UNIVERSITAT POLITÈCNICA DE VALÈNCIA

Escuela Técnica Superior de Ingeniería Informática

Diseño de un Framework de ciberseguridad empresarial contra el Ransomware mediante controles de prevención, detección y respuesta.

Trabajo Fin de Grado

Grado en Ingeniería Informática

AUTOR/A: Espinar Cuenca, Maria Belen

Tutor/a: Ruiz García, Juan Carlos

Cotutor/a externo: MILLET COLOMAR, ELOY

CURSO ACADÉMICO: 2021/2022

Resumen

La propuesta a presentar es la descripción de un Framework de defensa a nivel empresarial, para que las organizaciones puedan establecer una estrategia contra la amenaza del Ransomware, uno de los mayores problemas de la ciberseguridad en la actualidad. Se planteará un catálogo de controles de ciberseguridad destinados a actuar en las diferentes fases de la defensa frente a Ransomware, que son la prevención, detección y respuesta. La idea se dirige a empresas de tamaño medio/grande tanto del ámbito público como privado.

Palabras clave: Ransomware, defensa, Framework, empresarial, ciberseguridad.

Abstract

Enterprises require defensive frameworks against ransomware. The goal is to define protection strategies based on a catalog of cybersecurity controls. These controls will be established for managing the various defensive stages that can be deployed to fight against ransomware, which are prevention, detection, and reaction stages. This work can be of interest for medium and big enterprises.

Keywords : Ransomware, defense, Framework, Enterprises, cybersecurity.

Resum

La proposta a presentar és la descripció d'un *Framework* de defensa a nivell empresarial, perquè les organitzacions puguen establir una estratègia contra l'amenaça del *Ransomware*, un dels majors problemes de la ciberseguretat en l'actualitat. Es plantejarà un catàleg de controls de ciberseguretat destinats a actuar en les diferents fases de la defensa enfront de *Ransomware*, que són la prevenció, detecció i resposta. La idea es dirigeix a empreses de grandària mitjana/gran tant de l'àmbit públic com privat.

Paraules clau: *Ransomware*, defensa, *Framework*, empresarial, ciberseguretat.

Agradecimientos

Antes de comenzar con la lectura del documento, me gustaría darle las gracias a las personas que me han apoyado durante todo el proceso de redacción e investigación que ha conllevado este trabajo.

No sé cómo expresar el inmenso agradecimiento que siento hacía todo el equipo de Seidor que me han ayudado en cada uno de los pasos del proceso, que han aportado sus respuestas y su paciencia a mis interminables preguntas.

Mención especial a Eloy Millet, quien además de mi tutor y primer contacto en la empresa, ha sido un gran consejero para mí, todos estos meses y me ha enseñado a no centrarme en el color de las hojas de los árboles, sino en el bosque que hay alrededor.

A Servando González, quién me ayudó a entender que pedir ayuda de vez en cuando no es señal de debilidad sino de aprender que en un equipo no debemos resolver todo solos. A Enrique Izquierdo por empujarme a saltar solo cuando sabía que estaba lista, a Francisco Cuesta por ser una fuente de sabiduría y refranes populares y Juan Hidalgo quien me dio confianza para ser una más del equipo cuando aún no sabía dónde encajaba.

Quería también nombrar a Juan Carlos Ruiz, tutor en la UPV, que ha aguantado mis tribulaciones durante todos estos meses, sin una mala palabra o un gesto contrario y me ha apoyado en la idea de hacer un TFG algo especial.

Por último, pero no menos importante, a los compañeros de la carrera, amigos y la familia, ellos ya saben quién son y lo que han hecho.

A todos, gracias.

Tabla de contenidos

Tabla de Ilustraciones

Índice de Tablas

1. Introducción

1.1. Contexto

En la mayor parte de los casos, plantear actualmente un día en nuestras vidas sin utilizar, directa o indirectamente, un dispositivo electrónico es tan inverosímil como hubiera sido hace cientos de años salir a la calle sin ropa. Esto demuestra hasta qué punto las nuevas tecnologías son protagonistas en el día a día de muchos seres humanos. Todos estos sofisticados dispositivos de los que disponemos en la actualidad han sido creados para mejorar la vida de las personas y proporcionarles acceso a cosas que hace cincuenta años no eran más que ideas en la mente de novelistas de ciencia ficción. Poder mantener una conversación o una conexión digital en tiempo real y de manera inalámbrica con una persona o sistema ubicado en la otra parte del mundo es un avance que ha logrado que las personas podamos estar conectadas en todo momento y lugar, haciendo que la información pueda fluir de una manera más rápida de una punta del planeta a otro.

No sólo están presentes las nuevas tecnologías en la vida privada de cada persona, el mundo empresarial también se ha visto revolucionado con este boom tecnológico. Las empresas cada día son más dependientes de los avances tecnológicos, utilizando internet como una de las materias primas más importantes para la continuidad del negocio. Es raro encontrar en la actualidad una empresa (por pequeña que sea) que no posea una página web o algún tipo de huella digital (un correo electrónico de contacto, su teléfono publicado en Google, etc.). Esta hiperconexión es muy beneficiosa para hacer florecer los negocios, y nos ha ayudado en estos últimos años a avanzar en muchísimos campos fundamentales como la sanidad, la ciencia, el transporte o la generación de energía, por citar algunos.

Sin embargo, Internet puede ser un arma de doble filo en lo referente a la seguridad de los servicios digitales que se ofrecen y a la confidencialidad de los datos que éstos gestionan y almacenan. En efecto, la interconexión global que se necesita para producir los servicios informáticos que dan soporte a los nuevos modelos de negocio emergentes expone a las empresas a convertirse en objetivos de delincuentes que, desde la comodidad de sus hogares, pueden hacer un uso malintencionado de los medios digitales a su alcance para perpetrar sus fechorías. De hecho, el número y la gravedad de los ataques cibernéticos llevados a cabo en la última década por estos

ciberdelincuentes han demostrado su potencial para poder llegar a poner en jaque todo nuestro sistema de bienestar, y en ese sentido se está legislando y trabajando con el fin de preservar la disponibilidad de los múltiples servicios que sistemas informáticos nos ofrecen así como la integridad y la confidencialidad de los datos que estos manipulan.

Sin embargo, el problema que estamos exponiendo no es un problema que haya brotado de la nada ya que se sabe que, en menor o mayor medida, los cibercriminales llevan con nosotros más de cuarenta años.

1.1.1. El Primer Hacker

Como ya hemos mencionado, con la globalización de las empresas, algunos hackers y delincuentes, persiguiendo objetivos de tipo económico, han decidido que una manera rápida de enriquecerse es atacar a organizaciones y empresas en plena expansión.

Sin embargo, esta situación no es algo que se haya dado sólo en los últimos años. John Thomas Draper fue el primer Hacker informático reconocido [1]. Draper, también llamado Capitán Crunch, recibió este calificativo tras modificar la frecuencia del juguete que se obsequiaba con unos cereales (que podemos observar en la Ilustración 1. Obsequio de los cereales "Cap'n Crunch"). Él descubrió que si modificaba el tono de dicho juguete a 2600 Hz podía entrar en modo operador imitando la frecuencia que utilizaba el operador AT&T (Compañía Americana de comunicaciones) para indicar que la línea telefónica estaba lista para encaminar la llamada. De esta manera era como Draper realizaba el ataque, pirateando la línea telefónica y consiguiendo utilizar la infraestructura de comunicaciones de AT&T gratuitamente.

Ilustración 1. Obsequio de los cereales "Cap'n Crunch" [2]

En 1986, los hermanos Farooq Alvi pusieron en circulación el que es considerado actualmente como uno de los primeros códigos maliciosos que afectaban a los usuarios de ordenadores IBM: el virus ***Brain*** [3]. Los autores, lejos de querer perjudicar completamente a las personas que utilizaban el ordenador incluían en el virus su número de teléfono para que pudieran contactar con ellos para que limpiaran sus ordenadores, ya que su lo que realmente pretendían era localizar a las personas que utilizaban copias falsas de un software desarrollado por ellos.

Estos denominados hackers, fueron los primeros en actuar a favor de una empresa, ya que con su virus protegían los intereses de IBM encontrando a aquellos que se beneficiaban de copias ilegales.

1.1.2. Hacker vs. Ciberdelincuente

Llegados a este punto es interesante realizar una comparativa entre lo que entendemos por Hacker y por ciberdelincuente.

Por un lado, tenemos al denominado Hacker, que es aquella persona que trata de solventar, paliar o informar sobre los problemas de seguridad encontrados en programas, servicios, plataformas o herramientas informáticas que evalúa [4].

Ilustración 2. Tipos de Hackers [5]

Hay diferentes tipos de Hacker [6]

- **Hackers de sombrero Negro (o en inglés *black hats*):** Son criminales que entran en los ordenadores o servidores de particulares o empresas con intenciones maliciosas. Suelen perseguir fines ideológicos o económicos, y siempre buscan un resultado que les vaya a proporcionar un beneficio (reconocimiento o dinero).

- **Hackers de sombrero Blanco (o en inglés *white hats*)**: Esta versión de los Hackers sería la contraría a la anterior, son Hackers que utilizan sus conocimientos para encontrar brechas de seguridad y ayudar de este modo a que las organizaciones mejoren sus defensas, siempre con el permiso y conocimiento de las mismas.
- **Hackers de sombrero Gris (o en inglés *grey hats*)**: Es el equilibrio entre los dos anteriores. Son Hackers que, como en el caso de los de sombrero blanco, busca vulnerabilidades en los sistemas, pero en este caso sin el permiso o conocimiento de la empresa. Cuando encuentran estas vulnerabilidades suelen informar a las empresas incluyendo en ocasiones un presupuesto con el coste relativo al arreglo del problema. Aunque en países como EEUU esto puede hacerse, y en muchas ocasiones permite el descubrimiento de jóvenes talentos que son contratados por las empresas, cabe señalar que las prácticas de los hackers de sombrero gris son ilegales en Europa, y si las vulnerabilidades descubiertas se hacen pública pueden comportar procesos penales a sus descubridores.

Como podemos ver en las definiciones, los hackers no siempre tienen un objetivo malicioso en mente cuando buscan y descubren vulnerabilidades en un sistema, de hecho, hay Hackers “buenos” que forman parte de las plantillas de las empresas.

Por otro lado, el ciberdelincuente es una persona que trata de sacar un beneficio de los fallos existentes en las políticas o mecanismos de seguridad existentes en un sistema utilizando distintas técnicas de ataque como, por ejemplo, el Phishing, la ingeniería social o el malware [4]. En consecuencia, estos individuos pueden ser considerados como personas cuyas actividades se desarrollan fuera de la legalidad, de ahí el término ciberdelincuente.

Definidos, y distinguidos, los términos con los que vamos a designar a los grandes protagonistas del mundo digital que nos interesan en este trabajo, abordemos ahora su relevancia para el proyecto que nos concierne.

1.1.3. 2020, Pandemia mundial - Teletrabajo

En anteriores apartados, hemos hablado, de que los últimos años han resultado en un impulso para la ciberdelincuencia. En concreto, los últimos 3 años han sido decisivos para cimentar el escenario con el que nos encontramos. La situación a la que hacemos referencia está relacionada con la pandemia provocada por el COVID-19, y más

concretamente, con el aumento del Teletrabajo en todo el mundo que ha sido promovido por el confinamiento impuesto a la población. Las empresas que podían utilizar este recurso se vieron forzadas a llevar las oficinas de las organizaciones a las casas particulares, de una manera precipitada y en muchas ocasiones sin la seguridad que el edificio y los recursos de la empresa les proporcionaban.

Según un artículo que público BBVA en su página web, el teletrabajo se multiplicó por siete en 2020 [7], abriendo la puerta a establecer esta modalidad de trabajo como la predominante para el personal administrativo y técnico. Lejos de desaparecer cuando se levantaron las restricciones impuestas durante la pandemia, las organizaciones adoptaron este modelo como una manera de reducir costes y recuperar las pérdidas que el primer trimestre del año 2020 provocó. Esta medida de reducción de costes, que inicialmente ayudó a muchas empresas a mantenerse a flote, conllevó una diversificación tan grande de los sistemas informáticos desde los que los empleados trabajaban, que la seguridad de los equipos, y por tanto de los activos de la empresa que gestionan y almacenan, se hizo muy complejo de garantizar. Por supuesto, esta situación benefició a los amigos de lo ajeno que vieron en la falta de, o en el incorrecto, de mantenimiento de algunos equipos, brechas potenciales de seguridad que podrían explotarse con fines poco lícitos. En resumen, que permitir el trabajo remoto de los empleados, y por tanto, el acceso a activos de la organización desde casa, se reveló como una vulnerabilidad en sí misma para la seguridad de la empresa. Por tanto, si los dispositivos no están lo suficientemente protegidos existe un riesgo real de que éstos se conviertan en la puerta de entrada de malware a la red corporativa de la organización.

Este problema no es del todo desconocido, ya que con el desarrollo de los dispositivos móviles, cada vez son más los empleados que utilizan sus terminales personales (teléfonos inteligentes, tabletas o portátiles) para trabajar por la noche o los fines de semana. Esto se conoce como el problema del **BYOD**, del inglés, *Bring Your Own Device*, y plantea multitud de retos a las empresas para impedir que sus activos no sólo estén protegidos, sino que en caso de ser extraviados o robados, resulten inútiles en manos de terceros malintencionados [8]. Empresas conscientes de estos riesgos introducen en el material de bienvenida a nuevos empleados políticas sobre las buenas prácticas en caso del BYOD.

La guía de Ciberseguridad en el teletrabajo realizada por el INCIBE (Instituto Nacional de Ciberseguridad de España) en 2020 nos indica que "*La principal amenaza contra la mayoría de los dispositivos cliente de teletrabajo es el malware*." Por ello es

fundamental que los equipos de trabajo a distancia se sometan al mismo tipo de controles de seguridad que aquellos que se encuentran físicamente en el edificio de la organización, considerándolos así una parte de los activos a tener en cuenta cuando se realiza un estudio de la seguridad [9].

1.1.4. Estadísticas del INCIBE

El INCIBE recoge cada año en el Balance de ciberseguridad que hace las cifras sobre las alertas en el campo de los servicios públicos ofrecidos para proteger tanto a ciudadanos como a negocios. Si observamos los datos que se reportaron en 2019 plasmados en la Ilustración 3: Extracto del Balance de Ciberseguridad del INCIBE 2019, sobre los incidentes que fueron manejados por la institución en 2019.

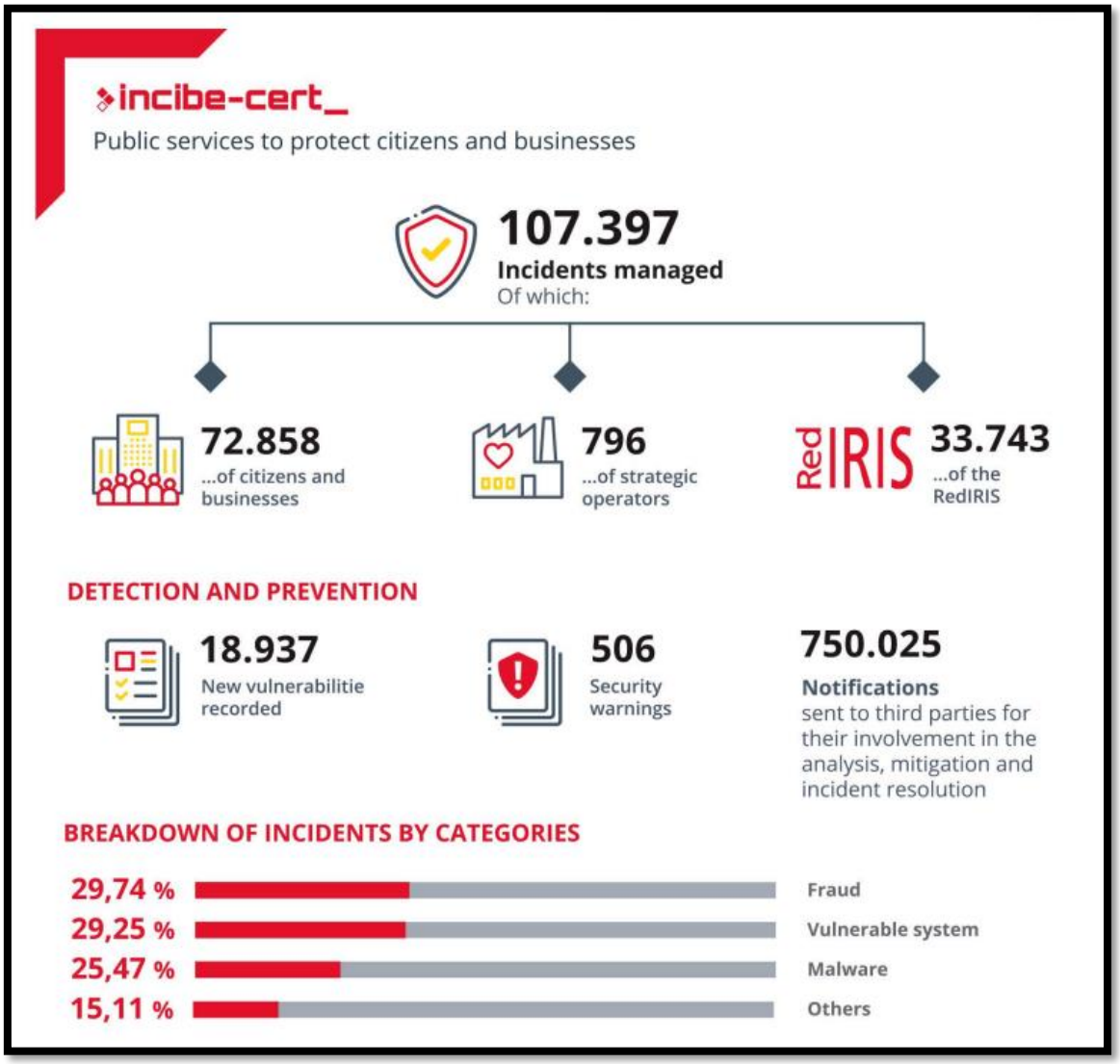


Ilustración 3: Extracto del Balance de Ciberseguridad del INCIBE 2019 [10]

El INCIBE gestionó un total de 107.397 incidentes relacionados con la ciberseguridad de los cuales el porcentaje más importante era de tipo Fraude [10] siendo el malware el tercer tipo de incidente de seguridad con mayor impacto en los sistemas de entre todos los reportados.

Como hemos ido adelantando en esta introducción, la ciberdelincuencia ha aumentado considerablemente los últimos años, sin embargo, hasta 2019 el tipo más común de ataque era el fraude.

En 2020 la tendencia cambió y el Malware subió desde la tercera posición que ocupó en el año 2019 hasta la primera posición, acumulando un total del 35.22% del total de ataques registrados por el INCIBE [11]. Estas cifras quedan reflejadas en la Ilustración 4: Extracto del Balance de Ciberseguridad del INCIBE 2020 . Reseñar también, que en general la cantidad de ataques se incrementó en más de 30000.

