Ransomware

Una guía de aproximación para el empresario

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA SEGUNDA 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 DE FIGURAS

1 INTRODUCCIÓN

Estamos inmersos en una evolución tecnológica originada por la irrupción de Internet, el crecimiento exponencial de dispositivos móviles, los servicios en la nube y, más recientemente, el Internet de las cosas (IoT). Como era de esperar, esta evolución no está exenta de riesgos, ya que las mismas ventajas de inmediatez, movilidad, ubicuidad, facilidad de pago, comunicación, etc. de las que se benefician empresas, gobiernos y usuarios, son también aprovechadas por los que se dedican a realizar actividades lucrativas maliciosas.

Dentro de las actividades maliciosas que aportan a los ciberdelincuentes un rápido beneficio económico, destaca por su éxito un tipo de *malware* (*software* malicioso) enfocado a la extorsión, denominado ***ransomware***, cuyo objetivo es bloquear el acceso al dispositivo afectado o a parte de la información que contiene para después pedir un **rescate** a cambio de su desbloqueo.

La proliferación de este tipo de *malware* está relacionada con los avances en criptografía (algoritmos de cifrado que permiten acceder a la información solamente a quien conoce la clave de desbloqueo), la proliferación de dispositivos conectados a Internet, así como cada vez la más amplia utilización de **sistemas de pago internacionales con monedas virtuales que permiten el anonimato,** como *bitcoins* **[REF - 1]**. Estas circunstancias permiten a los ciberdelincuentes obtener una **alta rentabilidad económica**, al proporcionarles no solo **diversidad y permeabilidad** de los objetivos para sus ataques, sino también una gran **facilidad para ocultarse.**

El *ransomware* afecta a cualquier usuario, negocio o actividad exigiendo el pago de un rescate a cambio de la devolución del acceso a su información. Este *malware* está afectando a usuarios domésticos, negocios, gobiernos e incluso servicios críticos, como hospitales o centrales energéticas. Un ataque de *ransomware* puede **causar pérdidas temporales o permanentes de información e interrumpir la actividad normal, ocasionando pérdidas económicas o de reputación** y, en algunos casos, **graves daños a la población, cuando los ataques se producen contra las infraestructuras críticas de un país.**

El *ransomware* afecta a todo tipo de equipos: ordenadores de sobremesa y portátiles, servidores web, servidores de ficheros, otros servidores y dispositivos móviles. Actualmente, el despegue del IoT y la conexión a Internet, cada vez mayor, de dispositivos industriales hasta ahora aislados, está propiciando un nuevo ámbito de actuación para los ciberdelincuentes. Estos dispositivos

1

automatizan, por ejemplo, la iluminación, la calefacción, la cadena de producción de sus empresas o el control de su flota de vehículos. Los ciberdelincuentes aprovechan las vulnerabilidades de estos dispositivos para, entre otras acciones, infectarlos con *ransomware*, obligando a las empresas a efectuar el pago de un rescate para poder recuperar el acceso a los mismos. En esta guía proponemos actuaciones para conocer, prevenir y mitigar esta amenaza.

2 ¿QUÉ ES EL *RANSOMWARE*?

"El ***ransomware* es un tipo de *malware*** en continua evolución que **impide el acceso a la información de un dispositivo**, amenazando con destruirla o hacerla pública si las víctimas no acceden a pagar un rescate en un determinado plazo."

El *ransomware* es un tipo de *malware* **[REF - 2]** en continua evolución que impide el acceso a la información de un dispositivo, amenazando con destruirla o hacerla pública si las víctimas no acceden a pagar un rescate en un determinado plazo.

El *ransomware* se propaga, como otros tipos de *malware*, por múltiples vías: a través de campañas de *spam* **[REF- 2]**, vulnerabilidades o malas configuraciones de *software*, actualizaciones de *software* falsas, canales de descarga de *software* no confiables y herramientas de activación de programas no oficiales (*cracking*). Los ciberdelincuentes tratan de que el usuario abra un archivo adjunto infectado o haga clic en un vínculo que le lleve al sitio web del atacante, donde será infectado.

Actualmente, además del bloqueo de la información, la tendencia **[REF - 3]** es que amenacen con la fuga de información confidencial al ámbito público (Internet), lo que podría ocasionarles además del perjuicio económico, daños reputacionales, y exponerles a multas por incumplimiento de GDPR **[REF - 4]**, en caso de que se trate de datos personales de sus clientes. Esto resulta en una extorsión más intensa y, por tanto, en un alcance mayor de los resultados económicos que pueden obtener los ciberdelincuentes.

2.1. ¿Por qué se llama así?

Ransomware se forma al unir «*ransom*» (del inglés, rescate) con «*ware*» (producto o mercancía, en inglés). Una vez que el delincuente **cifra los datos, pide un rescate** (*ransom*) a la víctima, a través de un mensaje o ventana emergente, realizando lo que llamaríamos un secuestro virtual.

Este mensaje, que suele ser amenazante y apremiante, advierte a la víctima de que la única forma mediante la que puede descifrar sus archivos, recuperar el sistema o evitar un posible filtrado de información, es realizar el pago de un rescate. Es habitual que incluyan un límite de tiempo para pagar, antes de que se produzca la destrucción total de los archivos secuestrados, su publicación o un incremento del valor del rescate, si no se paga a tiempo.

Generalmente, el rescate se solicita a través de alguna criptodivisa (moneda virtual) como, por ejemplo, *bitcoins*. Es frecuente que utilicen «muleros», que son intermediarios que transfieren el dinero

procedente de estas actividades ilícitas. Tanto las monedas virtuales como los muleros permiten al ciberdelincuente ocultar su rastro.

A cambio del pago, los ciberdelincuentes prometen facilitar el mecanismo para desbloquear el ordenador o descifrar los ficheros. Sin embargo, no existen garantías de recuperar la información, por lo que **se recomienda no pagar el rescate para evitar la proliferación de este tipo de amenazas**. Además, para acceder al mecanismo de desbloqueo dirigen a la víctima a un enlace que podría a su vez contener *malware* y causar otra infección, pudiendo robar también sus contraseñas o cualquier otra información sensible. Es muy frecuente que los ordenadores infectados por *ransomware* estén también infectados con otro tipo de *malware*.

2.2. ¿Qué son las criptodivisas y por qué piden el rescate en esta moneda?

Las criptodivisas son monedas virtuales que permiten el pago casi anónimo entre particulares, lo que dificulta su rastreo. Este anonimato es posible gracias a los servicios de *mixing* o *tumbling* de criptodivisas **[REF - 5]**, accesibles desde la red anónima Tor **[REF - 6]**, que mezclan los fondos de distintas carteras, realizando una especie de lavado de la criptomoneda que dificulta que se pueda seguir el rastro de las transacciones. Esto facilita que los cibercriminales puedan extorsionar a sus víctimas sin que la policía pueda seguirles de forma inmediata la pista.

2.3. ¿Cómo infecta el *ransomware* los dispositivos?

Como ocurre en el caso de otros tipos de *malware*, los ciberdelincuentes utilizan una o varias de estas vías para infectar a la víctima:

- **Aprovechan los agujeros de seguridad (vulnerabilidades) presentes en el *software*** de los equipos, sus sistemas operativos y sus aplicaciones. Los desarrolladores de *malware* disponen de herramientas que les permiten reconocer dónde están estos agujeros de seguridad e introducir así el *malware* en los equipos.

