Ciberdelitos / Ciberincidentes ¿Cómo comprometen a las organizaciones y usuarios?

ESTÍBALIZ BUSTO PÉREZ DE MENDIGUREN

MÁSTER EN CIBERSEGURIDAD Y PRIVACIDAD

TRABAJO FIN DE MÁSTER

Junio 2023

Tutor:

JORGE CHINEA LÓPEZ

Agradecimientos

Quiero expresar mi agradecimiento a todas y cada una de las personas que de forma directa o indirecta han hecho posible el presente Trabajo Fin de Máster.

En primer lugar, agradecer a mi tutor del TFM, Jorge Chinea, por haberme permitido llevar a cabo este proyecto; su disposición desde el primer momento ha sido fundamental en su realización.

Asimismo, agradecer también la comprensión y el esfuerzo de todos los profesores que he tenido durante el máster por su dedicación docente.

A mi familia, por orientarme y ayudarme a lo largo de mis estudios para continuar formándome y creciendo tanto personal como profesionalmente. Gracias a su esfuerzo mi deseo se ha hecho realidad.

Finalmente, a todas las personas que he conocido durante mi formación, que han aportado conocimientos y un buen ambiente para seguir aprendiendo.

Personalmente, el poder dar fin al Máster en Ciberseguridad es algo muy especial que llevo queriendo realizar desde que inicié mi trayectoria como Ingeniera Informática y me alegra haberlo podido compartir con todas estas personas mencionadas anteriormente.

Por todo ello, muchísimas gracias.

Dedicatoria

"Los sueños de los grandes soñadores jamás llegan a cumplirse, siempre son superados".

Alfred Lord Whitehead

Ficha del Trabajo Final

Título del trabajo:	*Ciberdelitos / Ciberincidentes: ¿Cómo comprometen a las organizaciones y usuarios?*
Nombre del autor:	*Estíbaliz Busto Pérez de Mendiguren*
Nombre del consultor/a:	*Jorge Chinea López*
Nombre del PRA:	Víctor García Font
Fecha de entrega	*06/2023*
Titulación o programa:	*Máster Universitario en Ciberseguridad y Privacidad*
Área del Trabajo Final:	*Seguridad Empresarial*
Idioma del trabajo:	*Castellano*
Palabras clave	*Ciberincidente, Phishing, Ransomware*

Resumen del Trabajo

La digitalización, las nuevas tecnologías e Internet han supuesto un importante cambio en nuestras vidas tanto a nivel personal como profesional. La conexión a Internet multiplica las vías de ataque y los ciberincidentes, los cuales pueden tener gran impacto con enormes repercusiones en pocos segundos en los usuarios y empresas. De aquí la importancia de la ciberseguridad.

En este Trabajo Fin de Máster se llevará a cabo un estudio de los ciberincidentes: clasificación, detección, nivel de peligrosidad e impacto, para posteriormente analizar dos de ellos: PHISHING (tipo de incidente: fraude) y RANSOMWARE (tipo de incidente: malware).

Para su estudio se procederá a ubicarlos en el tiempo desde sus orígenes hasta nuestros días, conocer sus tipos o variantes más frecuentes, así como sus mecanismos de acción e infección utilizados. A continuación, se analizarán diferentes medidas de seguridad para evitar estos ciberataques. Para finalizar, se darán a conocer sus repercusiones más importantes tanto en los usuarios como en las empresas del sector privado y público en la actualidad.

Abstract

Digitization, new technologies and Internet have brought about an important change in our lives, both personally and professionally. The Internet connection multiplies the ways of attack and cyber incidents, which can have a great impact with enormous repercussions in a few seconds for users and companies. Hence the importance of cybersecurity.

In this Final Master's Project, a study of cyber incidents will be carried out: classification, detection, level of danger and impact, to later analyze two of them: PHISHING (incident type: fraud) and RANSOMWARE (incident type: malware).

For their study, we will proceed to locate them in time from their origins to the present day, to know their most frequent types or variants, as well as their infection methods. Next, different security measures will be analyzed to avoid them. Next, different security measures will be analyzed to avoid these cyberattacks. Finally, its most important repercussions will be announced both for users and for companies in the private and public sector today.

Contenido

Índice de tablas

Índice de figuras

Acrónimos

CCN: Centro Criptológico Nacional

UOC: Universitat Oberta de Catalunya

CCEG: Competencia de compromiso ético y global

ODS: Objetivos de Desarrollo Sostenible.

CERT: Computer Emergency Response Team (Equipo de respuesta a emergencias informáticas)

CNI: Centro Nacional de Inteligencia

DNS: Domain Name System (Sistema de Nombres de Dominio)

ENS: Esquema Nacional de Seguridad.

INCIBE: Instituto Nacional de Ciberseguridad

IOCTA: Internet Organised Crime Threat Assessment

IoT: Internet of Things (Internet de las Cosas)

IP: Internet Protocol (Protocolo de Internet)

OSI: Oficina de Seguridad del Internauta

PYME: Pequeña y mediana empresa

TIC: Tecnologías de la información y la comunicación

VPN: Virtual Private Network (Red Privada Virtual)

APWG: Phishing Activity Trends Report (Grupo de Trabajo Anti Phishing)

1. Introducción

1.1. Contexto y justificación

Internet nos permite estar conectados constantemente a un mundo en plena transformación digital y los ciberdelincuentes están aprovechándose de dicho cambio para atacar las redes, las infraestructuras o los sistemas informáticos. Cada vez resulta más frecuente conocer cómo pequeñas, medianas o grandes empresas son víctimas de ciberataques, lo cual tiene una enorme repercusión tanto económica como social para los gobiernos, las empresas o los particulares.

La combinación de ingeniería social, phishing, malware (principalmente ransomware), redes TOR e incluso servicios de mensajería como Telegram son los principales puntos de apoyo para cometer ciberdelitos. Cualquiera de ellos es una fuente de problemas que no solo afecta a la privacidad de nuestros datos, sino que también destruye las posibilidades comerciales de cualquier empresa.

En los últimos datos publicados por INCIBE en su Balance de Ciberseguridad 2022, aparecen registrados **118.820 ciberincidentes**, casi un 9% más respecto al año anterior. Del total de esta cifra, más de 110.100 de los ciberincidentes afectaron a ciudadanos y empresas, 546 a operadores estratégicos (organización pública o privada responsable del funcionamiento de una infraestructura que resulta indispensable) y 7.980 a la Red Académica y de Investigación Española (RedIRIS) [1] [2].

En el ámbito de ciudadanos y empresas, de los 110.294 ciberincidentes más destacados registrados, un 22,3% más que en 2021, cabe destacar que 1 de cada 3 son una filtración de datos (sensibles, protegidos o confidenciales robados por una persona no autorizada); y 2 de cada 5 son vulnerabilidades de sistemas tecnológicos (debilidad de un sistema que puede poner en riesgo su seguridad) [1] [2].

En cuanto a los ciberincidentes más frecuentes, 1 de cada 4 son un **fraude online**, destacando el **phishing** con casi 17.000 incidentes, seguido del **malware** con más de 14.000 y, por último, el **ransomware**, con casi 450 incidentes. De aquí la relevancia de los dos ciberataques elegidos como objeto de estudio en el presente proyecto. Asimismo, durante 2022 INCIBE detectó más de 650 tiendas online fraudulentas, además de más de 5.000 incidentes que tienen que ver con contenido abusivo, como pornografía infantil, delitos de odio o ciberacoso [2].

No cabe duda de que los ciberdelincuentes son cada vez más ágiles y están mejor organizados, tal y como se manifiesta en la velocidad con que utilizan las nuevas tecnologías y el modo en que adaptan sus ataques cooperando entre sí. Además, los ciberdelincuentes, las víctimas y las infraestructuras técnicas están tan dispersos que, en ocasiones, resulta muy complicado investigar o emprender acciones judiciales. Por esto, resulta crucial protegerse de los ciberataques maliciosos y contar con mecanismos de defensa que nos ayuden a evitar fugas de información confidencial o pérdidas millonarias para cualquier empresa.

De aquí la importancia de la **ciberseguridad**, siempre entendida como una línea de defensa que individuos y empresas tienen para protegerse contra el acceso no autorizado a los centros de datos y otros sistemas informáticos. Sin embargo, la ciberseguridad no sólo debe proteger los sistemas, las

redes y los programas de los ataques online, sino que debe ayudar a prevenir los ciberataques que tienen como objetivo desactivar o interrumpir el funcionamiento de una red o un dispositivo.

1.2. Motivación

Mi gran **interés** y **curiosidad** por la ciberseguridad han hecho que me decidiera, sin duda alguna, por la realización de este proyecto como Trabajo de Fin de Máster. Además, la publicación en los medios de comunicación, a finales de diciembre de 2022, sobre cómo la COVID-19 había acelerado la digitalización acentuando la inseguridad de las organizaciones y usuarios ante la ciberdelincuencia, me hizo reflexionar sobre algo que ya venía pensando tiempo atrás y me entusiasmaba a la hora de poder ampliar mis conocimientos: la **ciberseguridad**.

El éxito de las redes sociales y la conexión a internet como herramientas virtuales hacen que sean frecuentadas por gran parte de la población sin tomar precauciones. De hecho, los ciberdelincuentes confían cada vez más en nuestra dependencia al mundo digital para cometer sus actos fraudulentos y, a pesar de ello, apenas se dedica la mínima atención en conocer cómo protegernos.

Por ello, considero que nuestro conocimiento del ámbito digital resulta crucial ya que, sólo así, se conseguirá el máximo provecho de todas las herramientas posibles evitando cometer errores por ignorancia y, definitivamente, reconsiderar la ciberseguridad como la ayuda para prevenir los ciberataques cuyo objetivo, no es otro que, hacer el mayor daño posible.

1.3. Objetivos

El objetivo principal de este Trabajo de Fin de Máster es concienciar al lector de la importancia de los ciberataques en general y, de dos de ellos, en particular: PHISHING (tipo de incidente: fraude) y RANSOMWARE (tipo de incidente: malware). Para ello, se establecen los siguientes objetivos:

- Realizar un estudio de los ciberincidentes centrado en su clasificación, detección y nivel de peligrosidad e impacto.
- Conocer y ubicarlos en el tiempo desde sus orígenes hasta nuestros días.
- Comprender en qué consiste el phishing y ransomware.
- Conocer sus tipos o variantes más frecuentes.
- Comprender sus mecanismos o métodos de acción e infección utilizados.
- Conocer las medidas de seguridad que se deben tomar a nivel de usuario y empresarial ante los mencionados ciberataques.
- Conocer el panorama actual y las repercusiones que tienen dichos ciberdelitos en el usuario y en la empresa tanto privada como pública.

Todos estos objetivos se irán consiguiendo a lo largo de las entregas parciales que se realizarán en el tiempo marcado por la ficha docente correspondiente.

1.4. Impacto ético, social y ambiental

La Universitat Oberta de Catalunya (UOC) está públicamente comprometida con la Competencia de compromiso ético y global (CCEG) y los Objetivos de Desarrollo Sostenible (ODS), los cuales se incluyen en el programa del máster con la siguiente definición:

"Actuar de manera honesta, ética, sostenible, socialmente responsable y respetuosa con los derechos humanos y la diversidad, tanto en la práctica académica como en la profesional, y diseñar soluciones para mejorar estas prácticas."

La CCEG aborda tres grandes dimensiones (Tabla 1-1) alineadas con los ODS. De los 17 objetivos que integran los ODS se señalarán y analizarán únicamente aquellos objetivos relacionados con el presente documento en sus diferentes etapas [3]:

	DISEÑO	DESARROLLO	CONCLUSIONES
Dimensión I. Sostenibilidad			
ODS 7. Energía asequible y limpia. **ODS 9. Industria, innovación e infraestructura.** **ODS 11. Ciudades y comunidades sostenibles.** **ODS 12. Consumo y producción responsable.** **ODS 13. Acción climática.** **ODS 14. La vida bajo el agua.** **ODS 15. La vida en la tierra.**	ODS 9	ODS 9 ODS 12	ODS 9
Dimensión II. Comportamiento ético y responsabilidad social (RS)			
ODS 1. No pobreza. **ODS 2. Hambre cero.** **ODS 3. Salud y bienestar.** **ODS 6. Agua limpia y saneamiento.** **ODS 8. Trabajo decente y crecimiento económico.** **ODS 16. Paz, justicia e instituciones sólidas.** **ODS 17. Alianzas para lograr objetivos.**		ODS 8 ODS 16 ODS 17	ODS 16
Dimensión III. Diversidad (género entre otros) y derechos humanos			
ODS 4. Educación de calidad. **ODS 5. Igualdad de género.** **ODS 10. Desigualdades reducidas.**	ODS 4 ODS 5 ODS 10	ODS 4 ODS 5	ODS 4 ODS 5

Tabla 1-1. Dimensiones alineadas con los ODS (Objetivos de Desarrollo Sostenible) relacionados con la Competencia de Compromiso Ético y Global (CCEG).

Fuente: Elaboración propia a partir de https://www.un.org/sustainabledevelopment/es/sustainable-development-goals/

A la hora de diseñar este documento, se ha tenido en cuenta que la información aportada sea accesible a todos los usuarios potenciando la inclusión de todas las personas independiente de su edad, sexo, discapacidad, raza, origen, religión o situación económica garantizando la igualdad de oportunidades como indica el **ODS 10** (Desigualdades reducidas) sobre Diversidad y derechos humanos.

Durante el desarrollo del presente TFM, se ha considerado el **ODS 12** (Consumo y producción responsable) sobre Sostenibilidad. Debido a la gran demanda de sitios Web no debemos usar las tecnologías modernas sin ningún tipo de control aumentando el ahorro energético, sino ayudar a los

países en desarrollo a fortalecer su capacidad científica y tecnológica para avanzar hacia un consumo y producción más responsable.

Por otro lado, si trabajamos con tecnologías modernas, la seguridad y protección de datos de los usuarios estará más garantizada. Esta es una manera de prevenir injusticias imposibilitando el cometido del delito en sí y abordando el **ODS 16** (Paz, justicia e instituciones sólidas) sobre Comportamiento ético y responsabilidad social. Todo ello, en base a conseguir la paz, justicia e instituciones sólidas ya que la inseguridad, las instituciones débiles y el acceso limitado a la justicia continúan suponiendo una grave amenaza para el desarrollo sostenible.

Además, promover el desarrollo de tecnologías, así como su divulgación y difusión a los países en desarrollo en condiciones favorables, según lo convenido de mutuo acuerdo, como indica el **ODS 17** (Alianzas para conseguir los objetivos). Para alcanzar este Objetivo de Desarrollo Sostenible, los gobiernos, la sociedad, los científicos, el mundo académico y el sector privado deben estar unidos.

Tanto a la hora de diseñar este documento como en sus conclusiones, se reafirmará cómo la innovación y el progreso tecnológico son claves para descubrir soluciones duraderas para los desafíos económicos; por ello, se apoya el acceso a la tecnología y comunicaciones esforzándose por proporcionar el acceso a Internet en los países menos adelantados, tal y como indica en el **ODS 9** (Industria, innovación e infraestructura) sobre la Sostenibilidad.

Además, tanto a la hora de diseñar este proyecto, como en su desarrollo o, incluso, en sus conclusiones, se ha tenido en cuenta la importancia de recibir una educación de calidad para llevar a cabo proyectos como el presente. Gracias al progreso económico y social aumenta el número de jóvenes y adultos con competencias necesarias, en particular técnicas y profesionales, para acceder al empleo, el trabajo decente y el emprendimiento, abordando el **ODS 4** (Educación de calidad).

Por último, en ninguno de estos tres momentos claves (diseño, desarrollo y conclusiones del TFM), se percibe la discriminación de género. La igualdad de género no sólo es un derecho humano, sino que es uno de los fundamentos esenciales para construir un mundo pacífico, próspero y sostenible, aspecto abordado en el **ODS 5** (Igualdad de género) sobre Diversidad y derechos humanos.

1.5. Metodología

Para poder superar los objetivos del presente documento se empleará una metodología tanto de investigación exploratoria como descriptiva y explicativa, tal y como se detalla a continuación [4]:

Para comenzar el estudio de los ciberincidentes, se utiliza una metodología **exploratoria** cuyo objetivo es realizar una visión general que permita familiarizarnos y establecer las bases para la investigación, a partir de toda la información y documentación obtenida para dicho propósito.

Seguidamente, para poder profundizar en el estudio de los ciberataques analizados, phishing y ransomware, se utiliza una metodología **descriptiva** porque permite definir, clasificar, catalogar o caracterizar con mayor minuciosidad el objeto de estudio ya definido en este párrafo.

Finalmente, se llevará una metodología **explicativa** no sólo para describir en profundidad ambos ciberataques, sino determinar sus orígenes o las causas de ambos y explicar por qué se producen.

Las técnicas utilizadas en la elaboración de este TFM serán la **investigación documental** y la **recopilación de información** obtenida a través del estudio e investigación de diferentes guías, manuales, documentos, páginas webs, foros … para poder descubrir los beneficios que nos puede aportar un mayor conocimiento de los ciberataques estudiados y hasta qué punto pueden comprometer a las organizaciones y los usuarios.

1.6. Planificación del Trabajo

La elaboración del presente documento consta de las siguientes fases principales:

1. **Planificación del proyecto.** Se establece el contexto y la justificación de la importancia que tiene la realización de este, así como la motivación que ha llevado a su puesta en marcha. Para ello, se enumeran los objetivos, se estudia el impacto ético, social y ambiental, se describe la metodología y técnicas de investigación a utilizar, así como la planificación temporal junto con el análisis de los riesgos del proyecto. Se continuará con la enumeración de los productos obtenidos durante su elaboración y se inicia la revisión del estado del arte. Para finalizar, se llevará a cabo una descripción de los recursos necesarios y el presupuesto del proyecto.

2. **Investigación y documentación.** Se utilizan las técnicas de investigación documental y de recopilación de información que completarán los apartados del presente documento:

   I. Estudio de los ciberincidentes: clasificación, detección, nivel de peligrosidad e impacto.

   II. Estudio de Phishing (tipo de incidente: fraude): definición, historia, tipos de fraude, variantes, mecanismos de infección y medidas de seguridad.

   III. Estudio de Ransomware (tipo de incidente: malware): definición, tipos, métodos de infección y medidas de seguridad (preventivas y reactivas).

   IV. Panorama actual: tendencia de los actuales ciberataques y sus consecuencias en el sector privado y público.

3. **Conclusiones.** Se presentan las conclusiones procedentes del estudio realizado y las dificultades tenidas durante su elaboración, los objetivos superados y las líneas posibles de futuro trabajo.

4. **Memoria Final.** Se entrega la memoria final del presente documento en el aula virtual.

5. **Presentación en vídeo.** Elaboración de un vídeo con una síntesis del trabajo realizado sobre una presentación de diapositivas.

6. **Defensa.** Período en el cual el tribunal realiza una serie de preguntas a las que se debe responder.

La planificación temporal de este documento definida mediante el diagrama de Gantt se puede ver en el [Anexo I. Planificación del Trabajo].

1.6.1. Riesgos del proyecto

En este subapartado dentro de la planificación del proyecto, a modo de reflexión, se llevará a cabo un breve análisis de los riesgos del presente proyecto ligado con los nuevos conocimientos sobre los ciberincidentes. Este nuevo conocimiento implica un alto grado de incertidumbre que conlleva superar los límites del denominado **estado del arte**, en este caso se refiere al límite del conocimiento humano acerca de dicha materia.

Esto hace que la gestión de riesgos en este tipo de proyectos de investigación sea aún más crítica que en otros, ya que cuanto mayor sea el nivel de incertidumbre, mayor será el número de riesgos presentes en el mismo [5].

A continuación, se analizarán los riesgos de este proyecto:

Riesgos de objetivos. No se deben proponer objetivos que sean imposibles de alcanzar debido a la falta de experiencia profesional en los tipos de incidentes a desarrollar.

Plan de acción. Apoyarse en la experiencia de la dirección del proyecto y elegir documentación de fuentes fiables.

Riesgos de personal. Dado que en este proyecto de investigación se desarrollan nuevos conocimientos, requerirá un equipo especializado integrado por investigadores con experiencia.

Plan de acción. Dado que el proyecto se lleva a cabo por una persona investigadora, la dirección debe ser consciente tanto de sus aportaciones como sus limitaciones para no perder el ritmo de trabajo.

Riesgos de coordinación. La colaboración y comunicación entre la dirección y la persona investigadora del proyecto son dos aspectos prioritarios para llevar a cabo su realización: intercambio de información, resolución de dudas, comentarios sobre las diferentes entregas …

Plan de acción. Desde el inicio del proyecto la dirección ha determinado tanto la forma de contacto como su flexibilidad para posibles modificaciones sin ningún problema. Ambas partes están de acuerdo y en constante comunicación para evitar problemas al respecto y avanzar según lo previsto.

Riesgos de cumplimiento de plazo. Uno de los grandes inconvenientes a los que se enfrenta este proyecto es el retraso de las entregas [6].

Plan de acción. Aunque resulte complicado prever los tiempos de ejecución, la persona investigadora debe cumplir con las fechas de entrega para no realizar retrasos “en cascada” a posteriori.

Riesgos tecnológicos. El presente proyecto de investigación depende, en gran parte, del buen funcionamiento de la tecnología para poder cumplir los objetivos establecidos en el apartado 1.3.

Plan de acción. Ir avanzando según la planificación realizada para poder hacer frente a posibles complicaciones si las hubiera.

Riesgos económicos. La variabilidad en los costes estimados afectaría al presupuesto realizado en el apartado 1.10 y sería un gran contratiempo totalmente inesperado.

Plan de acción. Si bien es cierto que el material utilizado no resultaría difícil remplazarlo (en cuanto a su adquisición), conllevaría un sobrecoste económico imprevisto en el presente proyecto.

1.7. Productos obtenidos

La Tabla 1-2 muestra los entregables obtenidos durante la elaboración del presente TFM:

ENTREGA	CONTENIDO	FECHA
PEC 1. Plan de trabajo	Primera fase sobre el plan de trabajo que será desarrollado en el Capítulo 1. Introducción.	14 de marzo de 2023
PEC 2. Entrega de seguimiento	Primera entrega de una parte de la memoria final donde se desarrollarán los capítulos: I. Estudio de los ciberincidentes. II. Estudio de Phishing.	11 de abril de 2023
PEC 3. Entrega de seguimiento	Segunda entrega de una parte de la memoria final donde se desarrollarán los capítulos: III. Estudio de Ransomware. IV. Panorama actual. V. Conclusiones.	9 de mayo de 2023
PEC 4. Memoria final	Memoria final del presente documento en el aula virtual.	13 de junio de 2023
Presentación en vídeo	Elaboración de un vídeo con una síntesis del trabajo realizado sobre una presentación de diapositivas.	20 de junio de 2023
Defensa del TFM	Período de tiempo en el cual el tribunal realiza una serie de preguntas a las que se debe responder.	30 de junio de 2023

Tabla 1-2. Productos obtenidos durante la elaboración del presente proyecto.

1.8. Estructura del Trabajo

El presente documento se estructura en seis capítulos descritos a continuación:

Capítulo 1 - "Introducción". Para contextualizar y justificar este proyecto, se comienza con una reflexión sobre la transformación digital que estamos viviendo y la importancia de la ciberseguridad como prevención de los ciberataques. Para continuar con la motivación que llevó a la elaboración de este proyecto, los objetivos, el impacto ético, social y ambiental, la metodología y técnicas de investigación a utilizar, así como la planificación temporal junto con el análisis de los riesgos del proyecto. Se continuará con la enumeración de los productos obtenidos durante su elaboración y se inicia la revisión del estado del arte. Finalmente, la descripción de los recursos necesarios y el presupuesto del presente proyecto son los apartados que completan dicho capítulo.

Capítulo 2 - "Estudio de los ciberincidentes". Dicho estudio estará centrado en su clasificación, su detección, su nivel de peligrosidad e impacto (siempre a partir de la información y documentación obtenida para tal propósito).

Capítulo 3 - "Estudio de Phishing". Se comenzará con su ubicación en el tiempo desde su origen hasta nuestros días. A continuación, se conocerán sus tipos más frecuentes, así como sus mecanismos de acción e infección utilizados. Para finalizar, se investigarán las medidas de seguridad más relevantes.

Capítulo 4 - "Estudio de Ransomware". Con similar estructura al capítulo anterior, se procederá a situar este ciberataque en el tiempo desde sus comienzos hasta nuestros días. Seguidamente, se conocerán sus tipos o variantes más frecuentes, así como sus métodos o mecanismos de acción e

infección utilizados. Para concluir, se investigarán las medidas de seguridad para tener en cuenta para evitar el mencionado ciberataque.

Capítulo 5 - "Panorama actual". Se mostrará la tendencia de los ciberataques actuales y de qué manera repercuten en el usuario y en la empresa tanto privada como pública.

Capítulo 6 - "Conclusiones". Se analizarán las conclusiones, las dificultades tenidas, los objetivos superados y las líneas de futuro trabajo a partir del presente proyecto.

"Bibliografía" con la lista numerada de las referencias bibliográficas utilizadas en la memoria.

Para finalizar, en los **"Anexos"** se desarrollarán en mayor profundidad algunos temas que, aunque no se consideren imprescindibles para el seguimiento del presente proyecto, se consideran de interés para su lector y cuyo objetivo es ampliar el contenido del documento principal.

1.9. Recursos necesarios y presupuesto del proyecto

Este proyecto se ha presupuestado en base a los recursos utilizados y el coste de cada uno de ellos, tal y como muestra, la tabla 1-3:

RECURSOS	USO	COSTES UNITARIOS	COSTES
Ordenador	Búsqueda y recopilación de la información para la posterior elaboración de la memoria final.	1.200 €	1.200 €
Conexión a Internet	Recopilación de datos.	38 € / mes	152 €
Herramientas	Aplicación de edición de textos.	0 €	0 €
Analista de seguridad	Nº de horas para la preparación del TFM por un analista junior de seguridad 50+75+75+75+20+5 = 300 horas	22 € / h	6.600 €
COSTE TOTAL			**7.952 €**

Tabla 1-3. Costes asociados al proyecto.

2. Estudio de los ciberincidentes

Los ciberdelincuentes siempre encuentran nuevas formas con las que atacar a los usuarios aprovechándose de nuestro desconocimiento o vulnerabilidades en nuestras defensas. Las consecuencias son muy diversas y sus formas de atacar cada vez más novedosas; aun así, antes de llevar a cabo una clasificación minuciosa de ellos, conviene saber hacia dónde van dirigidos [7]:

- Los ataques a **contraseñas** utilizan técnicas y herramientas para atacar a nuestras credenciales.
- Los ataques por **ingeniería social** pretenden conseguir que revelemos información personal o permitir al atacante tomar el control de nuestros dispositivos. Siempre están basados en el engaño y la manipulación, y suelen utilizarse como paso previo a un ataque por malware.
- Los ataques a **conexiones inalámbricas** utilizan diversos software y herramientas para saltarse las medidas de seguridad e infectar o tomar control de nuestros dispositivos. Se interponen en el intercambio de información entre el usuario y el servicio web para monitorizar y robar datos personales, bancarios, contraseñas …
- Los ataques por **malware** utilizan programas maliciosos para llevar a cabo acciones dañinas en un sistema informático y contra nuestra privacidad. Generalmente, buscan robar información, causar daños en el equipo, obtener un beneficio económico o tomar el control del equipo.

A continuación, en los siguientes apartados del Capítulo 2, se llevará a cabo una clasificación más detallada de los ciberincidentes, su detección, su nivel de peligrosidad e impacto siguiendo las directrices de la Guía Nacional de Notificación y Gestión de Ciberincidentes [7].