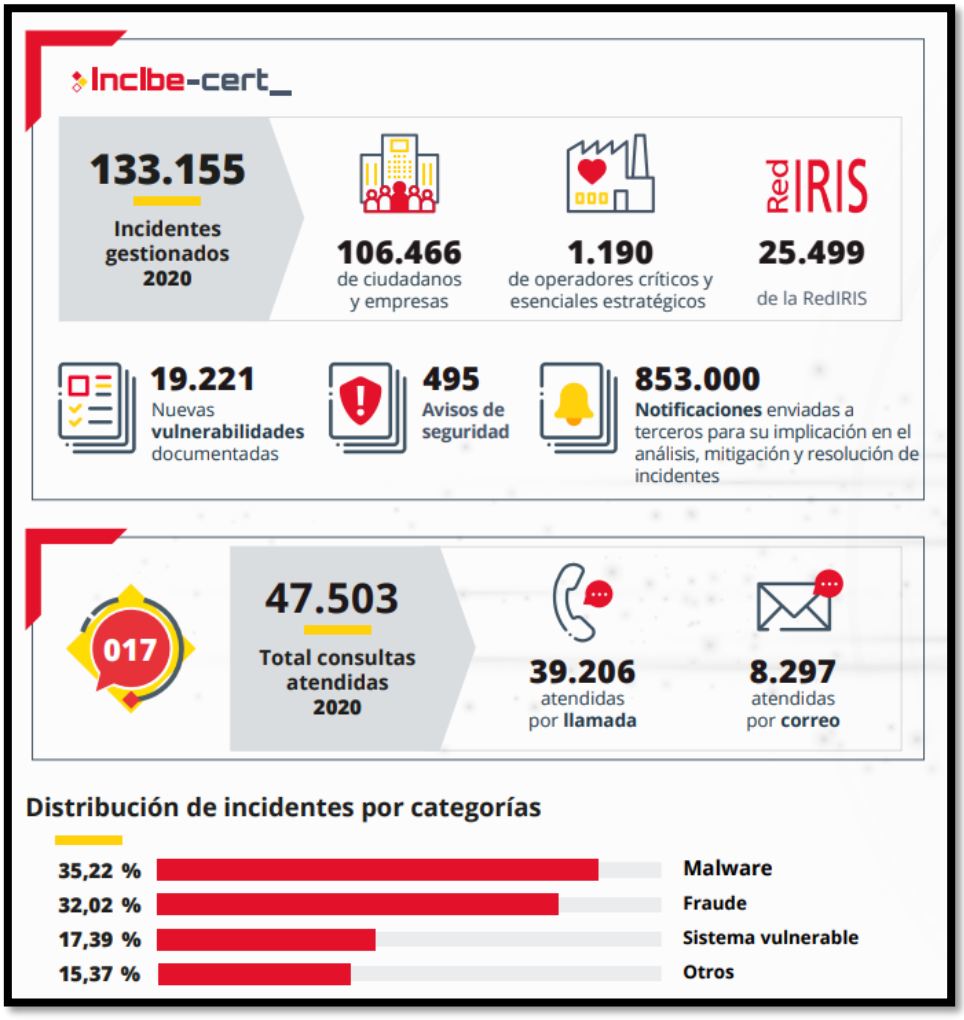


Ilustración 4: Extracto del Balance de Ciberseguridad del INCIBE 2020 [11]

El malware se convierte en la primera causa de preocupación para 2020. En 2021, el siguiente balance del INCIBE que podemos ver en la Ilustración 5: Balance de seguridad del INCIBE 2021 (el último que ha realizado el instituto ya que 2022 no ha finalizado) nos muestra que la tendencia de que el Malware sea la primera categoría de ataques de aquellos que registraron continúa presentándonos este problema como no un despunte que ocurrió en 2020 a causa de todas las modificaciones en las empresas provocadas por la pandemia, sino que es una tendencia que actualmente se mantiene.

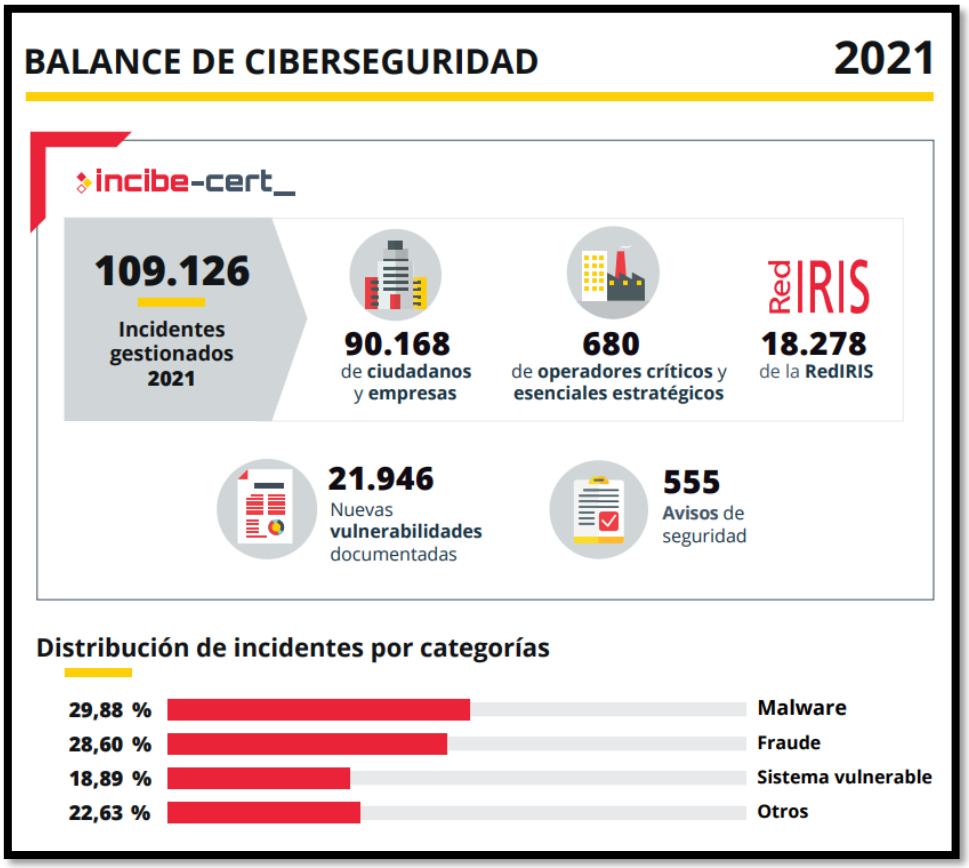


Ilustración 5: Balance de seguridad del INCIBE 2021 [12]

Pero ¿qué es el malware? Partiendo de la definición del mismo que se da en la referencia [15], la palabra "Malware" (Programa maligno) procede del inglés y es el resultado de abreviar en un único término la expresión anglosajona "*Malicious Software*". Por tanto, el término hace referencia a todo tipo de software o código que se utiliza para realizar acciones hostiles o intrusivas en el dispositivo o sistema de la persona u organización que lo recibe. Aunque existen muchas definiciones alternativas, y le son atribuidas muchas finalidades distintas, básicamente el malware suele ser utilizado para:

- Encriptar o eliminar datos confidenciales.

- Modificar o desviar las funciones básicas del ordenador.
- Espiar la actividad informática de los usuarios.
- Robar información confidencial o de interés.

Obviamente, todas estas acciones se llevan a cabo sin el consentimiento de la entidad (persona física u organización) que recibe el ataque. De hecho, la manera en la que el propio malware se propaga e infecta a otro sistema ha llevado a muchos a definir multitud de tipos distintos de malware, de entre los cuales los más comunes son:

- **Troyano**: Este tipo de malware se disfraza de programa "seguro" para que el usuario lo instale voluntariamente en su dispositivo, posteriormente, este Troyano introduce otro tipo de malware en el sistema. Viene en forma de cualquier tipo de documento con el que estemos íntimamente relacionados como un Word o un Excel. El problema de este tipo de malware es que no reconoceremos que es dañino hasta que no realice la acción por la cual fue creado. Muchas veces este tipo de malware también será portador de otro.
- **Virus**: Virus informático que, como su homónimo sanitario, busca infectar la máxima cantidad de dispositivos o sistemas a su alcance. Es un fragmento de código o software que tiene como principal característica su capacidad para replicarse y propagarse rápidamente de un sistema/dispositivo a otro.
- **Spyware**: Malware espía que suele ser introducido en los dispositivos a través de un Troyano y queda oculto en el sistema estudiando, entre otras cosas, las pulsaciones de teclado que realiza el usuario o capturas de pantalla. Su finalidad es conseguir información (como el número de la tarjeta bancaria, etc) del host que infecta.
- **Ransomware**: Es un malware del que hablaremos extensamente en el siguiente apartado por su relevancia en este proyecto. Para su definición, simplemente diremos aquí que es un tipo de malware que busca secuestrar un dispositivos, sistema o subsistema, sus datos.

1.1.5. Ransomware

Es un tipo de Malware cuya abreviatura viene del término en inglés "*Ransom software*" que, aunque rara vez se traduce, podría leerse como malware secuestrador. De hecho, su finalidad es la de secuestrar los datos de un dispositivo cifrándolos con un código desconocido por el usuario. Se dice que los datos "están secuestrados" porque si no se paga un rescate por los mismos los datos se pierden, al no poderse descifrar. Es por testo que el objetivo del Ransomware es siempre el de conseguir un rescate.

Independientemente de la forma en la que el Ransomware entra en nuestros dispositivos, si no detenemos su avance el resultado va a ser el mismo, el malware se ocupará de codificar toda aquella información a la que tiene acceso para después mostrar por pantalla un mensaje para indicarnos que somos víctimas de un ataque cibernético.

En este mensaje nos mostrará el tiempo que tenemos para poder pagar este rescate y el monedero virtual o lugar donde desea que realicemos el pago.

Ilustración 6: Ejemplos de pantalla mostrada por Ransomware [13]

Normalmente, después de infectar el dispositivo, como acabamos de explicar, este software malicioso suele mostrar una pantalla como las que muestra la Ilustración 6: Ejemplos de pantalla mostrada por Ransomware. Como se puede apreciar, las pantallas informan de las características del secuestro.

En muchas ocasiones se hace entrega de un código que desbloquea una pequeña parte de toda esta información codificada para mostrar la capacidad del ciberdelincuente de descifrar la información cifrada si el pago del rescate se hace efectivo. El pago se suele reclamar en criptomonedas ya que es la manera más compleja para poder rastrear el dinero hasta el atacante.

En 2021, según un informe que realizó SOPHOS [14] un 37% de las empresas que encuestó (5400 en 30 países diferentes), fue víctima de un Ransomware ese mismo año. El costo promedio aproximado para que las organizaciones rectifiquen los impactos del Ransomware (considerando el tiempo de inactividad, el tiempo de las personas, el costo del dispositivo, el costo de la red, la oportunidad perdida, el rescate pagado) fue

de 1.85 millones de dólares estadounidenses, más del doble de la cifra recogida en 2020 (0,76 millones de dólares).

Como podemos imaginar, después de toda la información que hemos expuesto la gravedad de sufrir un ataque de Ransomware puede llevar a muchas empresas a perder su capacidad de realizar su misión. Por ello la necesidad de crear un Framework de defensa contra el Ransomware para las empresas es primordial, ya que no solo los grandes empresarios están afectados por el problema, sino que cada uno de nosotros podemos ser víctima de un ataque de Ransomware. Las empresas deben de ser capaces de evaluar con el Framework la situación en la que se encuentran actualmente con referencia a su capacidad de defensa y saber qué puntos débiles poseen en sus sistemas de seguridad.

Debemos plantear la problemática teniendo en cuenta las deficiencias de la organización y el desconocimiento en muchas ocasiones de estas debilidades.

1.2. Motivación

Como acabamos de indicar, la necesidad de crear una guía de evaluación estructurada es fundamental para el continuado funcionamiento de las organizaciones. Limitándonos a las estadísticas que hemos expuesto, observábamos que el aumento de la ciberdelincuencia necesita de una reacción por parte de los empresarios, y de que se establezca una forma de asegurar la continuidad del negocio protegiendo los datos de la empresa. Esto resulta fundamental ya que dichos datos son al final uno de los activos más valiosos que las empresas poseen.

Todas aquellas empresas que desean certificar el nivel de seguridad de sus sistemas deben realizar un análisis de los mismos atendiendo a las directrices de las normas y estándares de seguridad existentes a tal efecto. Sin embargo, a excepción de aquellas empresas que contraten a un experto en seguridad, la interpretación de las normas es extensa, compleja y, en ocasiones, puede llevar al planteamiento de dudas por no existir una escala de evaluación adaptada. En efecto, en la mayor parte de los casos, la evaluación de los controles de seguridad es binaria, es decir, o bien se cumple o bien se falla, no existiendo la posibilidad de cumplir parcialmente (poco o mucho) con los mismos. Al no existir una zona gris, los resultados de las evaluaciones suelen generar muchas dudas en incluso inducir confusión, ya que muchas empresas no se

identifican ni con un extremo, ni con el otro, del cumplimiento del control de seguridad evaluado y, por tanto, no saben qué medidas adoptar para paliar sus carencias.

Por otro lado, y aun teniendo bien determinadas las carencias existentes en materia de protección, hay multitud de soluciones muy técnicas que son implementadas en productos distintos que se han diseñado específicamente para prevenir y combatir ataques, como el malware, en una empresa. Pensemos, por ejemplo, en los antivirus o en las extensiones anti-spam. Estas soluciones son excesivamente técnicas y resuelven problemas idénticos, o muy similares, y es, por tanto, difícil para un administrador promedio decantarse por la adopción de una u otra.

De esta reflexión surge la idea de crear un marco de trabajo con el que las empresas puedan tener una guía a la hora de evaluar su capacidad frente a ataques informáticos en general, y más concretamente, frente al Ransomware. Durante esta memoria nos referiremos a él como un **Framework**, término que hemos desarrollado en el glosario incluido al final de este documento. Este Framework establecerá unos buenos cimientos para el conocimiento de la organización en materia de ciberseguridad con una evaluación completa de controles específicos para ayudar a las empresas a prepararse para estas guerras digitales que no han hecho más que comenzar.

1.3. Impacto esperado

Este Framework abordará cada uno de los puntos del ciclo de vida de un ataque. Cuando hablamos de ciclo de vida, nos referimos a todas aquellas etapas por la que pasará un ataque, desde el momento inicial de estudio por parte del ciberdelincuente a la empresa hasta el final, cuando actúa secuestrando los datos escogidos. Así diferenciaremos las siguientes etapas: Reconocimiento, Acopio de Armas, Despliegue, Explotación, Instalación, Comando y control y Actuación sobre el objetivo. La descripción detallada de cada una de estas etapas se abordará en el capítulo 3 de esta memoria.

Este Framework se centrará en especificar paso a paso cuales son los aspectos que se han de revisar y así fortificar para prevenir una pérdida masiva de datos y la inutilización de los servicios de una organización (objetivo de cualquier ataque de Ransomware). El usuario podrá visualizar de manera clara y puntuable en qué estado se encuentra su organización y cuáles son los aspectos en los que más hincapié ha de hacer para protegerse frente a futuros ataques.

Este Framework permitirá a las empresas crear una instantánea de su seguridad frente al Ransomware, y parte, cuando no todas, las conclusiones del análisis serán extrapolables a otros ataques de malware.

1.4. Objetivos

A continuación, detallaremos los objetivos de nuestro Framework, diferenciando aquellos de carácter general y que engloban la totalidad del proyecto, de los que son más específicos, y se relacionan con las pequeñas metas que trataremos de conseguir con la implantación de este Framework.

1.4.1. Objetivo General

El objetivo principal de este proyecto es el siguiente:

- Generar una herramienta para evaluar la situación actual de una empresa con respecto a la defensa contra el Ransomware.

Este objetivo se refiere a la capacidad de dotar a una empresa de una herramienta (el Framework) que le permita evaluar el nivel de madurez aproximado en la que se encuentra su organización para defenderse ante un ataque de Ransomware.

1.4.2. Objetivos Específicos

Los objetivos específicos de este proyecto son:

- Proteger la información de los clientes y usuarios de estas empresas.
- Proteger la información corporativa.
- Concienciar a los empleados y usuarios de la existencia de amenazas y los medios actuales para combatirlas.
- Impedir el acceso a los ciberdelincuentes a la información.
- Impulsar buenas prácticas en la gestión de recursos de seguridad.

2. Estudio Estratégico

Como hemos hablado anteriormente, la amenaza del Ransomware es real y costó a empresas de todo el mundo más de 1,87 millones de dólares en 2021, lo que nos indica que no es un tema que podamos tratar a la ligera.

Afortunadamente las empresas no están completamente desprotegidas, en la actualidad existen herramientas/normativas/guías que las organizaciones pueden utilizar para informarse, evaluarse y tratar de protegerse contra los ataques de malware. Estas herramientas suponen un pilar fundamental para las organizaciones que quieran controlar de manera autónoma su nivel de ciberseguridad. Sin embargo, la gran cantidad de opciones disponibles en el mercado hace excesivamente laborioso poder encontrar una que se ajuste a todas y cada una de las necesidades que posee una organización en cierto momento. De hecho, con el cambio constante de las tecnologías esta búsqueda debería realizarse constantemente para actualizar las respuestas a las nuevas brechas o necesidades que se creen.

Por ello, en este apartado describiremos una serie de normas y protocolos que nos servirán de ejemplo de la cantidad de herramientas que tenemos al alcance. Todas ellas se encuentran en vigor y se establecieron para abordar diferentes aspectos de la protección contra el Ransomware y diversos ataques de una manera más generalizada.

Todos ellos pertenecen a organismos reconocidos, siendo utilizados como base para la definición de planes de evaluación, protección y contingencia en aquellas empresas que se preocupan en intentar combatir el malware. Haremos una breve descripción de ellos y nos centraremos en exponer las pequeñas deficiencias que encontramos al analizarlos.

2.1. Estándar NIST: Gestión de riesgo de ransomware: un perfil de marco de ciberseguridad

El NIST (National Institute of Standards and Technology) en el documento “Gestión de riesgo de Ransomware: un perfil de marco de ciberseguridad” [16] establece un perfil de Ransomware dirigido a “*Cualquier organización con recursos de ciberseguridad que pueda estar sujeta a ataques de Ransomware, independientemente del sector o tamaño.*”. En principio esta situación sería una gran ventaja para este marco

normativo, sin embargo, se recomienda tener control y conocimiento del Marco de Ciberseguridad del NIST, un documento muy extenso y bastante técnico.

Si nos centramos en el documento del NIST podemos ver que establece una serie de etapas en el procesamiento de un Ransomware (Identificar, proteger, detectar, responder y recuperar) y proporciona recomendaciones (herramientas y políticas) para hacer frente en cada una a este tipo de amenazas. Con referencia a nuestro Framework nos interesa analizar las tres primeras etapas que define el estándar, es decir, las de identificación, protección y detección.

Como ya hemos comentado, el documento establece una serie de directivas que relacionan diferentes aspectos de cada etapa con recomendaciones. Un ejemplo de estas directivas es la que podemos observar en la Ilustración 7: Extracto del documento NIST 8374. Una directiva contemplada en la función de identificar nos habla de la categoría de gestión del riesgo, indicando las subcategorías o referencias (un detalle que considerar es como considera una de las referencias la ISO 27001:2013, cuando no es la versión más reciente) y por último la aplicación al Ransomware, donde indica una recomendación basada en esta directiva concreta.

Categoría	Subcategoría y referencias informativas seleccionadas	Aplicación de ransomware
Identificar		
Estrategia de gestión de riesgo (ID.RM): se establecen las prioridades, restricciones, tolerancias a riesgo y suposiciones y se utilizan para apoyar las decisiones de riesgos operativos.	**ID.RM-1:** las partes interesadas organizacionales establecen, gestionan y acuerdan los procesos de gestión de riesgo **ISO/IEC 27001:2013** Cláusula 6.1.3, Cláusula 8.3, Cláusula 9.3 **NIST SP 800-53 Rev. 5** PM-4, PM-9	Establecer y hacer cumplir las políticas, los roles y las responsabilidades organizacionales depende de que las partes interesadas acuerden e implementen procesos de gestión de riesgo efectivos. Los procesos deben tomar en cuenta el riesgo de un evento de *ransomware*. Debe revisarse periódicamente que estas políticas reflejen la naturaleza dinámica del riesgo y la realidad de ajustes necesarios en el tiempo.

Ilustración 7: Extracto del documento NIST 8374 [16]

En consecuencia, el estándar nos proporciona un documento muy útil, aunque sus recomendaciones son genéricas y carece de una fase de evaluación con el objetivo de adecuar dichas recomendaciones a las necesidades concretas de cada empresa.

2.2. Estándar ISO 27001/2

El segundo de los ejemplos que vamos a presentar es la normativa ISO (Organización internacional de Normalización). Esta normativa incluye un conjunto de estándares con reconocimiento internacional que disponen de numeraciones para indicar los marcos de referencia que abordan en cada una de ellas. Concretamente las normas 27001/27002 desean proporcionar una serie de controles y recomendaciones para que las empresas puedan crear y aplicar protocolos de seguridad reglados. Establecen unos baremos para que las organizaciones tengan una referencia y adapten sus sistemas a la normativa vigente para garantizar las mejores prácticas.

Concretamente y para el tema que estamos abordando en este documento, nos centraremos en la norma ISO 27002:2022 [17] que establece en su control 8.7 una serie de guías de cumplimiento para proteger a la organización contra el software malicioso (malware). En ella se establece la importancia de implementar medidas para frenar estos ataques y además se incluye como punto de interés la concienciación adecuada del usuario en este aspecto. Hace un repaso de los puntos más importantes que la organización ha de tener presente para el desarrollo de una buena defensa contra cualquier tipo de malware. El propósito de este punto en el estándar ISO es garantizar la integridad de la información y otros activos que puedan verse perjudicados en caso de un ataque por ello hace referencia a todos los puntos fundamentales como:

- Implementación de controles que prevengan o detecten el uso de software no autorizado.
- Implementación de controles para prevenir el uso de sitios web maliciosos.
- Validación periódica del software y el contenido de los sistemas.

