Análisis de soluciones comerciales anti-ransomware para pymes

Nombre Estudiante
Antonio Dueñas Maribello

Nombre del Programa
Máster Universitario en Ciberseguridad y Privacidad

Área de trabajo final
Privacidad

Nombre Tutor/a de TF
Albert Jové Canela

Profesor/a responsable de la asignatura
Andreu Pere Isern Deyà

Fecha Entrega
17/06/2023

Universitat Oberta de Catalunya

FICHA DEL TRABAJO FINAL

Título del trabajo:	*Análisis de soluciones comerciales anti-ransomware para pymes*
Nombre del autor:	*Antonio Dueñas Maribello*
Nombre del consultor/a:	*Albert Jové Canela*
Nombre del PRA:	*Andreu Pere Isern Deyà*
Fecha de entrega (mm/aaaa):	*17/06/2023*
Titulación o programa:	Máster Universitario en Ciberseguridad y Privacidad
Área del Trabajo Final:	*Privacidad*
Idioma del trabajo:	*Castellano*
Palabras clave	*Ransomware, protección de datos, pyme*

Resumen del Trabajo

Los sistemas informáticos y las redes de comunicaciones tienen vulnerabilidades y sufren ataques que cada vez son más complejos y sofisticados.

Uno de estos ataques es el llamado ransomware y su objetivo es secuestrar los datos a cambio de un rescate.
Cada vez el ransomware está más presente en los medios de comunicación porque afecta a todos, tanto a empresas como usuarios/as.
Las empresas grandes tienen más recursos técnicos y económicos para defenderse, pero no es el caso de las pymes.

¿Qué soluciones informáticas anti-ransomware existen en el mercado para las pymes? ¿Qué problemas pueden solucionar? ¿Son fáciles de usar para gente no técnica? ¿Son efectivas? ¿Son económicas?
Este Proyecto Final de Máster quiere dar respuesta a estas preguntas mediante el análisis de diferentes soluciones de seguridad para pymes que hay en el mercado.
A través de los resultados de la encuesta realizada para conocer que entornos tecnológicos, conocimientos y soluciones de seguridad tienen las pymes y más concretamente, sobre el ransomware, se ha montado un laboratorio de seguridad informática para probar ransomware real mediante ataques de phishing por correo electrónico, siguiendo una metodología de trabajo y mostrando los resultados del análisis de las soluciones anti-ransomware, además de hacer unas recomendaciones.

Abstract

Computer systems and communications networks are not exempt from vulnerabilities and attacks and are becoming complex and sophisticated.

One of these attacks is called ransomware and its goal is to hijack data in exchange for a ransom.
Ransomware is increasing his presence in the media because it affects everyone, companies and users.
Large companies have more technical and economic resources to defend against it, but this is not the case of small and medium businesses SME.

What anti-ransomware solutions are there on the market for SME? What problems can they solve? Are they easy to use for non-technical people? Are they effective? Are they economical?
This Master's Final Project aims to answer these questions by analysing different security solutions for SMEs on the market.
Based on the results of the survey carried out to find out what technological environments, knowledge and security solutions SMEs have and, more specifically, about ransomware, a computer security laboratory has been set up to test real ransomware through phishing attacks by email, following a working methodology and showing the results of the analysis of anti-ransomware solutions, as well as making some recommendations.

Agradecimientos

A Yolanda por su contribución a mi vida y a este proyecto, a mi madre que está siempre conmigo, a mi padre, familia, amigos y amigas.

A Josep Albors y Guiu Ocón por darme su apoyo para que podamos divulgar y concienciar sobre la importancia de la seguridad informática.

A mi tutor Albert Jové, a Alberto, Ana María, Marta, José María, Rich y a las personas que en mayor o menor medida han participado en este trabajo, que es el inicio de algo nuevo que puede continuar.

Y a todas las pymes que han colaborado en la encuesta.

Índice

Lista de figuras

1. Introducción

Los ordenadores han tenido virus informáticos para fines de investigación desde el mismo origen de la computación. Estos virus tienen un funcionamiento similar a un virus biológico, se reproducen, se protegen, consumen recursos y ejecutan unas órdenes para causar daños.

Después apareció Internet, la red de redes que fue creada inicialmente para consultar y compartir información.

Ha ido evolucionando a lo que es hoy en día, gracias al aumento de la velocidad de las comunicaciones con tecnologías como la fibra óptica y ha ido extendiendo su uso no sólo al ámbito militar o educativo, sino también a las empresas y al público en general.

Ahora es posible hacer compras en línea, operaciones bancarias, trámites y gestiones administrativas tanto con la Administración Pública como con las empresas privadas, consultar el historial médico, estudiar a distancia, ver TV y escuchar música a la carta y más servicios.

Así los virus pueden propagarse por Internet y tener acceso a los datos de muchos sistemas informáticos (ordenadores, portátiles, móviles y servidores).

Los datos que viajan por Internet tienen un valor que se debe proteger, igual que se protege cualquier propiedad. Habrá datos con más valor y otros con menos y muchos datos según su naturaleza y criticidad, han de cumplir unas medidas de seguridad y normativas superiores al resto.

Las empresas, independientemente de su tamaño, ya sean pequeñas, medianas o grandes y los/las particulares han de guardar y proteger sus datos porque los sistemas informáticos, las redes de comunicaciones y los servicios en la nube (cloud) sufren ataques a diario y no están exentos de vulnerabilidades que se van corrigiendo a medida que se van encontrando.

Uno de los ataques que últimamente está más presente en los medios de comunicación es el ransomware, que está afectando a muchas empresas de diferentes sectores y tamaños.
Su objetivo consiste en secuestrar los datos y liberarlos a cambio de una cantidad de dinero que puede ser importante.

Las empresas grandes tienen recursos técnicos y económicos para defenderse del ransomware. ¿Qué recursos tienen las pymes? ¿Cómo pueden defenderse? ¿Qué pueden hacer en caso de ser atacados?

1.1. Contexto y justificación del Trabajo

El ransomware es uno de los ataques informáticos más frecuentes y que más ha aumentado en los últimos años. También ha aumentado la cantidad de datos robados. Lo dice el último informe sobre cibercriminalidad en España 2021 publicado por el Ministerio del Interior [1].
(Nota: El ransomware aplicaría a Intrusión, Malware, Robos de información porque el ransomware es una intrusión o acceso no autorizado a los sistemas, un tipo de malware que roba información para pedir un rescate, a modo de secuestro).

>> 3.1. Incidentes gestionados por el INCIBE-CERT

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 1. Incidentes gestionados por el INCIBE-CERT (extraído del Informe sobre cibercriminalidad en España 2021, pág. 40 [1]

También lo dice el último informe de la Agencia de la Unión Europea para la Ciberseguridad ENISA llamado “Thread Landscape 2022” de Noviembre de 2022

Figure 12 Time series of ransomware incidents from May 2021 to June 2022. In red bars the number of ransomware incidents is shown. In blue bars the cumulative amount of stolen data is shown

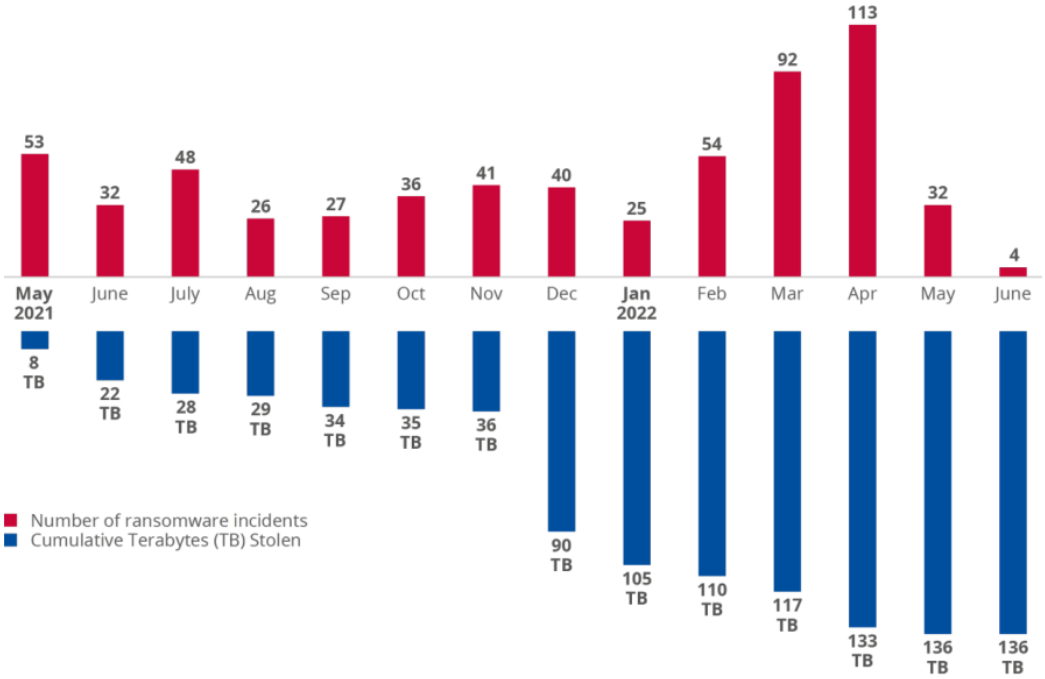


Figura 2. Incidentes de ransomware desde Mayo 2021 hasta Junio 2022 (extraída de ENISA Thread Landscape 2022 (November 2022), pág. 44 [2]

Y el informe de "The State of Ransomware in 2023" de BlackFog [2], empresa que recibió el premio de oro al mejor boletín de ciberseguridad del Año en la 19ª edición de los Premios Anuales de Ciberseguridad 2023 Globee por este informe.

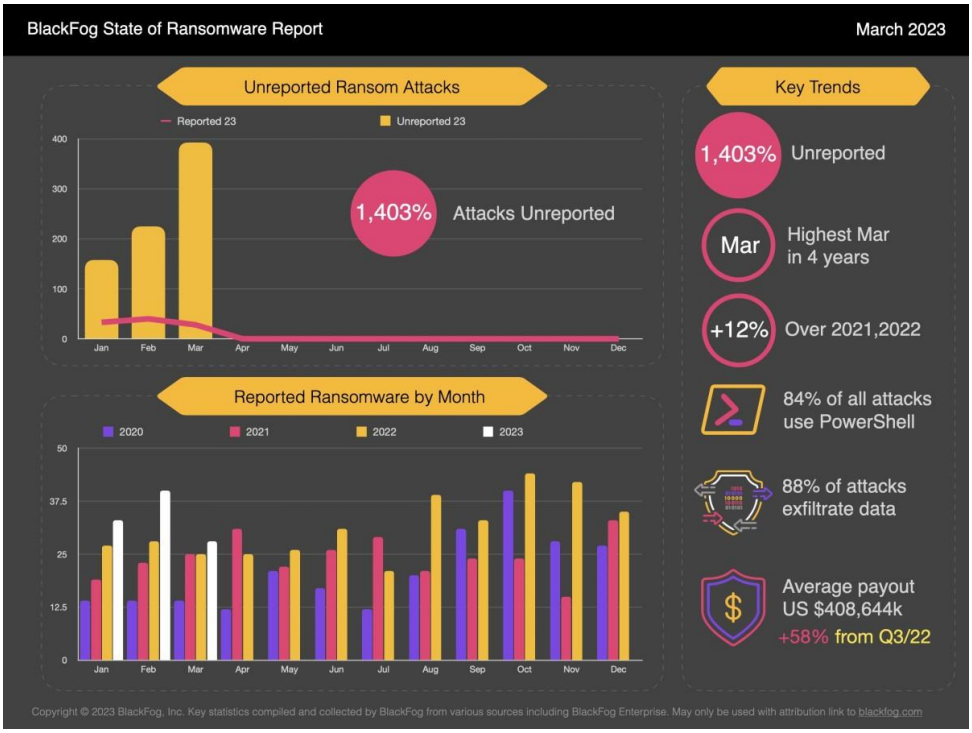


Figura 3. Informe de "The State of Ransomware in 2023" de BlackFog

El principal motivo del aumento de ataques de ransomware es debido a su rentabilidad, porque la víctima paga.

Existe un aumento de robos de la información, más que de ataques en sí, porque es más rentable la venta de los datos obtenidos que los ingresos por el rescate.

Este tipo de ataques está íntimamente relacionado con la protección de datos personales, por lo que hay que informar de ellos a las autoridades pertinentes (en España, es la Agencia Española de Protección de Datos, AEPD [3] o las autoridades autonómicas) por las consecuencias que pueden producirse por la fuga de información, teniendo un impacto empresarial y también en la continuidad de negocio.

De ahí la importancia de hacer un Trabajo Final de Máster sobre ransomware para comprender mejor las causas y los efectos de este tipo de ataques, encontrar soluciones para prevenirlos y ver cómo recuperarse en caso de haberlos sufrido dentro del contexto de una pyme.

Además, estos conocimientos e información son aplicables a otros ataques informáticos que también entran dentro de los sistemas para causar daños o robar datos.

1.2. Objetivos del Trabajo

El primer objetivo del análisis de las soluciones comerciales anti-ransomware que existen en el mercado para las pymes. es **conocer qué es el ransomware**, cómo se define, enumerar los tipos de ransomware que existen, explicar el funcionamiento del ransomware, qué medidas preventivas se pueden aplicar y en caso de sufrir un ataque, cómo poderse recuperar, algunos ejemplos de ransomware relevantes y sus características, y las responsabilidades legales que tienen las empresas en caso de sufrir un ataque.

El siguiente es estudiar como son las empresas **pymes**, para saber qué entornos tecnológicos tienen, su nivel de conocimientos en materia de seguridad informática y más concretamente de ransomware, qué presupuesto tienen para seguridad informática, qué soluciones tienen implementadas y las políticas de seguridad que tienen definidas.

Otro de ellos es **analizar** las diferentes **soluciones comerciales anti-ransomware para pymes** a nivel de características, funcionalidades, usabilidad, coste, efectividad y adecuación al entorno pyme.

Y el último objetivo es dar unas **recomendaciones** fruto del análisis anterior, con información técnica para personas con conocimientos técnicos y sin ellos, y que servirá de ayuda para la elección de productos y soluciones de diferentes fabricantes.

1.3. Impacto en sostenibilidad, ético-social y de diversidad

Las Naciones Unidas (ONU) aprobaron en 2015 la **Agenda 2030 sobre el Desarrollo Sostenible** para poder hacer diferentes acciones que mejoren la vida de todos y todas.

Esa Agenda tiene los llamados **17 Objetivos de Desarrollo Sostenible** (ODS) [4] y uno de ellos está relacionado con la Educación, el **ODS 4 Educación de Calidad** [5] cuyo objetivo es garantizar una educación inclusiva, equitativa y de calidad y promover oportunidades de aprendizaje durante toda la vida para todos.

En su apartado 4.7 dice "De aquí a 2030, asegurar que todos los alumnos adquieran los conocimientos teóricos y prácticos necesarios para promover el desarrollo sostenible, entre otras cosas mediante la educación para el desarrollo sostenible y los estilos de vida sostenibles, los derechos humanos, la igualdad de género, la promoción de una cultura de paz y no violencia, la ciudadanía mundial y la valoración de la diversidad cultural y la contribución de la cultura al desarrollo sostenible".

Una forma de desarrollar este apartado por parte de las Universidades es a través de las competencias de compromiso ético y global (CCEG).

La competencia de compromiso ético y global para estudios de Máster está definida como:
"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".
(Fuente: Documento "Guia transversal sobre la CCEG per a estudiants de TFx-EIMT" de la UOC)

Trabaja en tres grandes dimensiones:

- Sostenibilidad
- Comportamiento ético y responsabilidad social
- Diversidad y derechos humanos

Y cada una de estas dimensiones abarca diferentes objetivos de desarrollo sostenible.

Este Trabajo puede aplicar los siguientes ODS que se incluyen en las diferentes dimensiones:

I. Dimensión Sostenibilidad

- **ODS 7 Energía asequible y no contaminante** [6]. Las soluciones anti-ransomware pueden proteger los sistemas de energía que son infraestructuras críticas y uno de los objetivos de los atacantes.

- **ODS 9 Industria, innovación e infraestructura** [7]. Las soluciones anti-ransomware pueden proteger la infraestructura de la industria, evitando interrupciones de servicio que pueden afectar a la economía productiva.

- **ODS 11 Ciudades y comunidades sostenibles** [8]. Las soluciones anti-ransomware pueden proteger los sistemas críticos de los servicios urbanos de las ciudades como el transporte público, suministro de agua, gestión de residuos, … para que sean lugares seguros y sostenibles.

- **ODS 12 Producción y consumo responsables** [9]. Las soluciones anti-ransomware pueden proteger los sistemas de producción y suministro de bienes y servicios ayudando a reducir el desperdicio y los residuos.

- **ODS 13 Acción por el clima** [10]. Las soluciones anti-ransomware pueden ayudar a proteger infraestructuras críticas e interrupciones de suministro de energía, que en caso de producirse, provocarían un aumento en la demanda de energía y por tanto más emisiones que afectarían al cambio climático.

- **ODS 14 Vida submarina** [11]. Los sistemas anti-ransomware pueden proteger los sistemas de navegación, comunicación y control de embarcaciones, importantes para la seguridad de los/las trabajadores/as del mar, además de proteger los ecosistemas marinos. Todo esto ayuda a la conservación y sostenibilidad de los mares y océanos.

- **ODS 15 Vida de ecosistemas terrestres** [12]. Los sistemas anti-ransomware pueden proteger el medio ambiente si permiten que los sistemas de monitorización ambiental, forestal, de gestión de la conservación de la biodiversidad y la recogida de datos ambientales sigan funcionando.

II. Dimensión Comportamiento ético y responsabilidad social

- **ODS 1 Fin de la pobreza** [13]. Los sistemas anti-ransomware pueden evitar interrupciones en las empresas y organizaciones que se encargan de los productos y servicios esenciales como son la alimentación y la salud.

- **ODS 2 Hambre cero** [14]. Los sistemas anti-ransomware pueden evitar interrupciones en el suministro de alimentos, ayudando así a acabar con el hambre.

- **ODS 6 Agua limpia y saneamiento** [15]. Los sistemas anti-ransomware pueden proteger de interrupciones en el suministro y saneamiento de agua y así favorecer la gestión del agua.

- **ODS 8 Trabajo decente y crecimiento económico** [16]. Los sistemas anti-ransomware pueden prevenir interrupciones en la actividad empresarial y el trabajo, ayudando así al crecimiento económico.

- **ODS 16 Paz, justicia e instituciones sólidas** [17]. Los sistemas anti-ransomware pueden proteger las infraestructuras tecnológicas que pueden dar seguridad y estabilidad social, además de proteger la privacidad y los datos personales.

III. Dimensión Diversidad y derechos humanos

- **ODS 5 Igualdad de género** [18]. Los sistemas anti-ransomware pueden proteger a las organizaciones y servicios que trabajan en temas de igualdad de género, además de ayudar a que niñas y mujeres puedan usar tecnología de forma más segura.

- **ODS 10 Reducción de las desigualdades** [19]. Los sistemas anti-ransomware pueden ayudar a las personas más vulnerables y con menos recursos (**como es el caso de las pymes, objeto de este Trabajo**) a seguir funcionando sin interrupciones.

También hay que comentar que cualquier protección de seguridad informática como puede ser una solución anti-ransomware usa recursos de computación que se ejecutan continuamente en tiempo real para poder detectar los ataques y este proceso tiene un consumo energético.
Y como cada vez los ataques son más sofisticados y constantes, se necesitan de más recursos.

Y que el proceso de recuperación de un ataque de ransomware también requiere de un consumo energético extra para ejecutar una herramienta de desencriptación o recuperar los datos de las copias de seguridad.

1.4. Enfoque y método seguido

Para realizar este Trabajo y poder conseguir los objetivos marcados, se hacen tareas de investigación y búsqueda de información en Internet a fuentes importantes, especialistas y relevantes en la materia.

También se realiza un trabajo de campo en forma de encuesta online que se envía a pymes de diversos sectores y tamaños de toda España. Y se complementa con diversos informes sobre las pymes que se han seleccionado de Internet bajo unos criterios que se describen dentro de su apartado.

Además, se crea un **laboratorio de seguridad informática** con los entornos tecnológicos de las pymes obtenidos de la encuesta y los informes, donde se prueba ransomware real en un entorno controlado y se analiza el funcionamiento de las soluciones anti-ransomware elegidas bajo unos criterios y siguiendo una metodología que se describe dentro del análisis.

1.5. Planificación del Trabajo

- **Fase 1: Plan de Trabajo**
  - Presentación del problema a resolver.

- Objetivos para conseguir con la realización del Trabajo.
- Descripción del enfoque y la metodología que se usa durante el desarrollo del Trabajo.
- Listado de las tareas a realizar para conseguir los objetivos descritos.
- Planificación temporal de las tareas y sus dependencias.
- Primera parte del estado del arte

- **Fase 2: Desarrollo del Trabajo**
  - Segunda parte del estado del arte
  - Elaboración y envío de la encuesta
  - Selección de las soluciones comerciales anti-ransomware a analizar
  - Selección del ransomware real a analizar
  - Estudio y preparación del laboratorio de seguridad informática

- **Fase 3: Ejecución del Trabajo**
  - Instalación y configuración del laboratorio de seguridad informática
  - Instalación y configuración de las soluciones comerciales anti-ransomware seleccionadas
  - Ejecución del ransomware en el laboratorio.
  - Análisis de las soluciones comerciales anti-ransomware

- **Fase 4: Cierre del Trabajo**
  - Recogida de datos de la encuesta
  - Elaboración del informe resumen de la encuesta
  - Recogida de los resultados del análisis.
  - Redacción de las conclusiones
  - Planteamiento de futuros trabajos
  - Lectura y revisión de la memoria del TFM

Se puede ver la planificación temporal de las tareas mediante un diagrama de Gantt realizado con el software GanttProject que está en el Anexo I.

1.6. Breve sumario de productos obtenidos

El presente Trabajo genera los siguientes productos:

- Estado del arte del ransomware
- Encuesta de elaboración propia sobre pymes y ransomware y resumen con la información obtenida
- Análisis de las soluciones comerciales anti-ransomware para pymes, objeto de este Trabajo.
- Análisis de soluciones anti-ransomware existentes a nivel internacional y nacional.
- Conclusiones del análisis de soluciones comerciales anti-ransomware para pymes.

1.7. Breve descripción de los otros capítulos de la memoria

- **Capítulo 1. Introducción:**

Contiene el contexto y justificación del Trabajo, los objetivos del Trabajo, el impacto en sostenibilidad, ético-social y de diversidad, el enfoque y método seguido para la realización del Trabajo, la planificación del Trabajo y un breve sumario de productos obtenidos.

- **Capítulo 2. Estado del arte**
  Contiene una serie de definiciones de ransomware, los tipos de ransomware que existen, los mecanismos de actuación, las medidas preventivas y reactivas, ejemplos y responsabilidad legal ante el ransomware.
- **Capítulo 3. Análisis**
  Contiene los entornos de trabajo de las pymes que serán analizados a partir de la información de la encuesta, la descripción del laboratorio de seguridad informática, las muestras de ransomware usadas, la metodología de trabajo y la puesta en marcha y análisis de las soluciones anti-ransomware.
- **Capítulo 4. Resultados**
  Contiene los resultados del análisis de soluciones comerciales anti-ransomware para pymes.
- **Capítulo 5. Conclusiones y trabajos futuros**
  Contiene las conclusiones del análisis de soluciones anti-ransomware, así como los posibles trabajos futuros o continuación de este.
- **Capítulo 6. Glosario**
  Contiene las palabras técnicas y definiciones usadas en el Trabajo.
- **Capítulo 7. Bibliografía**
  Contiene la bibliografía y webs usadas para la elaboración del Trabajo.
- **Capítulo 8. Anexos**
  Contiene la información anexa del Trabajo.

2. Estado del arte

El estado del arte en un Trabajo Final de Máster sirve para explicar en qué punto se encuentra un tema desde el punto de vista académico, revisando los trabajos previos al estudio, argumentando la elección de estos y su relación con la investigación, además de lo que pueden aportar a la misma.

Para nuestro caso, se dan unas definiciones de ransomware, se explican los diferentes tipos de ransomware que existen, sus mecanismos de actuación y las medidas preventivas y reactivas que hay ante el ransomware.

También se aportan diversos análisis que existen de soluciones comerciales anti-ransomware para pymes, las pruebas realizadas y los resultados obtenidos.