2.1. Clasificación

Dado que todos los ciberincidentes no tienen las mismas características ni la misma peligrosidad, es necesario disponer de una taxonomía que ayudará a su análisis, contención y eliminación.

Los factores para tener en cuenta a la hora de establecer criterios de clasificación son [9]:

- Tipo de amenaza: código dañino, intrusiones, fraude, etc.
- Origen de la amenaza: Interna o externa.
- Categoría de seguridad de los sistemas afectados.
- Perfil de los usuarios afectados, su posición y sus privilegios de acceso a información sensible.
- Número y tipología de los sistemas afectados.
- Impacto que el incidente tenga en la organización.
- Requerimientos legales y regulatorios.

La combinación de uno o varios de estos factores es clave a la hora de determinar su peligrosidad y prioridad de actuación. En la Tabla 2-1 se muestra una clasificación de los ciberincidentes atendiendo al tipo de amenaza o incidente junto con una breve descripción y ejemplo de la mayoría de ellos:

CLASIFICACIÓN DE LOS CIBERINCIDENTES		
Clasificación	**Tipo de incidente**	**Descripción y ejemplo**
Contenido abusivo	**SPAM**	Correo electrónico masivo no solicitado que el receptor del contenido no ha autorizado.
	Delito de odio	Contenido difamatorio o discriminatorio. Ejemplos: ciberacoso, racismo, amenazas a una persona o dirigidas contra colectivos.
	Pornografía infantil o contenido sexual.	Material relacionado con pornografía infantil, violencia, etc.
Contenido dañino	**Sistema infectado**	Sistema infectado con malware. Ejemplo: sistema, computadora o teléfono móvil infectado con un rootkit.
	Servidor C&C (Mando y Control)	Conexión con servidor de Mando y Control (C&C) mediante malware o sistemas infectados.
	Distribución de malware	Recurso usado para distribución de malware.
	Configuración de malware	Recurso que aloje ficheros de configuración de malware. Ejemplo: ataque de webinjects para troyano.
Obtención de información	**Escaneo de redes (scanning)**	Envío de peticiones a un sistema para descubrir sus debilidades, recopilar información de alojamientos, servicios y cuentas. Ejemplos: peticiones DNS, ICMP, SMTP, escaneo de puertos.
	Análisis de paquetes (sniffing)	Observación y grabación del tráfico de redes.
	Ingeniería social	Recopilación de información personal sin el uso de la tecnología. Ejemplos: mentiras, trucos, sobornos, amenazas.
Intento de intrusión	**Explotación de vulnerabilidades conocidas**	Interrupción de un servicio mediante la explotación de vulnerabilidades con un identificador estándar. Ejs: cross site scripting (XSS), desbordamiento de buffer, puertas traseras.
	Intento de acceso con vulneración de credenciales	Múltiples intentos de vulnerar credenciales. Ejemplos: intentos de ruptura de contraseñas, ataque por fuerza bruta.
	Ataque desconocido	Ataque empleando exploit desconocido.
Intrusión	**Compromiso de cuenta con privilegios**	Compromiso de un sistema donde el atacante posee privilegios.
	Compromiso de cuenta sin privilegios	Compromiso de un sistema empleando cuentas sin privilegios.
	Compromiso de aplicaciones	Compromiso de una aplicación mediante la explotación de vulnerabilidades de software. Ejemplo: inyección SQL.
	Robo	Intrusión física. Ejemplo: acceso no autorizado a Centro de Proceso de Datos y sustracción de equipo.
Disponibilidad	**DoS (Denegación de Servicio)**	Ataque de Denegación de Servicio. Ejemplo: envío de peticiones a una aplicación web para interrumpir o ralentizar el servicio.
	DDoS (Denegación Distribuida de Servicio)	Ataque de Denegación Distribuida de Servicio. Ejemplos: inundación de paquetes SYN, ataques de reflexión y amplificación utilizando servicios basados en UDP.
	Mala configuración	Configuración incorrecta del software que provoca problemas de disponibilidad en el servicio. Ej: Servidor DNS con el KSK de la zona raíz de DNSSEC obsoleto.
	Sabotaje	Sabotaje físico. Ejemplos: cortes de cableados de equipos o incendios provocados.
	Interrupciones	Interrupciones por causas externas. Ejemplo: desastre natural.
Compromiso de la información	**Acceso no autorizado a información**	Acceso no autorizado a información. Ejemplos: robo de credenciales de acceso mediante interceptación de tráfico o acceso a documentos físicos.
	Modificación no autorizada de información	Modificación no autorizada de información. Ejemplos: modificación empleando credenciales sustraídas de un sistema, aplicación o encriptado de datos mediante ransomware.
	Pérdida de datos	Pérdida de información por fallo de disco duro o robo físico.
Fraude	**Uso no autorizado de recursos**	Uso de recursos para propósitos inadecuados. Ejemplo: uso de correo electrónico para participar en estafas piramidales.

	Derechos de autor	Instalación de software carente de licencia u otro material protegido por derechos de autor. Ejemplos: Warez.
	Suplantación	Una entidad suplanta a otra para obtener beneficios ilegítimos.
	Phishing	Suplantación de identidad para que el usuario revele sus credenciales.
Vulnerable	**Criptografía débil**	Servicios accesibles públicamente con criptografía débil. Ejemplo: servidores web susceptibles de ataques POODLE/FREAK.
	Amplificador DDoS	Servicios accesibles públicamente utilizados para la reflexión o amplificación de ataques DDoS. Ejemplos: DNS open-resolvers o Servidores NTP con monitorización monlist.
	Servicios con acceso potencial no deseado	Servicios accesibles públicamente potencialmente no deseados. Ejemplos: Telnet, RDP o VNC.
	Revelación de información	Acceso público a servicios en los que pueda revelarse información sensible. Ejemplos: SNMP o Redis.
	Sistema vulnerable	Sistema vulnerable. Ejemplos: mala configuración de proxy en cliente (WPAD), versiones desfasadas de sistema.
Otros	**Otros**	Todo incidente que no se recoja en ninguna categoría anterior.
	APT	Ataques dirigidos contra organizaciones concretas, sustentados en mecanismos muy ocultos, anónimos y persistentes.

Tabla 2-1. Clasificación / Taxonomía de los Ciberincidentes.

Fuente: Elaboración propia a partir de la Guía nacional de notificación y gestión de ciberincidentes. Aprobado por el Consejo Nacional de Ciberseguridad (21 de febrero de 2020). Obtenido de https://www.incibe-cert.es/taxonomia.

Los frecuentes ataques cibernéticos han hecho que incluyamos en nuestro vocabulario multitud de palabras y conceptos relacionados con esta materia. Para obtener una información más precisa sobre dicho vocabulario relacionado con este TFM, véase el [Anexo II. Glosario de términos].

2.2. Detección

En ocasiones, resulta complejo saber tanto si se ha producido un ciberincidente como evaluar su peligrosidad; aun así, los indicios pueden provenir de dos fuentes: los precursores y los indicadores.

Un **precursor** es un indicio de que puede ocurrir un incidente en el futuro. Un **indicador** es un indicio de que un incidente puede haber ocurrido o puede estar ocurriendo en este momento [10].

Algunos de estos ejemplos se mostrarán a continuación en la Tabla 2-2:

DETECCIÓN DE LOS CIBERINCIDENTES	
PRECURSOR	**INDICADOR**
Las entradas de log del servidor Web, con los resultados de un escáner de vulnerabilidades. El anuncio de un nuevo exploit, dirigido a una atacar una vulnerabilidad que podría estar presente en los sistemas de la organización. Las amenazas explícitas provenientes de grupos o entidades concretos.	El sensor de intrusión de una red emitiendo una alerta cuando ha habido un intento de desbordamiento de búfer contra de un servidor de base de datos. - Las alertas generadas por software antivirus. - La presencia de un nombre de archivo con caracteres inusuales. - Un registro de log sobre un cambio no previsto en la

	configuración de un host. - Los logs de una aplicación, advirtiendo de reiterados intentos fallidos de login desde un sistema externo desconocido. - La detección de un número importante de correos electrónicos con contenido sospechoso. - La desviación inusual del tráfico de la red interna.

Tabla 2-2. Detección de los Ciberincidentes.

Fuente: Elaboración propia a partir de https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/988-ccn-stic-817-gestion-de-ciberincidentes/file.html

Una vez detectado el ciberincidente, se debe determinar tanto su nivel de peligrosidad como su nivel de impacto, información que se abordará en los siguientes apartados.

2.3. Nivel de peligrosidad

Además de clasificar los ciberincidentes dentro de un determinado grupo, se debe determinar su nivel de peligrosidad: CRÍTICO, MUY ALTO, ALTO, MEDIO o BAJO. Para ello, se establecerán algunos Criterios de Determinación de Peligrosidad con los que se asignará su nivel de peligrosidad y se compararán las evidencias disponibles del ciberincidente con el tipo de incidente (Tabla 2-3) [11]:

CRITERIOS DE DETERMINACIÓN DEL NIVEL DE PELIGROSIDAD DE LOS CIBERINCIDENTES		
Nivel	**Clasificación**	**Tipo de incidente**
CRÍTICO	Otros	APT
MUY ALTO	Código dañino	Distribución de malware
		Configuración de malware
	Intrusión	Robo
	Disponibilidad	Sabotaje
		Interrupciones
ALTO	Contenido abusivo	Pornografía infantil, contenido sexual o violento inadecuado
	Código dañino	Sistema infectado
		Servidor C&C (Mando y Control)
	Intrusión	Compromiso de aplicaciones
		Compromiso de cuentas con privilegios
	Intento de intrusión	Ataque desconocido
	Disponibilidad	DoS (Denegación de servicio)
		DDoS (Denegación distribuida de servicio)
	Compromiso de la información	Acceso no autorizado a información
		Modificación no autorizada de información
		Pérdida de datos
	Fraude	Phishing
MEDIO	Contenido abusivo	Discurso de odio
	Obtención de información	Ingeniería social
	Intento de intrusión	Explotación de vulnerabilidades conocidas
		Intento de acceso con vulneración de credenciales
	Intrusión	Compromiso de cuentas sin privilegios
	Disponibilidad	Mala configuración
	Fraude	Uso no autorizado de recursos

		Derechos de autor
		Suplantación
	Vulnerable	Criptografía débil
		Amplificador DDoS
		Servicios con acceso potencial no deseado
		Revelación de información
		Sistema vulnerable
BAJO	Contenido abusivo	Spam
	Obtención de información	Escaneo de redes (scanning)
		Análisis de paquetes (sniffing)
	Otros	Otros

Tabla 2-3. Criterios de determinación del nivel de peligrosidad de los ciberincidentes.
Fuente: Guía nacional de notificación y gestión de ciberincidentes. Obtenido de https://www.incibe-cert.es/sites/default/files/contenidos/guias/doc/guia_nacional_notificacion_gestion_ciberincidentes.pdf. Febrero 2020.

2.4. Nivel de impacto

El Esquema Nacional de Seguridad (ENS) indica que el impacto de un ciberincidente en un organismo público se determina evaluando las **consecuencias** que el mismo ha tenido en las funciones de la organización, en sus activos o en los individuos afectados.

Los criterios para la determinar su nivel de impacto atienden a los siguientes parámetros [11]:

- Impacto en la Seguridad Nacional o en la Seguridad Ciudadana.
- Efectos en la prestación de un servicio esencial o en una infraestructura crítica.
- Tipología de la información o sistemas afectados.
- Grado de afectación a las instalaciones de la organización.
- Posible interrupción en la prestación del servicio normal de la organización.
- Tiempo y costes hasta la recuperación del normal funcionamiento de las instalaciones.
- Pérdidas económicas.
- Extensión geográfica afectada.
- Daños reputacionales asociados.

Los incidentes se asociarán a uno de los siguientes niveles de impacto: CRÍTICO, MUY ALTO, ALTO, MEDIO, BAJO o SIN IMPACTO teniendo en cuenta que es obligatorio notificarlos cuando se categoricen con un nivel CRÍTICO, MUY ALTO O ALTO.

A continuación, en la Tabla 2-4 se muestran los criterios de determinación del nivel de impacto de los ciberincidentes junto con sus posibles víctimas:

CRITERIOS DE DETERMINACIÓN DEL NIVEL DE IMPACTO DE LOS CIBERINCIDENTES	
Nivel	**Descripción**
CRÍTICO	- Afecta apreciablemente a la Seguridad Nacional. - Afecta a la seguridad ciudadana, con potencial peligro para la vida de las personas. - Afecta a una Infraestructura Crítica. - Afecta a sistemas clasificados SECRETO. - Afecta a más del 90% de los sistemas de la organización. - Interrupción en la prestación del servicio superior a 24 horas y al 50% de los usuarios. - El ciberincidente precisa para resolverse más de 100 Jornadas-Persona. - Impacto económico superior al 0,1% del P.I.B. actual. - Extensión geográfica supranacional. - Daños reputacionales muy elevados y cobertura continua en medios de comunicación internacionales.
MUY ALTO	- Afecta a la seguridad ciudadana con potencial peligro para bienes materiales. - Afecta apreciablemente a actividades oficiales o misiones en el extranjero. - Afecta a un servicio esencial. - Afecta a sistemas clasificados RESERVADO. - Afecta a más del 75% de los sistemas de la organización. - Interrupción en la prestación del servicio superior a 8 horas y al 35% de los usuarios. - El ciberincidente precisa para resolverse entre 30 y 100 Jornadas-Persona. - Impacto económico entre el 0,07% y el 0,1% del P.I.B. actual. - Extensión geográfica superior a 4 CC.AA. o 1 T.I.S. - Daños reputacionales a la imagen del país (marca España). - Daños reputacionales elevados y cobertura continua en medios de comunicación nacionales.
ALTO	- Afecta a más del 50% de los sistemas de la organización. - Interrupción en la prestación del servicio superior a 1 hora y al 10% de usuarios. - El ciberincidente precisa para resolverse entre 5 y 30 Jornadas–Persona. - Impacto económico entre el 0,03% y el 0,07% del P.I.B. actual. - Extensión geográfica superior a 3 CC.AA. - Daños reputacionales de difícil reparación, con eco mediático (amplia cobertura en los medios de comunicación) y afectando a la reputación de terceros.
MEDIO	- Afecta a más del 20% de los sistemas de la organización. - Interrupción en la presentación del servicio superior al 5% de usuarios. - El ciberincidente precisa para resolverse entre 1 y 5 Jornadas-Persona. - Impacto económico entre el 0,001% y el 0,03% del P.I.B. actual. - Extensión geográfica superior a 2 CC.AA. - Daños reputacionales apreciables, con eco mediático (amplia cobertura en los medios de comunicación).
BAJO	- Afecta a los sistemas de la organización. - Interrupción de la prestación de un servicio. - El ciberincidente precisa para resolverse menos de 1 Jornadas-Persona. - Impacto económico entre el 0,0001% y el 0,001% del P.I.B. actual. - Extensión geográfica superior a 1 CC.AA. - Daños reputacionales puntuales, sin eco mediático
SIN IMPACTO	- No hay ningún impacto apreciable.

Tabla 2-4. Criterios de determinación del nivel de impacto de los ciberincidentes y sus principales víctimas.

Fuente: Guía nacional de notificación y gestión de ciberincidentes. Obtenido de https://www.incibe-cert.es/sites/default/files/contenidos/guias/doc/guia_nacional_notificacion_gestion_ciberincidentes.pdf. Febrero 2020.

Una vez realizado el estudio de los ciberincidentes centrado en su clasificación, detección, nivel de peligrosidad e impacto, en los dos siguientes capítulos pasaremos a analizar dos de ellos por ser algunos de los más reincidentes: PHISHING y RANSOMWARE.

3. Estudio de Phishing

Los ciberataques de tipo phishing son uno de los principales tipos de **fraude** llevados a cabo por los ciberdelincuentes. Esto es debido a que, con poco esfuerzo, pueden lograr mucha información confidencial sobre una multitud de usuarios. A diferencia de otros tipos de ciberataques de Internet, el phishing no requiere conocimientos técnicos especialmente complejos. Al respecto, afirma Adam Kujawa, director de Malwarebytes Labs: *"el phishing es la forma más sencilla de ciberataque y, al mismo tiempo, la más peligrosa y efectiva. Eso se debe a que ataca el ordenador más vulnerable y potente del planeta: la mente humana"* [12].

Los autores del phishing no pretenden explotar una vulnerabilidad técnica en el sistema operativo, sino que utilizan "ingeniería social". En la mayoría de los casos, la parte más débil en un sistema de seguridad no es un fallo oculto en el código informático, sino el individuo que no comprueba la procedencia de un correo electrónico.

3.1. Historia del Phishing

Llevar a cabo una estafa de phishing es muy similar al de la pesca ("fishing" en inglés). Se prepara el "anzuelo" pensando en engañar a una víctima, se lanza y se espera a que "pique" [12].

En los años 70, época en la que apenas había ordenadores en red, se formó una subcultura para explotar el sistema telefónico. Estos primeros hackers se llamaban "phreaks", combinación de las palabras inglesas "phone" (teléfono) y "freak" (raro, friqui). El phreaking era una forma de hacer llamadas gratuitas de larga distancia a números que no aparecían en los listines de teléfonos.

La creación del término "phishing" se atribuyó a Khan C Smith a mediados de los años 90. Si bien es cierto que, la primera vez que se utilizó públicamente la palabra phishing fue el 2 de enero de 1996 en un grupo de noticias Usenet denominado AOHell. En ese momento, America Online (AOL) era el proveedor número uno de acceso a Internet, con millones de conexiones diarias.

Su popularidad le convirtió en la diana de los estafadores. Los hackers y piratas informáticos utilizaron dicha fama para comunicarse entre sí y realizar ataques de phishing contra usuarios legítimos haciéndose pasar por empleados para pedir que verificaran sus cuentas y facilitaran la información de facturación. Con el tiempo, el problema creció tanto que AOL tuvo que advertir a sus clientes que "nadie que trabaje en AOL le pedirá su contraseña o información de facturación".

En la década de 2000, el phishing se centró en explotar los sistemas de pago online y las redes sociales fueron su objetivo para conseguir el robo de identidad. Los clientes de PayPal recibieron correos electrónicos de phishing con enlaces al sitio web falso pidiéndoles que actualizaran los números de su tarjeta de crédito e información personal. The Banker informó del primer ataque conocido de phishing contra un banco en septiembre de 2003.

A mediados de la década de 2000, un software "llave en mano" de phishing ya circulaba en el mercado negro, mientras que grupos de hackers se organizaban para elaborar campañas de phishing.

En 2011, una presunta campaña china de phishing atacó cuentas de Gmail de altos cargos políticos y mandos militares de Estados Unidos y Corea del Sur, así como de activistas políticos chinos. Dos años más tarde, en 2013, se robaron 110 millones de registros de clientes y tarjetas de crédito de los clientes de Target, por medio de una cuenta suplantada con phishing.

El director de la campaña de Hillary Clinton en las elecciones presidenciales de 2016, John Podesta, fue víctima de un ataque de phishing que afirmaba que su contraseña de correo electrónico se había visto comprometida y tenía que cliquear para cambiarla.

En 2017, una estafa masiva de phishing engañó a los departamentos de contabilidad de Google y Facebook para que transfirieran más de 100 millones de dólares a cuentas bancarias en el extranjero bajo el control de un hacker.

Mientras que en 2015 únicamente se realizó un aviso de esta tipología, en 2020 llegaron a casi 30 (Figura 3-1) [13].

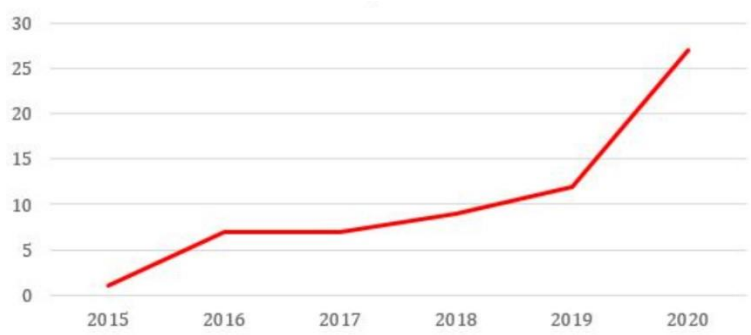


Figura 3-1. Avisos de tipo Phishing detectados.
Fuente: https://www.incibe.es/protege-tu-empresa/blog/tematicas-conoce-los-aspectos-esenciales-los-ataques-tipo-Phishing

Será en el tercer trimestre de 2022 (Figura 3-2), donde APWG (Phishing Activity Trends Report/Grupo de Trabajo Anti-Phishing) observó 1.270.883 ataques de phishing en total, un récord y el peor trimestre para phishing que APWG haya observado alguna vez [14].

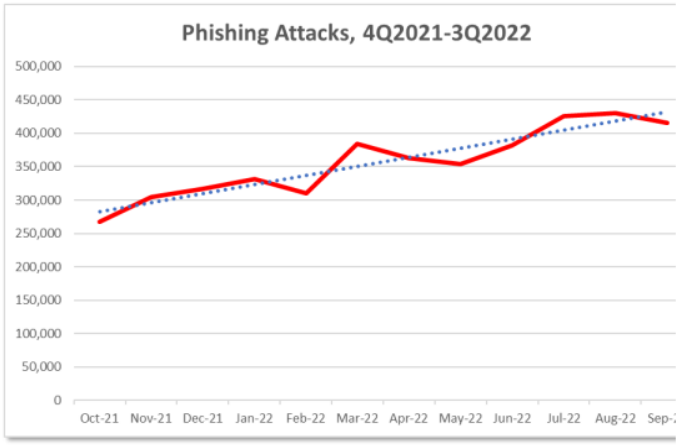


Figura 3-2. Ataques Phishing durante los últimos años.
Fuente. https://apwg.org/

En la actualidad, el ataque de tipo phishing es uno de los principales tipos de incidente de **fraude** más conocidos y extendidos por la Red. Para los ciberdelincuentes resulta sencillo enviar un correo electrónico a un usuario simulando ser una entidad legítima (red social, banco, institución pública, …) donde adjuntan archivos infectados o enlaces a páginas fraudulentas con el objetivo de robarle información privada, realizarle un cargo económico o infectar el dispositivo [15].

3.2. Phishing como tipo de incidente fraude

El correo electrónico es, hoy en día, una de las herramientas de comunicación más utilizadas en las organizaciones, por lo que se ha convertido en uno de los objetivos preferidos de los ciberdelincuentes, creciendo año tras año los ataques a través de este medio. Aunque las organizaciones han ido incorporando distintos métodos de defensa para mejorar su ciberseguridad: antivirus, cortafuegos, análisis de vulnerabilidades…, todo esfuerzo es insuficiente, si no se aplica una serie de buenas prácticas para la seguridad del correo electrónico [16].

Lo primero que se debe hacer es aprender a identificar dicho engaño ya que sólo así, se evitará que caigamos en la trampa y podamos disfrutar de Internet con mayor seguridad. Para ello, a continuación, se analizarán los **tipos de fraude más comunes** que circulan por la Red, detallando en qué consisten y cómo detectar cada uno de ellos [17]:

3.2.1. Falsos préstamos

A través de anuncios y webs de Internet, los ciberdelincuentes ofrecen préstamos muy atractivos con el objetivo de engañarnos. Las prácticas más seguras que debemos seguir son:

- Investigar al prestamista.
- Acudir a entidades oficiales de crédito.
- Revisar ortografía y gramática.
- Denunciar ante el banco.

3.2.2. Falso soporte técnico

Los ciberdelincuentes podrían pedirnos dinero por hacer una falsa reparación del dispositivo o instalarnos programas maliciosos para robar información privada y realizar acciones maliciosas o ilegales desde él. Las recomendaciones que se deben seguir son:

- Restablecer el dispositivo.
- Actualizaciones de seguridad.
- Cambiar las credenciales.
- Reportar el incidente.
- Llamar a nuestro Banco.
- Desinstalar las Apps e instalar Apps originales.

3.2.3. Falsas ofertas de empleo

Los ciberdelincuentes se aprovechan del desempleo, publicando falsas ofertas de empleo con las que obtener un beneficio económico solicitando pagos por adelantado en concepto de gestión, seguro médico, formación inicial, etc. Para no ser presa de su engaño, se debe:

- Revisar la web de la empresa.
- Revisar la redacción oferta.
- Compra material.
- Revisar la web de la empresa.
- Revisar la política protección datos.

3.2.4. Sextorsión

Consiste en chantajear con la publicación de fotos, vídeos o información íntima de nosotros, si no pagamos. En la mayoría de los casos, no tienen ningún material y se aprovechan del miedo o el desconocimiento para engañarnos. Por ello, debemos seguir algunas prácticas como:

- No revelar información.
- Mantener la calma.
- No abrir archivos adjuntos.
- No enviar dinero.
- Desconectar webcam y micrófono.

3.2.5. Perfiles falsos

La creación de perfiles falsos pretende dañar nuestra reputación online, extorsionarnos e incluso robarnos datos personales para cometer otras actividades fraudulentas. Debemos tener cuidado con la información que publicamos en Internet y seguir algunas recomendaciones, como:

- Recopilar pruebas.
- Hacer “Egosurfing”.
- Ejercer derechos ARCO.
- Mejorar la privacidad en las redes sociales.
- No aceptar peticiones de desconocidos.
- Ser selectivo.

3.2.6. Fraudes en compraventa de productos

El principal riesgo es que el vendedor o comprador nos engañe, de tal manera que realicemos el pago de un producto que nunca nos llegará o que enviemos el nuestro y no recibamos el pago. Por ello, no debemos olvidar las siguientes recomendaciones:

- Revisar comentarios.
- No fiarse de ofertas muy agresivas.
- Sospechar de las excusas.
- Aceptar métodos de pago seguros.
- Revisar el perfil vendedor/comprador.
- Denunciar anuncio fraudulento.

3.2.7. Tiendas online fraudulentas

Con el aumento de los marketplaces y las plataformas e-commerce, también crecen los intentos por robar nuestros datos y los timos por parte de los ciberdelincuentes. Este incita a la víctima a comprar algo por un precio demasiado bajo. Luego desaparece y nunca envían el artículo o de recibirlo, que se trate de una falsificación [18].

Las empresas cuentan con sistemas de seguridad que garantizan compras seguras online y sus plataformas solo serán seguras si incluyen la siguiente información:

- Información de la empresa: El NIF o Número de Identificación Fiscal y en parte inferior de la web en un enlace llamado “Aviso legal”.
- Datos que recoge y el uso que hace de ellos. Esta información podemos encontrarla dentro del área de “Privacidad” o en “Términos y condiciones del servicio”.
- No olvidar que tenemos derecho a que nuestros datos estén protegidos. Estos derechos se regulan por medio de la LOPD-GDD y los derechos ARCO.
- Certificado de seguridad: debemos comprobar que la web utiliza el protocolo de comunicación seguro HTTPS.
- Sellos de confianza. Revisar si dispone de uno de ellos.
- Políticas de envío y devolución. En caso de querer efectuar una devolución por la causa que sea, indicará quién asumirá los costes del envío y los plazos.

3.2.8. Falsos alquileres vacacionales

Anuncian inmuebles demasiado buenos y, cuando se muestra interés por ellos, tratarán de obtener nuestro dinero lo antes posible pidiendo pequeños pagos en concepto de fianza o reserva. Las prácticas más seguras que debemos seguir son [19]:

- Revisar las descripciones y las fotografías (calidad, número, robadas ...).
- Comparar el precio con el de mercado (demasiado barato para ser cierto).
- Analizar el perfil vendedor nuestra atención.
- No aceptar excusas y problemas del vendedor para comunicarse en la plataforma.
- No aceptar cualquier método pago.

- Buscar en Google Maps su ubicación.