Es un planteamiento que recorre todas las facetas más comunes en la prevención de un ataque de malware, sin embargo, hemos de destacar que como ocurre con las normativas especializadas de sectores técnicos el lenguaje que se utiliza para redactarlas está muy basado en el mundo empresarial y tiene tecnicismos que alguien poco relacionado con la ciberseguridad puede no comprender. Se necesita un amplio conocimiento del área para poder asimilar de una sola lectura cada una de las especificaciones que hace a lo largo del texto. Por ello, uno de los principales problemas que presenta el utilizar directamente este estándar ISO 27002:2022 como referencia para cimentar la seguridad de una organización es la falta de comprensión o

interpretación de la normativa a primera vista sin un interlocutor experimentado que haga de intérprete y traductor.

Además, hemos de recordar que el estándar está originalmente escrito en inglés por lo que una traducción en ocasiones demasiado literal de alguna de sus frases puede llevar a cierta confusión.

Como último punto a reseñar, la norma, aunque leída por una persona experta no deja de ser un escrito estandarizado, y por tanto las organizaciones en muchas ocasiones no tienen conciencia real de si cumplen o no los controles que establece si no se plantean las preguntas adecuadas. Esta norma está diseñada para todo tipo de organizaciones, independientemente de su tamaño por lo que es demasiado genérica para ahondar en las características de defensa de cada empresa. Este punto puede ser considerado una ventaja, pero en nuestro caso sería un inconveniente, especialmente para una PyME que carezca de personal especializado, dadas las distintas interpretaciones que podrían derivarse de la genericidad existente de la norma.

Por ejemplo, uno de los controles que plantea la norma consiste en: "*reducir las vulnerabilidades que puede ser explotadas por malware.*". El lector de esta frase puede interpretar que las vulnerabilidades deben ser inexistentes si hasta el momento no se ha recibido un ataque, o incluso asumir que, dado que se realizó un año atrás un análisis de vulnerabilidades, actualmente está cubierta esta parte. Estas respuestas enmascararían quizás una necesidad de replantearse el escaneo de vulnerabilidades. En cambio, si directamente se cuestionara si el escaneo de vulnerabilidades es una tarea recurrente, el usuario tendría una visión mucho más realista de su estructura con respecto a las vulnerabilidades existentes.

2.3. Guía Ransomware INCIBE

El documento "Ransomware: Una guía de aproximación para el empresario" es una guía que fue confeccionada por el INCIBE en 2017 [19]. En ella hace un estudio exhaustivo del Ransomware, abordando cuestiones como qué es el Ransomware, cómo podemos protegernos frente a esta amenaza y qué hacer en caso de infección. La guía repasa los principales puntos de prevención a la hora de protegerse del malware. La característica que la diferencia de los demás informes disponibles es que está muy orientada hacía el empleado como víctima, no la población en general, destacando temas como la ingeniería social.

Sin embargo, la guía data de hace 5 años, con lo que está desactualizada, y no considera aspectos tan importantes como el teletrabajo que, como ya hemos mencionado anteriormente, pueden permitir, si no son gestionados adecuadamente, la infección con Ransomware de las organizaciones.

2.4. Gestión de incidentes de Ransomware CCN-CERT BP/21

El siguiente documento fue escrito por el "CCN-CERT" (Centro Criptológico Nacional – *Computer Emergency Response Team)* Dentro de las guías que posee el CCN-CERT el documento al que haremos referencia en este apartado es el "CCN-CERT BP/21" que contiene una guía de gestión de incidentes de Ransomware [18]. De hecho, nos encontramos frente a un documento muy completo que nos indica que pasos debemos de seguir cuando estamos sufriendo un ataque de Ransomware. La parte técnica es extensa y da una visión amplia de las tecnologías a utilizar para combatir el malware.

Señalar que deja para el último apartado la parte de prevención, que aborda los siguientes cuatro puntos:

- Políticas de seguridad en el dominio.
- Políticas de seguridad a nivel de red.
- Realización de copias de seguridad.
- Aumento del análisis del contenido de las comunicaciones.

Es, por tanto, una guía muy completa que hace mucho hincapié en qué es lo que hay que hacer una vez se ha producido una infección. En el campo de la prevención, sin embargo, notamos que hay una parte fundamental que no nombra, el papel de los empleados en la prevención del Ransomware. Cuando habla de políticas de seguridad en el dominio indica que al usuario se le especifica que utilice contraseñas robustas y que las cambie regularmente, pero más allá de ese punto, el empleado no es nombrado en este apartado del documento obviando uno de los aspectos más importantes: la concienciación en materia de ciberseguridad al empleado. No especifica que se deben realizar formaciones periódicas para que el personal este prevenido de las amenazas actuales y sepa cuales son las buenas prácticas que debe realizar.

2.5. Evaluación en las empresas

Tras realizar este análisis de las normativas y guías que actualmente están disponibles para las empresas a la hora de enfrentarse al problema del Ransomware es

el momento de exponer cual es la manera en que las empresas interactúan y despliegan estas normativas.

Cuando una organización desea certificarse o crear un procedimiento adecuado de seguridad, acuden a estas herramientas y a personal especializado. Para evaluar la situación de las empresas en los aspectos que recogen estas herramientas, las consultoras forman cuestionarios que repasan cada uno de los controles de la normativa que el consultor o la organización consideran oportunos. Estos cuestionarios se proporcionan a las empresas para que los contesten, y a través de estas respuestas los consultores indican cuales son las deficiencias y los puntos que mejorar.

Como hemos visto en los ejemplos que tenemos arriba, hay una amplia gama de guías y estándares que las empresas pueden utilizar. Sin embargo, la muestra dada no es extensa y solo proporciona una pequeña muestra de la gran cantidad de opciones disponibles. Sin embargo, y lejos de resolver el problema, esta gran cantidad de alternativas disponibles genera una situación compleja, pues todos los distribuidores afirman que sus herramientas son excelentes y adecuadas para una completa defensa frente a Malware, cuando en realidad, y a pesar de tener grandes fortalezas, cada alternativa presenta también, como ya hemos comentado, algunas debilidades.

Esta gran cantidad de opciones que se presentan a las empresas son. Por tanto, comúnmente promocionadas como “aquello que la empresa necesita para acabar con el problema del Ransomware” cuando en realidad cada alternativa solo aborda uno, o un conjunto limitado, de los aspectos propios de este tipo de ataque. De ahí surge la necesidad de crear una herramienta o un Framework que unifique las recomendaciones de cada alternativa, pero atendiendo no sólo a las distintas etapas del ciclo de vida de un ciberataque de tipo Ransomware, sino también a las particularidades de cada empresa, en especial, cuando ésta es una PyME.

2.6. Resumen de alternativas

En la siguiente tabla vamos a hacer una breve comparación de las herramientas que hemos explicado, incluyendo el nombre, sus ventajas y debilidades, y en caso de que sea necesario alguna observación.

Tabla 1: Revisión de alternativas actuales en el mercado.

Nombre	Ventajas	Debilidades	Observaciones
Estándar NIST	Establece un perfil del Ransomware para especificar las características el ataque.	Es un estándar extenso y dada su complejidad, algunos de sus puntos pueden llevar a confusión lo que hace complicado el poder utilizarlo.	Para hacer un uso completo del estándar sería recomendable estar familiarizado con el estándar NIST completo.
ISO 27001/2	Establece una guía de actuación concreta y reducida sobre la protección contra el malware	No aborda en profundidad el tema del Ransomware. Es una definición demasiado genérica.	Es la más comúnmente utilizada en Europa.
INCIBE	Una guía para el empresario para que conozca la peligrosidad del malware y lo que puede hacer para combatirlo.	Desactualizado: Se realizó en 2017 y no contempla el teletrabajo como vector de ataque	Es una guía importante pero no todas las empresas conocen de ella.
CCN-CERT	Una guía para combatir el Ransomware una vez éste ha invadido un sistema.	El apartado de prevención es escaso, dejando partes importantes sin especificar.	Es poco conocido

Como podemos observar en la tabla, cada uno de los recursos que hemos explicado tienen una organización y esquema diferentes, pero todos ellos se basan en proponer recomendaciones específicas para mejorar la seguridad existente frente a ataques de Malware o Ransomware.

El Framework que vamos a presentar en este documento no se basa solo en ofrecer recomendaciones, sino que además va a ayudar a la evaluación de la seguridad en las empresas cubriendo dos aspectos que hasta el momento ninguno de los estándares y guías que hemos comentado trataba: el ciclo de vida de un ataque y la adaptación a la actualidad y a las necesidades específicas de cada PyME. Por ello va a ofrecer una cobertura más amplia de una forma dinámica que ayudará a comprender a las empresas cada uno de los pasos que debe ir cumpliendo supliendo de alguna manera la forma general y en ocasiones insuficiente en la que estos Frameworks cubren la defensa contra el Ransomware.

3. Desarrollo de la solución

Una vez analizadas las herramientas del mercado, es el momento de presentar el Framework como complemento para mitigar las debilidades existentes en ellos como hemos explicado en el apartado anterior. Hemos decidido utilizar el ciclo de vida de un ataque de Ransomware como elementos vertebrados de la propuesta [20] para ofrecer una visión específica y así cubrir la generalización que teníamos presente hasta el momento. Más específicamente hay dos razones principales por las que hemos decidido realizarlo de esta manera:

- Falta de un Framework con esta estructura en el mercado, por lo tanto, cubrir un hueco de mercado existente; y,
- Posibilidad de dar un peso, y por tanto una puntuación, a cada una de las etapas que identifiquemos en el ciclo de vida del Ransomware con respecto al nivel de defensa existentes en la organización evaluada.

Por estos motivos, considerando la importancia de las diferentes etapas del ataque vamos a adaptar nuestro Framework a sus fases, que explicaremos detenidamente a continuación.

3.1. Ciclo de vida de un ataque de Ransomware

El ciclo de vida de un ataque de Ransomware, como mencionamos ya en el capítulo 2 de esta memoria está formado por siete fases (ver Ilustración 8):

Ilustración 8:Ciclo de vida de un ciberataque

Las organizaciones evaluadas pueden mostrar distintas debilidades en cada una de estas fases. Puesto que, evitando o al menos mitigando, dichas debilidades es posible reducir el daño que puede producir el Ransomware en una organización, nuestra guía se enfocará atendiendo a las fases identificadas en este ciclo de vida.

Para poder comprender los controles de nuestro Framework es necesario entender las fases por los que pasa un Ransomware, por ello se describirán en los siguientes subapartados.

3.1.1 Reconocimiento

La primera fase de un ciberataque es la de "Reconocimiento". En esta fase nos encontramos un punto en la que el ciberdelincuente va a investigar y tratar de encontrar la forma en la que introducir este software malicioso en el sistema. Podrá ser, bien mediante un USB infectado, unos puertos públicos en los que pueda infiltrarse, recabando información sobre contraseñas utilizando "*Shoulder surfing*" (ver glosario) o bien mediante ingeniería social, es decir, utilizando los correos electrónicos como troyanos para introducir este software malicioso dentro de los dispositivos de la empresa. Estas estrategias de infiltración se listan en la Ilustración 9: Reconocimiento. Fase 1 del ciclo de vida de un ataque.

Ilustración 9: Reconocimiento. Fase 1 del ciclo de vida de un ataque Ransomware

Un estudio realizado en 2021 [18] indica que la forma más común de ataque mediante Ransomware es utilizar la ingeniería social como vector de ataque. De hecho, y tal y como detalla la Ilustración 10: Tendencia de vectores de ataque el Phishing (una técnica de ingeniería social, se puede ampliar el concepto en el Glosario) es la que representa el 52% de los vectores de ataque utilizados por los ciberdelincuentes para introducir Ransomware en las organizaciones.

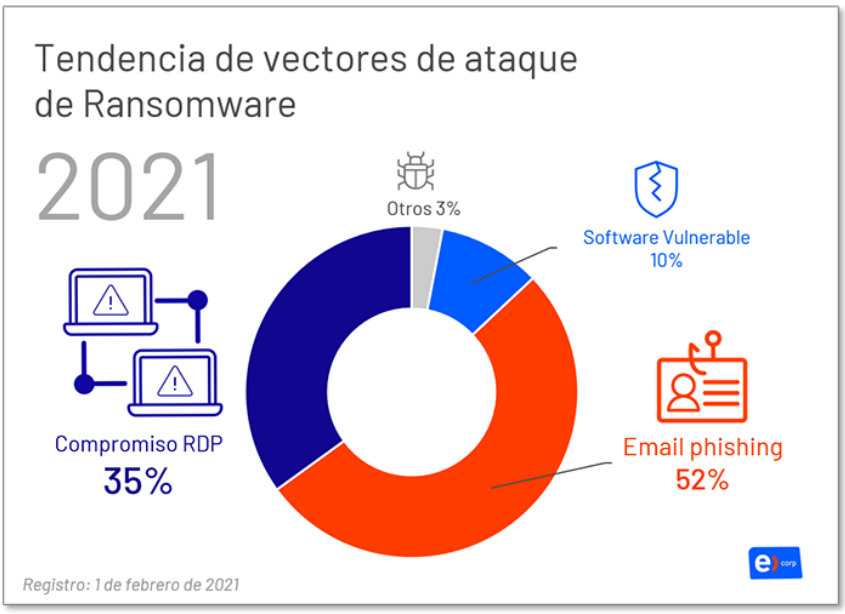


Ilustración 10: Tendencia de vectores de ataque [19]

Esta fase es una de las más crítica con respecto a las demás ya que si el ciberdelincuente no encuentra la manera de introducir este malware dentro de la organización no podrá llevar a cabo ningún ataque. Es fundamental que las empresas entiendan cuales son las amenazas actuales y la forma en que los ciberdelincuentes presentan sus ataques para así poder defenderse de ellos.

3.1.2 Acopio de Armas

La fase de Acopio de Armas o "*weaponization*" en inglés, hace referencia al paso en el que el ciberdelincuente va a seleccionar la, o las, herramienta(s) o arma(s) que va a utilizar contra la organización.

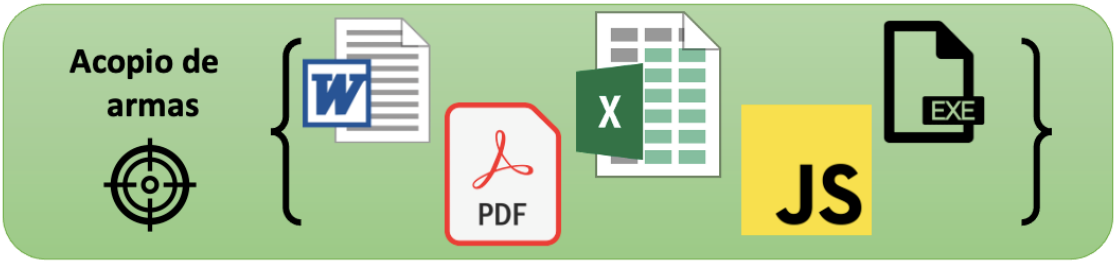


Ilustración 11: Acopio de Armas. Ciclo de vida de un ataque

Tras realizar el estudio en la fase anterior, el atacante establece cuál es la mejor manera de infiltrarse en la organización. Por ejemplo, si es una empresa que tiene una gran carga administrativa es común que la forma que adopte el ataque sea en forma de

documento de texto u hoja de cálculo, ya que la empresa está acostumbrada a recibir documentación por parte de personas externas a la organización e inicialmente no desconfiará si la dirección de envío o el asunto es vagamente familiar. En este caso puede insertar el código maligno en la macro del documento y de este modo infectar el dispositivo cuando lo abra. En otros casos la forma que tomará el ataque será en forma de ejecutable (.exe) o un archivo de JavaScript (.js).

Es un punto importante ya que adecuar el arma a utilizar muchas veces determinará la eficacia de un ataque por parte de los ciberdelincuentes.

3.1.3 Despliegue

La fase de despliegue hace referencia al momento en el que ciberdelincuente decide cómo va a utilizar su armamento.

Ilustración 12: Despliegue. Ciclo de vida de un ataque.

Como podemos ver en la Ilustración 12: Despliegue. Ciclo de vida de un ataque., hay diferentes modos para desplegar el malware. Algunos ejemplos pueden ser:

- Mediante email. Uno de los recursos más utilizados por su mínimo coste.
- USB. Conectar un USB a un dispositivo de la empresa.
- WhatsApp. Un inocente mensaje de WhatsApp con un enlace o un archivo para que el usuario interactúa con el.
- Páginas web maliciosas. En las que al entrar se descarga un malware que infecta el dispositivo al acceder a ellas.

Una vez el delincuente escoge la forma en que va a lanzar el malware, debe decidir cuándo lo despliega. Esta fase incluye no sólo el cómo, sino también el cuándo realizar el ataque.

3.1.4. Explotación

La fase de explotación engloba ese momento en el cual se ha desplegado el ataque y el usuario ha de interactuar con él.

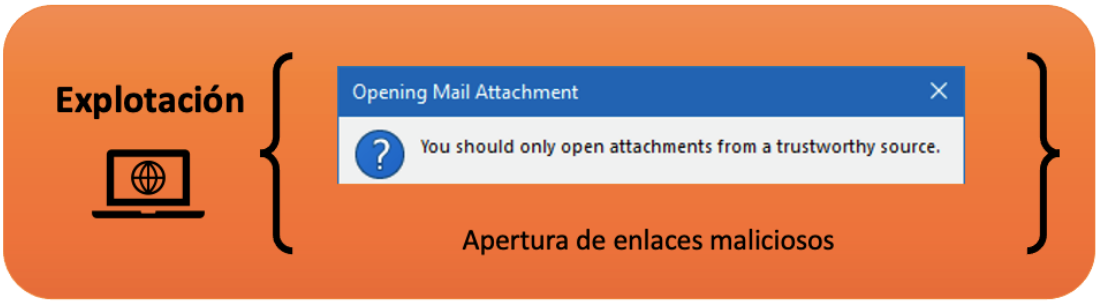


Ilustración 13: Explotación. Ciclo de vida de un ataque.

Como podemos observar en la Ilustración 13: Explotación. Ciclo de vida de un ataque., la explotación está relacionada con la activación del malware que suele estar ligado con el uso por parte de las víctimas de un enlace malicioso o la apertura de un adjunto. Este punto es crítico para el ciclo de vida de un ataque, pues no importa lo sofisticado o adecuado al objetivo que sea un ataque, si el usuario no interacciona con él, el atacante no podrá llegar a infectar el dispositivo.

El tipo de interacción difiere en función de la forma en la que el malware haya sido desplegado durante el ataque:

- Si ha llegado mediante un email y adopta la forma de un enlace a una página desde la que se carga el Malware, la interacción del usuario hará referencia a cuándo accede el usuario a ese enlace voluntariamente.
- Si llega por email en forma de un archivo adjunto, la explotación se llevará a cabo cuándo la víctima abra dicho archivo.
- Cuando el ataque se despliegue mediante una unidad USB, la acción que deberá realizar la víctima para activar el malware será la de conectar la unidad USB y/o abrir el archivo/s que lo contiene. Destacar que esta forma es la menos frecuente de todas.

3.1.5. Instalación

Como su propio nombre indica, durante esta fase el malware se instala en el dispositivo o dispositivos comprometidos, quedando a la espera de poder realizar la acción maligna para la que fue creado.

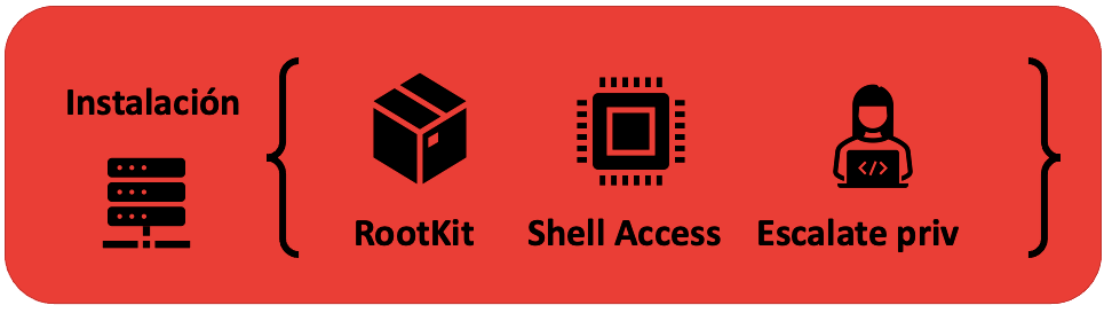


Ilustración 14: Instalación. Ciclo de vida de un ataque.

