perimetrales.
- **Aplicar las medidas de mitigación** indicadas en la fase de preparación previa.
- **Lecciones aprendidas.** Esta fase será vital para minimizar las consecuencias de un nuevo ataque. Se deberá estudiar el incidente valorando los aspectos a mejorar.

3.11. Ataques de *adware*

El *adware* es una de las vías utilizadas por los ciberdelincuentes para obtener beneficios de forma ilícita. Para llevarlo a cabo muestran anuncios manera intrusiva para los usuarios.

3.11.1. ¿Qué son los ataques de *adware*?

El *adware* es un tipo de software malicioso cuyo objetivo es mostrar anuncios publicitarios a su víctima con el fin de generar ingresos a los ciberdelincuentes. Este tipo de *malware* se instala en los dispositivos a través de diferentes vías, desde *software* gratuito que lo lleva añadido hasta programas no legítimos como los descargados de repositorios no oficiales o

3

explotando vulnerabilidades no parcheadas del navegador. El *adware*, en algunos casos, no es una gran molestia para el usuario, pero en otros llega a dificultar tanto las labores cotidianas que acaba afectando directamente a la eficiencia del usuario.

El *malvertising* [REF - 86], termino compuesto al contraer las palabras en inglés *malicious advertising* (publicidad maliciosa), es un tipo de *adware* **que consiste en camuflar malware en la publicidad mostrada en páginas web.** El *malvertising* tiene como objetivo infectar el dispositivo con *malware* para posteriormente realizar cualquier tarea maliciosa, al contrario que el *adware*, cuyo objetivo es mostrar publicidad.

3.11.2. ¿Cómo evitar los ataques de *adware*?

Para evitar que los dispositivos corporativos se infecten con esta amenaza se deben llevar a cabo las siguientes recomendaciones:

- ***Software* actualizado.** Todo el *software* que compone los dispositivos de la empresa deben estar actualizados a la última versión disponible, esto comprende tanto el sistema operativo como las herramientas que tenga instaladas.
- ***Software* de seguridad.** Los dispositivos deben contar con herramientas de seguridad instaladas, como es el antivirus, que debe mantenerse actualizado y activo en todo momento.

- ***Software* de fuentes oficiales.** Todo el *software* que se instale en los dispositivos corporativos debe proceder de la fuente legítima, evitando utilizar fuentes no confiables, ya que pueden contener *malware*.

- ***Plugins* o extensiones del navegador [REF - 87]**. Solamente se deben instalar los complementos de navegador estrictamente necesarios y que provengan de fuentes confiables. También se debe verificar antes de instalar cualquier complemento los permisos que solicita, evitando aquellos que requieren más de los necesarios.

3.11.3. ¿Qué hacer en caso de sufrir un ataque de *adware*?

Si algún dispositivo corporativo se ve afectado por una infección de *adware* se deben seguir los siguientes pasos:

- **Analizar completamente el dispositivo con una herramienta *antimalware***, eliminando cualquier archivo sospechoso de contener el *software* malicioso.

3

- **Comprobar los complementos instalados en el navegador web** **[REF - 69]**, eliminando aquellos que no provengan de fuentes oficiales o instaladas recientemente.

- **Desinstalar cualquier herramienta que no ha sido autorizada** en la política de aplicaciones permitidas **[REF - 88]** en la empresa. Es recomendable buscar por fecha de instalación.

3.12. Ataque de suplantación de proveedores

Los ataques de suplantación de proveedores pueden llegar a ser un gran problema para las empresas, ya que, creyendo hacer una transferencia bancaria al proveedor legítimo, se realiza en realidad a un ciberdelincuente.

3.12.1. ¿Qué son ataques de suplantación de proveedores?

En este tipo de incidente **el ciberdelincuente suplanta la identidad de un proveedor de la empresa**, y utilizando técnicas de ingeniería social consigue que la víctima realice una **transferencia bancaria al ciberdelincuente** pensando que se trata del proveedor legítimo.

Para perpetrar este tipo de ataques **los ciberdelincuentes suelen estudiar su objetivo con el fin de obtener toda la información posible**. Para ello, pueden valerse de información pública, como la disponible en la página web corporativa o redes sociales. En otras ocasiones **los ciberdelincuentes vulneran la seguridad de los sistemas** del proveedor o de la víctima consiguiendo aún más información. A veces utilizan los sistemas vulnerados de la empresa, como el servidor de correo electrónico, para llevar a cabo el ataque.