3.2.9. Bulos y noticias falsas “fake news”

Ante una situación de inseguridad, como es una crisis sanitaria, los ciberdelincuentes se aprovechan de nuestra desinformación para difundir una gran variedad de bulos y fraudes con el objetivo de desinformar, engañarnos o infectarnos para sacar provecho. Se hacen pasar por organizaciones benéficas y solicitan donaciones o se comunican con la víctima para reclamar dinero después de desastres naturales o eventos importantes. Para frenar a este tipo de fraude se recomienda seguir unas buenas prácticas [20]:

- No dejarnos llevar por noticias sobre temas de interés social o de actualidad que pretendan crear una alarma o atraer nuestra atención.
- Ser recelosos ante promociones, ofertas y descuentos, especialmente en época de rebajas o compras navideñas.

3.2.10. Citas y romance

Los ciberdelincuentes se aprovechan de las personas que buscan parejas románticas, a menudo a través de sitios web de citas, aplicaciones o redes sociales, haciéndose pasar por posibles compañeros/as. Juegan con desencadenantes emocionales para que se proporcione dinero, obsequios o detalles personales [21].

3.2.11. Criptomonedas

Son muy diversas y pueden ser intercambiadas por divisas tradicionales como el euro. Sin embargo, su uso no está amparado por las autoridades, por lo que el perjuicio ocasionado es responsabilidad del usuario. Están muy presentes en la financiación del terrorismo, chantajes y estafas como la sextorsión, blanqueo de dinero y compra y venta de productos ilegales en la “darkweb”, tales como drogas o medicamentos peligrosos o falsificados que pueden llegar a causar la muerte del consumidor [22].

3.2.12. Fraude bancario

Los ciberdelincuentes envían correos electrónicos de varios bancos con la esperanza de que realicemos las operaciones bancarias con, al menos, uno de ellos. Suelen fingir fingen ser compañeros de trabajo y solicitan inicios de sesión. Dado que muchas empresas contratan personal independiente que trabaja de forma remota, obtienen fácilmente el acceso a información confidencial tanto de empleados como de clientes.

Además, mediante las redes sociales, pueden averiguar con quién realizamos operaciones bancarias, qué servicios utilizamos, dónde trabajamos … Para frenar este tipo de fraude, los actuales servicios de monitoreo de crédito permiten realizar un seguimiento de los cambios que realizamos y nos avisa cada vez que actualizamos nuestro perfil [23].

3.2.13. Fraude de inversión

Para usuarios que buscan obtener rentabilidad de sus ahorros, las entidades bancarias ofrecen productos de inversión adaptados a distintos perfiles de cliente. Esto es aprovechado por los ciberdelincuentes para cometer sus estafas ofreciendo falsas ofertas de inversión a través de llamadas telefónicas prometiendo grandes beneficios en poco tiempo [24].

3.2.14. Robo de identidad

Forma de fraude de comercio electrónico donde se roban los datos sensibles de otra persona y los utilizan para llevar a cabo transacciones en sitios de comercio electrónico como la víctima [25].

3.2.15. Fraude de contracargo

Una de las formas más simples de fraude que no implica el robo de identidad. Un cliente pide artículos del sitio web utilizando una Visa o un servicio de tarjeta similar. Una vez que los artículos se envían de forma segura, el cliente inicia un contracargo, indicando que su identidad fue robada y afirma que el producto nunca fue recibido [25].

3.2.16. Fraude amistoso

Casi idéntico al fraude de contracargo, pero sin intención maliciosa. La transacción se realiza por un verdadero cliente, y el contracargo se inicia para algo inocente como creer que su paquete fue robado o no reconocer el nombre del comerciante en el estado de cuenta de su tarjeta de crédito [25].

3.2.17. Fraude limpio

Un ciberdelincuente utiliza una tarjeta de crédito robada evitando alertar a los detectores de fraude, ya ha robado la suficiente información sobre el titular de dicha tarjeta y puede pasar fácilmente la transacción como legítima [25].

3.2.18. Fraude de triangulación

El ciberdelincuente configura una tienda en línea falsa para recopilar los datos completos de un cliente. Una vez que la víctima ha "hecho un pedido", comete fraude limpio en el sitio de una tienda de comercio electrónico para enviar el artículo deseado al cliente, con frecuencia utilizando la información de la tarjeta de una víctima diferente [25].

3.2.19. Fraude de afiliados

El ciberdelincuente manipula los datos recopilados por el enlace de afiliado que les dio un minorista para hacer que dicho minorista les pague mucho más de lo que se les debe. Se puede hacer a través de un proceso automatizado o por personas reales que utilizan perfiles falsos [25].

3.2.20. Fraude de tarifas avanzadas y transferencias bancarias

El ciberdelincuente pide dinero por adelantado a cambio de recibir mucho más a posteriori [25].

3.3. Variantes de Phishing

A menudo los "ataques de pesca" intentan que los destinatarios de sus correos electrónicos abran un fichero adjunto malicioso o cliqueen en una URL no segura para entregar sus credenciales mediante páginas preparadas, números de tarjeta de crédito, etc. Actualmente existen muchas variantes o vías de comunicación, entre las cuales destacan [26]:

3.3.1. Ataque de pesca engañosa **(deceptive)**

Se considera el ataque más común y consiste en un atacante que envía al usuario un mensaje de correo electrónico haciéndose pasar por una persona, empresa o entidad. Con cualquier pretexto, solicita al usuario que introduzca información personal sensible que, será capturada por el atacante.

3.3.2. Ataque de pesca dirigido (spear)

Consiste en una modalidad phishing dirigida contra un objetivo específico, en el que los atacantes, mediante un correo electrónico, consiguen información confidencial de la víctima, que utilizarán para preparar el ataque.

3.3.3. Estafa del directivo (whaling)

Dirigido normalmente a ejecutivos con el objetivo de obtener autorizaciones de estos altos cargos para realizar transacciones fraudulentas. Consiste en suplantar identidades, creando falsos correos electrónicos y sitios web para obtener datos confidenciales.

3.3.4. Ataque por pesca de voz (vishing)

El atacante contacta con la víctima telefónicamente o mediante la voz por IP y le engaña para conseguir datos sensibles o recaudar fondos. Los estafadores se hacen pasar por fuentes de confianza para conseguir información confidencial como números de tarjetas de crédito.

3.3.5. Ataque de smishing

El contacto se realiza mediante SMS, en el cual el remitente es un nombre en lugar de un teléfono y este nombre suplanta una organización conocida, de forma que se engaña al usuario para que haga una acción determinada.

Cuando se utiliza el teléfono, el usuario se muestra menos receloso que con el ordenador. Sin embargo, la seguridad de los smartphones tiene limitaciones y no puede proteger contra el smishing. El cibercrimen dirigido a dispositivos móviles se está disparando y, aunque, los dispositivos Android siguen siendo el principal objetivo del malware, el smishing (como los propios SMS) funciona en distintas plataformas y ningún sistema operativo móvil puede protegerte de ataques de tipo

phishing. Se debe actuar con mucha prudencia ya que el ciberataque suele llevar el logo de la empresa o el nombre de la web a la que te redirecciona muy similar al de la página real.

3.3.6. Ataque de pharming

El objetivo es envenenar el DNS o de cambiar la dirección IP de una página web para redirigir la víctima a un portal web malicioso. Las estafas de pharming intentan convencer a las personas para interactuar con páginas web falsas con el fin de recopilar sus datos personales, como correos electrónicos y contraseñas, o infectar sus ordenadores con malware.

Algunos de los ataques de pharming que podemos destacar son [27]:

- Ataque a nivel mundial en 2007 donde más de 50 instituciones financieras fueron atacadas a través de una vulnerabilidad de Microsoft. Se atrajo a los clientes a una página falsa con código malicioso que se descargaba malware troyano y archivos de un servidor ruso. El servidor ruso se descargaba las credenciales de las víctimas que visitaban alguna de las páginas web bancarias afectadas antes de redirigirlas a la página web real. Millones de víctimas en los Estados Unidos, Europa y la región Asia-Pacífico se vieron afectadas.
- Ataque en Brasil en 2015 a través de un correo electrónico que afectó a los usuarios de Internet de Brasil. Los hackers aprovecharon un fallo en los routers domésticos para acceder a la administración, donde cambiaron los ajustes DNS a un servidor DNS malicioso.
- Ataque en Venezuela en 2019 donde los hackers aprovecharon la crisis humanitaria del país secuestrando una página web creada para que los voluntarios se registrasen ofreciendo su ayuda. Días después, apareció una página web fraudulenta con una apariencia idéntica.

3.4. Métodos de infección de Phishing

Un mensaje urgente o una promoción muy atractiva para motivarnos a cliquear en el enlace o archivo adjunto… suelen ser los cebos principales. Sin embargo, como hemos visto en el apartado anterior 3.3, también pueden utilizar otras vías de comunicación. Ahora bien, sea cual sea el medio utilizado, el phishing siempre tiene el mismo objetivo: obtener datos personales y/o bancarios de los usuarios haciéndonos creer que los estamos compartiendo con alguien de confianza. También, pueden utilizar esta técnica para que descarguemos malware con el que infectar y/o tomar control del dispositivo.

Por todo ello y para no convertirse en un objetivo fácil de los ciberdelincuentes, conviene reconocer algunos de sus **métodos de infección o mecanismos de acción** utilizados con mayor frecuencia [28]:

3.4.1. Contenido del mensaje o correo electrónico

Se debe actuar con mucha prudencia ante correos con mensajes extraños y que aparentan ser de entidades bancarias, una plataforma de pago, una red social, un servicio público o conocido (Dropbox, Facebook, Google Drive, Apple ID, Correos y Telégrafos, Agencia Tributaria, etc.).

Su objetivo es asustar al usuario para que actúe según las indicaciones de dicho mensaje. Siempre añaden un pretexto como “problemas técnicos o de seguridad”, y ofrecen una solución sencilla del tipo “acceda a su banco utilizando este enlace”. Además, suelen solicitar el nombre de usuario, claves y datos de acceso a las cuentas, algo que las entidades legítimas nunca harían (Figura 3-3).

Figura 3-3. Contenido sospechoso.

Fuente: https://www.osi.es/es/banca-electronica

3.4.2. Errores ortográficos y gramaticales

Debemos sospechar cuando hay errores gramaticales en el texto ya que pueden haber utilizado un traductor automático para la redacción del mensaje trampa: ausencia de tildes, errores gramaticales (enes en lugar de eñes) y de puntuación (Figura 3-3).

Asimismo, ningún servicio con reputación enviará a sus clientes una comunicación con una redacción informal y ortografía descuidada. Normalmente, este tipo de ciberdelincuentes son extranjeros y traducen sus mensajes al español con errores en forma de:

- Fallos semánticos: artículos “el” o “la” intercambiados.
- Palabras con símbolos extraños como “DescripciÃ?n”, caso muy frecuente cuando intentan escribir vocales acentuadas en un teclado no español.
- Frases mal construidas.

3.4.3. Comunicaciones impersonales

Cuando una entidad se dirige por correo a un usuario o cliente, siempre enviará correos electrónicos personalizados utilizando el nombre de la persona e incluso parte de su DNI. Si recibimos un correo no personalizado, estamos probablemente ante un caso de intento de estafa.

Al mismo tiempo, se debe tener presente que si un ciberdelincuente quiere estafar a una multitud de personas es muy complicado conocer el nombre de todas esas personas; por ello, utilizan fórmulas genéricas como “Estimado cliente”, “Hola”, “Hola amigo” … para evitar decir un nombre (Figura 3-4):

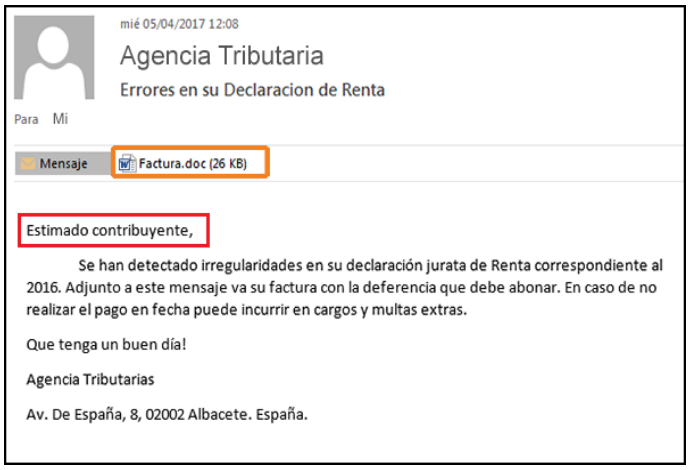


Figura 3-4. Comunicaciones impersonales.
Fuente: https://www.osi.es/es/banca-electronica

3.4.4. Sensación de urgencia

Cuando el mensaje nos obliga a tomar decisiones en un período de tiempo muy corto es mala señal: "*Una vez emitido este correo electrónico, tendrá un plazo de 8 horas para llevar a cabo dicha acción, de lo contrario…*" (Figura 3-5); si fuera así, debemos comprobar si la urgencia es real consultando la Policía, Guardia Civil, etc. Con esta sensación de urgencia, los ciberdelincuentes pretenden que su víctima se precipite en su decisión: visitar un enlace e indicar datos personales y/o contraseñas.

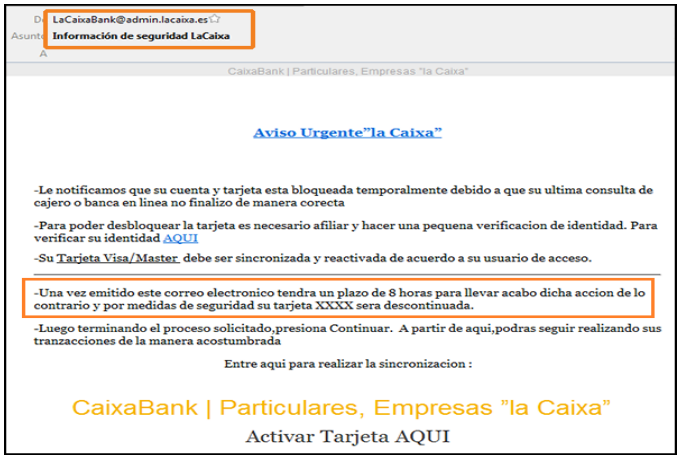


Figura 3-5. Generar una sensación de urgencia.
Fuente: https://www.osi.es/es/banca-electronica

3.4.5. Descarga de archivos adjuntos

No se debe descargar ningún archivo que nos haya solicitado el atacante, ni ceder el control de nuestro equipo por medio de algún software de control remoto.

3.4.6. Dominio del correo electrónico

Un servicio con prestigio utilizará sus propios dominios para las direcciones de email corporativas; por lo que debemos sospechar siempre que recibamos la comunicación desde un buzón de correo tipo @gmail.com, @outlook.com o similar.

3.4.7. Enlaces falseados utilizando redirectores y acortadores

Redirectores

En este tipo de estafa realizada por medio de redirectores se usan dos o más sitios webs. Los ciberdelincuentes pretenden que cliqueemos en un enlace para llevarnos a un sitio web fraudulento. En el mensaje hay un enlace que en lugar de llevarte a la web oficial "página legítima", te llevará a otra que aparentemente es igual o muy parecida (Figura 3-6). Para comprobar la verdadera dirección, debemos situar el puntero encima de dicho enlace observando la verdadera dirección que se muestra en la parte inferior izquierda del navegador.

Siempre tenemos que revisar si el texto del enlace facilitado en el mensaje coincide con la dirección a la que se refiere y si corresponde con la URL del servicio legítimo. Si queremos acceder a la web legítima, la mejor opción es escribir directamente en la barra de direcciones del navegador la dirección deseada, en lugar de acceder a una web a través de un enlace en el correo electrónico.

Figura 3-6. Enlace falseado utilizando redirectores.
Fuente: https://www.osi.es/es/banca-electronica

Los pasos dados por los ciberdelincuentes suelen ser los siguientes [29]:

- El enlace redirecciona a la web fraudulenta donde solicitan los datos de usuario.
- Si se introducen los datos de acceso a la banca online, en la siguiente pantalla se solicitarán los datos de su tarjeta.
- Una vez facilitados los datos de la tarjeta, los ciberdelincuentes solicitan la firma electrónica.
- En el último paso, se solicita una supuesta clave recibida por SMS. Después de introducirla, redirige al usuario a la web legítima de Ibercaja.

- Una vez introducidos los datos, ya estarán en poder de los ciberdelincuentes y podrán realizar acciones fraudulentas con ellos.

El uso de redirectores en páginas webs es relativamente normal (Figura 3-7), siendo sus principales casos los que aparecen a continuación [30]:

Figura 3-7. Aviso de redireccionamiento.
Fuente. https://www.blackploit.com/2019/05/bypass-redirect-check-google-youtube.html

Caso 1. Avisar al usuario que está saliendo del dominio principal. Este caso es utilizado por grandes sitios webs para evitar que nos redirijan a sitios webs maliciosos o con phishing sin previo aviso, como lo hace Google en este caso (Figura 3-8):

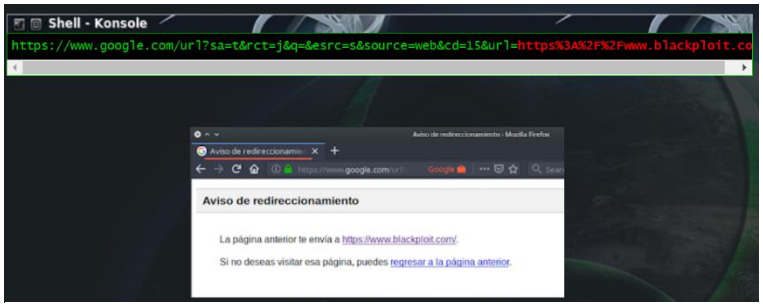


Figura 3-8. Caso 1 de redireccionamiento.
Fuente. https://www.blackploit.com/2019/05/bypass-redirect-check-google-youtube.html

Caso 2. Recolectar datos de navegación de los usuarios. Este caso es usado por grandes plataformas para separar las operaciones con la analítica del sistema. La Figura 3-9 muestra un ejemplo donde Twitter que usa su acortador t.co para redirigir todo el tráfico y poder analizar el comportamiento de sus usuarios.

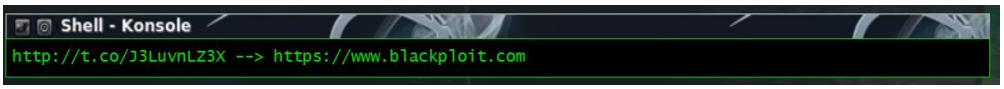


Figura 3-9. Caso 2 de redireccionamiento.
Fuente. https://www.blackploit.com/2019/05/bypass-redirect-check-google-youtube.html

Caso 3. Llevar al usuario a una página de publicidad para que haga click en algún anuncio de pago que contiene elementos gráficos atractivos (Figura 3-10).

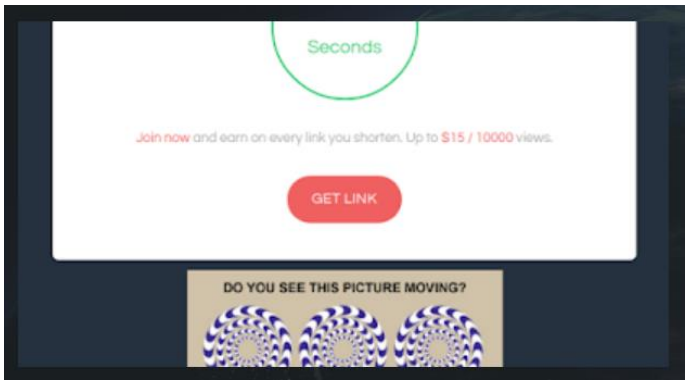


Figura 3-10. Caso 3 de redireccionamiento.
Fuente. https://www.blackploit.com/2019/05/bypass-redirect-check-google-youtube.html

Como veremos a continuación, usar un acortador es la mejor forma de hacer un redirector porque así te aseguras de que nadie pueda ingresar en la URL un parámetro malicioso.

Acortadores

Las URL acortadas nacen en el año 2001 porque algunas aplicaciones como las redes sociales solo permitían el envío de mensajes de un número reducido de caracteres. Su uso se ha extendido, principalmente, en los SMS para acortar URL que se introducen en los mismos. Como se ha visto en el subapartado anterior (Redirectores. Caso 2), también se utiliza mucho en plataformas como Twitter ya que solo permite publicar mensajes de 280 caracteres. Cabe destacar que Facebook, Twitter, LinkedIn y YouTube contienen recortadores de URL integrados en su propio servicio para facilitar esta tarea a los usuarios [31].

Por tanto, una URL acortada es solamente una dirección web con menos caracteres que la dirección de la página web original, pero que nos dirige al mismo sitio. Aunque al comienzo de esta nueva URL acortada aparece el nombre del servicio que la ha generado, la nueva URL es más práctica y a nivel estético más bonita que un enlace de dos líneas. Sin embargo, no nos proporciona información de la página a la que nos redirige; de hecho, si pasamos el cursor por encima del enlace solo veremos el enlace acortado, pero no su destino real, algo de lo que los ciberdelincuentes se aprovechan para poder engañar a los usuarios.

Aunque las URL acortadas no suponen un peligro por sí mismas, es importante que seamos conscientes de ellos y tomemos algunas precauciones:

- Debemos ser **cuidadosos con los enlaces acortados**, aunque se hayan generado con servicios conocidos.
- Podemos **instalar un complemento en el navegador**, como es el caso de Unshorten.link para Chrome que nos permita conocer la dirección original, detecte si puede contener malware o si puede tratarse de un phishing. Por otra parte, también existe para el navegador Mozilla Firefox la extensión Link Unshorten que realiza la misma función que la anterior para Chrome.

- Un **analizador de direcciones web o URL** nos permite analizar la URL que nos han enviado o a la que pretendemos acceder. Nos mostrará su URL completa y realizará un análisis de malware. Por ejemplo, para averiguar el enlace original podemos usar dos analizadores de URL online gratis como VirusTotal y URLVoid.
- **No proporcionar** ningún dato privado ni ninguna contraseña a páginas web con URL acortadas. Si accedemos a páginas de bancos o tiendas online donde introducimos nuestra tarjeta bancaria, debemos hacerlo desde la URL completa, asegurándonos siempre de que cumple con estándares de protección y navegación segura, como, por ejemplo, que tenga HTTPS.

Para concluir con este apartado, insistir, una vez más, que solo la **responsabilidad**, la **intuición**, la **disciplina** y el **sentido común**, junto con el **conocimiento** de cada uno de los puntos expuestos anteriormente, nos ayudarán a reconocer los mecanismos de acción utilizados en un intento de ataque de phishing. Todo ello, sin olvidar que el hecho de solicitar nuestros datos bancarios junto con los personales conlleva con casi toda seguridad hablar de fraude (Figura 3-11).

Figura 3-11. Fórmula FRAUDE.
Fuente. Elaboración propia a partir de https://www.osi.es/es/banca-electronica

3.5. Medidas de seguridad ante Phishing

El desarrollo digital no solo nos ha traído beneficios, sino también bastante inseguridad cibernética; por lo que, la prevención de ciberataques es algo esencial en cualquier tipo de empresa y usuario. De aquí la importancia de hacer un uso responsable de la red y evitar cualquier ciberataque que pueda poner en peligro la propia integridad, el presente y el futuro de la organización.

Por ello, las empresas deberían elaborar un **plan de ciberseguridad** efectivo que consiga evaluar los posibles riesgos, establecer objetivos, analizar las tecnologías disponibles para comprobar que sean seguras, seleccionar un marco de seguridad, revisar las políticas de seguridad, desarrollar el plan de gestión de riesgos, implementar el plan propiamente dicho y evaluar los resultados generados.

Un plan de ciberseguridad implica seleccionar e implementar acciones prácticas para proteger una empresa de amenazas externas e internas, por lo que los pasos generales a seguir para prevenir cualquier tipo de ciberataque son similares. Para obtener una información más detallada, véase el [Anexo III. Plan de Ciberseguridad].

A continuación, se señalarán las **medidas de seguridad** más importantes de ciberataques en Pymes [33], para posteriormente indicar algunas medidas muy básicas de prevención:

3.5.1. Gestión de riesgos

Cualquier tipo de empresa debe asegurarse en invertir en su ciberseguridad. Uno de los factores claves para la prevención de ciberataques es contar con una empresa de seguridad responsable y confiable. Asimismo, debemos ser conscientes de qué riesgos estamos dispuestos a asumir y evaluar la inversión para minimizarlos.

3.5.2. Protección de la red

Este es uno de los factores más importantes en la prevención de ciberataques, la red de la empresa debe estar protegida de ataques externos e internos. Para ello, se debe comprobar que el proveedor de internet utilice cortafuegos que permita controlar las conexiones de acceso a internet. La mejor recomendación es que un experto guíe para hallar la mejor solución para la empresa.

3.5.3. Actualización del Software

Normalmente, las empresas suelen comprar un software de seguridad informática y no se acuerdan de él hasta el día que tienen un problema, por lo que se debe estar al tanto de la fecha de actualización. Además, se recomienda realizar revisiones periódicas para detectar posibles debilidades que pueda tener el sistema de seguridad informático.

3.5.4. Control del uso de dispositivos extraíbles

Dentro de la empresa, se deben utilizar únicamente dispositivos extraíbles proporcionados por el administrador de sistemas: CD, memorias USB, DVD, tarjetas SD… Debe haber un control sobre ellos, estar informados de su contenido y escanearse periódicamente para evitar los virus o malware.

3.5.5. Perfiles de usuario

Se debe establecer un perfil con nombre y contraseñas para cada usuario, así como sus limitaciones dependiendo de su puesto laboral. Se recomienda tener mucho cuidado con el acceso a datos financieros, clientes, estrategias, etc.

3.5.6. Control de las redes y servicios

Dentro de los softwares de seguridad, suelen incluir como medida de prevención a ciberataques a pymes la posibilidad de monitorizar el protocolo de la red. De esta manera, se puede detectar si existe alguna actividad inusual o existen fallas de hardware. Ahora bien, si nos referimos a una gran organización, es necesario contar con servicios de análisis de tráfico, uso de IP y mucho más.

3.5.7. Educación de los empleados

Tanto una buena educación de los usuarios como un software antiphishing forman una doble barrera contra el citado ciberincidente; por ello, las empresas deberían invertir en programas de **concienciación** y **formación** para enseñar a sus empleados cómo reconocerlos y prevenirlos.

Con las **medidas básicas de prevención** que deberían conocer todos los usuarios (Tabla 3-1) se dará por finalizado este capítulo dedicado al estudio de phishing, dando paso al estudio de ransomware, información que se abordará en el siguiente capítulo.

MEDIDAS BÁSICAS DE PREVENCIÓN PHISHING
Verificar la fuente de información de los correos entrantes rechazando cualquiera que incida en que facilitemos datos confidenciales.
Prestar atención a los links para no cliquear en los enlaces que adjunten en el correo y que podrían dirigirnos a una web fraudulenta.
Actualizar las contraseñas de forma regular.
Introducir los datos confidenciales únicamente en webs seguras que empiecen por 'https://' y en el navegador debe aparecer el icono de un pequeño candado cerrado.
Revisar periódicamente las cuentas para controlar cualquier irregularidad en las transacciones online.
Evitar las ventanas emergentes.
Activar los firewalls como una forma efectiva de prevenir ataques externos ya que actúan como un escudo. Si usamos juntos con los firewalls de escritorio refuerzan su seguridad y evitan el phishing.
Activar todos los recursos: - Actualizar el navegador y antivirus de forma constante. - Descargar complementos gratuitos que detectan los signos de un sitio web malicioso o alertan sobre sitios de phishing conocidos.
No olvidar que también puede utilizar otras webs: ebay, Facebook, Pay Pal, etc. (no solo de banca online vive el phishing), domina idiomas y no reconoce fronteras.

