Centro Universitario de la Defensa en la Escuela Naval Militar

TRABAJO FIN DE MÁSTER

La ciberseguridad y sus herramientas.

Diseño, organización y despliegue, en las redes de una gran corporación.

Máster Universitario en Dirección TIC para la Defensa

ALUMNO: Ángel San José Arranz

DIRECTOR: Miguel Rodelgo Lacruz

CURSO ACADÉMICO: 2022-2023

Universidade Vigo

Centro Universitario de la Defensa
en la Escuela Naval Militar

TRABAJO FIN DE MÁSTER

La ciberseguridad y sus herramientas.
Diseño, organización y despliegue, en las redes de una gran corporación.

Máster Universitario en Dirección TIC para la Defensa

Especialidad de Sistemas y Tecnologías de la Información

Universidade Vigo

RESUMEN

Este Trabajo Final de Máster (TFM) pretende profundizar en el campo de la ciberseguridad, aclarando conceptos en materia de Seguridad de la Información, relativa a los CIS/TIC y ciberdefensa entre algunos otros.

Se pretende abordar como debe estar implementada la ciberseguridad en una gran corporación, y que herramientas son fundamentales desplegar para que sea efectiva, fácilmente controlable y aplicable, con una descripción genérica de las mismas, y sin referencia a productos de marcas determinadas.

Como algo de interés y novedoso, por ser algo que empieza a ser muy demandado en el mundo de la ciberseguridad, pero a lo que no aún no se ha dado una buena solución, se hará una descripción o esbozo de los requerimientos de una herramienta en particular, que integra a otras muchas herramientas de ciberseguridad, y sin la que muchas organizaciones o grandes empresas, no conseguirán una buena gestión de su seguridad en el futuro.

Dicha herramienta se trata de un Cuadro de Mando Integral (CMI), que permite la gestión y control de activos, de vulnerabilidades e incidentes, su seguimiento y resolución, todos ellos piezas fundamentales en materia de ciberseguridad e integrado en los diferentes niveles y roles de gobierno o actuación.

Se analizará el asunto desde el diseño para una gran red corporativa simulada con una casuística particular, en la que se pueden albergar dominios y sistemas sin clasificar, e incluso sistemas y servicios clasificados, adecuados eso sí al Esquena Nacional de Seguridad (ENS), en los que se integrarán tecnologías antiguas y modernas, como despliegues en la nube o equipos virtualizados.

Igualmente se desarrollará como debe articularse la organización en los diferentes niveles, pasando desde los Comités de Dirección, Grupos de Trabajo o Gabinetes de Crisis y los Centros de Ciberseguridad (COSC) o SOC.

Para enriquecer y hacer más interesante el trabajo, se incluirán gráficos y figuras, que faciliten la comprensión y seguimiento, a la vez que se incluirán ejemplos ficticios y reales de uso, en las descripciones que así lo requieran, con el objeto de hacer su lectura más amena.

No pretende ser un trabajo de interés técnico, o sólo para expertos en la materia de la ciberseguridad, sino ser una guía o referencia de inicio para los que pretendan abordar el diseño de la ciberseguridad, sin ninguna otra referencia de partida, o simplemente ser un texto de divulgación para enriquecer a quien lo lea en materia de ciberseguridad, que tan de moda esta hoy en día.

PALABRAS CLAVE

Ciberseguridad, gobernanza, políticas, guías, herramientas.

AGRADECIMIENTOS

Dedico este TFM a mi esposa Elisa y a mi hijo Carlos, por su enorme paciencia y comprensión, junto a su gran apoyo en todo momento, lo que me ha permitido sacar tiempo al tiempo, y poder realizar un trabajo de calidad, y en el que se ha volcado mucha dedicación.

También dedico este trabajo al profesor D. Miguel Rodelgo Lacruz, en agradecimiento a su magistral dirección, sus acertadas correcciones y sugerencias, que han contribuido sin lugar a dudas, a proporcionarle mayor calidad y coherencia.

CONTENIDO

Contenido 1

Índice de Figuras 4

1 Introducción 5

1.1 Marco conceptual 5

1.2 Motivación 6

1.3 Objetivos 7

1.4 Estructura y contenidos 8

2 Estado del arte 9

2.1 Actualidad 9

2.2 Definiciones 10

2.2.1 Ciberseguridad 10

2.2.2 Ciberdefensa 10

2.2.3 Ciberespacio 10

2.2.4 Incidente de seguridad 11

2.2.5 Ciberincidente 11

2.2.6 Cibercrimen o ciberdelito 11

2.2.7 Ciberterrorismo o terrorismo electrónico 11

2.2.8 Ciberataque 11

2.2.9 Ciberamenaza 12

2.2.10 Ciberespionaje 12

2.2.11 Hacktivismo 12

2.2.12 Análisis de riesgos 12

2.2.13 Activo 12

2.2.14 Auditoria de seguridad 12

2.2.15 Vulnerabilidad 13

2.2.16 Common Vulnerabilities and Exposures (CVE) 13

2.2.17 Análisis de vulnerabilidades 13

2.2.18 SOC / COCS o centros de operaciones de ciberseguridad 13

2.2.19 El Centro Criptológico Nacional (CCN) 13

2.2.20 Equipo de Respuesta ante Emergencias Informáticas (CERT), del inglés Computer Emergency Response Team 14

2.2.21 Computer Security Incident Response Team, (CSIRT) 14

2.2.22 El CCN-CERT 14

2.2.23 El INCIBE-CERT 14

2.3 Estrategias de seguridad, planes y leyes de ámbito Nacional e Internacional 14
2.3.1 Estrategia de Seguridad Nacional 14
2.3.2 La Agenda Digital 2025 15
2.3.3 Plan nacional de digitalización de las APP 15
2.3.4 Plan nacional de Ciberseguridad 16
2.3.5 Esquema Nacional de Seguridad (ENS) 16
2.3.6 Reglamento del Parlamento Europeo 17
3 Desarrollo del TFM 20
3.1 Introducción 20
3.2 Redes de una gran corporación 20
3.3 Políticas de Ciberseguridad, su diseño y su implementación 22
3.4 Marco de gobernanza y estructuras 26
3.5 Órgano de dirección 27
3.6 Órganos de control y coordinación 27
3.7 Órganos de operación y resolución 29
3.8 Guías de gestión de la ciberseguridad 30
3.8.1 Guía del Plan de Crisis 30
3.8.2 Guía de notificación de incidentes 32
3.8.3 Guía de gestión de incidentes 34
3.9 Herramientas de ciberseguridad, su diseño, su despliegue e integración 35
3.9.1 Cortafuegos o Firewall 36
3.9.2 Cortafuegos de aplicaciones web o WAF (web Application Firewall) 37
3.9.3 Sistema de Prevención de Intrusos IPS 37
3.9.4 NGFW (Firewall de última generación) 38
3.9.5 IDS o (Intrusion Detection System) 38
3.9.6 Gestión de eventos e información de seguridad (SIEM) 38
3.9.7 Detección y respuesta de endpoints (EDR / XDR) 38
3.9.8 Infraestructura de Clave Pública o PKI 39
3.9.9 Accesos seguros desde equipos externos VPN (SSL, iPSec) 40
3.9.10 Pentesting 41
3.9.11 Escáneres de vulnerabilidades 41
3.9.12 Autenticación robusta con doble factor de autenticación 43
3.9.13 Network Access Control (NAC) 43
3.9.14 Sandboxing 44
3.9.15 Formación 44
3.10 Herramienta de gestión integral 45

3.11 Contratación de servicios y suministro de ciberseguridad 47
3.12 Las auditorias de seguridad como herramienta de ciberseguridad 49
4 Conclusiones 51
4.1 Conclusiones del TFM 51
4.2 Consideraciones de futuro 52
5 Bibliografía 56
Anexo I: Ciberamenazas en el mundo 59
Anexo II: 14 tipos de ciberataque 61
Anexo III: Los 5 mayores ciberataques de la historia 65
Anexo IV: Estadísticas de ciberseguridad 67

ÍNDICE DE FIGURAS

Figura 1-1 Representación del ciberespacio. Fuente: [4] 6
Figura 2-1 Fuente: [4] 9
Figura 2-2 Logo del Plan Nacional. De Ciberseguridad. Fuente: [11] 16
Figura 2-3 Portada del Reglamento UE. [Elaboración Propia] 19
Figura 3-1 Red de una gran organización. [Elaboración Propia] 21
Figura 3-2 Ejemplo de panfleto. Fuente [12] 24
Figura 3-3 Cuadernos. Fuente: [13] 25
Figura 3-4 Órgano de dirección, de control y coordinación. Fuente: [4] 27
Figura 3-5 SOC de una gran organización. Fuente: [21] 28
Figura 3-6 Plan de Crisis de una organización tipo. [Elaboración propia] 32
Figura 3-7 Flujograma de notificación de incidentes. Fuente: [14] 33
Figura 3-8 Ciclo de vida de gestión de un incidente tipo. [Elaboración Propia] 34
Figura 3-9 Funcionamiento de un Firewall. Fuente: [15] 37
Figura 3-10 Esquema funcionamiento PKI. Fuente: [15] 40
Figura 3-11 Fases de Pentesting. Fuente: [15] 41
Figura 3-12 Cuadro de Mando Integral. Fuente: [25] 45
Figura 3-13 Logotipo del CESTIC 49
Figura 3-14 Logotipo del ENS. Fuente: [26] 50
Figura 3-15 Operadores con redes 5G en España en 2022 53
Figura 3-16 Chip cuántico. Fuente: [27] 55
Figura A1-1 Web que muestra las ciberamenazas en el mundo en tiempo real. Fuente: [28] 59

1 INTRODUCCIÓN

1.1 Marco conceptual

Hasta hace relativamente pocos años podría decirse que no más de diez o quince, el termino ciberseguridad era un vocablo con poca relevancia, o prácticamente desconocido para el común de los habitantes del planeta.

Hoy en día por diversos motivos ese vocablo tiene una relevancia superlativa, porque afecta a todas las naciones que componen la Tierra, independientemente de su ubicación, estado de desarrollo, riqueza, situación política, o incluso que estén en estado de paz, o de guerra.

Tanto es así, que relacionado con la ciberseguridad se desarrollan planes de nivel nacional e internacional, en grandes organizaciones como la OTAN, se dotan partidas presupuestarías bastante onerosas para atender esta materia (ejemplo los fondos de la Unión Europea para ciberseguridad), se dictan políticas de actuación en las administraciones públicas y en la empresas, y de forma muy especial en el ámbito militar, encuadrándose ya en lo que se denomina el ciberespacio, catalogándolo como la cuarta dimensión del campo de batalla.

- Pero de qué hablamos-, ¿qué se entiende por ciberseguridad?

Si atendemos a los significados del prefijo ciber y del término seguridad:

- Ciber: Indica relación con redes informáticas.
- Seguridad: cualidad de “seguro”, término que a su vez significa, algo libre y exento de riesgos.

Es por ello que podemos obtener una primera aproximación sobre el significado de ciberseguridad, como la acción de mantener redes informáticas exentas de riesgo y en libertad frente a cualquier acción por impedirla. Pero es necesario profundizar en dicha acepción para una mejor compresión del vocablo y su campo de acción.

Tradicionalmente se conoce la seguridad informática como la ciberseguridad, siendo su misión la de proteger, sistemas, redes y programas de ataques digitales, para preservar la confidencialidad, disponibilidad, e integridad de la información.

Aunque una más reciente sería la del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS) [3].

Ciberseguridad (seguridad de los sistemas de información): la capacidad de las redes y sistemas de información de resistir, con un nivel determinado de fiabilidad, toda acción que comprometa la disponibilidad, autenticidad, integridad o confidencialidad de los datos almacenados, transmitidos o tratados, o los servicios correspondientes ofrecidos por tales redes y sistemas de información o accesibles a través de ellos.

No debiendo confundirla con la seguridad de la información, que se encarga de los métodos y procesos que procuran proteger los activos de información en sus diferentes formas o estados, no centrándose únicamente en los sistemas computacionales.

Es por ello que puede decirse que la ciberseguridad para una gran organización está contenida dentro del proceso de seguridad de la información de ésta, y que será necesario que se establezca una estructura dentro de la organización, que se encargue de su diseño, organización, herramientas y despliegue en las redes informáticas.

1.2 Motivación

El ciberespacio podría definirse, como la dimensión espacial creada mediante la interconexión de ordenadores y redes digitales por todo el mundo, pero que es algo que va más lejos aún incluso, de lo que algunos podrían estar identificando como internet, dado que afecta además a leyes, normativas, procedimientos, organizaciones, países, personas, formas de uso e interacción, etc. Una recreación del mismo es lo que se quiere mostrar en la figura 1-1.

Figura 1-1 Representación del ciberespacio. Fuente: [4]

Este trabajo no pretende ser un trabajo de interés técnico o dedicado sólo para expertos en materia de la ciberseguridad, sino que pretende ser una guía o referencia de inicio, para todos aquellos neófitos o interesados en este mundo tan apasionante, que pretendan abordar el entendimiento de la ciberseguridad sin ninguna otra referencia de partida. Es por ello que podría catalogarse más bien como un ensayo o texto de divulgación, para enriquecer a quien lo lea en materia de ciberseguridad, que tan de moda esta hoy en día.