Los incidentes de suplantación de proveedores suelen ser **ataques elaborados utilizando diversas técnicas** que consiguen no alertar a la víctima. Algunas de las técnicas que utilizan son:

- **Falsificación del remitente.** Los ciberdelincuentes en este tipo de fraude suelen falsificar el correo del remitente para simular que pertenece a la empresa proveedora, para lo que utilizan la técnica del *email spoofing*. En otras ocasiones adquieren dominios web similares al del proveedor, técnica conocida como *typosquatting* **[REF - 8]**, variando algún carácter del dominio y haciendo que a simple vista parezca legítimo cuando en realidad no lo es.

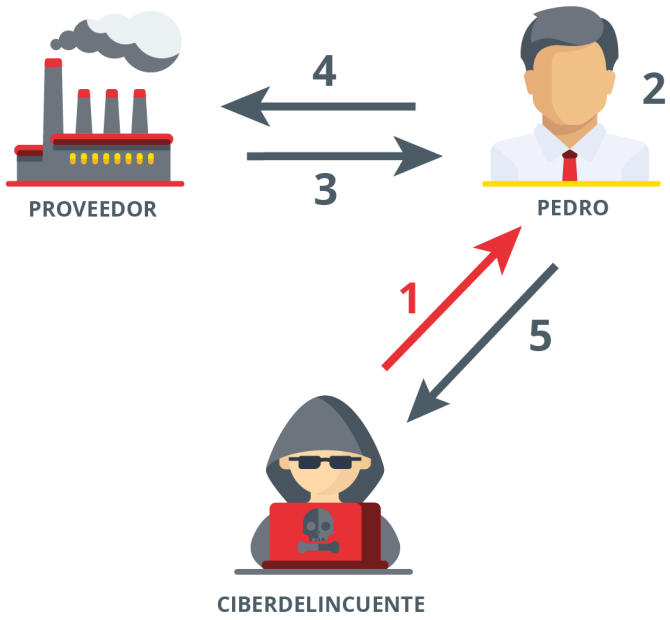
- **Redacción y forma de expresión.** La expresión en este tipo de correos suele ser correcta, sin faltas de ortografía ni errores gramaticales destacables, de

3

igual forma que en una comunicación legítima, ya que, en muchas ocasiones han estudiado la forma en que se comunican con sus clientes.

» **Estética y firma del correo.** La estética del correo y la firma del pie utilizada suele ser igual a la de los correos legítimos. De esta forma, los ciberdelincuentes evitan levantar sospechas sobre la comunicación fraudulenta.

A continuación se muestran algunas posibles situaciones en las que puede desarrollarse este tipo de fraude:



1. Envío del correo fraudulento que suplanta al legítimo proveedor por parte del ciberdelincuente a Pedro indicando el cambio de cuenta bancaria.

2. Pedro modifica los datos bancarios asociados a su proveedor legítimo por una cuenta controlada por el ciberdelincuente.

3. Solicitud de un nuevo envío de material de Pedro a su proveedor legítimo.

4. El proveedor legítimo llega a un acuerdo de precio y tiempos de entrega con Pedro sobre el nuevo pedido.

5. Pedro realiza la transferencia bancaria a la cuenta controlada por el ciberdelincuente.

Ilustración 27 Email spoofing como origen del ataque de suplantación de proveedor

3

1. El ciberdelincuente ataca y consigue acceder al buzón de correo del proveedor.

2. El ciberdelincuente envía un correo a Pedro desde el buzón legítimo del proveedor indicando el cambio de cuenta bancaria.