Tabla 3-1. Medidas básicas de prevención de Phishing.

Fuente: Elaboración propia a partir de Medidas de prevención de ciberataques en Pymes. (2022, 4 de noviembre). Obtenido de https://dirigentesdigital.com/tecnologia/las-7-mejores-medidas-de-prevencion-de-ciberataques-en-pymes

4. Estudio de Ransomware como incidente malware

El ransomware (del inglés ransom, 'rescate', y ware, acortamiento de software) o 'secuestro de datos' en español, es una extorsión realizada a través de un malware o programa dañino que se introduce en los equipos (ordenadores, portátiles y dispositivos móviles), restringe el acceso a determinadas partes o archivos del sistema operativo infectado y pide un rescate a cambio de quitar esta restricción. En sus orígenes, el pago se hacía a través de cuentas bancarias de países opacos, pero como se conseguía rastrear al ciberdelincuente, se pasó al uso de monedas virtuales no rastreables [34].

El malware es un programa malicioso que realiza acciones dañinas en un sistema informático de forma intencionada y sin el conocimiento del usuario. Algunos ejemplos de estas actividades maliciosas son el robo de información, dañar o causar un mal funcionamiento del sistema informático, provocar perjuicios económicos, chantajear a propietarios de los datos de sistemas informáticos, permitir el acceso de usuarios no autorizados, provocar molestias o una combinación de varias de estas actividades. Algunos tipos de ransomware cifran los archivos del sistema operativo inutilizando el dispositivo y coaccionando el usuario a pagar el rescate [26].

4.1. Historia del Ransomware

A finales de la década de 1980, el primer ransomware apareció con el propósito de bloquear el funcionamiento de puestos de trabajo a particulares y empresas. En 1989, el «troyano AIDS» fue el primero de la historia en un contexto de preocupación por la aparición del virus del SIDA.

A pesar de este golpe, los ataques DDoS y los gusanos acapararon toda la atención ya que podía ser rastreado por la información de pago. Casi 15 años tardaron en aparecer los nuevos ransomware, con la llegada de las monedas digitales y, posteriormente, de las criptomonedas, que permitieron mayor fluidez en los pagos de los rescates y en los cambios de moneda, así como su anonimato.

En 2005, PGPCoder (o Gpcode) fue uno de los primeros ejemplos de ransomware distribuido online. Su objetivo era infectar los sistemas Windows dirigiéndose a archivos con extensiones como .rar, .zip, .jpg, .doc o .xls. Mensajería, redes sociales, foros ... es la base sobre la que el ransomware WinLock vivió desde 2011 hasta 2014. Su objetivo era bloquear el acceso mostrando una ventana que contenía una foto pornográfica y una solicitud de pago mediante un servicio de SMS.

Tras su éxito, aparecieron otras variantes que usurpaban la imagen de las fuerzas de seguridad. Los internautas pagaban rápidamente para evitar cualquier represalia relacionada con la infracción de los derechos de autor o la distribución de contenidos pornográficos.

El año 2013 marcó la diferencia con el ransomware CryptoLocker. Con el uso de un servidor de mando y control, el ciberatacante puede hablar con la víctima, negociar, ampliar o reducir el plazo antes de la destrucción de los datos. Fue uno de los primeros que solicitaba un rescate en bitcoin.

En 2014, el ataque se amplió a tabletas y móviles Android. El año 2016 fue un año decisivo, pasó de registrarse de media un ataque cada 2 minutos a hacerlo cada 40 segundos, es decir, se triplicaron

los casos. Su objetivo era secuestrar datos del mayor número posible de equipos para bloquear completamente el acceso a ellos, si no se pagaba un rescate para desbloquearlos.

A finales de 2019 se introdujo el mecanismo de doble extorsión: la empresa afectada no solo es víctima de la petición de rescate, sino que también se ve amenazada con la reventa de sus datos en la *darknet*. Revelar parte de los datos robados era decisivo para convencer a las empresas contrarias a pagar el rescate, la mayoría de las veces en forma de código fuente o datos de clientes.

Una de las últimas revoluciones ha sido la aparición de plataformas de ransomware-as-a-service (RaaS). Estas alquilan sus soluciones maliciosas y cobran un porcentaje del rescate de las víctimas. Algunos atacantes, después de invertir en investigación y desarrollo de ransomware, crean franquicias para comercializarlo a otros grupos delictivos, como el caso de ransomware Conti.

En 2021, aparecieron los intermediarios de acceso inicial (IAB) en el mundo cibernético. Especializados en la intrusión en empresas, proporcionan acceso a las redes corporativas para que otros grupos maliciosos las utilicen para sus propios ataques. Además, con la aparición de nuevas tecnologías y el regreso de los conflictos geopolíticos, lo lógico es que aparezcan otras nuevas formas de ciberamenazas. Por tanto, todavía queda mucho por contar del futuro de ransomware [35].

4.2. Tipos de Ransomware

Ransomware, “software de secuestro”, se trata de un tipo de **malware** que consigue tomar el control del dispositivo para cifrar el acceso al mismo y/o nuestros archivos o discos duros. Normalmente, se transmite tanto como un troyano o como un gusano infectando el sistema operativo con un archivo descargado o exploiteando una vulnerabilidad de software.

Cuando el ransomware consigue propagarse en la red, los operadores utilizan métodos avanzados como la **exfiltración de datos**, que consiste en filtrar la información confidencial antes de cifrarla para hacer una doble extorsión: primero bloqueando el acceso y luego amenazando con publicar la información privada de tu empresa si no pagas el rescate [36].

“La exfiltración de información puede ser una amenaza incluso mayor que el ransomware porque los ciberatacantes desplazan grandes cantidades de datos secretos hacia los sistemas que controlan, para posteriormente proceder a extorsionar a la víctima, amenazando con divulgar esa información confidencial o vendiéndola a otros criminales” afirma Víctor Ruiz fundador de SILIKN.

Un ejemplo de esto ocurrió a principios de 2022, Nvidia se enfrentó al grupo criminal Lapsus$ y a la exposición pública del código fuente de una tecnología invaluable, ya que filtró el código fuente de la investigación Deep Learning Super Sampling (DLSS) de la compañía.

Cuando una compañía es víctima de la exfiltración de datos, las **consecuencias más evidentes** que conllevan son las siguientes [37]:

- **Pérdida de información.** Ante una exfiltración de datos es muy difícil recuperar el 100% de la información: documentaciones (números de tarjetas de crédito y credenciales de acceso), procesos de la compañía, información sobre proyectos, prepatentes... Todo ello, conllevaría una pérdida económica y estratégica.

- **Pérdida de negocio**. El tiempo destinado al restablecimiento de sistemas TI e información, supone una parada a la producción. Dicha interrupción del servicio hace que sus clientes pierdan la confianza en su empresa.
- **Dedicación de Recursos Humanos.** Como media, tras un ciberataque, las empresas necesitan un periodo de 6 meses para recuperarse y la implicación de muchos profesionales TI internos y externos es fundamental. Todo ello, supone un coste humano muy elevado para las pymes.
- **Responsabilidad ante terceros.** No podemos olvidar el daño que afecta a terceros (proveedores o clientes). Estos daños pueden venir en forma de incumplimiento de obligaciones y compromiso, pero también pueden suponer que información sensible de cuyo tratamiento somos responsables pueda verse comprometida y utilizada en perjuicio de terceros.
- **Pérdida reputacional y de clientes.** El cliente es consciente de los peligros que conlleva que sus datos acaben en manos de los ciberdelincuentes, por lo que perderá la confianza en su empresa y no utilizará sus servicios. Además, cuanta más notoriedad tenga la compañía, mayor será el coste reputacional.

Además, como ya se ha visto en el apartado 4.1, estos últimos años los softwares de secuestro han evolucionado de forma alarmante, los adversarios se han organizado en grupos (Conti, Lockbit, Sodinokibi o Pysa) y se han convertido en empresas de servicios tecnológicos expertos en extorsión. En estos casos, si el rescate a cambio de quitar la restricción de cifrado no funciona, buscan otras formas de ciberamenaza: la exposición pública de datos que han podido extraer del sistema atacado, borrar o inutilizar las copias de seguridad que hubieran podido quedar sin infectar …

Algunos de estos softwares de secuestro más importantes son [26]:

4.2.1. WannaCry

Este es un ejemplo real de ransomware muy conocido en todo el mundo. En el año 2017 se registró un ataque mundial que afectó a Telefónica, Iberdrola y Gas Natural, entre otras empresas en España.

La prensa informó de que unos 141.000 ordenadores habían sido atacados en todo el mundo. Los expertos argumentan que WannaCry usó la vulnerabilidad EternalBlue, desarrollada por la Agencia de Seguridad Nacional de los EE. UU. y filtrada por el grupo The Shadow Brokers, que permite atacar ordenadores con el sistema operativo Microsoft Windows no actualizado correctamente.

4.2.2. Cryptorbit

Este programa de ransomware, lanzado a principios de diciembre del 2013, tiene como objetivo todas las versiones de Windows, incluidas Windows XP, Windows Vista, Windows 7 y Windows 8.

Cuando está infectado, este ransomware explorará el ordenador y cifrará cualquier fichero de datos que encuentre, sea cual sea el tipo o extensión del fichero. Cuando cifra un fichero, también crea un fichero HowDecrypt.txt y un HowDecrypt.gif en cada carpeta donde un fichero ha sido cifrado. Los ficheros GIF y TXT contendrán instrucciones sobre cómo acceder a un lugar de pago que se puede utilizar para enviar en rescate. Este lugar de pago se encuentra en la red Tor y solo se puede realizar el pago en bitcoins.

4.2.3. CryptoLocker

Este ransomware, tipo troyano y extendió a finales del 2013, está dirigido a ordenadores con el sistema operativo Windows. Se distribuye como archivo adjunto de un correo electrónico o accediendo a través del puerto remoto 3389. Una vez activado, el software malicioso cifra ciertos tipos de archivos almacenados en discos locales y en unidades de red empleando criptografía de clave pública RSA y guardándose la clave privada en los servidores del software malicioso.

Una vez realizado el cifrado, muestra un mensaje en pantalla, donde ofrece descifrar los archivos afectados si se paga antes de una fecha indicada (con bitcoins o vales de prepago). Continúa diciendo que la clave privada será destruida del servidor y será imposible recuperarla si la fecha expira.

4.2.4. Ryuk

Cuando Ryuk infecta un sistema, primero desconecta 180 servicios y 40 procesos. Estos servicios y procesos evitan que Ryuk haga su trabajo o son necesarios para facilitar el ataque. Ryuk cifra archivos como, por ejemplo, fotografías, vídeos, bases de datos y documentos utilizando el ciframiento AES de 256 bits. Ryuk puede cifrar en unidades de red.

4.2.5. Hoax Ransomware

Este tipo de ransomware únicamente 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 [38].

4.2.6. Scareware

Utiliza el engaño del falso software o soporte. Suele aparecer como un anuncio molesto emergente informando de una supuesta infección por virus y aporta una solución fácil, descargando un programa de limpieza que casi siempre es el malware. El propio anuncio lanzado por la página visitada no suele suponer una amenaza, aunque se recomienda no cliquear en sus enlaces y prestar atención al cierre de la ventana emergente, ya que suele incluir botones de cierre falso [38].

4.2.7. 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 unos casos, informan del cifrado de archivos y el procedimiento para recuperarlos, pero los archivos están intactos. En este caso, solo se ha producido un bloqueo de la pantalla.
- En otros casos, un mensaje de las fuerzas de seguridad indica que se han detectado actividades ilegales y se solicita el pago de una sanción para desbloquear el equipo (conocido como el virus de la policía, pero en ningún caso tiene relación con ella) [38].

4.2.8. Ransomware de cifrado

Está 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 información para evitar que los datos puedan ser descifrados. Una vez que los ciberdelincuentes se apoderan de los archivos, no hay ningún software de seguridad ni restauración del sistema capaz de devolvérselos. Incluso pagando el rescate, no hay ninguna garantía de que los ciberdelincuentes le devuelvan los archivos. Dentro de esta variante hay una llamada wiper, que no devuelve el acceso a los archivos, simplemente los elimina [38].

4.2.9. Doxware

Emplea una técnica conocida como doxing, que consiste en amenazar al usuario con publicar los datos personales extraídos como se muestra en la Figura 4-1. La presión ejercida al usuario implica un incremento de la efectividad del ataque y beneficio para el ciberdelincuente [38].

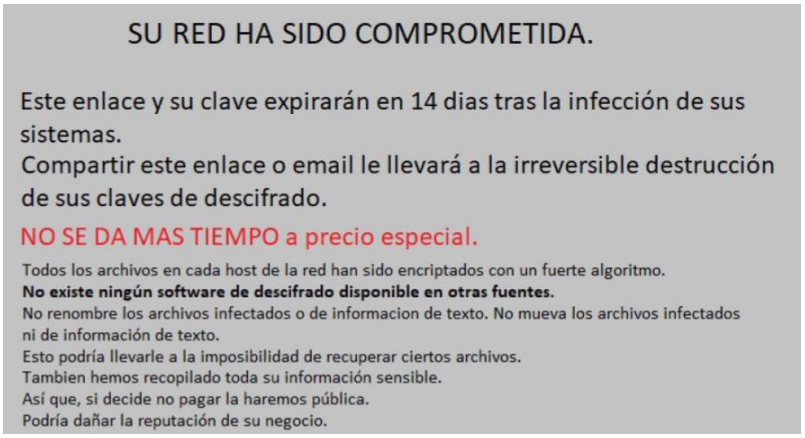


Figura 4-1. Ejemplo de un Ransomware de tipo doxware amenazando con filtrar datos privados.
Fuente. Ransomware. Una guía de aproximación para el empresario. INCIBE.

En definitiva, el ransomware es un ciberataque con mucho éxito para los ciberdelincuentes que afecta a todo tipo de empresas. Este tipo de malware, cada vez más sofisticado y destructivo, evoluciona para evadir las detecciones por parte de aplicaciones especializadas; por ello, resulta crucial conocer los mecanismos de acción utilizados por este ciberataque, información que enlaza con el siguiente apartado de este TFM.

4.3. Métodos de infección de Ransomware

El ciberataque tipo ransomware se propaga por medio de archivos adjuntos en correos electrónicos o desde páginas webs poco fiables que se ocultan detrás de descargas de juegos, películas o aplicaciones no legítimas y no somos conscientes del ataque hasta que es demasiado tarde.

No resulta extraño observar, como ocurre en otros tipos de malware, que los ciberdelincuentes utilicen una o varias de las siguientes formas para infectar a la víctima [38]:

4.3.1. Agujeros de seguridad en el software

Aprovechan los agujeros de seguridad o vulnerabilidades tanto en el software de los equipos como en sus sistemas operativos y sus aplicaciones para realizar sus ciberataques. Los desarrolladores de malware tienen herramientas que les permiten reconocer dónde están estos agujeros de seguridad e introducir así el malware en los equipos. Estas son algunas de las formas más frecuentes:

- Uso de servidores web desactualizados como vía de acceso para instalar el ransomware.
- Aprovechamiento de sistemas industriales conectados a Internet sin las medidas básicas de seguridad: equipos de control de climatización, fabricación de componentes … que no estaban conectados a ninguna red informática, y ahora son conectados a redes corporativas o Internet sin las mínimas medidas de seguridad.

4.3.2. Credenciales de acceso

Su objetivo es conseguir credenciales de acceso a los equipos con privilegios de administrador mediante engaños (phishing), debilidades de procedimiento (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 (incrustarlas 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 conectados a Internet, conservan las mismas credenciales genéricas (de fábrica o por defecto) de acceso y administración, están «hardcodeados» o carecen de ellas.

4.3.3. Envío de correos spam

El envío de correos spam se lleva a cabo 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 existe un porcentaje de receptores que cliquea o descarga el fichero.

4.3.4. Engaño a los usuarios

Consiste en engañar a los usuarios mediante publicidad maliciosa o malvertising inyectando malware en anuncios publicitarios de la Red. Este tipo de anuncios maliciosos, que informan de actualizaciones u otros avisos de seguridad, están hechos para incitar a la víctima a hacer clic en ellos. De hacerlo, estos descargan malware automáticamente en el dispositivo o redirigen al usuario a una página web maliciosa.

Aunque esta situación siempre es peligrosa, más aún cuando se trata de los dispositivos de empresa. La descarga de un malware puede llegar a comprometer la información confidencial del negocio, incluso llegando a exigir rescates económicos por ella [39].

4.3.5. Métodos como drive-by download y watering hole

El ciberdelincuente utiliza métodos como *drive-by download* y *watering hole,* enfocados a compañías, con altos niveles de seguridad, en las que los usuarios visitan frecuentemente sitios web de confianza relacionados con el contenido de la organización.

También utilizan técnicas de malvertising incrustando anuncios maliciosos en sitios web legítimos, previamente estudiados e infectados por los atacantes. Cuando el empleado de la compañía objetivo visite el sitio web infectado, infectará su equipo con malware y permitirá a los atacantes tomar el control del equipo del empleado para poder espiar y robar información de la compañía [40].

4.3.6. Servicios expuestos a Internet

Acceder de forma remota a equipos de la empresa o clientes es una gran ventaja que aumenta la productividad y permite no estar físicamente delante del equipo. Sin embargo, el ciberdelincuente aprovecha los servicios expuestos a Internet para atacar; por ejemplo, el escritorio remoto.

El acceso remoto sigue el modelo lógico de cliente-servidor. El equipo al que queremos acceder hace de «servidor», y el resto de los dispositivos que se conecten a él son los «clientes». Cuando se habilita esta funcionalidad se «abre» en el servidor un puerto, que suele ser el número 3389. Los puertos pueden entenderse como las vías de entrada y salida de información a Internet.

Si una comunicación no se realiza en el puerto correcto, será denegada. Además, habrá que configurar el router que da al servidor acceso a Internet, para que acepte las conexiones al escritorio remoto desde fuera de la red interna. Esto último no será necesario si utilizamos una solución VPN para cifrar las comunicaciones entre los equipos cliente y servidor. Por eso, todos los servicios expuestos a internet deben contar con las medidas de seguridad necesarias ya que son el origen de un incidente de seguridad, como puede ser una infección por ransomware [41].

Antes de finalizar con este apartado, insistir una vez más en cómo algunos ransomware vienen asociados a otros tipos de *malware* que roban información (cuentas de bancos, credenciales de acceso…), abren puertas traseras (backdoors) o instalan botnets. Con los avances en la complejidad de los algoritmos de cifrado, el ransomware mejora su mecanismo de extorsión. Mientras que en un principio, solo utilizaban programas que bloqueaban el sistema; actualmente, pueden cifrar la información de los discos duros y otros sistemas de almacenamiento de sus víctimas, haciendo más difícil su recuperación y aumentar el valor del rescate [38].

Por todo ello, resulta imprescindible señalar algunas de las medidas de seguridad, información que enlaza con el siguiente apartado.

4.4. Medidas de seguridad ante Ransomware

Los ataques de ingeniería social son muy similares a los tradicionales timos conocidos. El ciberdelincuente reúne toda la información posible sobre la empresa que va a atacar para conocer a

su víctima, selecciona a dicha víctima utilizando la información obtenida hasta que consigue su confianza y le pueda manipular para conseguir su objetivo: instalar un programa, enviar algunos correos... Una vez logrado, el ciberdelincuente se retirará para no levantar sospechas.

Antes de profundizar en las medidas de seguridad, vamos a mostrar algunas de las **medidas básicas** para evitar ser víctima de ransomware (Tabla 4-1) [42].

MEDIDAS BÁSICAS PARA EVITAR SER VÍCTIMA DE RANSOMWARE
- Configurar el correo electrónico con filtros antispam y autenticación de correos entrantes. - Revisar los enlaces antes cliquear y desconfiar de los ficheros adjuntos, aunque sean de contactos conocidos. - No contestar, ni abrir correos de usuarios desconocidos y eliminarlos directamente. - Instalar, únicamente, aplicaciones permitidas para el trabajo que provengan de fuentes oficiales. - Hacer copias de seguridad periódicas y comprueba que es posible restaurarlas. - Actualizar tus sistemas de manera automatizada y centralizada. - Proteger la seguridad del wifi. - Utilizar el criterio de «mínimos privilegios» en los mecanismos de control de acceso. - Diseñar tu red y los servicios que ofrezcas para seguir los principios de «mínima exposición» con herramientas de control perimetral, como cortafuegos y detectores de intrusiones. - Desactivar las opciones Autorun y Autoplay en las unidades externas (CD, USB,..) - Poner en marcha un «plan de contingencia y de respuesta ante incidentes» para estar preparado en caso de que ocurra. - Auditar, revisar los logs de los sistemas y escanear con frecuencia.

Tabla 4-1. Medidas básicas para evitar ser víctima de Ransomware.
Fuente: Elaboración propia a partir de Ransomware. Una guía de aproximación para el empresario. INCIBE, 2020
Obtenido de https://www.incibe.es/protege-tu-empresa/herramientas/servicio-antiransomware

Analizando en mayor profundidad este apartado, podemos encontrar **dos tipos de medidas de seguridad** para el protegernos o reducir los riesgos asociados al ransomware:

- **Medidas de seguridad preventivas o activas.** Su objetivo es proteger y evitar posibles daños en los sistemas informáticos. Dichas medidas no son efectivas por sí solas, sino que hay que aplicarlas en su conjunto como parte de una estrategia de seguridad [43].
- **Medidas de seguridad reactivas o pasivas.** Su finalidad es minimizar los efectos causados por la infección del ransomware.

4.4.1. Medidas de seguridad preventivas o activas.

1. Realizar copias de seguridad.

Esta es la **principal** medida que nos permitirá recuperar la actividad de nuestra empresa en **menos tiempo** y las recomendaciones básicas en cuanto a las copias de seguridad son:

- Cuando se sufre un ataque por ransomware hay tres opciones: pagar el rescate, recuperar la información desde una copia de seguridad o asumir que hemos perdido nuestros datos.

De las tres opciones, la mejor es recuperar los contenidos desde una copia de seguridad (backup); como estas también pueden fallar, se recomienda tener al menos tres copias de seguridad actualizadas en distintos soportes: disco duro específico para copias, USB externo y nube [38].

- Dado que algunas variantes de ransomware cifran la información de discos duros o sistemas de almacenamiento de red distintos al equipo infectado, lo mejor es almacenar la información en soportes externos no conectados a nuestra red.
- Dado que las copias de seguridad también pueden corromperse, es necesario un chequeo periódico de esa copia de respaldo y probar a restaurar algunos ficheros cada cierto tiempo.
- El periodo de conservación de las copias de seguridad dependerá tanto de las necesidades de cada organización como de los requerimientos legales a los que la empresa esté sujeta. A modo orientativo, INCIBE recomienda realizar [44]:
    a) Copias incrementales diarias.
    b) Copias totales una vez a la semana.
    c) Conservación de las copias totales un mes.
    d) Almacenamiento de la última copia del mes durante un año.
- En un mes se realizarían copias incrementales diariamente y 4 copias totales semanales. Cada copia total se conservará durante un mes y la última copia total de cada mes durante un año.

Finalmente, dado que el ransomware amenaza con el filtrado de tus datos, se debe cifrar la información más sensible para que, en caso de robo de los ficheros, los ciberdelincuentes no puedan hacer pública la información.

2. Navegar seguro utilizando redes privadas virtuales (VPN).

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 utiliza cuando estamos fuera de la empresa y queremos acceder a documentos que están en la intranet o en nuestro equipo corporativo. De esta forma, tendremos acceso a ellos y navegaremos seguros [43].

3. Concienciación y formación de los usuarios.

Aunque la formación para concienciar a los trabajadores es una de las medidas de seguridad en las que **menos se invierte y menos tiempo se dedica**, no debemos olvidar que es algo prioritario. Se recomienda llevar adelante un proceso de concienciación y formación de todos ellos para que comprendan los riesgos asociados al uso de recursos informáticos e Internet, y desarrollen hábitos y comportamientos que permitan realizar un uso responsable y seguro de los mismos [43].

Además, una de las mejores formas que existen para aprender a identificar técnicas de ingeniería social o a resolver un incidente de este tipo es entrenar a los empleados mediante juegos y simulaciones especialmente diseñadas para ello, sin riesgo de comprometer información confidencial. De hecho, algunas de estas iniciativas son las siguientes [45]:

- INCIBE ha diseñado un kit de concienciación como herramienta didáctica para concienciar y entrenar a los empleados en el uso seguro de la tecnología. Su objetivo es evitar los incidentes de ciberseguridad que afectan a las empresas para que su implantación puedan llevarla a cabo en todos los sectores, sin tener conocimientos previos [46].
- INCIBE ha desarrollado un *"Juego de rol. ¿Estás preparado para ser atacado?"* para pymes en el que se plantean cinco escenarios que pueden afectar a cualquier empresa. El primero es "*¡Infección por ransomware!"*, donde los participantes podrán entrenarse de este tipo de situación para que, en caso de materializarse, puedan responder más ágilmente [47].
- INCIBE ha creado un videojuego *"Hackend, se acabó el juego"* de carácter formativo donde confluyen diferentes amenazas y cuyo objetivo es saber cómo gestionarlas [48].
- Para sectores empresariales con ciertas particularidades: industria, comercio, ocio, … INCIBE lanza una formación básica que comienza por el itinerario interactivo que más se adapte a su sector. Los itinerarios consisten en videos cortos interactivos presentados por dos personajes preocupados por la ciberseguridad, donde nos mostrarán las distintas situaciones cotidianas que pueden afectar a la organización y las acciones que puedes implementar para protegerla [49].
- CSIRT-CV (Computer Security Incident Response Team – Comunidad Valenciana) unidos a la iniciativa de ENISA (Agencia Europea de la Ciberseguridad) pretende concienciar y dotar a las empresas de herramientas y servicios que ayuden a incrementar su nivel de ciberseguridad. El mes de octubre de cada año, se celebra el Mes Europeo de la Ciberseguridad y este pasado año 2022, por poner un ejemplo, estuvo centrado en combatir el phishing y el ransomware [50].

4. Mantener actualizados el sistema operativo y las aplicaciones.

Se deben **mantener actualizados** los navegadores web, sistemas operativos en sus últimas versiones y todos los programas para reducir la posibilidad de ser infectado por ransomware, asegurando que tengan habilitada la instalación de actualizaciones de forma automática. Los ciberdelincuentes se aprovechan de los bugs y falta de las actualizaciones en el sistema operativo y en aplicaciones tradicionales como navegadores (Internet Explorer, Edge, Firefox, Chrome y Safari), Java y Adobe Reader, entre otros.

Para usuarios avanzados podría ser posible filtrar Javascript, Java y otros plugins el navegador a través de la extensión NoScript (para Firefox) y ScriptSafe (Chrome) [43].

5. Configuración del correo.

Como ya se ha indicado anteriormente en el apartado 3.4 del presente proyecto, el correo electrónico es considerado como una de las principales vías de entrada de ciberataques. Insistir, de nuevo, en que mediante correos fraudulentos que puedan contener adjuntos con malware o enlaces maliciosos, los ciberdelincuentes intentarán robarnos las contraseñas de acceso y engañarnos para que instalemos malware o visitemos páginas donde infectarnos.

Por ello, los servidores de correo electrónico deben:

- Contar con filtros activado y configurados de spam evitando que lleguen al buzón de los empleados.
- Evitar el email *spoofing* o suplantación de correo electrónico utilizando autenticación de correos entrantes.
- Escanear los correos entrantes y salientes con un antivirus actualizado para detectar amenazas y filtrar ficheros maliciosos, fijándose en las extensiones de los archivos recibidos y su coherencia con el nombre.
- Deshabilitar las macros o un previsualizador de documentos, 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.
- Utilizar entornos virtuales para abrir los archivos sospechosos [38].