  - Algunas variedades de *ransomware* utilizan **servidores web desactualizados** como vía de acceso para instalar el *ransomware*.

  - También se aprovechan de sistemas industriales conectados a Internet sin las medidas básicas de seguridad. Por ejemplo, cada vez hay más equipos de control de climatización, fabricación de

componentes u otros dispositivos industriales que no estaban conectados a ninguna red informática, y ahora son conectados a redes corporativas o Internet sin las mínimas medidas de seguridad.

» **Consiguen credenciales de acceso a los equipos con privilegios de administrador** mediante engaños (*phishing* **[REF- 2]** y sus variantes), debilidades de procedimiento (por ejemplo, no obligar a cambiar el usuario y contraseña establecidos por defecto), vulnerabilidades del *software* o utilización de malas prácticas de diseño como el *hard-code* de contraseñas (que consiste en incrustar las mismas en el código fuente de los programas). Con el acceso a estas cuentas podrán instalar *software*, en este caso *malware*, en los equipos.

- Muchos de los dispositivos industriales y dispositivos IoT que se están conectando últimamente a Internet, conservan las mismas credenciales genéricas (de fábrica o por defecto) de acceso y administración, están «hardcodeados» o simplemente carecen de ellas.

» **Engañan a los usuarios, mediante técnicas de ingeniería social, [REF - 7]** para que instalen el *malware*. Esta es la vía más frecuente y la más fácil para el ciberdelincuente. Por ejemplo, mediante el envío de un correo falso o *phishing* con un enlace o un adjunto con una supuesta factura que en realidad instala el *malware*. También utilizan estas técnicas a través de redes sociales o servicios de mensajería instantánea.

» **Envían correos *spam*** con enlaces web maliciosos o ficheros que contienen el *malware*. A pesar de que la mayoría de los servicios de correo electrónico los filtran, siempre hay un porcentaje de receptores que van a hacer clic o descargar el fichero.

» **Utilizan métodos conocidos como *drive-by download* y *watering hole* [REF - 8]**, que consisten en dirigir a las víctimas a sitios web infectados previamente, descargando el *malware* sin que ellas se percaten, aprovechando las vulnerabilidades de su navegador. También utilizan técnicas de ***malvertising* [REF - 9]**, que consiste en incrustar anuncios maliciosos en sitios web legítimos. Cuando el usuario visita ese sitio web del anuncio, que generalmente suplanta a otro legítimo, puede ser infectado sin necesidad de descargar ninguna aplicación. Esta técnica se emplea para instalar *malware*, que a su vez puede derivar en una infección por *ransomware*.

2

- **Aprovechan servicios expuestos a Internet**, como por ejemplo, el escritorio remoto **[REF- 10]**, que permiten abrir una puerta a un posible ataque. Estos servicios expuestos si no cuentan con las medidas de seguridad necesarias pueden suponer el origen de un incidente de seguridad, como puede ser una infección por *ransomware*.

2.4. Tipos de *ransomware*

De menor a mayor importancia podemos clasificar el *ransomware* en general en:

- ***Hoax ransomware:*** solo simula el cifrado utilizando técnicas de ingeniería social para extorsionar al usuario, exigiéndole un pago por recuperar sus archivos o evitar que sean eliminados. Se trata en realidad de un tipo de *ransomware* simulado.

- ***Scareware:*** utiliza el señuelo del falso *software* o soporte. Generalmente, aparece en forma de anuncio molesto emergente que informa de una supuesta infección por virus y aporta una solución fácil y rápida, descargando un programa de limpieza que casi siempre es el *malware*. El propio anuncio emergente lanzado por la página visitada no suele suponer una amenaza en sí mismo, aunque se recomienda no hacer clic en sus enlaces y prestar atención al cierre de la ventana emergente, ya que suele incluir botones de cierre falso.

- **Bloqueadores de pantalla:** impiden el uso del dispositivo mostrando una ventana que ocupa toda la pantalla y no permite ser cerrada. En la ventana, generalmente, pueden aparecer dos tipos de mensaje:

  - En algunos casos se informa del cifrado de archivos y el procedimiento para recuperarlos, pero los archivos están intactos. En este caso, únicamente se ha producido un bloqueo de la pantalla.

  - En otros casos, un mensaje de las fuerzas de seguridad indican que se han detectado actividades ilegales y se solicita el pago de una sanción para desbloquear el equipo (también conocido como el virus de la policía **[REF - 11]**), pero en ningún caso este mensaje tiene relación con las fuerzas de seguridad estatales.

- ***Ransomware* de cifrado:** considerado el más peligroso de todos. Su principal objetivo es el cifrado de la información para exigir un rescate. Los ciberdelincuentes hacen uso de los últimos avances en cifrado de

2

información para evitar que los datos puedan ser descifrados. Dentro de esta variante hay una llamada *wiper*, que no devuelve el acceso a los archivos, simplemente los elimina.

» ***Doxware:*** emplea una técnica conocida como *doxing* **[REF - 12]**, que consiste en amenazar al usuario con hacer públicos los datos personales extraídos. Esta técnica provoca un aumento de la presión al usuario, lo que se traduce en un incremento de la efectividad del ataque y del beneficio para el ciberdelincuente.

Ilustración 1: Ejemplo de un ransomware de tipo doxware amenazando con filtrar datos privados

En resumen, el *ransomware* es una actividad delictiva muy ventajosa para los ciberdelincuentes que afecta a todo tipo de empresas **[REF - 13]**. Desde sus comienzos, este tipo de *malware* se ha ido haciendo cada vez más sofisticado y destructivo, evolucionando para evadir las detecciones por parte de aplicaciones especializadas **[REF - 14]**. Algunos *ransomware* vienen asociados a otros tipos de *malware* que roban información (cuentas de bancos, credenciales de acceso...), abren puertas traseras (*backdoors*) **[REF - 2]** o instalan *botnets* **[REF - 15]**. Se adaptan incluso con mensajes de rescate en el idioma de las víctimas. También aparecen nuevas variantes para dispositivos móviles, industriales e IoT, y nuevas formas de extorsión, como las amenazas de difundir la información obtenida, antes mencionado como *doxing*. Por otra parte, la aparición de las criptomonedas y sus mecanismos de «lavado» garantizan un sistema de pago anónimo de los rescates.

Los avances en la complejidad de los algoritmos de cifrado permitieron que mejoraran su mecanismo de extorsión. Antes solo utilizaban programas que bloqueaban el sistema; ahora, pueden cifrar también la información que se

2

encuentra en los discos duros y otros sistemas de almacenamiento de sus víctimas, haciendo más difícil su recuperación. Esto permite aumentar el valor del rescate. Algunas variedades cifran, además del equipo infectado, los dispositivos de almacenamiento conectados, los dispositivos de almacenamiento en red compartidos que tengan asociados o los servicios en la nube que estén mapeados en el ordenador infectado.

3 ¿CÓMO PUEDO PROTEGERME?

"Para protegerte ante el *ransomware* es necesario evitar **caer víctima de engaños** conociendo las técnicas de ingeniería social más comunes, **y configurar y mantener los sistemas evitando que sean técnicamente vulnerables.**"

Para protegerse ante el *ransomware* es necesario adoptar una serie de buenas prácticas y considerar dos propósitos principales: por una parte, evitar caer víctimas de engaños conociendo las técnicas de ingeniería social más comunes; y por otra parte, configurar y mantener los sistemas evitando que sean técnicamente vulnerables. Los apartados siguientes desarrollan estas buenas prácticas.