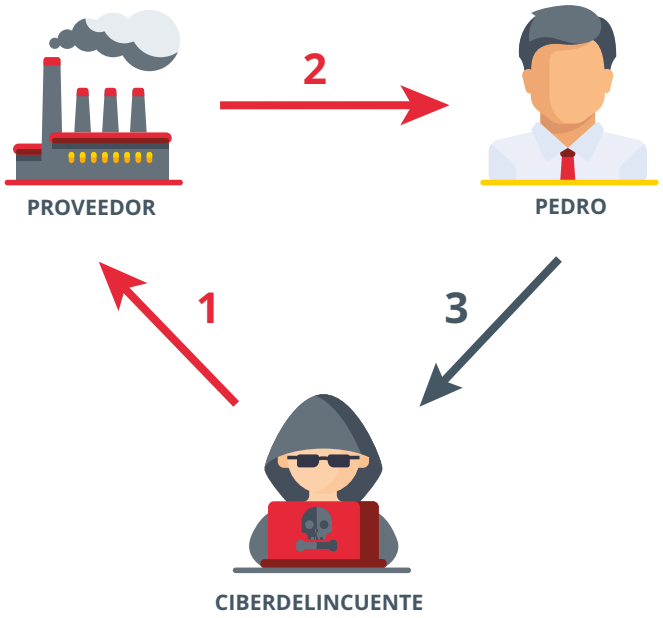
3. Pedro modifica la cuenta bancaria del legítimo proveedor por una controlada por el ciberdelincuente.

4. Solicitud de un nuevo envío de material de Pedro a la cuenta del proveedor controlada por el ciberdelincuente.

5. El ciberdelincuente responde a Pedro desde el buzón legítimo del proveedor acordando precio y tiempos de entrega.

6. Pedro realiza la transferencia bancaria a la cuenta controlada por el ciberdelincuente.

Ilustración 28 Ataque a la empresa proveedora como origen del incidente



1. El ciberdelincuente ataca y consigue acceder al buzón de correo del proveedor.

2. El ciberdelincuente envía un correo a Pedro desde el buzón legítimo del proveedor reclamando el pago de una factura y aportando los nuevos datos bancarios alegando cualquier excusa sobre la cuenta bancaria del proveedor legítimo.

3. Pedro realiza la transferencia bancaria a la cuenta controlada por el ciberdelincuente.

Ilustración 29 Ataque al proveedor y solicitud de cambio de número de cuenta

3.12.2. ¿Cómo evitar los ataques de suplantación de proveedores?

Identificar este tipo de ataques puede ser complejo, por lo que es importante prestar atención a solicitudes en las que se vea afectada información bancaria o personal, aunque parezcan legítimas a simple vista. Algunos de los indicadores a tener en cuenta son:

- **Comprobar la dirección del remitente.** Se ha de verificar que la dirección del remitente es legítima. Para ello, se deben comprobar las cabeceras del correo **[REF - 89]**. También se debe tener cuidado con la técnica de *typosquatting*, ya que un simple caracter es suficiente para que, si la víctima no pone especial atención, considere que el dominio utilizado en el correo es legítimo.

3

» **Las peticiones que tengan que ver con información bancaria o cualquier otro tipo de información sensible es recomendable verificarlas utilizando un canal de comunicación alternativo.** En caso de utilizar el correo electrónico para verificarla, nunca se responderá al correo recibido. Se creará un nuevo hilo de correos empleando una dirección conocida de la empresa.

3.12.3. ¿Qué hacer en caso de sufrir un ataque de suplantación de proveedores?

Cuando se sufre un incidente de este tipo se debe denunciar lo sucedido a las Fuerzas y Cuerpos de Seguridad del Estado (Policía Nacional **[REF - 90]** o Guardia Civil **[REF - 91]**). También se puede notificar el incidente al servicio de Respuesta y Soporte **[REF - 63]** ante incidentes de seguridad de INCIBE.

4 DECÁLOGO DE RECOMENDACIONES DE SEGURIDAD

Para reducir el riesgo de que la empresa sufra un incidente de seguridad se deben tener en cuenta el siguiente decálogo de recomendaciones:

1. Ante correos electrónicos de **remitentes desconocidos se deben extremar las precauciones**, ya que puede tratarse de una comunicación fraudulenta.

2. Los **remitentes de los correos electrónicos pueden estar falseados.** Es necesario saber identificar este tipo de comunicaciones **[REF - 7]** para evitar caer en el fraude.

3. Un solo caracter en el nombre de dominio (web y correo electrónico) puede llegar a provocar un incidente de seguridad. Es necesario conocer **la técnica del *typosquatting* [REF - 5]** para evitar ataques cuyo origen sea el correo electrónico.

4. Si un correo presenta **enlaces externos a páginas web o documentos adjuntos, se han de extremar las precauciones**, y es recomendable analizarlos con herramientas en línea o con el antivirus del dispositivo.