2.1. Definición de ransomware

Existen muchas definiciones de ransomware, para un público con mayor o menor conocimiento técnico sobre el tema.

Y en un contexto de pymes, normalmente los conocimientos técnicos en seguridad informática no son muy especializados.

Se han seleccionado diversas definiciones de ransomware de los mayores expertos en seguridad informática que son los fabricantes de soluciones de seguridad y de ellos, los que tienen en su portfolio, soluciones para pymes.

Y también, se han seleccionado definiciones de los organismos y fuerzas de seguridad que no tienen intereses comerciales y son conocedores del tema, al tener equipos especializados de ciberseguridad, porque se enfrentan a diario a ataques informáticos. Además, tienen un sentido de servicio de ayuda a los/las ciudadanos/as, divulgación y concienciación, aspectos importantes en este Trabajo.

A continuación, se detallan las mejores empresas de seguridad informática según AV-TEST, empresa independiente de análisis de seguridad informática, a las que ha otorgado un premio en 2022 (AV-TEST Award 2022 [20]). Éstas han escrito unas definiciones de ransomware que se pueden consultar en la bibliografía a través de las siguientes referencias:

Mejores empresas de seguridad informática según AV-TEST
Sophos [21] Empresa británica (UK) de software y hardware de seguridad. Desarrolla productos para puntos finales de comunicación (endpoints), cifrado, seguridad de redes y seguridad del correo electrónico
Bitdefender [22]

Empresa con sede central en Rumanía que desarrolla y ofrece productos y servicios de ciberseguridad, incluyendo protección de endpoints, seguridad gestionada y en la nube, software antivirus y seguridad IoT
Kaspersky [23] Empresa rusa que desarrolla y comercializa antivirus, seguridad en Internet, gestión de contraseñas, seguridad para puntos finales y otros productos y servicios de ciberseguridad
Microsoft [24] Empresa con sede central en Estados Unidos que desarrolla software, incluyendo soluciones de seguridad
McAfee [25] (ahora **Trellix**) Empresa con sede central en Estados Unidos que desarrolla hardware, software y servicios para investigar ataques de ciberseguridad, proteger contra software malicioso y analizar riesgos de seguridad informática
Norton [26] Empresa con sede central en Estados Unidos que desarrolla soluciones antivirus y antimalware
Trend Micro [27] Empresa japonesa que desarrolla software de seguridad empresarial para servidores, contenedores y entornos de computación en nube, redes y puntos finales

AV-Comparatives, empresa independiente de análisis de seguridad informática también tiene un premio en 2022 a las mejores empresas de ciberseguridad (AV-Comparatives Awards 2022 [28]) y muchas de ellas también han ganado los premios de AV-TEST.
A continuación, se detallan las empresas ganadoras diferentes y las referencias a sus definiciones de ransomware:

Mejores empresas de seguridad informática según AV-Comparatives
ESET [29] Empresa con sede central en **República** Checa que desarrolla software de seguridad
Panda Security (adquirida por **WatchGuard** [30]) Empresa con sede central en Estados Unidos que desarrolla software de seguridad

También se detallan los organismos y fuerzas de seguridad más relevantes a nivel autonómico, nacional e internacional y las referencias a sus definiciones de ransomware:

Organismos y fuerzas de seguridad
Agència de Ciberseguretat de Catalunya [31] Agencia encargada de establecer el servicio público de ciberseguridad y trabaja para garantizar y aumentar el nivel de seguridad de las redes y los sistemas de información en Cataluña, así como la confianza digital de la ciudadanía
Instituto Nacional de Ciberseguridad de España **INCIBE** [32] Es una sociedad mercantil estatal que se dedica a dar soporte en materia de seguridad informática a los ciudadanos, empresas públicas y privadas, así como

a las administraciones públicas y sus organismos, y a las instituciones académicas y de investigación, especialmente aquellas que gestionan infraestructuras críticas
Agencia de la Unión Europea para la Cooperación Policial **Europol** [33] Órgano encargado de facilitar las operaciones de lucha contra la delincuencia en el seno de la Unión Europea (UE)
Agencia de la Unión Europea para la Ciberseguridad **ENISA** [34] Agencia para mejorar las redes y la seguridad de la información en la Unión Europea
Organización Internacional de Policía Criminal **Interpol** [35] Organización que se centra en la seguridad pública, terrorismo, crimen organizado, tráfico de drogas, tráfico de armas, tráfico de personas, lavado de dinero, pornografía infantil, delitos económicos y corrupción.
National Cyber Security Centre **NCSC** [36] Organización del Gobierno del Reino Unido que ofrece asesoramiento y apoyo a los sectores público y privado sobre cómo evitar las amenazas a la seguridad informática.
Federal Bureau of Investigation **FBI** [37] Servicio de seguridad y de inteligencia nacional de Estados Unidos
National Institute of Standards and Technology **NIST** [38] Agencia para promover la innovación y la competencia industrial en Estados Unidos
Cybersecurity and Infrastructure Security Agency **CISA** [39] Agencia del Departamento de Seguridad Nacional de Estados Unidos que se encarga de reforzar la ciberseguridad y la protección de infraestructuras en todos los niveles de la Administración.

2.2. Tipos de ransomware

Hasta no hace mucho había 2 tipos de ransomware [40]:

1. **Ransomware de cifrado** (crypto ransomware ó encryptor): Este tipo de ransomware encripta los archivos de la víctima y solicita un rescate para proporcionar la clave de descifrado. Es el tipo más común.

2. **Ransomware de bloqueo de sistema** (locker ransomware): Este tipo de ransomware bloquea la pantalla (screen locker) del dispositivo o el sistema operativo y muestra un mensaje que indica que se ha cometido una infracción y que se debe pagar un rescate para desbloquear el dispositivo.

Pero los ataques de ransomware están evolucionando y llegando a las empresas y usuarios/as de nuevas formas [41]:

3. **Scareware** Crea un mensaje falso sobre virus que infectan el ordenador o dispositivo de un usuario y normalmente se solicita un pago al propietario para resolver los problemas que son falsos. También se le llama “virus de la policía”.

4. **Ransomware de filtración de datos** (leakware ó extorsionware): Este tipo de ransomware roba datos sensibles de la víctima y amenaza con

publicarlos o venderlos a menos que se pague un rescate. Puede ser una evolución del ransomware de bloqueo de sistema. Y también convertirse en un ransomware de doble y triple extorsión donde no solo cifra los archivos del sistema, sino que también amenaza con publicar información confidencial si no se paga el rescate.

5. **Ransomware como servicio** (RaaS) [42]: Es un modelo de negocio creado para ayudar a los hackers a agilizar sus ataques automatizando las tareas, desde el envío del ransomware, hasta el cobro de los pagos y la restauración del acceso de los usuarios. De esta manera, los ciberdelincuentes que quieren realizar el ataque y no tienen el nivel técnico para hacerlo, contratan el servicio de un kit de RaaS en la Web Oscura (Dark Web [43]) y lo ponen en funcionamiento.

También existen las llamadas **familias de ransomware** que son grupos de programas maliciosos que comparten características comunes en su diseño y funcionamiento, y que se utilizan para llevar a cabo ataques de ransomware.
Están relacionadas con el RaaS.

2.3. Funcionamiento del ransomware

Los ataques de ransomware son muy eficaces porque el atacante estudia a la víctima para hacer acciones que bloquean, cifran, eliminan o roban activos (Lock, Encrypt, Delete or Steal (LEDS)), tal como explica ENISA [44].

El ransomware funciona siguiendo unas fases [45] [46] :

1. El atacante obtiene el acceso a la red:
   Mediante un software descargable, donde se aprovecha de una vulnerabilidad o añade un programa malicioso, una web o mensaje de correo electrónico de tipo phishing [47] se consigue entrar en la red.

2. Escalada de privilegios:
   Sirve para obtener acceso a niveles más altos de privilegios en un sistema comprometido. Normalmente se hace explotando una vulnerabilidad del sistema o mediante una aplicación instalada.
   El atacante una vez dentro de la red consigue tener permisos de administrador de sistemas y así poder escalar privilegios y ejecutar cualquier programa.
   De esta forma se pueden saltar los controles de seguridad y los permisos de usuario para cifrar archivos importantes o extenderse a otros sistemas.

3. Evasión de defensas:
   El ransomware puede usar técnicas de ofuscación de código para ocultar su verdadera funcionalidad y evitar su detección por parte de los programas antivirus.
   Puede usar ataques de día cero (day zero) que son vulnerabilidades desconocidas y que no podrían ser detectadas por los antivirus.
   También aprovecharse de herramientas de administración remota para infiltrarse en los sistemas.

Y además, el ransomware puede de detectar si se está ejecutando en un entorno de pruebas (sandbox) y puede evitar ser detectado.
Una vez el atacante está dentro del sistema, le interesa que no salten las alarmas y como ahora tiene permisos de administrador, puede desactivarlas o desinstalar el software de seguridad que exista.

4. Descubrimiento de la red:
   Para conocer bien el entorno de la víctima, es necesario saber qué arquitectura tiene a nivel de servidores y equipamiento de red y seguridad.
   Para eso el ransomware puede hacer un escaneo de puertos de red para identificar los sistemas vulnerables y los objetivos a atacar.
   También aprovecharse de herramientas de administración remota para infiltrarse en los sistemas.
   Y detectar si se dispone de copias de seguridad que podrían usar para anular el ataque.

5. Movimiento lateral [48]:
   Y para saber más de la red, se usa el movimiento lateral que es el conjunto de técnicas que utilizan los atacantes para que un malware pueda propagarse desde una máquina comprometida a otras máquinas en la misma red.
   Una vez que se escanean los puertos de red y se identifican sistemas vulnerables, se explotan las vulnerabilidades para ganar el acceso a los sistemas, también robando credenciales o aprovechando herramientas de administración remota.

6. Ejecución del ransomware:
   En esta última fase, donde los atacantes cifran los datos y luego exigen un pago para acceder a la clave de descifrado.
   En algunos casos, la ejecución del ransomware puede ser muy rápida, especialmente si se utiliza un exploit para aprovechar una vulnerabilidad en el sistema y descargar y ejecutar el malware de manera eficiente. Pero en otros casos, la ejecución del ransomware puede tomar más tiempo debido a la necesidad de propagarse a través de la red, la detección de software antivirus y medidas de seguridad, y el cifrado de grandes cantidades de archivos.

   Es importante decir que cuanto más tiempo esté el ransomware activo en el sistema, mayor será el daño que puede causar, ya que cifrará más archivos y posiblemente propagará el malware a otros sistemas de la red. Por tanto, es posible que haya pasado bastante tiempo desde la infección, hasta que se produce el ataque final con el cifrado.

2.4. Medidas preventivas ante el ransomware

Los fabricantes de soluciones de seguridad informática Sophos [49], Bitdefender [50], Kaspersky [51], Microsoft [52], McAfee [53], Norton [54], Trend

Micro [55], ESET [29], Watchguard [56] y otras, junto con los organismos y fuerzas de seguridad Agència de Ciberseguretat de Catalunya [57], INCIBE [58], Europol [59], ENISA [60], Interpol [35], National Cyber Security Center (NCSC) [61], FBI [37] (ver también Prevención y respuesta al ransomware para los CISO [62], NIST [63] [64], CISA [39] y más, publican información sobre qué medidas se pueden tomar para prevenir los ataques de ransomware.

Haciendo un resumen de esta información, las medidas preventivas ante el ransomware son:

Seguir prácticas seguras en Internet:

- No hacer clic en enlaces no seguros sin conocer su verdadero origen.
- No abrir archivos adjuntos de correo electrónico sospechosos
- Implementar o activar funciones de bloqueo de anuncios y filtros antispam.
- Evitar revelar información personal

A nivel de sistemas operativos:

- Mantener actualizados el sistema operativo y los programas, sobre todo a nivel de parches y actualizaciones de seguridad
- Utilizar sólo fuentes de descarga conocidas
- Utilizar la autenticación de doble factor (2FA) o multifactor (MFA).
- Utilizar contraseñas robustas y complejas, administradas mediante un gestor de contraseñas y renovarlas periódicamente.
- Limitar los derechos de acceso de las cuentas de usuario y de los Administradores solo con aquellos permisos que necesiten.
    - No utilizar cuentas con permisos de administrador
- Limitar el acceso a las carpetas compartidas de la red en función de las necesidades de la empresa.
- Desactivar los recursos compartidos administrativos.
- Bloquear la ejecución de nuevos procesos desconocidos en los servidores, en excepción de ventanas de administración (Control restrictivo de aplicaciones).
- Considerar la posibilidad de desactivar las macros de los archivos de Microsoft Office.
- Restringir el uso de PowerShell
- Proteger los controladores de dominio (DC)
- Desactivar la sincronización persistente
- Organizar los datos y separar física y lógicamente. Una forma de separar aplicaciones o sistemas críticos es utilizar entornos virtualizados
- Disponer de un sistema de almacenamiento e indexación de logs centralizado.

A nivel de red

- Segmentar la LAN de la empresa en subredes y conectarlas al cortafuegos para limitar el movimiento lateral y el posible impacto del ransomware, u otros ataques, dentro de la red
- Identificar los sistemas de red que están expuestos externamente, ejecutando un escaneado de puertos en las direcciones IP WAN. Identificar cuáles de los sistemas de red están haciendo reenvío de puertos en esos puertos expuestos.
- Supervisar constantemente los registros de red en busca de conexiones externas entrantes y bloquee esas IP en su cortafuegos.
- Los administradores de red deben supervisar los sistemas en tiempo real para detectar cualquier comportamiento sospechoso, como un uso elevado de la CPU.
- Asegurar los siguientes protocolos de red: SSH, FTP, RDP, SMB, VNC, HTTP
- Desactivar o limitar el RDP si no se necesita y utilizar limitación de velocidad, 2FA o una VPN.

A nivel de soluciones de seguridad

- Instalar software antivirus con protección contra ransomware, a ser posible multicapa
- Proteger con contraseña las configuraciones de las soluciones de seguridad para evitar que sean desactivadas por un ciberdelincuente
- Instalar un cortafuegos o firewall
- Instalar detectores de intrusos (IDS)
- Tener filtros de spam para evitar que los emails de phishing lleguen al buzón de los empleados
- Adquirir soluciones de seguridad DNS. Las soluciones de seguridad DNS (Domain Name System) son herramientas y servicios diseñados para proteger y asegurar las comunicaciones y la infraestructura de DNS en una red. El DNS es un protocolo fundamental en Internet que se encarga de traducir los nombres de dominio legibles para los humanos en direcciones IP numéricas Pueden ser de gran utilidad para proteger de malware y phishing entre otras.
- Aislamiento remoto del navegador (Remote browser isolation, RBI). El RBI es una solución de seguridad para proteger los sistemas, donde el navegador de Internet se ejecuta remotamente en un sitio seguro y así no se descargan ni guardan datos de los usuarios.
- Utilizar servicios VPN en redes Wi-Fi públicas

A nivel de copias de seguridad

- Realizar copias de seguridad periódicamente y mantenerlas fuera de la red y en ubicaciones externas donde los atacantes no puedan

encontrarlas. Que sigan la regla 3-2-1, es decir, mantener por lo menos tres copias, en dos formatos distintos y una de las copias en otra ubicación.
- Guardar las copias de seguridad en un lugar diferente al del servidor de ficheros
- Proteger las copias de seguridad con autenticación de doble factor o multifactor
- Automatizar las copias de seguridad siempre que sea posible
- Es fundamental mantener copias de seguridad encriptadas y fuera de línea de los datos, y comprobar periódicamente las copias de seguridad

A nivel de seguridad de otros dispositivos

- Tener visibilidad de los dispositivos de extremo.
- No utilizar nunca memorias USB desconocidas
- No instalar aplicaciones móviles de proveedores/fuentes desconocidas
- Comprobar los dispositivos IoT o cualquier otro dispositivo de red en busca de vulnerabilidades (cámaras CCTV, servidores NAS, routers).
- Invertir en una póliza de seguros que cubra los daños por ataques de ransomware.

A nivel de formación y concienciación

- Aprender de los errores de otros
- Formar a los/as empleados/as en seguridad informática, la identificación de intentos de ingeniería social y correos electrónicos de phishing.

2.5. Medidas reactivas ante el ransomware

Los fabricantes de soluciones de seguridad informática, Sophos [65], Bitdefender [66], Kaspersky [67], Microsoft [68], McAfee [69], Norton [70], ESET [71] y otros, junto con los organismos y fuerzas de seguridad, Agència de Ciberseguretat de Catalunya [57], INCIBE [58], Europol [72], ENISA [73], National Cyber Security Center (NCSC) [74], FBI [75], NIST [38], CISA [76] y más, publican información sobre cómo solucionar los daños producidos por los ataques de ransomware (medidas reactivas).

De forma resumida, las medidas reactivas ante el ransomware son:

Mantener la calma

Localizar dónde ha llegado la intrusión

Detener la propagación

- Aislar y desconectar rápidamente los dispositivos infectados para evitar que el ransomware siga propagándose por la red. Si no es posible aislar

las máquinas, hacer una imagen del sistema y una captura de la memoria y luego apagar los sistemas.
- Cerrar las conexiones entrantes y salientes
- Desconectar los dispositivos de almacenamiento externos
- Desactivar las tareas de mantenimiento porque seguirán ejecutándose según lo programado, independientemente de un ataque de ransomware.

Investigar
- Determinar el vector de ataque, cómo ha entrado y qué grupos lo utilizan normalmente, es decir, iniciar el proceso de caza de la amenaza
- Avisar al asesor jurídico y/o delegado de protección de datos y evaluar si hay que hacer la comunicación
- El Administrador de TI debe recopilar los registros pertinentes y los posibles indicadores de compromiso, como binarios, notas de petición de rescate, direcciones IP, entradas del registro u otros archivos
- Hacer una foto del mensaje de ransomware

Evaluar los daños
- Comprender a qué ha tenido acceso el ransomware en su ordenador.

Proteger y limpiar las máquinas infectadas
- Identificar la cepa del ransomware para identificar eficazmente el código de cifrado que se necesita para desbloquear su dispositivo
- Buscar si existe un descifrador para el ransomware que ha atacado
    - Visitar “The No More Ransom Project” [77], una iniciativa de Europol que puede desencriptar 162 variantes de ransomware.
- Asegurar que los productos de seguridad funcionan correctamente.

Recuperar los datos
- Confirmar si las copias de seguridad se han visto afectadas
- Bloquear el acceso a los sistemas de copia de seguridad hasta que se elimine la infección.
- Borrar el disco duro de forma segura y reinstalar el sistema operativo
- Recuperar las copias de seguridad externas o en la nube de tus datos
- Cambiar las credenciales de todos los administradores de la red.

Aprender de la experiencia
- Ayudar a evitar que se repita un ataque. Analizar cuáles eran los puntos débiles, qué podría haber hecho de otra manera y qué buenas prácticas se ha aprendido en el proceso

Decidir si pagar o no pagar
- No pagar en ninguna circunstancia. Es un tema de oferta y demanda. Si nadie pagara, no sería negocio y dejarían de hacer estos ataques. Pagar

el rescate exigido puede no ser efectivo porque los ciberdelincuentes no son de fiar y pueden o no devolver sus datos tras el pago

- Ponerse en contacto con las fuerzas de seguridad para **denunciar** el ransomware
- Ponerse en contacto con los proveedores que puedan ayudar.
- Recordar a los empleados las políticas de prensa y redes sociales para mantener el control de las comunicaciones de cara al público

2.6. Ejemplos de ransomware

Según los informes de los laboratorios de investigación de diferentes fabricantes de seguridad informática y Fuerzas de Seguridad, las familias de ransomware más activas en el 2022 y en el primer trimestre del 2023 a nivel global son:

ESET

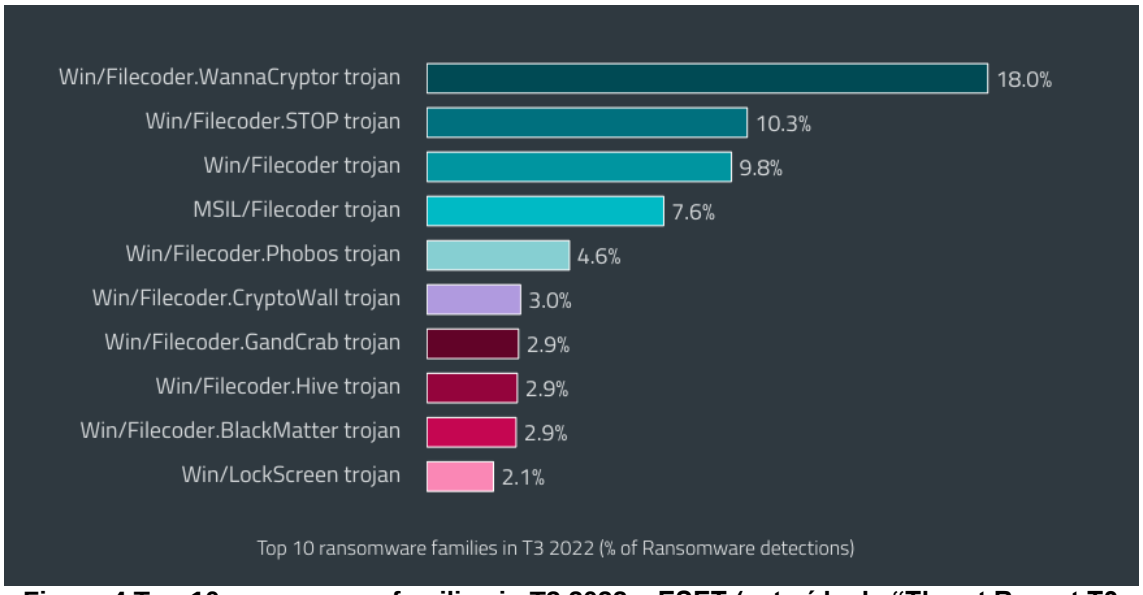


Figura 4.Top 10 ransomware families in T3 2022 – ESET (extraída de "Threat Report T3 2022" de ESET, pág. 18 [79])

Trend Micro

OCT		NOV		DEC	
Locky	753	Wannaren	2,507	Locky	677
Cerber	379	Locky	718	Gorf	548
GandCrab	265	Hive	485	BlackCat	457
Hive	249	Cerber	348	Cerber	365
LockBit	194	Cryptophp	324	GandCrab	237
StopCrypt	160	GandCrab	247	Cobra	228
Magniber	157	BlackCat	194	LockBit	201
Crypwall	148	LockBit	185	Crypwall	146
Cobra	140	StopCrypt	182	Conti	111
Maze	123	Zeppelin	177	Cryptesla	101

Table 8. The top 10 ransomware families in terms of ransomware file detections in machines in the fourth quarter of 2022 (notable ransomware families highlighted)

Source: Trend Micro Smart Protection Network

Figura 5. Top 10 ransomware families Q4 2022 – Trend Micro (extraída de "LOCKBIT, BLACKCAT, AND ROYAL DOMINATE THE RANSOMWARE SCENE" de Trend Micro, pág. 4 [80])

Trellix

Informe Cuarto Trimestre 2022 [78]	Informe Tercer Trimestre 2022 [79]
1. Cuba	1. LockBit
2. Hive	2. HelloXD
3. LockBit	3. Zeppelin
4. Zeppelin	4. Phobos
5. Yanluowang	5. BlackCat

FBI:

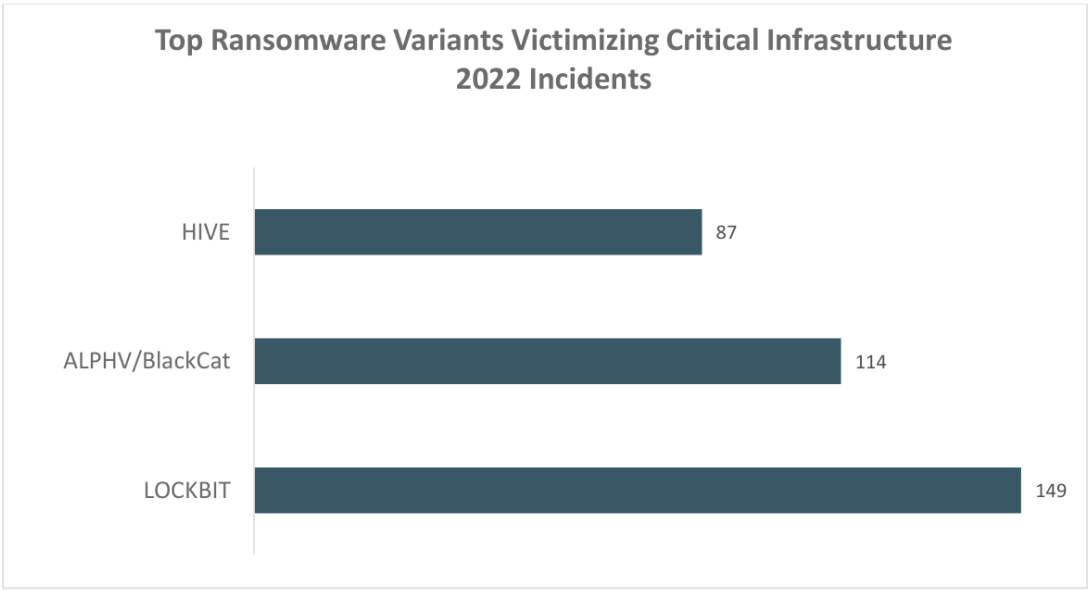


Figura 6. Top Ransomware 2022 – FBI (extraída de "FBI Internet Crime Report 2022", pág. 15 [83]