Dado que los temas tratados en este trabajo son de rápida evolución con el tiempo, se debe remarcar la posibilidad de que no esté completamente actualizado las últimas tecnologías o tendencias del momento, siendo la fecha más actual de los datos contemplados en el mismo el mes de diciembre 2022.

Por último, es necesario mencionar, que para la elaboración del documento se ha empleado la terminología contemplada por la Real Academia de la Lengua (RAE), y en caso de no estar contemplado algún término, se ha utilizado el más común o conocido.

Para la elaboración de dicho trabajo, se han consultado ciertos ensayos y publicaciones relacionadas con la materia, se ha asistido a diversas exposiciones de productos de empresas que trabajan en desarrollar herramientas de ciberseguridad, pero ha sido el trabajo diario en dicho campo, el que ha posibilitado obtener la mayor parte de los datos y argumentos que en él se esgrimen y desarrollan.

No en vano, una de las mayores fuentes de donde se han extractado bastantes ideas y se han reforzado conceptos, ha sido el acceso y seguimiento de información relacionada con multitud de casos de ciberataques, que se han incrementado de forma diferente pero en claro aumento sobre muchos países, a raíz del conflicto de la invasión de Ucrania por parte de Rusia.

No solo han proliferado, o se ha descubierto multitud de grupos de cibercriminales que apoyan la causa rusa, sino que también se han organizado grupos de hacktivistas que actúan en beneficio de Ucrania, junto con los propios servicios de ciberdefensa que igualmente despliegan ambos países.

Motivado por este conflicto, en la cumbre de la OTAN desarrollada en Madrid el pasado mes de junio 2022, se sentaron las bases para nuevas y más acciones coordinadas por los países miembros en materia de ciberseguridad y ciberdefensa. Lo cual no deja de ser una manifestación de lo importante que este campo de acción va a ser en el futuro, a la hora de mantener el orden mundial y la seguridad de las organizaciones y los países, llegando como es el caso de España, a ser uno de los principales temas en los que se incrementa la preocupación, y fruto de ello la inversión de grandes sumas de dinero, como queda claramente patente en el Plan Nacional de Ciberseguridad.

Para obtener una visión global de la situación a nivel mundial, sobre datos y estadísticas relativos al mundo de la ciberseguridad y que reafirman más si cabe su importancia, el lector puede acudir al anexo IV de este TFM donde podrá deleitarse con su lectura, encontrado que muchos de los cuales son bastante curiosos, cuando no alarmantes.

1.3 Objetivos

Los objetivos fundamentales perseguidos, y que ya se dejan entrever en el propio título son los siguientes:

- Revisar las diferentes estrategias que a nivel del Estado se han ido desarrollando y llevado a la práctica, fruto de la situación o la coyuntura de cada momento, así como la revisión de parte de la legislación que en materia de ciberseguridad se está generando, como parte intrínseca y fundamental de la ciberseguridad, ya que está asumiendo una relevancia muy considerable, tanto es así que parece ser uno de los motores que más impulsan el avance en materia de ciberseguridad en este momento.

- El estudio de los requerimientos de ciberseguridad de una gran corporación, analizando los motivos de los que emanan, confrontados con sus posibles consecuencias en caso de no aplicarlos, y todo ello argumentado con diferentes casuísticas que pueden darse. Junto con un análisis organizacional de la corporación, para atender al desarrollo y la implementación de la política de ciberseguridad, la generación de la múltiple y variada documentación a desarrollar, al objeto de resolver los incidentes que se produzcan, y así poder comprender los diferentes roles en la organización, y diferentes situaciones que puedan darse.

- La exposición, análisis y diseño de las herramientas, que en materia de ciberseguridad se despliegan en una gran organización, basado en opiniones, casos de uso y experiencias con ellas. Describiendo de forma generalista los requerimientos fundamentales que deberá de cumplir el caso concreto de una herramienta de integración de herramientas de ciberseguridad. Dicha herramienta deberá ser desarrollada en la organización o adquirida por la misma, si se quieren tener ciertas garantías de que se implementa adecuadamente la ciberseguridad y de que no se está derrochando capital, en soluciones que no solo no se integran, si no que dejan fisuras importantes en la seguridad de la organización.

1.4 Estructura y contenidos

Una vez desarrollado el marco conceptual, expresada la motivación del autor y manifestados los objetivos que pretenden lograr con el desarrollo de este TFM, sería muy grato haber conseguido motivar o abrir el apetito por el conocimiento de conceptos básicos pero fundamentales sobre el apasionante mundo de la ciberseguridad. Pero en caso de no haberlo logrado aún, parece lógico y acertado dedicar este pequeño subapartado a mostrar el resto de la estructura y organización del trabajo, al objeto de una mejor orientación a lector que podrá optar por una lectura completa o parcial de este TFM, en base a sus ya conocimientos anteriores sobre la materia, o en su avidez por conocer o resolver inquietudes.

En el capítulo 2 se desarrollará el estado del arte, mostrando unos flecos de la actualidad del momento, para pasar a realizar una definición de una serie de conceptos empleados a lo largo del trabajo y considerados como básicos, para así entender mucho mejor el mundo de la ciberseguridad. Finalmente, en este capítulo se hará un breve esbozo de las estrategias nacionales, así como de los planes y leyes en el ámbito nacional e internacional, que afectan a la ciberseguridad.

Seguidamente ya en el capítulo 3 y como fundamental, es en el que se desarrolla el núcleo de TFM, donde ya se describirán las estructuras, organizaciones, guías, planes y procedimientos, así como las herramientas que deberán ser implementadas en la organización, para materializar una adecuada ciberseguridad.

El capítulo 4 es en el que ya se establecen una serie de conclusiones a modo de resumen, la cuales aparte de hacer una breve exposición de las ideas y conceptos desgranados en la consecución del trabajo, buscan ciertamente la reflexión del lector sobre lo que ha leído, y pretenden en cierta forma conseguir unos momento de juicio crítico con lo expuesto en el trabajo, enriquecido todo ello con unas últimas consideraciones finales, para enlazar este trabajo con otros campos de interés y de mucha importancia en el futuro.

Finalmente el trabajo contiene un capítulo 5, donde se recogen las numerosas referencias sobre trabajos y páginas web consultadas para poder efectuar este trabajo, junto con un apartado último dedicado a los anexos, donde se exponen una serie de cuadros para que el lector pueda consultarlo durante la lectura del TFM y hacerse una idea real de la situación descrita.

2 ESTADO DEL ARTE

2.1 Actualidad

Figura 2-1 Fuente: [4]

La seguridad en las tecnologías de información y comunicaciones (TIC) en sus orígenes, no era una consideración imprescindible en su diseño, dado que chocaba directamente con la finalidad principal en el despliegue de las redes telemáticas, que era su facilidad de uso, mediante condiciones de comunicación adecuadas, y protocolos y enlaces cada vez más rápidos y eficientes. Sin embargo, a día de hoy una vez alcanzada ya sobradamente su fácil implementación y uso, hacen que ese paradigma haya cambiado, siendo la preocupación principal la de proporcionar seguridad a las TIC.

La civilización en la actualidad está en lo que podríamos denominar "la era de la información", y la confianza depositada por los usuarios en las redes y sus plataformas de servicios es tal, que no solo las emplean para realizar sus transacciones bancarias, comunicaciones de datos y actos administrativos, sino también como medios de comunicación y relación social mediante diferentes plataformas, incluso depositando en ella en lo que se denomina la nube, infinidad de datos de carácter sensible o íntimo, como lo son las fotografías, videos, documentos, etc.

Es por ello que la seguridad de la información en las TIC en definitiva, la ciberseguridad, es quizá la funcionalidad más importante a satisfacer para cualquier tipo de usuario de las redes y sus servicios y ya no es un tema desconocido, del que mucha gente ya habla con cierta agilidad, que está presente en nuestro día a día. Un ejemplo claro son las múltiple imágenes y logos que se muestran en Internet como la de la figura 2-1, que claramente muestra la importancia de la seguridad en las redes y que todo el mundo ya conoce e identifica.

Para ello existen multitud de soluciones o herramientas que bien de forma individual o bien de forma conjunta, deben ser implementadas en redes, servicios, plataformas y aplicaciones, al objeto de satisfacer la demanda actual.

No existe una solución maestra o única, sino que es necesario analizar dónde, por qué y para qué deben implementarse. Pero lo que sí está claro es que son necesarias, están en continua evolución y van a quedarse durante muchos años, hasta que quizá mediante las herramientas de ciberseguridad cuántica, deban adoptar otro prisma.

Con esta breve exposición del estado del arte, y con la esperanza de haber abierto el apetito por conocer de los posibles lectores de este TFM, queda claramente sentenciado que la ciberseguridad se trata de un *trending topic* entre los asuntos de actualidad, además de una cuestión o una tarea pendiente,

para ser acometida por numerosos actores como son las grandes organizaciones, los Estados, las empresas, los fabricantes, las organizaciones gubernamentales, y los propios usuarios de las TIC.

2.2 Definiciones

Para una mejor comprensión del mundo de la ciberseguridad, se deben conocer algunos conceptos sobre los que se fundamenta este análisis, tales como ciberseguridad, ciberdefensa, ciberespacio, incidente de seguridad, ciberincidente, cibercrimen o ciberdelito, ciberterrorismo, ciberataque y sus tipos más conocidos, ciberamenaza, ciberespionaje, hacktivismo, análisis de riesgos, activos, análisis de vulnerabilidades, auditoria de seguridad, vulnerabilidad CVE,s, análisis de vulnerabilidades, SOC/COCS, CCN, CERT, CSIRT, CCN CERT, INCIBE CERT.

2.2.1 Ciberseguridad

La Unión Internacional de Telecomunicaciones (ITU) define el termino como el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones , formación, prácticas idóneas, seguros y tecnologías, que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberespacio. [5]

El Comité sobre Sistemas de Seguridad Nacional (CNSS) de EEUU, lo define como la prevención contra el daño, la protección, o el restablecimiento de computadoras, sistemas de comunicación electrónica, comunicaciones por cable e inalámbricas, incluyendo la información contenida en los mismos, con el objetivo de asegurar su disponibilidad, integridad, autenticación, confidencialidad y no repudio. [1,2]

El Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad define ciberseguridad como, la capacidad de las redes y sistemas de información de resistir, con un nivel determinado de fiabilidad, toda acción que comprometa la disponibilidad, autenticidad, integridad o confidencialidad de los datos almacenados, transmitidos o tratados, o los servicios correspondientes ofrecidos por tales redes y sistemas de información o accesibles a través de ellos. [3]

2.2.2 Ciberdefensa

La ciberdefensa, además de prevenir los ataques como hace la ciberseguridad, da respuesta a los mismos con nuevos ataques con fin de salvaguardar la seguridad [6].

Podríamos definirla como el conjunto de acciones y operaciones activas o pasivas, desarrolladas en el ámbito de las redes, sistemas, equipos, enlaces y personal de los recursos informáticos de la organización, a fin de asegurar el cumplimiento de las misiones o servicios para los que fueran concebidos, a la vez que se impide que posibles atacantes los utilicen para cumplir los suyos.

2.2.3 Ciberespacio

El Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad define ciberespacio como dominio global y dinámico compuesto por infraestructuras de tecnología de la información -incluyendo internet-, redes de telecomunicaciones y sistemas de información que configura un ámbito virtual.

Según la RAE es el ámbito virtual creado por medios informáticos. [7]

2.2.4 Incidente de seguridad

El Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad define Incidente de seguridad como, suceso inesperado o no deseado con consecuencias en detrimento de la seguridad de las redes y sistemas de información.

2.2.5 Ciberincidente

El Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad define ciberincidente como, incidente relacionado con la seguridad de las tecnologías de la información y las comunicaciones que se produce en el ciberespacio.

2.2.6 Cibercrimen o ciberdelito

Es una actividad delictiva que afecta o abusa de una computadora, una red informática o un dispositivo en red. La mayor parte del cibercrimen, pero no todos, lo perpetran cibercriminales o hackers que desean ganar dinero. El cibercrimen lo cometen personas u organizaciones. Algunos cibercriminales están organizados en grupos, utilizan técnicas avanzadas y cuentan con grandes habilidades técnicas. Otros son hackers novatos. En raras ocasiones, el cibercrimen tiene como objetivo dañar las computadoras por motivos distintos a la obtención de dinero. Estos pueden ser políticos o personales.[8]

La mayor parte del cibercrimen se divide en dos categorías principales:

- Actividad delictiva dirigida a las computadoras que suele implicar virus y otros tipos de malware.
- Actividad delictiva que utiliza computadoras para cometer otros delitos que puede implicar el uso de computadoras o redes para propagar malware, información ilegal o imágenes ilegales.

2.2.7 Ciberterrorismo o terrorismo electrónico

Es el uso de medios de tecnologías de información, informática, comunicación, electrónica o similar, buscado el propósito de generar terror o generar miedo en una población, clase dirigente o gobierno, causando con ello una violación a la libre voluntad de las personas.