5. Todos los **dispositivos de la empresa** y las herramientas que tienen instaladas estarán **siempre actualizadas** a la última versión disponible.

6. Los dispositivos de la empresa contarán con a**plicaciones antivirus instaladas y actualizadas.**

7. Ante cualquier tipo de incidente de seguridad es recomendable ponerlo en conocimiento de Las Fuerzas y Cuerpos de Seguridad del Estado **[REF - 9]** (FCSE) y el centro de respuesta a incidentes de INCIBE **[REF - 63]**.

8. Si en un incidente de seguridad se ven afectados datos de carácter personal se deberá poner en conocimiento de la Agencia Española de Protección de Datos **[REF - 18]** (AEPD).

4

9. El correo electrónico no es el único canal de comunicación que utilizan los ciberdelincuentes. Se debe **tener también especial precaución con llamadas telefónicas y comunicaciones de aplicaciones de mensajería instantánea, mensajes SMS o redes sociales.**

10. Ante solicitudes que requieran **la modificación de datos bancarios, se debe verificar dicha solicitud por un canal de comunicación alternativo y confiable.**

11. Los correos de **extorsión a causa de un supuesto vídeo privado** son un fraude. Hay que **eliminarlos directamente, ya que dicho vídeo no existe.**

12. Siempre se utilizarán **contraseñas robustas** para acceder a los distintos servicios corporativos. Además, se **evitará reutilizar contraseñas** en más de un servicio y, siempre que sea posible, habilitar un doble factor de autenticación.

13. Se **realizarán copias de seguridad periódicas** de la información de la empresa y se comprobará que es posible su restauración.

5 REFERENCIAS

[REF – 1]. **Ingeniería social: técnicas utilizadas por los ciberdelincuentes y cómo protegerse** https://www.incibe.es/protege-tu-empresa/blog/ingenieria-social-tecnicas-utilizadas-los-ciberdelincuentes-y-protegerse

[REF - 2]. **¿Sabes cómo funciona un ciberataque que utiliza ingeniería social?** https://www.incibe.es/protege-tu-empresa/blog/sabes-funciona-ciberataque-utiliza-ingenieria-social

[REF - 3]. **Ejemplo de fraude telefónico** https://www.youtube.com/watch?v=-dp6bF3DPvN4

[REF - 4]. **Tecnología y formación para proteger tu dominio de correo electrónico** https://www.incibe.es/protege-tu-empresa/blog/tecnologia-y-formacion-proteger-tu-dominio-correo-electronico

[REF - 5]. **Cybersquatting, qué es y cómo protegerse** https://www.incibe.es/protege-tu-empresa/blog/cybersquatting-y-protegerse

[REF - 6]. **Día Mundial del Correo: cómo detectar correos fraudulentos** https://www.incibe.es/protege-tu-empresa/blog/dia-mundial-del-correo-detectar-correos-fraudulentos

[REF - 7]. **¿Dudas sobre la legitimidad de un correo? Aprende a identificarlos** https://www.incibe.es/protege-tu-empresa/blog/dudas-legitimidad-correo-aprende-identificarlos

[REF - 8]. **Aprende a detectar el cybersquatting contra tu marca** https://www.incibe.es/protege-tu-empresa/blog/aprende-detectar-el-cybersquatting-tu-marca

[REF - 9]. **Reporte de fraude** https://www.incibe.es/protege-tu-empresa/reporte-fraude

[REF - 10]. **Recolección de pruebas digitales: testigos online** https://www.incibe.es/protege-tu-empresa/blog/recoleccion-pruebas-digitales-testigos-online

[REF - 11]. **¿Estás preparado para hacer frente a una fuga de datos?** https://www.incibe.es/protege-tu-empresa/blog/estas-preparado-hacer-frente-fuga-datos

[REF – 12]. **Copia de carbón oculta** https://es.wikipedia.org/wiki/Copia_de_carb%C3%B3n_oculta

[REF - 13]. **Historias reales: mi trabajo robaron y mi proyecto plagiaron** https://www.incibe.es/protege-tu-empresa/blog/historias-reales-mi-trabajo-robaron-y-mi-proyecto-plagiaron

[REF - 14]. **¿Sabías que existen distintos tipos de cifrado para proteger la privacidad de nuestra información en Internet?** https://www.osi.es/es/actualidad/blog/2019/07/10/sabias-que-existen-distintos-tipos-de-cifrado-para-proteger-la-privacidad