El malware al entrar en el dispositivo se instala de manera que lanza una señal a su creador o controlador para indicar que el despliegue ha comenzado y que ya he entrado en el sistema. La siguiente fase esta muy ligada a esta.

3.1.6. Comando y control

La fase de comando y control es una fase que estará latente en algunos tipos de malware.

Ilustración 15: Comando y control. Ciclo de vida de un ataque.

En el caso del Ransomware la fase de Comando y control es fundamental y determinará la gravedad de un ataque de este estilo, ya que cuando el dispositivo es infectado no se activa automáticamente el Ransomware, sino que el troyano que ha sido el transporte del mismo informa a su creador de que ha depositado su carga en el

dispositivo y que ya puede proceder a la búsqueda de su objetivo final, de esta forma el ciberdelincuente buscará acceso al lugar donde puede crear más daño: Un directorio activo, una base de datos desprotegida, un servidor de almacenamiento de información, etc.

Si se trata de un servidor, por ejemplo, el Ransomware se propagará y no se detendrá hasta que alcance el sistema servidor. Como muestra la Ilustración 14 (del apartado anterior), este proceso de propagación en el sistema puede comportar el uso de algún tipo de rootkit (o software malicioso diseñado para permanecer oculto en un ordenador mientras proporciona acceso y control remotos) que el atacante podrá utilizar para abrir un shell y hacerse con los privilegios necesarios para poder instalar su Ransomware. En algunos Ransomware más sofisticados, este proceso de búsqueda, elevación de privilegios e instalación está automatizado.

Uno de los puntos más determinantes a tener en cuenta en el caso del Ransomware es la velocidad con la que actúa, una rapidez que no permite que se pueda interceptar este punto. Cabe reseñar que las últimas dos fases que hemos explicado tienen una relación muy estrecha y se pasa de una de ellas a la otra de una manera muy rápida.

3.1.7. Actuación en el objetivo

Esta última fase, hace referencia al ataque en si como se puede apreciar en la Ilustración 16: Actuación en el objetivo. Ciclo de vida de un ataque.

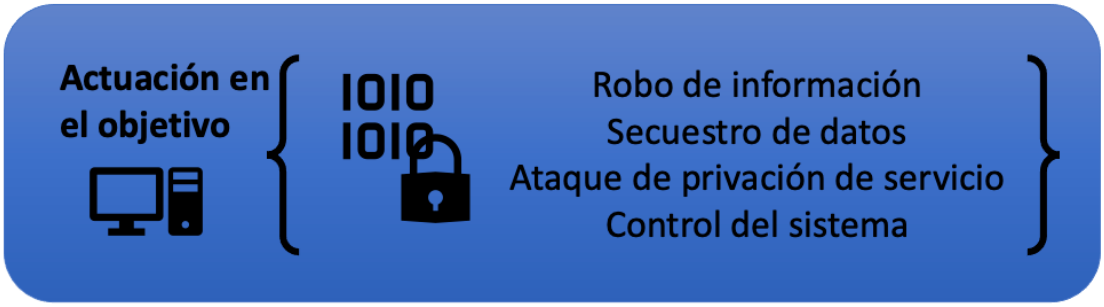


Ilustración 16: Actuación en el objetivo. Ciclo de vida de un ataque.

En el caso concreto del Ransomware, su ataque se traducirá en un secuestro de los datos del sistema atacado. Además, el Ransomware, desplegará una pantalla en la

que informará a la víctima del ataque y de que ha tomado cautivos todos los datos disponibles una vez haya finalizado esta codificación. Obviamente, si el sistema no está bien protegido toda la información de la organización puede estar potencialmente en peligro.

Cuando hablábamos de velocidad, nos referíamos a que el ciberdelincuente una vez ha encontrado el lugar donde desea desplegar el malware, lo que desea es infectar el mayor número posible de archivos en el menor tiempo, por ello cuando empieza a codificar lo que hará será codificar las cabeceras de los documentos y archivos, no el documento completo, de este modo el dispositivo no podrá reconocer el documento por lo que no podrá mostrarlo, capturando de manera efectiva la información que tiene dentro.

Codificar una cabecera es mucho más sencillo que codificar un archivo completo por lo que en poco tiempo (una ventana de tiempo que tienen establecida muy pequeña que apenas durará algunos minutos) tendrán la mayoría de los archivos cautivos. De este modo pueden mostrar por pantalla la ventana que indique al usuario que es víctima de un Ransomware (Ventana de la cual hemos mostrado algunos ejemplos en la Ilustración 6: Ejemplos de pantalla mostrada por Ransomware), el que acabamos de explicar es un ejemplo de actuación de algunos malware.

En resumidas cuentas, el ciclo de vida de un ataque está bien establecido y se pueden identificar piezas clave en la seguridad de las organizaciones en cada uno de los apartados que lo componen. De ahí que nuestra propuesta quiera afrontar estos puntos poco a poco, ya que como hemos expuesto, aunque llegue a nuestra bandeja de correo electrónico un email cargado con un Ransomware en forma de documento, si nuestra concienciación en ciberseguridad es adecuada, cortaremos el ciclo de una manera rápida y sencilla, reportando con un clic el email fraudulento y conservando la información de la organización.

3.2. Estructura general del Framework propuesto

Una vez hemos establecido el esqueleto básico del ciclo de vida de un ataque, vamos a presentar cual será la organización de nuestro Framework, que va a estar basado en las mimas fases. Por cada una de las fases estableceremos una serie de cuestiones (controles) para evaluar la protección de la que dispone la empresa entrevistada.

Específicamente, lo que haremos será realizar una serie de preguntas para que la empresa valore de forma objetiva en qué posición se encuentra de defensa frente al ataque en cada fase.

Iniciamos, con la **fase de reconocimiento** que irá asociada a la de **acopio de armas** en las que vamos a tratar todos aquellos temas referentes a la concienciación de los empleados y las buenas prácticas que realiza la empresa a nivel de concienciación y protección de sus activos, tanto a nivel lógico como físico. También incluiremos el contacto con los grupos de interés para mantenerse informado de las novedades en materia de amenazas cibernéticas. Un índice de este apartado sería el siguiente:

- Protección de dispositivos físicos.
- Protección de contraseñas.
- Protección de personas.
- Conocimiento de amenazas.
- Contacto con organizaciones especializadas.

El siguiente apartado de nuestro Framework se centra en **las fases de despliegue y explotación** de un ataque. En este caso nos centraremos en tres partes fundamentales.

- Ejercicios de concienciación.
- Formaciones.
    - Navegación segura
    - Uso correcto del correo electrónico
- Política de dispositivos externos de almacenamiento

Estas dos fases están íntimamente relacionadas con las anteriores, pero tratan otros temas referentes al despliegue (phishing, ingeniería social, etc.) y a la explotación (no hacer clic en enlaces, antispam en el correo electrónico).

Las fases de **instalación** y **comando y control** son fases en las que el atacante despliega el malware y busca su objetivo dentro de los dispositivos de la empresa. Son las fases más técnicas y sus preguntas estarán más orientadas a zonas más concretas de la empresa como su red. Hay una serie de puntos importantes que debemos abordar.

- Seguridad en las Comunicaciones.

  - Fragmentación de la red.
  - Filtración de correo electrónico
  - Bloqueo de macros
- Protección anti malware
- Análisis de malware en los dispositivos.

Por último, en la fase de **Actuación en el objetivo,** la fase en la que finalmente se realiza el impacto. Esta fase tiene mucha relación con planes de contingencia y como recuperar la información una vez se ha dado el ataque, por ello estableceremos los siguientes puntos:

- Plan de contingencia.
- Copias de seguridad.

3.3. Controles

En este punto vamos a especificar las preguntas (a las cuales también llamaremos controles) que vamos a utilizar para evaluar cada uno de los apartados que hemos propuesto en el apartado anterior. Cada una de ellas está incluida en una de las fases del ciclo de vida de un ciberataque. Vamos a mostrar ejemplos de las preguntas que se pueden encontrar en cada uno de los apartados, aquellas que son más significativas. En el Anexo I: Árbol de decisión y puntuación de los controles podemos ver todas las preguntas conforme aparecen en el Framework.

❖ Reconocimiento y Acopio de armas
  - ➢ Protección de dispositivos físicos.
    - ¿Se realizan revisiones periódicas del estado de los dispositivos físicos de los empleados?
    - En situaciones de teletrabajo ¿están protegidos los dispositivos que la empresa le proporciona al trabajador con un antivirus y/o un firewall?
  - ➢ Protección de contraseñas (Empleados).
    - ¿Existe y se cumple una política específica sobre la creación y cambio de contraseñas al iniciar la relación laboral?
    - ¿Se obliga a los usuarios a crear contraseñas suficientemente robustas (Más de 12 caracteres que incluyan mayúsculas, minúsculas, números y símbolos)?
  - ➢ Protección de personas.

        - ¿se proporciona a los empleados de una guía con sus derechos y deberes como empleados para la seguridad de la información?
    - Conocimiento de amenazas.
        - ¿Se proporciona a los empleados de algún manual acerca de los peligros del malware y como enfrentarse a él?
    - Contacto con organizaciones especializadas.
        - ¿Se mantiene por parte de la empresa contacto con organizaciones como el INCIBE o CCN (en forma de boletín) para estar actualizado de las amenazas existentes y poder actualizar a los empleados?

- Despliegue y explotación
    - Ejercicios de concienciación.
        - ¿Se realizan campañas de simulación de Phishing para toda la empresa (todos aquellos usuarios que dispongan de correo electrónico corporativo activo) cada cuatro meses?
        - ¿Se evalúa el nivel de concienciación de los empleados de toda la empresa con algún test?
    - Formaciones.
        - ¿Se realizan formaciones en concienciación de ciberseguridad a todos los empleados?
        - Navegación segura:
            - ¿Se proporciona algún material o guía al empleado para que practique una navegación web segura?
        - Uso correcto del correo electrónico:
            - ¿Existe un control de los dispositivos que tienen acceso al correo electrónico?
            -
    - Política de dispositivos externos de almacenamiento
        - ¿Existe un protocolo o política de actuación para el uso de dispositivos de almacenamiento externos?
        - ¿Se utilizan bloqueadores de ejecución de USB para limitar el acceso del USB al ordenador?

- Instalación y Comando y control
    - Seguridad en las Comunicaciones.

- Fragmentación de la red.
  - ¿Existe fragmentación en la red corporativa?
- Filtración de correo electrónico
  - ¿Se realiza un filtrado del correo electrónico que llega a los buzones corporativos?
- Bloqueo de macros
  - ¿Están activadas las macros en la organización?
- ¿Utiliza el trabajador conexiones de red seguras?

➢ Protección anti malware
- ¿Tienen configurados los dispositivos algún tipo de antivirus?
- ¿Se utilizan VPN cuando se realiza teletrabajo?

➢ Análisis de malware en los dispositivos
- ¿Se realizan escaneos de los dispositivos en busca de malware o vulnerabilidades cada tres meses?

❖ Actuación en el objetivo

➢ Plan de contingencia.
- ¿Existe un plan de contingencia establecido en el plan de continuidad de negocio que especifique un escenario como un ataque de Ransomware?

➢ Copias de seguridad.
- ¿Existen copias de seguridad de la información de la organización?
- ¿Las copias de seguridad están almacenadas en el servidor de la organización junto a la información?
- ¿Se almacenan copias de seguridad en entornos no conectados a la red como cajas fuertes, etc.?

3.4. Herramientas utilizadas

Hemos utilizado las siguientes herramientas para confeccionarla:

Ilustración 17: Herramientas del Paquete Office utilizadas

- **MSOffice Word:** Editor de texto utilizado para desarrollar la memoria.
- **MSOffice Excel**: Hoja de cálculo del paquete Office utilizada para escribir el Framework. Se ha utilizado este programa por su facilidad de utilización y las características que aporta.
- **MSOffice PowerPoint:** Se ha utilizado para realizar los diagramas del ciclo de vida de un ataque de Ransomware.
- **Drawio**: Utilizado para diseñar el árbol de decisión.

3.5. Estructura del documento

El Framework propuesto es un documento Excel, que constará de tres hojas principales:

- La primera hora será el cuestionario, en el que incluirá las preguntas que se realizarán a la organización de las que hemos hablado en apartados anteriores y pueden verse en el Anexo I.
- La segunda hoja Incluye la puntuación en porcentaje de cada una de las cuestiones, con las recomendaciones asociadas (solo en caso de que en la anterior hoja se haya respondido que no a la pregunta) y la puntuación general del Framework.
- La tercera hoja será la leyenda para que aquella persona que maneje el Framework pueda interpretar el cuestionario y aplicarlo. Además, se dispondrá de la relación de apartado y recomendación que utilizaremos para la página anterior.

A continuación, después de esta breve explicación de la estructura, vamos a detallar cada una de las hojas y su composición.

3.5.1. Cuestionario

El cuestionario se presenta en forma de tabla, con tres columnas principales y una secundaria. Tiene el aspecto que podemos ver en la Ilustración 18: Extracto del Framework de defensa. Hoja: Cuestionario:

Apartado	Pregunta	Respuesta (Sí o No)	Observaciones
	1. Reconocimiento y Acopio de Armas		
	1.1 Protección de dispositivos físicos		
1.1.1	¿Se realizan revisiones periódicas del estado de los dispositivos físicos de los empleados?		
1.1.2	En situaciones de teletrabajo, ¿utiliza el trabajador un teléfono móvil que le proporciona la empresa?		
1.1.3	En situaciones de teletrabajo, ¿utiliza el trabajador un ordenador portátil que le proporciona la empresa?		
1.1.4	En situaciones de teletrabajo, ¿utiliza el trabajador una conexión a internet que le proporciona la empresa?		
1.1.5	¿Están protegidos los dispositivos que la empresa le proporciona al trabajador con un antivirus y/o un firewall?		
	1.2 Protección de contraseñas		
1.2.1	¿Existe una política específica sobre la creación y cambio de contraseñas al iniciarse la relación laboral?		
1.2.2	¿Se obliga a los usuarios a crear contraseñas suficientemente robustas? Robustez adecuada: 12 caracteres, mayúsculas, minúsculas, números y simbolos.		
1.2.3	¿Se exige a los usuarios que modifiquen su contraseña cada tres meses?		
1.2.4	¿Se exige a los usuarios que modifiquen su contraseña cada año?		
1.2.5	¿Se le da algún tipo de indicación al usuario de como configurar la complejidad de su contraseña?		

Ilustración 18: Extracto del Framework de defensa. Hoja: Cuestionario

Las tres columnas principales son aquellas que hacen referencia al apartado (numeración que seguiremos dentro del Framework), pregunta (donde se describe la pregunta) y Respuesta (donde la organización contestará de manera concisa con un sí o un no la pregunta planteada).

La pregunta se responde con un sí o un no que se podrá seleccionar en la columna como se muestra en la Ilustración 19: Extracto del Framework de defensa, selección de respuesta

Apartado	Pregunta	Respuesta (Sí o No)
	1. Reconocimiento y Acopio de Armas	
	1.1 Protección de dispositivos físicos	
1.1.1	¿Se realizan revisiones periódicas del estado de los dispositivos físicos de los empleados?	
1.1.2	En situaciones de teletrabajo, ¿utiliza el trabajador un teléfono móvil que le proporciona la empresa?	Si / No
1.1.3	En situaciones de teletrabajo, ¿utiliza el trabajador un ordenador portátil que le proporciona la empresa?	
1.1.4	En situaciones de teletrabajo, ¿utiliza el trabajador una conexión a internet que le proporciona la empresa?	

Ilustración 19: Extracto del Framework de defensa, selección de respuesta

La columna secundaria de la que hablamos es la columna de observaciones que quedará a disposición de la organización para que pueda expresar algún detalle sobre su respuesta en caso de que lo considere oportuno.

3.5.2. Recomendaciones y resultados

La segunda página que compone el Framework es aquella que especifica las recomendaciones y los resultados que tiene la forma que podemos ver en la Ilustración 20: Extracto del Framework de defensa. Hoja: Recomendaciones y resultado.

Apartado	Pregunta	Valoración	Recomendación
1. Reconocimiento y Acopio de Armas - 25%			
1.1 Protección de dispositivos físicos - 20%			
1.1.1	¿Se realizar revisiones periódicas del estado de los dispositivos físicos de los empleados?	20%	-
1.1.2	En situaciones de teletrabajo ¿Utiliza el trabajador un teléfono móvil que le proporciona la empresa?	20%	-
1.1.3	En situaciones de teletrabajo ¿Utiliza el trabajador un ordenador portátil que le proporciona la empresa?	20%	-
1.1.4	En situaciones de teletrabajo ¿Utiliza el trabajador una conexión a internet que le proporciona la empresa?	20%	-
1.1.5	¿Están protegidos los dispositivos que la empresa le proporciona al trabajador con un antivirus y/o un firewall?	20%	-

Ilustración 20: Extracto del Framework de defensa. Hoja: Recomendaciones y resultado

En esta hoja podemos apreciar que se compone de tres partes principales, la primera parte como se aprecia, tendremos de nuevo las preguntas con las que estamos familiarizados, el apartado y dos columnas nuevas:

- **Valoración**: En esta columna se indica el porcentaje de peso de la pregunta frente al subapartado o sección al que corresponde.
- **Recomendaciones**: En esta columna aparecerá en función de si la respuesta es afirmativa o no la recomendación asociada a la pregunta:
    - Si la respuesta es Si, se cumple el control, por lo que no es necesario que se indique la recomendación ya que se ha indicado que la empresa realiza la acción correctamente.
    - Si la respuesta es No, aparecerá la recomendación asociada al control, que esta detallada en la página de leyendas.

Apartado	Pregunta	Valoración	Recomendación
1. Reconocimiento y Acopio de Armas - 25%			
1.1 Protección de dispositivos físicos - 20%			
1.1.1	¿Se realizar revisiones periódicas del estado de los dispositivos físicos de los empleados?	20%	-
1.1.2	En situaciones de teletrabajo ¿Utiliza el trabajador un teléfono móvil que le proporciona la empresa?	20%	En caso de que sea posible que la organización le entregue al trabajador un dispositivo configurado por ellos y en caso de que tenga que usar el propio que guarde las medidas de seguridad adecuadas. Establecer una política de uso correcto de dispositivos en teletrabajo.
1.1.3	En situaciones de teletrabajo ¿Utiliza el trabajador un ordenador portátil que le proporciona la empresa?	20%	-
1.1.4	En situaciones de teletrabajo ¿Utiliza el trabajador una conexión a internet que le proporciona la empresa?	20%	En caso de que sea posible que la organización le entregue al trabajador un dispositivo configurado por ellos y en caso de que tenga que usar el propio que guarde las medidas de seguridad adecuadas. Establecer una política de uso correcto de dispositivos en teletrabajo.
1.1.5	¿Están protegidos los dispositivos que la empresa le proporciona al trabajador con un antivirus y/o un firewall?	20%	-

Ilustración 21: Extracto Framework de defensa. Hoja: Recomendaciones y resultado con recomendaciones presentes.

Presentemos un ejemplo que clarifique el uso del Framework que estamos describiendo. Como podemos ver en la Ilustración 21: Extracto Framework de defensa. Hoja: Recomendaciones y resultado con recomendaciones presentes. en el caso de que el control 1.1.2 y 1.1.4 hayan sido respondidos negativamente la recomendación aparecerá en el espacio dedicado para ello. La segunda y tercera parte de la hoja son las puntuaciones:

Respuesta en el cuestionario	Puntuación de la organización
Resultado Apartado =	3
Resultado Subapartado =	0,6
Si	0,2
No	0
No	0
Si	0,2
Si	0,2

Ilustración 22: Extracto del Framework: Resultados del cuestionario

En la Ilustración 22: Extracto del Framework: Resultados del cuestionario podemos ver un extracto del primer subapartado del apartado uno, se compone de dos columnas, la primera indica si el control ha sido puntuado afirmativa o negativamente, mientras que la segunda columna muestra la puntuación en función del porcentaje. En caso afirmativo, se sumará la puntuación, en caso de respuesta negativa, la puntuación se restará.