2.2.8 Ciberataque

El Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad define ciberataque como, cualquier conducta dolosa de individuos u organizaciones, conocidos o no, desarrollada a través del ciberespacio contra sistemas de información, con el propósito de sustraer, alterar, abusar, desestabilizar, inutilizar, destruir o eliminar activos.

Según la web Wikipedia [9], es cualquier maniobra ofensiva de explotación deliberada que tiene para desestabilizar o dañar un sistema informático (ordenador, red privada, etcétera). El atacante es un individuo u organización que intenta obtener el control de un sistema informático para utilizarlo con fines maliciosos, robo de información o de hacer daño a su objetivo. Un ciberataque utiliza códigos maliciosos, para corromper los códigos, datos privados o algoritmos, generando consecuencias que comprometen y vulneran la seguridad de los sistemas de información.

Para ver la definición de algunos de los más representativos, se ha incluido el anexo II donde se pueden consultar 14 de ellos.

2.2.9 Ciberamenaza

El Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad define ciberamenaza como, amenaza a los sistemas y servicios presentes en el ciberespacio o alcanzables a través de éste.

2.2.10 Ciberespionaje

Es el acto o práctica de obtener secretos sin el permiso del poseedor de la información (personal, sensible, propietaria o de naturaleza clasificada), de individuos, competidores, rivales, grupos, gobiernos y enemigos para ventaja personal, económica, política o militar usando métodos en Internet, redes o computadoras individuales a través del uso de técnicas de *cracking* y software maliciosos incluyendo troyanos y *spyware*. [9]

Puede ser totalmente perpetrado en línea desde las computadoras de escritorio de profesionales en las bases en países muy lejanos o puede implicar la infiltración en el hogar por espías convencionales entrenados en computación o en otros casos puede ser la obra criminal de un *hacker* malicioso amateur y programadores de software.

2.2.11 Hacktivismo

La palabra hacktivismo surge de la unión de dos términos como son *hacker* y activismo. Por un lado, el hacker es aquella persona que detecta brechas de seguridad en los equipos informáticos. Por otro, el activismo se refiere a la participación en movimientos políticos o sociales con ánimos reivindicativos. [10]

Entonces, el hacktivista es aquella persona que se aprovecha de sus conocimientos en la rama de la tecnología y la informática para detectar vulnerabilidades en equipos y sistemas, con el objetivo de penetrar en ellos y reivindicar alguna causa social o política. Generalmente, los hacktivistas trabajan en grupos y tienen como objetivos grandes empresas y corporaciones, gobiernos u otro tipo de instituciones con peso en el ámbito económico, político o social.

2.2.12 Análisis de riesgos

El Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad define análisis de riesgos como, el estudio de las consecuencias previsibles de un posible incidente de seguridad, considerando su impacto en la organización (en la protección de sus activos, en su misión, en su imagen o reputación, o en sus funciones) y la probabilidad de que ocurra.

2.2.13 Activo

El Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad define activo como, componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (*software*), equipos (*hardware*), comunicaciones, recursos administrativos, recursos físicos y recursos humanos.

2.2.14 Auditoria de seguridad

El Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad define auditoria de seguridad como, un proceso sistemático, independiente y documentado que persigue

la obtención de evidencias objetivas y su evaluación objetiva para determinar en qué medida se cumplen los criterios de auditoría en relación con la idoneidad de los controles de seguridad adoptados, el cumplimiento de la política de seguridad, las normas y los procedimientos operativos establecidos, y detectando desviaciones a los antedichos criterios.

2.2.15 Vulnerabilidad

Se define como la debilidad que puede ser explotada en un ciberataque con la intención de lograr acceso no autorizado, o realizar acciones no autorizadas sobre un sistema informático, pudiendo permitir a los atacantes la ejecución de código malicioso, acceder a la memoria del sistema, instalar diferentes tipos de malware, o incluso robar, destruir o modificar datos confidenciales.

Vulnerabilidades del día cero, son las vulnerabilidades desconocidas para los usuarios y para el fabricante del producto. Esto supone que aún no hayan sido arregladas, y suelen ser objetivo de numerosos ataques por este motivo.

2.2.16 Common Vulnerabilities and Exposures (CVE)

Se trata de una lista de vulnerabilidades y exposiciones de seguridad de la información, que es divulgada públicamente.

MITRE (es una empresa sin fines de lucro constituida en 1958; tiene sus orígenes en el Instituto Tecnológico de Massachusetts (MIT) que lanzó en 1999 la lista de vulnerabilidades, para identificar y categorizar vulnerabilidades en software y firmware como si se tratase de un diccionario gratuito, para que las organizaciones mejoren su seguridad cibernética.

2.2.17 Análisis de vulnerabilidades

Es el proceso dentro de una organización en el que se estudian las vulnerabilidades que pueden afectar los activos de la organización, para aumentar la seguridad del entorno de trabajo evitando que se produzcan posibles ataques. Es utilizado para identificar vulnerabilidades en los sistemas, en sistemas eléctricos o de comunicación.

2.2.18 SOC / COCS o centros de operaciones de ciberseguridad

Un centro de operaciones de ciberseguridad (COCS), o SOC para abreviar, es una amalgama centralizada de personas, procesos y tecnología que trabajan para proteger los sistemas y redes de una organización a través de la monitorización, detección, prevención y análisis continuos de las amenazas cibernéticas.

Estos pueden ser internos a la organización o externos, por medio de servicios subcontratados.

2.2.19 El Centro Criptológico Nacional (CCN)

Es el organismo responsable de garantizar la seguridad las Tecnologías de la Información y la Comunicación (TIC) en las diferentes entidades del Sector Público, así como la seguridad de los sistemas que procesan, almacenan o transmiten información clasificada.

2.2.20 Equipo de Respuesta ante Emergencias Informáticas (CERT), del inglés Computer Emergency Response Team

Es un centro de respuesta para incidentes de seguridad en tecnologías de la información. Está formado por un grupo de expertos responsable del desarrollo de medidas preventivas y reactivas ante incidencias de seguridad en los sistemas de información. Un CERT estudia el estado de seguridad global de redes y ordenadores y proporciona servicios de respuesta ante incidentes a víctimas de ataques en la red, publica alertas relativas a amenazas y vulnerabilidades y ofrece información que mejora la seguridad de estos sistemas.

2.2.21 Computer Security Incident Response Team, (CSIRT)

Equipo de Respuesta ante Incidencias de Seguridad Informáticas para referirse al mismo concepto que CERT. De hecho, el término CSIRT es el que se suele usar en Europa en lugar del término protegido CERT, que está registrado en EE.UU. por CERT Coordination Center (CERT/CC).

2.2.22 El CCN-CERT

Es la Capacidad de Respuesta a Incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN. Este servicio se creó en el año 2006 como CERT Gubernamental Nacional español y sus funciones quedan recogidas en la Ley 11/2002 reguladora del Centro Nacional de Inteligencia (CNI), el RD 421/2004 de regulación del CCN y en el RD 311/2022, de 3 de mayo, que regula el Esquema Nacional de Seguridad.

Su misión, por tanto, es contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas, incluyendo la coordinación a nivel público estatal de las distintas capacidades de respuesta a incidentes o centros de operaciones de ciberseguridad existentes.

2.2.23 El INCIBE-CERT

INCIBE-CERT es el centro de respuesta a incidentes de seguridad de referencia para los ciudadanos y entidades de derecho privado en España operado por el Instituto Nacional de Ciberseguridad (INCIBE), dependiente del Ministerio de Asuntos Económicos y Transformación Digital, a través de la Secretaría de Estado de Digitalización e Inteligencia Artificial.

2.3 Estrategias de seguridad, planes y leyes de ámbito Nacional e Internacional

Para un mejor entendimiento del estado del arte de la ciberseguridad, en este apartado se va a realizar una breve descripción de diferentes documentos, que reflejan de una forma muy contundente, la imperiosa necesidad de acometer el asunto de la ciberseguridad a nivel Nacional de una forma completa, trasversal y contemplando todos los escenarios y mecanismos que el Estado puede manejar, y que de no ser así sería muy difícil que lograse el objetivo perseguido.

2.3.1 Estrategia de Seguridad Nacional

El Consejo de Ministros aprobó el pasado 28 de diciembre de 2021 la nueva Estrategia de Seguridad Nacional (ESN) 2021. Esta nueva estrategia, actualiza la del año 2017.

En el citado documento se muestra una mayor sensibilidad hacia la ciberseguridad y refleja en relación a la trasformación digital, que se hace patente que la magnitud y frecuencia de los ciberincidentes y del uso ilícito del ciberespacio han aumentado en los últimos años y han convertido la ciberseguridad en una prioridad de organizaciones y gobiernos.

En relación al ciberespacio establece que, en términos de ciberseguridad, se requiere garantizar el uso seguro y fiable del ciberespacio, para proteger los derechos y las libertades de los ciudadanos y promover el progreso socio económico. Para ello es importante incrementar las capacidades (tecnológicas, humanas y económicas) de la ciberseguridad nacional dirigidas a la prevención, detección, respuesta, recuperación, investigación y defensa activa.

En la Administración pública, es ineludible avanzar en el modelo de gobernanza de la ciberseguridad nacional, sobre la base de una mayor eficiencia en los recursos y la integración de las capacidades nacionales. En este sentido, el centro de operaciones de ciberseguridad permitirá, mediante la prestación de servicios horizontales, aumentar las capacidades de vigilancia, detección y respuesta ante ciberataques contra la administración general del Estado y sus organismos públicos, así como contra las administraciones autonómicas y locales.

Un aspecto relevante será el desarrollo de las infraestructuras de ciberseguridad en las Comunidades y Ciudades Autónomas. Prioridades adicionales son la creación de un sistema de observación y medición de la situación de la ciberseguridad nacional y la puesta en marcha de una plataforma nacional de notificación y seguimiento de ciberincidentes que permita medir el intercambio de información entre organismos públicos y privados en tiempo real.

2.3.2 La Agenda Digital 2025

Se aprobó en julio de 2020, presentado, un plan que destinará 140.000 millones de euros, entre otras cosas, para que al menos el 25% del volumen de negocio de las pymes españolas, provenga del comercio electrónico, en el 2025. El Plan viene acompañado de 50 medidas agrupadas en diez ejes estratégicos, con los que se pretende impulsar la transformación digital en el país

Es el 4º el que establece:

En éste entorno digital, se hace más necesario que nunca el disponer de seguridad adecuada a las nuevas necesidades. Para ello, se busca disponer de 20.000 especialistas en ciberseguridad, Inteligencia Artificial y datos en 2025 gracias, entre otros aspectos, al polo de actividad empresarial que supone el entorno del Instituto Nacional de Ciberseguridad (INCIBE).

Los objetivos planteados al respecto son:

- Incrementar las capacidades de ciberseguridad de ciudadanía y empresas.
- Fomentar el desarrollo del ecosistema empresarial en el sector ciberseguridad.
- Potenciar la visibilidad internacional de España en ciberseguridad.

2.3.3 Plan nacional de digitalización de las AAPP

Fue aprobado en febrero de 2021 y en su EJE 1.Transformación digital de la administración del estado, establece en su medida 9 relativa a la creación de un centro de operaciones de ciberseguridad con las siguientes misiones:

- Garantizar la seguridad de las infraestructuras, comunicaciones y servicios digitales prestados por las Administraciones Públicas.
- Constitución del Centro de Operaciones de Ciberseguridad (COCS) para toda la AGE y sus organismos públicos, de protección frente a amenazas de ciberseguridad.

- Monitorizar los principales indicadores en el ámbito de la ciberseguridad a través de un cuadro de mando y fomenta así las sinergias con otros organismos europeos en esta materia.

2.3.4 Plan nacional de Ciberseguridad

Figura 2-2 Logo del Plan Nacional de Ciberseguridad. Fuente: [11]

Estrategia aprobada por el gobierno de España el 29 de marzo del 2022 en consejo de ministros, que tiene como principal objetivo el de concretar, a través de actuaciones y proyectos específicos, para los tres próximos años, medidas recogidas en la Estrategia Nacional de Ciberseguridad 2019.

El Plan contiene más de 130 actuaciones, cuya implementación asciende a un importe total de 1000 millones de euros. Una parte importante de ellas ya tienen adjudicada su financiación. El resto se ejecutará en años próximos, una vez se disponga de los recursos económicos necesarios. Una gran parte de las medidas incluidas en el plan están vinculadas al Plan de Recuperación, Transformación y Resiliencia. Uno de los logos fácilmente reconocibles de dicho plan, es el que aprece en la figura 2-2.

2.3.5 Esquema Nacional de Seguridad (ENS)

El Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad sustituye al Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la administración electrónica.

El Real Decreto 311/2022 actualiza el Esquema Nacional de Seguridad (ENS) para:

- Primero, alinear el ENS con el marco normativo y el contexto estratégico existentes para garantizar la seguridad en la Administración Digital. Para lograrlo, se clarifica el ámbito de aplicación del ENS y se actualizan las referencias al marco legal vigente, de manera que se simplifiquen y armonicen los mandatos del ENS.
- Segundo, introducir la capacidad de ajustar los requisitos del ENS para garantizar su adaptación a la realidad de ciertos colectivos o tipos de sistemas, atendiendo a la semejanza de los riesgos a los que están expuestos sus sistemas de información.
- Tercero, reforzar la protección frente a las tendencias en ciberseguridad mediante la revisión de los principios básicos, los requisitos mínimos y las medidas de seguridad que deben adoptarse por las entidades sujetas al ENS.