[REF - 15]. **Herramientas colaborativas: medidas básicas de seguridad** https://www.incibe.es/protege-tu-empresa/blog/herramientas-colaborativas-medidas-basicas-seguridad

[REF - 16]. **Cómo gestionar una fuga de información. Una guía de aproximación al empresario** https://www.incibe.es/protege-tu-empresa/guias/guia-fuga-informacion

[REF - 17]. **Protección de datos y administración local** https://www.aepd.es/sites/default/files/2019-09/guia-proteccion-datos-administracion-local.pdf

[REF - 18]. **Brechas de seguridad** https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/brechas-de-seguridad

[REF - 19]. **Borrado seguro de la información. Una aproximación para el empresario** https://www.incibe.es/protege-tu-empresa/guias/borrado-seguro-informacion-aproximacion-el-empresario

[REF - 20]. **Clasificación de la información. Políticas de seguridad para la pyme** https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/clasificacion-informacion.pdf

[REF - 21]. **Kit de concienciación** https://www.incibe.es/protege-tu-empresa/kit-concienciacion

[REF - 22]. **¿Conoces la nueva norma para la gestión de la privacidad?** https://www.incibe.es/protege-tu-empresa/blog/conoces-nueva-norma-gestion-privacidad

[REF - 23]. Control de acceso. Políticas de seguridad para la pyme https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/control-de-acceso.pdf

[REF - 24]. Antimalware. Políticas de seguridad para la pyme https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/antimalware.pdf

[REF - 25]. Copias de seguridad: una guía de aproximación para el empresario https://www.incibe.es/protege-tu-empresa/guias/copias-seguridad-guia-aproximacion-el-empresario

[REF - 26]. DLP protege tus datos contra fugas de información https://www.incibe.es/protege-tu-empresa/blog/dlp-protege-tus-datos-fugas-informacion

[REF - 27]. La importancia de proteger la información mediante acuerdos de confidencialidad https://www.incibe.es/protege-tu-empresa/blog/importancia-proteger-informacion-mediante-acuerdos-confidencialidad

[REF - 28]. Historias reales: un falso proveedor a mi empresa se la jugó https://www.incibe.es/protege-tu-empresa/blog/historias-reales-falso-proveedor-mi-empresa-se-jugo

[REF - 29]. Avisos de seguridad https://www.incibe.es/protege-tu-empresa/avisos-seguridad

[REF - 30]. Avisos de seguridad de tipo phishing https://www.incibe.es/protege-tu-empresa/avisos-seguridad/filtro/phishing

[REF - 31]. Avisos de seguridad con la etiqueta #CiberCOVID19 https://www.incibe.es/protege-tu-empresa/avisos-seguridad/filtro/CiberCOVID19

[REF - 32]. Informe de transparencia de Google https://transparencyreport.google.com/safe-browsing/search

[REF - 33]. Free website security check & malware scanner https://sitecheck.sucuri.net/

[REF - 34]. Virustotal https://www.virustotal.com/gui/home/url

[REF - 35]. URL haus https://urlhaus.abuse.ch/

[REF - 36]. **Unshorten.It!** https://unshorten.it/

[REF - 37]. **Puntos de contacto para empresas** https://www.incibe.es/formulario-contacto-empresas

[REF - 38]. **Historias reales: el fraude del CEO** https://www.incibe.es/protege-tu-empresa/blog/historias-reales-el-fraude-del-ceo

[REF - 39]. **Fraude del CEO** https://www.incibe.es/protege-tu-empresa/avisos-seguridad/fraude-del-ceo

[REF - 40]. **Fraude con un Deepfake: el lado oscuro de la inteligencia artificial** https://www.pandasecurity.com/spain/mediacenter/noticias/fraude-deepfake-voz/

[REF - 41]. **Fraude de RRHH** https://www.incibe.es/protege-tu-empresa/avisos-seguridad/fraude-rrhh

[REF - 42]. **Las 2 caras de las criptomonedas** https://www.osi.es/es/campanas/criptomonedas

[REF - 43]. **¿Humano o bot? Protege tu web con sistemas captcha** https://www.incibe.es/protege-tu-empresa/blog/humano-o-bot-protege-tu-web-sistemas-captcha