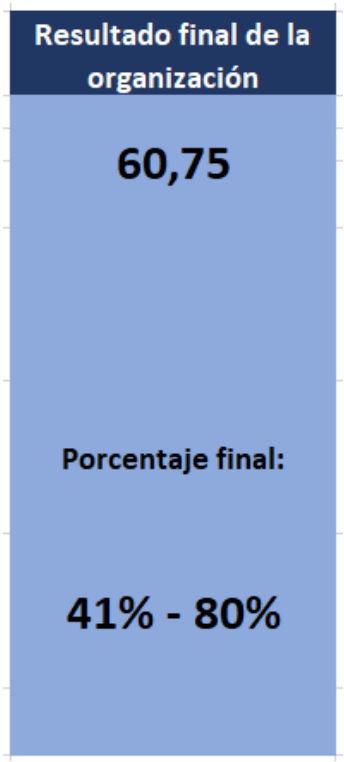


Ilustración 23: Extracto del Framework de defensa: Resultado final de la organización

En esta última parte que podemos ver en la Ilustración 23: Extracto del Framework de defensa: Resultado final de la organización tendremos la suma de la puntuación total, que nos permitirá ver en qué porcentaje de los cuatro que definiremos más adelante se encuentra la organización.

3.5.3. Leyenda

La última hoja de nuestro documento será una explicación de las diferentes escalas que vamos a utilizar a lo largo del documento. Además, incluye todas las recomendaciones asociadas a los apartados que podemos ver de manera amplia en el Anexo II.

De las escalas que tenemos en la tercera hoja del documento, la primera que vamos a desarrollar será:

Tabla 2: Respuestas al cuestionario

Respuesta al cuestionario
Sí. Si se cumple lo estipulado en la pregunta en su totalidad.
No. Si no se cumple lo estipulado en la pregunta en su totalidad.

Indica la manera en la que se han de responder las preguntas del cuestionario. La segunda escala que encontramos en esta página del documento es una pieza importante que relacionaremos con la Ilustración 23: Extracto del Framework de defensa: Resultado final de la organización.

Tabla 3: Resultado final del cuestionario dividido en porcentajes

Resultado final del cuestionario en porcentajes
100%
81% - 99%
41% - 80%
0% - 40%

En ella mostramos los porcentajes del resultado de la puntuación del cuestionario. Las únicas puntuaciones aceptables serán:

- 100%
- 81% - 99%

Las otras dos opciones serán consideradas un fallo en la seguridad de la empresa que indica que es vulnerable (41%-80%) o muy vulnerable (0% - 40%) a un ataque de Ransomware.

Por último, en la hoja de Leyendas tendremos como íbamos indicando la relación de todas las recomendaciones con sus respectivos apartados que se encuentra en su totalidad descrito en el Anexo II.

3.6. Método de puntuación Framework propuesto

El sistema de valoración de este cuestionario va a ser el siguiente:

- El cuestionario total tiene una puntuación de un 100%, que indicará el grado de protección que posee la empresa frente a amenazas de Ransomware. Dentro de este porcentaje vamos a determinar una serie de franjas.
    - 0% al 40% La protección es baja, se recomienda encarecidamente realizar acciones para mejorar la protección de la organización frente a Ransomware ya que podemos determinar que **no se encuentra protegida de manera aceptable.**
    - Del 41% al 80% la protección es media, existen medidas de protección que son importantes pero la protección no es óptima. Se recomienda que se cubran las fases que no estén por encima del 60% y se mejoren las que sí lo estén. En conclusión, en esta franja podemos determinar que **se encuentra protegida de manera aceptable pero no óptima.**
    - Del 81% al 99%, la organización está en un punto de protección recomendado donde las modificaciones o procesos que tenga que realizar para llegar al 100% serán pocos y se recomienda encarecidamente que se alcancen. Determinamos que **la organización se encuentra protegida frente al Ransomware de una manera óptima.**
    - 100%. La organización en el momento en que se pasa el cuestionario cumple todos los puntos planteados. **La organización se encuentra protegida del Ransomware de manera robusta.** En este caso la recomendación será realizar el cuestionario cada seis meses para comprobar que no falla ninguno de los aspectos anteriormente planteados con la rotación de personal, equipos o software.
- Cada apartado o bloque (los bloques son las etapas, por ejemplo, Bloque 1: Reconocimiento y Acopio de Armas) tiene un porcentaje determinado en función de los 6 bloques totales. No todos los bloques tendrán el mismo porcentaje, al lado de cada título de bloque podremos ver su peso en referencia al total de 100%

- Cada subapartado (subapartado, por ejemplo,1.1 Protección de dispositivos físicos) tendrá un porcentaje dentro de su apartado para darle el valor correspondiente sobre el 100% del peso asociado al apartado al que pertenece. La puntuación de los subapartados será obtenida mediante la suma de los porcentajes de las preguntas, aunque la puntuación pueda ir más allá de 100%, el máximo será 100%. Esto sucede porque existen alternativas complementarias, por ejemplo de protección o detección, que si se cumplen simultáneamente sumas más allá de ese valor máximo que es posible obtener del 100%.
- Un subapartado esta dividido en secciones, los controles de estas secciones se puntuarán de la misma manera que los subapartados.

El esquema final que quedará plasmado será el siguiente:
Framework:

- Apartados
    - Subapartados
        - Secciones

Podemos ver el cuadro resumen con las puntuaciones de cada apartado, subapartado, sección y pregunta en el **Anexo I**.

Destacar que hay 3 preguntas que tienen puntuación negativa, lo que significa que si la respuesta a las mismas es un si, la puntuación en vez de sumar al total restará. Las preguntas son las siguientes:

2.3.3	¿Se permite el uso de dispositivos USB no autorizados o proporcionados por la empresa para almacenar información de la misma?
3.1.3	¿Están activadas las macros en la organización?
3.1.6	¿La conexión que utiliza el empleado tiene la IP abierta?

La respuesta afirmativa a estas preguntas supone una penalización sobre el resultado final. Para especificar de forma más clara la utilización del sistema de puntuación vamos a plantear un ejemplo:

El apartado 1 tiene un peso final del 20% de la puntuación total del cuestionario, El subapartado 1.1 tiene un peso del 20% del total del apartado 1 y la pregunta 1.1.1 significa el 20% de la puntuación. Si la organización responde afirmativamente tiene el total de la puntuación:

- **Subapartado 1.1**: 20%
- **Apartado 1**: 20 * 0.2 = 4
- **Puntuación en el cuestionario global** = 4 * 0.2 = 0.8

Con esa pregunta respondida de manera afirmativa se obtendría una puntuación del 0.8% sobre cuestionario global. Replicando esta ecuación, en función de los porcentajes expuestos en el Anexo I construiremos la puntuación final del Framework, una puntuación que irá de 0 a 100.

Los porcentajes que podemos ver en el Anexo I: Árbol de decisión y puntuación de los controles no han sido seleccionados de una manera aleatoria. El nivel de importancia reflejado en los porcentajes está basado en su gran mayoría en la importancia que la normativa ISO 27001:2022 le da a muchos de los aspectos que se exponen en las preguntas, que aunque no especificados para la protección contra el Ransomware, se consideran relacionados con la seguridad de la información. Por ello la decisión de valorar algunos elementos más que otros no es completamente subjetiva sino que tiene una base en la normativa citada.

3.7 Despliegue del Framework propuesto

Una vez hemos desarrollado el Framework y su utilización, es necesario explicar de qué manera se va a proporcionar a las empresas. El ideal es que la propia organización quiera determinar sus deficiencias para protegerse, la realidad es que, en ocasiones, hasta que no sufren un ataque o un intento de ataque no se dan cuenta de la importancia de protegerse ante malware y en concreto ante el Ransomware.

Una vez la empresa comunica la necesidad de estudiar las defensas que poseen, es cuando se presenta el Framework, que se cumplimentará en una entrevista entre los responsables del departamento de IT o de ciberseguridad y aquel que presenta el Framework.

Mediante la entrevista se completan las preguntas del Framework, es importante que las persona que ayuda a la empresa a rellenarlo tenga conocimiento de las normativas básicas (ISO 27001 y ISO 27002) para poder ayudar a resolver posibles dudas que puedan surgir.

Una vez finaliza la entrevista, el especialista que maneja el Framework tendrá una aproximación del resultado de la entrevista de forma numérica y gracias a las recomendaciones incluidas en el Framework tendrá una guía para presentar lo que la empresa debería realizar para mejorar aquellos puntos donde flaquea.

3.8 Árbol de decisión

Como hemos ido describiendo, el cuestionario se divide en apartados, estas secciones con sus subapartados y controles van a formar arboles de decisión que determinarán caminos de decisiones. Habrá caminos de comportamiento adecuado y caminos de comportamiento inadecuado o escaso. Si utilizamos ejemplos de la primera fase: *Reconocimiento y Acopio de Armas* podemos ver las diferentes formas que puede tomar la decisión de cada subapartado.

Reseñar que se puede ver el árbol de decisión completo dividido por apartados en el Anexo I: Árbol de decisión y puntuación de los controles.

Hay dos tipos de Subapartados principales:

- Caminos con el mismo peso: En este caso, como podemos ver en la Ilustración 24: Subapartado Protección de personas indica en color verde ambos caminos, lo que significa que para conseguir la mayor puntuación que ofrece el apartado, es necesario que se cumplan ambos. Esto hace referencia a que los controles del subapartado aunque tengan diferente puntuación, todos son necesarios para alcanzar el 100%.

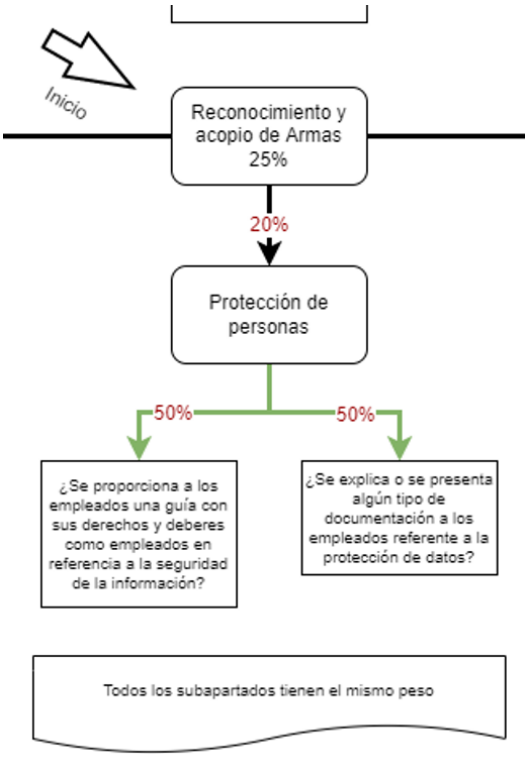


Ilustración 24: Subapartado Protección de personas. Árbol de decisión

En la ilustración que acabamos de presentar podemos ver que de sus dos opciones ambas están valoradas en 50% y para poder alcanzar la máxima puntuación del apartado, es necesario que la respuesta a ambas sea un sí.

El segundo tipo de camino es el siguiente:

- Caminos con diferente peso y opciones: En este caso, se indica el caminó que se irá cumpliendo en función de las respuestas que se toma, si se responde si, a la pregunta se obtendrá una puntuación mientras que si se responde no se continuará hacía abajo.

Como nos muestra la imagen siguiente, en este caso si simplemente se responde que si al primer control *(¿Existe un conocimiento reglado por parte de todos los empleados mediante charlas o formaciones de las amenazas a las que se pueden enfrentar en su día a día en la empresa?)* la máxima puntuación es obtenida y no será necesario que responda a las demás cuestiones ya que está implícito que si esa es afirmativa todas las demás lo serán pues son variaciones de la misma pregunta. En caso de que la respuesta a esta primera pregunta sea negativa, tendrá que pasar a la siguiente y la máxima puntuación que podrá obtener tras ese No será de un 80% como

queda reflejado en la flecha correspondiente. Así de nuevo se plantea una pregunta que si es contestada afirmativamente "anulará" a las siguientes ya que no será necesario responderlas.

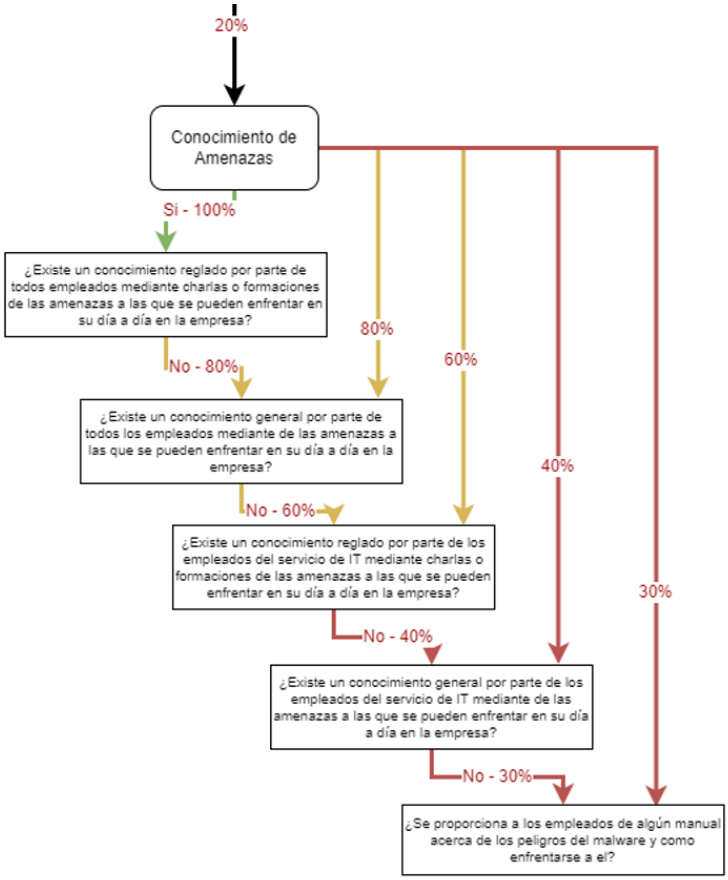


Ilustración 25: Conocimiento de Amenazas. Árbol de decisión.

Indicar, que los colores que muestras las flechas representan lo siguiente:

- El camino óptimo es verde,
- El camino básico medio es amarillo
- El camino escaso es rojo.

Hay que destacar que en cada una de las líneas tenemos el peso del control frente al 100% del subapartado.

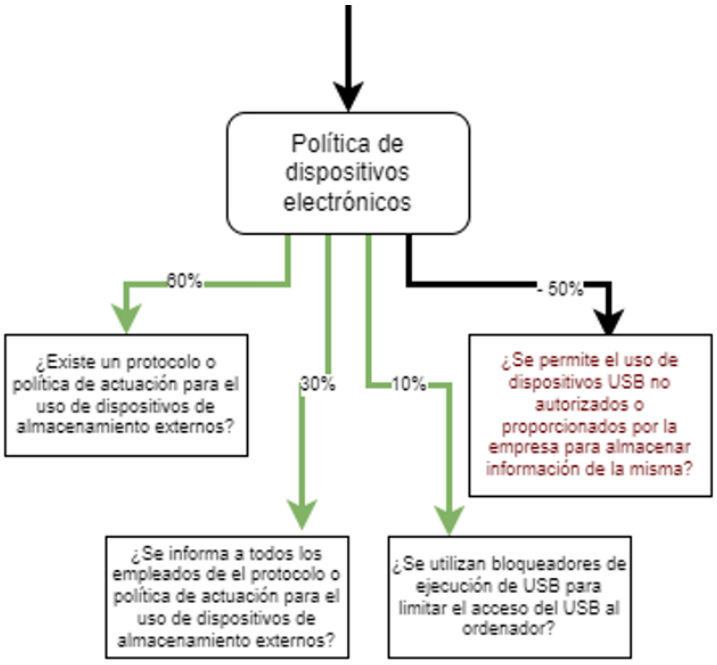


Ilustración 26: Política de dispositivos electrónicos. Árbol de decisión

Por último, podemos observar que en la Ilustración 26: Política de dispositivos electrónicos. Árbol de decisión aparece una línea en negro con un porcentaje en negativo. Esta hará referencia a la existencia de algunos controles cuyas preguntas en vez de sumar, restan ya que son acciones que no son adecuadas dentro del mundo de la ciberseguridad.

Esta ayuda visual nos proporcionará un complemento al Framework para indicarle al usuario que lo utilice el significado de sus respuestas. En caso de que exista una pregunta negativa dentro de las opciones, se visualizará de la siguiente manera.

4. Evaluación

Una vez definido el Framework es necesario que se realice una pequeña crítica constructiva del mismo, por lo que hemos proporcionado el Framework unido a una serie de preguntas a personal especializado en ciberseguridad de la empresa Seidor para que realice una evaluación sincera del diseño de la herramienta.

La muestra de población a la que hemos ofrecido este documento para que realice su evaluación, es una muestra pequeña, ya que se ha proporcionado solo al equipo de ciberseguridad de Seidor como hemos nombrado, en específico a la división de Seguridad de la información. Este equipo está dividido en dos secciones, la sección técnica donde se realizar tareas como Hacking ético o gestión de incidentes y la sección de seguridad de la información que abarca tareas como auditorias internas de seguridad, revisiones de la ISO y de procedimientos asociados. Hemos eliminado a los consultores Junior puesto que aún continúan en procesos de formación y comerciales ya que considerábamos que su conocimiento sobre las normas y demás procedimientos no era lo suficientemente extenso. La selección nos ha dejado una población de seis personas con conocimientos adecuados para poder hacer la evaluación.

Debido a que la evaluación se proporcionó en Agosto, periodo donde muchos trabajadores disfrutan de sus vacaciones, al final obtuvimos cuatro respuestas. Destacar que los perfiles que respondieron a la evaluación son los siguientes:

- Cybersecurity Service Delivery Manager
- Cybersecurity Auditor
- Cybersecurity Presales Specialist
- Consultor Senior en ciberseguridad

Esta evaluación constará de dos partes, la primera una batería sencilla de preguntas que pueden ser respondidas escogiendo de entre las opciones propuestas (Excelente, Bueno, Suficiente y Deficiente). La segunda parte constará de un único apartado en el que se le indica a la persona que anote cualquier observación sobre la evaluación del Framework o alguna propuesta de mejora.

Las preguntas de la primera parte son las siguientes:

I. ¿Cuál es tu opinión al respecto del diseño del Framework en general?
II. ¿Crees que los apartados son adecuados para el tema que trata (Ransomware)?

III. ¿consideras que el lenguaje utilizado es comprensible para que cualquier organización pueda utilizarlo?
IV. ¿Consideras complicada su utilización?
V. ¿Es útil (en tu opinión) que proporcione feedback en forma de Recomendaciones en aquellos controles que no cumplan?

Cada una de estas preguntas cubren un aspecto evaluable del Framework fundamental para su futura utilización en el mundo de la empresa.

Se va a entregar utilizando la herramienta de Google: Google Forms, para hacerlo de una manera dinámica y poder recoger las respuestas de manera clara. En la ilustración 27 podemos ver la apariencia del formulario de evaluación que se les proporcionará a los usuarios junto al Framework para que realicen la evaluación.

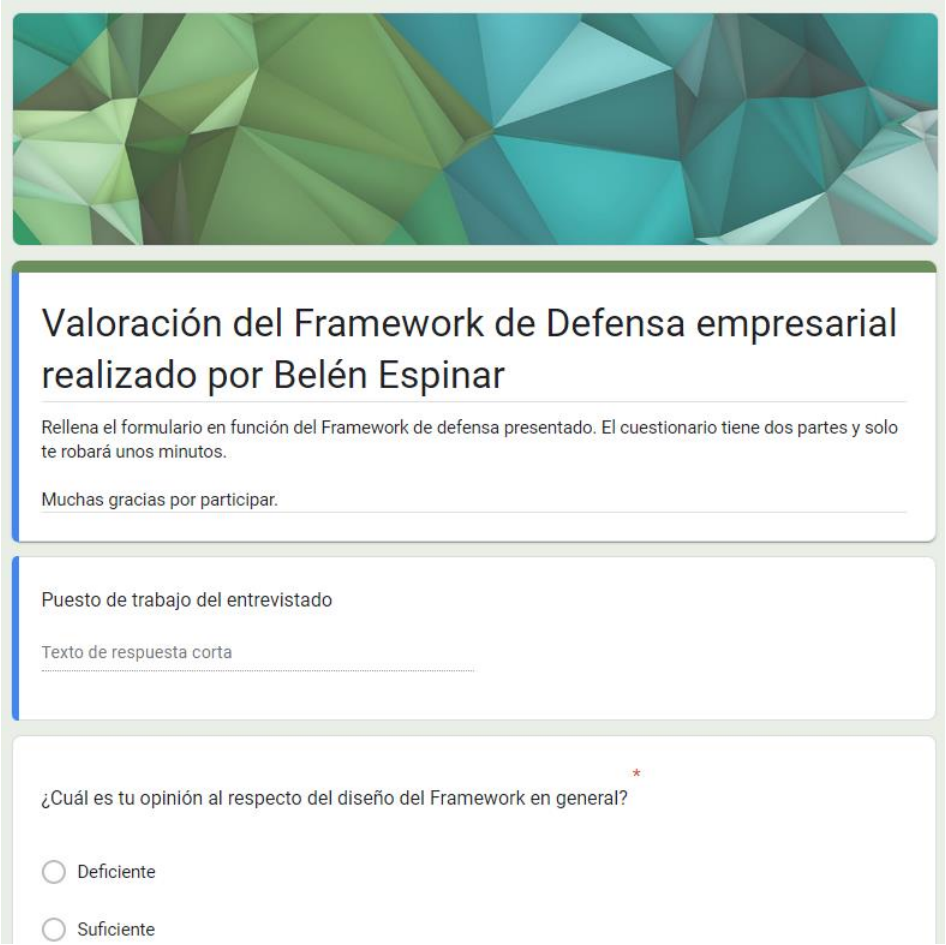


Ilustración 27: Formulario de evaluación del Framework

Los resultados obtenidos fueron los siguientes:

¿Cuál es tu opinión al respecto del diseño del Framework en general?