Los sistemas afectados deberán adecuarse a lo dispuesto en el real decreto en un plazo de veinticuatro meses contados a partir de su entrada en vigor.

Objetivos:

- Crear las condiciones necesarias de seguridad en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos, que permita el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.
- Promover la gestión continuada de la seguridad.
- Promover la prevención, detección y corrección, para una mejor resiliencia en el escenario de ciberamenazas y ciberataques.
- Promover un tratamiento homogéneo de la seguridad que facilite la cooperación en la prestación de servicios públicos digitales cuando participan diversas entidades. Esto supone proporcionar los elementos comunes que han de guiar la actuación de las entidades del Sector Público y de sus proveedores tecnológicos en materia de seguridad de las tecnologías de la información.
- Servir de modelo de buenas prácticas, en línea con lo apuntado en las recomendaciones de la OCDE Digital Security Risk Management for Economic and Social Prosperity OECD Recommendation and Companion Document.

2.3.6 Reglamento del Parlamento Europeo

Cabe reseñar en este apartado, para dar un mayor realce o énfasis de la importancia del asunto a tratar en este TFM que, en el mes de septiembre del 2022, en el seno de la Unión Europea, se ha emitido una propuesta de Reglamento del Parlamento Europeo y del Consejo, relativo a los requisitos horizontales de ciberseguridad para los productos con elementos digitales y por el que se modifica el Reglamento (UE) 2019/1020. Dicha propuesta que ya está lo sufrientemente trabajada y consensuada con los estados miembros será aprobada en breve, y será de total aplicación en la UE.

El objetivo fundamental de este reglamento será el establecer:

- Normas para la introducción en el mercado de productos con elementos digitales a fin de garantizar la ciberseguridad de dichos productos.
- Requisitos esenciales para el diseño, el desarrollo y la fabricación de productos con elementos digitales y las obligaciones de los operadores económicos en relación con dichos productos, en lo que respecta a la ciberseguridad.
- Requisitos esenciales para los procesos de gestión de la vulnerabilidad establecidos por los fabricantes para garantizar la ciberseguridad de los productos con elementos digitales a lo largo de todo el ciclo de vida, y las obligaciones de los operadores económicos en relación con dichos procesos.
- Normas relativas a la vigilancia del mercado y a la aplicación de los requisitos y las normas antes mencionados.

Todo ello con la finalidad de armonizar y racionalizar el panorama normativo de la UE mediante la introducción de requisitos de ciberseguridad para los productos con elementos digitales y evitar el solapamiento de requisitos establecidos en diferentes actos legislativos.

La adopción de este Reglamento favorecerá una mayor seguridad jurídica para los operadores y los usuarios de toda la Unión, así como una mejor armonización del mercado único europeo, y establecerá condiciones más viables para los operadores que desearan acceder al mercado de la UE.

Su ámbito de aplicación es a los productos con elementos digitales cuyo uso previsto o razonablemente previsible incluya una conexión de datos directa o indirecta, lógica o física, a un dispositivo o red. Quedando exentos los regulados por el Reglamento (UE) 2017/745, el Reglamento (UE) 2017/746, el Reglamento (UE) 2019/2144, y el Reglamento (UE) 2018/1139.

Para dar contenido y entender el Reglamento en cuestión hay que dar respuesta a las siguientes preguntas, y que son emitidas en el informe que emite el grupo de trabajo que ha desarrollado el borrador:

¿Cuál es el problema y por qué es un problema en la UE?

Los productos consistentes en equipos informáticos (hardware) y programas informáticos (software) a menudo se enfrentan a ciberataques llevados a cabo con éxito, lo que eleva el coste anual mundial estimado de la ciberdelincuencia a 5,5 billones EUR en 2021. Estos productos enfrentan dos problemas principales que suponen costes adicionales para los usuarios y la sociedad: 1) un bajo nivel de ciberseguridad, que se refleja en vulnerabilidades generalizadas y en la oferta insuficiente e incoherente de actualizaciones de seguridad para hacerles frente, y 2) una comprensión de la información y un acceso a ella insuficientes por parte de los usuarios, lo que les impide elegir productos con las características de ciberseguridad adecuadas o utilizarlos de manera segura.

La ciberseguridad de los productos con elementos digitales tiene una importante dimensión transfronteriza, ya que los productos fabricados en un país a menudo se utilizan en todo el mercado interior. Además, es habitual que los incidentes que inicialmente afectan a una única entidad o Estado miembro se expandan en minutos a todo el mercado interior.

Si bien la legislación vigente sobre el mercado interior se aplica a determinados productos con elementos digitales, actualmente la mayoría de los productos consistentes en equipos informáticos y programas informáticos no están contemplados en ninguna norma de la Unión Europea (UE) que regule su ciberseguridad. En particular, el marco jurídico actual de la UE no aborda la ciberseguridad de los programas informáticos no incorporados, aun cuando los ataques de ciberseguridad se centran cada vez más en las vulnerabilidades de estos productos, lo que genera considerables costes sociales y económicos. Algunos ejemplos recientes son el programa espía Pegasus, que aprovechó vulnerabilidades en teléfonos móviles, o el programa de chantaje de tipo gusano WannaCry, que explotó una vulnerabilidad Windows y afectó a ordenadores de todo el mundo.

¿Qué se pretende conseguir?

Se identificaron dos objetivos principales para garantizar el correcto funcionamiento del mercado interior: 1) crear condiciones que permitan el desarrollo de productos con elementos digitales seguros, garantizando que los productos consistentes en equipos informáticos y programas informáticos se introduzcan en el mercado con menos vulnerabilidades y que los fabricantes se tomen en serio la seguridad a lo largo de todo el ciclo de vida de un producto; y 2) crear condiciones que permitan a los usuarios tener en cuenta la ciberseguridad a la hora de elegir y utilizar productos con elementos digitales. Se establecieron cuatro objetivos específicos: i) garantizar que los fabricantes mejoren la seguridad de los productos con elementos digitales desde la fase de diseño y desarrollo y a lo largo de todo el ciclo de vida; ii) garantizar un marco de ciberseguridad coherente y facilitar su cumplimiento por parte de los fabricantes de equipos y programas informáticos; iii) mejorar la transparencia de las características de seguridad de los productos con elementos digitales; y iv) permitir a las empresas y a los consumidores utilizar productos con elementos digitales de forma segura.

¿Cuál es el valor añadido de la actuación de la UE en este ámbito (respecto a la subsidiariedad)?

La importante naturaleza transfronteriza de la ciberseguridad y el aumento de los incidentes, cuyas repercusiones pueden extenderse a otros países, sectores y productos, hacen que los Estados miembros por sí solos no puedan alcanzar eficazmente los objetivos planteados. Habida cuenta de la dimensión mundial de los mercados de los productos con elementos digitales, los Estados miembros hacen frente en su territorio a los mismos riesgos para un mismo producto con elementos digitales. El mosaico de normas nacionales con posibles divergencias que está surgiendo corre el riesgo de poner barreras a un mercado único abierto y competitivo para los productos con elementos digitales. Por lo tanto, se hace necesaria la acción conjunta a escala de la UE para aumentar el nivel de confianza entre los usuarios y el atractivo de los productos con elementos digitales introducidos en el mercado de la UE. La acción conjunta también beneficiaría al mercado interior al proporcionar seguridad jurídica y condiciones de competencia equitativas para los fabricantes de productos con elementos digitales.

Bruselas, 15.9.2022
COM(2022) 454 final

2022/0272 (COD)

Propuesta de

REGLAMENTO DEL PARLAMENTO EUROPEO Y DEL CONSEJO

relativo a los requisitos horizontales de ciberseguridad para los productos con elementos digitales y por el que se modifica el Reglamento (UE) 2019/1020

(Texto pertinente a efectos del EEE)

{SEC(2022) 321 final} - {SWD(2022) 282 final} - {SWD(2022) 283 final}

Figura 2-3 Portada del Reglamento UE. [Elaboración Propia]

3 DESARROLLO DEL TFM

3.1 Introducción

Como ya se establecía con antelación en cuanto a la pretensión de este TFM, su objetivo no es el de ser un trabajo de interés técnico o dedicado sólo para expertos en materia de la ciberseguridad, sino que pretende ser una guía o referencia de inicio, para todos aquellos neófitos o interesados en este mundo tan apasionante, que pretendan abordar el entendimiento de la ciberseguridad sin ninguna otra referencia de partida.

Es por lo que ha sido necesario extenderse en cierto modo en la redacción del capítulo estado del arte, al objeto de que proporcione al interesado o neófito lector, una sólida base de conocimientos básicos en materia de ciberseguridad, que no solo le habrá su apetito por adentrarse en adquirir más conocimientos, sino que además le permitan seguir el hilo conductor que se va a ir desarrollando en la consecución del trabajo.

Es necesario reseñar que los datos aportados y contenidos en el presente ensayo son genéricos, en base a experiencias, análisis y estudios del autor, refrendados con opiniones de especialistas en la materia, pero que sin centrarse en ningún órgano en concreto, podrían extrapolarse a un gran número de administraciones o empresas de características similares, de forma total o parcial.

Todos los datos en los contenidos son de dominio público y accesible por las diferentes fuentes de información consultadas y referenciadas en el apartado correspondiente de la bibliografía.

Del mismo modo hay que señalar que la difusión parcial o total del contenido del mismo, debe ser solicitada al dueño titular de los derechos de autor sobre el documento, en su momento de publicitación.

3.2 Redes de una gran corporación

Para entender el mundo que abarca o mejor dicho sobre el que actuaría la ciberseguridad en el presente trabajo, lo primero que hay que delimitar es éste, o al menos intentar que el mundo sea de alguna forma tangible, medible bajo ciertos parámetros, o al menos entendible, o reconocible por su estructura.

No tendría sentido hablar de ciberseguridad, sus políticas, estructuras y organizaciones, y herramientas aplicadas a la red de Internet global, y mucho menos a un simple ordenador desplegado en un domicilio para uso familiar.

En el caso que nos compete, la red de la corporación se compondría a modo de ejemplo de:

- Una WAN de empresa distribuida en múltiples sucursales nacionales e internacionales.
- Conexiones a Internet a través de un NODO frontera que hace de DMZ, estando esas conexiones contratadas a un proveedor de servicios.
- Interconexiones a otras empresas de un mismo *Holding*, con las que comparte determinados servicios (intranet administrativa).
- Que dispone de 3 CPDS propios, que actúan de respaldo entre sí.
- Realiza copias de seguridad sobre icloud privada e icloud pública.
- Tiene contratados servicios en icloud en modo SaaS.
- Emplea conexiones VPN con los empleados remotos.
- Tiene varias páginas web públicas para su negocio.

- Son unos 40000 empleados en más de 500 sedes.

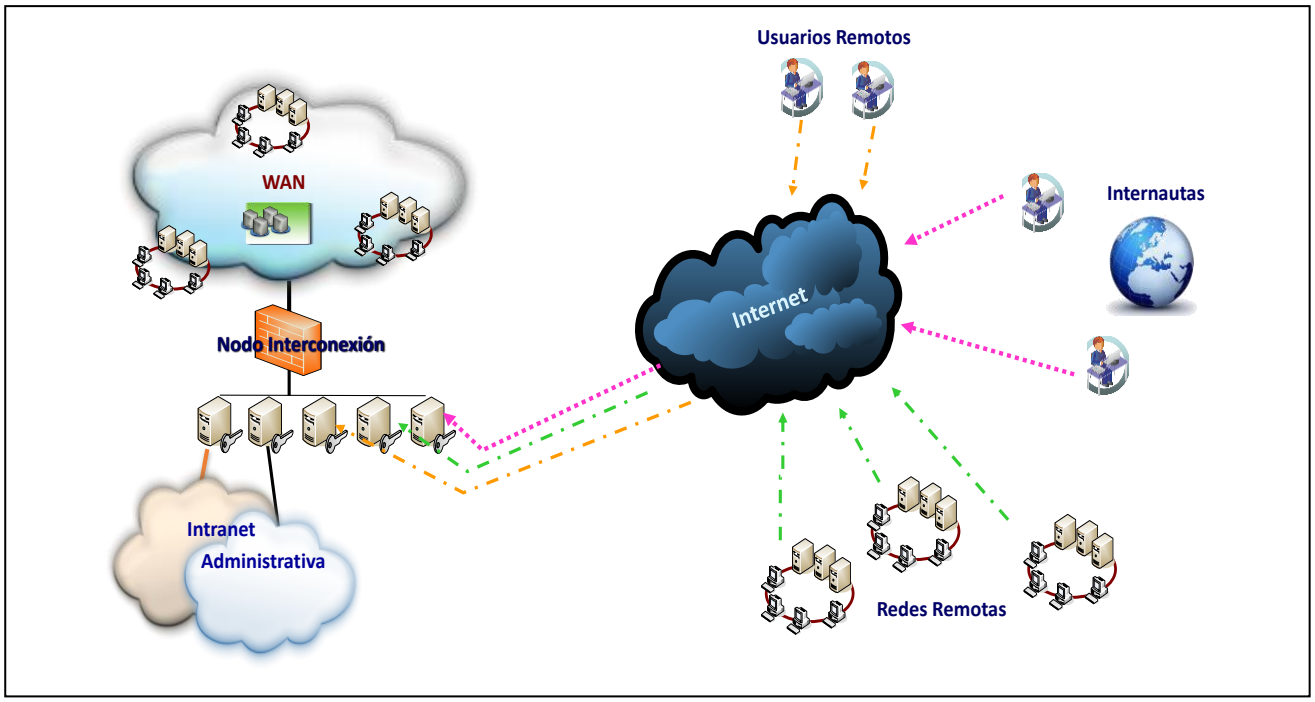


Figura 3-1 Red de una gran organización. [Elaboración Propia]

Esta red de la corporación tendría varias capas de seguridad a modo de piel de cebolla, las cuales le van confiriendo distintos niveles de protección o seguridad y sobre los cuales se van implementando las diferentes herramientas de ciberseguridad. Pero por simplificar más el ámbito de análisis desarrollado en el TFM, hablaremos de una superficie de exposición interna, y una superficie de exposición externa a proteger.