[REF - 44]. **Owasp** https://owasp.org/

[REF - 45]. **Medidas de prevención contra ataques de denegación de servicio** https://www.incibe.es/protege-tu-empresa/blog/medidas-prevencion-ataques-denegacion-servicio

[REF - 46]. **Protégete frente al defacement y que no le cambien la cara a tu web** https://www.incibe.es/protege-tu-empresa/blog/protegete-frente-al-defacement-y-no-le-cambien-cara-tu-web

[REF - 47]. **Protege tu web** https://www.incibe.es/protege-tu-empresa/que-te-interesa/protege-tu-web

[REF - 48]. **Protección de la página web. Políticas de seguridad para la pyme** https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/proteccion-pagina-web.pdf

[REF - 49]. ¿Qué aporta un certificado digital SSL a mi sitio web? ¿Cómo seleccionar uno? https://www.incibe.es/protege-tu-empresa/blog/certificado-digital-ssl-sitio-web-seleccionar-uno

[REF - 50]. Si tu web cuenta con certificado de seguridad, comprueba que utilizas una versión segura del protocolo TLS https://www.incibe.es/protege-tu-empresa/blog/si-tu-web-cuenta-certificado-seguridad-comprueba-utilizas-version-segura-del

[REF - 51]. Medidas de seguridad avanzadas en WordPress I https://www.incibe.es/protege-tu-empresa/blog/medidas-seguridad-avanzadas-wordpress-i

[REF - 52]. Medidas de seguridad avanzadas en WordPress II https://www.incibe.es/protege-tu-empresa/blog/medidas-seguridad-avanzadas-wordpress-ii

[REF - 53]. Gestor de contenidos https://www.incibe.es/protege-tu-empresa/avisos-seguridad/filtro/gestor-contenidos

[REF - 54]. Contraseñas. Políticas de seguridad para la pyme https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/contrasenas.pdf

[REF - 55]. Gestión de log. Políticas de seguridad para la pyme https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/gestion-logs.pdf

[REF - 56]. WAF: cortafuegos que evitan incendios en tu web https://www.incibe.es/protege-tu-empresa/blog/waf-cortafuegos-evitan-incendios-tu-web

[REF - 57]. Claves para escoger el proveedor de seguridad que más se ajusta a tus necesidades https://www.incibe.es/protege-tu-empresa/blog/claves-escoger-el-proveedor-seguridad-mas-se-ajusta-tus-necesidades

[REF - 58]. RGPD para pymes https://www.incibe.es/protege-tu-empresa/rgpd-para-pymes

[REF - 59]. Ley de Servicios de la Sociedad de la Información y del Comercio Electrónico http://www.lssi.gob.es/Paginas/index.aspx

[REF - 60]. Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia https://www.boe.es/buscar/act.php?id=BOE-A-1996-8930

[REF - 61]. Respuesta incidentes: ya he restaurado los sistemas. ¿Y ahora qué? https://www.incibe.es/protege-tu-empresa/blog/respuesta-incidentes-he-restaurado-los-sistemas-y-ahora

[REF - 62]. Notificación de brechas de seguridad de los datos personales (art. 33 RGPD) https://sedeagpd.gob.es/sede-electronica-web/vistas/formBrechaSeguridad/procedimientoBrechaSeguridad.jsf

[REF - 63]. Respuesta a incidentes https://www.incibe-cert.es/respuesta-incidentes

[REF - 64]. ¿Es seguro tu escritorio remoto? https://www.incibe.es/protege-tu-empresa/blog/seguro-tu-escritorio-remoto

[REF - 65]. Ayuda ransomware https://www.incibe.es/protege-tu-empresa/herramientas/servicio-antiransomware

[REF - 66]. No More Ransom https://www.nomoreransom.org/

[REF - 67]. Copias de seguridad. Políticas de seguridad para la pyme https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/copias-seguridad.pdf

[REF - 68]. ¿Microsoft te ha llamado sin haberlo solicitado? https://www.osi.es/es/actualidad/blog/2019/04/04/microsoft-te-ha-llamado-sin-haberlo-solicitado

[REF - 69]. Navegación segura y privada para ti y tu empresa. Parte II https://www.incibe.es/protege-tu-empresa/blog/navegacion-segura-y-privada-ti-y-tu-empresa-parte-ii