Bitdefender

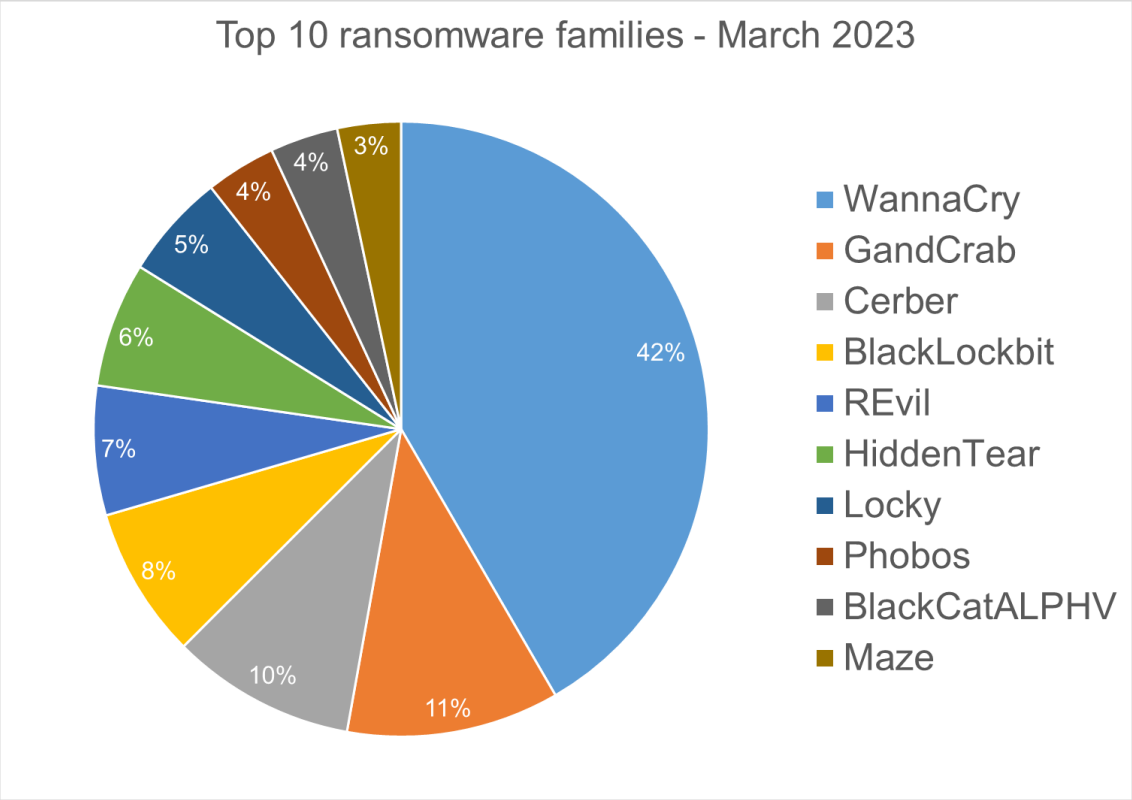


Figura 7. Top 10 ransomware families – March 2023 – Bitdefender [84]

Como se puede observar en las figuras anteriores, las familias de ransomware van evolucionando y cambiando muy rápidamente, apareciendo nuevas variantes en cuestión de meses o trimestres. También van desapareciendo algunas familias, a medida que se van extendiendo las soluciones para su mitigación.

A continuación, se explican las características de las familias de ransomware más relevantes según la información anterior.

Cuba [80] [81]	
Descripción	Cuba es una familia de malware. Tiene como objetivos a las empresas financieras, administración pública, sanidad, industria y TIC.
Implementación	Cuba está desarrollado en el lenguaje de programación C++.
Método de infección	Cuba infecta usando técnicas de phishing, enviando correos electrónicos con ficheros adjuntos maliciosos que sirven para explotar vulnerabilidades. También usa vulnerabilidades de Microsoft Exchange Server, herramientas de acceso remoto vía Remote Desktop Protocol (RDP) y credenciales robadas.
Funcionamiento	Usa PSExec [82], una especie de terminal telnet ligero que también sirve para ejecutar órdenes remotamente y

	también PowerShell para moverse lateralmente por la red. Hace una doble extorsión. Cifra la información y luego se exige un pago. Si no se hace, publicarán los datos robados.

Hive [83] [84] [85]	
Descripción	Hive es un ransomware que opera como un servicio (RaaS). Tiene como objetivos a las empresas e infraestructuras críticas y con especial interés en Hospitales y Sanidad.
Implementación	Las muestras de código dañino de Hive están desarrolladas en el lenguaje de programación Go y compiladas a 32 y 64 bits para Windows. Están empaquetadas con UPX [86]. También hay versiones de código dañino para Linux.
Método de infección	Hive infecta usando técnicas de phishing, enviando correos electrónicos con ficheros adjuntos maliciosos que sirven para explotar vulnerabilidades. También usa herramientas de acceso remoto vía Remote Desktop Protocol (RDP) como Cobalt Strike, ConnectWise para moverse lateralmente por la red.
Funcionamiento	Una vez obtiene las credenciales y entra en los sistemas, intenta evitar la detección del ransomware identificando los procesos de copias de seguridad y antivirus. Borra todas las copias instantáneas y para el servicio de copias. Además, borra todos los registros de eventos (logs). Hace una doble extorsión. Cifra la información y luego se exige un pago, amenazando con publicar parte de la información robada en el blog que exponen a través de la red Tor.

LockBit 3.0 [87] [88]	
Descripción	LockBit 3.0 (conocido como “LockBit Black”) es la continuación de LockBit 2.0 y LockBit. Es un ransomware que opera como un servicio (RaaS). Comparte varias similitudes con el código de otras familias de ransomware, como DarkSide y BlackMatter. Tiene como objetivos a las organizaciones del sector público y empresas del sector TIC.
Implementación	Tiene su propio entorno de desarrollo “builder” [89] para

	crear variantes.
Método de infección	LockBit infecta usando técnicas de phishing, enviando correos electrónicos con ficheros adjuntos maliciosos que sirven para explotar vulnerabilidades. También usa credenciales de VPN y herramientas de acceso remoto vía Remote Desktop Protocol (RDP) robadas.
Funcionamiento	Para moverse lateralmente por la red, usa PSExec [82], una especie de terminal telnet ligero que también sirve para ejecutar órdenes remotamente. Intenta hacer una escalada de privilegios para poder obtener información de los sistemas, dominios, almacenamiento de los datos. Luego termina los procesos y servicios. Borra todas las copias instantáneas y todos los registros de eventos (logs). Hace una triple extorsión. Encripta los datos y si no se paga el rescate, hace públicos los datos robados y lanzan una denegación de servicio (DoS) a los sistemas.

BlackCat / ALPHV [90] [91]	
Descripción	BlackCat (también llamado ALPHV) es un ransomware que opera como un servicio (RaaS). Comparte varias similitudes con el código de otras familias de ransomware, como DarkSide y BlackMatter. Tiene como objetivos a empresas de varios sectores como ingeniería, obra civil, telecomunicaciones, farmacéuticas.
Implementación	Está desarrollado en el lenguaje de programación Rust y funciona para Windows y Linux.
Método de infección	BlackCat infecta a través de herramientas de acceso remoto vía Remote Desktop Protocol (RDP) y credenciales robadas. También explotando vulnerabilidades de Microsoft Exchange Server.
Funcionamiento	Una vez ha accedido a los sistemas, comprometen al Directorio Activo y las cuentas de Administradores para configurar una política de grupo (GPO) que instala el ransomware por todos los sistemas de la red. Luego mediante scripts con PowerShell y software de acceso remoto como Cobalt Strike desconectan los sistemas de seguridad y desinstalan los antivirus. Hace una triple extorsión. Encripta los datos y si no se

	paga el rescate, hace públicos los datos robados y lanza una denegación de servicio (DoS) a los sistemas.

WannaCry [92] [93] [94]	
Descripción	Wannacry es un ransomware que ataca ordenadores con una versión de Windows antigua. Tiene como objetivos a empresas de varios sectores como sanidad, industria, energía, educación, comunicaciones y administración pública.
Implementación	La mayor parte del código fuente de WannaCry está escrito en el lenguaje de programación C++, pero también incluye código escrito en otros lenguajes, como C# y Visual Basic.
Método de infección	Wannacry usando técnicas de phishing, enviando correos electrónicos con ficheros adjuntos maliciosos que sirven para explotar vulnerabilidades o webs que contienen ficheros maliciosos. Explota una vulnerabilidad de Windows Server Messaging Block (SMB, protocolo que permite comunicar diferentes sistemas dentro de una red.) llamada EternalBlue que donde se puede ejecutar código de forma remota mediante una solicitud de uso compartido de impresoras y archivos de Windows
Funcionamiento	Una vez ha accedido a los sistemas, busca los archivos más importantes, documentos de Microsoft Office, archivos de audio MP3, archivos de vídeo MKV y los encripta, apareciendo en pantalla, información para hacer el pago y obtener el desbloqueo. Además, copia en Tor las acciones que ha hecho.

2.7. Soluciones comerciales anti-ransomware

Existe un abanico importante de soluciones anti-ransomware en el mercado.

En función del tipo y el entorno tecnológico que tenga el cliente, además del presupuesto, podrá tener diferentes opciones tecnológicas para protegerse contra el ransomware.

Los tipos más habituales de cliente de software anti-ransomware son:

- Consumidor (consumer) o usuario doméstico
- Pyme
- Empresa

Normalmente existen diferencias entre las versiones pyme y empresa respecto a la de consumidor. Las versiones pyme y empresa tienen funcionalidades avanzadas respecto a la versión consumidor, además de poder disponer de un soporte técnico especializado.

Las soluciones **antivirus** de diferentes fabricantes tienen funcionalidades anti-malware y anti-ransomware. Pueden detectar, prevenir y eliminar software malicioso. Su funcionamiento se basa en el análisis de comportamiento, reconocimiento de patrones y la detección heurística para identificar y detener los intentos de ransomware antes de que se ejecute y comience a encriptar los datos o a robarlos.

También existen otras soluciones de seguridad llamadas "**endpoints**" donde los dispositivos finales, ordenadores, portátiles, móviles, tabletas están conectados a la red y gracias a soluciones de seguridad que llevan integradas como son antivirus, firewall, anti-malware, detección de intrusos y control de aplicaciones, quedan protegidos de forma integrada.

Ahora, con la integración de la inteligencia artificial a los "endpoints", se les está dando más capacidades para analizar el comportamiento y reconocimiento de patrones, sobre todo para detectar nuevas variantes donde todavía no hay una solución.
Es el caso de los llamados **EDR** (Endpoint Detection and Response). Su objetivo es la detección temprana y respuesta ante amenazas. Para hacerlo se monitoriza continuamente los dispositivos y anomalías para tener una mejor protección ante incidentes de seguridad.

Recientemente han aparecido los **XDR** (Extended Detection and Response) que es una evolución de los EDR donde se detectan y responden a amenazas en la infraestructura. Correlacionando datos entre los diferentes componentes, se pueden detectar amenazas más sofisticadas y nuevas.

Y también existen soluciones que sólo borran los ransomware, pero no ofrecen ningún tipo de protección ante incidentes, es más una protección reactiva ante un incidente de seguridad.

En el **Apartado 3.6 Análisis existentes de soluciones comerciales anti-ransomware** de este Trabajo hay información sobre las distintas soluciones anti-ransomware para pymes de diferentes fabricantes que han sido analizadas por empresas y organismos independientes especializados en seguridad informática.

2.8. Responsabilidad legal

Sufrir un ataque de ramsomware no sólo puede tener consecuencias técnicas o de negocio, también a nivel legal.
Las empresas han de tomar medidas técnicas y organizativas para evitar los ataques de ransomware y en caso de sufrir un ataque, poderlo detectar de forma rápida, **evaluar** sus consecuencias y minimizar su **impacto**, también a nivel de derechos y deberes de las personas a las que se han visto afectados sus datos.
También las empresas tienen la obligación de proteger los datos personales que procesan y **notificar antes de 72 horas** a las autoridades de protección de

datos competentes como la AEPD [3] y a los individuos afectados en caso de una **violación de datos personales**. Estas autoridades pueden sancionar o no si se han tomado las medidas de seguridad adecuadas o si ha habido alguna actuación negligente del incidente.
Por lo tanto, en caso de sufrir un ataque de ransomware, las empresas tienen ciertas responsabilidades legales en relación con el **Reglamento General de Protección de Datos (RGPD)** [95].

También se han de denunciar los ataques de ransomware a las Fuerzas y Cuerpos de Seguridad del Estado porque en la mayoría de los casos, incurren en un delito.

Es necesario tener una buena gestión de riesgos y gobernanza para tener información que servirá para la denuncia como:

- Categorías de datos personales afectados
- Número de registros afectados
- Número de personas afectadas
- Tipología de la brecha de seguridad (disponibilidad y/o confidencialidad)
- En caso de afectar a la disponibilidad, capacidad para reestablecerla sin causar daño o nivel de daño potencial
- En caso de afectar a la confidencialidad, riesgo real de identificación de las personas y nivel de daño potencial

El Responsable del Tratamiento de datos de la empresa ha de tener esta información para el cumplimiento de los requisitos de responsabilidad proactiva, tal como exige el RGPD como son:

- **Artículo 33 RGPD** [96]**: Notificación de una violación de la seguridad de los datos personales a la autoridad de control.**
  Existe la obligación de notificar las brechas de seguridad a la autoridad de control [97], a menos que sea improbable que la brecha suponga un riesgo para los derechos y libertades de las personas afectadas, dentro de las 72 horas siguientes a que la persona responsable sea consciente de que el hecho se ha producido.
- **Artículo 34 RGPD** [98]**: Comunicación de una violación de la seguridad de los datos personales al interesado.**
  Existe la obligación de comunicar la brecha de seguridad a las personas afectadas [99] en caso de que sea probable un alto riesgo para sus derechos y libertades. El objetivo de la comunicación a estas personas afectadas es permitir que puedan tomar medidas para protegerse de las consecuencias.

Además, los empresarios pueden recibir reclamaciones de sus clientes o de terceros por la pérdida de los datos y también por los perjuicios que puede causar esa pérdida [100].

- **Artículo 1101 del Código Civil** [101]: “Quedan sujetos a la indemnización de los daños y perjuicios causados los que en el cumplimiento de sus obligaciones incurrieren en dolo, negligencia o morosidad, y los que de cualquier modo contravinieren al tenor de aquéllas”. **Y siguientes**.

- **Artículo 1902 del Código Civil**: El que por acción u omisión causa daño a otro, interviniendo culpa o negligencia, está obligado a reparar el daño causado".
- **Artículo 1089 del Código Civil**: "Las obligaciones nacen de la ley, de los contratos y cuasi contratos, y de los actos y omisiones ilícitos o en que intervenga cualquier género de culpa o negligencia".

3. Análisis de soluciones comerciales anti-ransomware para pymes

A partir de los datos de la encuesta de elaboración propia que se ha hecho a pymes para conocer sus entornos tecnológicos de trabajo, se quiere implementar una infraestructura lo más similar posible a la que tienen las pymes y que se analicen las soluciones anti-ransomware para pymes en ese entorno.

Siguiendo la forma en la que se analizan los virus biológicos, analizar diferentes soluciones comerciales anti-ransomware para pymes, sería como analizar las diferentes vacunas existentes para un virus y sus variantes. Y este análisis se tiene que hacer en un ambiente controlado y seguro por si hay fugas o complicaciones.
Por este motivo se crea un laboratorio de seguridad informática donde se prueban diversas soluciones comerciales anti-ransomware usando muestras reales de ransomware y realizando pruebas mediante una metodología de trabajo. Una vez acabadas las pruebas, se ofrecen unos resultados y conclusiones para ayudar a la elección de las soluciones más adecuada para las diferentes pymes.

3.1. Encuesta

La encuesta sirve para recopilar información de un grupo de personas o empresas, con el fin de obtener datos estadísticos para una investigación académica, como en este Trabajo.

El motivo y valor de esta encuesta para pymes sobre ransomware es porque no existen muchas que puedan ser consultadas de forma pública.
La mayoría están hechas por fabricantes de soluciones de seguridad informática y ahora recientemente hay algunas realizadas por empresas de seguros.

Se ha elaborado la encuesta para saber los conocimientos que tienen las pymes sobre seguridad informática y más concretamente sobre ransomware. También para saber los entornos tecnológicos que tienen, sistemas informáticos, sistemas operativos, redes, soluciones de seguridad, copias de seguridad y las políticas de seguridad que han definido.
Además, saber si han sufrido o conocen a alguien que haya tenido un ataque de ransomware , cómo lo solucionaron y cuánto dinero les costó.

La encuesta se ha hecho en formato “ciego”, sin recoger datos identificativos de las empresas participantes, para mantener el anonimato de las empresas y cumplir con la normativa de protección de datos.

Para confeccionar la encuesta se ha usado un formulario online creado con **Google Forms** con las preguntas organizadas en varios bloques o secciones. En este caso hay 6 secciones.

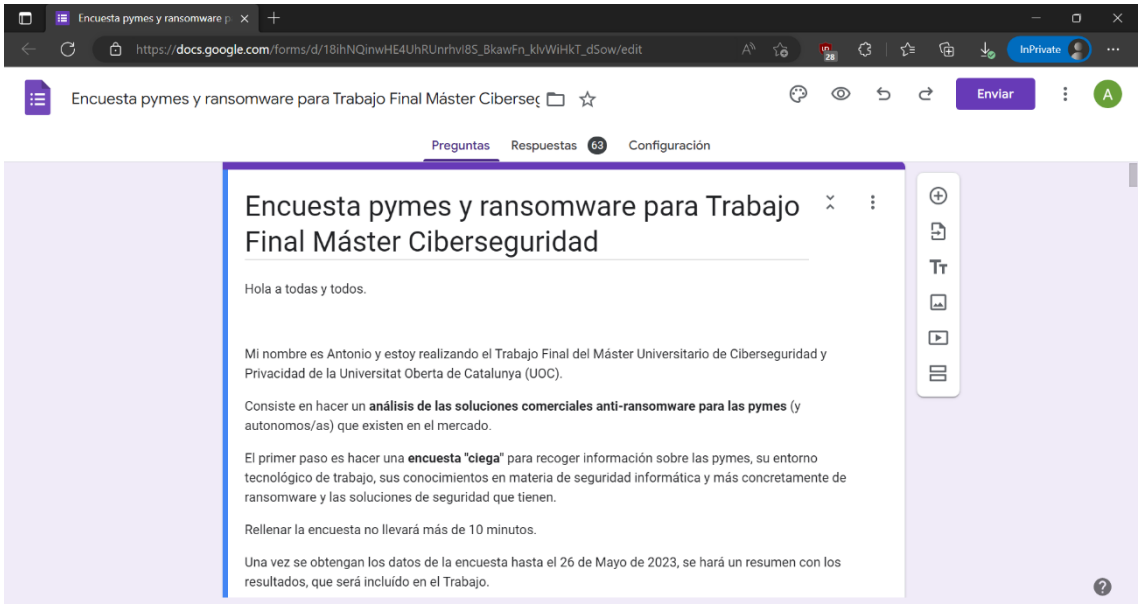


Figura 8. Encuesta pymes y ransomware

https://docs.google.com/forms/d/e/1FAIpQLSdtIPkrYYRfxO4uxJK1oCU4wlZNo8QNFMMuXXdlmFtl3htMig/viewform?usp=sf_link

Como respuesta a las preguntas, se ha de seleccionar una opción de las disponibles. Las opciones tienen unos rangos de valores prefijados en el contexto de las preguntas, para facilitar el análisis y la representación gráfica de los resultados.
La gran mayoría de respuestas son obligatorias, aunque hay algunas no obligatorias de texto libre.

La encuesta se enviado de forma directa a pymes que son contactos con las que ya se tiene un consentimiento para las comunicaciones.
No se ha usado ningún software de buzoneo para evitar ser considerado spam.

Se han obtenido 80 encuestas rellenadas.
Al ser un tema muy sensible y de actualidad, ha habido mucha resistencia para rellenar las encuestas. Se ha preguntado si la encuesta era spam, si el enlace contenía un virus, desconocer el destino de los datos a pesar de informarlo al inicio de la encuesta y no querer revelar según qué información, cosa que ha hecho que se añada una respuesta como “Prefiero no decirlo”.

IMPORTANTE: Se pone a disposición de cualquier interesado/a el archivo con las respuestas obtenidas de la encuesta que puede ser utilizado para otros proyectos donde la información obtenida sea aplicable.

Resumen con los resultados de la encuesta

A partir de las respuestas de la encuesta, se extrae la siguiente información relativa a las pymes y el ransomware:

La mayoría de las pymes pertenecen a los sectores (según CNAE) de Información y Comunicaciones, Actividades profesionales, científicas y técnicas, Otros servicios e Industria manufacturera.

Poco más de la mitad de las empresas son micropymes, de 1 a 10 empleados.
Una micropyme tiene de 1 a 10 empleados y un volumen de negocio de menos de 2 millones de euros.
Las micropymes representan el grueso del tejido empresarial español según cifras del último informe de la Dirección General de Industria y de la Pequeña y Mediana Empresa. Ministerio de Industria, Comercio y Turismo de Marzo de 2023 [102].

La facturación habitual es menos de 100.000 € anuales, seguido de entre 2 y 5 millones € y entre 250.000 y 500.000 €.

Algo más de la mitad de las pymes tienen ordenadores (clientes) y uno o varios servidores, y el resto sólo ordenadores.

El 71,3% usan el sistema operativo Microsoft Windows y después macOS (Apple) en los ordenadores.

El sistema operativo más usado en servidores es Windows Server y después, Linux.

Un 85% tiene una red local LAN cableada.
Y prácticamente todas tienen una red wifi.

A nivel de almacenamiento en la nube, el más usado es Google Drive, seguido de Otros y Microsoft OneDrive.

El 76,3% de las pymes encuestadas hacen teletrabajo y el 65% usan una VPN para tener acceso remoto seguro. Por tanto, la VPN es el sistema de conexión remota segura más usado para hacer teletrabajo.

A nivel de soluciones de seguridad informática, el 36,3% usan un antivirus de de pago y el 26,3% un antivirus gratuito. Las soluciones “endpoint” sólo las tienen un 16,3%.
Por tanto, la opción preferida por la pyme para su seguridad es un antivirus de pago, aunque existe mucha pyme con un antivirus gratuito. El antivirus representa más de la mitad de las soluciones de seguridad que tiene la pyme, respecto a otras soluciones.

Un 65% de las pymes tienen un firewall diferente del que viene por defecto en el sistema operativo.

En el 41,3% de los casos, hay una persona responsable de la seguridad, seguido de un 16,3% que trabajan con una empresa externa.

A nivel de presupuesto destinado a seguridad informática, el 23,8% es de menos de 2.000 € anuales (166,66 € mensuales) seguido de un 21,3% que dice no disponer de presupuesto. Esto indica la falta de recursos económicos que tienen las pymes. Son cantidades muy bajas para el coste que podría tener recuperar la información secuestrada o perdida.

La mayoría conoce y es capaz de definir qué es ransomware con sus propias palabras.

El 73,8% dice no haber sufrido un ataque de ransomware.
Esta cifra puede llevarnos a conclusiones equivocadas porque o no han querido manifestar que han tenido un ataque de ransomware o que a lo mejor tienen al intruso dentro y no se han dado cuenta, porque no se ha activado el ataque con el secuestro.
Las que han dicho que han tenido un ataque de ransomware, lo solucionaron pagando, restaurando los sistemas o contando con la ayuda de un proveedor.