La superficie interna, estaría compuesta por todos los activos (servidores y equipos de usuario), componentes de red, dispositivos IoT, servicios, aplicaciones, sistemas y DMZ.

La superficie externa sería la que alberga la intranet administrativa, los usuarios externos y sedes remotas, así como los servicios como icloud o web contratados, desplegados en Internet y que son de terceros, pero que deben ser protegidos, dado que la información que obra en su poder es de la empresa que los contrata.

En este tipo de organizaciones tan extensas y complejas, evidentemente para que estén seguras no solo basta con implementar y atender a la ciberseguridad, ya que esta no es suficiente por sí sola, sino que además hay que desplegar paralelamente las políticas y elementos de la ciberdefensa. Y aunque no es objeto de estudio en este trabajo, se hace necesario exponer una serie de consideraciones, que servirán para entender mucho mejor el porqué de la importancia de la ciberseguridad.

Aunque ya se trató su definición en el anterior capitulo, una explicación simple y lógica que nos hace más fácil su comprensión, y lo que le diferencia y entrelaza con la ciberseguridad, sería la de explicarlo analizando como si se tratase de un sistema de misiles antiaéreo.

Groso modo un sistema de misiles antiaéreo se compone de una dirección de tiro, que dirige las órdenes de fuego y el guiado de los misiles, un radar de control 3D (tridimensional) de largo alcance, y los lanzadores de misiles propiamente dichos. La red a proteger seria el territorio Nacional.

En este caso la seguridad de que no vamos a ser atacados no es total, pero el efecto disuasorio de ver el sistema desplegado y operativo vigilante en todo momento, ya proporciona bastante seguridad. Eso podría identificarse con la ciberseguridad, que no tiene por qué disparar los misiles sino simplemente estar alerta, pero con todo preparado. Evidentemente el sistema esta vigilante en todo momento, tanto la dirección de tiro como el radar, lo que identificaría como el trabajo conjunto de ambas disciplinas ciberdefensa y ciberseguridad. Pero no será hasta el momento que se detecta el ataque, cuando se aplique la defensa, es decir se lanzan los misiles y se guían al objetivo, lo cual sería ya el trabajo de la ciberdefensa.

Con este ejemplo aunque muy simplista, lo que se quiere mostrar es que tanto ciberseguridad como ciberdefensa, están operando paralelamente en todo momento. Una disuade, analiza situaciones y evita enfrentamientos, mientras que la otra responde y en este caso contraataca defendiendo. Pero algo más importante es señalar que muchas de las herramientas se comparten, aunque tienen una finalidad diferente y pueden aplicarse simultanea o en diferentes momentos.

Como puede verse en el ejemplo, no se ha atribuido un componente de forma clara a ninguna de las áreas, sino que son las acciones, y en definitiva la misión de cada componente las que trabajan en un área u otra.

Si bien es verdad que también hay que aclarar que, en la práctica hay herramientas diseñadas para uso en ciberseguridad y otras para ciberdefensa, lo cual daría motivo para otro trabajo haciendo una comparación entre las mismas, pero que no se abordará a lo largo de este TFM.

3.3 Políticas de Ciberseguridad, su diseño y su implementación

La ciberseguridad en el mundo es entendida de forma muy similar, por todo el que trabaje o se vea condicionado o afectado por ella, pero esto no significa que la solución implementada o en síntesis la aplicación de las políticas de ciberseguridad sean las mismas, ni tan si quiera parecidas, y esto se debe a que hay que valorar otros muchos factores que tienen que ver con la misma.

Estos varían desde la naturaleza del negocio, tipo y numero de activos manejados, amplitud de la organización en extensión y número de empleados, sensibilidad de la información manejada, o los requisitos de confidencialidad, disponibilidad, autenticidad, integridad de la misma, y otros muchos más.

En el caso de una gran organización, no así en las pequeñas, y dada la trascendencia de las TIC en el momento en el que nos encontramos, se da por hecho que el departamento que las trata, junto por supuesto con el tema de la ciberdefensa, debe estar adecuadamente dimensionado. Es por lo que se asume que las políticas son desarrolladas íntegramente en la empresa, salvo alguna necesidad puntual, motivo por el que deben generar toda la documentación que a continuación se expone.

En el caso de pequeñas empresas, es lógico generalizar que el diseño y aplicación de la ciberseguridad se deje en manos de terceros contratados para tal fin, o que se empleen los mecanismos que proporciona el Estado, en beneficio de la ciberseguridad de las PYMES, en este caso se refiere al INCIBE-CERT, y a las demás entidades de la administración general del Estado correspondiéndole al COCS de la SGAD (secretaria general de la administración digital) de la AGE.

Por ser interesante para conocer la magnitud y tipo de medidas adoptadas en materia de ciberseguridad, adjunto se enumeran las capacidades con las que se dota a este último COCS.

Capacidades del COCS del AGE.

- Prevención de incidentes de ciberseguridad
    - Análisis de vulnerabilidades automatizado
    - Pruebas de seguridad de Caja Gris

    - Prueba de seguridad de Caja Negra
    - Análisis de seguridad de código
    - Pruebas de seguridad de Caja Blanca
    - Vigilancia digital
- Protección de la seguridad
    - Seguridad perimetral
    - Navegación limpia
    - Correo limpio
    - Acceso remoto seguro
- Detección de incidentes de ciberseguridad
    - Provisión de un EDR
    - Monitorización de eventos de seguridad
    - Detección de incidentes de seguridad
    - Búsqueda proactiva de amenazas
    - Detección de fuga de información
    - Servicios de alerta temprana
- Gestión y respuesta ante incidentes de ciberseguridad
    - Soporte a la gestión
    - Análisis forense
    - Laboratorio de análisis malware
    - Copia y descifrado de trafico de internet.
- Asesoramiento especializado en ciberseguridad
    - Asesoramiento legal
- Apoyo a la gestión de ciberseguridad

Por lo expuesto anteriormente se tienen que fijar unos **planes de actuación** en materia de seguridad de la empresa, diseñados desde la alta dirección, en la que deben participar en una comisión interdepartamental, en la que lo conveniente sería que participase el CEO, pero en la que como mínimo debe participar el CIO *(Chief Information Officer*) de la empresa, en el que además de otras parcelas relativas a la seguridad personal, documental, de instalaciones debe diseñarse los objetivos estratégicos que seguirá el plan general sobre ciberseguridad, que en el caso de organizaciones como el MINISDEF se denomina área SEGINFOSIT.

De ese plan de actuación se derivan los **planes de acción** que ya son los que desarrollan los objetivos establecidos en el plan de actuación, desgranándolos en una serie de líneas de acción a seguir, adecuadas eso si a un margen de tiempo fijado por años o a una situación determinadas. Esto quiere decir, que tanto los planes de actuación como los planes de acción, son temporales y deben fijarse por periodos de tiempo establecidos de antemano.

Una posible solución es fijar una temporalidad de entre 5 y 6 años para los planes de actuación, teniendo que ser ajustados o revisados cada 2 -3 años, mientras que los planes de acción deben revisarse cada año, al objeto de poder mesurar de forma más clara los progresos, las carencias, o las necesidades sobrevenidas.

Cabe destacar que para el caso concreto de algún tipo de situación excepcional, que ocupa un breve espacio de tiempo o que afecta a un grupo limitado de activos o segregados del resto, sería aconsejable diferenciar su tratamiento del resto y realizar una especie de plan de acción exprés, o diseñado exprofeso, por un margen de tiempo inferior a un año, motivo por el que no debería ser considerado como un plan de acción normal.

Derivado de los **planes anuales de acción**, habría que desarrollar lo que se considera documentación de segundo y tercer nivel, siendo la de segundo las guías de aplicación de la seguridad planeada, en este caso **guías de ciberseguridad**, y las **instrucciones técnicas**, que serían los documentos de tercer nivel, pensados para descender en la definición de acciones pero ya a un nivel muy técnico.

Para el caso de las guías de ciberseguridad, se trata de dar unas normas mínimas de actuación y comportamiento de los usuarios, dado que son el eslabón más débil de la cadena y son el objetivo de multitud de diferentes tipos de ataque.

Muchas veces esas guías son simplemente **panfletos** como el que se muestra en la figura 3-2, correos o anuncios de normas de comportamiento ante algún ataque identificado, y otras veces se materializarán en campañas diseñadas exprofeso ante situaciones especiales, aunque la gran mayoría son parte del desarrollo de las líneas de actuación del plan de actuación de ciberseguridad de la empresa.

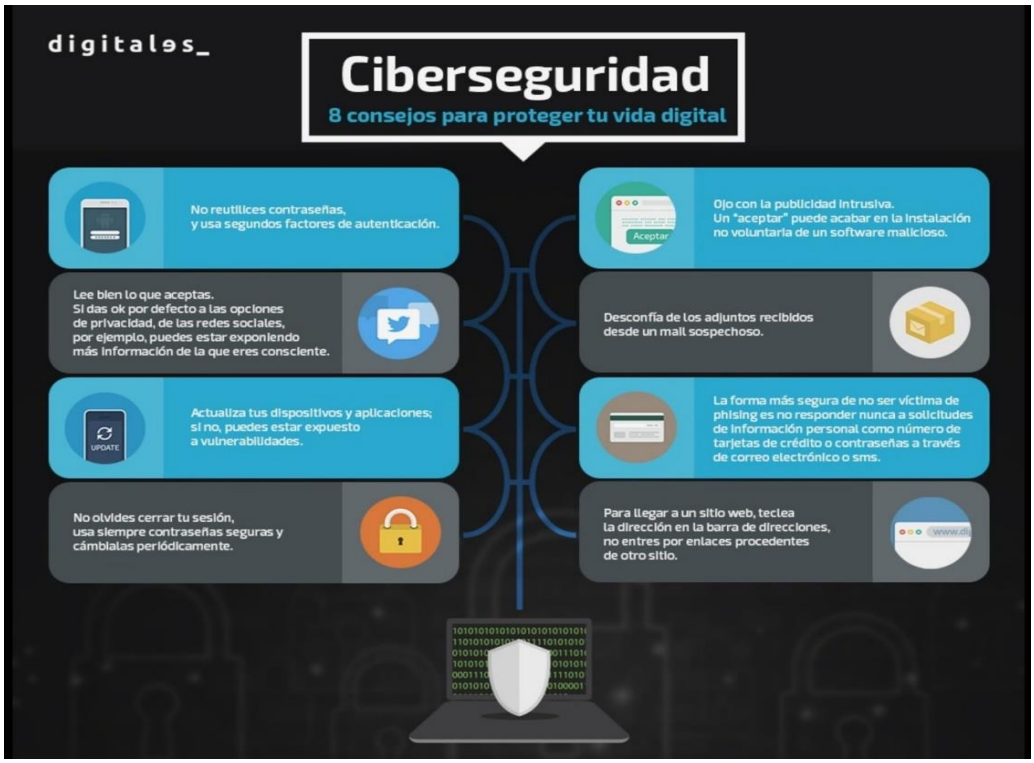


Figura 3-2 Ejemplo de panfleto. Fuente [12]

En resumen partiendo del modelo de negocio en cuestión y de la dirección de la empresa, se deben elaborar una serie de documentos fundamentales para desplegar la política de ciberseguridad y estos son la propia política de seguridad de la empresa, el plan de actuación para implementar esa política, los planes de acción que desarrollan el plan anterior, siendo el de ciberseguridad el que nos compete en este TFM, planes exprés en su caso, guías de aplicación de la ciberseguridad e instrucciones técnicas de ciberseguridad.

Existen también otros documentos emitidos por organizaciones como el CCN, que sirven de apoyo en materia de ciberseguridad como son los **cuadernos de ciberseguridad** representado en la figura 3-3, al objeto de extender la cultura de ciberseguridad entre los usuarios, desarrollar y colaborar en acciones de sensibilización, formación, divulgación y buenas prácticas de seguridad.