6. Aplicar un modelo de mínimos privilegios o LUA.

Se debe impedir que los empleados instalen aplicaciones no permitidas y usar filtros para controlar el tráfico de navegación en la empresa, autorizando las páginas estrictamente indispensables. Para ello, la mejor recomendación sería tener **dos cuentas configuradas**:

Cuenta de Administrador con privilegios de administrador para poder gestionar el sistema y la instalación del software, con la precaución de renombrar la cuenta bajo un seudónimo para no revelar su identidad.

Cuando un usuario o administrador inicia una sesión con derechos administrativos, todos los programas ejecutados, exploradores y clientes de correo, también disponen de esos derechos. En caso de que dicho software active algún tipo de malware, puede instalarse sin enterarnos [51].

Cuenta de Usuario o Usuarios con privilegios mínimos y limitados con el acceso a la manipulación de la configuración del equipo y su software totalmente restringido.

Si un ransomware se ejecuta con esta cuenta se limita su rango de actuación y no podrá desconectar las herramientas de seguridad del equipo. Muchos ransomware, como SamSam, utilizan técnicas de explotación de vulnerabilidades en el sistema para obtener privilegios de administración y poder actuar. Por lo tanto, para disminuir el riesgo de una infección por ransomware, cada usuario debe acceder sólo a la información y recursos necesarios [51].

7. Mostrar las extensiones de los archivos.

Dado que el sistema operativo Windows oculta las extensiones para tipos de archivos conocidos (.EXE, .TXT, .SCR, etc.), es recomendable **activar** la visualización de la extensión de los archivos y, así, será más fácil detectar archivos maliciosos con doble extensión.

Se debe evitar esta confusión ya que un método tradicional de propagación de malware utiliza extensiones dobles para engañar al usuario. Por ejemplo, si el archivo se llama file.pdf.exe o archivo.docx.scr, Windows mostrará file.pdf o archivo.docx [43].

Filtrar archivos con extensiones peligrosas.

Además, las organizaciones que tengan la administración de su servidor de correo deben filtrar archivos adjuntos con extensiones peligrosas (ejecutables y scripts) a través de listas negras. Dependiendo del tamaño de la organización, se pueden implementar listas blancas, aunque a mayor tamaño, mayor complejidad [43].

Para empezar, se deberían bloquear al menos los tipos de archivos mostrados en la Tabla 4-2:

TIPOS DE ARCHIVOS A BLOQUEAR		
BAT	CMD	COM
CPL	DLL	EXE
JAR	JS / JSE	LNK
MSI	PIF	PS1
SCR	VBE / VBS	ZIP / RAR / 7z (y otros comprimidos)

Tabla 4-2. Tipos de archivos a bloquear.

Fuente: Cristian Borghello, Marcelo Temperini, Mauro Gioino, Nicolás Gustavo, Bruna Matías Sequeira, Maximiliano Macedo & Walter Heffel (2018, septiembre). Guía para evitar infecciones de RANSOMWARE. Versión 1.1. Obtenido de https://owasp.org/www-pdf-archive/Owasp-guia-evitar-Ransomware_es.pdf

8. Mínima exposición de la red interna al exterior: segmentar la red.

Evitar exponer al exterior la red interna de la empresa ya que un cortafuegos o firewall, en ocasiones, no tiene acceso desde el exterior de la red. Para evitar esta posible brecha de seguridad existe una configuración denominada **zona desmilitarizada** o **DMZ** (Figura 4-2). Esta red DMZ (Demilitarized Zone) deberá estar especialmente controlada y monitorizada, siendo recomendable instalar detectores de intrusos y tener mucho cuidado a la hora de proteger y configurar sus servidores [52].

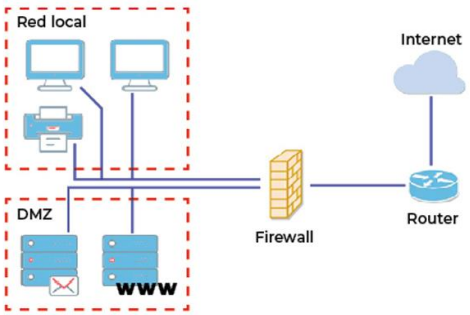


Figura 4-2. Esquema DMZ y cómo protege la red interna frente a ataques externos.

Fuente: DMZ: qué es, para qué sirve y cómo configurarlo. (2021, junio). Obtenido a partir de https://www.redusers.com/noticias/publicaciones/dmz/

La **segmentación de la red** a través de VLAN (Red de Área Local Virtual) y ACL (Lista de Control de Acceso), permite controlar el tráfico entre redes de distinta relevancia (por ejemplo, la LAN de usuarios y la LAN de los servidores) [53].

Para ello, la red se dividirá en subredes aumentando el número de ordenadores conectados a ella (Figura 4-3) y, a su vez, aumentará el rendimiento, teniendo en cuenta que existe una única topología, un mismo protocolo de comunicación y un solo entorno de trabajo.

Realizar una segmentación de red o *subnetting* evita exponer los servicios internos al exterior o que toda se infecte toda la red, aunque no evita que un ataque de ransomware acceda a los sistemas.

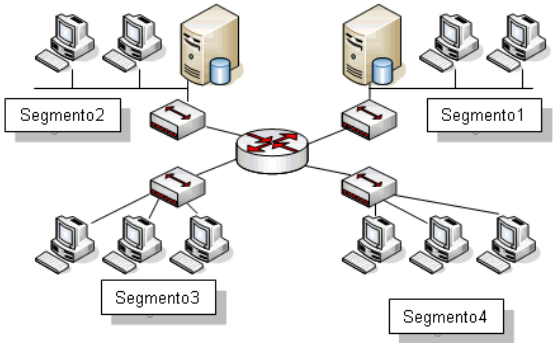


Figura 4-3. Segmentación de la red.

Fuente: Segmentación y Direccionamiento IP. Obtenido a partir de https://www.winex.com.py/2017/03/05/segmentacion-y-direccionamiento-ip/

9. Utilizar soluciones antivirus e instalar herramientas de terceros.

Se recomienda utilizar, al menos, **dos antivirus**: uno en dispositivos ubicados en el perímetro de la red (firewall y correo corporativo) y otro para los clientes internos y estaciones de trabajo. Aunque ningún antivirus es infalible, tener dos o más productos en distintos niveles de la organización multiplica la posibilidad de detección. La mayoría de los antivirus actuales permiten analizar el interior de archivos comprimidos en busca de malware. Estos archivos serán analizados siempre que no tengan contraseña. En el caso de Windows 10 (ediciones posteriores a 2018), se puede utilizar la protección de carpetas específica contra ransomware (Figura 4-4), configurando esta opción dentro del Centro de Seguridad de Windows Defender [54].

Figura 4-4. Centro de seguridad de Windows Defender.

Fuente: Monrás, Alex (S. D.) Habilitar Acceso Controlado a Carpetas en Windows 10. Obtenido de https://dominiogeek.com/acceso-controlado-carpetas-windows-10/

Para evitar el pago de licencias adicionales, se puede utilizar un producto de pago y uno gratuito Open Source. Debido a la constante actividad del malware, los antivirus suelen tardar un promedio de 48 horas en reaccionar ante un nuevo tipo de amenaza.

Además, conviene conocer que las **herramientas anti-ransomware** (Tabla 4-3) son una medida adicional que funcionan junto con las soluciones antivirus. Sus proveedores son empresas de seguridad especializadas en antivirus que surgen como vacuna de variantes de ransomware [43].

HERRAMIENTAS ANTI-RANSOMWARE	
AntiRansom	Aplicación de seguridad desarrollada especialmente por Security by Default para detectar este tipo de malware en Windows.
CryptoPrevent	Aplicación de seguridad para Windows diseñada originalmente por d7xTech para prevenir la infección de CryptoLocker que surgió a fines de 2013.
BDAntiransomware	"Vacuna" lanzada por BitDefender para brindar protección contra versiones de las familias CTB-Locker, Locky y TeslaCrypt.
Latch Antiransomware Tool	Herramienta publicada por Eleven Paths que añade una capa de autorización sobre carpetas "protegidas", de forma que deniega cualquier tipo de operación de escritura o borrado de los archivos.
Kaspersy NoRansom	Conjunto de herramientas para descifrar varios tipos de Ransomware.
Avast	Ha publicado Ransomware Decryption Tools.
MalwareHunterTeam	Ha desarrollado la herramienta ID-Ransomware que identifica varios tipos de malware.
PowerShell y Bash	Detecta la modificación de ciertos archivos señuelos en Windows y Linux.
NoMoreRansom	Ha publicado una lista que permite buscar el tipo de Ransomware que ha infectado un sistema y comprobar si existe una solución de descifrado disponible.

Tabla 4-3. Herramientas anti-ransomware.

Fuente: Cristian Borghello, Marcelo Temperini, Mauro Gioino, Nicolás Gustavo, Bruna Matías Sequeira, Maximiliano Macedo & Walter Heffel (2018, septiembre). Guía para evitar infecciones de RANSOMWARE. Versión 1.1. Obtenido dehttps://owasp.org/www-pdf-archive/Owasp-guia-evitar-Ransomware_es.pdf

10. Deshabilitar algunos recursos o funciones [43].

Deshabilitar el escritorio remoto. En aplicaciones de escritorio remoto como RDP (nativo de Windows), VNC o TeamViewer, es común aprovechar las vulnerabilidades o el uso de débiles contraseñas. Por ello, estas aplicaciones deben ser deshabilitadas y, de requerirse un acceso remoto, se recomienda la implementación de una VPN, cuya configuración se limite sólo a los equipos necesarios dentro de la red corporativa.

En el marco de un modelo de defensa en profundidad, se propone fortalecer (proceso de hardening) las conexiones RDP con el cifrado de las comunicaciones a través de certificados digitales basados en PKI (X.509), preferentemente emitidos por una entidad certificante (CA) externa de confianza (Symantec, Comodo, Goddady, etc). Otra posibilidad es usar Remote Desktop Web Client o Remoto Desktop Service (RDS).

Además, se recomienda aplicar los siguientes controles sobre las conexiones de escritorio remoto:

- Establecer una contraseña robusta.
- Habilitar el doble factor de autenticación (2FA).
- Utilizar las últimas versiones disponibles con todas las actualizaciones y parches.

Desactivar las macros y ActiveX. Una de las técnicas de propagación utilizada por el ransomware es el envío de documentos adjuntos maliciosos de ofimática (DOCX, XLSX, ODT, etc.) a través de correos electrónicos. Estos documentos contienen macros que son ejecutadas automáticamente al abrir el documento. Después, la macro descarga y ejecuta un archivo EXE que infecta el sistema. Así que, nunca se debe abrir un archivo de ofimática que haya sido recibido por correo electrónico si resulta sospechoso o su remitente es desconocido y, si se abre, nunca permitir la ejecución de macros.

Por su parte, los ActiveX permiten realizar distintos tipos de acciones sobre el sistema operativo, lo cual también podría ser utilizado para infectarlo. Se recomienda desactivar las macros y ActiveX a través de una política de grupo (GPO) o manualmente en la herramienta ofimática utilizada.

Deshabilitar servicios de scripting y consolas. Existen campañas de spam que contienen archivos adjuntos comprimidos como ZIP y RAR con archivos VBS (VisualBasicScript) o JS (JavaScript). Si el usuario ejecuta el script adjunto, posteriormente se descarga y ejecuta el malware (.EXE) que suele ser un ransomware.

Por defecto, los sistemas operativos Windows abren archivos de scripts con la aplicación Windows Based Script Host (WSH). Por tanto, se recomienda deshabilitar el servicio a través de una GPO o localmente, así como deshabilitar o desinstalar Windows Power Shell y CMD ya que la mayoría de los usuarios que no sean administradores no requieren estas herramientas.

Cuando no sea posible deshabilitar dichos servicios, se recomienda configurar la apertura de los archivos de scripts con un editor de texto.

Desactivar Autorun/Autoplay. Desde 2006 con el lanzamiento de Windows Vista, el servicio de "Autorun/Autoplay" en medios de almacenamiento externos, como USB y CD, se encuentra desactivado por defecto.

En algunas ocasiones, el malware se propaga a través de dispositivos USB, por lo que dicha función debe ser desactivada de forma tal que el archivo autorun no se ejecute automáticamente cuando se inserta un dispositivo externo.

Deshabilitar o eliminar protocolos obsoletos. Cualquier software sin soporte del fabricante o próximo a expirar se considera "obsoleto" y debería ser reemplazado por versiones actualizadas para solucionar vulnerabilidades de seguridad o directamente retirados. La implementación del protocolo SMBv1 en Windows es un claro ejemplo ya que está considerado como uno de los vectores de infección utilizados por el ransomware Wannacry.

11. Revisar recursos compartidos y unidades externas [43].

Realizar **revisiones** de recursos compartidos (unidades de disco, impresoras, carpetas, etc.) y unidades externas (pendrives, tarjetas de memoria, discos rígidos, etc.) conectadas a los equipos, para ver si es necesario que permanezcan compartidos o no y, de ser necesario, establecer los permisos mínimos para un uso correcto. Si se detectaran dispositivos que no sean utilizados, deberán

ser desconectados, de forma que, si se produce una infección, se evite la propagación del malware por la red de la organización, minimizando el impacto en otros equipos.

12. Deshabilitar ejecución de archivos temporales [43].

En Windows, al evitar el uso de permisos administrativos, los archivos descargados por el usuario se almacenan en carpetas locales y temporales de su perfil (Tabla 4-4):

CARPETAS LOCALES y TEMPORALES			
%AppData%\	%LocalAppData%\	%ProgramData%\	%LocalAppData%\Temp\
%Temp%\	%userprofile%\	%WinDir%\temp\	%WinDir%\SysWow\

Tabla 4-4. Carpetas locales y temporales.

Fuente. Elaboración propia a partir de Cristian Borghello, Marcelo Temperini, Mauro Gioino, Nicolás Gustavo, Bruna Matías Sequeira, Maximiliano Macedo & Walter Heffel (2018, septiembre). Guía para evitar infecciones de RANSOMWARE. Versión 1.1. Obtenido de https://owasp.org/www-pdf-archive/Owasp-guia-evitar-Ransomware_es.pdf

Dado que el malware suele ejecutarse en alguno de estos directorios, se deben bloquear los permisos de ejecución sobre ellos para que los archivos dañinos no se puedan ejecutar. Para bloquear el acceso a estos directorios, se pueden utilizar las directivas de restricción de software local o las GPO de Directorio Activo (”secpol.msc”).

Algunos ejemplos para bloquear serían los mostrados en la Tabla 4-4:

LISTA DE EJEMPLOS A BLOQUEAR	
%AppData%*.exe	%AppData%**.exe
%LocalAppData%*.exe	%LocalAppData%**.exe
%LocalAppData%\Temp*.zip*.exe	%LocalAppData%\Temp\7z**.exe
%LocalAppData%\Temp\Rar**.exe	%LocalAppData%\Temp\wz**.exe
%ProgramData%*. exe	%Temp%*.exe
%Temp%**.exe	%userprofile%*.exe
%WinDir%\temp*.exe	%WinDir%\SysWow*.exe

Tabla 4-5. Lista de ejemplos a bloquear.

Fuente. Elaboración propia a partir de Cristian Borghello, Marcelo Temperini, Mauro Gioino, Nicolás Gustavo, Bruna Matías Sequeira, Maximiliano Macedo & Walter Heffel (2018, septiembre). Guía para evitar infecciones de RANSOMWARE. Versión 1.1. Obtenido de https://owasp.org/www-pdf-archive/Owasp-guia-evitar-Ransomware_es.pdf

La Figura 4-5 muestra una regla de configuración local donde se restringe la ejecución de archivos .exe en el directorio %AppData%\.

Los usuarios de Linux deberían tener idénticas consideraciones en el directorio “/tmp” y con el perfil propio del usuario (“~/”). En el caso de Mac OS, además se debería proteger “~/Library/”, este sistema operativo almacena los archivos de configuración de las aplicaciones instaladas.

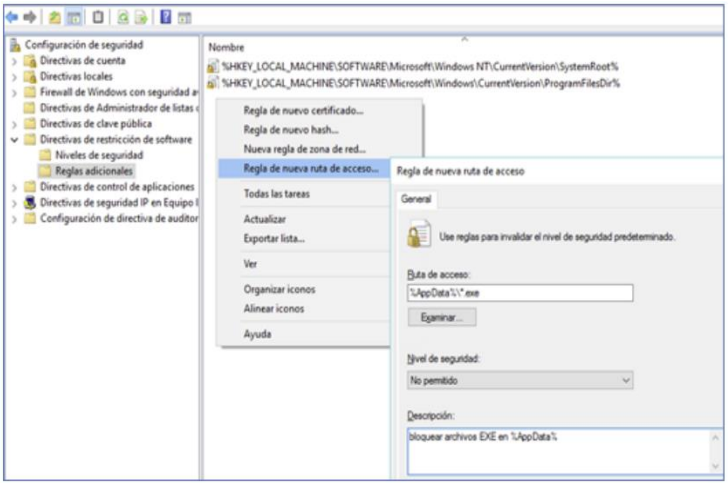


Figura 4-5. Configuración de seguridad.

Fuente: Cristian Borghello, Marcelo Temperini, Mauro Gioino, Nicolás Gustavo, Bruna Matías Sequeira, Maximiliano Macedo & Walter Heffel (2018, septiembre). Guía para evitar infecciones de RANSOMWARE. Versión 1.1. Obtenido de https://owasp.org/www-pdf-archive/Owasp-guia-evitar-Ransomware_es.pdf

13. Utilizar antispam, firewall y filtro de contenido [43].

Su objetivo es proteger la infraestructura y evitar que la amenaza llegue a los usuarios.

Filtrado a nivel de firewall. El ransomware debe comunicarse con un centro de Comando y Control (C&C) a través de Internet para enviar las contraseñas de cifrado y recibir instrucciones. El uso de firewall es fundamental en el bloqueo de este canal de comunicación entre el malware y su C&C. Los firewalls actuales permiten configurar listas blancas y negras de sitios webs y aplicaciones que se conectan a Internet.

Los firewalls tipo appliance permiten configurar opciones de tráfico de red, listas blancas y negras de sitios webs y aplicaciones que se conectan a Internet. A través de los filtros de contenido y las listas negras se pueden bloquear los sitios utilizados para propagar el malware y los archivos ejecutables del ransomware, que intentan conectarse al C&C. Con las listas blancas se puede permitir sólo dominios utilizados para las actualizaciones del software y del sistema operativo.

Filtrado web (proxy). Se debe bloquear la conexión a sitios web:

- Según su geolocalización: el tráfico proveniente de Asia y países de Europa del Este.
- Según su dominio de nivel superior. En Spamhaus se encuentra un listado de dominios sospechosos por naturaleza.
- Según su contenido del sitio: spam, phishing, evasión de proxy, pornografía, y otras categorías de sitios web innecesarios para las operaciones normales de la organización.

Filtrado de nodos TOR. Si se dispone de un Proxy, Firewall o cualquier otro sistema de seguridad perimetral, será posible añadir reglas para bloquear accesos hacia nodos de la red TOR. Para facilitar el bloqueo, existe una lista de nodos dependiendo de su IP pública. Se puede agregar una lista de direcciones, que se actualiza cada 30 minutos y permite identificar nodos TOR.

Si se administra un servidor web, se puede efectuar este mismo tipo de restricción mediante los archivos de configuración propios del webserver.

Filtrado de correos. Los módulos que se deben configurar en los servidores o gateway de correo son:

- Antispam, para filtrar o bloquear cualquier tipo de correo basura.
- Filtrado del contenido, para analizar y bloquear malware o archivos ejecutables, analizar archivos comprimidos, bloquear URLs maliciosas…

El servicio antispam debe configurarse para bloquear cualquier tipo de archivo ejecutable o comprimido. Existen soluciones gratuitas y de pago e incluso algunos productos antivirus ofrecen la posibilidad de incorporar estos filtros a su solución tradicional de detección. Dos soluciones antispam Open Source son Radical Spam y Mail Cleaner.

14. Restaurar el sistema [43].

La funcionalidad "Restaurar sistema" de los sistemas operativos Windows permite **recuperar** el sistema operativo a un estado anterior a un incidente. Se debe tener en cuenta que el ransomware también utiliza este servicio para eliminar las copias de seguridad; por tanto, será útil sólo en el caso que el malware no las haya eliminado. De todas formas, la mejor recomendación es tenerlo habilitado y, así, aumentar las probabilidades de recuperar el sistema afectado.

15. Bloquear publicidad y ventanas emergentes [43].

Con frecuencia se encuentra malware incrustado en publicidades de sitios web o malvertising y solo visitando un sitio de este tipo, se puede infectar el sistema de la víctima de forma automática.

Para protegerse se debe **instalar** un complemento en el navegador que bloquee las ventanas emergentes y la publicidad. Dos bloqueadores efectivos, AdBlock y AdBlock Plus, pueden complementarse configurando en el navegador el bloqueo de las ventanas emergentes.

16. Apagar conexiones inalámbricas [43].

En los dispositivos móviles (teléfonos, tablets y notebooks) se debe deshabilitar el uso de redes inalámbricas (bluetooth, infrarrojo y Wi-Fi) porque disminuye el riesgo de propagación de malware a través de dispositivos conectados automáticamente y sobre los que no existe ningún control.

Aislar el equipo. Si se sospecha haber ejecutado un ransomware, debemos desconectar la red y apagar el equipo. Aunque no es una solución, siempre es preferible tener solo algunos archivos cifrados y no todos. Sin embargo, se debe prestar especial atención a este procedimiento porque algunas de sus variantes eliminan de manera parcial los archivos después de cada reinicio.

17. Proteger el MBR (Master Boot Record) [43].

Consiste en código ejecutable almacenado en el primer sector (sector 0) de un disco duro, que inicia el arranque (Boot Loader) del sistema operativo. El MBR contiene información sobre las particiones del disco y su sistema de archivo. Dado que el MBR se ejecuta antes que el propio sistema operativo, también puede ser manipulado por un ransomware para ganar persistencia en el equipo.

Por citar un ejemplo, HDDCryptor, Petya y Satana explotan esta vulnerabilidad. Para prevenir la modificación del sector 0 de todos los dispositivos conectados a un sistema, se puede utilizar la **herramienta MBRFilter**, la cual brinda una protección a nivel del sistema operativo.

18. Realizar auditorías [38].

Debemos 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. Actualmente, esta tarea está simplificándose debido a su automatización, aunque sigue siendo necesario que las realice personal especializado de la empresa o un servicio externo. Cuando solicitamos una auditoría para prevención del ransomware los aspectos y distintos **tipos de pruebas** para considerar deben ser los mostrados en la Tabla 4-6:

AUDITORÍA PARA PREVENCIÓN DEL RANSOMWARE	
Aspectos	**Tipos de pruebas**
Protección antivirus, antispam y de filtrado de contenidos.	**Test de penetración:** conjunto de pruebas a las que se somete a una aplicación, servicio o sistema para encontrar huecos o fallos a través de los cuales sería posible conseguir acceso no autorizado a información de la empresa. **Auditoría de red:** analizar la red de la empresa en busca de puertos abiertos, recursos compartidos, servicios o electrónica de red. También se emplean herramientas que permiten realizar la catalogación de las infraestructuras conectadas a la red, detectar versiones de dispositivos inseguros, versiones de software o la necesidad de instalar actualizaciones o parches. **Auditoría de seguridad perimetral:** proceso destinado a determinar el nivel de seguridad de las barreras que protegen la red de comunicaciones de una organización de los riesgos del exterior y del interior. Está más especializada que la anterior en detectar fallos de seguridad desde el punto de vista del exterior. **Auditoría web:** analiza las vulnerabilidades o los fallos de seguridad o 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.
Administración de permisos de usuarios y accesos a servicios.	
Seguridad de los dispositivos móviles.	
Gestión automatizada de actualizaciones y parches.	
Detección de vulnerabilidades.	
Monitorización del uso de los recursos informáticos y de red.	
Monitorización y análisis de eventos de seguridad en tiempo real (SIEM).	

Tabla 4-6. Auditoría para prevención del Ransomware.
Fuente: Elaboración propia a partir de Ransomware. Una guía de aproximación para el empresario. INCIBE, 2020

19. Plan de Actuación o Respuesta ante Incidentes [38].

Contar con un Plan de Actuación o Respuesta ante Incidentes, es decir, un conjunto ordenado de acciones enfocadas a prevenir la ocurrencia de los ciberincidentes y, en caso de que ocurran, restaurar los niveles de operación lo antes posible.

El proceso de gestión de incidentes consta de diferentes fases y, aunque todas son necesarias, algunas pueden estar incluidas como parte de otras o tratarse de manera simultánea. En la Figura 4-6 se muestran las **diferentes fases** de la gestión de ciberincidentes.

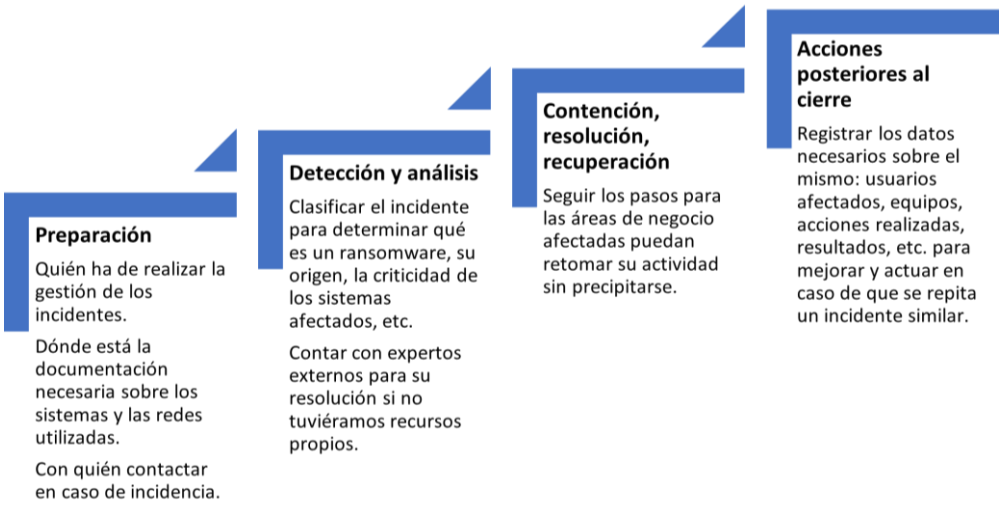


Figura 4-6. Fases de un plan de respuesta a incidentes.
Fuente. Elaboración propia a partir de Ransomware. Una guía de aproximación para el empresario. INCIBE. 2020

Para obtener una información más detallada sobre cada una de las fases que aparecen en este proceso de Gestión, véase el [Anexo IV. Gestión de Incidentes].

Antes de finalizar con este apartado, insistir en el uso responsable de la red, evitando cualquier ataque que pueda poner en peligro la propia integridad, el presente y el futuro de la organización. Por ello, las empresas deberían elaborar un **plan de ciberseguridad** que consiga evaluar los posibles riesgos, establecer objetivos, analizar las tecnologías disponibles para comprobar que sean seguras, seleccionar un marco de seguridad, revisar las políticas de seguridad, desarrollar el plan de gestión de riesgos, implementar el plan propiamente dicho y evaluar los resultados generados.

Como ya se ha visto en el apartado 3.5, un plan de ciberseguridad implica seleccionar e implementar acciones prácticas para proteger una empresa de amenazas externas e internas, por lo que los pasos generales a seguir para prevenir cualquier tipo de ciberataque son similares al anterior. Para obtener una información más detallada, véase el [Anexo III. Plan de Ciberseguridad].