El 61,8% de las pymes dicen conocer a alguna empresa que ha tenido un ataque de ransomware y resolvieron el problema restaurando los sistemas.

Respecto a la protección de datos, se ha preguntado por las copias de seguridad, donde el 33,8% usa un sistema de copias de seguridad gestionado por un proveedor, seguido de un 27,9% que usa un disco duro externo USB.
El 60,3% hace copias de seguridad diarias, seguido de un 13,2% que las hace semanalmente.

El 69,1% hace una segunda copia de seguridad y el 63,2% la tiene fuera del edificio habitual donde trabajan para así protegerla en caso de robo, fallo o catástrofe en el edificio.

El servicio de correo electrónico más usado es gestionado por un proveedor, teniendo un dominio propio. Luego está Microsoft Exchange Server en servidores propios.

El 82,4% de las pymes hace una gestión de usuarios, carpetas y recursos de la red.

Y el 69,1% tiene mecanismos de autentificación de doble factor (2FA).

El 61,8% tiene una política de renovación de contraseñas.

A nivel de continuidad de negocio, el tiempo objetivo de recuperación, (cuántas horas/días/semanas podrías estar sin tener acceso a los datos) (Recovery

Time Objective, RTO) y el objetivo de punto de recuperación (cuántos datos podría llegar a perder) (Recovery Point Objective, RPO) son muy importantes.
A nivel de RTO, el 25% de las pymes consideran que pueden estar sin acceso a los datos 1 día. El 23,5%, 4 horas. Y otro 20,6% no lo saben.
A nivel de RPO, el 27,9% de las pymes consideran que podrían perder los datos de 1 día. Luego, el 17,6% no lo saben.

Y respecto a cuánto dinero se han gastado para recuperar los datos después de un ataque, el 82,4% de las pymes dice nada, seguido del 8,8% que prefiere no decirlo.
Por tanto, ese resultado genera dudas porque siempre hay un coste para recuperar los datos, ya sea para ejecutar el plan de recuperación o para pagar el rescate, cosa que se confirma porque la siguiente respuesta más elegida es que no quieren decir la cantidad gastada para el rescate.

3.2. Laboratorio de seguridad informática

Se ha escogido como entorno para el laboratorio de seguridad, el necesario para simular un ataque de ransomware mediante **phishing**, es decir, que los vectores de ataque son el **correo electrónico** o pendrives, discos duros externos. Estos correos tienen código malicioso que debe ser bloqueado y eliminado por las soluciones de seguridad.

Para implementar un servicio de correo electrónico, se siguen los datos de la encuesta relacionados con este tema, donde dicen que el entorno más habitual para pymes es con ordenadores con sistema operativo **Windows** y que el servicio de **correo electrónico** más usado es **gestionado por un proveedor** y usando un **dominio propio**.

Se ha hecho toda la configuración del laboratorio de seguridad en un **entorno físico** y real, con un **servidor y un cliente** sin virtualizar, debido a que muchos ransomware detectan que existen máquinas virtuales y no se ejecutan ni actúan porque se pueden apagar esas máquinas virtuales de forma rápida, se pueden aislar y así minimizar el alcance del ataque.

3.2.1. Hardware para el laboratorio de seguridad informática:

Servidor (nombre: *server*)	Ordenador con: • Procesador Intel i3-350M 2.26 GHz • Memoria RAM 4 GB DDR3 • Disco duro SSD 240 GB • Tarjeta de red Gigabit Ethernet
Ordenador cliente (nombre: *PC1*)	Portátil con: • Procesador Intel i3 7100U 2.4 GHz • Memoria RAM 8 GB DDR4 • Disco duro SSD 240 GB

	• Tarjeta de red wifi
Red local **LAN**	Conexión mediante el switch de 4 puertos Gigabit Ehternet que incorpora el router de conexión a Internet
Red **wifi**	Conexión mediante el router de conexión a Internet
Conexión a **Internet**	Router con salida a Internet
Diversos **pendrives** y **discos duros externos** para tener las imágenes de los sistemas operativos y las copias de seguridad del entorno para una rápida recuperación.	

3.2.2. Software para el laboratorio de seguridad informática:

Servidor

- Sistema operativo Linux **Ubuntu Server 22.04**
- Software servidor de DNS **DNSmasq 2.86** [103]
- Software para dar servicio de correo electrónico con el agente de transferencia de correo **Postfix 3.64** [104] y con el servidor de correo IMAP **Dovecot** 2.3.16 [105]
- Software de clonación de discos duros **Clonezilla**

Cliente

- Sistema operativo **Microsoft Windows 10 Home versión 22H2**
- Cliente de correo electrónico **Mozilla Thunderbird 102**

Herramientas para desarrollar el ataque de phishing

- **SendEmail** [106] para el envío de correos personalizables desde la línea de comandos
- **Resource Hacker** [107] para ayudar a ocultar archivos dentro de otros archivos (esteganografía)
- Editor HTML online

En el servidor Ubuntu llamado *server* se ha hecho una configuración creando un usuario llamado usuario1.

El servidor DNS (*dns.server.com*) nos permite tener un dominio interno propio, para nuestro caso, *server.com*.
Se ha configurado el DNS para que primero consulte las direcciones del dominio propio y si no las encuentra, que haga las consultas a otros servidores de DNS externos.

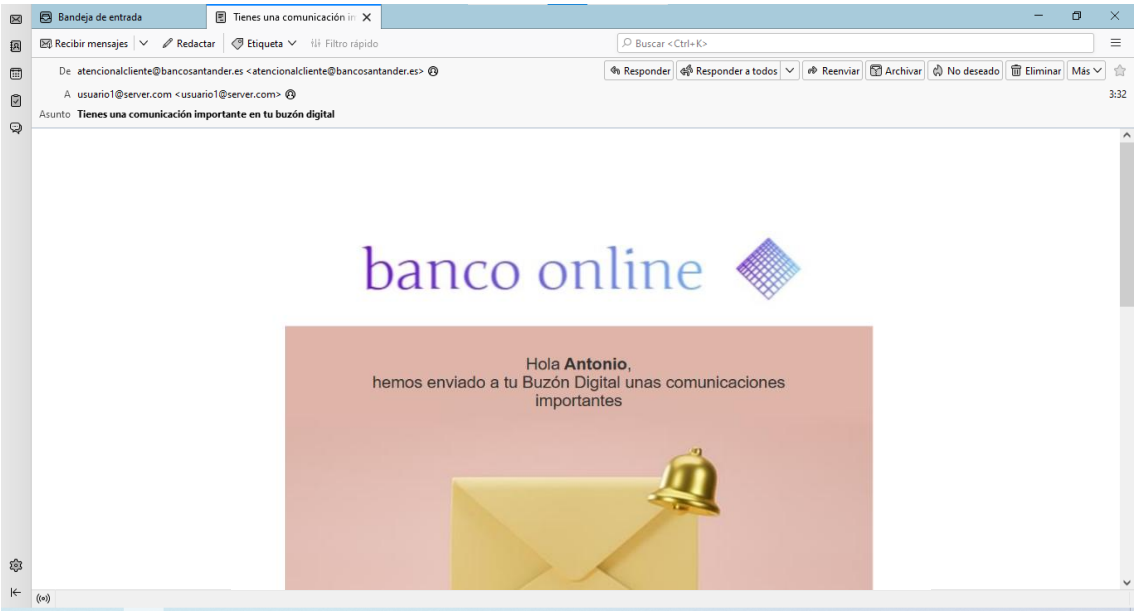
Postfix y Dovecot (*mail.server.com*) nos permiten tener el servidor de correo electrónico IMAP para enviar y recibir correos electrónicos que serán consultados a través de un cliente de correo como Thunderbird (NOTA: No se

ha podido probar con otros clientes de correo electrónico usados por las pymes como Microsoft Outlook incluido en el software Microsoft Office 365).

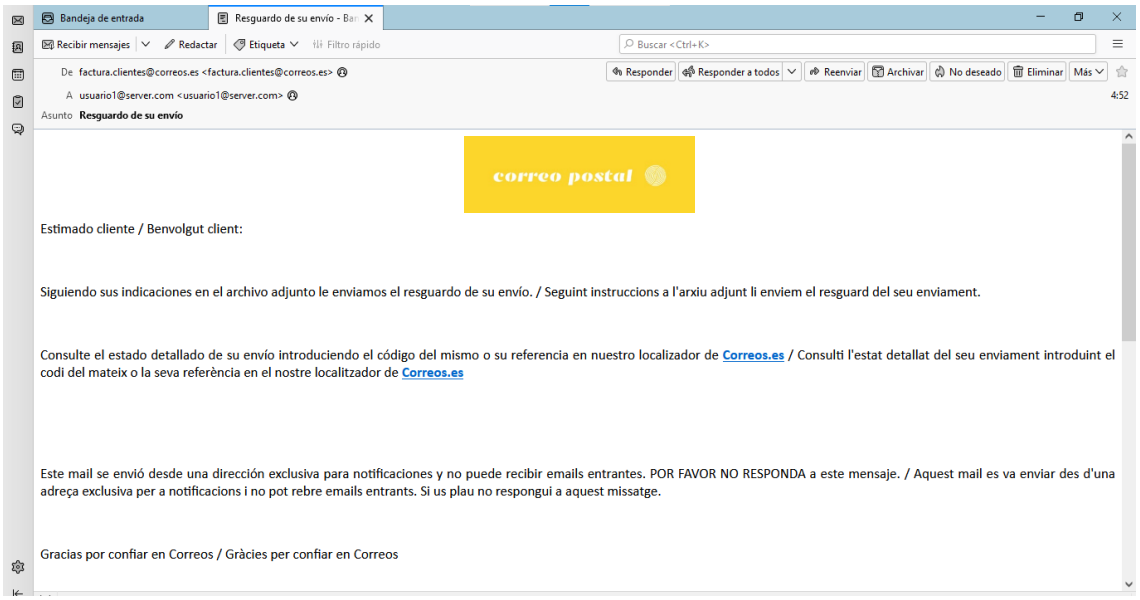
El envío de correos desde el servidor hacia un cliente (origen del mensaje) se ha hecho usando el software SendEmail que permite el envío de correos con los datos deseados, falseando el remitente y más parámetros, siendo una herramienta utilizada para hacer phishing.

Para generar los correos electrónicos de phishing, se configura SendEmail para que envíe un correo con un remitente y un título falsos y lo más realísticos posibles (son técnicas de Ingeniería Social, “Social Networking”), con un cuerpo o contenido generado en lenguaje HTML con un texto copiado de la web o de un correo que se quiere suplantar y con un archivo adjunto con código malicioso, en este caso, con ransomware.
Para este Trabajo se han creado 2 correos HTML;

- Banco online (correo electrónico: atencionalcliente@bancosantander.es)



- Correo postal (correo electrónico: factura.clientes@correos.es)



Se han hecho varios clones (copias de seguridad idénticas al sistema original) del servidor y el cliente con Clonezilla, con diferentes versiones con cambios de configuración y de software instalado, para recuperar el servicio de forma rápida en el caso que no se detectara un ransomware y se infectara el sistema.
Además, este método de recuperación es muy práctico y rápido para tener un sistema en un punto determinado, evitando la desinstalación de software que siempre deja archivos residuos y posibles problemas de compatibilidad.

Consideraciones:
No es recomendable tener varias soluciones anti-ransomware instaladas en una misma máquina porque podrían considerarse como un ente extraño y dar falsos positivos, además de consumir más recursos de hardware.

3.2.3. Entorno de red para el laboratorio de seguridad informática

El servidor se conecta al switch que incorpora el router mediante un cable Ethernet.
El cliente se conecta al router mediante wifi.

Se ha extremado la seguridad a nivel de red haciendo un aislamiento para no impactar con el resto de los equipos conectados.
Para ello se ha utilizado el servicio **DHCP** del router, modificado en rango de IPs que vienen configuradas por defecto, pasado ahora a tener desde la IP 192.168.1.30 a la 192.168.1.99.
De esta forma, el DHCP no podrá asignar una IP al servidor.
Lo ideal sería aislar la red mediante VLANs, o con diversos routers y firewalls, pero para eso de debería disponer de la electrónica de red adecuada.

El **servidor Linux** (*server.server.com*) se ha configurado con una **IP estática**, la 192.168.1.100**,** porque para tener un servidor de correo, es necesario que

tenga una IP estática o pública y también un servidor de nombres DNS para tener un dominio.

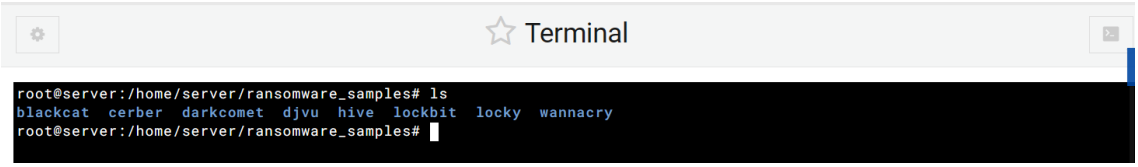
Para este análisis, se ha usado el mismo servidor Linux para diversos servicios.

- DNS (*dns.server.com*) con IP 192.168.1.100
- Correo electrónico (*mail.server.com*) con IP 192.168.1.100

3.2.4. Muestras reales de ransomware

Se han seleccionado los ransomware más activos y recientes que aparecen en este Trabajo para ser probados en el laboratorio:

- BlackCat
- Cerber
- DarkComet. Se ha usado en la asignatura de Análisis Forense del Máster de Ciberseguridad y Privacidad de la UOC
- DJVU (STOP)
- HIVE
- Lockbit
- Locky
- WannaCry

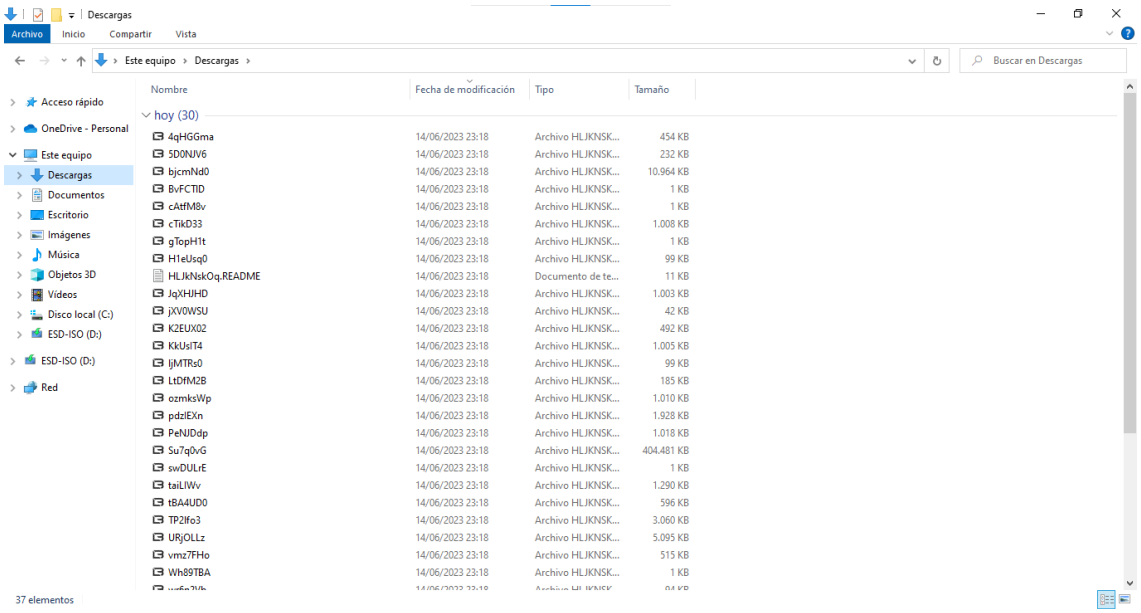


Se han descargado muestras de las webs:

- Triage [108]
- Malware Bazaar [109]

Para la descarga y manipulación del ransomware se usa una máquina virtual **Virtualbox** con el sistema operativo Linux **Lubuntu 18.04**, porque los antivirus de Windows pueden detectar el código maligno y eliminarlo antes de hacer el análisis.

Se ha probado el funcionamiento del ransomware **WannaCry** en el ordenador cliente Windows 10 PC1 desactivando el antivirus que viene por defecto, Microsoft Windows Defender y tras ejecutarlo, encripta el contenido del disco duro:



3.3. Soluciones comerciales anti-ransomware para pymes analizadas

Existen en el mercado muchos fabricantes de seguridad informática con soluciones para pymes, por lo que la elección de uno u otro no es tarea fácil.

Para hacer este Trabajo sobre soluciones anti-ransomware para pymes se han utilizado los siguientes criterios de selección de fabricantes de seguridad:

- Tener **soluciones específicas para pymes** en su porfolio**.** De esta manera pueden conocer el entorno de trabajo de las pymes y ofrecer soluciones más adaptadas a ellas.
- Tener oficinas en España, además de mayoristas y una red de distribuidores comerciales, con soporte técnico local. De esta manera pueden ofrecer una ayuda más cercana y directa.
- Tener un laboratorio de investigación propio (**Research Lab**). Con el laboratorio, los fabricantes son capaces de detectar nuevos ataques y ofrecer soluciones más rápidas y novedosas, porque es fundamental el tiempo de respuesta ante cualquier evento de seguridad.
- Ser los productos seleccionados para el programa de ayudas para pymes llamado **Kit Digital** [110]. El Kit Digital es una subvención anual, para adquirir soluciones de ciberseguridad, además de otras soluciones tecnológicas. De esta manera, las pymes pueden beneficiarse de unas soluciones ya empaquetadas que pueden ser aplicadas en pymes parecidas y por tanto, aprovechar ese conocimiento existente y experiencias sobre uso y funcionamiento.

Con estas premisas, han sido elegidas las soluciones endpoint anti-ransomware para pymes de las empresas:

- **ESET** y su **Protect Cloud** [111]
- **Sophos** y su **Intercept X Advanced with XDR** [112]
- **Bitdefender** y su **GravityZone Business Security** [113]

Todas estas soluciones comparten características y funcionalidades y se han seleccionado estas versiones de productos porque además de ser para pymes, tienen protección anti-ransomware y seguridad para el correo, funcionalidades importantes para poder analizar el ataque vía phishing.

Disponen de una consola de gestión vía cloud que permite el análisis remoto por parte de los servidores de los fabricantes de seguridad, además de la gestión de los equipos.
También tienen una versión instalable (on premise) en la infraestructura tecnológica de los clientes, pero requieren de unos requerimientos hardware importantes.

Y tienen un agente que se instala en los clientes, en este caso, en PC1.

A nivel de comercialización se pueden adquirir a través de las webs de los fabricantes de seguridad informática o a través de su canal de distribuidores.

Y a nivel de licenciamiento, este tipo de soluciones anti-ransomware analizadas tienen un precio anual por dispositivo y se vende en paquetes de un número determinado de dispositivos que se puede ir aumentando según las necesidades.

	. Número dispositivos	Precio	Precio por dispositivo
ESET Protect Complete	5	353,32 € / año	70,66 € / año
Sophos Intercept X Advanced with XDR	9	123,42 € / año	13,71 € / año
Bitdefender GravityZone Business Security (*) falta añadir EDR/XDR)	3	100,99 € / año	33,66 € / año

3.4. Metodología de análisis

Para poder sistematizar el análisis y realizar las pruebas de las diferentes soluciones anti-ransomware para pymes para conseguir unos resultados comparando los mismos aspectos, se seguirá el siguiente proceso en el orden indicado:

1. Evaluar el **proceso de instalación** del software

En un entorno pyme donde no hay muchos recursos especializados en informática, se valora positivamente que el software sea rápido y fácil de instalar.
Al ser un software que tiene una parte de **gestión central** y **agentes** en los diferentes dispositivos, se tendrá en cuenta estas dos partes.

Además, también se evaluará el **tiempo de instalación** tanto de la parte central como de los dispositivos.

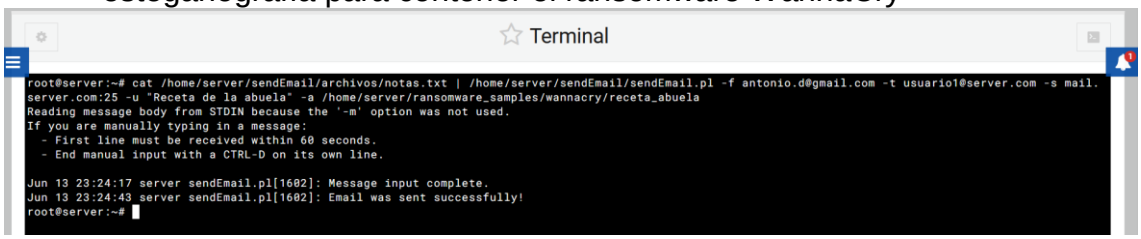
2. Evaluar la **usabilidad**

Para una pyme, la facilidad de uso es importante. Necesitan ser productivos con pocos recursos y de forma rápida. Si un software es usable, nos hará más productivos. La usabilidad se medirá viendo que la interfaz de usuario es intuitiva, fácil de entender y cumple su función de forma eficiente.
Para este Trabajo se evalúa la usabilidad tanto de la parte de consola central como de los agentes.

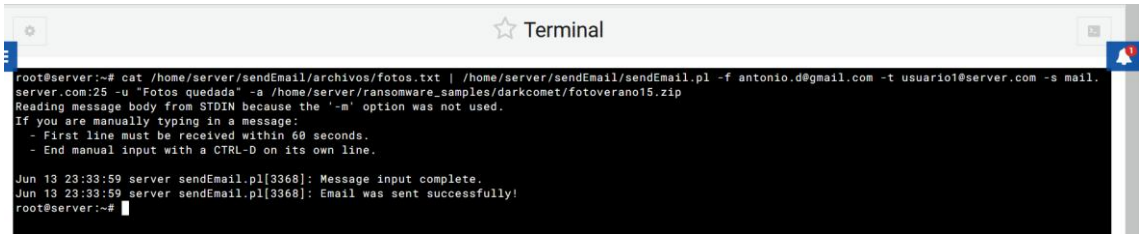
3. Evaluar la capacidad de **detección**

Para detectar ransomware por parte de las soluciones anti-ransomware, es necesario ponerlas a prueba, lanzando un ataque y viendo su capacidad de detección.
También se tiene que conocer su capacidad de detección **en tiempo real** y también cuando hace un **escaneo** de forma **manual**.
Las pruebas de detección de ransomware se hacen de la siguiente forma:

- Envío de correo electrónico con archivos adjuntos:
  - Archivo <receta_abuela.txt> que ha sido tratado con esteganografía para contener el ransomware WannaCry



  - Archivo <fotoverano.15.zip> que continue un archivo .scr con un ransomware DarkCOMET (usado en la asignatura de Análisis Forense del Máster de Ciberseguridad de la UOC)



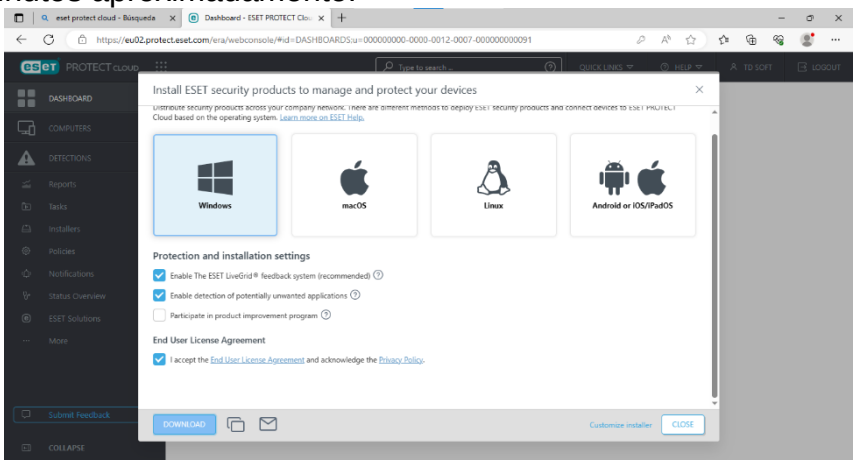
  - Archivo ejecutable *.exe con un ransomware de la lista.