Figura 3-3 Cuadernos. Fuente: [13]

Aunque no son propiamente dichas como políticas de ciberseguridad en exclusividad, dado que afectan también a otras áreas de la organización, pero por su especial relevancia es necesario referir en este TFM la **política de salvaguarda de datos**, **copias de seguridad** y en algunos casos también conocidos como *Golden Copy*, y **la política de segmentación de la red**.

El correcto almacenamiento de la información es un proceso vital en la operación de cualquier organización. Es por ello que, la gestión de las copias de seguridad supone el punto de partida para garantizar la disponibilidad de la información, debiéndose implementar las medidas necesarias para garantizar su acceso.

Asegurar el acceso a la información en cualquier momento y bajo cualquier circunstancia, es un proceso que requiere un correcto alineamiento y despliegue de medidas de seguridad, incluyendo medidas organizativas, la gestión de las copias de seguridad y sus medidas de seguridad, atendiendo además a su creación, restauración, transporte, almacenamiento etc, son procesos necesarios que deben definirse y documentarse adecuadamente, en aras a desarrollar los planes de contingencia y continuidad de servicio, sin perjuicio de los pertinentes planes de recuperación ante desastres.

Es por ello que dicha política deberá centrarse en:

- La gestión de las réplicas de datos (o copias de seguridad) que se realizan sobre los datos del negocio (datos alojados en las bases de datos de las aplicaciones o los sistemas de información).
- Definir las medidas de seguridad, tanto físicas como lógicas, que deben implementarse sobre las copias de seguridad.
- Establecer una política de copias de seguridad sobre la tipología de la información.
- Establecer los periodos mínimos de retención de la información, garantizando de esta manera el correcto cumplimiento de la normativa vigente.
- Esta política afectará a los datos que estén tanto en instalaciones internas como en externas, así como en la nube.

Además esta política debería definir:

- Tipos de copia de seguridad.

- Periodicidad.
- Lugar de almacenamiento.
- Formato de las copias de seguridad.
- Procedimiento de validación de las copias de seguridad.

La política de segmentación de la red se establece fundamentalmente para evitar que la red sea plana, y que un posible atacante pueda aprovechar esa vulnerabilidad en el inadecuado diseño de la red, para realizar ataques mediante desplazamientos laterales fundamentalmente, que de haber estado segmentadas hubieran sido muy difíciles de llevar a cabo.

La segmentación por resumirlo de una forma simple consistiría en la creación de múltiples vlan destinadas a diferentes propósitos, de tal manera que, aunque se hubiera producido un determinado ataque sobre un activo de una determinada vlan, este no podría replicarse sobre otras partes más sensibles de la organización donde hubiese activos fundamentales como servidores de correo, controladores de dominio, balanceadores, servidores de impresión, gestores de identidades, servidores web, etc.

Por lo general esta política tiene mucho interés para empresas con múltiples delegaciones, departamentos, o de grandes dimensiones en general, no siendo tan necesaria para pequeñas organizaciones, con apenas sedes remotas.

3.4 Marco de gobernanza y estructuras

En el anterior apartado se expuso como se materializa en documentos esa política de ciberseguridad a implementar, es por ello que siguiendo una estructura lógica en el hilo conductor de este TFM, parece necesario establecer, sobre que estructuras organizacionales debiera descansar esa política, en resumen en que marco de gobierno gobernanza nos estamos moviendo.

Con ello no quiere darse a entender que solo exista una estructura fija o que no haya más posibilidades, sino que se quiere mostrar al menos una de las que funcionan, por estar pensada para hacer frente a situaciones que ya se han planteado en la realidad, o que sin haberse producido al menos han sido ensayadas con éxito.

Este marco debe contar con al menos tres estructuras u órganos diferenciados, siendo el más alto el de **dirección**, uno intermedio el de **control y coordinación**, y el más bajo el de **operación y resolución**. Todos ellos forman parte de una organización que si bien es verdad tiene la típica estructura piramidal, la forma de integrarse en estos órganos deberá ser fundamentalmente transversal, es decir formados por miembros de todos los departamentos, con la intención de que la resolución de las acciones sea tratada de forma capilarizada, profunda, ágil y dinámica, sin los típicos cuellos de botella.

3.5 Órgano de dirección

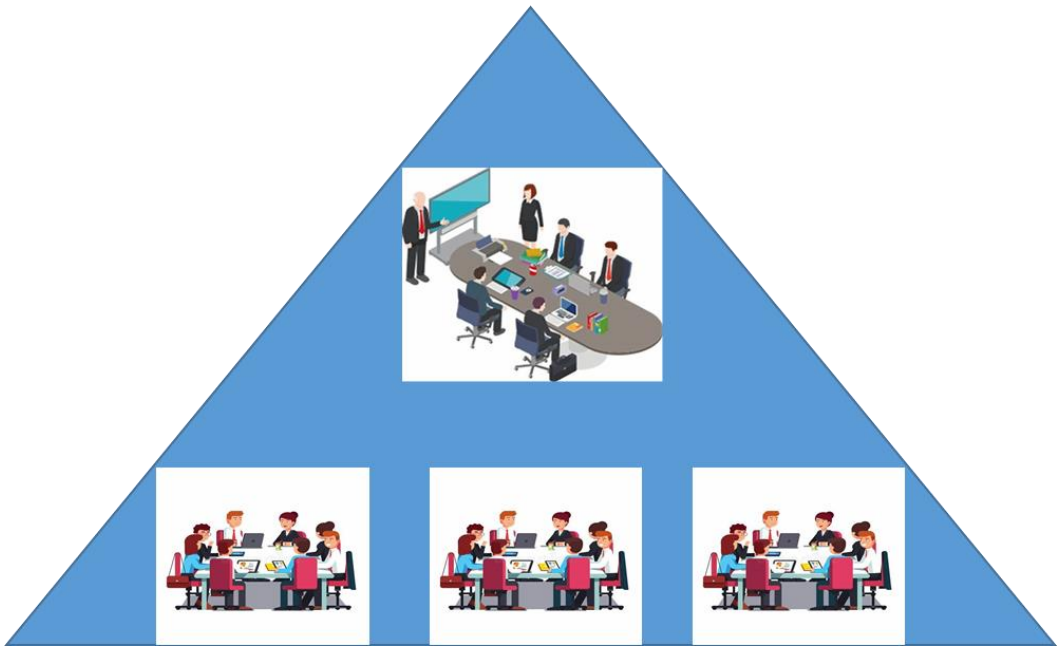


Figura 3-4 Órgano de dirección, de control y coordinación. Fuente: [4]

El órgano de dirección, estaría constituido por un grupo de personas, con capacidad de tomar decisiones importantes tanto en materia económica, de nivel de servicio o productivo, como de decisión en materia de seguridad en la empresa. En no pocas ocasiones, por necesidad de acometer un ciberincidente ocurrido en la organización, será necesario que la totalidad de la actividad incluyendo la productiva, deba ser paralizada.

Este hecho afecta tanto a temas económicos, ya sea por la disminución de la producción, o porque haya que adoptar una solución que requiera de un desembolso económico de cierta magnitud, a la vez que también se tendrán que tomar decisiones relativas a la seguridad, en el caso de que por ejemplo la información se vea afectada de alguna forma, o incluso se vea afectado el normal funcionamiento de las TIC.

Aunque la composición no está definida, parece lógico que esta estructura esté dirigida por el CEO o un directivo de su confianza, junto con directivos de otros departamentos o áreas, entre los cuales si debe aparecer como miembro obligado el CIO y muy probablemente el director de asuntos económicos.

3.6 Órganos de control y coordinación

Los órganos de control y coordinación pueden ser uno o varios como el que aparece representado en la figura 3-4, en función de la entidad de la organización, en este caso hablaremos de dos de ellos, el de coordinación que sería un órgano formado por representantes de diferentes secciones o departamentos de la organización, que también es conocido como el “comité de crisis” y el órgano de control que sería el SOC.

Figura 3-5 SOC de una gran organización. Fuente: [4]

El SOC o Centro de Operaciones de ciberseguridad, es el lugar de la organización donde se centraliza la gestión de la práctica totalidad de las herramientas y desde donde se controla la situación de ciberseguridad, en la figura 3-5 aparece una posible recreación de uno de ellos. Éste podría definirse como un grupo de personas que de forma centralizada, actúan sobre procesos y tecnologías, con el objetivo de proteger los sistemas y redes, mediante la monitorización, detección, prevención y análisis continuos de las ciberamenaza a las que puede estar sometida la organización. Los SOC analizan toda la actividad del sistema y funcionan de forma muy similar en todas las organizaciones. Al detectar amenazas a través de un conjunto de procesos, herramientas y soluciones tecnológicas, pueden descubrir y responder rápidamente a cualquier amenaza y / o ataque.

Los equipos que integran generalmente pueden definirse en tres grupos:

- Directores o supervisores: Se encargan de dirigir y supervisar el equipo, crean procesos y acciones y avalúan las respuestas.
- Analistas: Detectan, analizan y responden a amenazas, e implementan las soluciones propuestas por la dirección.
- Ingenieros o técnicos: Mantienen y explotan las herramientas y sistemas de seguridad.

Por la ubicación del SOC pueden ser internos y externos.

Los internos pertenecerían a la propia organización, y a su vez éstos podrían ser puros con todo su personal perteneciente a la organización, o híbridos si ciertos servicios están proporcionados por personal externo a la organización contratado para una determinada función. Por otro lado estarían los SOC externos, que serían igualmente puros si están subcontratados mediante servicios a otra empresa externa especializada en el asunto, fuera de la propia organización, o híbridos si alguna tarea es realizada internamente dentro de la organización.

Ambas modalidades presentan ventajas e inconvenientes siendo las más reseñables las siguientes:

SOC externo

Ventajas

- Ya no es necesaria una fase de capacitación y tienen acceso directamente a la experiencia.
- No necesitan un tiempo de implementación demasiado amplio.
- Los equipos que lo forman, usan herramientas especializadas que conocen en profundidad.
- Al estar experimentados y especializados son escalables.
- Monitorizarán generalmente 24x7.
- Siguen amenazas e innovan a la vez que los propios atacantes, realizando servicios de inteligencia de amenazas.
- El coste es más reducido que un interno.

Inconvenientes

- No tienen el mismo grado de conocimiento de las infraestructuras internas de la organización, que sí tendría un equipo dedicado que fuese de la propia organización.
- Se está facilitando acceso a información a terceros, aumentando así la superficie de ataque, y el riesgo para la organización.

SOC interno

Ventajas

- No se facilitan datos a terceros, como información o estabilidad de la red.
- El equipo está familiarizado y motivado con la seguridad de la organización.
- Todos los procesos de resolución se hacen a nivel interno, siendo la comunicación interna mucho más ágil y rápida.
- La inteligencia, amenazas y soluciones, quedan aprendidas y almacenadas dentro de la organización.
- Las herramientas y estrategias de seguridad son personalizadas para adaptarse a la organización.

Inconvenientes

- El coste de crear e implementar un equipo desde cero es mucho más elevado.
- Preparar a un equipo lleva mucho tiempo en formación y capacitación.
- Si no se dispone de una herramienta integradora de las demás herramientas de ciberseguridad desplegadas, dada su propia heterogeneidad, esto provocará que el tiempo de acción para resoluciones, sea más elevado.

3.7 Órganos de operación y resolución

Una vez más hay que diferenciar que en función del tamaño y complicación de la organización, este tercer órgano podría estar integrado dentro del propio SOC, formado parte del equipo aunque bajo la dependencia de un responsable diferenciado del director del SOC, debido a que su misión principal es la gestión y supervisión de la red y de los servicios que se despliegan sobre la misma, pero no en materia exclusiva de seguridad de la red.

Aunque también podría constituirse con el personal integrante del departamento TIC, al que se le comunicarían las acciones necesarias que se deberían desarrollar para paliar algún ciberincidente, o también para contribuir a la correcta implementación de la política de ciberseguridad. Cuando estos

órganos están separados, forman parte de lo que se conocen como CEGES, o centro de gestión de servicios.

Pero igualmente hay que señalar que puede ocurrir lo contrario, es decir que el CEGES dada su dimensión y como órgano base de la creación de la infraestructura TIC de la organización, tenga un órgano interno que se dedique a la ciberseguridad.

No obstante esta no es la última posibilidad, dado que gracias a las múltiples opciones que se están dando con la contratación de servicios en la nube, en las diferentes modalidades, pudiera ocurrir que el propio departamento TIC ya pertenezca a un proveedor externo, lo cual no significa que el equipo no existiese en la estructura de gobernanza de una organización, sino que es de un tercero, con las ventajas y perjuicios que esto pudiera acarrear.

3.8 Guías de gestión de la ciberseguridad

Ya se expuso en el punto 3.3, que existían unas guías de aplicación de la política de ciberseguridad, pero estas no deben confundirse con las guías de gestión de ciberseguridad, que lo que definen es el procedimiento que debe seguirse para detectar, alertar, e informar sobre un ciberincidente, así como realizar la propia gestión de la resolución propiamente dicha, en la que además se define quién y cómo se debería participar en la citada resolución.

Estas acciones se plasman en lo que se conocen como **guías del plan de crisis, guías de notificación de incidentes y guías de gestión de incidentes**.