3.1 Concienciación y formación

En el momento de edición de esta guía, la mayor parte de las infecciones por *ransomware* están teniendo lugar por medio de engaños de ingeniería social, y aproximadamente casi el 75% de las veces logran llevar a cabo con éxito el ciberataque. Los usuarios son engañados para realizar una determinada acción de su interés, que permitirá al ciberdelincuente instalar un *malware* con el que podrá infectar el dispositivo.

Es esencial que **formemos y concienciemos a nuestros empleados, enseñándoles a reconocer estas situaciones y cómo actuar en consecuencia.**

Los usuarios han de conocer las políticas **[REF - 16]** de la empresa en materia de ciberseguridad, como por ejemplo, las relativas al uso permitido de aplicaciones y dispositivos, el uso de wifis públicas, la seguridad en el puesto de trabajo y en movilidad o la política de contraseñas.

3.1.1. ¿Cómo funciona un ataque de ingeniería social?

Los ataques de ingeniería social **[REF - 17]** no son muy distintos de los clásicos timos. El ciberdelincuente sigue los mismos pasos que el timador presencial: reconocimiento, establecimiento, contacto y confianza, y manipulación para obtener su objetivo y alejarse del escenario sin levantar sospechas.

3

El primer paso es intentar reunir toda la información posible sobre la empresa que le pueda ser útil para conocer a su víctima, como listados de empleados y teléfonos, departamentos, ubicación, proveedores, etc.

A continuación seleccionará una víctima (generalmente un empleado o algún colaborador de la empresa) y tratará de establecer alguna relación con ella que le permita ganarse su confianza, para lo que utilizará información obtenida de un servicio de su confianza: su banco, la empresa de mantenimiento informático, una situación particular, etc.

Una vez se ha ganado su confianza, manipula a la víctima para obtener los datos que necesita (credenciales, información confidencial, etc.) o conseguir que realice alguna acción por él (instalar un programa, enviar algunos correos, hacer algún ingreso...).

Las técnicas para conseguir la confianza y manipular a la víctima son diversas y se aprovechan:

- del respeto a la autoridad, cuando el atacante se hace pasar por un responsable superior de la empresa o por un miembro de las Fuerzas y Cuerpos de Seguridad del Estado (FCSE);
- de la voluntad de ser útil, ayudar o colaborar que se aprecia en entornos laborales y comerciales;
- o del temor a perder algo, como en los mensajes en los que se pide hacer un ingreso para obtener un trabajo, una recompensa, un premio, etc.
- también apelan al ego de los individuos al decirles que han ganado un premio o han conseguido algo y que para obtenerlo tienen que realizar una acción que en otro caso no harían;
- o crean situaciones de urgencia y consiguiendo los objetivos por pereza, desconocimiento o ingenuidad de la víctima.

Por último, tras conseguir su objetivo tienen que apartarse sin levantar sospechas. En ocasiones, destruyen las pruebas que puedan vincularles con alguna actividad delictiva posterior que ejecuten con la información obtenida (por ejemplo, accesos no autorizados si obtienen las credenciales, publicación de información comprometida...).

3

3.1.2 ¿Cómo reconocer un ataque de ingeniería social?

Para evitar el *ransomware*, o cualquier tipo similar de ataque realizado mediante ingeniería social, desconfíe de todos los mensajes recibidos por correo electrónico, SMS, aplicaciones de mensajería instantánea o redes sociales, en el que se le coaccione o apremie a hacer una acción ante una posible sanción.

Como pautas generales, para evitar ser víctima de fraudes de tipo *ransomware* se aconseja:

- **No abrir correos de usuarios desconocidos o que no haya solicitado,** elimínelos directamente. No conteste en ningún caso a estos correos.
- **Revisar los enlaces antes de hacer clic** aunque sean de contactos conocidos. Desconfíe de los enlaces acortados o utilice algún servicio para expandirlos antes de visitarlos.
- **Desconfiar de los ficheros adjuntos** aunque sean de contactos conocidos.
- **Tener siempre actualizado el sistema operativo y el *software antimalware*** desde repositorios oficiales. En el caso del *software antimalware* comprobar además que se encuentra activo.
- **Asegurarse de que las cuentas de usuario de sus empleados usan contraseñas robustas y no tienen más permisos de los necesarios** para desempeñar su labor.
- Únicamente **instalar aplicaciones permitidas y necesarias para el trabajo que provengan de fuentes oficiales.**

3.2. Prevención

Para evitar el *ransomware* podemos adoptar una serie de medidas técnicas para que nuestros sistemas no tengan agujeros de seguridad, manteniéndolos actualizados y bien configurados.

En primer lugar, tendremos que **adoptar un buen diseño** de nuestra red, por ejemplo, realizando *subnetting* o segmentación de redes, para evitar que expongamos servicios internos al exterior y que toda la red se pueda ver comprometida, de manera que sea más difícil para el ciberdelincuente infectarnos.

3

Por otra parte, se han de describir de forma clara y concisa las actuaciones para **mantener actualizado todo el *software*** de los dispositivos, **realizar copias de seguridad** periódicas, **controlar los accesos, restringir el uso de aplicaciones o equipos no permitidos, desactivar los complementos o extensiones no utilizadas** de los navegadores, **actuar de forma rápida** en caso de incidente, **mostrar las extensiones de archivo y formar a los usuarios** en la detección de amenazas mediante esta técnica.

No debemos olvidar tampoco la instalación y actualización periódica de *software* específico conocido como *antiransomware*, además de los antivirus convencionales y otras herramientas *antimalware*.

Por último, la **vigilancia** y las **auditorías** van a mantenernos alerta ante cualquier sospecha.

3.2.1 Copias de seguridad

En caso de que seamos objeto de un ataque de *ransomware*, la **principal medida de seguridad** que va a permitirnos recuperar la actividad de nuestra empresa en poco tiempo, es realizar copias de seguridad o *backups* **[REF -19]**.

Estas son las recomendaciones básicas en cuanto a las copias de seguridad:

- Haz y conserva al menos **tres copias de seguridad actualizadas y en distintos soportes.** En el caso de que hayamos sufrido un ataque por *ransomware* tenemos tres opciones: pagar el rescate, recuperar la información desde una copia de seguridad o asumir que hemos perdido nuestros datos. De estas tres opciones, la mejor, sin lugar a dudas, es recuperar nuestros contenidos desde un *backup*. Y como los *backups* también pueden fallar, se recomienda mantener al menos tres copias actualizadas en todo momento, por ejemplo: disco duro específico para copias, USB externo y nube.

- Guarda las copias de seguridad en un **lugar diferente al del servidor de ficheros.** Dado que existen variantes de *ransomware* que cifran la información (incluidos los ficheros de las copias de seguridad) de discos duros o sistemas de almacenamiento de red distintos al equipo infectado, lo ideal es almacenarlos, siempre que sea posible, en discos físicos (DVD o *Blu-Ray*) o en soportes externos no conectados a nuestra red).