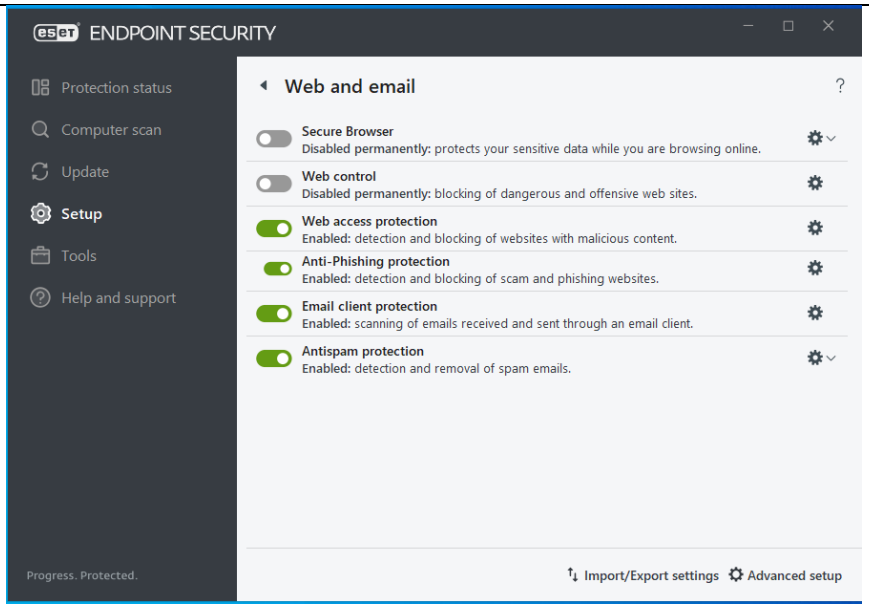
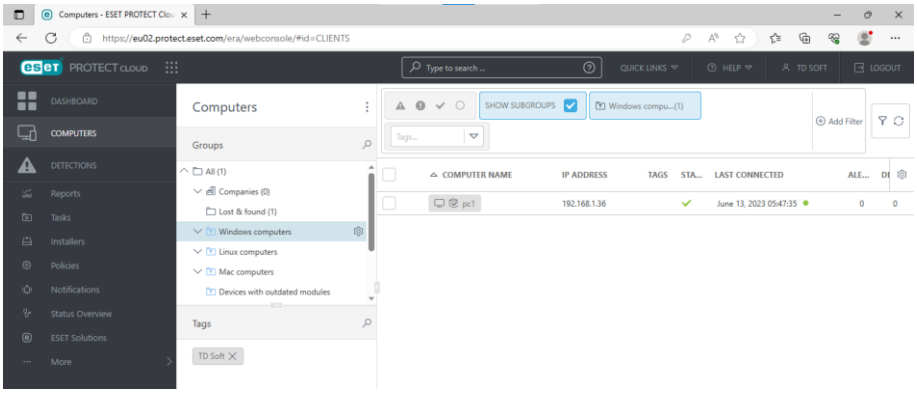
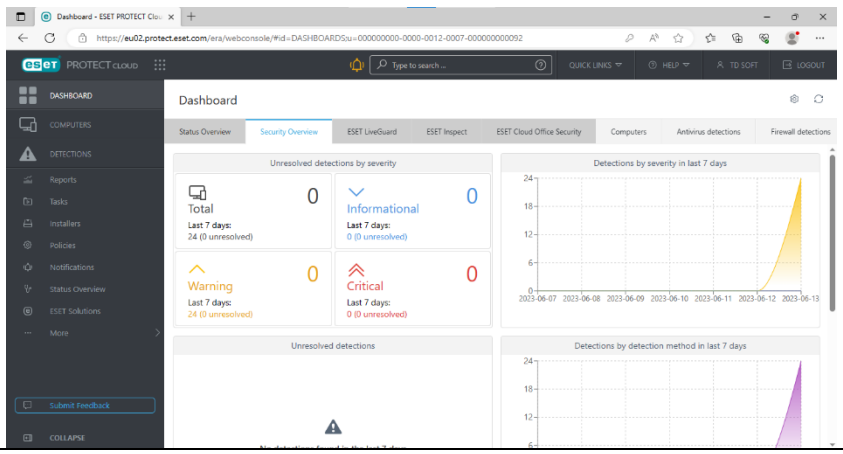
- Conexión de un pendrive en el ordenador que contiene todas las muestras reales de ransomware

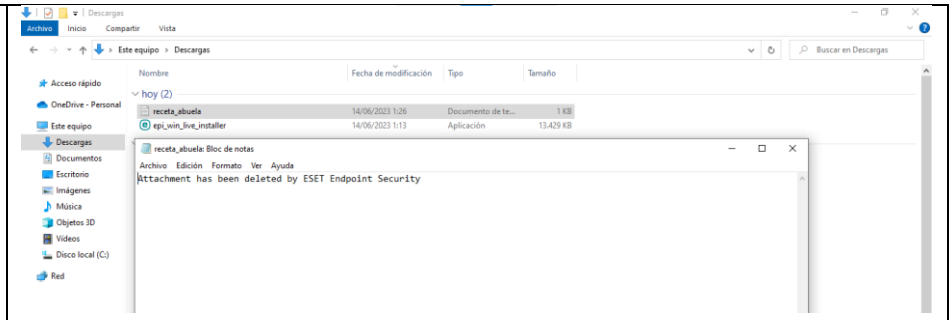
4. Evaluar el **uso de recursos**

Un software es eficiente si hace su función usando el menor número de recursos de computación posible que son el procesador, la memoria y el disco duro.
Se debe medir el uso de recursos en tiempo real o cuando se lanza una orden de escaneo o cuando se detecta un ataque.
Para ello ser usarán las aplicaciones y recursos del sistema operativo para poder analizar este uso.

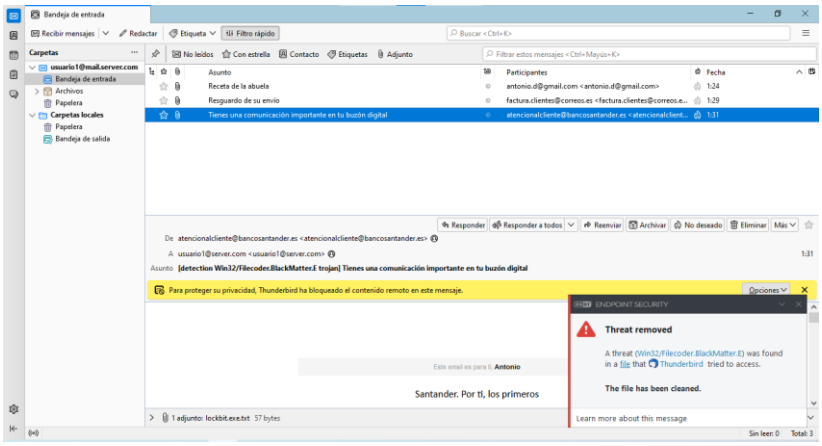
3.5. Análisis de soluciones comerciales anti-ransomware

ESET	
Instalación	La instalación requiere dar de alta a un usuario en un formulario web. Una vez confirmados los datos, tarda aproximadamente 10 minutos en hacer el proceso de instalación y configuración de la parte central. A continuación, aparece una pantalla para descargarse el agente y luego el proceso de instalación del agente de unos 5 minutos aproximadamente.  El idioma por defecto es el inglés. Luego se pueden configurar las opciones del agente que básicamente son activar o desactivar servicios de protección.

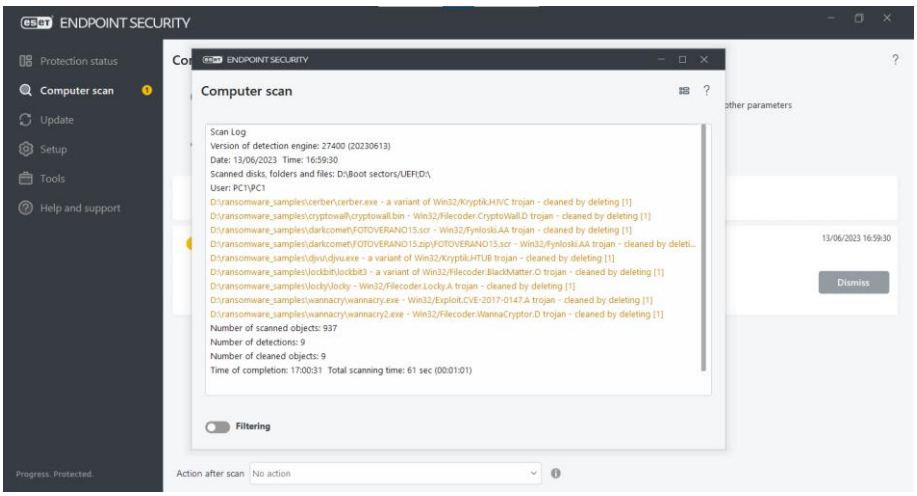
	
Usabilidad	La consola de gestión en el cloud permite ver información de los dispositivos conectados.  También ofrece información de los ataques producidos y estadísticas. 
Detección	El correo electrónico con el archivo adjunto <receta_abuela.txt> no es detectado cuando llega al buzón. Hay que abrirlo y descargarlo para que ESET lo detecte y borre.

<table>
<tr><td></td><td>


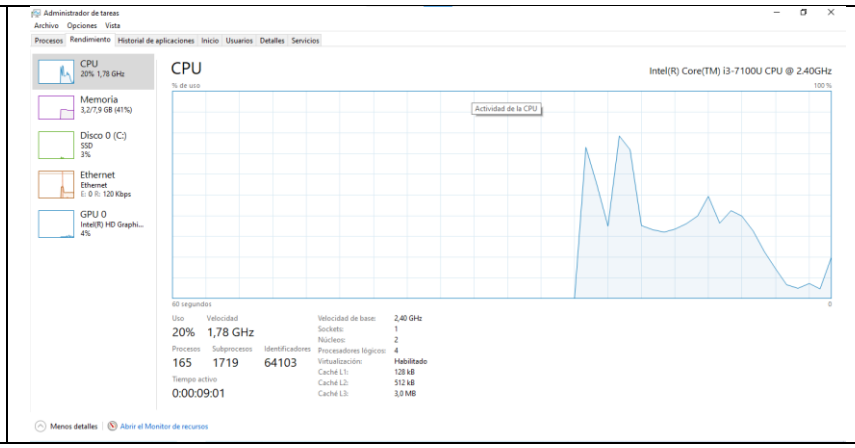
El correo electrónico con el archivo adjunto <lockbit.exe> es detectado cuando llega al buzón sin abrirlo ni leerlo y queda en cuarentena, incluso cuando se intenta descargar.

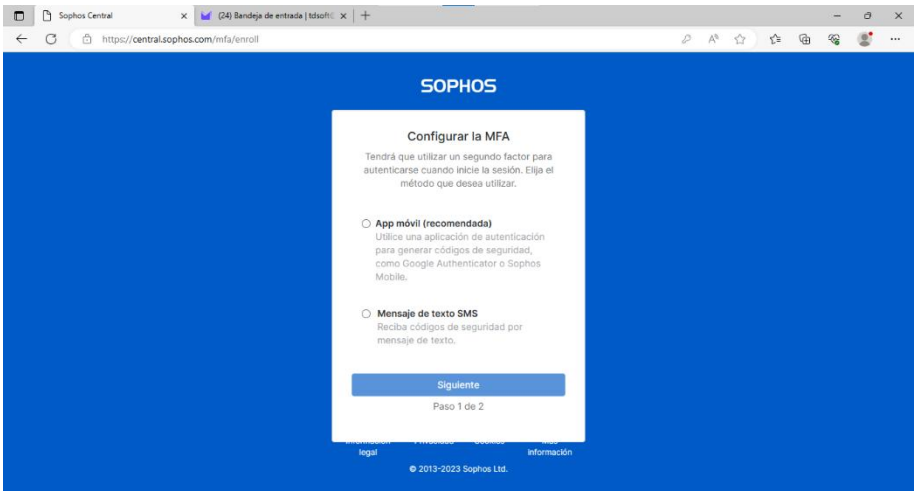


Conectando un pendrive con archivos de ransomware al ordenador, el agente no los detecta sin ejecutarlos. Hay que escanear el pendrive para que ESET los detecte y borre.

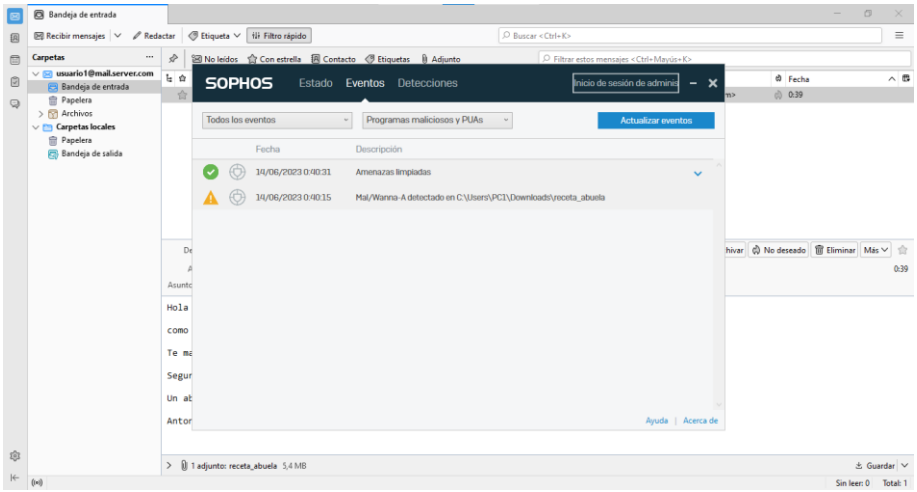


</td></tr>
<tr><td>Recursos</td><td>Teniendo el ordenador en reposo sin escanear nada nuevo tiene un consumo de memoria RAM del 41%, CPU del 20% y el disco duro del 3%.</td></tr>
</table>

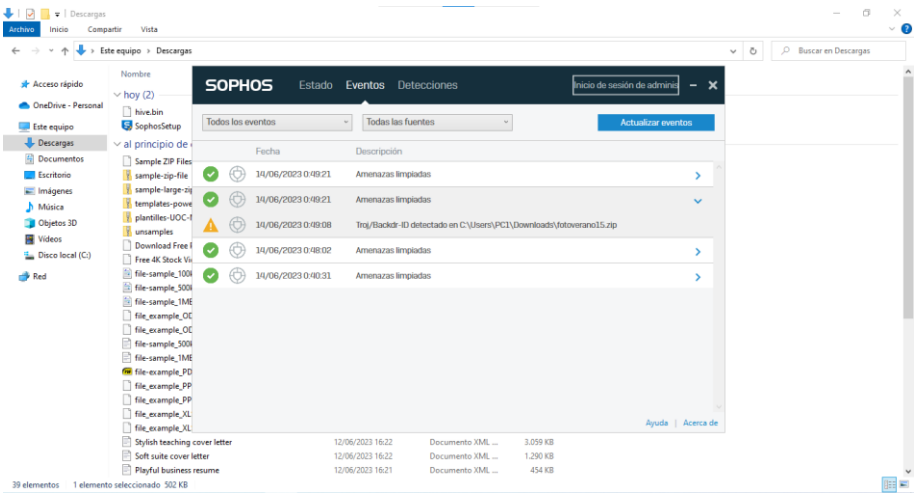

Administrador de tareas
Archivo Opciones Vista
Procesos Rendimiento Historial de aplicaciones Inicio Usuarios Detalles Servicios
CPU
20% 1,78 GHz
Memoria
3,2/7,9 GB (41%)
Disco 0 (C:)
SSD
3%
Ethernet
Ethernet
E: 0 R: 120 Kbps
GPU 0
Intel(R) HD Graphi...
4%
CPU
Intel(R) Core(TM) i3-7100U CPU @ 2.40GHz
% de uso
100 %
Actividad de la CPU
60 segundos
0
Uso
20%
Velocidad
1,78 GHz
Procesos
165
Subprocesos
1719
Identificadores
64103
Tiempo activo
0:00:09:01
Velocidad de base: 2,40 GHz
Sockets: 1
Núcleos: 2
Procesadores lógicos: 4
Virtualización: Habilitado
Caché L1: 128 kB
Caché L2: 512 kB
Caché L3: 3,0 MB
Menos detalles
Abrir el Monitor de recursos

Sophos	
Instalación	La instalación requiere dar de alta a un usuario en un formulario web. El idioma por defecto es el español. Tiene un mecanismo extra de seguridad para entrar al sistema (MFA) mediante el envío de un mensaje SMS de texto o mediante el móvil.  Una vez confirmados los datos, tarda aproximadamente 10 minutos en hacer el proceso de instalación y configuración de la parte central. A continuación, aparece una pantalla para descargarse el agente y luego el proceso de instalación del agente de unos 5 minutos aproximadamente. 
Usabilidad	La consola de gestión en el cloud permite ver información del número de ataques, estadísticas e información técnica de los ataques de una forma amena y clara, además de permitir hacer informes automáticos

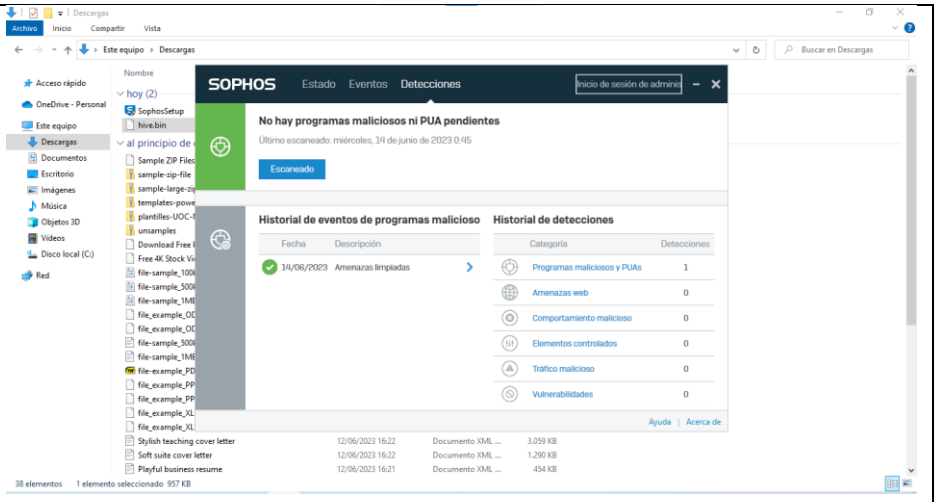
<table>
<tr><td></td><td> 
</td></tr>
<tr><td>Detección</td><td>El correo electrónico con el archivo adjunto <receta_abuela.txt> es detectado cuando llega al buzón sin abrirlo ni leerlo y queda en cuarentena, incluso cuando se intenta descargar.

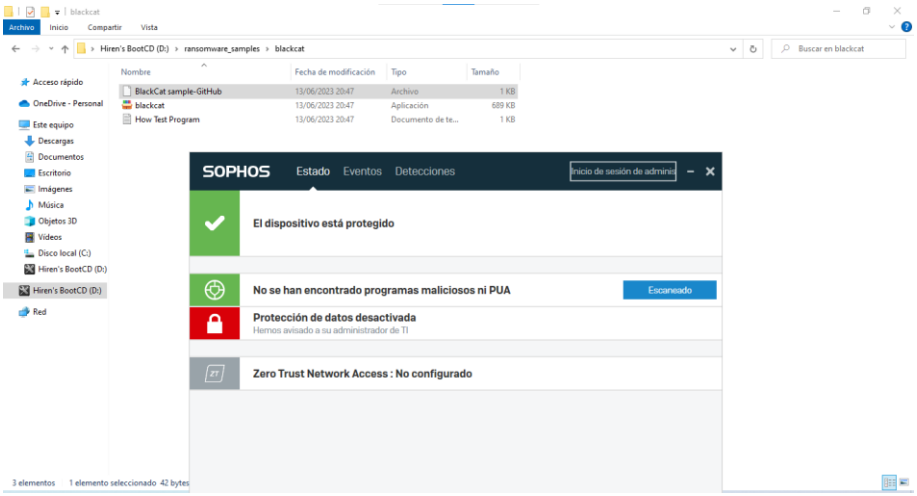
El correo electrónico con el archivo adjunto <fotoverano15.zip> no es detectado cuando llega al buzón y es en el momento de descargarlo cuando lo detecta.

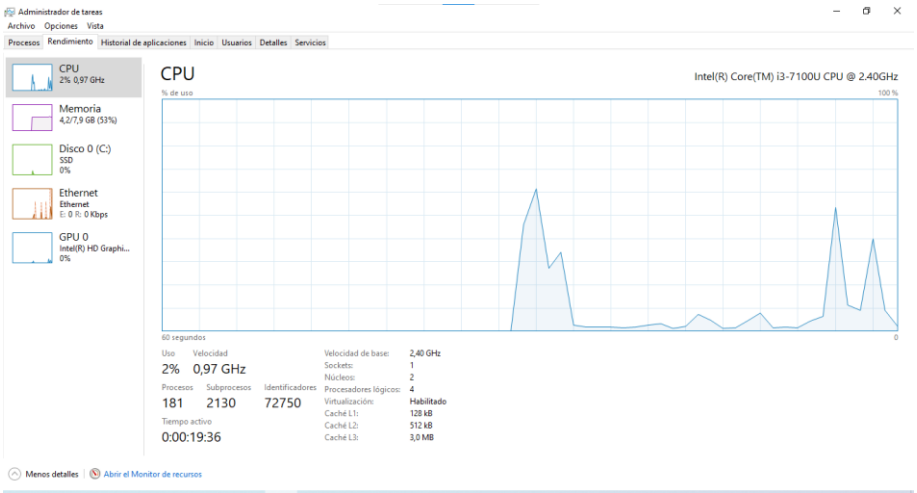
Con el correo con el adjunto del ransomware Hive, tampoco es detectado en tiempo real, hay que descargarlo y ejecutarlo. Entonces así si lo detecta.</td></tr>
</table>

<table>
<tr>
<td></td>
<td>


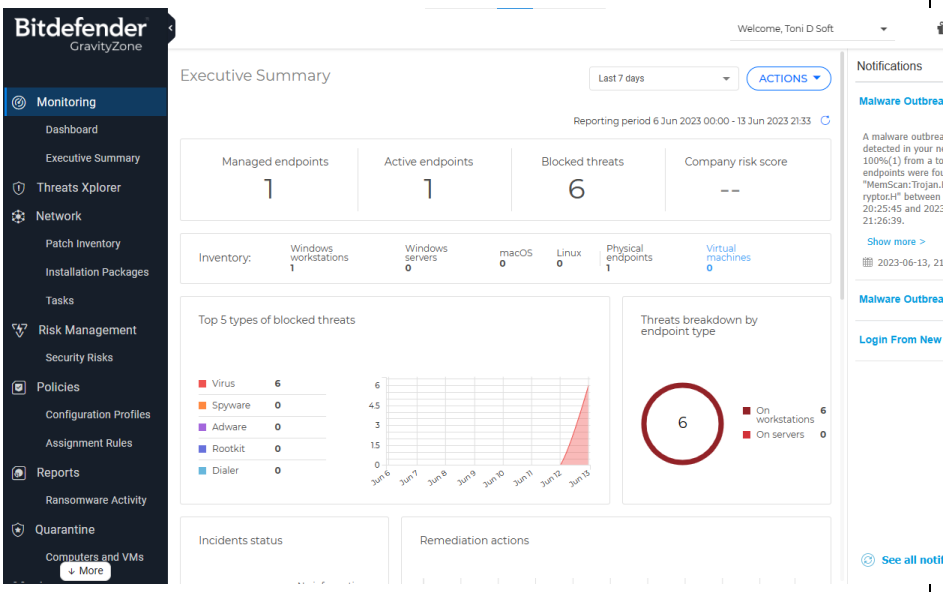
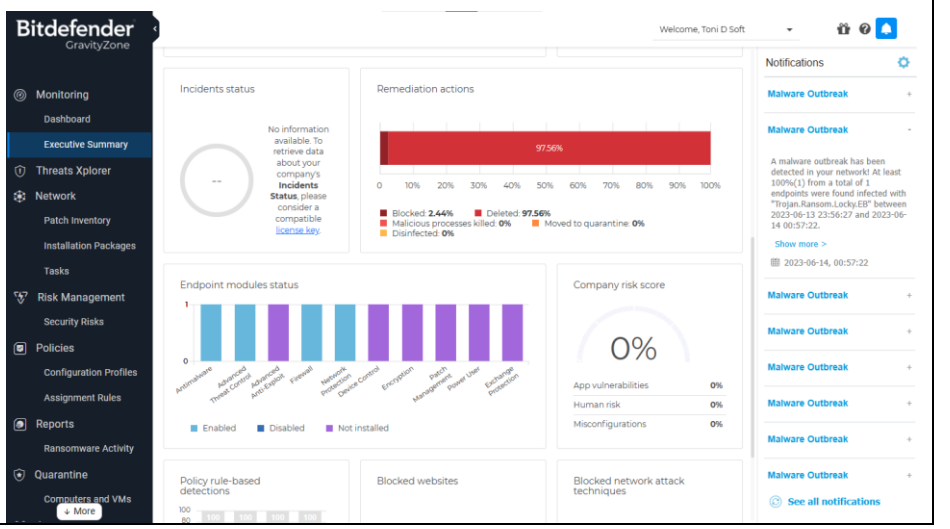
Conectando un pendrive con archivos de ransomware, el agente no los detecta sin ejecutarlos. Hay que ejecutarlos para que Sophos los detecte y borre.