3 respuestas

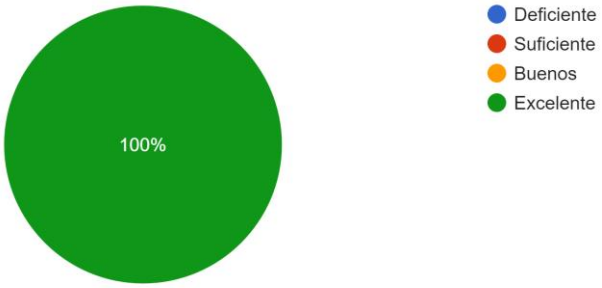


Ilustración 28: Respuesta a la pregunta de evaluación 1

¿Crees que los apartados son adecuados para el tema que trata (Ransomware)?

3 respuestas

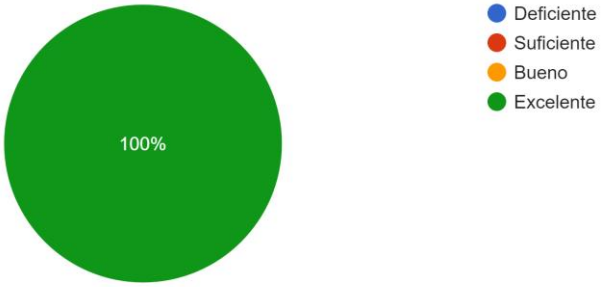


Ilustración 29: Respuesta a la pregunta de la evaluación 2.

¿Consideras que el lenguaje utilizado es comprensible para que cualquier organización pueda utilizarlo?

3 respuestas

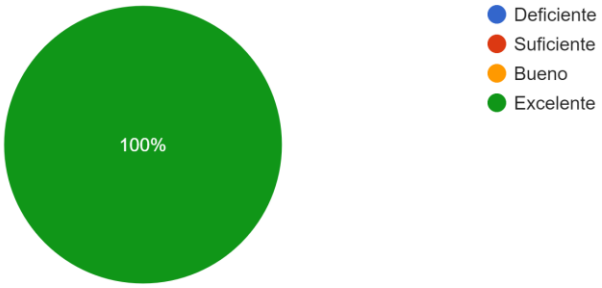


Ilustración 30: Respuesta a la pregunta de la evaluación 3.

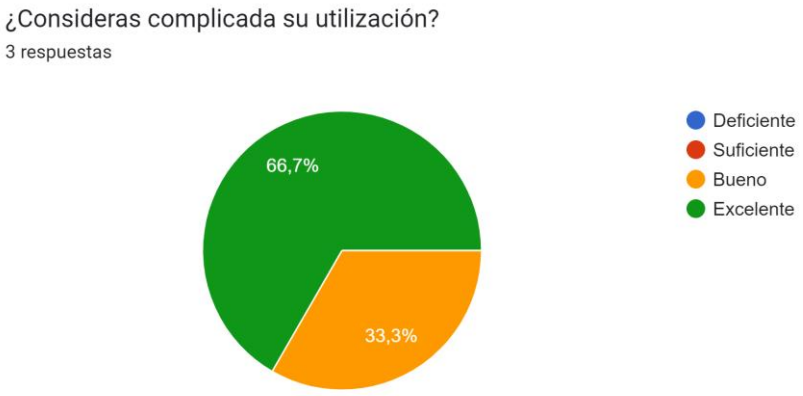


Ilustración 31: Respuesta a la pregunta de la evaluación 4.

Ilustración 32: Respuesta a la pregunta de la evaluación 5.

La respuesta a la encuesta por parte de los entrevistados valora positivamente el trabajo realizar viendo una utilidad práctica del Framework en un contexto de explotación y uso real orientado a mejorar la protección existente en una empresa frente al Ransomware. Las respuestas reflejan que los usuarios consideran que es una herramienta que podría ser fácilmente utilizada en el ecosistema Seidor para futuros proyectos o en otras consultoras que se dediquen a la misma rama.

La segunda parte de la evaluación, como hemos comentado con anterioridad, han sido las observaciones y propuestas de mejora, paso a citarlas a continuación:

- *"Considero un formulario apropiado en todas sus facetas. Clarificador, si ser extenso. Y el resultado que proporciona es de una ayuda inestimable para cualquier*

empresa interesada en conocer el estado de su nivel de protección frente a la defensa de posibles vulnerabilidades."

- *"Como punto de mejora incluiría un gráfico o mapa de calor por cada apartado para ver la situación inicial de la organización."*
- *"El documento es muy completo cubriendo áreas que son relevantes a lo largo de todo el proceso de prevención y gestión de un Ransomware. Al añadir recomendaciones a seguir en el caso de los puntos del Framework que no se cumplen se ayuda al usuario a mejorar la postura de seguridad frente a esta amenaza."*
- *"Me parece muy positivo el hecho de que el documento no tenga un formato rígido y que se pueda adaptar a las realidades presentes o futuras que puedan aparecer en el entorno de los Ransomware."*
- *"El Framework es además aplicable de forma general a los procesos y técnicas implantadas en una empresa o proceso para protegerse de amenazas en general."*
- *"Quizás sería interesante asociar un coste a cada uno de los porcentajes, en función de lo que perderían si llegasen a sufrir un ataque"*

Las observaciones han sido útiles, constructivas y aportan sugerencias de interés para mejorar el cuestionario de cara al futuro, las sugerencias, como introducir un diagrama en el que se pueda ver en qué posición se encuentra la empresa, son variables para tener en cuenta para una segunda versión de la herramienta. Otras sin embargo, se han podido introducir en la versión que presentamos en este documento. Me gustaría destacar un comentario en concreto que se ha utilizado para mejorar la herramienta, consistía en eliminar una de las preguntas por la dificultad del empresario de poder llevar a cabo la opción que solicita. El comentario (que no hemos incluido en los anteriores) es el siguiente:

- *"¿Se podría eliminar la cuestión 1.1.4? es muy complicado poder implantar eso en las empresas."*

La pregunta en conflicto fue la siguiente: *1.1.4. En situaciones de teletrabajo ¿Utiliza el trabajador una conexión a internet que le proporciona la empresa?*, la sugerencia era eliminarla porque, aunque sea interesante que los trabajadores de una empresa solo utilizaran una red proporcionada por la organización para su día a día laboral, es realmente complicado y muy costoso poder proporcionar a todos los empleados en teletrabajo una red independiente a cuenta de la organización, tanto si hablamos de empresas pequeñas que aunque tengan pocos trabajadores tengan un

presupuesto apretado, como empresas grandes con miles de empleados. Es prácticamente imposible proporcionar a todas ellas internet de manera independiente a su red doméstica. Aunque algunas normas indiquen que lo ideal sería esta situación, es demasiado costoso en la actualidad, por lo que es casi imposible que se cumpla este control.

Este ejemplo de cambio gracias a las sugerencias de los expertos es el tipo de ideas que queremos recolectar con la evaluación del Framework. Por lo que a pesar de que el colectivo entrevistado ha sido reducido, la información recolectada ha sido de gran valor.

5. Conclusiones

Para finalizar, es momento de hacer una recapitulación sobre la herramienta que hemos creado y que hemos conseguido. Al inicio de este documento exponíamos el porqué es necesaria en la situación actual una herramienta unificada, el objetivo principal de nuestra herramienta era:

- Generar una guía para evaluar la situación actual de una empresa con respecto a la defensa contra el Ransomware.

Este objetivo ha sido cumplido ya que hemos creado un Framework sólido de evaluación de la seguridad de una empresa (independientemente de su tamaño) que ayudará a las organizaciones a entender mediante una puntuación basada en las respuestas a nuestras preguntas, en que punto están con respecto a la seguridad frente a un Ransomware. Por ello, podremos ofrecerles una visión general y específica de su situación.

Si hablamos de los objetivos específicos que exponíamos seguidamente, establecimos cinco, los cuales además de recordar explicaremos como se han ido cumpliendo, especificando que partes del Framework cumplen con que objetivo:

- *Proteger la información de los clientes y usuarios de estas empresas.* En general todo el Framework está orientado a proteger la información de los clientes y usuarios de la organización entrevistada, en cada fase se pone en peligro esta información ya que el objetivo final de un ataque de Ransomware es el secuestro de datos. Por ello cada uno de los apartados cumple con este punto. Si tuviéramos que concretar y dar un capítulo especial hablaríamos del punto 4.2 en el que hablamos de la gestión de las copias de seguridad donde se guardaría la información de clientes y usuarios.
- *Proteger la información corporativa.* Para proteger la información corporativa hemos de centrarnos en el último apartado, en concreto en el 4.2 donde habla de las copias de seguridad donde guardaría la información de la organización. A pesar de que como explicábamos en el punto anterior durante todo el proceso se trata de proteger la información, en concreto ese punto sería el más referido.
- *Concienciar a los empleados y usuarios de la existencia de amenazas y los medios actuales para combatirlas.* Dentro del apartado de “Despliegue y

explotación" todo el apartado esta inclinado a cumplir con este objetivo ofreciendo: Ejercicios de concienciación y formaciones para cumplir con la concienciación de los empleados de forma que cubriremos este punto.

- *Impedir el acceso a los ciberdelincuentes a la información.* Este punto lo cumplimos con las medidas y recomendaciones que se ofrecen a la organización para proteger y aumentar la seguridad de sus defensas frente un ataque de Ransomware.
- *Impulsar buenas prácticas en la gestión de recursos de seguridad.* Como en el punto anterior, las recomendaciones cubrirían este objetivo, ya que en todas ellas se impulsan las buenas prácticas. Por exponer un ejemplo podemos ir a la Recomendación asociada al punto 4.2.7 "Realizar copias de seguridad con frecuencia diaria o la que determine el RPO." En la que se fomenta no solo a realizar copias de seguridad sino además a determinar un RPO, un punto fundamental para cada una de las empresas que deseen tener una buena conciencia de su seguridad de la información.

Como podemos observar los objetivos se han cubierto en el desarrollo de la herramienta. Sin embargo, no hemos creado un Framework estático sin posibilidad de modificación. Gracias a la ayuda inestimable de los comentarios de los profesionales que han participado en la evaluación del Framework, hemos extraído una serie de mejoras a implementar en las siguientes versiones del Framework. Entre ellas:

- La posibilidad de introducir una correlación entre el nivel de defensa y la posible pérdida monetaria para la empresa en caso de ser víctimas de Ransomware. De esta manera al especificar el coste de este ataque, podremos valorar si la solución de implantar todas las medidas y recomendaciones propuestas es rentable o si solo algunas de ellas lo son. De esta manera la organización puede valorar que puntos puede permitirse cubrir para mejorar la seguridad.

Este punto de rentabilizar la mejora en función de la pérdida será muy interesante para plantear a empresas que no tengan un presupuesto grande, pueden priorizar algunas mejoras como concienciar a los empleados frente a segmentar la red, que en principio puede ser más costoso.

Para finalizar, recalcar la idea de que esta herramienta pueda estar en constante evolución, pero no solo serán expertos los que ayuden a mejorar el Framework, los

propios usuarios en las entrevistas nos ayudarán a comprender las partes que necesitan mejorar, que puntos son adecuados y cuales necesitan una revisión. La mejora como en un buen método científico ha de ser siempre constante y con una lógica que la soporte.

Con este proyecto aprovecho para poder plasmar no solo todo el conocimiento adquirido en la rama de Sistemas de información que me impulso en decantarme por la parte de la normativa y la ciberseguridad, sino además el de la experiencia profesional que he recabado en la empresa donde actualmente estoy empleada: SEIDOR SOLUTIONS. Además, creo que es muy importante resaltar la importancia de la protección de la información, uno de los activos más valiosos en una organización, que muchas veces se asume segura por profesionales de la informática, y es necesaria para mantener la integridad, confidencialidad y disponibilidad de los activos y servicios de la organización.

Glosario

A continuación, detallaremos la terminología que utilizaremos durante el documento:

- **Usuarios**: Empleados o responsables que serán los encargados de proporcionar la información. Serán las personas dentro de la empresa que interactuarán con el Framework propuesto.
- **Organización/Empresa**: Ambas palabras serán utilizadas para definir la empresa destino del Framework, incluyendo a instituciones del ámbito público o privado y de mediano o gran tamaño.
- **Framework**: Esquema o marco de trabajo que nos ofrecerá una estructura para elaborar un proyecto con objetivos específicos, una plantilla que sirve como punto de partida para la organización para desarrollar en este caso concreto la defensa ante el Ransomware.
- **INCIBE**: Instituto nacional de ciber seguridad.
- **CCN**: Centro nacional de criptología.
- **Malware** (software malicioso): Hace referencia a todo tipo de software o código que se utiliza para realizar acciones hostiles o intrusivas en el dispositivo de la persona que los recibe,
- **Shoulder surfing:** Se refiere al tipo de ingeniería social donde los ciberdelincuentes espían de manera presencial a sus víctimas. En lugares como el metro o una cafetería, cuando un usuario accede a sus cuentas personales los ciberdelincuentes roban información cuando las víctimas introducen sus contraseñas.
- **Phishing**: Parte de los métodos de ingeniería social en los cuales los ciberdelincuentes utilizan un email como cebo para realizar actividades delictivas como: robo de información, cifrado de datos, instalación y propagación de malware,
- **Ingeniería social:** Determinamos ingeniería social a todas aquellas técnicas que realizan los ciberdelincuentes con el objetivo de engañar a las víctimas para conseguir un beneficio.
- **Ciclo de vida**: Todas aquellas etapas por las que tiene que pasar un ataque para lanzarse. Desde el periodo en que se estudia el punto de entrada en un dispositivo/organización hasta el momento en que finaliza su actuación maliciosa.

- **Servicio de IT**: Conjunto de tecnología y persona o personas encargadas dentro de una empresa de proporcionar las aplicaciones y servicios informáticos que sustentas las actividades de negocio.
- **RPO**: RPO (Recovery Point Objective) RPO se refiere al volumen de datos en riesgo de pérdida que la organización considera tolerable.

Referencias

[1]. ©2022 AT&T Intellectual Property. “¿Quienes somos?”. https://www.att.com (revisado el 27 de Mayo de 2022)

[2]. “The Deep Web”(2015) Capitain Crunch and his toy whistle[Imagen] The Deep Web. https://sites.psu.edu/thedeepweb/2015/09/17/captain-crunch-and-his-toy-whistle/

[3]. Del Corral, Pedro (08 de Noviembre de 2020) “¿Cómo era ser un hacker en los 90? Así se reían de El Pentágono”. La Razón. https://www.larazon.es/tecnologia/20201108/twqwge32nnae7gf23skhmgeiw4.html (revisado el 27 de Mayo de 2022)

[4]. INCIBE (2022). “Hacker vs Ciberdelincuente”. https://www.incibe.es/aprendeciberseguridad/hacker-vs-ciberdelincuente (revisado el 20 de Julio de 2022)

[5]. “Black Hat Gray Hat White Hat”[Imagen] Hackerscenter. https://www.hackerscenter.com/wp-content/uploads/2022/03/black-hat-gray-hat-white-hat.png

[6]. © 2022 AO Kaspersky Lab. All Rights Reserved.(2022) “Black hat, White hat, and Gray hat hackers – Definition and Explanation”. Kaspersky. https://www.kaspersky.com/resource-center/definitions/hacker-hat-types (revisado el 17 de junio de 2022)

[7]. © Banco Bilbao Vizcaya Argentaria, S.A. 2022 (22 de Mayo de 2022) ”El Teletrabajo se multiplicó por siete en España en 2020” https://www.bbva.com/es/el-teletrabajo-se-multiplico-por-siete-en-espana-en-2020/ (revisado el 14 de Agosto de 2022)

[8]. Jessica Keyes, "Bring Your Own Devices (BYOD) Survival Guide, Ed. Auerbach Publications , 451 páginas, ISBN: 978-1466565036, Abril 2016. (revisado el 17 de julio de 2022)

[9]. INCIBE (2017) “Guía ciberseguridad en el trabajo” [Infografía] Incibe.

[10]. INCIBE (2020) “Balance de Ciberseguridad 2019” [Infografía]. Incibe. https://www.incibe.es/sites/default/files/paginas/que-hacemos/balance_ciberseguridad_2019_incibe.pdf (revisado el 11 de agosto de 2022)

[11]. INCIBE (2021) “Balance de Ciberseguridad 2020” [Infografía]. Incibe. https://www.incibe.es/sites/default/files/paginas/que-

hacemos/balance_ciberseguridad_2020_incibe.pdf (revisado el 11 de agosto de 2022)

[12]. INCIBE (2022) “Balance de Ciberseguridad 2021” [Infografía]. Incibe. https://www.incibe.es/sites/default/files/paginas/que-hacemos/balance_ciberseguridad_2021_incibe.pdf (revisado el 11 de agosto de 2022)

[13]. OSI. Oficina de seguridad del internauta. (2016) “El ransomware, cada vez más peligroso. Protégete”. Blog OSI. https://www.osi.es/es/actualidad/blog/2016/05/31/el-ransomware-cada-vez-mas-peligroso-protegete (revisado el 17 de junio de 2022)

[14]. Sophos. (Año) “Ransomware”[Infografía] URL

[15]. © 2022 Oracle “¿Qué es el Malware?” ORACLE. https://www.oracle.com/es/database/security/que-es-el-malware.html (revisado el 20 de Julio de 2022)

[16]. Barker, William C; Fisher, William; Scarfone, Karen; Souppaya, Murugiah (2022) “Gestión de riesgo de ransomware: un perfil de marco de ciberseguridad”. NIST https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8374.spa.pdf (revisado el 26 de julio de 2022)

[17]. International Organization for Standardization (2022) ISO 27002:2022 (revisado el 22 de julio de 2022)

[18]. CCN-CERT(Abril 2021) “Gestión de incidentes de Ransomware CCN-CERT BP/21”[Infografía]. CCN-CERT. https://www.ccn-cert.cni.es/informes/informes-de-buenas-practicas-bp/5864-ccn-cert-bp-21-gestion-de-incidentes-de-ransomware/file.html (revisado el 7 de agosto de 2022)

[19]. CyberSecure (2021) “Ransomware 2021 en el panorama de amenazas” [Imagen] Boletines de Seguridad. https://portal.cci-entel.cl/Threat_Intelligence/Boletines/778/ (revisado el 26 de julio de 2022)