[REF - 70]. Microsoft alerta sobre un aumento de estafas de soporte técnico, donde se utiliza ilegalmente su marca, e insta a reforzar la seguridad a los usuarios https://news.microsoft.com/es-es/2020/06/26/microsoft-alerta-sobre-un-aumento-de-estafas-de-soporte-tecnico-donde-se-utiliza-ilegalmente-su-marca-e-insta-a-reforzar-la-seguridad-a-los-usuarios/

[REF - 71]. Qué hacer ante una estafa de soporte técnico https://www.youtube.com/watch?v=41ZhJ8xekAQ

[REF - 72]. Notificar una estafa de soporte técnico https://www.microsoft.com/es-es/concern/scam

[REF - 73]. Detectada campaña de correos fraudulentos que difunden malware utilizando como gancho un falso pedido https://www.incibe.es/protege-tu-empresa/avisos-seguridad/detectada-campana-correos-fraudulentos-difunden-malware

[REF - 74]. Virustotal https://www.virustotal.com/gui/home/upload

[REF - 75]. MetaDefender https://metadefender.opswat.com/?lang=en

[REF - 76]. Jotti's https://virusscan.jotti.org/es-ES

[REF - 77]. Primeros pasos en la respuesta a incidentes https://www.incibe.es/protege-tu-empresa/blog/primeros-pasos-respuesta-incidentes

[REF - 78]. Respuesta a incidentes: tomando evidencias y recuperando la actividad https://www.incibe.es/protege-tu-empresa/blog/respuesta-incidentes-tomando-evidencias-y-recuperando-actividad

[REF - 79]. Guía para la gestión y notificación de brechas de seguridad https://www.aepd.es/sites/default/files/2019-09/guia-brechas-seguridad.pdf

[REF - 80]. Qué es una botnet y cómo saber si tu empresa forma parte de ella https://www.incibe.es/protege-tu-empresa/blog/botnet-y-saber-si-tu-empresa-forma-parte-ella

[REF - 81]. Oleada de correos fraudulentos que amenazan con "hackear" tu empresa https://www.incibe.es/protege-tu-empresa/avisos-seguridad/oleada-correos-fraudulentos-amenazan-hackear-tu-empresa

[REF - 82]. Importante oleada de ransomware afecta a multitud de equipos https://www.incibe.es/protege-tu-empresa/avisos-seguridad/importante-oleada-ransomware-afecta-multitud-equipos

[REF - 83]. La importancia de separar la información pública de la interna mediante zonas desmilitarizadas (DMZ) https://www.incibe.es/protege-tu-empresa/blog/segmentacion-dmz

[REF - 84]. UTM, un firewall que ha ido al gimnasio https://www.incibe.es/protege-tu-empresa/blog/utm-firewall-ha-ido-al-gimnasio

[REF - 85]. Soluciones WAF https://www.incibe.es/protege-tu-empresa/catalogo-de-ciberseguridad/buscador-soluciones?combine=waf&term_node_tid_depth_join=All&field_sol_dimension_tid=All&field_sol_empresa_target_id=All&field_sol_gratuito_value=All&submit=Buscar

[REF - 86]. ¿Sabes lo que es el malvertising y cómo estar protegido frente a él? https://www.osi.es/es/actualidad/blog/2015/05/08/sabes-lo-que-es-el-malvertising-y-como-estar-protegido-frente-el

[REF - 87]. Riesgos en el uso de extensiones para los navegadores y medidas de seguridad https://www.incibe.es/protege-tu-empresa/blog/riesgos-el-uso-extensiones-los-navegadores-y-medidas-seguridad

[REF - 88]. Aplicaciones permitidas. Políticas de seguridad para la pyme https://www.incibe.es/sites/default/files/contenidos/politicas/documentos/aplicaciones-permitidas.pdf

[REF - 89]. ¿Tu empresa ha sido víctima de un incidente de seguridad? Repórtalo https://www.incibe.es/protege-tu-empresa/blog/tu-empresa-ha-sido-victima-incidente-seguridad-reportalo

[REF - 90]. Cuerpo Nacional de Policía colaboración ciudadana https://www.policia.es/colabora.php

[REF - 91]. saber identificar este tipo de comunicaciones https://www.gdt.guardiacivil.es/webgdt/pinformar.php

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA TERCERA DEL GOBIERNO
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD
017
protege tu empresa