3.8.1 Guía del Plan de Crisis

Cuando las capacidades de una Organización deben ponerse a prueba para superar circunstancias excepcionales, es necesario disponer de los medios e instalaciones adecuados, de sistemas de comunicaciones e información seguras y confiables, así como del personal con los conocimientos, instrucción y la experiencia necesarios.

Todo ello debe quedar integrado, además, por unos procedimientos completos y sencillos que permitan optimizar los recursos disponibles, de manera que la organización supere la transición desde la situación de normalidad a la de crisis sin solución de continuidad, haciendo posible una rápida y eficaz adaptación del conjunto de la misma a la nueva situación.

El objeto del Plan de Crisis ante Ciberincidentes, es el de establecer la organización y procedimientos que adoptará la corporación en una situación de crisis, consecuencia de una amenaza cierta o de la materialización ya producida de cualquier ciberataque, identificando la forma de activación, las acciones y las responsabilidades de los elementos de su organización en esta nueva situación, recogiéndolos en el presente documento.

El Plan de Crisis es el procedimiento director de la gestión de la situación de crisis ante ciberincidentes de la organización, cuyo objetivo es facilitar la toma de decisiones y el seguimiento de las acciones consiguientes, mediante el adecuado y permanente conocimiento de la situación y de las opciones disponibles al respecto, estableciendo un ciclo de la decisión ágil y efectivo, adaptado a las circunstancias particulares de la crisis.

Debe ser distribuido entre los miembros de la organización que tengan “necesidad de conocer”, especialmente entre los miembros que conforman el Comité de Crisis ante ciberincidentes, sin perjuicio

de que se adopten las debidas garantías sobre los datos de carácter personal de los integrantes (identificación de los mismos, y números de contacto).

El Comité de Crisis ante ciberincidentes es el órgano encargado de la gestión de la crisis a alto nivel dentro de la organización. Es el órgano encargado de asesorar al CEO en la toma de decisiones y de coordinar las acciones necesarias para la prevención o la resolución de los incidentes que hayan sido calificados como crisis (grado de clasificación CRÍTICO/MUY ALTO de impacto y/o peligrosidad) o puedan tener este impacto en la organización, determinando o validando las estrategias de análisis, de prevención, contención y mitigación que permitan mantener o recuperar la normalidad en las operaciones en el menor tiempo posible.

Los principales cometidos del Comité de Crisis ante ciberincidentes son:

- Comprender el estado de situación y realizar una previsión de escenarios:
    - Evaluar toda la información recibida sobre la alerta o el incidente, realizar una valoración inicial de su impacto (real o potencial) y de las consecuencias sobre la entidad y las partes interesadas.
    - Mantener una previsión del impacto potencial y las consecuencias para la entidad, considerando los riesgos emergentes y los escenarios hacia donde puede evolucionar para poder acometer medidas de anticipación.
- Coordinar acciones y facilitar la toma de decisiones:
    - Supervisar las medidas implementadas y las decisiones tomadas previamente por los equipos de respuesta u otros comités operativos, asegurando que los procedimientos puestos en marcha para la resolución sean los más eficaces y eficientes.
    - Activar la movilización de recursos extraordinarios cuando sea preciso.
    - Hacer un seguimiento de las acciones en curso, manteniendo actualizando de manera permanente el documento correspondiente.
    - Actuar como centro de referencia de información durante la respuesta al incidente y su posterior recuperación, tanto ante los agentes internos como externos (Administración y otros) involucrados o concernidos por el incidente.
    - Asegurar las relaciones y la interlocución con todas las partes interesadas.
    - Asegurar una comunicación adecuada definiendo una estrategia de comunicación interna y externa, acorde a su misión, su propósito y sus valores, incluyendo las acciones de concienciación necesarias.
    - Designar el portavoz y asegurar que se llevan a cabo las medidas de comunicación previamente diseñadas, ya sea en medios, redes sociales, marcos asociativos, etc.
    - Velar por salvaguardar la confianza, la reputación y la imagen.
- Coordinar las acciones de vuelta a la normalidad y de análisis posterior al incidente:
    - Asegurar que se llevan a cabo las acciones pertinentes y dar por finalizada la crisis, una vez las condiciones estén cumplidas.
    - Extraer lecciones identificadas y elementos de mejora, como parte del proceso de Lecciones Aprendidas (LL.AA).

A continuación, se muestra un diagrama de las fases que conforman el Plan de Crisis ante ciberincidentes:

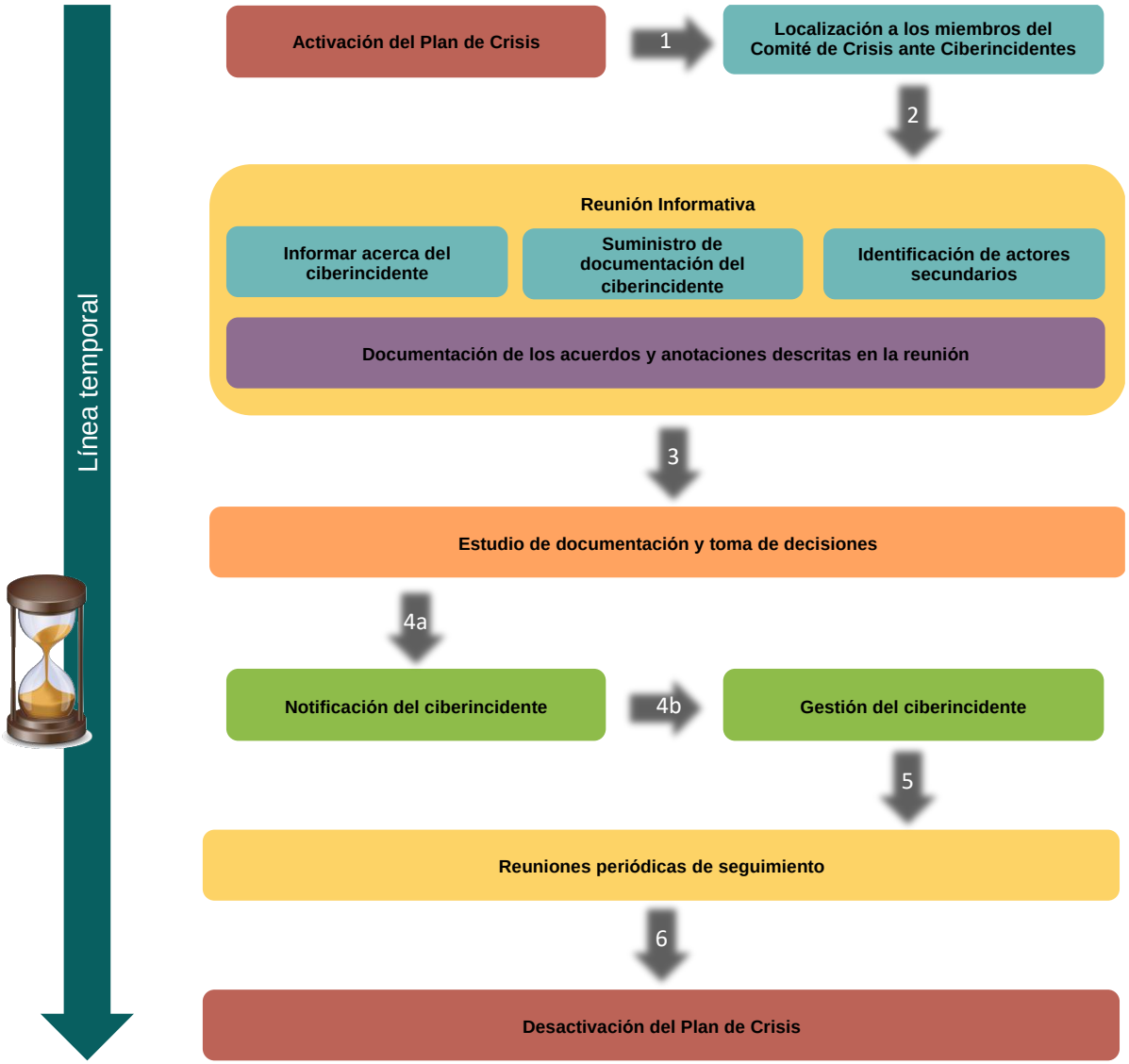


Figura 3-6 Plan de Crisis de una organización tipo. [Elaboración propia]

3.8.2 Guía de notificación de incidentes

El objeto del presente documento es establecer un marco de referencia en el ámbito de la detección, clasificación y notificación de ciberincidentes. Esto incluye la implantación de unos criterios mínimos exigibles y de obligaciones de informar en los casos que determine la legislación vigente.

La resolución de ciberincidentes de seguridad queda fuera del alcance del presente documento, correspondiéndole a la guía de gestión de incidentes.

La guía debe establecer el impacto de los incidentes de seguridad.

El impacto de los incidentes de seguridad, dependerá de la naturaleza del valor de la información comprometida. La valoración del impacto del incidente se realizará atendiendo a los siguientes parámetros:

- Impacto en la Seguridad de la organización y sus empleados.
- Efectos en la prestación de un servicio esencial o en una infraestructura critica.

- Tipología de la información afectada.
- Grado de afectación a las instalaciones de la organización.
- Posible interrupción en la prestación del servicio normal de la organización.
- Tiempo y costes propios y ajenos hasta la recuperación del normal funcionamiento de las instalaciones.
- Pérdidas económicas.
- Extensión geográfica afectada.
- Daños reputaciones asociados.

Los incidentes se asociarán a alguno de los siguientes niveles de impacto:

- CRÍTICO / MUY ALTO / ALTO / MEDIO / BAJO / SIN IMPACTO.

Todos los ciberincidentes cuya notificación sea preceptiva deben notificarse a través del sistema de ventanilla única de notificación. Para ello, el CCN-CERT ha creado la herramienta "Listado Unificado de Coordinación de Incidentes y Amenazas" (LUCIA).

A continuación se muestra un flujograma de las acciones a realizar para notificar un incidente.

Figura 3-7 Flujograma de notificación de incidentes. Fuente: [14]

3.8.3 Guía de gestión de incidentes

La presente guía desarrollará la contención, mitigación, recuperación y acciones post-incidente, de los ciberincidentes.

El ciclo de vida de gestión de un ciberincidente se compone de las siguientes fases:

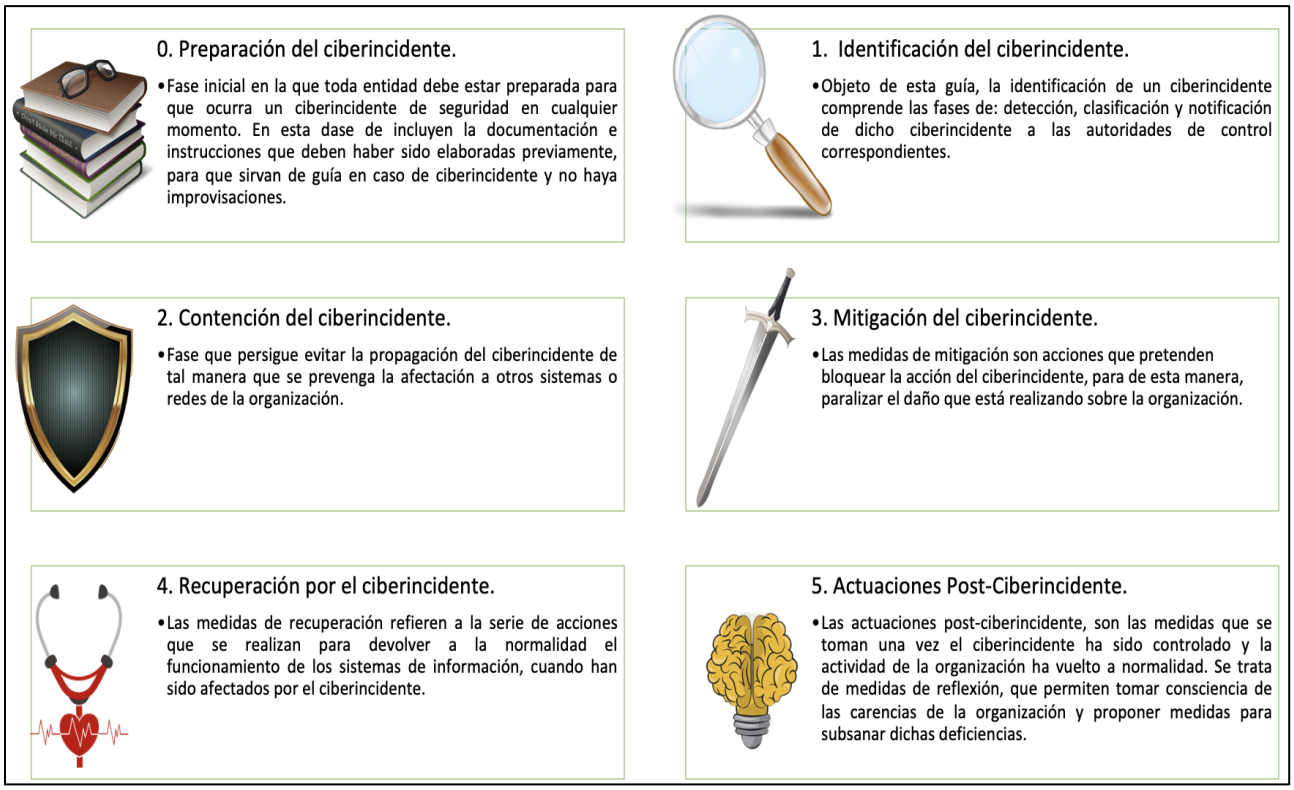


Figura 3-8 Ciclo de vida de gestión de un incidente tipo. [Elaboración Propia]

Debe tenerse en cuenta que en algunos tipos de ciberincidentes, la línea entre una fase y otra puede ser muy delgada, y se pueden superponer acciones entre varias fases. El objeto de esta guía es mostrar cuales son los pasos de forma generalista, para que el responsable pueda encomendarlos, sin perjuicio de superponer fases de forma simultánea, en función del tipo de ciberincidente y grado de experiencia.