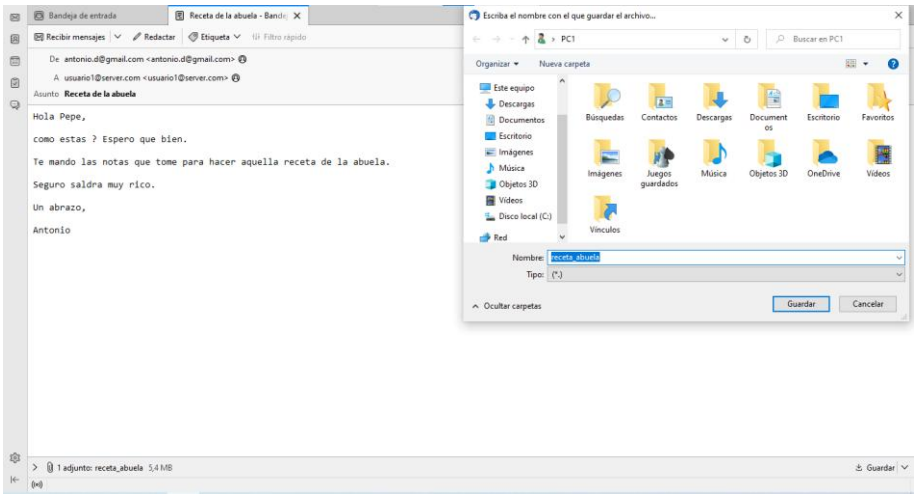
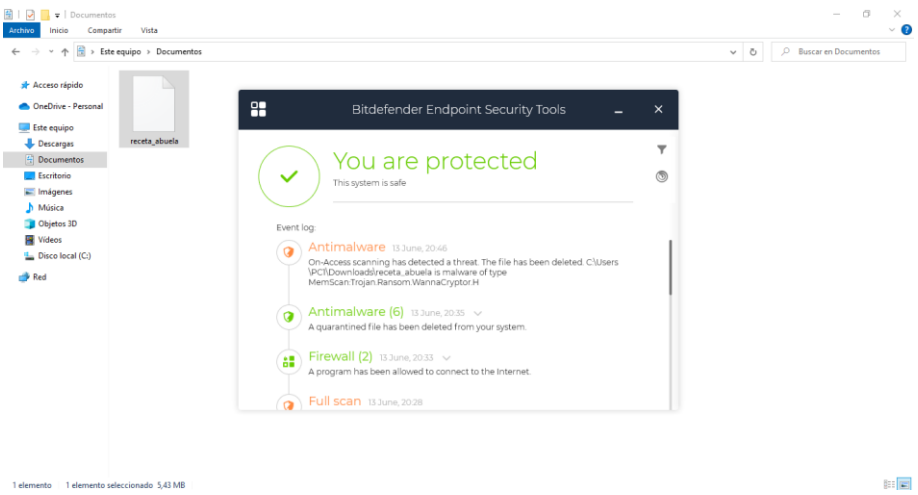
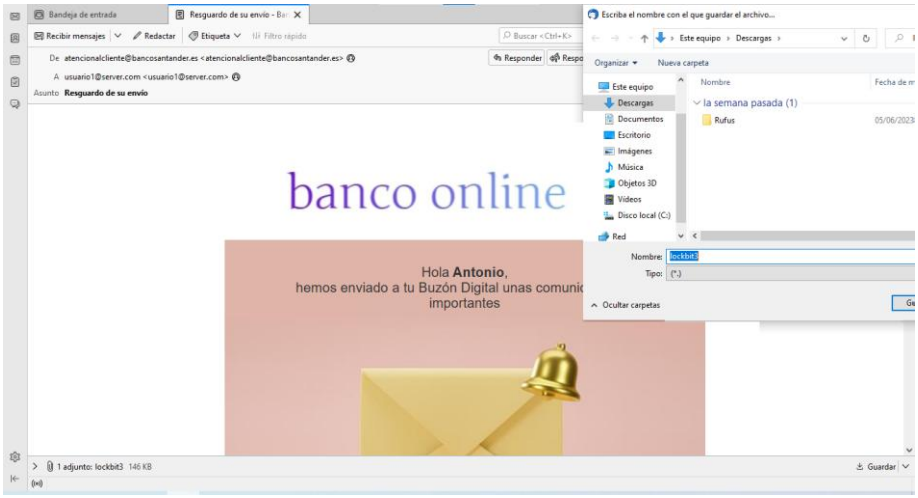


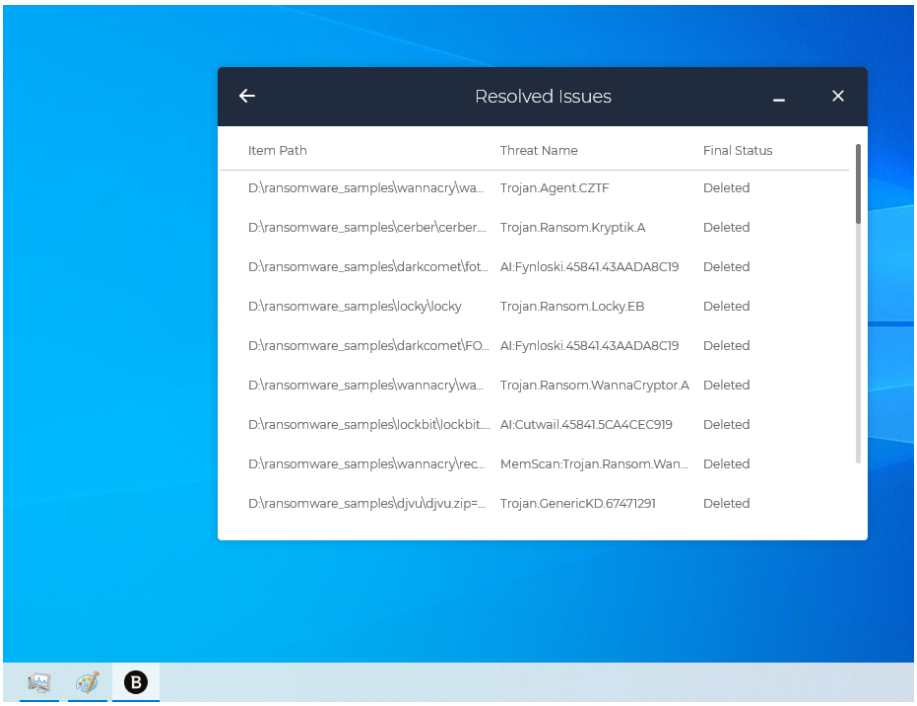
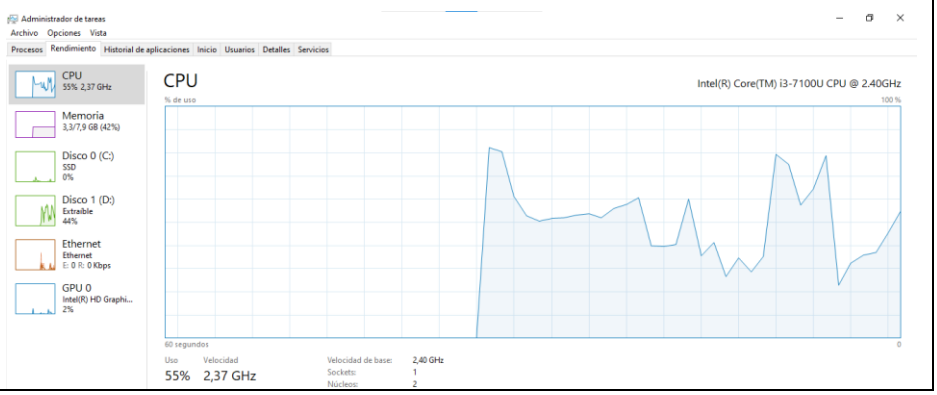
</td>
</tr>
<tr>
<td>Recursos</td>
<td>
Teniendo el ordenador en reposo sin escanear nada nuevo tiene un consumo de memoria RAM del 53%, CPU del 2% y el disco duro del 0%



</td>
</tr>
</table>

Bitdefender	
Instalación	La instalación requiere dar de alta a un usuario en un formulario web. Una vez confirmados los datos, tarda aproximadamente 10 minutos en hacer el proceso de instalación y configuración de la parte central. A continuación, aparece una pantalla para descargarse el agente y luego el proceso de instalación del agente de unos 5 minutos aproximadamente. El idioma por defecto es el inglés. Luego se pueden configurar las opciones del agente que básicamente son activar o desactivar servicios de protección.
Usabilidad	La consola de gestión en el cloud permite ver información del número de ataques, estadísticas e información técnica de los ataques de una forma amena y clara, además de permitir hacer informes automáticos.  

Detección	El correo electrónico con el archivo adjunto <receta_abuela.txt> no es detectado en tiempo real, sólo cuando se descarga e intenta ejecutar.   Igual pasa con el resto de los casos de correos con adjuntos. 

	Conectando un pendrive con archivos de ransomware, el agente no los detecta sin ejecutarlos. Hay que ejecutarlos para que Bitdefender los detecte y borre. 
Recursos	Teniendo el ordenador en reposo sin escanear nada nuevo tiene un consumo de memoria RAM del 42%, CPU del 55% y el disco duro del 0% 

3.6. Análisis existentes de soluciones comerciales anti-ransomware

Para poder encontrar información y análisis de productos o soluciones que pueden ser informáticos o no, normalmente se busca la información que pueden proporcionar los propios fabricantes en diferentes canales de comunicación escritos o digitales. En los digitales, se pueden consultar en sus propias webs:

- **Hojas de productos** (datasheets) que tienen las características y funcionalidades de los productos
- **Libros blancos** (whitepapers) que son documentos que ayudan a entender un tema, proporcionando análisis, comparativas, pruebas y más información
- Manuales de uso
- Sección de Soporte

Esta información es pública, excepto algunos informes internos o material de marketing y ventas para analizar los productos en relación con la competencia. Además, tampoco se publica la metodología de trabajo utilizada o las pruebas que se han hecho.

Para el caso de este Trabajo, los **fabricantes de soluciones de seguridad informática** hacen análisis y estudios de sus productos y soluciones frente a su competencia, desde un punto de vista de marketing y comercial.

La parte técnica es tratada de forma más superficial o no es accesible de forma pública para su consulta.

Normalmente, los fabricantes de seguridad tienen soluciones diferentes para el usuario final, pymes y grandes empresas.

Si son fabricantes para pymes, se pueden encontrar algunos análisis para pymes, pero si son fabricantes que también tienen soluciones para grandes empresas, tienen más foco en los análisis para las grandes y no tanto para las pymes, a pesar de tenerlas en su catálogo.

Y muchos de los análisis de estos fabricantes suelen ser de parte, al obedecer a los intereses de las empresas que los elaboran.

NOTA: Las soluciones anti-ransomware pueden ser una funcionalidad de la solución de antivirus o un módulo que se puede añadir al antivirus. Dependerá de cada fabricante que se considere de una forma u otra y esto también se verá en los diferentes análisis que se adjuntarán.

Existen **empresas de Consultoría y Auditoría** que realizan análisis y estudios sobre seguridad informática y ransomware. La mayoría son para grandes empresas y tienen un coste importante. También hacen estudios para pymes, con un coste.
Tenemos a Deloitte, Gartner, IDC

Existen **revistas especializadas** que realizan análisis mediante un equipo de analistas, técnicos/as y colaboradores/as donde normalmente publican sus pruebas, análisis, Pros y Contras, comentarios y conclusiones.
En pocas ocasiones publican la metodología de trabajo que han usado.
Muchas revistas están patrocinadas por fabricantes, por lo que su opinión puede verse condicionada.

De toda la información que se puede disponer en Internet, se han seleccionado las webs que tienen sus propios/as analistas, técnicos/as, investigadores/as y/o colaboradores/as, que pueden dar información y opinión técnica imparcial, siempre que estas revistas no sean patrocinadas por los fabricantes, como pasa en algunos casos.

Además, la búsqueda se ordena por el criterio de autoridad, es decir, la relevancia en un tema (la autoridad es una métrica que sustituye a la métrica de PageRank de Google que se utiliza para evaluar la importancia y relevancia de las páginas web).

Por orden de importancia en función del posicionamiento global y el número de visitas, tendríamos la siguiente clasificación de webs con análisis de soluciones anti-ransomware:

	Posicionamiento global	**Visitas totales**
Tom's Guide [114]	3.025	25,7 M
TechRadar [115]	3.307	24,6 M
PCMag [116]	3.743	21,7 M
Software Testing Help [117]	11.479	7,5 M
Cybernews [118]	23.360	3,6 M
Comparitech [119]	26.927	3,3 M
SafetyDetectives [120]	29.219	2,7 M
CRN [121]	71.733	1,2 M
SoftwareLab [122]	303.755	0,1922 M
Experte [123]	488.773	0,1132 M

Figura 9. Webs internacionales de análisis de soluciones anti-ransomware ordenadas por posicionamiento global usando la herramienta Similarweb.

Y a nivel nacional, tenemos:

	Posicionamiento global	Visitas totales
ADSLZone [124]	9.566	8,7 M
Computer Hoy [125]	9.701	8,6 M
Genbeta [126]	10.766	8,1 M
Professional Review [127]	35.772	2,4 M
Revista BYTE [128]	407.010	0,1079 M

Figura 10. Webs nacionales de análisis de soluciones anti-ransomware ordenadas por posicionamiento global usando la herramienta Similarweb.

También existen **empresas analistas independientes** especializadas en seguridad informática que hacen análisis de forma regular, publicando sus trabajos, explicando su metodología y los resultados obtenidos como:

- AV-TEST - The Independent IT-Security Institute [129]
- AV-Comparatives [130]
- Virus Bulletin [131]
- SE Labs [132]
- MRG Effitas [133]
- NSS Labs [134]
- Cybersecurity Ventures [135]

Usan un lenguaje muy técnico y esto implica que se dirijan a personas con conocimientos en el tema.

Y algunas **empresas de seguros** como Hiscox [136], AIG [137] y Beazley [138] también están haciendo análisis y estudios sobre seguridad informática, ransomware y pymes, para poder ofrecer a sus clientes más información sobre los riesgos y coberturas de sus productos de seguros, al tener que asegurar los activos de sus clientes.

4. Resultados

A partir del análisis de las soluciones anti-ransomware para pymes de ESET, Sophos y Bitdefender se obtienen unos resultados que pueden ayudar a elegir una solución u otra en función de las necesidades de las empresas, conocimientos en seguridad informática y presupuesto.

En el apartado de instalación, las 3 soluciones lo hacen de la misma manera, primero registrando al usuario, se hace un proceso de instalación de la consola que puede tardar unos 10 minutos y luego hay que instalar el agente en los diferentes dispositivos.

Sobre usabilidad y facilidad de uso del software, existen algunas diferencias.
El idioma por defecto es el inglés.

La información proporcionada sobre los ataques es diferente según sea el fabricante de software de seguridad.
Y los agentes no dan mucha información sobre los ataques, únicamente que están activo, en funcionamiento y que han detectado un ataque.

Respecto a la capacidad de detección, todas las soluciones han sido capaces de detectar el ransomware antes que se ejecutara y actuara. Hay algunas que incluso lo detectan y eliminan en tiempo real antes que se descarguen los adjuntos con la infección.
Por tanto, no ha habido infección después de probar hasta 8 tipos distintos de ransomware con el mismo hardware y con las distintas soluciones comerciales anti-ransomware para pymes.

Y a nivel de consumo de recursos, Sophos es la solución que más recursos hardware usa, en concreto a nivel de memoria RAM. El resto de las soluciones consumen de forma parecida.

5. Conclusiones y trabajos futuros

5.1. Conclusiones

Este Trabajo tiene 4 bloques importantes de contenidos:

- Estado del arte
- Laboratorio de seguridad informática
- Análisis de soluciones comerciales anti-ransomware.
- Encuesta sobre pymes y ransomware

Se han cumplido los objetivos marcados en este Trabajo que son conocer cómo ataca el ransomware a través del correo electrónico con archivos maliciosos adjuntos y como protegerse desde un punto de vista práctico, montando un laboratorio de seguridad informática, probando ransomware real y viendo cómo funcionan diversas soluciones comerciales anti-ransomware, con sus pros y contras.

Además, se ha hecho un trabajo de campo en forma de encuesta para conocer a las pymes a nivel tecnológico y su relación con el ransomware. No existen muchas encuestas públicas de este tipo y por eso se consideró que podía ser interesante, además de aprovechable para otros Trabajos incluso de otras disciplinas.

Y se considera que puede dar pie a más trabajos relacionados en base a este o aprovechando algunos componentes.
Además, este Trabajo puede servir para hacer difusión y concienciación sobre la importancia de la seguridad informática y más con el ransomware que está cada vez más presente.

Ha sido un trabajo duro, de investigación y pruebas, con varias eventualidades técnicas importantes que implicaron un cambio de configuración, pero consiguiendo los objetivos.

Para finalizar, como diría la frase de Confucio: “No son mejores los más fuertes, sino los que se levantan primero”
Aplicado al mundo de la seguridad informática, se puede tener la mejor solución de seguridad del mercado, tener muchos recursos y dinero, pero los sistemas y el software no son perfectos, están hechos por humanos y tienen vulnerabilidades, por tanto, es necesario saber cómo recuperarse de la forma más rápida, y así, levantarse primero.

5.2. Trabajos futuros

Como el ransomware va evolucionando a diario, es necesario estar actualizados a nivel de conocimientos y herramientas, para hacer frente a nuevas amenazas y ataques que puedan aparecer.

Por este motivo, los trabajos futuros pueden ser una actualización o evolución de los existentes.

Este Trabajo se ha focalizado en el vector de ataque de phishing para introducir el ransomware en los sistemas. Como hay más vectores de ataque, se podrían estudiar para otros trabajos futuros.

Como se han analizado 3 soluciones comerciales, otro trabajo futuro relacionado sería analizar otras soluciones comerciales de otros fabricantes. En el Trabajo se apuntan unas listas de fabricantes de soluciones anti-ransomware.

Hablando de soluciones comerciales, también existen soluciones anti-ransomware gratuitas que se podrían analizar para ver su efectividad y también sus diferencias con las versiones comerciales.

Normalmente la seguridad en los dispositivos móviles no está muy tratada y podría ser un trabajo futuro, poder analizar soluciones anti-ransomware para ellos que se podrían integrar con los ordenadores y que son gestionados por los endpoints.

También se podría utilizar el laboratorio existente para analizar otro tipo de software malicioso que no tenga como vector de ataque el correo electrónico.

Y además la información de la encuesta sobre los entornos tecnológicos que tienen las pymes, puede ser aprovechada para otros trabajos que tengan que estudiar a las pymes y otros aspectos que se incluyen en la encuesta.

6. Glosario

Malware
Software creado interferir en el funcionamiento normal de un ordenador.
Es un término genérico para virus, troyanos y otros programas informáticos destructivos que los ciberdelincuentes utilizan para infectar sistemas y redes con el objetivo de acceder a información sensible.

Ref: https://www.paloaltonetworks.com/cyberpedia/what-is-malware

Ransomware
El ransomware es un modelo de negocio delictivo que utiliza software malicioso para retener archivos, datos o información valiosos a cambio de un rescate. Las víctimas de un ataque de ransomware pueden ver sus operaciones gravemente degradadas o cerradas por completo.

Ref: https://www.paloaltonetworks.com/cyberpedia/what-is-ransomware

Endpoint
La seguridad de puntos finales (“endpoint”), al igual que la detección y respuesta de puntos finales, es el proceso de protección de dispositivos como estaciones de trabajo, servidores y otros dispositivos (que pueden aceptar un cliente de seguridad) frente a amenazas maliciosas y ciberataques. El software de seguridad de puntos finales permite a las empresas proteger de las ciberamenazas los dispositivos que los empleados utilizan para su trabajo los servidores que se encuentran en una red o en la nube.

Ref:https://www.fortinet.com/lat/resources/cyberglossary/what-is-endpoint-security

EDR (Endpont Detection and Response)
La detección y respuesta en puntos finales (EDR) puede detectar amenazas en los puntos finales de su organización y responder a ellas. Puede analizar la naturaleza de la amenaza y proporcionar a su equipo de TI información sobre cómo se inició, adónde ha viajado, qué está haciendo actualmente y cómo detener el ataque por completo.

Ref: https://www.fortinet.com/resources/cyberglossary/what-is-edr

XDR (Extended Detection and Response)
Basado en Endpoint Detection and Response (EDR), Extended Detection and Response (XDR), también conocido como "detección y respuesta multicapa".

XDR recopila, normaliza y luego correlaciona datos en una variedad de capas de seguridad, incluyendo puntos finales, firewalls, correo electrónico, servidores, cargas de trabajo en la nube y la red general. XDR es un nuevo enfoque alternativo a la detección tradicional y la respuesta a incidentes, que integra procedimientos de detección y respuesta en múltiples entornos para reducir el tiempo medio de detección y reparación de ataques.

Ref: https://www.fortinet.com/resources/cyberglossary/what-is-XDR

Phishing

El phishing es un tipo de amenaza de ciberseguridad que se dirige directamente a los usuarios a través del correo electrónico, mensajes de texto o mensajes directos. Durante una de estas estafas, el atacante se hará pasar por un contacto de confianza para robar datos como nombres de usuario, números de cuenta e información de tarjetas de crédito. El phishing es un tipo de ataque de ingeniería social en el que un ciberdelincuente utiliza el correo electrónico u otros mensajes de texto para robar información confidencial. Mediante el uso de una dirección de correo electrónico creíble, un atacante pretende engañar al objetivo para que confíe en él lo suficiente como para divulgar datos personales, como credenciales de inicio de sesión, números de tarjetas de crédito o información de cuentas financieras.
Ref: https://www.fortinet.com/resources/cyberglossary/phishing

Esteganografia

La esteganografía (del griego στεγανος steganos, "cubierto" u "oculto", y γραφος graphos, "escritura") trata el estudio y aplicación de técnicas que permiten ocultar mensajes u objetos, dentro de otros, llamados portadores, para que no se perciba su existencia.
Ref: https://es.wikipedia.org/wiki/Esteganograf%C3%ADa

7. Bibliografía

[1] Ministerior del Interior, «Informe sobre la cibercriminalidad en España 2021,» [En línea]. Available: 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. [Último acceso: Abril 2023].

[2] BlackFog, «The State of Ransomware in 2023,» 3 Abril 2023. [En línea]. Available: https://www.blackfog.com/the-state-of-ransomware-in-2023/. [Último acceso: Abril 2023].

[3] «Agencia Española de Protección de Datos,» [En línea]. Available: https://www.aepd.es/. [Último acceso: 05 2023].

[4] Naciones Unidas, «Objetivos y metas de desarrollo sostenible,» 17 Septiembre 2015. [En línea]. Available: https://www.un.org/sustainabledevelopment/es/objetivos-de-desarrollo-sostenible/. [Último acceso: Marzo 2023].

[5] Naciones Unidas, «Educación - Desarrollo Sostenible,» 7 Enero 2015. [En línea]. Available: https://www.un.org/sustainabledevelopment/es/education/. [Último acceso: Marzo 2023].

[6] Naciones Unidas, «Energía,» 7 Enero 2015. [En línea]. Available: https://www.un.org/sustainabledevelopment/es/energy/. [Último acceso: Marzo 2023].

[7] Naciones Unidas, «Infraestructura,» 7 Enero 2015. [En línea]. Available: https://www.un.org/sustainabledevelopment/es/infrastructure/. [Último acceso: Marzo 2023].