- Si haces copia de seguridad y la alojas en la nube (*backup* en *cloud*), esta se sincroniza continuamente. Recuerda que algunas familias de *ransomware*

3

también cifran y bloquean las copias de seguridad en la nube, por lo que es conveniente **desactivar la sincronización persistente.**

- Comprueba regularmente que las copias de seguridad que tienes almacenadas **funcionan correctamente y sabes los pasos para recuperarlas.** Las copias de seguridad también pueden corromperse. Por ello, es necesario un chequeo periódico de esa copia de respaldo, para lo que hay que probar a restaurar algunos ficheros cada cierto tiempo.

- Finalmente, **para evitar el *ransomware* que amenaza con el filtrado de tus datos, cifra la información más sensible para que, en caso de robo de tus ficheros, los ciberdelincuentes no puedan hacer pública la información.** No olvides que no debes guardar la clave de cifrado en el mismo dispositivo, y si empleas un certificado para descifrarla, guárdalo en una memoria USB y mantenla desconectada de tus equipos.

3.2.2. Navega seguro

Utiliza **redes privadas virtuales (VPN, por sus siglas en inglés)** **[REF - 20]** siempre que sea posible. Las redes privadas virtuales son un tipo de conexión de red en el que el tráfico viaja cifrado y en el que los atacantes no pueden visualizar su contenido. Este tipo de conexiones se suelen utilizar cuando estamos fuera de la empresa y queremos acceder a cualquier documento que tengamos en la intranet o en nuestro equipo corporativo. De esta forma, tendremos acceso a todos nuestros documentos y a la vez navegaremos seguros.

Evita visitar también sitios web de contenido dudoso. Como se ha comentado anteriormente, existen páginas web que, aparentando ser legítimas, esconden los llamados *exploit kits*, que detectan las vulnerabilidades de nuestro navegador web y las aprovechan para instalar *ransomware* en nuestro dispositivo. Para evitar esto, como siempre, es recomendable **mantener actualizados los navegadores web,** el sistema operativo y, por supuesto, **cualquier solución de seguridad** que empleemos, **sin olvidar la lógica y el sentido común en nuestras actividades online.**

3.2.3. Actualiza

Los ciberdelincuentes se aprovechan de las vulnerabilidades o agujeros de seguridad en el *software*, los sistemas operativos o el *firmware*, incluso de forma automatizada (*exploit kits*). Por ello, cuanto más actualizados estén los sistemas que utilizas, menos vulnerabilidades tendrán y más difícil será que puedan entrar o infectarte.

3

Asegúrate de que los sistemas operativos, aplicaciones y dispositivos tengan habilitada la **instalación de actualizaciones de forma automática.**

Si utilizas *software* a medida, asegúrate de que en su diseño se han tenido en cuenta requisitos de seguridad y que cuentas con actualizaciones. Solicita la asistencia de expertos en auditorías del *software* para evitar las vulnerabilidades de este tipo de *software*.

3.2.4. Mínimos privilegios

Un principio básico de seguridad es mantener los privilegios de seguridad al mínimo; es decir, evitar que los usuarios y grupos de usuarios tengan más privilegios de los que necesitan. Esto es posible gestionando los privilegios para acceder a la información o para instalar *software*.

Para los usuarios generales se han de utilizar **cuentas que tengan privilegios limitados,** en lugar de las cuentas con privilegios de «administrador». Así evitamos que los usuarios generales tengan acceso a servicios, información o procedimientos que no necesitan para su actividad. Esto proporciona una protección adicional al impedir que se instalen distintos tipos de *malware*, por error o si perdieran o les robaran sus credenciales. Las cuentas con privilegios deben ser solo utilizadas por los administradores. Estos son algunos consejos básicos en cuanto al uso de cuentas de usuario:

- **Utiliza contraseñas robustas [REF - 21]**. Generalmente, los atacantes obtienen una mayor tasa de éxito cuanto más fácil sea descifrar nuestra contraseña. Para ello, utilizan herramientas específicas de descifrado basadas generalmente en palabras de diccionario. Por este motivo, es de vital importancia utilizar siempre contraseñas robustas y políticas de bloqueo (en aquellos sistemas que lo permitan por directivas) para que, en caso de que se realice un número determinado de intentos de acceso sin éxito al sistema, se bloquee al atacante durante un tiempo que le impida desarrollar un ataque de descifrado por fuerza bruta, es decir, probando combinaciones aleatorias de letras, símbolos y números. Este tiempo de bloqueo hace que el tiempo de descifrado sea lo suficientemente grande como para desistir e intentarlo con otra víctima cuyo perfil de seguridad sea más bajo.

- **No utilices cuentas con permisos de administrador.** Si usamos este tipo de usuario y nuestra contraseña llega a manos del atacante, este tendrá un control total sobre nuestro equipo. Si, en cambio, usamos cuentas de usuario con permisos limitados, hacemos que el atacante lo tenga más difícil para llegar a datos críticos.

3

- **Elimina o deshabilita aquellas cuentas de usuario que no sean necesarias.** Cualquier cuenta que tenga acceso a nuestro equipo es una posible fuente de acceso al mismo. No hace falta tener una cuenta de «invitado». Si no usamos algo, mejor quitarlo. También debemos eliminar las cuentas que ya no se utilicen y la de los empleados que no pertenezcan ya a nuestra empresa.

- **No utilices pósits para anotar las contraseñas de tu empresa,** cualquier persona ajena podría verlas. Utiliza los gestores de contraseñas, aplicaciones específicas para que no tengas que recordar más que una sola contraseña (la del gestor) para todo.

Una buena práctica también es **organizar los datos** **[REF - 22]** según su importancia para la empresa: en qué parte de la organización se utilizan, por quién y las medidas de seguridad que necesitan. Así se podrán aplicar medidas para **separar física y lógicamente** los lugares donde se ubica la información y aplicar controles de acceso por perfiles o grupos (por ejemplo, los de contabilidad acceden a los programas y datos de contabilidad, pero no a otros) o medidas de protección especiales (como cifrado) en casos de información más sensible o confidencial. Una forma de separar aplicaciones o sistemas críticos es **utilizar entornos virtualizados** **[REF - 23]**.

No debemos olvidar guardar *logs* (registros) del uso de ficheros y del acceso externo a los dispositivos perimetrales (rúteres, cortafuegos, etc.) que nos permitirán poder investigar cualquier posible incidencia y aportar datos en caso de denuncia o poder demostrar ante un seguro (ciberseguro) **[REF - 24]** que efectivamente hemos sufrido un ataque.

Asimismo, es recomendable utilizar políticas para **evitar que los empleados instalen aplicaciones no permitidas** y usar filtros para controlar el tráfico de navegación en la empresa, autorizando las páginas confiables y aquellas estrictamente indispensables.

Las políticas de restricción del uso del *software* también pueden incluir controles para evitar que se ejecute *malware* desde carpetas temporales de los navegadores o desde programas de compresión/descompresión de ficheros o las carpetas ocultas del sistema. Actualmente, algunos sistemas operativos ya incorporan sistemas específicos de protección contra el *ransomware*.