4.4.2. Medidas de seguridad reactivas o pasivas.

Recordad, antes de entrar a fondo con este tipo de medidas y como se indicó al comienzo de este apartado 4.4, que el objetivo de las estas es minimizar los efectos causados por la infección del ransomware. Para ello, sus campos de actuación definidos son:

A. Procedimiento general.

En el momento en que se produce una infección por ransomware se comenzarán a cifrar los ficheros del equipo y los mapeados en las unidades conectadas, tanto dispositivos físicos como unidades de red. La mayoría de las veces, somos conscientes de la infección cuando el ransomware ha finalizado su ejecución y todos los ficheros se han cifrado. Sin embargo, existe la posibilidad de que no haya terminado su ejecución, permitiéndonos recuperar la clave de cifrado o evitar que más ficheros sean cifrados. Por ello, se deben seguir los siguientes pasos [55]:

1. **Desconectar las unidades de red**, esto supone "tirar del cable" de red (o desactivar las interfaces inalámbricas). Así, se podría llegar a evitar el cifrado de ficheros en unidades de red accesibles, en el caso de que el ransomware aún no hubiera finalizado su ejecución.

2. **Comprobar si el proceso dañino aún sigue ejecutándose.** El proceso dañino podría haberse inyectado en otro legítimo o haber finalizado su ejecución. Sin embargo, en caso de identificarse el proceso en cuestión (usando herramientas como Process Explorer de Sysinternals), desde el Administrador de Tareas de Windows (Taskmanager) se realizará un dump (volcado de la memoria) del proceso dañino. Para ello, hay que hacer clic derecho sobre el proceso y seleccionar la opción "Crear archivo de volcado" (se guardará en %TMP%). Una vez volcado, guardarlo en un sistema aislado (Figura 4-7).

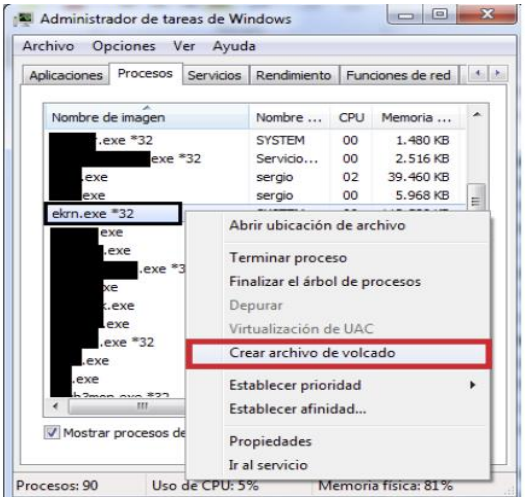


Figura 4-7. Realización de volcado de memoria de un proceso.

Fuente: CCN-CERT IA-11/18 Medidas de seguridad contra ransomware (2018, mayo). https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/2877-ccn-cert-ia-11-18-medidas-de-seguridad-contra-ransomware/file.html

3. **Finalizar la ejecución del proceso dañino.** Para ello existen dos alternativas:

- Si se ha identificado el proceso se debe parar su ejecución desde el Administrador de Tareas de Windows: clic derecho sobre el proceso y seleccionar la opción "Finalizar el árbol de procesos" (Figura 4-8) o "Finalizar tarea".

  Si no se ha podido identificar el proceso, se recomienda apagar el equipo de manera manual e inmediata.

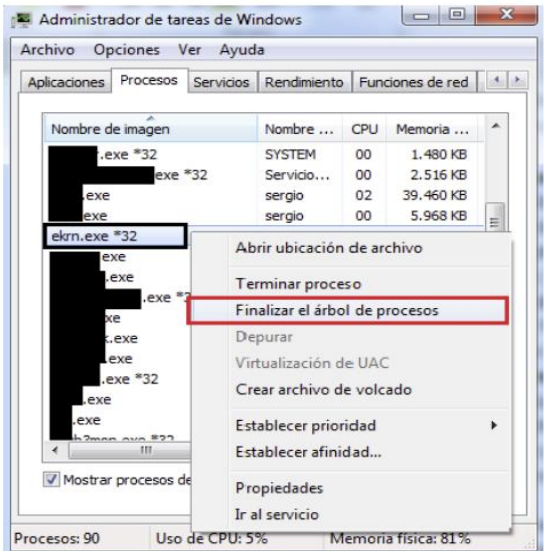


Figura 4-8. Finalización del proceso.

Fuente: CCN-CERT IA-11/18 Medidas de seguridad contra ransomware (2018, mayo). https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/2877-ccn-cert-ia-11-18-medidas-de-seguridad-contra-ransomware/file.html

4. **Arrancar el equipo en Modo Seguro.** Antes de que arranque Windows de manera convencional se pulsará la tecla F8 para acceder al menú de arranque avanzado, desde donde se seleccionará iniciar desde "Modo Seguro" (Figura 4-9). De este modo, evitaremos que el ransomware vuelva a arrancar de nuevo en caso de que fuera persistente.
5. **Realizar una copia de seguridad del equipo**. Esta copia tendrá todos los ficheros cifrados y no cifrados, y deberá realizarse en un dispositivo de almacenamiento externo aislado de la red. En caso de que no pudieran descifrarse los ficheros es importante conservarlos, ya que en un futuro puede que se rompa el cifrado o se liberen las claves del C&C.
6. **Comunicar el incidente de seguridad al equipo/persona competente** (CCN-CERT por ejemplo). La información que ha de adjuntarse en la incidencia está reflejada en el siguiente apartado B. Comunicación del Incidente.
7. **Valorar el escenario.** Para determinar si es posible recuperar los ficheros cifrados, se seguirán los pasos descritos en el apartado C. Valoración de Escenarios.

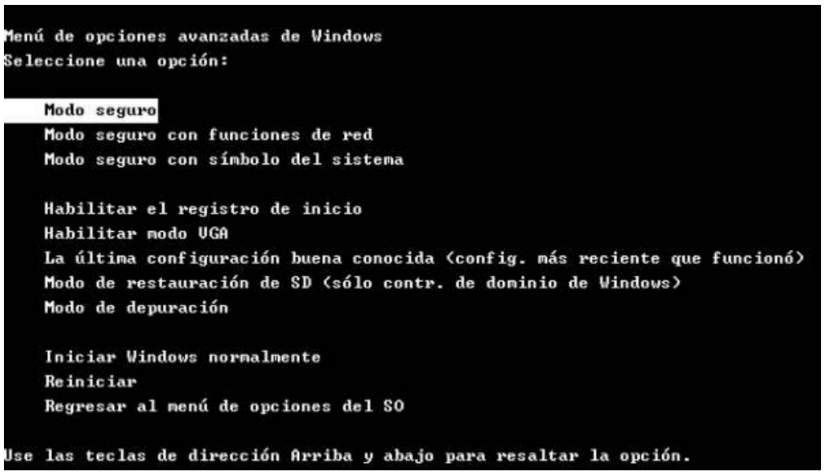


Figura 4-9. Inicio en modo seguro.

Fuente: CCN-CERT IA-11/18 Medidas de seguridad contra ransomware (2018, mayo). https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/2877-ccn-cert-ia-11-18-medidas-de-seguridad-contra-ransomware/file.html

B. Comunicación del incidente.

Después de una infección por ransomware, debemos de responder a preguntas que sirvan al equipo de seguridad a la hora de gestionar la incidencia [55]:

- ¿Disponen de copia de seguridad de los datos cifrados? En caso de disponer de un backup de los datos afectados por el ransomware se realizará una copia de seguridad de los ficheros cifrados (por si el proceso de restauración fallara). Después, se desinfectará el/los equipo/s afectado/s, y finalmente se restaurarán los datos originales.
- ¿Dónde se encuentra la infección? Determinar cuáles son los equipos afectados. En cada uno de ellos habrá que realizar las acciones descritas en el apartado A. Procedimiento general.
- ¿Se han cifrado las unidades de red (si las hubiera mapeadas)? Muchas veces, los activos más importantes se encuentran en unidades de red, por lo que se debe determinar si el ransomware ha accedido a los mismos. No obstante, tan pronto como se sea consciente de la infección, hay que “tirar del cable de red”.
- ¿Se han cifrado todos los formatos de ficheros? ¿Cuáles? La respuesta determinará la familia de ransomware.
- ¿Qué mensaje de rescate se muestra al usuario? Una vez finaliza su ejecución, el ransomware mostrará, o depositará en el equipo, las instrucciones para “rescatar” los ficheros cifrados.
- ¿Cómo se produjo la infección (adjunto en correo electrónico, etc.)? Conseguir la muestra del binario causante de la infección, permitirá al equipo de seguridad determinar qué ransomware ha producido la infección y si es posible la recuperación de los ficheros.

- ¿Han llevado a cabo alguna medida para desinfectar el/los equipo/s afectado/s? Si se ha realizado la copia de seguridad del equipo desde el modo seguro, se puede proceder a la desinfección del equipo. No obstante, se debe esperar la respuesta del equipo de seguridad, ya que se pueden recuperar las claves de cifrado utilizando el "Shadow Volume Copy".

Además, toda la información adicional que pueda ser considerada de interés habrá de adjuntarse en la incidencia (muestras de ficheros cifrados y originales con distintas extensiones y tamaños, volcado de memoria del ransomware, etc.).

C. Valoración de escenarios.

A la hora de intentar recuperar los ficheros cifrados, se pueden dar varios escenarios posibles; partiendo del más favorable al más desfavorable, estos son [48]:

ESCENARIO 1: Se dispone de backup completo del equipo afectado. En este escenario se procedería a desinfectar el equipo afectado para posteriormente restaurar la copia de seguridad.

ESCENARIO 2: Existe una herramienta que permite el descifrado. Sólo unas pocas variantes de ransomware son descifrables, bien porque se han obtenido todas las claves de cifrado tras la intervención del servidor C&C o porque existe una vulnerabilidad conocida en el código dañino que permite el descifrado de los ficheros.

ESCENARIO 3: Se dispone de Shadow Volume Copy. Bastaría con restaurar las copias de seguridad que realiza Windows automáticamente de los ficheros, utilizando Shadow Explorer. En muchos casos el ransomware imposibilitará esta acción.

ESCENARIO 4: Se pueden recuperar los ficheros utilizando software forense. En ocasiones algunos programas forenses son capaces de recuperar algunos ficheros originales borrados por el ransomware.

ESCENARIO 5: Conservar los ficheros cifrados a buen recaudo, ya que es posible que en el futuro puedan ser descifrados con una herramienta específica.

Concluyendo con este capítulo, recordad que el ransomware se manifiesta cuando el daño ya está hecho, es decir, cuando la información ha sido bloqueada. En ese instante, se nos muestra un mensaje que advierte de este hecho pidiendo un rescate para su liberación. Dicho mensaje suele incluir amenazas de destrucción total de la información si no se paga e insistir a realizar el pago de manera urgente. Por ello, se debe insistir que el pago del rescate para recuperar la información no es garantía de recuperar el acceso a la información secuestrada y, únicamente, se consigue reavivar este tipo de ataques. Por ello, es importante **no pagar** nunca el rescate [42].

Después de conocer los tipos o variantes más frecuentes de los dos ciberataques objeto de estudio, sus mecanismos o métodos de infección utilizados y sus medidas seguridad; en el próximo capítulo, se abordará la tendencia de los ciberataques actuales y de qué manera repercuten en el usuario y en la empresa tanto privada como pública.

---

5. Panorama actual

Las nuevas tecnologías abren excelentes oportunidades de crecer como sociedad, al mismo tiempo que generan mayor inseguridad. Por ello, la ciberseguridad es ahora más importante que nunca.

En relación con las principales tendencias de las amenazas relacionadas con la Cibercriminalidad, un organismo de referencia es EUROPOL. Dicho organismo, a través de sus informes anuales (Internet Organised Crime Threat Assessment - IOCTA), analiza cuales son. Las conclusiones extraídas del informe de 2021 son [58]:

- El **ransomware** se ha aprovechado de las vulnerabilidades del teletrabajo.
- El **aumento de mercado online** conlleva un incremento de las actividades intrusivas informáticas: phishing, robos de identidad, banca online, etc.
- La **creciente venta de productos médicos** falsificados, como consecuencia de la pandemia generada por la Covid-19.
- La **Covid-19** ha provocado un mayor acceso de la población infantil a contenidos en línea, con los riesgos que ello conlleva.
- El **comercio y la venta de datos privados**, al amparo de accesos ilegales informáticos, es un mercado floreciente.

Una vez vista la tendencia de los ciberataques actuales, vamos a analizar sus consecuencias y, posteriormente, conocer sus repercusiones tanto en el sector privado como público.

5.1. Consecuencias del ciberataque

Ante el éxito de un ciberataque, tanto el usuario como la empresa se ve notablemente **afectado**. Las fugas de información, el robo de identidad, los problemas con los dispositivos y el ciberdelito pueden tener un gran impacto. Además, su coste puede ir más allá de lo económico si sufre ciberacoso, donde se incluye hasta el acoso sexual.

La gravedad de las consecuencias puede variar según el **tiempo** que se emplee en recuperar la actividad, no es lo mismo recuperar la información en un par de días que en un período más largo. Cuanto más tiempo se tarde en continuar con la actividad, mayores serán las consecuencias en cuanto a las pérdidas económicas, en el daño en la reputación o imagen, en la productividad y en la responsibilidad penal o civil.

Las empresas afectadas por cualquier tipo de ciberataque no solo tienen pérdidas económicas, sino que también sufren el impacto de **forma indirecta**. En caso de fuga de datos confidenciales, no sólo se ve seriamente dañada su reputación, sino también la confianza que trasmite a sus clientes. El ser víctima de un ciberataque proyecta una imagen de vulnerabilidad y baja solvencia tecnológica. El riesgo reputacional cada vez preocupa más a las empresas, siendo de los más difíciles de gestionar ya que por su naturaleza cambiante y subjetiva requiere de una monitorización constante.

Los riesgos y daños son cada vez más **devastadores** y exigen agilidad empresarial para sobrevivir. Lo que complica la gestión de riesgos es que, hasta ahora, casi podían gestionarse individualmente; sin embargo, actualmente los riesgos son más numerosos, menos previsibles e interactúan entre ellos generando un sinfín de nuevos escenarios e implicaciones, como se muestra en el ejemplo del efecto cascada (Figura 5-1) que puede generar una brecha de seguridad [57].

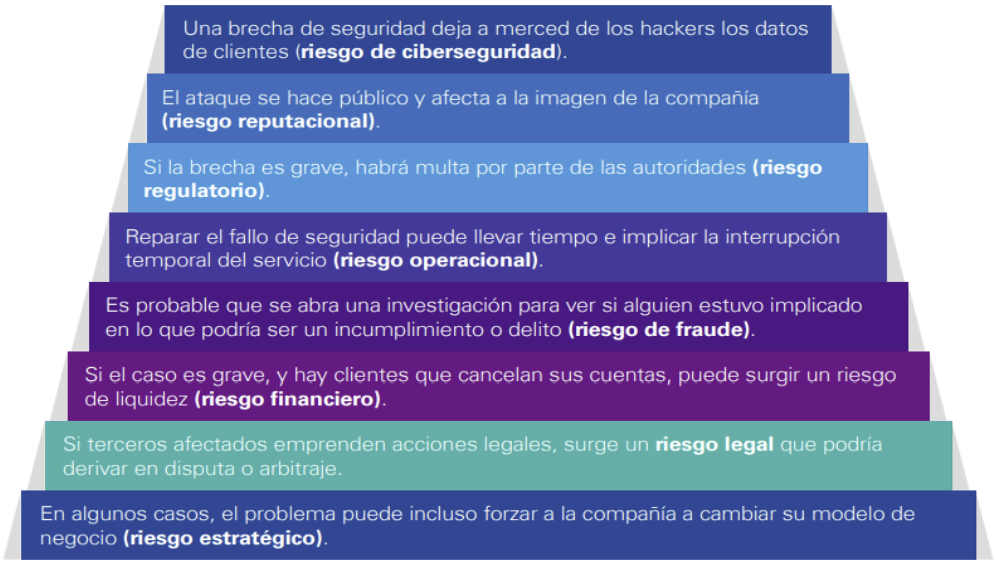


Figura 5-1. Efecto cascada de un ciberincidente.

Fuente: Vientos de Camino (2019, febrero). Obtenido de https://www.tendencias.kpmg.es/wp-content/uploads/2019/04/Informe_Riesgos_Abril2019.pdf

5.1.1. Sector privado

Las repercusiones de los ciberincidentes en el sector privado son más que notables. Sin embargo, hay que tener en cuenta que conocer con exactitud las pérdidas en este sector resultaba muy difícil hasta 2016, ya que la empresa privada no estaba obligada a hacer públicos estos datos y, de hecho, no lo hacía para que no se viera afectada su **reputación o confianza** hacía sus clientes.

Sólo en 2018, el número de afectados por WannaCry (apartado 4.2.1) fue de más de 1.000 millones en todo el planeta y ocasionó pérdidas aproximadas de 4.000 millones de dólares.

En España, la empresa más afectada fue Telefónica (Figura 5-2) además de centrales energéticas, aeropuertos e importantes compañías relacionadas con el transporte público y las comunicaciones, cuyos nombres se mantienen en secreto para no favorecer la aparición de nuevos ciberataques [56].

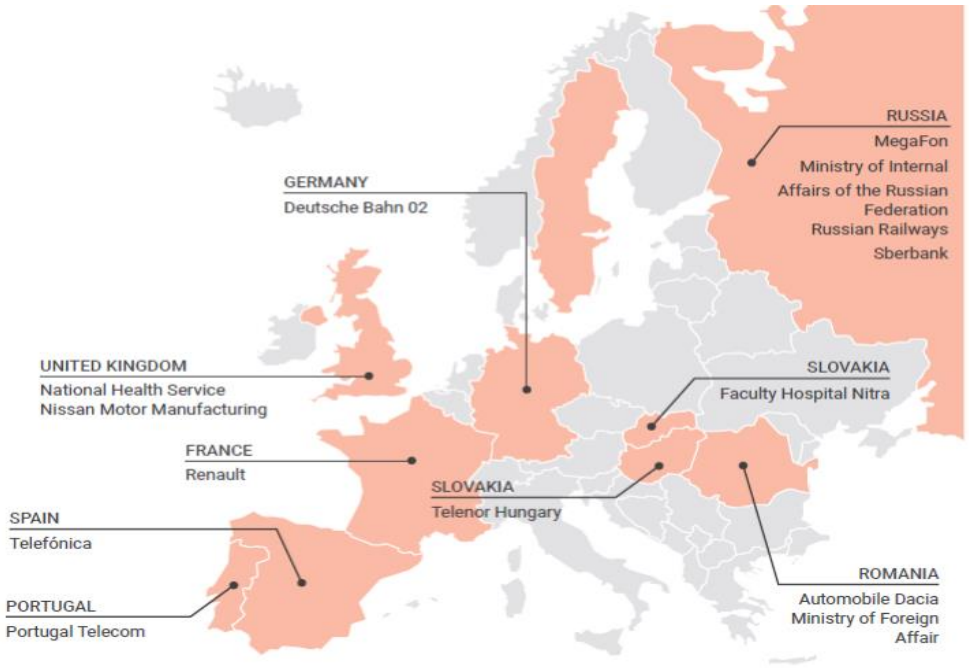


Figura 5-2. Países y principales blancos de Wannacry en Europa.

Fuente: Panorama actual de la ciberseguridad en España. Retos y oportunidades para el sector público y privado. Obtenido de https://www.ospi.es/export/sites/ospi/documents/documentos/Seguridad-y-privacidad/Google_Panorama-actual-de-la-ciberseguridad-en-Espana.pdf

IOACTA 2018 Europol.

Los ciberataques aumentaron de manera brutal de 2015 a 2016. Este último año, INCIBE registró un total de 115.257 ciberincidentes, lo que representa un aumento del 231% respecto a 2015. Destacando al mismo tiempo, un aumento del 241% respecto al número de ciberincidentes hacia ciudadanos y empresas y el 368% en lo que se refiere a operadores estratégicos y críticos durante ese mismo período. En 2017 se estabiliza el número total de ciberataques, a pesar de los 885 ciberincidentes registrados hacia operadores estratégicos y críticos con un aumento del 185% con respecto al año anterior (Figura 5-3).

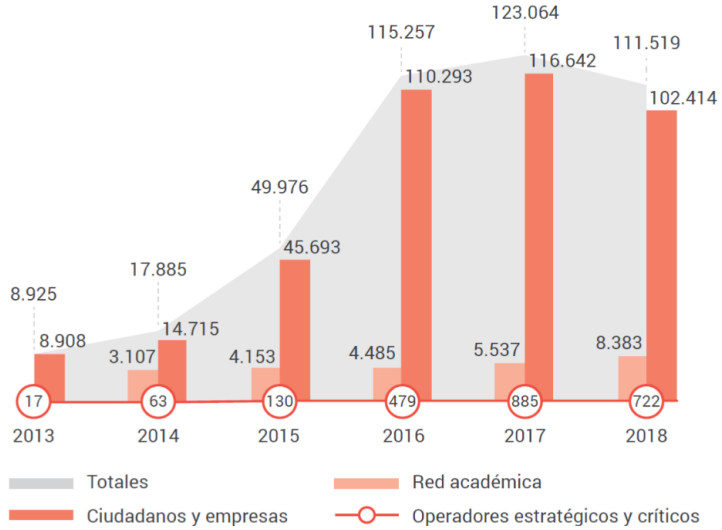


Figura 5-3. Número de incidentes registrados en España en los últimos años por INCIBE.

Fuente: Panorama actual de la ciberseguridad en España. Retos y oportunidades para el sector público y privado. Obtenido de https://www.ospi.es/export/sites/ospi/documents/documentos/Seguridad-y-privacidad/Google_Panorama-actual-de-la-ciberseguridad-en-Espana.pdf

Será a partir de 2018 cuando se aprecia mayor **variedad** en la tipología de los ciberincidentes y el número total de ciberincidentes registrados dejará de aumentar a esa velocidad, a excepción del año 2020 debido a las razones ya expuestas al comienzo de este capítulo (Figura 5-4) [1].

Tipo de incidente	INCIDENTES GESTIONADOS					
	2016	2017	2018	2019	2020	2021
Intrusión	14.373	19.275	8.541	6.479	9.557	7.039
Fraude	11.843	11.959	55.932	31.938	42.641	31.213
Malware	76.811	81.090	27.016	27.358	46.893	32.605
SPAM	10.279	7.957	0	0	0	0
Disponibilidad	495	514	100	58	1.971	7.177
Intento de intrusión	381	1.435	396	1.518	1.289	1.753
Robos de información	37	47	63	77	161	920
Contenido Abusivo			9.353	4.064	2.986	5.253
Recolección de información			5.605	84	87	106
Sistema Vulnerable			3.731	31.414	23.161	20.609
Otros	1.038	787	782	4.407	4.409	2.451

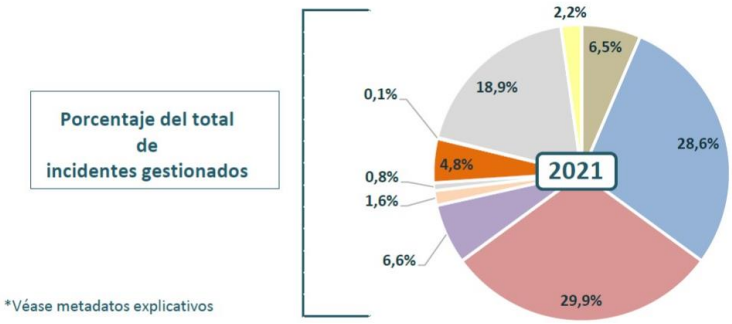


Figura 5-4. Tipo y número de incidentes gestionados.

Fuente: GOBIERNO DE ESPAÑA. MINISTERIO DEL INTERIOR. Informe sobre la cibercriminalidad en España 2021. SEC (Sistema Estadístico de Criminalidad). Obtenido de https://www.interior.gob.es/opencms/pdf/archivos-y-documentacion/documentacion-y-publicaciones/publicaciones-descargables/publicaciones-periodicas/informe-sobre-la-cibercriminalidad-en-Espana/Informe_cibercriminalidad_Espana_2021_126200212.pdf

Para finalizar con este sector, referirnos al apartado 1.1. Contexto y justificación, donde se indican los últimos datos publicados por INCIBE en su Balance de Ciberseguridad 2022. De los 118.820 ciberincidentes registrados, casi un 9% más respecto al año 2021. Analizando en número de **ciberincidentes más frecuentes** en función de su tipología, se concluye que 1 de cada 4 son un **fraude online**, destacando el **phishing** con casi 17.000 incidentes, seguido del **malware** con más de 14.000 y, por último, el **ransomware**, con casi 450 incidentes [2].

5.1.2. Sector público

El incremento en el número de ciberataques registrados contra el Estado español no se debe únicamente a un aumento real de la cifra, sino también a la **mayor capacidad** para detectarlos. En 2018, el Centro Nacional de Inteligencia (CNI) registró 38.000 incidentes de ciberseguridad, lo que representa un aumento del 43% respecto a 2017 (Figura 5-5) [56].

Los 82.530 ciberincidentes detectados por CCN-CERT durante el año 2020 frente a los 43.000 registrados el año anterior suponen un crecimiento respecto a los años previos, también fruto de la automatización introducida en los sistemas de detección de ataques del CCN-CERT que le ha permitido notificar más incidentes [59].

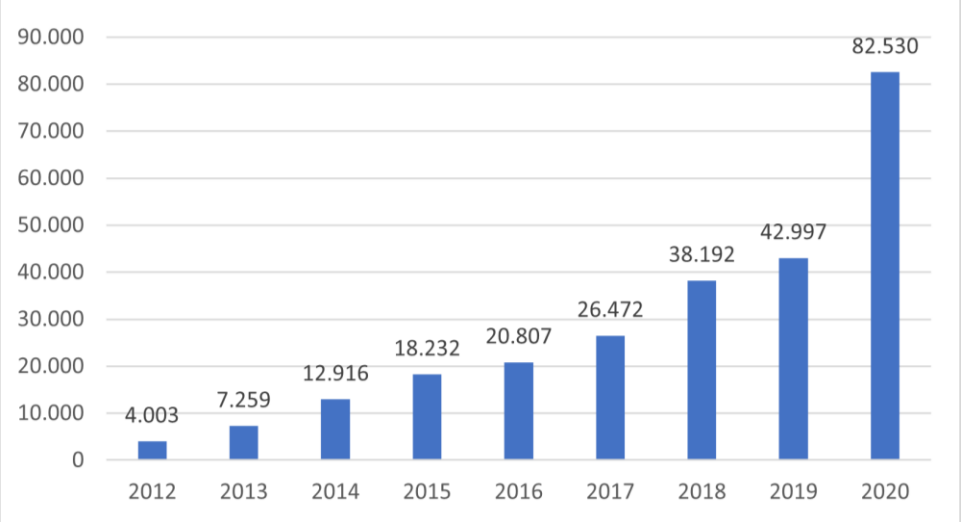


Figura 5-5. Número de ciberincidentes gestionados por CCN-CERT desde 2012 a 2020.

Fuente: Elaboración propia a partir de Ciberamenazas y Tendencias. CCN-CERT. 2020. Obtenido de https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/6338-ccn-cert-ia-13-21-ciberamenazas-y-tendencias-edicion-2021-1/file.html

Resulta obvio que los ciberatacantes utilizaron la crisis sanitaria para lanzar campañas de **spear phishing** (apartado 3.3.2). Además, se detectó un aumento de **aplicaciones fraudulentas** con contenido dañino con **malware** insertado para seguir su evolución durante los meses del estado de alarma y en medio de una gran confusión.