[8] Naciones Unidas, «Ciudades,» 7 Enero 2015. [En línea]. Available: https://www.un.org/sustainabledevelopment/es/cities/. [Último acceso: Marzo 2023].

[9] Naciones Unidas, «Consumo y producción sostenibles,» 14 Enero 2015. [En línea]. Available: https://www.un.org/sustainabledevelopment/es/sustainable-consumption-production/. [Último acceso: Marzo 2023].

[10] Naciones Unidas, «Cambio climático,» 7 Enero 2015. [En línea]. Available: https://www.un.org/sustainabledevelopment/es/climate-change-2/. [Último acceso: Marzo 2023].

[11] Naciones Unidas, «Océanos,» 7 Enero 2015. [En línea]. Available: https://www.un.org/sustainabledevelopment/es/oceans/. [Último acceso: Marzo 2023].

[12] Naciones Unidas, «Bosques, desertización y diversidad biológica,» 7

Enero 2015. [En línea]. Available: https://www.un.org/sustainabledevelopment/es/biodiversity/. [Último acceso: Marzo 2023].

[13] Naciones Unidas, «Pobreza,» 18 Julio 2018. [En línea]. Available: https://www.un.org/sustainabledevelopment/es/poverty/. [Último acceso: Marzo 2023].

[14] Naciones Unidas, «Hambre y seguridad alimentaria,» 7 Enero 2015. [En línea]. Available: https://www.un.org/sustainabledevelopment/es/hunger/. [Último acceso: Marzo 2023].

[15] Naciones Unidas, «Agua y saneamiento,» 7 Enero 2015. [En línea]. Available: https://www.un.org/sustainabledevelopment/es/water-and-sanitation/. [Último acceso: Marzo 2023].

[16] Naciones Unidas, «Crecimiento económico,» 7 Enero 2015. [En línea]. Available: https://www.un.org/sustainabledevelopment/es/economic-growth/. [Último acceso: Marzo 2023].

[17] Naciones Unidadas, «Paz y Justicia,» 14 Enero 2015. [En línea]. Available: https://www.un.org/sustainabledevelopment/es/peace-justice/. [Último acceso: Marzo 2023].

[18] Naciones Unidas, «Igualdad de género y empoderamiento de la mujer,» 7 Enero 2015. [En línea]. Available: https://www.un.org/sustainabledevelopment/es/gender-equality/. [Último acceso: Marzo 2023].

[19] Naciones Unidas, «Reducir las desigualdades entre países y dentro de ellos,» 7 Enero 2015. [En línea]. Available: https://www.un.org/sustainabledevelopment/es/inequality/. [Último acceso: Marzo 2023].

[20] AV-TEST, «AV-TEST Award 2022,» [En línea]. Available: https://www.av-test.org/en/news/av-test-award-2022-tested-and-award-winning-security/. [Último acceso: Marzo 2023].

[21] Sophos, «Ransomware: Frequently asked questions,» 7 Marzo 2022. [En línea]. Available: https://support.sophos.com/support/s/article/KB-000036269. [Último acceso: Marzo 2023].

[22] Bitdefender, «What is Ransomware? Prevention & Data Recovery,» 23 Abril 2019. [En línea]. Available: https://www.bitdefender.com/consumer/support/answer/24260/. [Último acceso: Marzo 2023].

[23] Kaspersky, «Ransomware: definición, prevención y eliminación,» 2022, 18 Febrero. [En línea]. Available: https://www.kaspersky.es/resource-center/threats/ransomware. [Último acceso: Marzo 2023].

[24] Microsoft, «What is ransomware ?,» [En línea]. Available: https://www.microsoft.com/en-us/security/business/security-101/what-is-ransomware. [Último acceso: Marzo 2023].

[25] McAfee, «¿Qué es el malware?,» 15 Mayo 202. [En línea]. Available: https://www.mcafee.com/es-es/antivirus/malware.html. [Último acceso: Marzo 2023].

[26] Norton, «100+ ransomware statistics for 2023 and beyond,» [En línea]. Available: https://us.norton.com/blog/emerging-threats/ransomware-

statistics. [Último acceso: Marzo 2023].

[27] Trend Micro, «Protección contra en ransomware,» [En línea]. Available: https://www.trendmicro.com/es_es/forHome/campaigns/ransomware-protection.html. [Último acceso: Marzo 2023].

[28] AV-Comparatives, «AV-Comparatives Awards 2022,» 24 Febrero 2023. [En línea]. Available: https://www.av-comparatives.org/av-comparatives-awards-2022/. [Último acceso: Marzo 2023].

[29] ESET, «ESET Ransomware: Cómo afecta a tu empresa,» [En línea]. Available: https://www.eset.com/es/ransomware-empresas. [Último acceso: Marzo 2023].

[30] Watchguard, «Ransomware,» [En línea]. Available: https://www.watchguard.com/es/wgrd-solutions/security-threats/ransomware. [Último acceso: Marzo 2023].

[31] Agència de Ciberseguretat de Catalunya, «Ransomware: què és i que faig ?,» [En línea]. Available: https://ciberseguretat.gencat.cat/ca/detalls/noticia/Ransomware-que-es-i-que-faig. [Último acceso: 8 Marzo 2023].

[32] INCIBE, «Qué es el ransomware y cómo recupero mi información,» 16 Abril 2020. [En línea]. Available: https://www.incibe.es/protege-tu-empresa/blog/el-ransomware-y-recupero-mi-informacion. [Último acceso: Marzo 2023].

[33] Europol, «Ransomware: What you need to know,» Europol, [En línea]. Available: https://www.europol.europa.eu/cms/sites/default/files/documents/ransomware-what_you_need_to_know.pdf. [Último acceso: Marzo 2023].

[34] ENISA, «Glossary: Ransomware,» 2017. [En línea]. Available: https://www.enisa.europa.eu/topics/incident-response/glossary/ransomware. [Último acceso: Marzo 2023].

[35] Interpol, «Cybercrime – #YouMayBeNext,» [En línea]. Available: https://www.interpol.int/Crimes/Cybercrime/Cybercrime-YouMayBeNext. [Último acceso: Marzo 2023].

[36] NCSC - Gov.uk, «A guide to ransomware,» [En línea]. Available: https://www.ncsc.gov.uk/ransomware/home. [Último acceso: Marzo 2023].

[37] Federal Bureau of Investigation (FBI), «Ransomware,» 3 Abril 2020. [En línea]. Available: https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/ransomware. [Último acceso: Marzo 2023].

[38] NIST, «Ransomware,» 27 Septiembre 2021. [En línea]. Available: https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/ransomware. [Último acceso: Marzo 2023].

[39] Cybersecurity and Infrastructure Security Agency CISA, «Ransomware Guide,» [En línea]. Available: https://www.cisa.gov/stopransomware/ransomware-guide. [Último acceso: Marzo 2023].

[40] Kaspersky, «Ransomware attacks and types – how encryption Trojans differ,» 9 Febrero 2022. [En línea]. Available:

https://www.kaspersky.com/resource-center/threats/ransomware-attacks-and-types. [Último acceso: Marzo 2023].

[41] Norton, «Types of ransomware to recognize + ransomware protection tips,» [En línea]. Available: https://us.norton.com/blog/malware/types-of-ransomware. [Último acceso: Marzo 2023].

[42] WeLiveSecurity by ESET, «Ransomware como servicio (RaaS): qué es y cómo funciona este modelo,» 23 Febrero 2022. [En línea]. Available: https://www.welivesecurity.com/la-es/2022/02/23/ransomware-as-a-service-raas-que-es-como-funciona/. [Último acceso: Marzo 2023].

[43] WeLiveSecurity by ESET, «Qué es la DarkWeb, la DeepWeb y la DarkNet y cuáles son sus diferencias,» 23 Marzo 2023. [En línea]. Available: https://www.welivesecurity.com/la-es/2023/03/23/que-es-darkweb-deepweb-darknet-diferencias/. [Último acceso: Marzo 2023].

[44] ENISA, «Ransomware: Publicly Reported Incidents are only the tip of the iceberg,» 29 Julio 2022. [En línea]. Available: https://www.enisa.europa.eu/news/ransomware-publicly-reported-incidents-are-only-the-tip-of-the-iceberg. [Último acceso: Marzo 2023].

[45] RedesZone, «Cómo funciona un ataque ransomware y qué herramientas se usan,» 7 Junio 2020. [En línea]. Available: https://www.redeszone.net/tutoriales/seguridad/ataques-ransomware-como-son-herramientas/. [Último acceso: Marzo 2023].

[46] Artic Wolf, «How ransomware works,» 29 Marzo 2023. [En línea]. Available: https://arcticwolf.com/resources/blog/how-ransomware-works/. [Último acceso: Marzo 2023].

[47] Bitdefender, «¿Qué es el Phishing? Reconocer y evitar las estafas de phishing,» 6 Septiembre 2022. [En línea]. [Último acceso: Marzo 2023].

[48] Cloudflare, «¿Qué es el movimiento lateral?,» [En línea]. Available: https://www.cloudflare.com/es-es/learning/security/glossary/what-is-lateral-movement/. [Último acceso: Marzo 2023].

[49] Sophos, «Recursos de Sophos para detener el Ransomware,» [En línea]. Available: https://www.sophos.com/es-es/content/ransomware. [Último acceso: Marzo 2023].

[50] Bitdefender, «Antimalware > Best practices > Protecting from ransomware,» [En línea]. Available: https://www.bitdefender.com/business/support/en/77212-151120-best-practices.html. [Último acceso: Marzo 2023].

[51] Kaspersky, «Ransomware protection: How to keep your data safe in 2023,» 27 Enero 2023. [En línea]. Available: https://www.kaspersky.com/resource-center/threats/how-to-prevent-ransomware. [Último acceso: Marzo 2023].

[52] Microsoft Security Blog, «3 steps to prevent and recover from ransomware,» 7 Septiembre 2021. [En línea]. Available: https://www.microsoft.com/en-us/security/blog/2021/09/07/3-steps-to-prevent-and-recover-from-ransomware/. [Último acceso: Marzo 2023].

[53] McAfee, «How to prevent A ransomware attack,» [En línea]. Available: https://www.mcafee.com/en-us/antivirus/how-to-prevent-ransomware-attacks.html. [Último acceso: Marzo 2023].

[54] Norton, «What is ransomware? Ransomware explained and how it works,» [En línea]. Available: https://us.norton.com/blog/malware/ransomware-5-dos-and-donts. [Último acceso: Marzo 2023].

[55] Trend Micro, «Ransomware: Solutions, Best Practice Configuration and Prevention using Trend Micro products,» 29 Julio 2021. [En línea]. Available: https://success.trendmicro.com/dcx/s/solution/1112223-ransomware-solutions-best-practice-configuration-and-prevention-using-trend-micro-products. [Último acceso: Marzo 2023].

[56] Watchguard, «Tres Consejos de Mejores Prácticas para Prevenir Ataques de Ransomware,» [En línea]. Available: https://www.watchguard.com/es/wgrd-resource-center/report/ransomware-consejos-de-mejores-practicas-es-419. [Último acceso: Marzo 2023].

[57] Agència de Ciberseguretat de Catalunya, «Comunicat de ciberseguretat Amenaça Ransomware,» 29 Noviembre 2021. [En línea]. Available: https://ciberseguretat.gencat.cat/web/.content/04_actualitat/Avisos/2021/PDF/Comunicat-de-ciberseguretat-Ransomware_10112021.pdf. [Último acceso: Marzo 2023].

[58] INCIBE, «Ransomware - Una guía de aproximación para el empresario,» 2020. [En línea]. Available: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ransomware.pdf. [Último acceso: Marzo 2023].

[59] Europol, «Tips & advice to prevent ransomware from infecting your electronic devices,» [En línea]. Available: https://www.europol.europa.eu/operations-services-and-innovation/public-awareness-and-prevention-guides/tips-advice-to-prevent-ransomware-infecting-your-electronic-devices. [Último acceso: Marzo 2023].

[60] ENISA, «Ransomware De enero de 2019 a abril de 2020,» [En línea]. Available: https://www.enisa.europa.eu/publications/report-files/ETL-translations/es/etl2020-ransomware-ebook-en-es.pdf. [Último acceso: Marzo 2023].

[61] NCSC - Gov.uk, «Prevent and protect against ransomware,» [En línea]. Available: https://www.ncsc.gov.uk/ransomware/home#section_4. [Último acceso: Marzo 2023].

[62] Federal Bureau of Investigation (FBI), «Ransomware prevention and response for CISOs,» 14 Julio 2016. [En línea]. Available: https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view. [Último acceso: Marzo 2023].

[63] NIST, «Ransomware protection and response,» 4 Mayo 2021. [En línea]. Available: https://csrc.nist.gov/projects/ransomware-protection-and-response. [Último acceso: Marzo 2023].

[64] NIST, «Quick steps you can take now to PROTECT yourself from the threat of ransomware,» [En línea]. Available: https://csrc.nist.gov/CSRC/media/Projects/ransomware-protection-and-response/documents/NIST_Ransomware_Tips_and_Tactics_Infographic.pdf. [Último acceso: Marzo 2023].

[65] Sophos, «Ransomware: Recovery and removal,» 8 Febrero 2023. [En línea]. Available: https://support.sophos.com/support/s/article/KB-000036273?language=en_US#Anchor4. [Último acceso: Marzo 2023].

[66] Bitdefender, «The clock is ticking: What to do immediately after a ransomware attack,» 28 Marzo 2022. [En línea]. Available: https://businessinsights.bitdefender.com/the-clock-is-ticking-what-to-do-immediately-after-a-ransomware-attack. [Último acceso: Marzo 2023].

[67] Kaspersky, «Han cifrado tus datos, ¿y ahora qué?,» 19 02 2021. [En línea]. Available: https://www.kaspersky.es/blog/ransomware-attack-what-to-do/24774/. [Último acceso: Marzo 2023].

[68] Microsoft, «10 things you should do after a ransomware attack,» 18 Noviembre 2022. [En línea]. Available: https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/10-things-you-should-do-after-a-ransomware-attack. [Último acceso: Marzo 2023].

[69] McAfee, «What are ransomware attacks? An in-depth guide,» 27 Junio 2022. [En línea]. Available: https://www.mcafee.com/learn/what-are-ransomware-attacks-an-in-depth-guide/. [Último acceso: Marzo 2023].

[70] Norton, «Ransomware – what can you do about it,» [En línea]. Available: https://us.norton.com/blog/emerging-threats/ransomware-what-can-you-do-about-it. [Último acceso: Marzo 2023].

[71] ESET, «RANSOMWARE Security Tips for SMBs,» 2022. [En línea]. Available: https://www.eset.com/fileadmin/ESET/INT/Pages/SMB_topic_pages/Ransomware_LP_2022/Ransomware_Security_Tips_for_SMBs.pdf. [Último acceso: Marzo 2023].

[72] Europol, «Hit by ransomware? No More Ransom now offers 136 free tools to rescue your files,» [En línea]. Available: https://www.europol.europa.eu/media-press/newsroom/news/hit-ransomware-no-more-ransom-now-offers-136-free-tools-to-rescue-your-files. [Último acceso: Marzo 2023].

[73] ENISA, «ENISA Threat Landscape for ransomware attacks. 2022,» 29 Julio 2022. [En línea]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-ransomware-attacks/view/++widget++form.widgets.execSummary/@@download/ENISA+Threat+Landscape+for+Ransomware+Attacks.pdf. [Último acceso: Marzo 2023].

[74] NCSC - Gov.uk, «Respond and recover from ransomware,» [En línea]. Available: https://www.ncsc.gov.uk/ransomware/home#section_6. [Último acceso: Marzo 2023].

[75] Federal Bureau of Investigation (FBI), «Ransomware: What It Is & What To Do About It,» 02 04 2021. [En línea]. Available: https://www.ic3.gov/Content/PDF/Ransomware_Fact_Sheet.pdf. [Último acceso: Marzo 2023].

[76] Cybersecurity and Infrastructure Security Agency CISA, «I've been hit by ransomware!,» [En línea]. Available: https://www.cisa.gov/stopransomware/ive-been-hit-ransomware . [Último acceso: Marzo 2023].

[77] Europol, «The No More Ransom Project,» 2021. [En línea]. Available: https://www.nomoreransom.org/. [Último acceso: Abril 2023].

[78] Trellix, «The threat report: February 2023,» [En línea]. Available: https://www.trellix.com/en-us/advanced-research-center/threat-reports/feb-2023.html#globalransomware. [Último acceso: Abril 2023].

[79] Trellix, «The threat report: Fall 2022,» [En línea]. Available: https://www.trellix.com/en-us/advanced-research-center/threat-reports/nov-2022.html#globalRansomware. [Último acceso: Abril 2023].

[80] Trend Micro, «Ransomware spotlight: Cuba,» 7 Diciembre 2022. [En línea]. Available: https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-cuba. [Último acceso: Abril 2023].

[81] Cybersecurity and Infrastructure Security Agency CISA, «#StopRansomware: Cuba Ransomware,» 5 Enero 2023. [En línea]. Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-335a. [Último acceso: Abril 2023].

[82] Microsoft, «PsExec - sysinternals,» [En línea]. Available: https://learn.microsoft.com/en-us/sysinternals/downloads/psexec. [Último acceso: Abril 2023].

[83] INCIBE, «Estudio del análisis de HIVE,» Diciembre 2021. [En línea]. Available: https://www.incibe.es/sites/default/files/contenidos/estudios/doc/incibe-cert_estudio_analisis_hive_2021_v1.pdf. [Último acceso: Abril 2023].

[84] Cybersecurity and Infrastructure Security Agency CISA, «#StopRansomware: Hive ransomware,» 25 Noviembre 2022. [En línea]. Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-321a. [Último acceso: Abril 2023].

[85] Trend Micro, «Ransomware spotlight: Hive,» 18 Marzo 2022. [En línea]. Available: https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-hive. [Último acceso: Abril 2023].

[86] Github.io, «UPX: The Ultimate Packer for eXecutables,» [En línea]. Available: https://upx.github.io/. [Último acceso: Abril 2023].

[87] Trend Micro, «Ransomware spotlight: LockBit,» 8 Febrero 2022. [En línea]. Available: https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-lockbit. [Último acceso: Abril 2023].

[88] Cybersecurity and Infrastructure Security Agency CISA, «#StopRansomware: LockBit 3.0,» 16 Marzo 2023. [En línea]. Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-075a. [Último acceso: Abril 2023].

[89] Malwarebytes, «A first look at the builder for LockBit 3.0 Black,» 23 Septiembre 2022. [En línea]. Available: https://www.malwarebytes.com/blog/news/2022/09/lockbit-builder-leaked-by-disgruntled-developer. [Último acceso: Abril 2023].

[90] Trend Micro, «Ransomware spotlight: BlackCat,» 27 Octubre 2022. [En línea]. Available:

https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-blackcat. [Último acceso: Abril 2023].

[91] Federal Bureau of Investigation (FBI), «BlackCat/ALPHV Ransomware Indicators of Compromise,» 19 Abril 2022. [En línea]. Available: https://www.ic3.gov/Media/News/2022/220420.pdf. [Último acceso: Abril 2023].

[92] Trend Micro, «WannaCry/Wcry Ransomware: How to Defend against It,» 13 Mayo 2017. [En línea]. Available: https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/wannacry-wcry-ransomware-how-to-defend-against-it. [Último acceso: Abril 2023].

[93] Sophos, «Sophos guidance on WannaCry ransomware,» 15 Mayo 2017. [En línea]. Available: https://news.sophos.com/en-us/2017/05/15/sophos-guidance-on-wannacry-ransomware/. [Último acceso: Abril 2023].

[94] Europol, «Wannacry Ransomware,» 6 Noviembre 2017. [En línea]. Available: https://www.europol.europa.eu/wannacry-ransomware. [Último acceso: Abril 2023].

[95] Agencia Española de Protección de Datos (AEPD), «Brechas de seguridad: Ransomware y gestión del riesgo,» 15 Diciembre 2020. [En línea]. Available: https://www.aepd.es/es/prensa-y-comunicacion/blog/brechas-de-seguridad-ransomware. [Último acceso: Abril 2023].

[96] RGPD, «Artículo 33 UE Reglamento general de protección de datos,» [En línea]. Available: https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32016R0679&from=ES#d1e3494-1-1. [Último acceso: Abril 2023].

[97] Agencia Española de Protección de Datos (AEPD), «Notificación de brechas de datos personales a la Autoridad de Control,» [En línea]. Available: https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/brechas-de-datos-personales-notificacion. [Último acceso: Abril 2023].

[98] RGPD, «Artículo 34 UE Reglamento general de protección de datos,» [En línea]. Available: https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32016R0679&from=ES#d1e3550-1-1. [Último acceso: Abril 2023].

[99] Agencia Española de Protección de Datos (AEPD), «Comunicación de brechas de datos personales a los interesados,» 20 Octubre 2022. [En línea]. Available: https://www.aepd.es/es/derechos-y-deberes/cumple-tus-deberes/medidas-de-cumplimiento/comunicacion-de-brechas-de-datos. [Último acceso: Abril 2023].

[100] HispaColex Abogados, «¿Qué responsabilidad legal pueden tener la empresa y los empleados ante un ciberataque?,» 10 Diciembre 2020. [En línea]. Available: https://www.hispacolex.com/blog/blog-derecho-seguros/que-responsabilidad-legal-pueden-tener-la-empresa-y-los-empleados-ante-un-ciberataque/. [Último acceso: Abril 2023].

[101] BOE, «BOE-A-1889-4763 Real Decreto de 24 de julio de 1889 por el que se publica el Código Civil,» [En línea]. Available: https://www.boe.es/eli/es/rd/1889/07/24/(1)/con. [Último acceso: Abril

2023].

[102] Dirección General de Industria y de la Pequeña y Mediana Empresa. Ministerio de Industria, Comercio y Turismo, Marzo 2023. [En línea]. Available: http://www.ipyme.org/es-ES/ApWeb/EstadisticasPYME/Documents/CifrasPYME-marzo2023.pdf. [Último acceso: Abril 2023].

[103] Dnsmasq, «Dnsmasq,» [En línea]. Available: https://dnsmasq.org/. [Último acceso: 05 2023].

[104] «Postfix,» [En línea]. Available: http://www.postfix.org/. [Último acceso: 05 2023].

[105] Dovecot, «Dovecot | The Secure IMAP Server,» [En línea]. Available: https://www.dovecot.org/. [Último acceso: 05 2023].

[106] «SendEmail | GitHub,» [En línea]. Available: https://github.com/zehm/sendEmail. [Último acceso: 06 2023].

[107] «Resource Hacker,» [En línea]. Available: http://www.angusj.com/resourcehacker/. [Último acceso: 05 2023].

[108] Triage, «Triage,» [En línea]. Available: https://tria.ge/. [Último acceso: 05 2023].

[109] M. Bazaar. [En línea]. Available: https://bazaar.abuse.ch/. [Último acceso: 05 2023].

[110] M. d. A. E. y. T. Digital, «Kit Digital Ciberseguridad,» [En línea]. Available: https://www.acelerapyme.gob.es/kit-digital/ciberseguridad. [Último acceso: 05 2023].

[111] ESET, «ESET PROTECT Complete,» [En línea]. Available: https://www.eset.com/es/empresas/pack-complete-protection/. [Último acceso: 05 2023].

[112] Sophos, «Intercept X Endpoint,» [En línea]. Available: https://www.sophos.com/es-es/products/endpoint-antivirus.

[113] Bitdefender, «GravityZone Business Security,» [En línea]. Available: https://www.bitdefender.es/business/smb-products/business-security.html. [Último acceso: 05 2023].

[114] T. Guide, «The best antivirus software 2023: Free and paid options,» 11 04 2022. [En línea]. Available: https://www.tomsguide.com/us/best-antivirus,review-2588.html. [Último acceso: 05 2023].

[115] TechRadar, «Best ransomware protection of 2023,» 24 6 2022. [En línea]. Available: https://www.techradar.com/best/best-ransomware-protection. [Último acceso: 5 2023].

[116] PCMAG, «The best ransomware protection for 2023,» 24 4 2017. [En línea]. Available: https://www.pcmag.com/picks/the-best-ransomware-protection. [Último acceso: 05 2023].

[117] [En línea]. Available: https://www.softwaretestinghelp.com/anti-ransomware-software/. [Último acceso: 05 2023].

[118] Cybernews.com. [En línea]. Available: https://cybernews.com/best-antivirus-software/best-ransomware-protection/. [Último acceso: 05 2023].