3

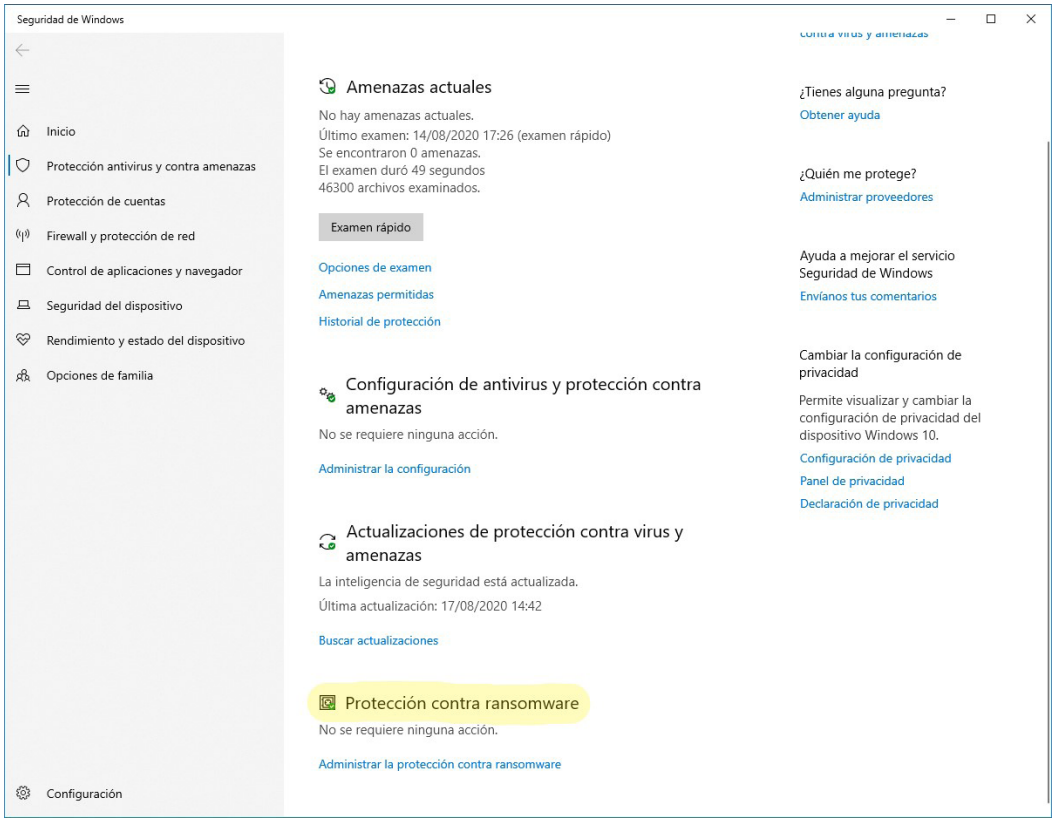

Ilustración 2: Ejemplo de protección integrada contra ransomware en un Windows® 10 Pro

3.2.5. Mínima exposición

Otro principio básico de seguridad es el de **mínima exposición**; es decir, evitar la exposición al exterior de la red interna de la empresa o de aquella información o servicio que no necesita ser accedido desde el exterior de la misma.

Las empresas necesitan ofrecer algunos servicios a través de Internet a sus clientes o trabajadores: correo electrónico, página web corporativa, aplicaciones remotas o repositorios de ficheros. Algunas empresas optan por la subcontratación de estos servicios, otras prefieren hacerlo internamente y asumen la instalación y gestión de los servidores y equipos en sus propios locales, de forma que puedan ahorrar costes y aumentar el control sobre su información.

En este caso es necesario separar los servidores accesibles desde el exterior de los servidores privados de nuestra organización. Para hacer que aquellos servidores que queremos sean accesibles desde Internet, es necesario abrir una parte de nuestra red, evitando siempre que el resto de la misma quede desprotegida: esto se consigue mediante el uso de cortafuegos.

3

Un **cortafuegos o *firewall*** **[REF - 25]** es un sistema de seguridad capaz de establecer reglas para bloquear o permitir conexiones de entrada o salida de nuestra red. Para que el cortafuegos «sepa» lo que está permitido y lo que no, deberemos configurar:

- Qué tipo de conexiones permitimos (web, correo, chat, descargas P2P, etc.).
- En qué sentido las permitimos: entrantes (desde Internet) o salientes (hacia Internet).
- A qué equipos afecta (a todos los equipos, solo a uno o a un conjunto de ellos).
- Qué direcciones IP están bloqueadas (por estar en listados de IP maliciosas).

Actualmente, existen cortafuegos de código abierto (*open source*) **[REF - 26]**, es decir, mantenidos por una comunidad de usuarios que generalmente suelen ser gratuitos y de alta eficiencia y seguridad y que, además, permiten el uso corporativo. Algunos de estos cortafuegos incluyen lo que se denomina IDS e IPS **[REF - 27]**, sistemas de prevención y detección de intrusiones que ayudarán a mantener segura la red interna de nuestra empresa mediante un control pasivo y activo simultáneamente.

Además, una medida básica de seguridad es deshabilitar el protocolo de acceso remoto (RDP o escritorio remoto en Windows) **[REF- 10]** a los sistemas si no se está utilizando o cambiar el puerto por defecto en caso de ser utilizado. Actualmente, no se considera seguro el acceso al escritorio remoto de forma directa, es recomendable implementar el uso de redes VPN o utilizar sistemas específicos más seguros, como *Direct Access* de Microsoft **[REF - 28]**.

En ocasiones, un cortafuegos no es suficiente para proteger nuestros servidores internos. Una vez hemos permitido el acceso a nuestra red, un posible atacante podría aprovechar una vulnerabilidad de nuestro servidor para comprometerlo, y desde ahí, intentar atacar a otros servidores o dispositivos de la red interna a los que, en un principio, no tiene acceso desde el exterior de la red. Para evitar esta posible brecha de seguridad existe una configuración denominada **zona (o red) desmilitarizada o DMZ** **[REF - 29]**.

3

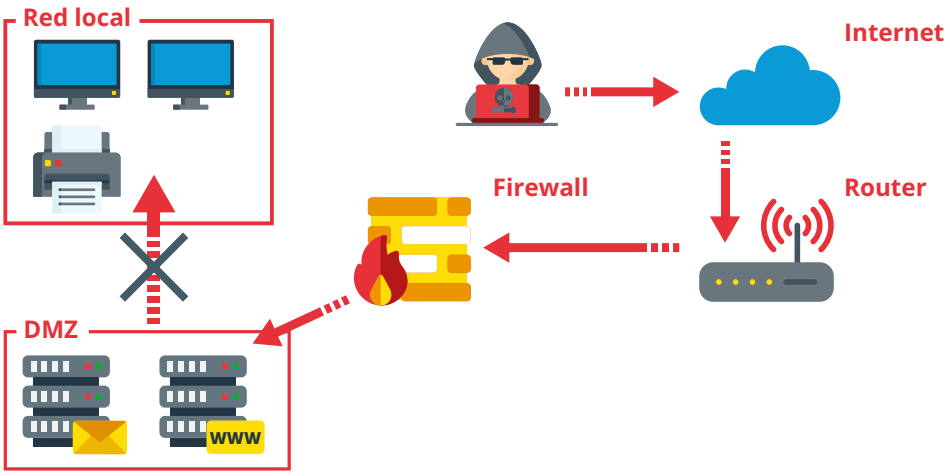

Ilustración 3: Esquema DMZ y cómo protege la red interna frente a ataques externos

Una red DMZ es una red aislada del resto de la red interna, donde se ubican únicamente los servidores que deben ser accesibles desde Internet. De esta forma, si se ataca y compromete uno de estos servidores, el resto de la red estará protegida.