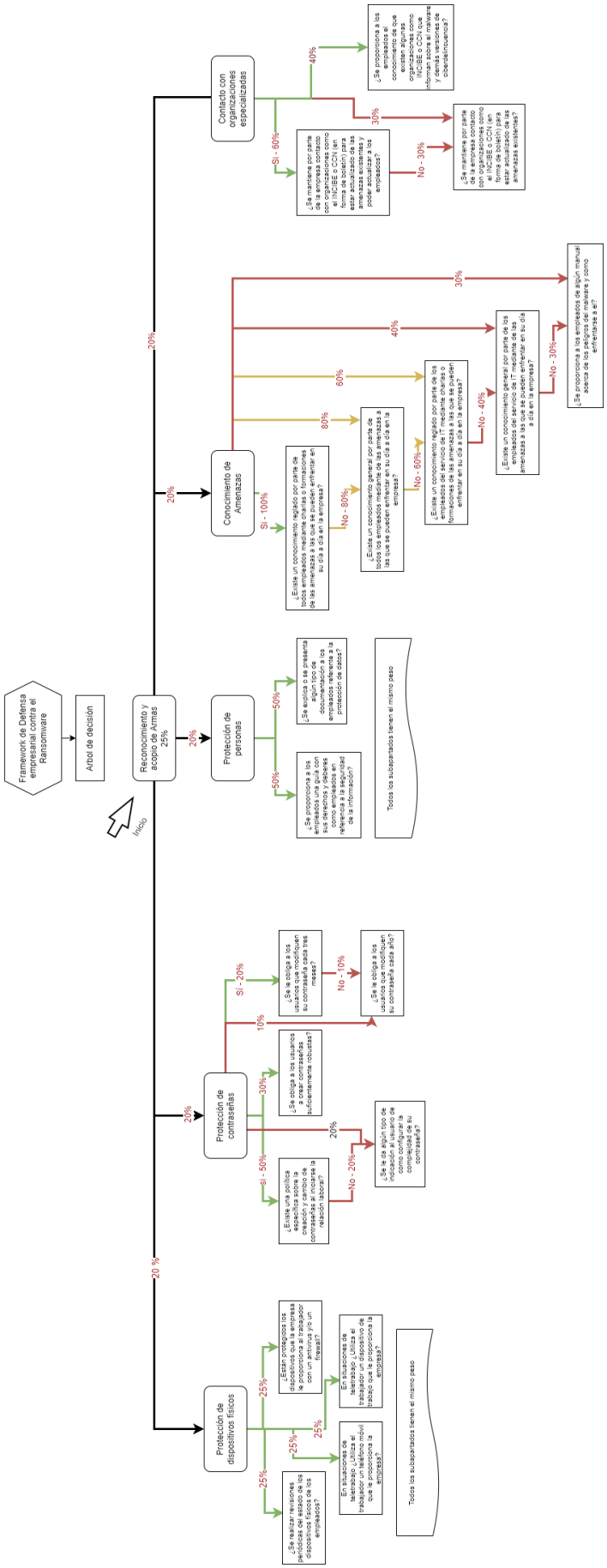
[20]. INCIBE (Enero 2020) “Las siete fases de un ciberataque ¿las conoces?”, https://www.incibe.es/protege-tu-empresa/blog/las-7-fases-ciberataque-las-conoces (revisado por última vez el 01 de septiembre de 2022)

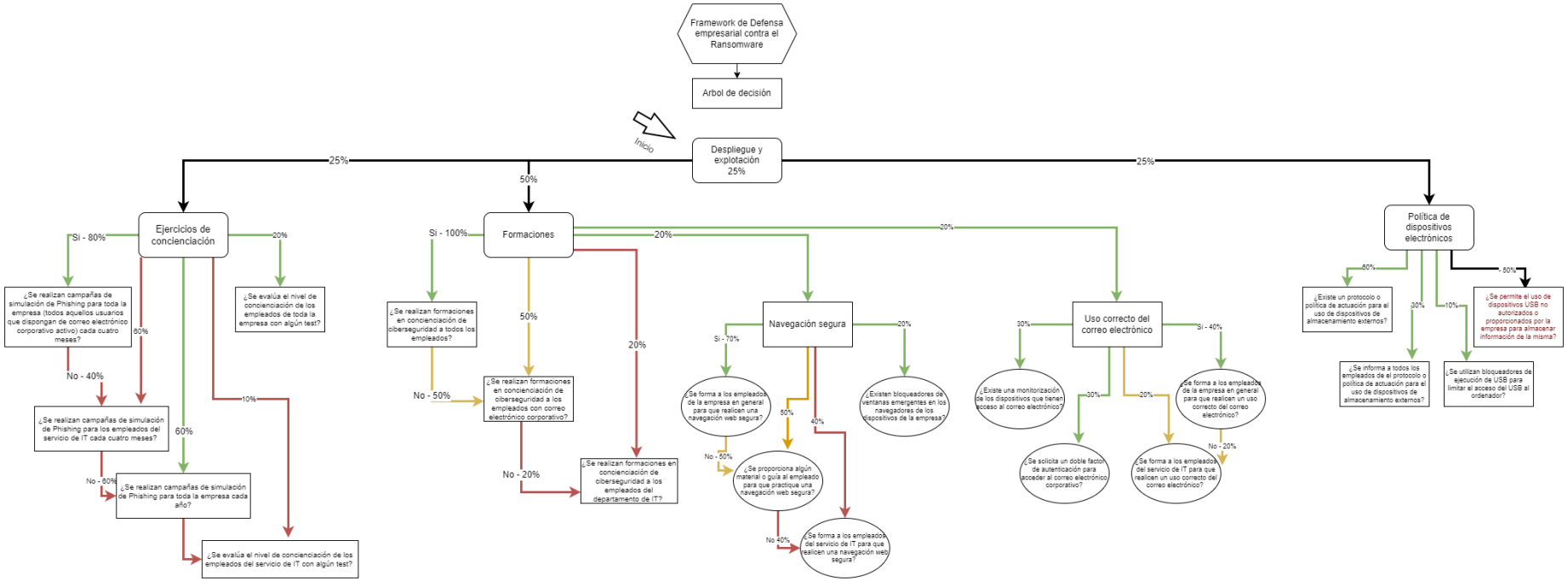
Anexo I: Árbol de decisión y puntuación de los controles

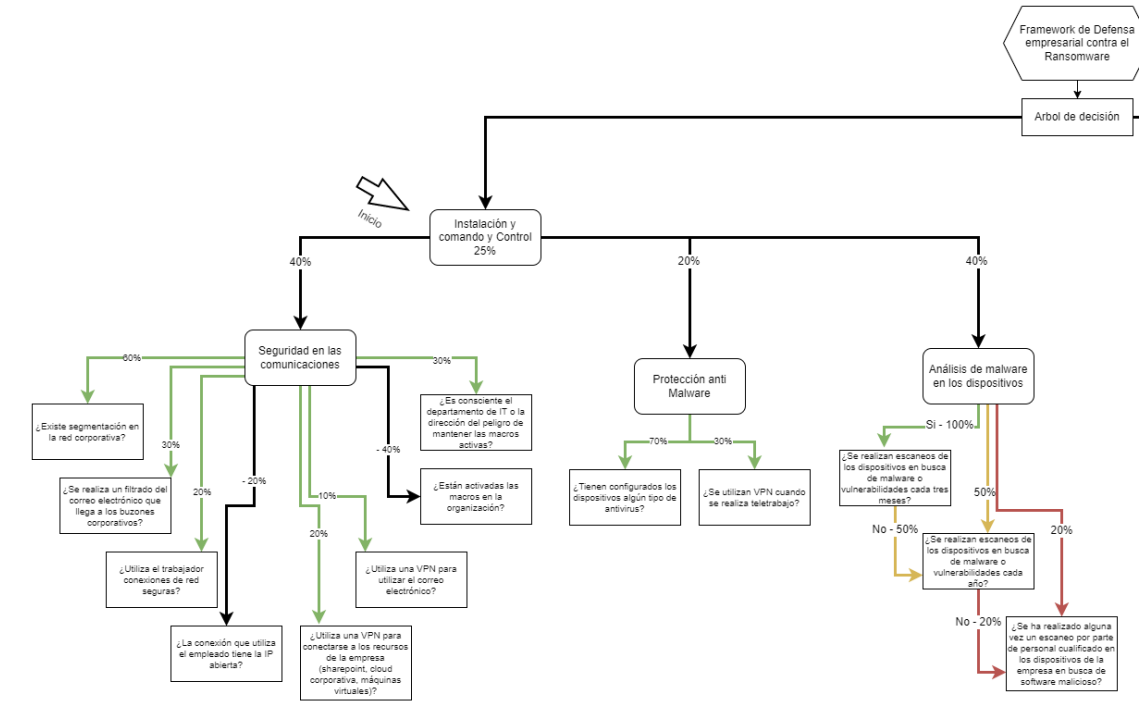
Vamos ilustrar en este Anexo I, el árbol de decisión de cada uno de los apartados, que nos indicará los caminos óptimos como hemos especificado. Además, seguidamente mostraremos la tabla completa de las puntuaciones y porcentajes de todos los controles del Framework.

Los diagramas de los arbole de decisión están ordenados en función de los apartados que hemos especificado en el apartado 3:

- **Fases de reconocimiento** y **acopio de armas**:
  - Protección de dispositivos físicos.
  - Protección de contraseñas.
  - Protección de personas.
  - Conocimiento de amenazas.
  - Contacto con organizaciones especializadas.
- **Fases de despliegue y explotación**:
  - Ejercicios de concienciación.
  - Formaciones.
    - Navegación segura
    - Uso correcto del correo electrónico
  - Política de dispositivos externos de almacenamiento
- **Fases de instalación** y **comando y control**:
  - Seguridad en las Comunicaciones.
    - Fragmentación de la red.
    - Filtración de correo electrónico
    - Bloqueo de macros
  - Protección anti malware
  - Análisis de malware en los dispositivos.
- **Actuación en el objetivo:**
  - Plan de contingencia.
  - Copias de seguridad.


Framework de Defensa empresarial contra el Ransomware
Arbol de decisión
Reconocimiento y acopio de Armas 25%
Protección de personas
Conocimiento de Amenazas
Contacto con organizaciones especializadas
Protección de contraseñas
Protección de dispositivos físicos
Inicio
20%
20%
20%
20 %
50%
50%
¿Se explica o se presenta algún tipo de documentación a los empleados sobre la protección de datos?
¿Se proporciona a los empleados una guía con sus derechos y deberes como empleados en referencia a la seguridad de la información?
Todos los subapartados tienen el mismo peso
SI - 100%
No - 80%
¿Existe un conocimiento regalado por parte de todos empleados mediante charlas o formaciones de las amenazas a las que pueden enfrentar en su día a día en la empresa?
¿Existe un conocimiento general por parte de todos los empleados sobre las amenazas a las que se pueden enfrentar en su día a día en la empresa?
No - 60%
¿Existe un conocimiento regalado por parte de los empleados del servicio de IT mediante charlas o formaciones de las amenazas a las que se pueden enfrentar en su día a día en la empresa?
No - 40%
¿Existe un conocimiento general por parte de los empleados del servicio de IT mediante de las amenazas a las que se pueden enfrentar en su día a día en la empresa?
No - 30%
¿Se proporciona a los empleados de algún manual acerca de los peligros del malware y como evitarlos y el?
SI - 60%
¿Se mantiene por parte de la empresa contacto con organizaciones como el INCIBE o CCN (en España) para estar actualizado de las amenazas existentes y poder actualizar a los empleados?
No - 30%
¿Se mantiene por parte de la empresa contacto con organizaciones como el INCIBE o CCN (en España) para estar actualizado de las amenazas existentes?
¿Se proporciona a los empleados el conocimiento de que existen diversas organizaciones como INCIBE o CCN que informan sobre malware y demás versiones de ciberdelincuencia?
SI - 20%
No - 10%
¿Se le obliga a los usuarios que modifiquen su contraseña cada tres meses?
¿Se le obliga a los usuarios que modifiquen su contraseña cada año?
SI - 50%
No - 20%
¿Existe una política relacionada con la creación y cambio de contraseñas al iniciarse la relación laboral?
¿Se le da algún tipo de indicación a la hora de como configurar la complejidad de su contraseña?
¿Se realizan revisiones periódicas del estado de los dispositivos físicos de los empleados?
En trabajos de teletrabajo ¿Utiliza el trabajador un teléfono móvil que le proporciona la empresa?
En trabajos de teletrabajo ¿Utiliza el trabajador un dispositivo de trabajo que le proporciona la empresa?
¿Están protegidos los dispositivos que la empresa le proporciona al trabajador con un antivirus y/o un firewall?
Todos los subapartados tienen el mismo peso


Framework de Defensa empresarial contra el Ransomware
Arbol de decisión
Inicio
Despliegue y explotación 25%
25%
50%
25%
Ejercicios de concienciación
Si - 80%
20%
¿Se realizan campañas de simulación de Phishing para toda la empresa (todos aquellos usuarios que dispongan de correo electrónico corporativo activo) cada cuatro meses?
¿Se evalúa el nivel de concienciación de los empleados de toda la empresa con algún test?
60%
No - 40%
¿Se realizan campañas de simulación de Phishing para los empleados del servicio de IT cada cuatro meses?
10%
60%
No - 60%
¿Se realizan campañas de simulación de Phishing para toda la empresa cada año?
¿Se evalúa el nivel de concienciación de los empleados del servicio de IT con algún test?
Formaciones
Si - 100%
20%
20%
¿Se realizan formaciones en concienciación de ciberseguridad a todos los empleados?
50%
20%
No - 50%
¿Se realizan formaciones en concienciación de ciberseguridad a los empleados con correo electrónico corporativo?
No - 20%
¿Se realizan formaciones en concienciación de ciberseguridad a los empleados del departamento de IT?
Navegación segura
Si - 70%
20%
¿Se forma a los empleados de la empresa en general para que realicen una navegación web segura?
¿Existen bloqueadores de ventanas emergentes en los navegadores de los dispositivos de la empresa?
50%
40%
No - 50%
¿Se proporciona algún material o guía al empleado para que practique una navegación web segura?
No 40%
¿Se forma a los empleados del servicio de IT para que realicen una navegación web segura?
Uso correcto del correo electrónico
30%
Si - 40%
¿Existe una monitorización de los dispositivos que tienen acceso al correo electrónico?
¿Se forma a los empleados de la empresa en general para que realicen un uso correcto del correo electrónico?
30%
20%
No - 20%
¿Se solicita un doble factor de autenticación para acceder al correo electrónico corporativo?
¿Se forma a los empleados del servicio de IT para que realicen un uso correcto del correo electrónico?
Política de dispositivos electrónicos
60%
30%
10%
¿Existe un protocolo o política de actuación para el uso de dispositivos de almacenamiento externos?
¿Se informa a todos los empleados de el protocolo o política de actuación para el uso de dispositivos de almacenamiento externos?
¿Se utilizan bloqueadores de ejecución de USB para limitar el acceso del USB al ordenador?
¿Se permite el uso de dispositivos USB no autorizados o proporcionados por la empresa para almacenar información de la misma?


Framework de Defensa empresarial contra el Ransomware
Arbol de decisión
Inicio
Instalación y comando y Control 25%
40%
20%
40%
Seguridad en las comunicaciones
Protección anti Malware
Análisis de malware en los dispositivos
60%
30%
¿Existe segmentación en la red corporativa?
¿Es consciente el departamento de IT o la dirección del peligro de mantener las macros activas?
30%
20%
- 20%
10%
- 40%
¿Se realiza un filtrado del correo electrónico que llega a los buzones corporativos?
¿Están activadas las macros en la organización?
¿Utiliza el trabajador conexiones de red seguras?
20%
¿Utiliza una VPN para utilizar el correo electrónico?
¿La conexión que utiliza el empleado tiene la IP abierta?
¿Utiliza una VPN para conectarse a los recursos de la empresa (sharepoint, cloud corporativa, máquinas virtuales)?
70%
30%
¿Tienen configurados los dispositivos algún tipo de antivirus?
¿Se utilizan VPN cuando se realiza teletrabajo?
Si - 100%
50%
20%
¿Se realizan escaneos de los dispositivos en busca de malware o vulnerabilidades cada tres meses?
No - 50%
¿Se realizan escaneos de los dispositivos en busca de malware o vulnerabilidades cada año?
No - 20%
¿Se ha realizado alguna vez un escaneo por parte de personal cualificado en los dispositivos de la empresa en busca de software malicioso?

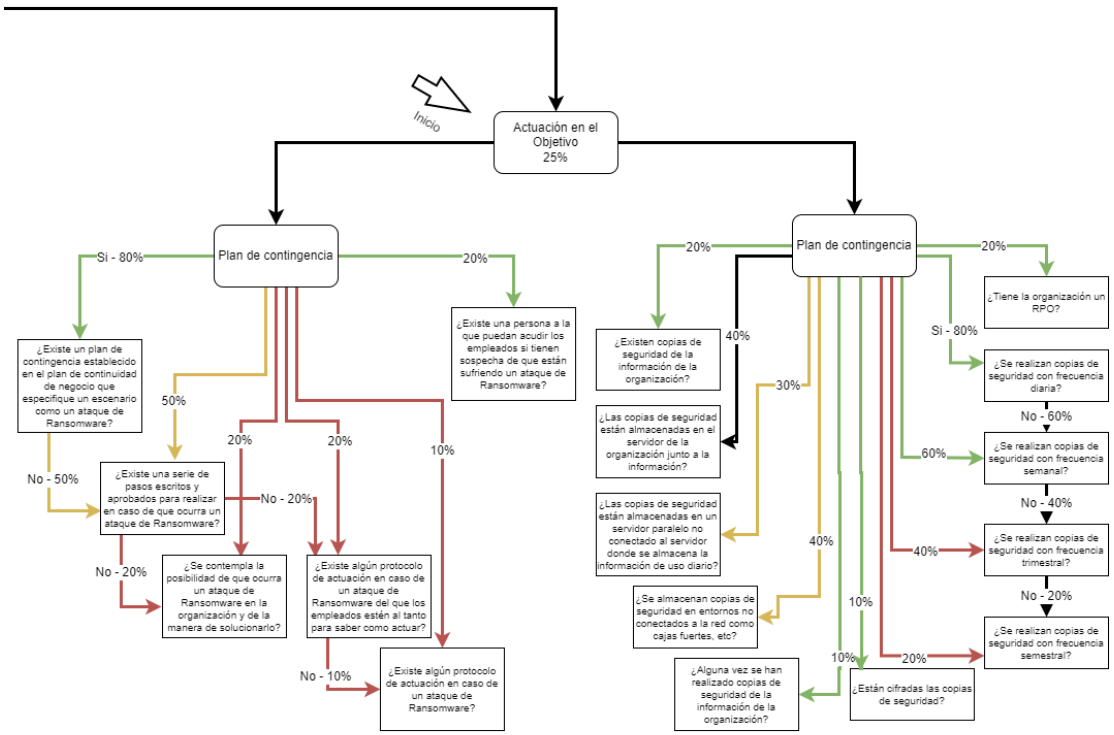

Inicio
Actuación en el Objetivo 25%
Plan de contingencia
Plan de contingencia
Si - 80%
20%
¿Existe un plan de contingencia establecido en el plan de continuidad de negocio que especifique un escenario como un ataque de Ransomware?
¿Existe una persona a la que puedan acudir los empleados si tienen sospecha de que están sufriendo un ataque de Ransomware?
50%
20%
20%
10%
No - 50%
¿Existe una serie de pasos escritos y aprobados para realizar en caso de que ocurra un ataque de Ransomware?
No - 20%
No - 20%
¿Se contempla la posibilidad de que ocurra un ataque de Ransomware en la organización y de la manera de solucionarlo?
¿Existe algún protocolo de actuación en caso de un ataque de Ransomware del que los empleados estén al tanto para saber como actuar?
No - 10%
¿Existe algún protocolo de actuación en caso de un ataque de Ransomware?
20%
40%
30%
40%
10%
10%
20%
¿Existen copias de seguridad de la información de la organización?
¿Las copias de seguridad están almacenadas en el servidor de la organización junto a la información?
¿Las copias de seguridad están almacenadas en un servidor paralelo no conectado al servidor donde se almacena la información de uso diario?
¿Se almacenan copias de seguridad en entornos no conectados a la red como cajas fuertes, etc?
¿Alguna vez se han realizado copias de seguridad de la información de la organización?
¿Están cifradas las copias de seguridad?
20%
Si - 80%
No - 60%
60%
No - 40%
40%
No - 20%
¿Tiene la organización un RPO?
¿Se realizan copias de seguridad con frecuencia diaria?
¿Se realizan copias de seguridad con frecuencia semanal?
¿Se realizan copias de seguridad con frecuencia trimestral?
¿Se realizan copias de seguridad con frecuencia semestral?