En 2020 también aumentaron de forma drástica los ataques de **ransomware**, tanto en su versión clásica como en la cada vez más habitual de doble extorsión (cifrado y publicación de datos robados).

El ransomware ha puesto el foco en organismos públicos, industria e infraestructuras críticas, usando diferentes tipos para extorsionar a sus víctimas y obtener un gran rendimiento económico [59].

Durante 2021, el número de ataques siguió la tendencia de finales de 2020, la cual tuvo un incremento muy importante respecto al primer semestre. A pesar de ello, los números son muy similares entre trimestres, habiendo una variación de apenas un 1% (Figura 5-6) [60].

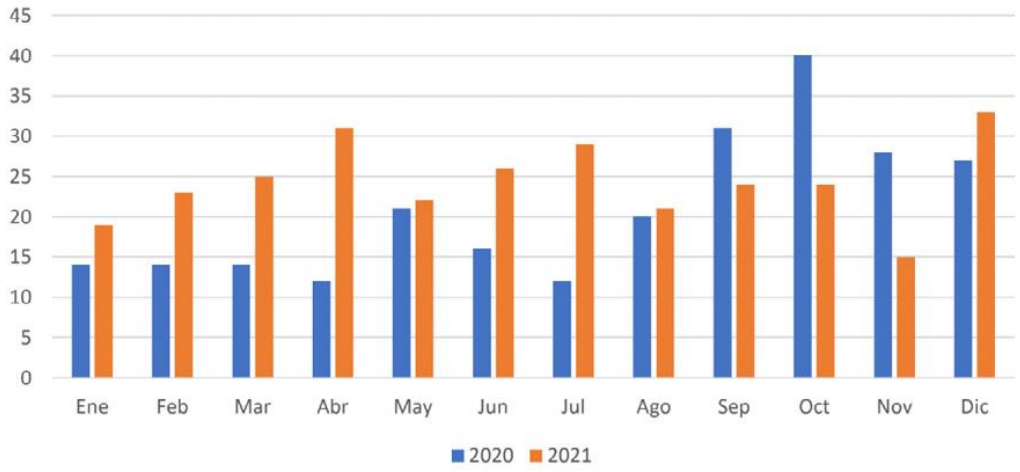


Figura 5-6. Ataques públicos de ransomware por mes.

Fuente: Ciberamenazas y Tendencias. CCN-CERT. 2022. Obtenido de https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/6786-ccn-cert-ia-24-22-ciberamenazas-y-tendencias-edicion-2022-1/file.html

Para concluir con este capítulo, cabe señalar que el **ransomware** se establece en la vía de ataque preferida de los ciberdelincuentes, que tienden hacia métodos de secuestro de la información cada vez más sofisticados y selectivos. Los ataques se han dirigido tanto a sectores **públicos** como **privados**, de diversos tamaños y nacionalidades. Esto ha permitido a los ciberatacantes incrementar tanto el importe del rescate solicitado como la probabilidad de que la víctima pague el rescate.

El conflicto en Ucrania, el ransomware y en la cadena de suministro o las operaciones contra infraestructuras críticas tanto en el ámbito IT como en el OT son algunas de las acciones que se han incrementado en 2022 y se mantendrán en los próximos meses [61].

Una vez finalizado el proceso de elaboración del presente TFM, se expondrán tanto las reflexiones y conclusiones como las dificultades tenidas en el mismo, información que se abordará en el siguiente capítulo.

6. Conclusiones

6.1. Conclusiones

Desde la aparición de Internet y las nuevas tecnologías, nuestro mundo ha dado un giro de 180º a todos los niveles. La digitalización implica adaptarse al nuevo entorno tecnológico y representa grandes **beneficios** para todas las organizaciones y usuarios; pero, al mismo tiempo, nos expone a ciertos **riesgos** que deberíamos conocer.

2020 será recordado como un año especialmente disruptivo, de los que marcan un antes y después, y no solo por la **crisis sanitaria** mundial, sino también por la **transformación digital.** Esta última ha hecho que estemos hiperconectados, que nuestros días transcurran prácticamente en línea, y que movernos por el ciberespacio sea normal, tanto en la vida personal como en la profesional.

Insistir, de nuevo, cómo la combinación de ingeniería social, phishing, malware (principalmente ransomware), redes TOR e incluso servicios de mensajería como Telegram son los principales puntos apoyo para cometer los ciberdelitos por parte de diferentes grupos cibercriminales. A medida que Internet de las cosas (IoT) evoluciona y los dispositivos inteligentes ganan popularidad, los ciberdelincuentes disfrutan de mayores oportunidades para romper las medidas de seguridad, logran el acceso no autorizado y cometen sus ciberdelitos. Cualquiera de ellos es una fuente de problemas ya que no solo afectan a la **privacidad** de nuestros datos como usuarios, sino que también **destruyen** las posibilidades comerciales de cualquier empresa. Todo esto, sin olvidar, la enorme **repercusión económica y social** para cualquier usuario, empresa o, incluso, el propio gobierno.

Ratificar la relevancia de los dos ciberincidentes elegidos como objeto de estudio en el presente TFM, como se indicó en su comienzo (apartado 1.1), con los datos recogidos sobre los ciberincidentes más frecuentes, donde 1 de cada 4 son un **fraude online**, destacando el **phishing** con casi 17.000 ciberincidentes, seguido del **malware** con más de 14.000 y, por último, el **ransomware**, con casi 450.

Además, si tenemos en cuenta que el 80% de estos ciberdelitos se produce por errores humanos, resulta crucial **protegerse** de los ataques maliciosos incidiendo en campañas de **concienciación y sensibilización** de los usuarios y empresas para reconocer los ciberataques, así como la adopción de una serie de **medidas de seguridad preventivas** (actualización de software, uso de antivirus…) sobre los sistemas de información y el uso de ellas con el objetivo de minimizar los posibles riesgos.

Otra pregunta interesante sería si los **esfuerzos** que hacen las empresas o, incluso el Gobierno, van en la correcta dirección. Aunque todavía queda mucho camino por recorrer, es cierto que se están adoptando medidas preventivas de sensibilización e información sobre ciberseguridad implicando tanto al **sector público** como **privado**, así como contratos de personal cualificado en esta materia.

Definitivamente, para evitar ser víctimas de ciberataques, es importante conocer y seguir una serie de **buenas prácticas** concediendo a la **ciberseguridad** la importancia que se merece. Siempre debe ser entendida como una línea de defensa que individuos y empresas tienen para **protegerse** no sólo contra el acceso no autorizado a los centros de datos y otros sistemas informáticos, sino como una forma de ayudar a **prevenir** los ataques que tienen como objetivo desactivar o interrumpir el funcionamiento de una red o un dispositivo.

6.2. Objetivos superados

Una vez hechas las reflexiones y conclusiones pertinentes, afirmar que se ha conseguido el objetivo de este TFM que era el estudio de los dos ciberincidentes elegidos por su relevancia, análisis, prevención y medidas de seguridad. No obstante, las **dificultades** tenidas en su elaboración han sido:

- La abundante información que existe sobre este tema obliga a dedicar mucho tiempo a su lectura y estudio de la misma para no confiarnos en lo primero que se publica. No toda ella es fiable, hay que comprobar su fuente porque hay mucha "basura" y se debe tener mucha precaución para hacer una buena selección de esta.
- Cuando se requiere buscar información más específica, dicha información se mezcla con otros ámbitos y se desvía del objetivo a conseguir, con lo cual se emplea mucho más tiempo en seleccionarla.
- En los foros, blogs… existe mucha información demasiado repetitiva sobre los ciberataques.

No obstante, el haber cursado asignaturas relacionadas con la Ciberseguridad durante el Grado de Informática "Redes y Seguridad" y "Auditoría Informática" o en el propio Máster en Ciberseguridad "Fundamentos de Ciberseguridad", "Sistemas de Gestión de Seguridad de la Información" y "Análisis Forense", entre otras, ha facilitado la comprensión de la información obtenida para llevar a cabo este proyecto.

6.3. Futuro trabajo

Por otro lado, si nos parásemos a reflexionar sobre **posibles líneas futuras** de actuación basadas en este TFM, mencionaré algunas de ellas para tener en cuenta:

- Sería interesante aprender de las dificultades tenidas ya mencionadas e intentar aprovecharlas para que, en sucesivas ocasiones, no se caiga en el mismo error o no se trabaje durante tantas horas en vano.
- Se podría crear un tutorial compartiendo los conocimientos adquiridos para poder avanzar con firmeza en la investigación de los ciberincidentes.
- Además, considero que sería de gran provecho comenzar con una buena formación sobre los ciberdelitos, insistiendo en la importancia de la concienciación y sensibilización de los usuarios y empresas para reconocer los ciberataques.
- Por último, y aunque el futuro sea incierto, con toda certeza que dependerá de la tecnología. Por ello, el objetivo de la ciberseguridad es construir confianza ofreciendo seguridad a individuos, empresas y gobiernos. En definitiva, proteger a la sociedad; y, en esto, todas las personas podemos y debemos participar de forma activa.
- Por todo ello, se dan por alcanzados todos los objetivos del presente TFM y se concluye el trabajo realizado, mencionando un futuro proyecto como la extensión del mismo y la utilización de la información expuesta en el aquí presente.

Bibliografía

Todas las direcciones URL que aparecen a continuación, han sido comprobadas y validadas a fecha de **8 de junio de 2023.**

[1] GOBIERNO DE ESPAÑA. MINISTERIO DEL INTERIOR. *Informe sobre la cibercriminalidad en España 2021.* SEC (Sistema Estadístico de Criminalidad)
https://www.interior.gob.es/opencms/pdf/archivos-y-documentacion/documentacion-y-publicaciones/publicaciones-descargables/publicaciones-periodicas/informe-sobre-la-cibercriminalidad-en-Espana/Informe_cibercriminalidad_Espana_2021_126200212.pdf
[2] INCIBE. *Balance de Ciberseguridad 2022.*
https://www.incibe.es/sites/default/files/paginas/que-hacemos/balance_ciberseguridad_2022_incibe.pdf
[3] NACIONES UNIDAS. *Objetivos de desarrollo sostenible, 2030.* (S. D.)
https://www.un.org/sustainabledevelopment/es/sustainable-development-goals/
[4] METODOLOGÍA. Concepto. (2013-2023) Enciclopedia. Etecé. (S. D.)
https://concepto.de/metodologia/
[5] Qué es la gestión de riesgos y cómo aplicarla a tu proyecto en solo 6 pasos (2023, febrero).
https://asana.com/es/resources/project-risk-management-process
[6] HERRERO, P. Riesgos que se deben dominar al gestionar un proyecto. Sage Group. (2023)
https://www.sage.com/es-es/blog/riesgos-que-se-deben-dominar-al-gestionar-un-proyecto/
[7] INCIBE y OSI. *Guía de ciberataques. Todo lo que debes saber a nivel de usuario.* (S. D.)
https://www.osi.es/sites/default/files/docs/guia-ciberataques/osi-guia-ciberataques.pdf
[8] INCIBE. *Guía nacional de notificación y gestión de ciberincidentes. Aprobado por el Consejo Nacional de Ciberseguridad. Gobierno de España.* (2020, 28 de abril).
https://www.incibe-cert.es/guias-y-estudios/guias/guia-nacional-notificacion-y-gestion-ciberincidentes
[9] INCIBE. *Clasificación de los ciberincidentes*. (S. D.)
https://www.incibe-cert.es/taxonomia
[10] *Guía de Seguridad de las TIC CCN-STIC 817. Esquema Nacional de Seguridad. Gestión de Ciberincidentes.* (2020, abril).
https://www.ccn-cert.cni.es/series-ccn-stic/800-guia-esquema-nacional-de-seguridad/988-ccn-stic-817-gestion-de-ciberincidentes/file.html
[11] INCIBE. *Guía nacional de notificación y gestión de ciberincidentes.* Aprobado por el Consejo Nacional de Ciberseguridad. Gobierno de España. (2020, 21 de febrero).
https://www.incibe-cert.es/sites/default/files/contenidos/guias/doc/guia_nacional_notificacion_gestion_ciberincidentes.pdf
[12] *Suplantación de identidad (Phishing)* (2022).
https://es.malwarebytes.com/Phishing/
[13] INCIBE. *Temáticas: conoce los aspectos esenciales de los ataques de tipo phishing*. (2021, 19 de enero)
https://www.incibe.es/protege-tu-empresa/blog/tematicas-conoce-los-aspectos-esenciales-los-ataques-tipo-phishing
[14] APWG. *GLOBAL PHISHING SURVEY* (2023)
https://apwg.org/globalphishingsurvey/
[15] INCIBE. *Phishing: El anzuelo en tu bandeja de entrada.* (S D.)
https://www.incibe.es/aprendeciberseguridad/Phishing
[16] INCIBE. *Los riesgos y las medidas de seguridad del correo electrónico.* (2023, 28 de febrero)
https://www.incibe.es/protege-tu-empresa/blog/filtro/fraude

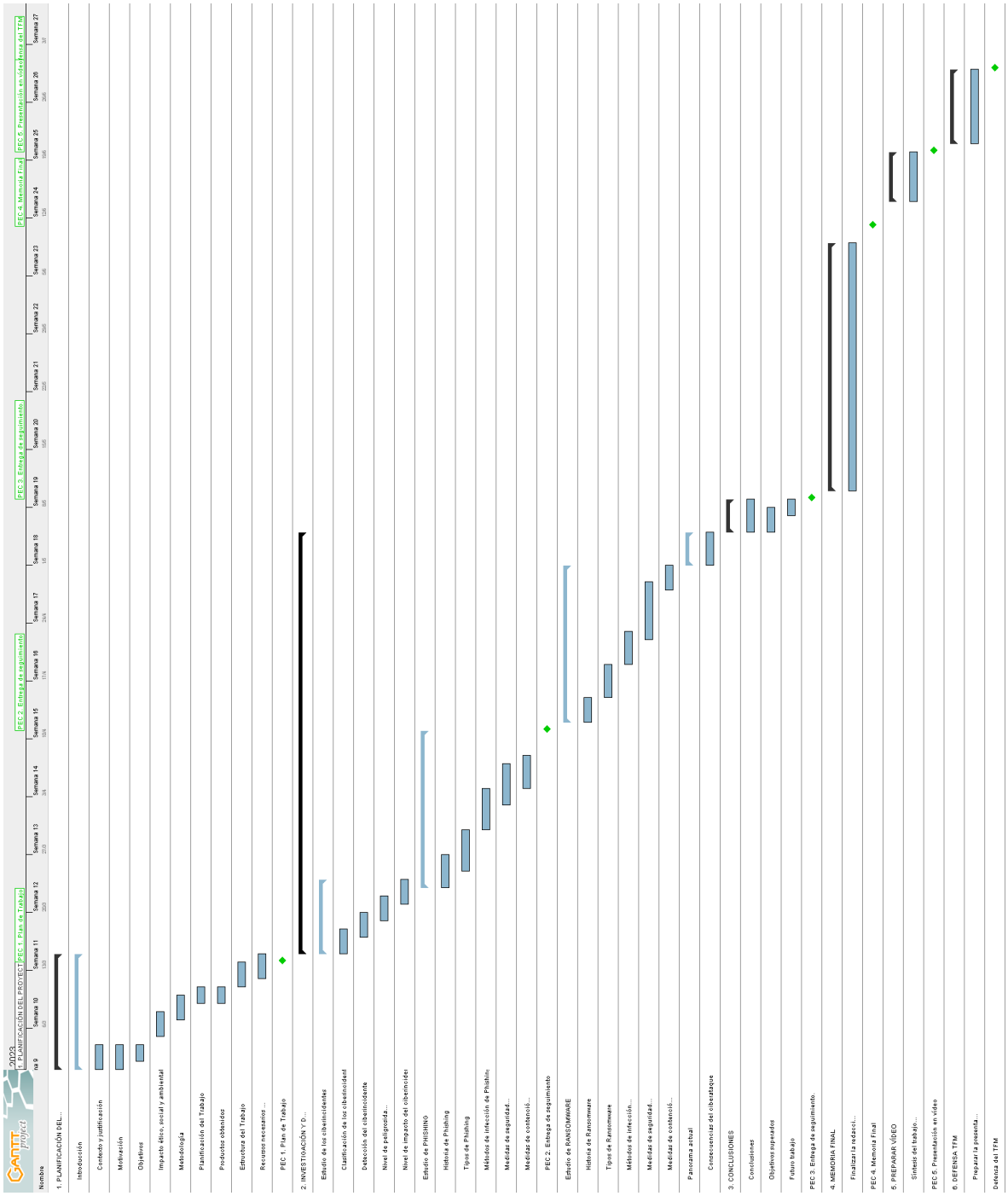
[17] OSI. *Guía para identificar fraudes online.* (S.D.)
https://www.osi.es/es/guia-fraudes-online
[18] OSI. *Cómo comprar online y no caer en el intento.* (2019, 19 de junio).
https://www.osi.es/es/campanas/compras-seguras-online
[19] OSI. *Alquileres vacacionales.* (S.D.)
https://www.osi.es/es/campanas/alquileres-vacacionales
[20] OSI. *Identificando bulos, noticias falsas y fraudes en la Red.* (2020, 23 de marzo)
https://www.osi.es/es/campanas/bulos-fake-news-fraudes
[21] SCAMWATCH. *Types of scams.* ACCC. Australian Competition & Consumer Commission (S.D.)
https://www.scamwatch.gov.au/types-of-scams
[22] OSI. *Las dos caras de las criptomonedas*. (2019, 7 de agosto)
https://www.osi.es/es/campanas/criptomonedas
[23] Credit Angel. *Fraud & identity theft protection.* (S. D.)
https://www.creditangel.co.uk/help/a-guide-to-the-most-common-fraud-methods
[24] CAIXABANK. *Inversiones fantasma: así funciona la estafa que puede costarte tus ahorros.* (2023).
https://www.caixabank.es/particular/seguridad/fraude-inversiones.html?loce=sh-part-Seguridad-FraudeDigital-4-destacado-Seguridad-InversionesFantasmaAsiFuncionaEstafaQuePuedeCostarteTusAhorros-NA
[25] Ecommerce Guide. *La guía completa para el fraude del comercio electrónico y la prevención.* (2017, 18 de mayo).
https://ecommerceguide.com/es/guias/ecommerce-fraud-2/
[26] Joan Mir Rubio. *Ataques*. Coordinado por Helena Rifà Pous. Fundació Universitat Oberta de Catalunya (FUOC). (2022, octubre).
[27] *Ataques de Pharming.* (2022, 29 de septiembre).
https://www.avast.com/es-es/c-pharming
[28] OSI. *Conoce a fondo qué es el Phishing*. (S. D.)
https://www.osi.es/es/banca-electronica
[29] INCIBE. *Detectada una campaña de phishing suplantando a Ibercaja.* (2021, 1 de julio).
https://www.incibe.es/empresas/avisos/ibercaja-victima-phishing
[30] Romero, L. *Saltar la confirmación de redireccionamiento en Google y Youtube. (2019, 13 de mayo).*
https://www.blackploit.com/2019/05/bypass-redirect-check-google-youtube.html
[31] INCIBE. *URL acortadas: consideraciones a tener en cuenta.* (2022, 2 de noviembre).
https://www.incibe.es/ciudadania/blog/url-acortadas-consideraciones-tener-en-cuenta
[32] *¿Cómo elaborar un plan de ciberseguridad?* (2022, 7 de julio).
https://blog.wearedrew.co/ciberseguridad/como-elaborar-un-plan-de-ciberseguridad
[33] *Medidas de prevención de ciberataques en Pymes.* (2022, 4 de noviembre).
https://dirigentesdigital.com/tecnologia/las-7-mejores-medidas-de-prevencion-de-ciberataques-en-pymes
[34] *Wikipedia.* Ransomware. (2022, 23 de diciembre).
https://es.wikipedia.org/wiki/Ransomware
[35] Poitevin, V., *Historia de los Ramsomware.* (2023, 5 de enero).
https://www.stormshield.com/es/noticias/breve-historia-de-los-Ransomware/#:~:text=En%201989%2C%20el%20%C2%ABtroyano%20AIDS,y%20particulares%20de%2090%20pa%C3%ADses
[36] *Ruiz, V. ¿Puede la exfiltración de datos ser más peligrosa que el mismo ransomware? (2022, 24 de agosto)*
https://es.linkedin.com/pulse/puede-la-exfiltraci%C3%B3n-de-datos-ser-m%C3%A1s-peligrosa-que-el-victor-ruiz?trk=pulse-article_more-articles_related-content-card

[37] *TICPymes. 5 consecuencias del robo de información sensible. (2021, 9 de junio)*
https://www.ticpymes.es/tecnologia/noticias/1126357049504/5-consecuencias-del-robo-de-informacion-sensible.1.html
[38] INCIBE. RANSOMWARE. *Una guía de aproximación para el empresario.* (2021, 20 de abril).
https://www.incibe.es/protege-tu-empresa/guias/ransomware-guia-aproximacion-el-empresario
[39] INCIBE. *Blog. Artículos relacionados con: Amenazas.* (S. D.)
https://www.incibe.es/protege-tu-empresa/blog/filtro/amenazas
[40] INCIBE. *Ataques 'Watering hole': en qué consisten y cómo protegerse.* (2020, 23 de julio).
https://www.incibe.es/protege-tu-empresa/blog/ataques-watering-hole-consisten-y-protegerse
[41] INCIBE. *¿Es seguro tu escritorio remoto?* (2019, 22 de agosto).
https://www.incibe.es/protege-tu-empresa/blog/seguro-tu-escritorio-remoto
[42] INCIBE. Ayuda ransomware. (S. D.)
https://www.incibe.es/protege-tu-empresa/herramientas/servicio-antiransomware
[43] Cristian Borghello, Marcelo Temperini, Mauro Gioino, Nicolás Gustavo, Bruna Matías Sequeira, Maximiliano Macedo & Walter Heffel. Guía para evitar infecciones de RANSOMWARE. Versión 1.1 (2018, septiembre).
https://owasp.org/www-pdf-archive/Owasp-guia-evitar-Ransomware_es.pdf
[44] INCIBE. *Copias de seguridad: una guía de aproximación para el empresario.* (2018).
https://www.incibe.es/sites/default/files/contenidos/guias/guia-copias-de-seguridad.pdf
[45] INCIBE. *TemáTICas Ransomware.* (S. D.)
https://www.incibe.es/protege-tu-empresa/tematicas/ransomware
[46] INCIBE. *Kit de concienciación.* (S. D.)
https://www.incibe.es/protege-tu-empresa/kit-concienciacion
[47] INCIBE. Juego de rol. ¿Estás preparado para ser atacado? (S. D.)
https://www.incibe.es/protege-tu-empresa/juego-rol-pyme-seguridad
[48] INCIBE. Hackend, se acabó el juego. (S. D.)
https://www.incibe.es/protege-tu-empresa/hackend
[49] INCIBE. Itinerarios interactivos (S. D.)
https://www.incibe.es/protege-tu-empresa/itinerarios-interactivos
[50] CSIRT-CV (Computer Security Incident Response Team / Centro Seguridad TIC de la Comunidad Valencian) *Tutoriales.* (2023)
https://concienciat.gva.es/
[51] Miguel A. Perez. *Qué es el Principio de Mínimo Privilegio y cómo puede salvar tu ordenador*. (2014).
https://blogthinkbig.com/principio-de-minimo-privilegio
[52] Winex Paraguay. *Segmentación y Direccionamiento IP.* (2017, 5 de marzo).
http://www.winex.com.py/2017/03/05/segmentacion-y- direccionamiento-ip/
[53] *DMZ: qué es, para qué sirve y cómo configurarlo.* (2021, 15 de junio).
https://www.redusers.com/noticias/publicaciones/dmz/
[54] Monrás, Alex. *Habilitar Acceso Controlado a Carpetas en Windows 10.* (S. D.)
https://dominiogeek.com/acceso-controlado-carpetas-windows-10/
[55] *CCN-CERT IA-11/18 Medidas de seguridad contra Ransomware* (2018, mayo)
https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/2877-ccn-cert-ia-11-18-medidas-de-seguridad-contra-ransomware/file.html
[56] GOOGLE. *Panorama actual de la ciberseguridad en España. Retos y oportunidades para el sector público y privado.* (S. D.)
https://www.ospi.es/export/sites/ospi/documents/documentos/Seguridad-y-privacidad/Google_Panorama-actual-de-la-ciberseguridad-en-Espana.pdf

[57] *Vientos de Camino* (2019, febrero).
https://www.tendencias.kpmg.es/wp-content/uploads/2019/04/Informe_Riesgos_Abril2019.pdf
[58] EUROPOL. *Internet Organised Crime Threat Assessment (IOCTA).* 2021.
https://www.europol.europa.eu/cms/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2021.pdf
[59] CCN-CERT. *Ciberamenazas y Tendencias*. 2021.
https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/6338-ccn-cert-ia-13-21-ciberamenazas-y-tendencias-edicion-2021-1/file.html
[60] CCN-CERT. *Ataques públicos de ransomware por mes*. Obtenido de Ciberamenazas y Tendencias. 2022.
https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/6786-ccn-cert-ia-24-22-ciberamenazas-y-tendencias-edicion-2022-1/file.html
[61] CCN-CERT. *El incremento en la explotación de vulnerabilidades críticas marca una tendencia en ciberseguridad.* (2022, 14 de noviembre)
https://www.ccn-cert.cni.es/seguridad-al-dia/novedades-ccn-cert/12129-el-incremento-en-la-explotacion-de-vulnerabilidades-criticas-marca-una-tendencia-en-ciberseguridad.html

Anexos

Anexo I. Planificación del Trabajo



Anexo II. Glosario de términos ordenados alfabéticamente

Como ya se ha señalado en el apartado 2.1, los frecuentes ciberataques han hecho que tengamos que incluir en nuestro vocabulario habitual diferentes términos en los que conviene insistir para su mejor comprensión y algunos de los cuales aparecen en el presente TFM. Todos ellos han sido seleccionados y ordenados alfabéticamente con el fin de agilizar su búsqueda [7]:

GLOSARIO DE TÉRMINOS	
Término	**Definición**
Acceso no autorizado	Proceso por el cual un usuario accede sin vulnerar ningún servicio, sistema o red, a consultar contenido, sistemas de información y/o comunicación para los cuales no está debidamente autorizado, o no tiene autorización tácita o manifiesta.
Acoso	Referido a acoso virtual o ciberacoso, se trata del uso de medios de comunicación digitales para acosar a una persona, o grupo de personas, mediante ataques personales, divulgación de información privada o íntima, o falsa.
APT (Advanced Persitent Threat) / AVT (Advanced Volatility Threat)	Este tipo de amenazas persistentes son ataques dirigidos contra organizaciones concretas, sustentados en mecanismos muy sofisticados de ocultación, anonimato y persistencia. Esta amenaza habitualmente emplea técnicas de ingeniería social para conseguir sus objetivos junto con el uso de procedimientos de ataque conocidos.
Ataque cibernético	Un ataque cibernético o informático es un intento organizado de causar daños en una determinada red informática, bien sea por una motivación económica, social o política. La mayor parte de estos ataques comienzan con la difusión de programas maliciosos (virus), que se aprovechan tanto de los fallos de seguridad en los sistemas informáticos de las empresas, como de los propios empleados.
Ataque por fuerza bruta	Proceso por el cual un atacante trata de vulnerar un sistema de validación por credenciales de acceso, contraseña o similar, mediante el empleo de todas las combinaciones posibles, con el fin de acceder a sistemas de información y/o comunicación para los cuales no tiene privilegios o autorización.
Baiting	Se trata de una técnica de ingeniería social. El cibercriminal deja un cebo, en forma dispositivo de almacenamiento (CD, USB…), infectado con un malware. Se deja "olvidado" en un lugar público (ascensores, baños…), para que se encuentre fácilmente. Si la víctima abre ese dispositivo desde su ordenador, el sofware malicioso se instalará y el hacker podrá acceder así a los datos personales del usuario.
Bitcoin	Bitcoin es la moneda de Internet. Su origen se remonta al año 2009, cuando el grupo o individuo bajo el pseudónimo Satoshi Nakamoto creó una moneda electrónica que solo podía usarse en la red. Es la moneda más usada en las ciber extorsiones por la dificultad que supone hacer un tracking de su circulación. La legalidad de los bitcoins está en entredicho y puede considerarse como alegal.
Bot o botnet	Un bot es un programa automatizado que puede usarse tanto con fines lícitos (sistemas de atención al cliente automatizados) como ilícitos (ataques DDoS o difusión de bulos). Cuando están organizados en una red controlada de forma remota por un ciberdelincuente hablamos de botnet. Pueden utilizarse para llevar a cabo un amplio espectro de actividades maliciosas, como envíos masivos de SPAM o ataques de denegación de servicio.
Ciberamenaza	Amenaza a los sistemas y servicios en el ciberespacio o alcanzables a través de este.
Ciberespacio	Espacio virtual que engloba todos los sistemas TIC, tanto sistemas de información como sistemas de control industrial. El ciberespacio se apoya en la disponibilidad de Internet como

	red de redes, enriquecida con otras redes de transporte de datos.
Ciberincidente	Todo hecho que tenga efectos adversos reales en la seguridad de las redes y sistemas de información.
Ciberriesgo	Se trata de un tipo de riesgo derivado del uso de las nuevas tecnologías por el que la privacidad, la información confidencial de una empresa o el correcto funcionamiento de sus sistemas informáticos –entre otros factores– pueden verse afectados.
Ciberseguridad	Parte de la seguridad que se ocupa de los delitos cometidos en el ciberespacio y la prevención de los estos.
Command and Control (C&C)	Referido a paneles de mando y control (también referenciados como C2), por el cual atacantes cibernéticos controlan determinados equipos zombie infectados con muestras de la misma familia de software dañino. El panel de comando y control actúa como punto de referencia, control y gestión de los equipos infectados.
Conexión sospechosa	Todo intercambio de información a nivel de red local o pública, cuyo origen o destino no esté plenamente identificado, así como la legitimidad de los mismos.
Correo masivo no solicitado (SPAM)	Correo electrónico no solicitado que se envía a un gran número de usuarios o un número elevado de correos electrónicos enviados a un mismo usuario en un corto espacio de tiempo.
Criptografía	Técnica que consiste en cifrar un mensaje, conocido como texto en claro, convirtiéndolo en un mensaje cifrado o criptograma, que resulta ilegible para todo aquel que no conozca la clave mediante la cual ha sido cifrado.
DDoS (Distributed Denial of Service)	Denegación distribuida de servicio: Variante de DoS en el que la remisión de peticiones se lleva a cabo de forma coordinada desde varios puntos hacia un mismo destino. Para ello se emplean redes de bots, generalmente sin el conocimiento de los usuarios.
DNS Open-Resolver	Servidor DNS capaz resolver consultas DNS recursivas procedentes de cualquier origen de Internet. Este tipo de servidores suele emplearse por usuarios malintencionados para la realización de ataques DDoS.
DoS (Denial of Service)	Ataque de denegación de servicio: Conjunto de técnicas que tienen por objetivo dejar un servidor inoperativo. Mediante este tipo de ataques se busca sobrecargar un servidor y de esta forma impedir que los usuarios legítimos puedan utilizar los servicios por prestados por él provocando su colapso.
Extorsión	Obligar a una persona o mercantil, mediante el empleo de violencia o intimidación, a realizar u omitir actos con la intención de producir un perjuicio a esta, o bien con ánimo de lucro de la que lo provoca.
Gusano	Programa malicioso que tiene como característica principal su alto grado de dispersabilidad. Su fin es replicarse a nuevos sistemas para infectarlos y seguir replicándose a otros equipos informáticos, aprovechándose de todo tipo de medios como el correo electrónico, IRC, FTP, correo electrónico, P2P y otros protocolos específicos o ampliamente utilizados.
Hacker	El hacker es una persona con extraordinarios conocimientos informáticos, tanto si los pone en práctica con fines legales o ilegales. En general, los hackers podrían dividirse en dos tipos: los White Hat (encuentran vulnerabilidades en los sistemas y los corrigen) y los Black Hat (tratan de vulnerar y robar información con fines ilícitos).
ICMP	Protocolo de control de mensajes de Internet.
Ingeniería social	Técnicas que buscan la revelación de información sensible de un objetivo mediante el uso de métodos persuasivos y con ausencia de voluntad o conocimiento de la víctima.
Inyección SQL	Tipo de explotación, consistente en la introducción de cadenas mal formadas de SQL, o cadenas que el receptor no espera o controla debidamente; las cuales provocan resultados no esperados en la aplicación o programa objetivo, y por la cual el atacante produce efectos inesperados y para los que no está autorizado en el sistema objetivo.
Malvertising o adware	Tipo de software que muestra publicidad de forma automática al usuario sin que este haya dado su permiso explícito para generar beneficios a sus creadores. Este tipo de malware varía desde poco invasivo (muestra algún anuncio durante un proceso determinado) a muy invasivo,

	con casos en los que llega a inutilizar el dispositivo que ataca.
Malware (código dañino)	Palabra que deriva de los términos malicious y software. Cualquier pieza de software que lleve a cabo acciones como extracción de datos u otro tipo de alteración de un sistema puede categorizarse como malware.
Otros fraudes	Engaño económico con la intención de conseguir un beneficio, y con el cual alguien resulta perjudicado.
Pharming	Ataque informático que aprovecha vulnerabilidades de los servidores DNS (Domain Name System). Al tratar de acceder el usuario al sitio web, el navegador redirigirá al usuario a una dirección IP donde se aloja una web maliciosa que suplanta la auténtica, y en la que el atacante obtendrá información sensible de los usuarios.
Phishing	Estafa cometida a través de medios telemáticos mediante la cual el estafador intenta conseguir, de usuarios legítimos, información confidencial (contraseñas, datos bancarios, etc.) de forma fraudulenta empleando métodos de ingeniería social.
Proxy	Ordenador, generalmente un servidor, intermedio usado en las comunicaciones entre otros dos equipos, siendo normalmente usado de manera trasparente para el usuario.
Ransomware	Malware que infecta una máquina, de modo que el usuario es incapaz de acceder a los datos almacenados en el sistema. La víctima recibe posteriormente algún tipo de comunicación en la que se le coacciona para que se pague una recompensa que permita acceder al sistema y los archivos bloqueados.
RDP (Remote Desktop Protocol)	Protocolo propietario desarrollado por Microsoft que permite la comunicación en la ejecución de una aplicación entre una terminal y un servidor Windows.
Redes y sistemas de información	Se entiende por este concepto uno de los tres siguientes puntos: - Una red de comunicaciones electrónicas en el sentido del artículo 2, letra a), de la Directiva 2002/21/CE. - Todo dispositivo o grupo de dispositivos interconectados o relacionados entre sí en el que uno o varios de ellos realizan, mediante un programa, el tratamiento automático de datos digitales. - Los datos digitales almacenados, tratados, recuperados o transmitidos mediante elementos contemplados anteriormente para su funcionamiento, utilización, protección y mantenimiento
RGPD	Reglamento General de Protección de Datos, reglamento EU 2016/679.
Robo de credenciales de acceso	Acceso o sustracción no autorizada a credenciales de acceso a sistemas de información y/o comunicación.
Rootkit	Conjunto de software dañino que permite el acceso privilegiado a áreas de una máquina, mientras que al mismo tiempo se oculta su presencia mediante la corrupción del Sistema Operativo u otras aplicaciones. Su propósito por tanto de un rootkit es enmascarar eficazmente payloads y permitir su existencia en el sistema.
Seguridad en redes y sistemas de información	Capacidad de las redes y sistemas de información de resistir, con un nivel determinado de fiabilidad, toda acción que comprometa la disponibilidad, autenticidad, integridad o confidencialidad de los datos almacenados, transmitidos o tratados, o los servicios ofrecidos por tales redes y sistemas de información o accesibles a través de ellos.
Spear Phishing	Variante del Phishing mediante la que el atacante focaliza su actuación sobre un objetivo concreto.
Suplantación de identidad	Actividad maliciosa en la que un atacante se hace pasar por otra persona para cometer algún tipo de fraude o acoso.
Taxonomía	Clasificación u ordenación en grupos de objetos o sujetos que poseen unas características comunes.
Telnet	Protocolo de red que permite acceder a otra máquina para manejarla remotamente como si estuviéramos sentados delante de ella.
Troyano	Tipo de malware que se enmascara como software legítimo con la finalidad de convencer a la víctima para que instale la pieza en su sistema. Una vez instalado, el software dañino tiene la

	capacidad de desarrollar actividad perjudicial en segundo plano. Un troyano no tiene la capacidad de replicarse, pero puede tener gran capacidad dañina en un sistema a modo de troyanos o explotando vulnerabilidades de software.
Virus	Tipo de malware cuyo principal objetivo es modificar o alterar el comportamiento de un sistema informático sin el permiso o consentimiento del usuario. Se propaga mediante la ejecución en el sistema de software, archivos o documentos con carga dañina, adquiriendo la capacidad de replicarse de un sistema a otro. Los métodos más comunes de infección se dan a través de dispositivos extraíbles, descargas de Internet y archivos adjuntos en correos electrónicos. No obstante, también puede hacerlo a través de scripts, documentos, y vulnerabilidades XSS presentes en la web.
VNC (Virtual Network Computing)	Programa de software libre basado en una estructura cliente-servidor que permite observar remotamente las acciones del ordenador servidor a través de un ordenador cliente.
Webinject	Herramienta gratuita y de código abierto diseñada principalmente para automatizar la prueba de las aplicaciones y servicios web.

Tabla 0-1. Glosario de términos.

Fuente: Elaboración propia a partir de "Guía nacional de notificación y gestión de ciberincidentes". Aprobado por el Consejo Nacional de Ciberseguridad. Gobierno de España. (2020, 21 de febrero). Obtenido https://www.incibe-cert.es/sites/default/files/contenidos/guias/doc/guia_nacional_notificacion_gestion_ciberincidentes.pdf

Anexo III. Pasos para la elaboración de un plan de Ciberseguridad

Como ya se ha hecho referencia en los apartados 3.5 y 4.4 respectivamente, se debe evitar cualquier ciberataque que ponga en peligro la propia integridad, el presente y el futuro de la organización. Por lo que, las empresas deberían elaborar un plan de ciberseguridad que implique seleccionar e implementar acciones prácticas para protegerse de amenazas externas e internas.

El Plan de Ciberseguridad debe ayudar a establecer una estrategia que se implemente en una organización y donde se incluyan las medidas técnicas, legales y organizativas pertinentes. A continuación, se indicarán los pasos a seguir de un plan modelo de ciberseguridad (Figura 0.2), junto con una breve explicación de cada uno de ellos [32]:

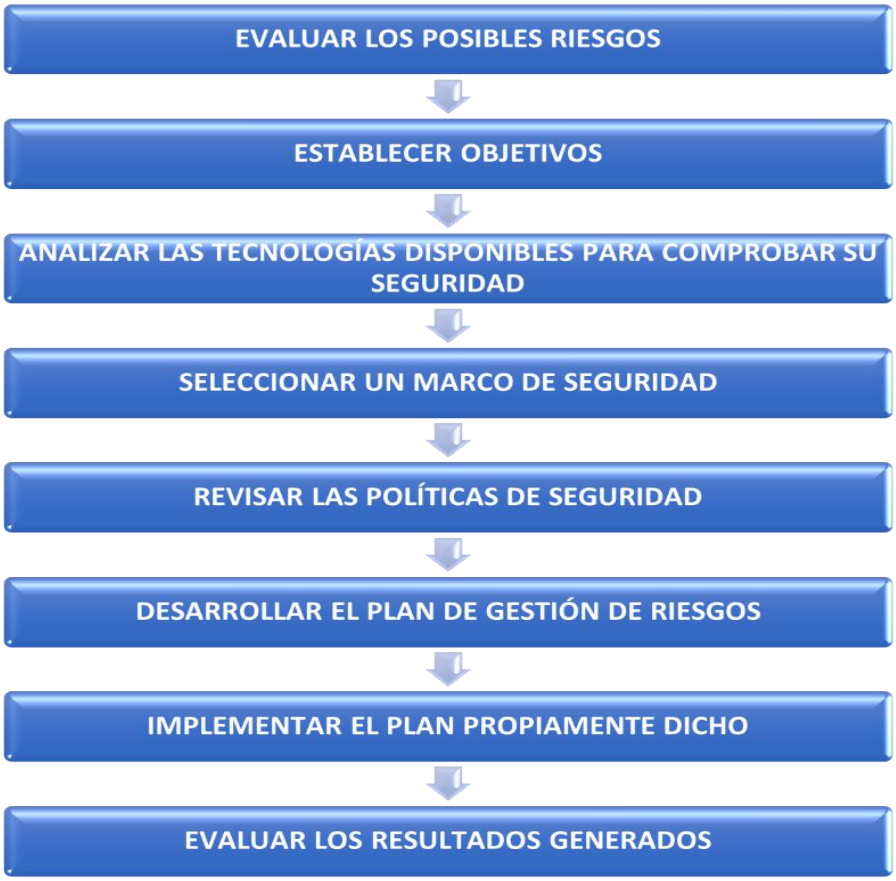


Figura 0-1. Pasos de un Plan modelo de Ciberseguridad.

Fuente. Elaboración propia a partir de https://blog.wearedrew.co/ciberseguridad/como-elaborar-un-plan-de-ciberseguridad.

1. Realizar una evaluación de riesgos de seguridad.

En primer lugar, se debe realizar una evaluación de riesgos de seguridad empresarial de IT para que la empresa evalúe, identifique y modifique su postura de seguridad general. Esta evaluación requerirá la colaboración de múltiples grupos y propietarios de datos. Este proceso es necesario para obtener el compromiso de la dirección y, así, asignar recursos e implementar las soluciones de seguridad adecuadas.

Una evaluación integral de los riesgos de seguridad también ayuda a determinar el valor de los distintos tipos de datos generados y almacenados en toda la empresa. Si no se valoran los diversos tipos de datos, es casi imposible priorizar y asignar recursos tecnológicos donde más se necesitan.

Para evaluar con precisión el riesgo, la administración debe detectar las fuentes de datos más valiosas para la organización, dónde se encuentra el almacenamiento y sus debilidades asociadas.

2. Establecer objetivos de seguridad.

Un componente clave de la estrategia de un plan de ciberseguridad es garantizar que vaya acorde con los objetivos comerciales de la empresa. Una vez que se marcan dichos objetivos, se puede iniciar la implementación de un programa proactivo de ciberseguridad para toda la organización.

Esta sección identifica varias áreas que pueden ayudar a elaborar los objetivos de seguridad.

3. Evaluar la tecnología existente.

Una vez que se han identificado los activos, se procederá a la evaluación de la tecnología. Los siguientes pasos son determinar si estos sistemas cumplen con las mejores prácticas de seguridad, comprender cómo funcionan en la red y quién respalda la tecnología dentro de la empresa.

4. Seleccionar un marco de seguridad.

Los resultados de la evaluación de riesgos de ciberseguridad, la evaluación de vulnerabilidades y la prueba de irrupción ayudarán a determinar qué marco de trabajo seleccionar.

Actualmente, existen múltiples marcos disponibles que pueden ayudar a crear y respaldar un plan de ciberseguridad. El marco de seguridad proporcionará la orientación sobre los controles necesarios para monitorear y medir continuamente la postura de seguridad de la organización.

5. Revisar las políticas de seguridad.

El objetivo de las políticas de seguridad es llegar a todas las amenazas de seguridad e implementar estrategias de ciberseguridad.

Una empresa puede tener una política de seguridad general y políticas secundarias específicas para abordar diversas tecnologías en la organización. Para garantizar que las políticas de seguridad estén actualizadas y enfrentar las amenazas emergentes, se recomienda una revisión exhaustiva de ellas.

6. Crear un plan de gestión de riesgos.

La creación de un plan de gestión de riesgos proporciona un análisis de los riesgos potenciales que pueden afectar a la empresa. Este enfoque posibilita que la empresa identifique y analice los riesgos que podrían afectar negativamente a la organización antes de que ocurran.

Las siguientes políticas son ejemplos de políticas de mejores prácticas que se pueden incorporar a su plan de gestión de riesgo:

- Política de privacidad de datos: establece que la gobernanza en torno al manejo de los datos corporativos se maneja y protege adecuadamente.
- Política de retención: describe cómo se deben almacenar o archivar varios tipos de datos corporativos, dónde y durante cuánto tiempo.

- Política de protección de datos: establece cómo la empresa maneja los datos personales de sus empleados, clientes, proveedores y otros terceros.
- Plan de respuesta a incidentes: describe las responsabilidades y los procedimientos que deben seguirse para garantizar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad.

7. Implementar el plan de ciberseguridad.

En esta etapa del plan de ciberseguridad, las evaluaciones están casi finalizadas junto con los planes de políticas. Ahora es el momento de priorizar los esfuerzos de mejora y asignar tareas a los equipos:

- Asignar elementos de mejora por prioridad a los equipos internos: si la empresa tiene un departamento de gestión de proyectos, se puede contar con este equipo para gestionar el proyecto.; si no hay un equipo de proyecto disponible, hay que trabajar con los equipos internos y planificar los esfuerzos.
- Establecer objetivos de plazos de mejora realistas: establecer plazos demasiado agresivos y poco realistas solo conducirá al fracaso.

8. Evaluar la estrategia de seguridad implementada.

Este paso final en la creación de un plan de ciberseguridad es el comienzo de un apoyo continuo a la estrategia de seguridad. Los factores amenazantes continuarán explotando vulnerabilidades, por lo que la estrategia de ciberseguridad tiene que ser monitoreada y probada regularmente para garantizar que los objetivos del plan vayan de acorde con el panorama de amenazas.

Los objetivos de la estrategia para el plan de ciberseguridad no suelen cambiar, ya que deben alinearse con los objetivos del negocio; sin embargo, el panorama de amenazas cambia frecuentemente. Se debe revisar la estrategia para determinar si existen fallos en el programa; por lo que, un seguimiento anual es un período de revisión generalmente aceptado.

En definitiva, la importancia de un **Plan de Ciberseguridad** radica en la ayuda que proporciona a reducir los riesgos con respecto a la ciberseguridad de una empresa. Al mismo tiempo, establece una línea de base para el programa de seguridad de una empresa que permite adaptarse continuamente a las amenazas y riesgos emergentes, anticipando en lo posible la violación de datos de terceros.

Anexo IV. Gestión de incidentes

Como se ha indicado anteriormente en el presente proyecto (apartado 4.4.1.) otra medida de carácter preventivo es contar con un Plan de Actuación o Respuesta ante Incidentes, cuyas fases se explican más detalladamente a continuación [8]:

Figura 0-2. Fases de Gestión de un Ciberincidente.

Fuente: Guía nacional de notificación y gestión de ciberincidentes. (2020, 21 febrero). Aprobado por el Consejo Nacional de Ciberseguridad. Gobierno de España. Obtenido de https://www.incibe-cert.es/sites/default/files/contenidos/guias/doc/guia_nacional_notificacion_gestion_ciberincidentes.pdf

1. PREPARACIÓN

En esta fase inicial, toda entidad debe estar preparada para cualquier suceso que pudiera ocurrir. Una buena anticipación y entrenamiento previo es clave para realizar una gestión eficaz de un incidente, para lo que hace falta tener en cuenta tres pilares fundamentales: las personas, los procedimientos y la tecnología.

Algunos de los puntos más relevantes en esta fase son:

- Disponer de información actualizada de contacto, tanto de personal interno como externo, a implicar en otras fases de gestión del ciberincidente, así como las distintas vías de contacto disponibles en cada caso.
- Mantener las políticas y procedimientos actualizados; especialmente todos los relativos a gestión de incidentes, recogida de evidencias, análisis forense o recuperación de sistemas.
- Herramientas para utilizar en todas las fases de gestión de un ciberincidente.
- Formación del equipo humano para mejorar las capacidades técnicas y operativas.

- Realizar análisis de riesgos que permita disponer de un plan de tratamiento de riesgos que permita controlarlos pudiendo ser mitigados, transferidos o aceptados.
- Ejecución de ciberejercicios a fin de entrenar las capacidades y procedimientos técnicos, operativos, de gestión y coordinación.

2. IDENTIFICACIÓN

El objetivo de esta fase es tener la capacidad de identificar o detectar cualquier ciberincidente que pueda sufrir una organización, para lo cual es importante realizar una monitorización lo más completa posible. Además, se debe tener en cuenta de que no todos los eventos o alertas de ciberseguridad son ciberincidentes.

Una correcta identificación o detección se basa en los siguientes principios:

- Registrar y monitorizar los eventos de las redes, sistemas y aplicaciones.
- Recolectar información situacional que permita detectar anomalías.
- Disponer de capacidades para descubrir ciberincidentes y comunicarlos apropiadamente.
- Recopilar y almacenar de forma segura todas las evidencias.
- Compartir información con otros equipos internos y externos de forma bidireccional para mejorar las capacidades de detección.

3. CONTENCIÓN

En el momento que se ha identificado un ciberincidente la máxima prioridad es contener el impacto en la organización de forma que se puedan evitar la propagación a otros sistemas o redes evitando un impacto mayor, y la extracción de información fuera de la organización.

En esta fase se evalúa toda la información disponible para realizar una clasificación y priorización del ciberincidente en función del tipo y de la criticidad de la información y los sistemas afectados. Seguidamente, se identifican posibles impactos en el negocio y en función de los procedimientos se trabaja en la toma de decisiones con las unidades de negocio apropiadas y/o a los responsables de los servicios potencialmente afectados.

Durante esta fase se debe:

- Registrar y monitorizar los eventos de las redes, sistemas y aplicaciones.
- Recolectar información situacional que permita detectar anomalías.
- Disponer de capacidades para descubrir ciberincidentes y comunicarlos a los contactos apropiados.
- Recopilar y almacenar de forma segura todas las evidencias.
- Compartir información con otros equipos internos y externos de forma bidireccional para mejorar las capacidades de detección.

4. MITIGACIÓN

Las medidas de mitigación dependerán del tipo de ciberincidente, ya que en algunos casos será necesario contar con apoyo de proveedores de servicios y en otros ciberincidentes puede suponer incluyo el borrado completo de los sistemas afectados y recuperación desde una copia de seguridad.

A pesar de que las medidas de mitigación dependen del tipo de ciberincidente y su afectación, algunas recomendaciones en esta fase son:

- Determinar las causas y los síntomas del ciberincidente para determinar las medidas de mitigación más eficaces.
- Identificar y eliminar todo el software utilizado por los atacantes. A menudo la forma que ofrece más garantías de eliminar todo rastro de un incidente pasa por un nuevo plataformado de la máquina.
- Recuperación de la última copia de seguridad limpia.
- Identificar servicios utilizados durante el ataque, ya que en ocasiones los atacantes utilizan servicios legítimos de los sistemas atacados.

5. RECUPERACIÓN

La finalidad de la fase de recuperación consiste en recuperar la información y la actividad normal de la empresa lo antes posible (Figura 0-2). Por ello, es importante no precipitarse en la puesta en producción de sistemas que se han visto implicados en ciberincidentes. Conviene prestar especial atención a estos sistemas durante la puesta en producción y buscar cualquier actividad sospechosa, definiendo un período de tiempo con medidas adicionales de monitorización [38].

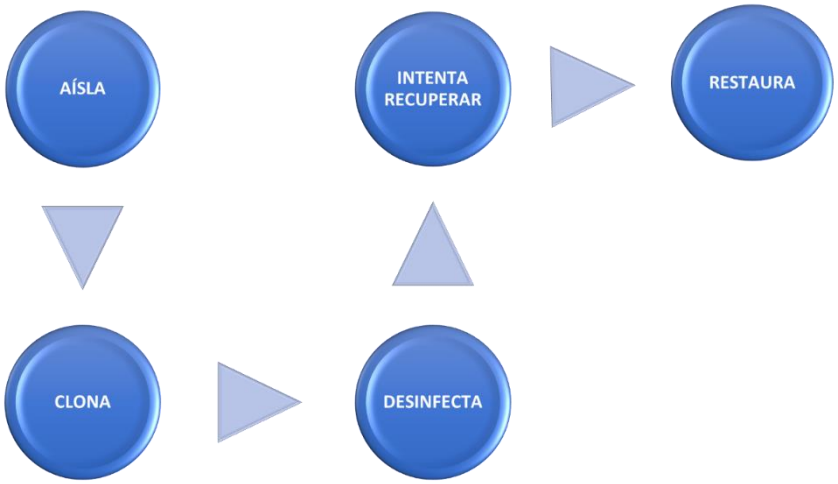


Figura 0-3. Cómo recuperarse de un ataque por ransomware.

Fuente. Elaboración propia a partir RANSOMWARE. Una guía de aproximación para el empresario. (2021, 20 de abril). Obtenido a partir de https://www.incibe.es/protege-tu-empresa/guias/ransomware-guia-aproximacion-el-empresario

Aislar los equipos. El aislamiento inmediato de los equipos infectados evitará que el ciberataque se propague a otros dispositivos. No se debe confiar en discos duros, unidades de red o servicios en la nube que estén conectados por si el ransomware se hubiera propagado y los hubiera infectado:

- Cambiar, lo antes posible, todas las contraseñas de red y de cuentas online. La contraseña debe ser robusta, fuerte y única para cada servicio.

Clonar los discos duros. La clonación de los discos duros de los equipos infectados debe ser completa para mantener el dispositivo original e intentar recuperar los datos sobre el clon:

- Conectar el disco duro del equipo afectado a otro ordenador aislado de la red y no arrancar con él, utilizarlo solo para comprobar qué información se ha salvado y hacer una copia. Salvar solo los datos importantes (documentos, fotos, certificados…), en lugar de archivos ejecutables o programas que puedan volver a infectar al equipo.
- Recoger y aislar muestras de ficheros cifrados o del propio ransomware, como el fichero adjunto en el mensaje desde el que nos infectamos.
- Cambiar el disco duro afectado, extraerlo y conservarlo como prueba por si, apareciera una solución de descifrado de la información que permitiera recuperar su contenido.
- Denunciar el incidente ante la Guardia civil o la Policía Nacional.

Desinfectar el disco clonado. Para desinfectar el disco clonado se debe utilizar una herramienta antivirus o antimalware actualizada eliminando el software malicioso y sus posibles persistencias antes de recuperar los datos, ya que, de lo contrario, podrían volver a ser cifrados.

Recuperar y restaurar los equipos. Para poder continuar con la actividad se debe reinstalar el equipo con el software original o arrancar en modo seguro y recuperar un *backup* previo si fuera posible.

6. ACTUACIONES POST-INCIDENTE

Una vez controlado el ciberincidente y la actividad vuelve a la normalidad, es momento de llevar a cabo un proceso al que no se le suele dar toda la importancia merecida: las lecciones aprendidas.

Conviene pararse a reflexionar sobre lo sucedido, analizando las causas del problema, cómo se ha desarrollado la actividad durante la gestión del ciberincidente y todos los problemas asociados a la misma. La finalidad de este proceso es aprender de lo sucedido y tomar las medidas adecuadas para evitar que una situación similar se pueda repetir, además de mejorar los procedimientos.

Por último, se realizará un informe del ciberincidente que deberá detallar la causa del ciberincidente y coste (especialmente, en términos de compromiso de información o de impacto en los servicios prestados), así como las medidas que la organización debe tomar para prevenir futuros ciberincidentes de naturaleza similar.