Esta red DMZ, por el hecho de estar expuesta a ataques desde Internet, deberá estar especialmente controlada y monitorizada, siendo muy recomendable **instalar detectores de intrusos**, tener especial cuidado a la hora de **proteger y configurar sus servidores** y considerarlos prioritarios a la hora de **instalar actualizaciones y parches de seguridad críticos.**

Algunos ejemplos de equipos candidatos a estar dentro de una DMZ serían:

- Servidores de correo y *Webmail*.
- Servidores de VPN (redes privadas virtuales). Antes de desplegar este tipo de servidores es recomendable realizar un estudio de las necesidades y topología de la red de la empresa.
- Servidores DNS (Servidor de Nombres de Dominio).

Si contratamos servicios tecnológicos o externalizamos alguno de ellos sobre las instalaciones de proveedores, hemos de incluir en los acuerdos de nivel de servicio **[REF - 30]** las cláusulas que nos permitan verificar que toman estas medidas de mínima exposición y el resto de medidas técnicas de este apartado.

3

3.2.6. Configurar el correo electrónico

El correo electrónico es una de las principales vías de entrada de correos de *phishing* con los que intentarán robarnos las contraseñas de acceso a nuestros servicios, y otros con engaños para que instalemos *malware* o visitemos páginas donde infectarnos. Por ello, los servidores de correo electrónico deben:

- Contar con **filtros de *spam* para evitar que los *emails* de *phishing* lleguen al buzón de los empleados**. Este filtro debe estar activado y configurado y revisarse de forma continua. De esta manera, se evita que el empleado tome la decisión de abrir ficheros adjuntos o que haga clic en enlaces potencialmente peligrosos para él y para la empresa. En algunas ocasiones, el propio proveedor de dominio aporta un filtro de *spam* con varios niveles de sensibilidad, que es mantenido por ellos y que puede ser activado para todas las direcciones de correo de la empresa, ahorrándonos así el coste y tiempo de mantenimiento.

- Evitar el *email spoofing* o suplantación de correo electrónico utilizando **autenticación de correos entrantes** (existen distintos protocolos que pueden ayudar si se implementan y configuran: *Sender Policy Framework* (SPF), *Domain Message Authentication Reporting and Conformance* (DMARC) y *Domain Keys Identified Mail* (DKIM) **[REF - 31]**.

- **Escanear los correos entrantes y salientes** con un antivirus actualizado para detectar amenazas y filtrar ficheros potencialmente maliciosos. Es recomendable fijarse siempre en las extensiones de los archivos recibidos y ver si son coherentes con el nombre, por ejemplo: «factura.pdf.exe» no es un archivo legítimo, sino todo lo contrario. Este tipo de prácticas es muy común en los correos que contienen *malware*. Para poder visualizar las extensiones de archivo deberá estar habilitada esta opción específicamente en algunos sistemas.

- **Deshabilitar las macros** de los ficheros de Office o de cualquier otra suite ofimática, o bien, utilizar un previsualizador de documentos (existen alternativas online) en lugar de abrir los ficheros directamente con los programas ofimáticos.

- **Desactivar la visualización en formato HTML** en las cuentas de correo críticas o a disposición del público para contactar con la empresa. Este formato permite incluir un lenguaje de programación denominado *JavaScript*, muy utilizado para funcionalidades que nos ofrece el correo electrónico. Esta funcionalidad puede hacer que los *spammers* verifiquen

3

que la dirección de correo electrónico es válida o redirigir el navegador web del usuario a una página maliciosa que acabe infectando nuestro ordenador. De esta manera, no sería posible la visualización de correos electrónicos atractivos, pero sería mucho más seguro.

» **Utilizar entornos virtuales** para abrir los archivos sospechosos. No los abras directamente en un equipo de la empresa con información sensible. Recientemente, en algunas versiones de Windows 10, generalmente usadas en empresas, existe la opción «*Sandbox*», un entorno virtual de muy rápida ejecución pensado para estos casos. Si tu sistema no dispone de esta opción, puedes emplear herramientas de terceros como *Cuckoo Sandbox* **[REF - 32]**, compatible con la mayoría de plataformas.

3.2.7. Plan de respuesta a incidentes

Otra acción de carácter preventivo es la de contar con un plan de actuación o respuesta ante incidentes **[REF - 33]**. Esta es una representación esquemática de las fases que ha de tener:

Ilustración 4 Fases de un plan de respuesta a incidentes

» En la fase de **preparación** tenemos que tener en cuenta:

- Quién ha de realizar la gestión de los incidentes dentro de la empresa.

- Dónde está la documentación necesaria sobre los sistemas y redes que se usan en la organización. Habrá que definir cuál es la actividad normal que nos permita detectar actividades sospechosas que sean indicios de incidentes.

- Con quién tendremos que contactar en caso de incidencia. Por ejemplo, en el caso de servicios externalizados, el responsable es el proveedor. También es útil, en caso de sufrir un incidente,

3

contactar con algún centro de respuesta ante incidentes, como puede ser INCIBE-CERT de INCIBE **[REF - 34]**, en el que nos indicarán cómo podemos recuperar nuestros archivos si existiera ya algún mecanismo exitoso.

- En la fase de **detección y análisis** se ha de **clasificar el incidente** para determinar qué es un *ransomware*, su origen, la criticidad de los sistemas afectados, etc. También en esta fase hay que escalar el incidente, en el caso de que no tengamos recursos propios para resolverlo o necesitemos contar con expertos externos para su resolución.

- En la fase de **contención, resolución y recuperación**, se han de seguir los pasos para recuperar la actividad y los datos que se indican en el punto 4.1.

- **Una vez cerrado el incidente** debemos registrar todos los datos necesarios sobre el mismo: usuarios afectados, equipos, qué acciones se han tomado, resultados, etc. Con esto se pueden detectar mejoras para actuar en caso de que se repita un incidente similar.

3.2.8. Audita

Una buena práctica básica es **escanear los equipos con un *software antimalware*** y programarlo para que se ejecute periódicamente. Este *software* ha de estar actualizado y activo.

También es recomendable realizar periódicamente una **auditoría** a nuestros sistemas, tanto para poner a prueba nuestros mecanismos de seguridad como para comprobar nuestra capacidad de defensa ante los ataques. En la actualidad, esta tarea se está simplificado de forma significativa, pues existen productos y servicios para automatizarla. No obstante, sigue siendo necesario que las realice personal especializado de la empresa o, en caso de no contar con dicho personal, un servicio externalizado.

Estos son los aspectos que deben considerarse, para prevención del *ransomware*, cuando solicitamos una auditoría:

- protección **antivirus, antispam** y de filtrado de contenidos;

- administración de permisos de usuarios **y accesos** a servicios;

- seguridad de los **dispositivos móviles**;

3

- gestión automatizada de **actualizaciones y parches**;
- detección de **vulnerabilidades**;
- monitorización del **uso de los recursos** informáticos y de red; y
- monitorización y análisis de **eventos de seguridad** en tiempo real (SIEM).

Estos son los distintos tipos de pruebas que puedes solicitar:

- **Test de penetración:** es un tipo de auditoría técnica que consiste en un conjunto de pruebas a las que se somete a una aplicación, servicio o sistema, con el objetivo de encontrar huecos o fallos a través de los cuales sería posible conseguir acceso no autorizado a información de la empresa.

- **Auditoría de red:** permite analizar la red de la empresa en busca de puertos abiertos, recursos compartidos, servicios o electrónica de red (rúter, *switch*, etc.). Además, en esta auditoría se emplean herramientas que permiten realizar la catalogación de las infraestructuras conectadas a la red o incluso detectar versiones de dispositivos inseguros, versiones de *software* o la necesidad de instalar actualizaciones o parches.