Tabla 4: Porcentajes de puntuación de los controles del Framework

Apartado	Pregunta	Valoración
1. Reconocimiento y Acopio de Armas		25%
1.1 Protección de dispositivos físicos		20%
1.1.1	¿Se realizar revisiones periódicas del estado de los dispositivos físicos de los empleados?	25%
1.1.2	En situaciones de teletrabajo, ¿utiliza el trabajador un teléfono móvil que le proporciona la empresa?	25%
1.1.3	En situaciones de teletrabajo, ¿utiliza el trabajador un dispositivo de trabajo que le proporciona la empresa?	25%
1.1.4	¿Están protegidos los dispositivos que la empresa le proporciona al trabajador con un antivirus y/o un firewall?	25%
1.2 Protección de contraseñas		20%
1.2.1	¿Existe una política específica sobre la creación y cambio de contraseñas al iniciarse la relación laboral?	50%
1.2.2	¿Se obliga a los usuarios a crear contraseñas suficientemente robustas? Robustez adecuada: 12 caracteres, mayúsculas, minúsculas, números y símbolos.	30%
1.2.3	¿Se exige a los usuarios que modifiquen su contraseña cada tres meses?	20%
1.2.4	¿Se exige a los usuarios que modifiquen su contraseña cada año?	10%
1.2.5	¿Se le da algún tipo de indicación al usuario de como configurar la complejidad de su contraseña?	20%
1.3 Protección de personas		20%
1.3.1	¿Se proporciona a los empleados una guía con sus derechos y deberes como empleados en referencia a la seguridad de la información?	50%
1.3.2	¿Se explica o se presenta algún tipo de documentación a los empleados referente a la protección de datos?	50%
1.4 Conocimiento de amenazas		20%
1.4.1	¿Existe un conocimiento reglado por parte de todos los empleados mediante charlas o formaciones de las amenazas a las que se pueden enfrentar en su día a día en la empresa?	100%

1.4.2	¿Existe un conocimiento general por parte de todos los empleados, de manera autodidacta, de las amenazas a las que se pueden enfrentar en su día a día en la empresa en materia de ciberseguridad?	80%
1.4.3	¿Existe un conocimiento reglado por parte de los empleados del servicio de IT mediante charlas o formaciones de las amenazas a las que se pueden enfrentar en su día a día en la empresa? (en caso de que la empresa disponga de este departamento)	60%
1.4.4	¿Existe un conocimiento general por parte de los empleados del servicio de IT mediante de las amenazas a las que se pueden enfrentar en su día a día en la empresa? (en caso de que la empresa disponga de este departamento)	40%
1.4.5	¿Se proporciona a los empleados algún manual acerca de los peligros del malware y como enfrentarse a el?	30%
1.5 Contacto con organizaciones especializadas		20%
1.5.1	¿Se mantiene por parte de la empresa contacto con organizaciones como el INCIBE o CCN (en forma de boletín) para estar actualizada de las amenazas existentes y poder actualizar a los empleados?	60%
1.5.2	¿Se mantiene por parte de la empresa contacto con organizaciones como el INCIBE o CCN (en forma de boletín) para estar actualizada de las amenazas existentes?	30%
1.5.3	¿Se proporciona a los empleados el conocimiento de que existen algunas organizaciones como INCIBE o CCN que informan sobre el malware y demás versiones de ciberdelincuencia?	40%
2. Despliegue y explotación		25%
2.1 Ejercicios de concienciación		25%
2.1.1	¿Se realizan campañas de simulación de Phishing para toda la empresa (todos aquellos usuarios que dispongan de correo electrónico corporativo activo) cada cuatro meses?	80%
2.1.2	¿Se realizan campañas de simulación de Phishing para toda la empresa cada año?	40%
2.1.3	¿Se realizan campañas de simulación de Phishing para los empleados del servicio de IT cada cuatro meses? (en caso de que la empresa disponga de este departamento)	60%

2.1.4	¿Se realizan campañas de simulación de Phishing para los empleados del servicio de IT cada año? (en caso de que la empresa disponga de este departamento)	30%
2.1.5	¿Se evalúa el nivel de concienciación de los empleados del servicio de IT con algún test? (en caso de que la empresa disponga de este departamento)	10%
2.1.6	¿Se evalúa el nivel de concienciación de los empleados de toda la empresa con algún test?	20%
2.2 Formaciones		50%
2.2.1	¿Se realizan formaciones en concienciación de ciberseguridad a todos los empleados?	100%
2.2.2	¿Se realizan formaciones en concienciación de ciberseguridad a los empleados con correo electrónico corporativo?	50%
2.2.3	¿Se realizan formaciones en concienciación de ciberseguridad a los empleados del departamento de IT? (en caso de que la empresa disponga de este departamento)	20%
2.2.4 Navegación segura		20%
2.2.4.1	¿Se proporciona algún material o guía al empleado para que practique una navegación web segura?	50%
2.2.4.2	¿Se forma a los empleados de la empresa en general para que realicen una navegación web segura?	70%
2.2.4.3	¿Se forma a los empleados del servicio de IT para que realicen una navegación web segura? (en caso de que la empresa disponga de este departamento)	40%
2.2.4.4	¿Existen bloqueadores de ventanas emergentes en los navegadores de los dispositivos de la empresa?	20%
2.2.5 Uso correcto del correo electrónico		20%
2.2.5.1	¿Existe una monitorización de los dispositivos que tienen acceso al correo electrónico?	30%
2.2.5.2	¿Se solicita un doble factor de autenticación para acceder al correo electrónico corporativo?	30%
2.2.5.3	¿Se forma a los empleados de la empresa en general para que realicen un uso correcto del correo electrónico?	40%
2.2.5.4	¿Se forma a los empleados del servicio de IT para que realicen un uso correcto del correo electrónico? (en caso de que la empresa disponga de este departamento)	20%

2.3 Política de dispositivos electrónicos		25%
2.3.1	¿Existe un protocolo o política de actuación para el uso de dispositivos de almacenamiento externos?	60%
2.3.2	¿Se informa a todos los empleados del protocolo o política de actuación para el uso de dispositivos de almacenamiento externos?	30%
2.3.3	¿Se permite el uso de dispositivos USB no autorizados o proporcionados por la empresa para almacenar información de la misma?	50%
2.3.4	¿Se utilizan bloqueadores de ejecución de USB para limitar el acceso del USB al ordenador?	10%
3. Instalación y Comando y control		25%
3.1. Seguridad en las comunicaciones		40%
3.1.1	¿Existe segmentación en la red corporativa?	60%
3.1.2	¿Se realiza un filtrado del correo electrónico que llega a los buzones corporativos?	30%
3.1.3	¿Están activadas las macros en la organización?	40%
3.1.4	¿Es consciente el departamento de IT o la dirección del peligro de mantener las macros activas?	30%
3.1.5	¿Utiliza el trabajador conexiones de red seguras?	20%
3.1.6	¿La conexión que utiliza el empleado tiene la IP abierta?	20%
3.1.7	¿Utiliza una VPN para conectarse a los recursos de la empresa (*sharepoint, cloud* corporativa, máquinas virtuales)?	20%
3.1.8	¿Utiliza una VPN para utilizar el correo electrónico?	10%
3.2 Protección anti malware		20%
3.2.1	¿Tienen configurados los dispositivos algún tipo de antivirus?	70%
3.2.2	¿Se utilizan VPN cuando se realiza teletrabajo?	30%
3.3 Análisis de malware en los dispositivos		40%
3.3.1	¿Se realizan escaneos de los dispositivos en busca de malware o vulnerabilidades cada tres meses?	100%
3.3.2	¿Se realizan escaneos de los dispositivos en busca de malware o vulnerabilidades cada año?	50%
3.3.3	¿Se ha realizado alguna vez un escaneo por parte de personal cualificado en los dispositivos de la empresa en busca de software malicioso?	20%
4. Actuación en el objetivo		25%
4.1 Plan de contingencia		40%

4.1.1	¿Existe un plan de contingencia establecido en el plan de continuidad de negocio que especifique un escenario como un ataque de Ransomware?	80%
4.1.2	¿Existe una serie de pasos escritos y aprobados para realizar en caso de que ocurra un ataque de Ransomware?	50%
4.1.3	¿Se contempla la posibilidad que ocurra un ataque de Ransomware en la organización y de la manera de solucionarlo?	20%
4.1.4	¿Existe algún protocolo de actuación en caso de un ataque de Ransomware del que los empleados estén al tanto para saber como actuar?	20%
4.1.5	¿Existe algún protocolo de actuación en caso de un ataque de Ransomware?	10%
4.1.6	¿Existe una persona a la que puedan acudir los empleados si tienen sospecha de que están sufriendo un ataque de Ransomware?	20%
4.2 Copias de seguridad		60%
4.2.1	¿Existen copias de seguridad de la información de la organización?	20%
4.2.2	¿Las copias de seguridad están almacenadas en el servidor de la organización junto a la información?	40%
4.2.3	¿Las copias de seguridad están almacenadas en un servidor paralelo no conectado al servidor donde se almacena la información de uso diario?	30%
4.2.4	¿Se almacenan copias de seguridad en entornos no conectados a la red como cajas fuertes, etc?	40%
4.2.5	¿Tiene la organización un RPO?	20%
4.2.6	¿Se realizan copias de seguridad con frecuencia diaria?	80%
4.2.7	¿Se realizan copias de seguridad con frecuencia semanal?	60%
4.2.8	¿Se realizan copias de seguridad con frecuencia trimestral?	40%
4.2.9	¿Se realizan copias de seguridad con frecuencia semestral?	20%
4.2.10	¿Alguna vez se han realizado copias de seguridad de la información de la organización?	10%
4.2.11	¿Están cifradas las copias de seguridad?	10%

Como ya hemos indicado en el apartado correspondiente las siguientes preguntas que están resaltadas en color morado, tienen una puntuación negativa, lo que significa que en caso de que la respuesta sea afirmativa, su puntuación no sumará, sino

restará. Y la recomendación aparecerá en su cuadrícula correspondiente cuando la respuesta sea sí.

Anexo II: Recomendaciones para los controles

A continuación, vamos a especificar todas las recomendaciones relacionadas con los controles. Recordemos que estas recomendaciones se mostrarán en el Framework en el caso en que la organización responda NO al control.

Tabla 5: Recomendaciones

Apartado	Recomendación
1.1.1	Realizar revisiones periódicas del estado de los dispositivos físicos. Un dispositivo sin actualizar u obsoleto puede tener brechas de seguridad que dejen vulnerable el dispositivo a ataques de Ransomware y se conviertan en entrada a la red corporativa.
1.1.2	En caso de que sea posible que la organización le entregue al trabajador un dispositivo configurado por ellos y en caso de que tenga que usar el propio, que guarde las medidas de seguridad adecuadas. Establecer una política de uso correcto de dispositivos en teletrabajo.
1.1.3	En caso de que sea posible que la organización le entregue al trabajador un dispositivo configurado por ellos y en caso de que tenga que usar el propio, que guarde las medidas de seguridad adecuadas. Establecer una política de uso correcto de dispositivos en teletrabajo.
1.1.4	Establecer una política de uso correcto de dispositivos en teletrabajo.
1.2.1	Establecer una política de buenas prácticas respecto a las contraseñas
1.2.2	Establecer una política de buenas prácticas respecto a las contraseñas
1.2.3	Aconsejar a los usuarios que cambien la contraseña cada tres meses
1.2.4	Aconsejar a los usuarios que cambien la contraseña cada tres meses
1.2.5	Establecer una política de buenas prácticas respecto a las contraseñas
1.3.1	Proporcionar a los empleados una guía con derechos y responsabilidades en la utilización de la información de la empresa que incluya elementos de seguridad y de la LGPD
1.3.2	Proporcionar a los empleados una guía con derechos y responsabilidades en la utilización de la información de la empresa que incluya elementos de seguridad y de la LGPD

1.4.1	Realizar formaciones en materia de las amenazas existentes y la seguridad de la información.
1.4.2	Realizar formaciones en materia de las amenazas existentes y la seguridad de la información.
1.4.3	Realizar formaciones en materia de las amenazas existentes y la seguridad de la información.
1.4.4	Realizar formaciones en materia de las amenazas existentes y la seguridad de la información.
1.4.5	Crear una guía o *newsletter* sobre los peligros actuales con referencia al malware a los que se pueden enfrentar diariamente en sus puestos de trabajo.
1.5.1	Revisar de manera periódica las webs de organizaciones especializadas en Ciberseguridad para estar al tanto de las amenazas existentes.
1.5.2	Revisar de manera periódica las webs de organizaciones especializadas en Ciberseguridad para estar al tanto de las amenazas existentes.
1.5.3	Proporcionar a los empleados las direcciones de las páginas web de las organizaciones relacionadas con la ciberseguridad y animarles a que se mantengan informados.
2.1.1	Realizar campañas de simulación para los empleados de la empresa cada 4/6 meses.
2.1.2	Realizar campañas de simulación para los empleados de la empresa cada 4/6 meses.
2.1.3	Realizar campañas de simulación para los empleados de la empresa cada 4/6 meses.
2.1.4	Realizar campañas de simulación para los empleados de la empresa cada 4/6 meses.
2.1.5	Evaluar a los empleados de la organización con test para valorar su nivel de concienciación en materia de ciberseguridad.
2.1.6	Evaluar a los empleados de la organización con test para valorar su nivel de concienciación en materia de ciberseguridad.
2.2.1	Realizar formaciones en materia de las amenazas existentes y la seguridad de la información.
2.2.2	Realizar formaciones en materia de las amenazas existentes y la seguridad de la información.

2.2.3	Realizar formaciones en materia de las amenazas existentes y la seguridad de la información.
2.2.4.1	Realizar formaciones con respecto a la navegación segura. Establecer una política de Navegación segura en la web.
2.2.4.2	Realizar formaciones con respecto a la navegación segura. Establecer una política de Navegación segura en la web.
2.2.4.3	Realizar formaciones con respecto a la navegación segura. Establecer una política de Navegación segura en la web.
2.2.4.4	Instalar bloqueadores de ventanas emergentes en los navegadores web
2.2.5.1	Controlar el acceso de los dispositivos mediante doble factor de autenticación.
2.2.5.2	Controlar el acceso de los dispositivos mediante doble factor de autenticación.
2.2.5.3	Instruir a los empleados en el uso correcto del correo electrónico
2.2.5.4	Instruir a los empleados en el uso correcto del correo electrónico
2.3.1	Establecer un protocolo o política de actuación para el uso de dispositivos de almacenamiento externo e informar del mismo a los empleados.
2.3.2	Establecer un protocolo o política de actuación para el uso de dispositivos de almacenamiento externo e informar del mismo a los empleados.
2.3.3	Establecer un protocolo o política de actuación para el uso de dispositivos de almacenamiento externo e informar del mismo a los empleados.
2.3.4	Utilizar bloqueadores de ejecución de USB para limitar el acceso del USB al ordenador.
3.1.1	Fragmentación de la red para proteger la infraestructura frente a un ataque de Ransomware
3.1.2	Realizar un filtrado del correo electrónico mediante antispam configurado en la plataforma de correo corporativa.
3.1.3	Mantener las macros desactivadas en la organización para proteger del software malicioso que pudieran contener los archivos que llegan por correo electrónico.
3.1.4	Concienciar al departamento de IT y la Dirección del peligro. Concienciación en ciberseguridad.

3.1.5	Proporcionar al trabajador de herramientas para que trabaje en conexiones seguras como una VPN de la empresa, etc.
3.1.6	Recomendarle al trabajador que se conecta a una IP abierta que utilice la VPN de la empresa para proteger la comunicación.
3.1.7	Recomendarle al trabajador que utilice la VPN de la empresa para proteger la comunicación.
3.1.8	Recomendarle al trabajador que utilice la VPN de la empresa para proteger la comunicación.
3.2.1	Configurar un antivirus en los dispositivos de los empleados.
3.2.2	Utilizar VPN para reforzar la seguridad a la hora de utilizar la red cuando se encuentra el empleado fuera del alcance de la red corporativa.
3.3.1	Realizar escaneos en busca de vulnerabilidades de forma recurrente al menos cada 6 meses.
3.3.2	Realizar escaneos en busca de vulnerabilidades de forma recurrente al menos cada 6 meses.
3.3.3	Realizar escaneos en busca de vulnerabilidades de forma recurrente al menos cada 6 meses.
4.1.1	Establecer un plan de contingencia y documentarlo de manera formal para poder seguirlo en caso de que ocurra un ataque de Ransomware.
4.1.2	Establecer un plan de contingencia y documentarlo de manera formal para poder seguirlo en caso de que ocurra un ataque de Ransomware.
4.1.3	Establecer un plan de contingencia y documentarlo de manera formal para poder seguirlo en caso de que ocurra un ataque de Ransomware.
4.1.4	Establecer un plan de contingencia y documentarlo de manera formal para poder seguirlo en caso de que ocurra un ataque de Ransomware.
4.1.5	Establecer un plan de contingencia y documentarlo de manera formal para poder seguirlo en caso de que ocurra un ataque de Ransomware.
4.1.6	Determinar una persona responsable para que cualquier empleado con sospecha de que se pueda estar realizando un ataque de Ransomware a la organización pueda localizarlo y actuar en consecuencia.
4.2.1	Realizar copias de seguridad con frecuencia semanal.
4.2.2	No almacenar las copias de seguridad en el mismo servidor donde esta la información de la organización de uso diario. Guardarlas en una parte de la red segmentada o en una localización que no este

	conectada a la red para que en el caso de un ataque no se pierda toda la información.
4.2.3	No almacenar las copias de seguridad en el mismo servidor donde esta la información de la organización de uso diario. Guardarlas en una parte de la red segmentada o en una localización que no este conectada a la red para que en el caso de un ataque no se pierda toda la información.
4.2.4	Almacenar las copias de seguridad en cajas fuertes o dispositivos no conectados a la red.
4.2.5	Determinar un RPO
4.2.6	Realizar copias de seguridad con frecuencia diaria o la que determine el RPO.
4.2.7	Realizar copias de seguridad con frecuencia diaria o la que determine el RPO.
4.2.8	Realizar copias de seguridad con frecuencia diaria o la que determine el RPO.
4.2.9	Realizar copias de seguridad con frecuencia diaria o la que determine el RPO.
4.2.10	Realizar copias de seguridad con frecuencia diaria o la que determine el RPO.
4.2.11	Cifrar las copias de seguridad para proporcionar una capa de protección extra a la información

ANEXO III: OBJETIVOS DE DESARROLLO SOSTENIBLE

Grado de relación del trabajo con los Objetivos de Desarrollo Sostenible (ODS).

Objetivos de Desarrollo Sostenibles	Alto	Medio	Bajo	No Procede
ODS 1. **Fin de la pobreza.**				x
ODS 2. **Hambre cero.**				x
ODS 3. **Salud y bienestar.**				x
ODS 4. **Educación de calidad.**				x
ODS 5. **Igualdad de género.**				x
ODS 6. **Agua limpia y saneamiento.**				x
ODS 7. **Energía asequible y no contaminante.**				x
ODS 8. **Trabajo decente y crecimiento económico.**	x			
ODS 9. **Industria, innovación e infraestructuras.**				x
ODS 10. **Reducción de las desigualdades**.				x
ODS 11. **Ciudades y comunidades sostenibles**.				x
ODS 12. **Producción y consumo responsables.**		x		
ODS 13. **Acción por el clima.**				x
ODS 14. **Vida submarina.**				x
ODS 15. **Vida de ecosistemas terrestres.**				x
ODS 16. **Paz, justicia e instituciones sólidas.**	x			
ODS 17. **Alianzas para lograr objetivos.**				x

Reflexión sobre la relación del TFG/TFM con los ODS y con el/los ODS más relacionados.

Este trabajo fin de Grado está relacionado íntimamente con el ODS 16, relacionado con la seguridad de las organizaciones en aspectos como el fraude y la seguridad en las operaciones. Es necesario que toda organización pueda llevar a cabo su actividad de negocio sin tener que preocuparse de la mala intención de los delincuentes, por ello, la finalidad de la herramienta que proponemos es proteger a las empresas de la guerra cibernética que están sufriendo en la actualidad, ayudará a proteger a las organizaciones de sobornos y fraudes, lo que es una de las metas de este ODS 16.

Con respecto al ODS 8, dado que este TFG está orientado al mundo empresarial el crecimiento económico es pieza fundamental de este mercado. Poder proteger uno de los activos más importantes de las organizaciones como es la información, garantizará que no habrá agentes externos que obstaculicen este crecimiento. Además de que promoverá formación y seguridad a los empleados lo que cumple con algunas de las metas destacadas de este ODS.

En cuanto al ODS 12, su relación no es tan estrecha como en las anteriores, pero las recomendaciones proporcionadas pueden ayudar a realizar un consumo responsable de activos, optimizando su utilización para fomentar la protección, promocionando el reciclaje de dispositivos tecnológicos que con un sistema de borrado y formateo completo pueden ayudar a bajar el consumo de material tecnológico. En vez de eliminar un dispositivo corporativo de un usuario tras su cese en la empresa, un formateo concienzudo puede ayudar a evitar un consumo excesivo de recursos mejorando el ciclo de vida de los activos y aumentando la eficiencia del gasto tecnológico en la organización.