[119] Comparitech, «6 best ransomware protection tools for 2023 (paid &

free),» 22 11 2019. [En línea]. Available: https://www.comparitech.com/net-admin/ransomware-protection-tools/. [Último acceso: 05 2023].

[120] SafetyDetectives, «10 best antivirus software in 2023: Windows, android, iOS & mac,» 06 11 2021. [En línea]. Available: https://www.safetydetectives.com/. [Último acceso: 05 2023].

[121] CRN, «10 ransomware protection tools you need to know about,» 17 9 2020. [En línea]. Available: https://www.crn.com/slide-shows/security/10-ransomware-protection-tools-you-need-to-know-about. [Último acceso: 5 2023].

[122] SoftwareLab, «The 5 best antivirus (2023): Comparison of June,» [En línea]. Available: https://softwarelab.org/best-antivirus-software/. [Último acceso: 05 2023].

[123] Experte.com, «Best anti-ransomware 2023: TOP 5 defenders against ransomware,» [En línea]. Available: https://www.experte.com/antivirus/anti-ransomware. [Último acceso: 05 2023].

[124] ADSLZone, «Antiransomware, la solución de seguridad para proteger tus datos,» 30 5 2020. [En línea]. Available: https://www.adslzone.net/reportajes/antivirus/anti-ransomware/. [Último acceso: 05 2023].

[125] Computerhoy.com, «Mejores antivirus para PC y móvil de 2022: ¿qué debes tener en cuenta para protegerte?,» [En línea]. Available: https://computerhoy.com/antivirus. [Último acceso: 05 2023].

[126] Genbeta.com, «Los 12 mejores antivirus de 2023 para Windows hasta la fecha,» 05 04 2023. [En línea]. Available: https://www.genbeta.com/a-fondo/once-mejores-antivirus-2022-para-windows-ahora. [Último acceso: 05 2023].

[127] P. Review, «▷ Mejores antivirus del mercado 2023 para PC, PAGO y GRATIS,» 15 09 2022. [En línea]. Available: https://www.profesionalreview.com/software/mejores-antivirus/. [Último acceso: 05 2023].

[128] R. B. TI, «Comparativa: 9 soluciones de seguridad Endpoint 2019,» 11 12 2019. [En línea]. Available: https://revistabyte.es/comparativa/comparativa-soluciones-seguridad-endpoint/. [Último acceso: 05 2023].

[129] Av-test, «Av-test,» [En línea]. Available: https://www.av-test.org/. [Último acceso: 05 2023].

[130] AV-Comparatives, «AV-Comparatives,» 28 7 2014. [En línea]. Available: https://www.av-comparatives.org/.

[131] Virusbulletin.com, «Virusbulletin.com,» [En línea]. Available: https://www.virusbulletin.com/. [Último acceso: 05 2023].

[132] S. Labs, «IT security testing by SE Labs: Next-gen, full attack chain testing,» 22 2 2020. [En línea]. Available: https://selabs.uk/. [Último acceso: 05 2023].

[133] M. Effitas, «MRG Effitas - world-leading, independent IT security testing,» 12 2 2015. [En línea]. Available: https://www.mrg-effitas.com/.

[Último acceso: 05 2023].

[134] N. Labs, «NSS Labs,» 25 9 2020. [En línea]. Available: https://nsslabs.com/. [Último acceso: 05 2023].

[135] C. Magazine, «Cybercrime Magazine - page one for the cybersecurity industry,» 26 12 2018. [En línea]. Available: https://cybersecurityventures.com/. [Último acceso: 05 2023].

[136] Hiscox.es, «Informe de Ciberpreparación de Hiscox 2022,» [En línea]. Available: https://www.hiscox.es/informe-de-ciberpreparacion-de-hiscox-2022. [Último acceso: 05 2023].

[137] aig, «Cyber insurance,» [En línea]. Available: https://www.aig.com/home/risk-solutions/business/cyber. [Último acceso: 05 2023].

[138] beazley, «Cyber,» [En línea]. Available: https://www.beazley.com/en-us/products/cyber-usa. [Último acceso: 05 2023].

[139] Naciones Unidas, «Infraestructura,» [En línea]. Available: https://www.un.org/sustainabledevelopment/es/infrastructure/. [Último acceso: Marzo 2023].

[140] ENISA, «ENISA Threat Landscape 2022,» 3 Noviembre 2022. [En línea]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022. [Último acceso: Marzo 2023].

[141] FBI, «Internet Crime Report 2022,» [En línea]. Available: https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf. [Último acceso: Abril 2023].

[142] Bitdefender, «Bitdefender Threat Debrief | April 2023,» Abril 2023. [En línea]. Available: https://www.bitdefender.com/blog/businessinsights/bitdefender-threat-debrief-april-2023/. [Último acceso: Abril 2023].

[143] Trend Micro, «LOCKBIT, BLACKCAT, AND ROYAL DOMINATE THE RANSOMWARE SCENE,» 21 Febrero 2023. [En línea]. Available: https://documents.trendmicro.com/assets/rpt/ransomware-in-q4-2022.pdf. [Último acceso: Abril 2023].

[144] ESET, «Threat Report T3 2022,» Abril 2023. [En línea]. Available: https://web-assets.esetstatic.com/dsg/ebooks/eset-threat-report-t3-2022.pdf. [Último acceso: Abril 2023].

[145] Symantec, «LockBit: Ransomware puts servers in the crosshairs,» 20 Julio 2022. [En línea]. Available: https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/lockbit-targets-servers. [Último acceso: Abril 2023].

[146] Bitdefender, «How to Protect Against "WannaCry" Ransomware,» 15 Mayo 2017. [En línea]. Available: https://www.bitdefender.com/blog/hotforsecurity/how-to-protect-against-wannacry-ransomware/.

[147] Fortinet, «What is WannaCry Ransomware Attack?,» [En línea]. Available: https://www.fortinet.com/resources/cyberglossary/wannacry-ransomware-attack. [Último acceso: Abril 2023].

[148] CSIRT, «Inicio Equipos de Ciberseguridad y Gestión de Incidentes españoles,» [En línea]. Available: https://www.csirt.es/. [Último acceso:

Abril 2023].

[149] «Best ransomware protection of 2023,» 24 6 2022. [En línea]. Available: Best ransomware protection of 2023. [Último acceso: 5 2023].

8. Anexos

8.1. Anexo I Planificación del Trabajo

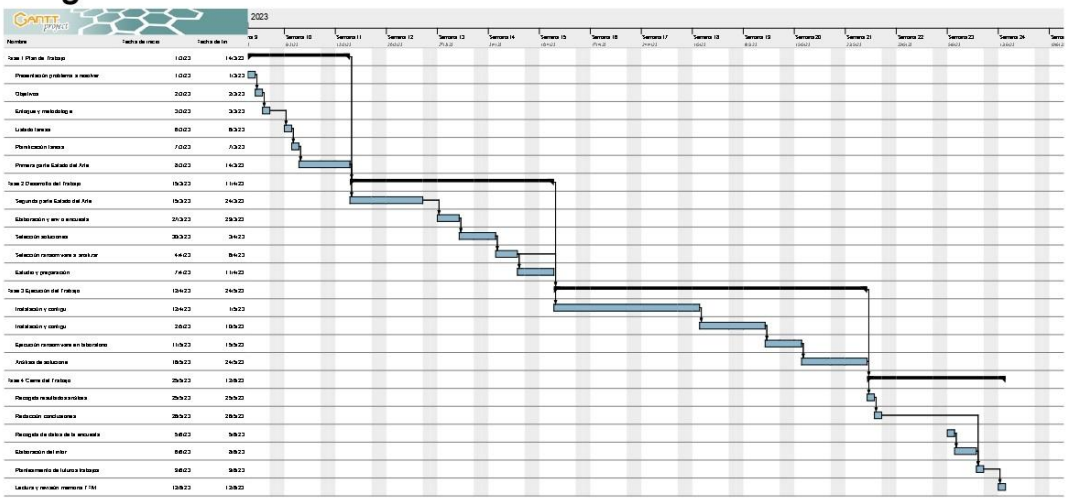
TFM

Tarea

Nombre	Fecha de inicio	Fecha de fin
Fase 1 Plan de Trabajo	1/3/23	14/3/23
Presentación problema a resolver	1/3/23	1/3/23
Objetivos	2/3/23	2/3/23
Enfoque y metodología	3/3/23	3/3/23
Listado tareas	6/3/23	6/3/23
Planificación tareas	7/3/23	7/3/23
Primera parte Estado del Arte	8/3/23	14/3/23
Fase 2 Desarrollo del Trabajo	15/3/23	11/4/23
Segunda parte Estado del Arte	15/3/23	24/3/23
Elaboración y envío encuesta	27/3/23	29/3/23
Selección soluciones anti-ransomware	30/3/23	3/4/23
Selección ransomware a analizar	4/4/23	6/4/23
Estudio y preparación laboratorio seguridad informática	7/4/23	11/4/23
Fase 3 Ejecución del Trabajo	12/4/23	24/5/23
Instalación y configuración laboratorio seguridad	12/4/23	1/5/23
Instalación y configuración soluciones comerciales anti-ransomware	2/5/23	10/5/23
Ejecución ransomware en laboratorio	11/5/23	15/5/23
Análisis de soluciones comerciales anti-ransomware	16/5/23	24/5/23
Fase 4 Cierre del Trabajo	25/5/23	12/6/23
Recogida de datos de la encuesta	5/6/23	5/6/23
Elaboración del informe resumen de los resultados	6/6/23	8/6/23
Recogida resultados análisis	25/5/23	25/5/23
Redacción conclusiones	26/5/23	26/5/23
Planteamiento de futuros trabajos	9/6/23	9/6/23
Lectura y revisión memoria TFM	12/6/23	12/6/23

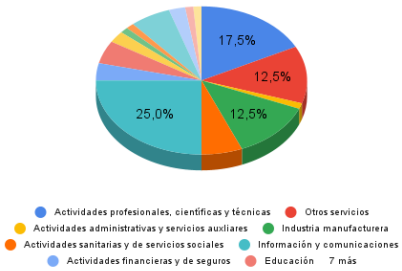
TFM

Diagrama de Gantt

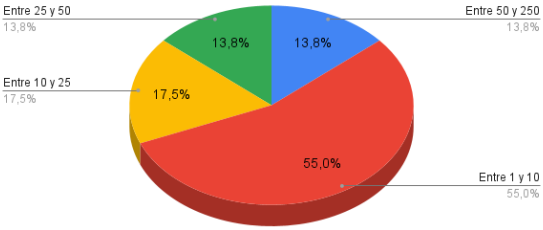


8.2. Anexo II Encuesta pymes y ransomware

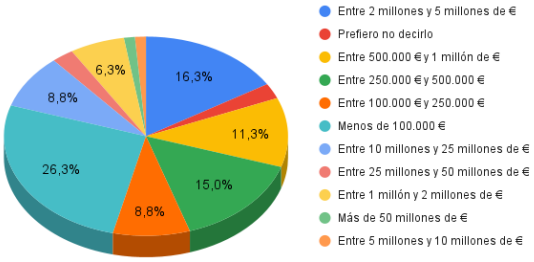
1. Sector de tu empresa (según CNAE)



2. Número de empleados

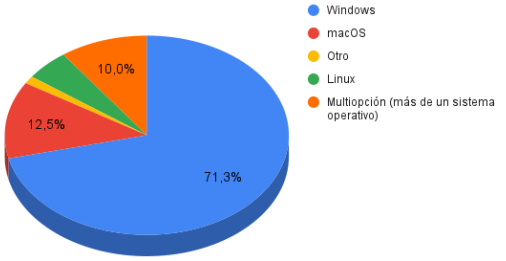


3. Facturación anual (en Euros)

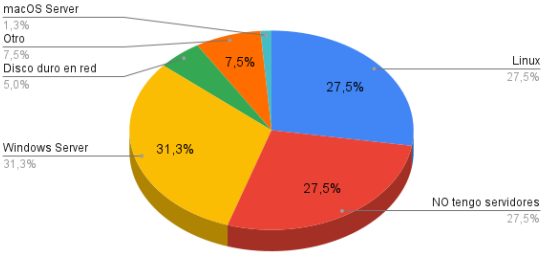


4. Qué entorno informático tienes para trabajar ?

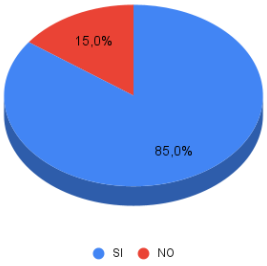
5. Qué sistema operativo usan tus ordenadores ?



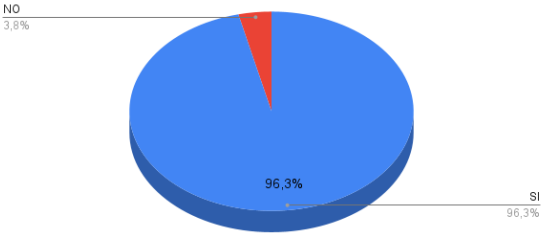
6. Qué sistema operativo usan mayormente tus servidores ?



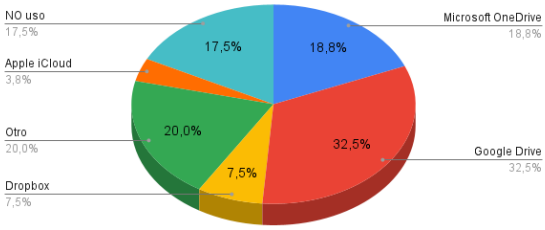
7. Tienes una red local (LAN) ?



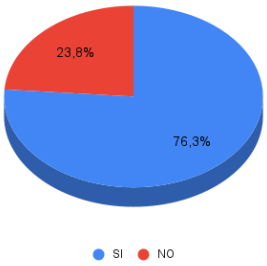
8. Tienes una red wifi ?



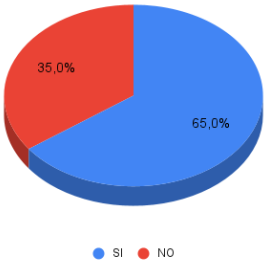
9. Usas almacenamiento en el cloud ? Cuál ?



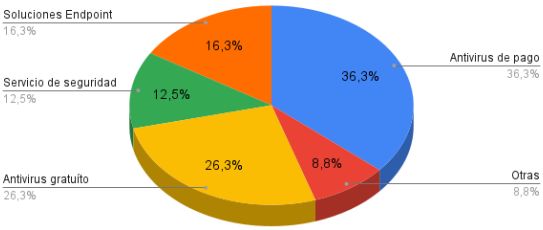
10. Haces teletrabajo ?



11. Tienes acceso remoto seguro por VPN ?

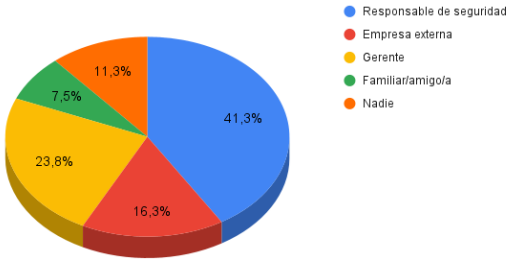


12. Qué solución de seguridad tienes ?

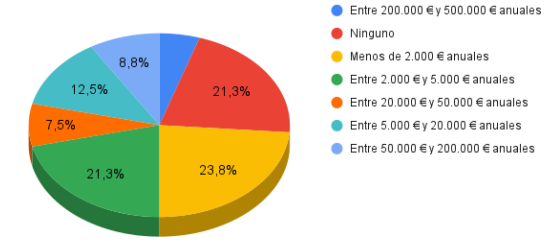


13. Tienes firewall ?

14. Quién se ocupa de la seguridad informática ?



15. Qué presupuesto (en Euros) anual tienes para informática y/o seguridad informática ?



16. Conoces qué es el ransomware ? Lo podrías explicar con tus palabras ?

69 respuestas

Creo que es una especie de troyano o virus que roba los datos internos.

Malware criptografico que cifra tus datos al infectar, bloquenadoleos, y exige pago de dinero o criptomonedas para obtener la clave de descifrado

software para tomar el control total o parcial de un sistema

Malware que bloquea los equipos

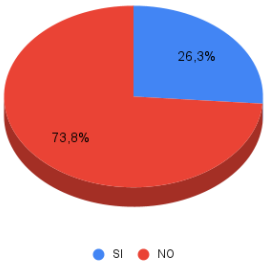
Bloqueo del acceso a los propios datos por programas maliciosos

Que te roban datos a través de la red

Bloque mediante encriptación de tus propios datos

Programa que una vez ejecutado "secuestra" los datos de los equipos afectados y que habitualmente piden

17. Has sufrido algún ataque de ransomware ?



18. En caso afirmativo, cuáles fueron las consecuencias del ataque de ransomware ?

12 respuestas

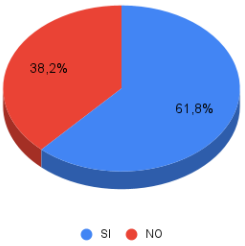
- Perdida de tiempo hasta restaurar.
- Denial of service
- Pérdida de datos
- Ninguna se contuvo a tiempo.
- Lo solucionamos. Pero fue hace años en otra empresa mas grande.
- Ninguna. Eliminación de la máquina atacada, que estaba aislada del resto y no tenía datos sensibles. Restauración de backup y a correr.
- N/A
- Servicios caídos durante unos días hasta su recuperación
- Para algún pc mal, en servidores no prosperó

19. En caso afirmativo, cómo resolviste la situación ?

26 respuestas

- La empresa proveedora del servidor nos lo solucionó
- Pagando y cambiando toda la estrategia de IT
- cliente. Auditoría de seguridad, destinar presupuesto y poner la ciberseguridad como tema prioritario
- n/a
- Llamaron al informático
- Reiniciando backups
- Restaurando desde red limpia

20. Conoces a alguien que haya tenido un ataque de ransomware ?

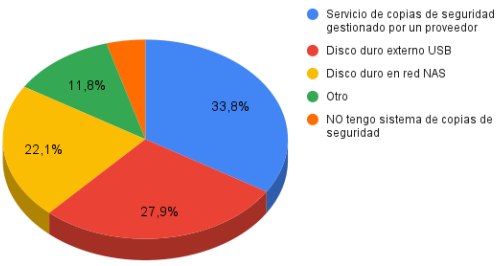


21. En caso afirmativo, cómo resolvieron la situación ?

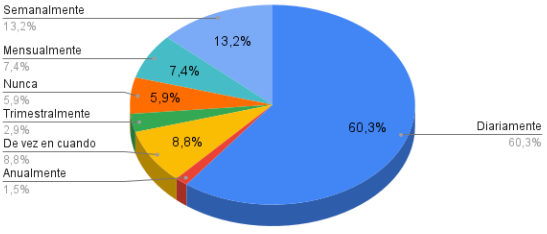
30 respuestas

- Pagando
- recuperando copias de seguridad
- ninguna, no hubo pero me obliga a contestar
- No lo sé, le pasó a un cliente y no me dijeron qué método utilizaron para resolver el problema.
- La mayoría con difícil solucion al no tener copias de seguridad.
- Tirando de copias de seguridad
- Cambio políticas acceso a Internet e instalación de endpointd
- Backup
- No

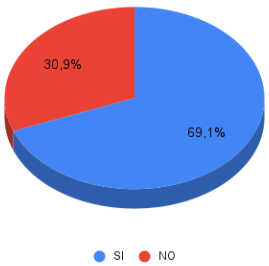
22. Tienes algún sistema de copias de seguridad ? Cuál ?



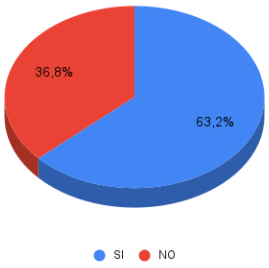
23. Con qué frecuencia haces las copias de seguridad ?



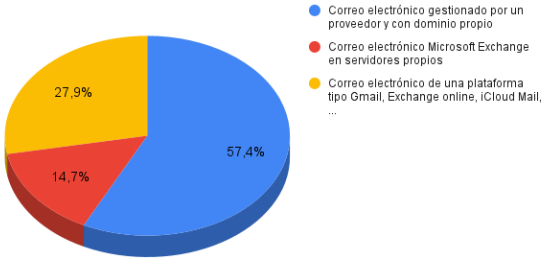
24. Haces una segunda copia de seguridad ?



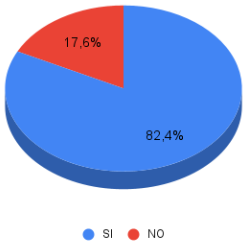
25. La segunda copia de seguridad está fuera del edificio ?



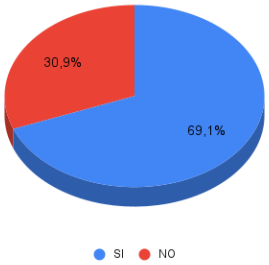
26. Qué tipo de servicio de correo electrónico utilizas ?



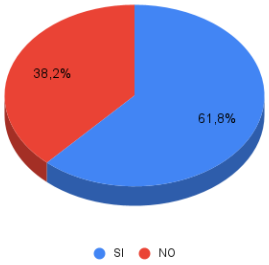
27. Haces una gestión de usuarios, permisos de carpetas y recursos de red ?



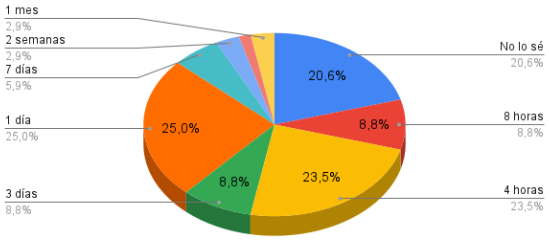
28. Tienes una autentificación de doble factor ?



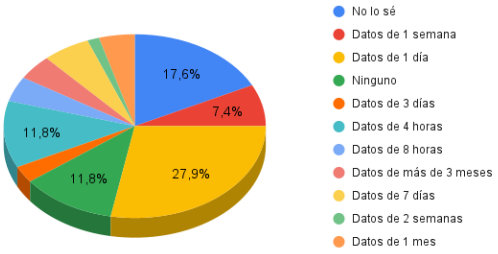
29. Tienes definida una política de renovación de contraseñas ?



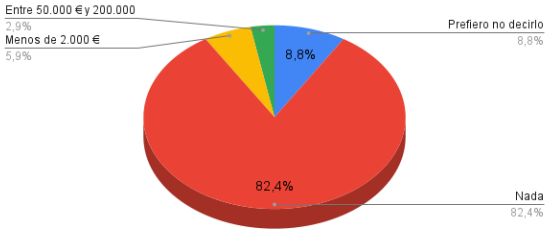
30. Cuántas horas/días/semanas podrías estar sin tener acceso a los datos ? (Recovery Time Objective)

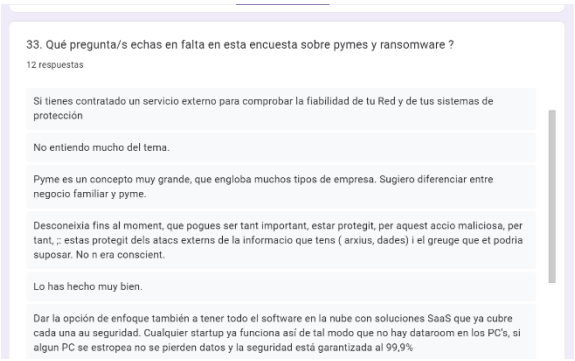


31. Cuántos datos podrías llegar a perder ? (Recovery Point Objective)



32. Cuánto ha gastado (en Euros) tu empresa en la recuperación de datos tras un ataque de ransomware ?




33. Qué pregunta/s echas en falta en esta encuesta sobre pymes y ransomware ?

12 respuestas

Si tienes contratado un servicio externo para comprobar la fiabilidad de tu Red y de tus sistemas de protección

No entiendo mucho del tema.

Pyme es un concepto muy grande, que engloba muchos tipos de empresa. Sugiero diferenciar entre negocio familiar y pyme.

Desconeixia fins al moment, que pogues ser tant important, estar protegit, per aquest accio maliciosa, per tant, ;: estas protegit dels atacs externs de la informacio que tens (arxius, dades) i el greuge que et podria suposar. No n era conscient.

Lo has hecho muy bien.

Dar la opción de enfoque también a tener todo el software en la nube con soluciones SaaS que ya cubre cada una au seguridad. Cualquier startup ya funciona así de tal modo que no hay dataroom en los PC's, si algun PC se estropea no se pierden datos y la seguridad está garantizada al 99,9%