- **Auditoría de seguridad perimetral:** se trata de un proceso destinado a determinar el nivel de seguridad de las barreras que protegen la red de comunicaciones de una organización de los riesgos que provienen del exterior y del interior. Podríamos englobarla dentro de la auditoría de red, aunque está más especializada en detectar fallos de seguridad desde el punto de vista del exterior.

- **Auditoría web:** analiza los fallos de seguridad o vulnerabilidades que afectan al funcionamiento de una página web.

- **Auditoría forense:** auditoría posterior a un incidente de ciberseguridad para identificar las causas que lo produjeron. Tiene como objetivo recabar y preservar las pruebas o evidencias de un incidente para, tras su posterior análisis, saber qué y cómo ha ocurrido, aprender de ello y depurar las posibles consecuencias legales.

En INCIBE tenemos a tu disposición el "Catálogo de soluciones y empresas de ciberseguridad" **[REF - 24]** donde podrás encontrar servicios de auditoría, entre otros.

4 ¿QUÉ HACER SI ME AFECTA?

"Si has sufrido un **incidente de seguridad: *ransomware***, lo primero es apagar el equipo afectado, no pagar nunca el rescate, aplicar el plan de respuestas ante incidentes y utilizar la copia de seguridad de tu información."

Si has sufrido un incidente de seguridad en el que tus datos han sido cifrados y te están extorsionando para que pagues un rescate, has de conocer cómo actuar. Recuerda que lo primero es apagar el equipo afectado para que no se extienda a otros dispositivos de la red interna. En todos los casos debes seguir estas dos recomendaciones:

- **No pagar nunca el rescate**, ya que esto no garantiza que puedas recuperar la información ni que no vuelvan a exigirte un segundo rescate.
- Si contamos con un **plan de respuesta ante incidentes** **[REF - 35]**, lo aplicaremos para poder minimizar en la medida de lo posible los daños causados y recuperar la actividad corporativa lo antes posible. Este plan de respuesta nos marcará las pautas a seguir para la obtención de evidencias que sirvan para una posible denuncia de la acción delictiva.
- Si no tienes plan de respuesta ante incidentes, utiliza la última **copia de seguridad** de tu información para recuperar la información perdida.

4.1. ¿Cómo recupero mi actividad y mis datos?

Con el objetivo de recuperar la actividad lo antes posible y evitar mayores pérdidas económicas, podemos realizar una serie de acciones encaminadas a recuperar los datos y continuar con el normal funcionamiento de la actividad empresarial:

4

Ilustración 5 Etapas para recuperar la actividad de la empresa

1. Aísla el equipo de la red: esto evitará que el ciberataque se propague a otros dispositivos. Sospecha de discos duros, unidades de red o servicios en la nube que tuvieras conectados por si el *ransomware* se hubiera propagado y también estuvieran afectados.

- **Cambia inmediatamente todas las contraseñas** de red y de cuentas online. Una vez se ha eliminado el *ransomware*, vuelve a cambiarlas. Recuerda que una contraseña debe ser robusta, fuerte y única para cada servicio.

2. Clona el disco duro: se recomienda realizar una clonación completa del disco. De esta manera, podrás mantener el dispositivo original y así intentar recuperar los datos sobre el clon. Si no existiera solución a día de hoy, es posible que en el futuro sí la haya, por lo que podrías llegar a recuperar tus ficheros.

- Como solución en caso de que no exista denuncia, **conecta el disco duro del equipo afectado a otro** ordenador aislado de la red y preparado para pruebas y no arranques con él, utilízalo de «esclavo» para poder comprobar qué información se ha salvado y **hacer una copia**. Debes tener cuidado de **salvar solo los datos importantes (documentos, fotos, certificados…) y no archivos ejecutables o programas** que puedan volver a infectar de nuevo al equipo.

- Si fuera posible **recoge y aísla muestras de ficheros cifrados o del propio *ransomware***, como el fichero adjunto en el mensaje desde el que nos infectamos.

4

» **Denuncia el incidente [REF - 36 Y 37]**:

- Guardia civil – Grupo de delitos telemáticos
- Policía Nacional – Brigada de Investigación Tecnológica (BIT)

» **Cambia el disco duro.** También puedes extraer el disco duro afectado y conservarlo como prueba o mantenerlo almacenado por si, posteriormente, aparece una solución de descifrado de la información que permita recuperar su contenido.

3. Desinfecta el disco clonado: sería el siguiente paso para intentar después recuperarlo. Para ello, se debe utilizar una herramienta antivirus o *antimalware* actualizada. Es muy importante eliminar el *software* malicioso y sus posibles persistencias antes de recuperar los datos, ya que si no se hace, podrían volver a ser cifrados.

4. Recupera y restaura los equipos para continuar con la actividad. Si fuera posible reinstala el equipo con el *software* original o arranca en modo seguro y recupera un *backup* previo si lo tuvieras.

A) Intenta recuperar los datos: con el disco desinfectado podremos iniciar el proceso para intentar recuperar los datos.

Se recomienda utilizar la página web www.nomoreransom.org **[REF - 38]**, que es un proyecto colaborativo avalado por la **EUROPOL** y que cuenta con una base de datos de ataques de este tipo, así como las soluciones (si existieran). Accede a la sección de *Crypto-sheriff* para identificar correctamente la variante que te ha infectado. Te harán falta dos ficheros cifrados o la nota de rescate. Recuerda **leer antes las normas para el envío de datos.**

» **Si existe una solución,** la página te ofrecerá la herramienta para descifrar los ficheros y un manual explicativo que contiene la información detallada de cómo utilizarla. Léela con detalle antes de ponerla en práctica y contacta con tu soporte informático.

» **Si no existe solución,** conserva el disco cifrado por si apareciera una solución en el futuro.

Puedes contactar con la **Línea de Ayuda en Ciberseguridad [REF - 39] de INCIBE** para ampliar información sobre otras fuentes de desinfección posibles, así como herramientas de descifrado **[REF – 40]** que vayan apareciendo.

4

Si cuentas con un antivirus en tu empresa, contacta con su proveedor de *software* por si hubieran desarrollado una herramienta específica. En caso contrario, puedes consultar el "Catálogo de empresas y soluciones de ciberseguridad" **[REF - 24]**.

B) Restaura la copia de seguridad

Revisa si el sistema de ficheros del sistema operativo cuenta con *shadow copy* o *snapshot*, que mantienen copias de versiones anteriores de ficheros. Localiza una copia previa a la infección y restáurala. Habrás perdido datos, pero podrás continuar con tu actividad.

Finalmente, utiliza un disco nuevo o formateado, además de una instalación en limpio del sistema operativo, y restaura la copia de seguridad más reciente anterior a la infección. En caso de haber descifrado la información, puedes transferirla a tu instalación en el nuevo soporte.

4.2. ¿Por qué no has de pagar el rescate?

Si te ha ocurrido un incidente tendrás muchas dudas sobre si acceder a pagar el rescate o no. Nuestra recomendación es que **no pagues el rescate que te exigen los ciberdelincuentes** **[REF - 41]** por los siguientes motivos:

- **Pagar no te garantiza que vuelvas a tener acceso a los datos,** recuerda que se trata de delincuentes.
- **Si pagas es posible que seas objeto de ataques posteriores,** pues ya saben que estás dispuesto a pagar.
- Puede que **soliciten una cifra mayor una vez hayas pagado.**
- Pagar **fomenta el negocio de los ciberdelincuentes.**

5 REFERENCIAS

[REF - 1]. **Wikipedia - Bitcoin -** https://es.wikipedia.org/wiki/Bitcoin

[REF - 2]. **Incibe - Glosario -** https://www.incibe.es/protege-tu-empresa/guias/glosario-terminos-ciberseguridad-guia-aproximacion-el-empresario

[REF - 3]. **WeliveSecurity – Ransomware y filtración de información: una tendencia que se consolidó en 2020 -** https://www.welivesecurity.com/la-es/2020/05/29/ransomware-filtracion-informacion-tendencia-consolido-2020/

[REF - 4]. **Incibe - ¿Cómo nos afecta la derogación del escudo de privacidad entre Europa y EE.UU.? -** https://www.incibe.es/protege-tu-empresa/blog/nos-afecta-derogacion-del-escudo-privacidad-europa-y-eeuu

[REF - 5]. **Bitcoinmix - Bitcoins irrastreables -** https://bitcoinmix.org/es

[REF - 6]. **The Tor Project -** https://www.torproject.org/

[REF - 7]. **Incibe - ¿Sabes cómo funciona un ciberataque que utiliza ingeniería social? -** https://www.incibe.es/protege-tu-empresa/blog/sabes-funciona-ciberataque-utiliza-ingenieria-social

[REF - 8]. **Incibe - Ataques "Watering hole": en qué consisten y cómo protegerse -** https://www.incibe.es/protege-tu-empresa/blog/ataques-watering-hole-consisten-y-protegerse

[REF - 9]. **Incibe - ¿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 - 10]. **Incibe - ¿Es seguro tu escritorio remoto? -** https://www.incibe.es/protege-tu-empresa/blog/seguro-tu-escritorio-remoto

[REF - 11]. **Incibe - Virus muestra un falso mensaje del Cuerpo Nacional de Policía -** https://www.osi.es/es/actualidad/avisos/2012/01/virus-muestra-un-falso-mensaje-del-cuerpo-nacional-de-policia

[REF - 12]. Welivesecurity by ESET - Ransomware y filtración de información: una tendencia que se consolidó en 2020 - https://www.welivesecurity.com/la-es/2020/05/29/ransomware-filtracion-informacion-tendencia-consolido-2020/

[REF - 13]. Incibe - Bitácora - https://www.incibe-cert.es/search/site/ransomware?f%5B0%5D=bundle%3Abitacora

[REF - 14]. Incibe - Protegiendo nuestra empresa con productos anti-malware - https://www.incibe.es/protege-tu-empresa/blog/protegiendo-nuestra-empresa-productos-anti-malware

[REF - 15]. Incibe - Servicio Antibotnet - https://www.incibe.es/protege-tu-empresa/herramientas/servicio-antibotnet

[REF - 16]. Incibe - Políticas de seguridad para la pyme - https://www.incibe.es/protege-tu-empresa/herramientas/politicas

[REF - 17]. Incibe - Luchando contra la ingeniería social: el firewall humano - https://www.incibe.es/protege-tu-empresa/blog/luchando-ingenieria-social-el-firewall-humano

[REF - 18]. Incibe - Kit concienciación - https://www.incibe.es/protege-tu-empresa/kit-concienciacion

[REF - 19]. Incibe - 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 - 20]. Incibe - Conéctate a tu empresa de forma segura desde cualquier sitio con una VPN - https://www.incibe.es/protege-tu-empresa/blog/conectate-tu-empresa-forma-segura-cualquier-sitio-vpn

[REF - 21]. Incibe - Celebra el Día Mundial de las Contraseñas, la puerta de entrada a todos tus servicios - https://www.incibe.es/protege-tu-empresa/blog/celebra-el-dia-mundial-las-contrasenas-puerta-entrada-todos-tus-servicios

[REF - 22]. Incibe - Primeros pasos para clasificar la información de tu organización - https://www.incibe.es/protege-tu-empresa/blog/primeros-pasos-clasificar-informacion-tu-organizacion

[REF - 23]. Incibe - La virtualización puede ser la solución a tus problemas - https://www.incibe.es/protege-tu-empresa/blog/virtualizacion-puede-ser-solucion-tus-problemas

[REF - 24]. Incibe - Catálogo de empresas y soluciones de ciberseguridad - https://www.incibe.es/protege-tu-empresa/catalogo-de-ciberseguridad/

[REF - 25]. Incibe - Firewall tradicional, UTM o NGFW. Diferencias, similitudes y cuál elegir según tus necesidades - https://www.incibe.es/protege-tu-empresa/blog/firewall-tradicional-utm-o-ngfw-diferencias-similitudes-y-cual-elegir-segun

[REF - 26]. Pfsense - Firewall IDS/IPS - https://www.pfsense.org/

[REF - 27]. Incibe - ¿Qué son y para qué sirven los SIEM, IDS e IPS? - https://www.incibe.es/protege-tu-empresa/blog/son-y-sirven-los-siem-ids-e-ips

[REF - 28]. Microsoft – DirectAccess - https://docs.microsoft.com/es-es/windows-server/remote/remote-access/directaccess/directaccess

[REF - 29]. Incibe - Qué es una DMZ y cómo te puede ayudar a proteger tu empresa - https://www.incibe.es/protege-tu-empresa/blog/dmz-y-te-puede-ayudar-proteger-tu-empresa

[REF - 30]. Incibe - El eslabón perdido entre el contrato y la ciberseguridad - https://www.incibe.es/protege-tu-empresa/blog/el-eslabon-perdido-el-contrato-y-ciberseguridad

[REF - 31]. Incibe - 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 - 32]. CuckoSandBox - https://cuckoosandbox.org/

[REF - 33]. Incibe - Plan de contingencia y continuidad de negocio, ¿qué herramientas necesito? - https://www.incibe.es/protege-tu-empresa/blog/plan-contingencia-y-continuidad-negocio-herramientas-necesito

[REF - 34]. INCIBE CERT – Centro de Respuesta a incidentes - https://www.incibe-cert.es/respuesta-incidentes

[REF - 35]. Incibe - Plan de contingencia y continuidad de negocio, ¿qué herramientas necesito? - https://www.incibe.es/protege-tu-empresa/blog/plan-contingencia-y-continuidad-negocio-herramientas-necesito

[REF - 36]. Guardia Civil Grupo de Delitos Telemáticos - https://www.gdt.guardiacivil.es/webgdt/home_alerta.php

[REF - 37]. Policía Nacional – Brigada de Investigación Tecnológica - https://www.policia.es/colabora.php

[REF - 38]. No More Ransom - Herramientas anti-ransomware - www.nomoreransom.org

[REF - 39]. Incibe - Línea de ayuda en ciberseguridad - https://www.incibe.es/linea-de-ayuda-en-ciberseguridad

[REF - 40]. Incibe - Ayuda anti-ransomware - https://www.incibe.es/protege-tu-empresa/herramientas/servicio-antiransomware

[REF - 41]. Sophos - El Estado de Ransomware 2020 - https://news.sophos.com/es-419/2020/05/12/el-estado-de-ransomware-2020/

GOBIERNO DE ESPAÑA
VICEPRESIDENCIA SEGUNDA 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