Dado que las demás fases dependerán de la casuística particular, solo se describirá las acciones más importantes de la fase de Preparación ante el incidente.

En esta fase se procede a la "preparación previa" que consiste en disponer de los recursos oportunos ante la materialización del ciberincidente. Cabe destacar, que esta fase no es meramente técnica, sino más bien organizativa, donde el departamento correspondiente debe prever de antemano, las necesidades técnicas, económicas y recursos necesarios para poder afrontar con diligencia un ciberincidente. Por ello, deben desarrollarse los procedimientos y normas pertinentes que permitan, la correcta superación de cualquier ciberincidente. Destacándose, entre otros, los siguientes puntos:

- Desarrollar los sistemas de información atendiendo al principio de seguridad por defecto y desde el diseño.
- Disponer de información actualizada de contacto, tanto de personal interno como externo, a implicar en otras fases de gestión del ciberincidente, así como las distintas vías de contacto

disponibles en cada caso. Para ello, deberá tenerse en cuenta lo dispuesto en los Planes de actuación ante ciberincidentes.

- Mantener las políticas y procedimientos actualizados. Especialmente todos los relativos a gestión de ciberincidentes, recogida de evidencias, análisis forense o recuperación de sistemas.
- Disponer de las herramientas a utilizar en todas las fases de gestión del ciberincidente.
- Disponer de los planes de contingencia, continuidad de negocio, recuperación ante desastres, BIA (Bussiness Impact Analysis), o análisis de impacto de negocio etc. definidos y actualizados.
- Formación y concienciación del equipo humano para mejorar las capacidades técnicas y operativas. Es especialmente importante la concienciación de los usuarios finales, para que sepan cómo actuar y reportar un ciberincidente desde sus primeras fases de exposición (esto permite reducir el impacto de la materialización de la amenaza).
- Realización de simulación de ejercicios de actuación ante ciberincidentes, de tal manera que se puedan medir y gestionar los tiempos de actuación, en busca de la mejora continua.
- Ejecución de ciberejercicios a fin de entrenar las capacidades y procedimientos técnicos, operativos, de gestión y coordinación. Se deben disponer de los medios técnicos necesarios que permitan efectuar con solvencia la redundancia de los servicios críticos esenciales de la organización.
- Realizar análisis de riesgos que permita disponer de un plan de tratamiento de riesgos que permita controlarlos pudiendo ser mitigados, transferidos o aceptados.
- Preparación de plantillas de comunicación, notas de prensa etc. ante la posibilidad de tener que hacer manifestaciones públicas del ciberincidente.
- Disponer de partidas económicas necesarias para desarrollar las acciones anteriores.

3.9 Herramientas de ciberseguridad, su diseño, su despliegue e integración

A continuación se exponen algunos de los motivos, pero no los únicos, por los que se deben implementar herramientas de ciberseguridad en empresas y organizaciones:

- La cantidad de datos que manejan las empresas y organizaciones ha crecido de forma desorbitada, principalmente por la era de la digitalización en la que estamos inmersos.
- La seguridad de la información en las organizaciones es algo crucial, para cumplir los requerimientos legales, y la credibilidad y confiabilidad de las mismas.
- Así lo corroboran informes como el de Empleos Emergentes España de Linkedin, en el que el especialista en ciberseguridad ocupa el puesto número cinco. Además, el mismo estudio indica que **el número de expertos en el ámbito en el país ha aumentado un 60,01% respecto al año anterior** y que las habilidades relacionadas con la ciberseguridad son de las más demandadas por las empresas, seguida de la automatización de procesos y marketing.
- Según el balance anual publicado por el Instituto Nacional de Ciberseguridad (INCIBE), **durante 2020 se gestionaron nada menos que 133.155 incidentes de ciberseguridad**. Esto supone un aumento del 24% respecto a los 107.397 que se registraron el año anterior.
- La multitud de ataques de diferente naturaleza que se producen en cada momento en todo el planeta, como aparece reflejado en el anexo I de este TFM, en relación a una consulta realizada sobre la página web e *Karspesky* y los que se produjeron en el pasado pero con una gran repercusión que aparecen descritos en el anexo III.

Aunque la lista de herramientas podría ser muy numerosa y todas ellas cumplen su función dentro de la ciberseguridad, no es necesario desplegar todas y cada una de ellas en el seno de una organización, dado que la seguridad total no es posible, ni tampoco los recursos económicos son infinitos en ninguno de los casos.

Bastará con analizar las características de la organización, los activos e información a proteger, y los recursos disponibles, para que mediante la definición de la política de ciberseguridad, se establezcan unas necesidades a cubrir dentro de las posibilidades económicas y de los riesgos asumidos, que definirán qué tipo de herramientas es necesario implementar.

Es en base a estos principios y a la descripción del tipo de organización que se está analizando en este TFM, se determinan como necesarias para una ciberseguridad bastante más que aceptable, las distintas herramientas que a continuación se describen. Para la descripción de las mismas se han empleado las definiciones y conceptos de las diferentes páginas referenciadas en la bibliografía.

3.9.1 Cortafuegos o Firewall

Muchas personas pueden considerarlos obsoletos o poco importantes, pero la realidad es que los firewalls son herramientas de ciberseguridad indispensables para el bloqueo de amenazas. Y aunque los más antiguos tuvieran estructuras muy simples y solo fuesen eficaces para amenazas fáciles, a día de hoy existen versiones más avanzadas capaces de clasificar los archivos según muchos parámetros. Su función principal es inspeccionar el tráfico de la web, identificar usuarios y bloquear accesos no autorizados. [15]

Se trata del núcleo de las herramientas de ciberseguridad. Su trabajo es evitar el acceso no autorizado a una red privada y puede implementarse como hardware, software o una combinación de ambos. Todos los mensajes que entran o salen de la intranet pasan a través del firewall y este examina y bloque aquellos que no cumplen con los criterios de seguridad específicos. En la figura 3-9 se muestran las dos claras zonas de una organización, que se delimitan o separan mediante cortafuegos.

Por otro lado, aunque es muy útil, también tiene limitaciones. Un ciberdelincuente experto podría crear datos y programas que pasen como datos confiables para poder pasar desapercibido. A pesar de esto, siguen siendo muy útiles en la protección de ataques maliciosos menos sofisticados en nuestro sistema.

Un caso particular seria el Firewall NAT.

Un firewall NAT funciona al permitir que el tráfico de Internet pase a través de la puerta de enlace solo si un dispositivo en la red privada lo solicita. Se descartan todas las solicitudes o paquetes de datos no solicitados, lo que impide la comunicación con dispositivos potencialmente peligrosos en Internet. Si el tráfico entrante de Internet no tiene una dirección IP privada para reenviar más allá de la puerta de enlace, el cortafuegos NAT sabe que el tráfico no es solicitado y debe descartarse.

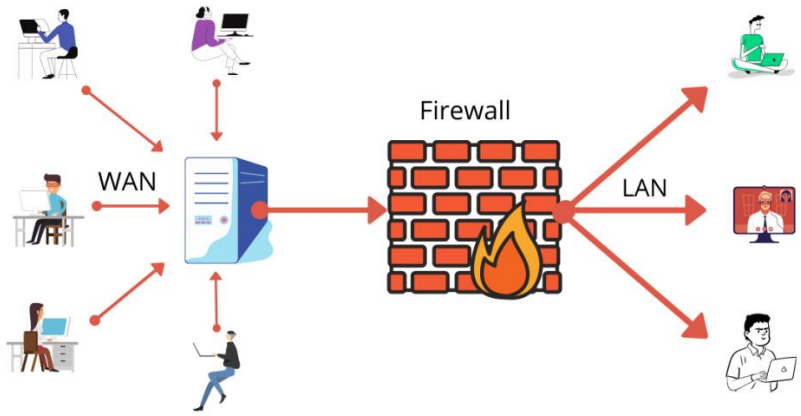


Figura 3-9 Funcionamiento de un Firewall. Fuente: [15]

3.9.2 Cortafuegos de aplicaciones web o WAF (web Application Firewall)

Un WAF (*Web Application Firewall*) protege a las aplicaciones *web* de diversos ataques a la capa de aplicación, como el *cross-site scripting* (XSS), la inyección de SQL y el envenenamiento de *cookies*, entre otros. Los ataques a las aplicaciones son la principal causa de infracción (son la puerta de acceso a sus datos importantes). Colocando un WAF adecuado, se pueden bloquear los distintos ataques cuyo objetivo es poner en peligro los sistemas accediendo a esos datos. [15]

El WAF protege sus aplicaciones web filtrando, vigilando y bloqueando todo el tráfico HTTP/S malicioso que se dirija hacia ellas e impide que salga de ellas cualquier dato no autorizado. Lo hace adhiriéndose a un conjunto de políticas que distinguen entre tráfico malicioso y seguro. Al igual que un servidor *proxy* actúa como intermediario para proteger la identidad de un cliente, un WAF funciona de manera similar pero a la inversa (se llama *proxy* inverso), actuando como un intermediario que protege el servidor de aplicaciones web de un cliente potencialmente malicioso.

Un WAF puede ser un software, un dispositivo o un servicio prestado. Las políticas se pueden personalizar para satisfacer las necesidades exclusivas de su aplicación o conjunto de aplicaciones web. Aunque muchos WAF requieren actualizar las políticas regularmente para abordar nuevas vulnerabilidades, los avances en el aprendizaje automático permiten a algunos WAF actualizarse automáticamente. Esta automatización es cada vez importante, dado que el panorama de amenazas sigue creciendo en complejidad y ambigüedad.

3.9.3 Sistema de Prevención de Intrusos IPS

Un IPS es un producto de seguridad con un enfoque más amplio. Normalmente se basa en firmas y políticas, lo que significa que puede comprobar vulnerabilidades y vectores de ataque conocidos en función de una base de datos de firmas y en las políticas establecidas. El IPS establece una norma basada en esta base de datos y estas políticas y luego envía alertas si el tráfico se desvía de la norma. Las firmas y las políticas van creciendo a medida que se conocen nuevas vulnerabilidades. En general, el IPS protege el tráfico a través de una gama de protocolos como DNS, SMTP, TELNET, RDP, SSH y FTP. El IPS normalmente opera y protege las capas 3 y 4., las capas de red y de sesión, aunque algunos pueden ofrecer una protección limitada en la capa de aplicación (capa 7). [16]

3.9.4 NGFW (Firewall de última generación)

Vigila el tráfico que sale a Internet (a través de sitios web, cuentas de correo electrónico y SaaS). En pocas palabras, protege al usuario (frente a la aplicación web). El NGFW obliga a cumplir las políticas basadas en el usuario y agrega contexto a las políticas de seguridad, aparte de otras funciones como el filtrado de URL, antivirus/anti-malware, y potencialmente, sus propios sistemas de prevención de intrusos (IPS). Mientras que el WAF suele ser un proxy inverso (utilizado por los servidores), el NGFW suele ser un *proxy* de avance (utilizado por clientes como navegador). [16]

3.9.5 IDS o (Intrusion Detection System)

Es un software de seguridad cuya función es detectar accesos no autorizados en un sistema o una red de ordenadores, y en base a ello, generar algún tipo de alerta o *log* para que posteriormente pueda ser gestionado por el administrador de sistemas correspondiente. [17]

A diferencia de un IPS (*Intrusion Prevention System*), el IDS no actúa ante un posible ataque, simplemente alerta del mismo. Podríamos decir que el IPS es en base, la misma idea, pero que, al detectar una intrusión, ejerce alguna función determinada en base al tipo de ataque, para prevenir que este llegue a ser efectuado o mitigarlo en caso de que ya se haya materializado.

Tipos en base a su radio de acción:

- HIDS (*HostIDS*) – Monitorea el tráfico entrante y saliente de un host específico. Sólo actúa en el host en el que está corriendo (recomendado para servidores web).
- NIDS (*NetworkIDS*) – Captura todo el tráfico de la red y detecta tráfico inusual (están constituidos por un sniffer).

3.9.6 Gestión de eventos e información de seguridad (SIEM)

SIEM recopila, agrega, analiza y almacena grandes volúmenes de datos de registro de toda la empresa. Originalmente, tenía un enfoque muy amplio: recopilar datos de eventos y registros de prácticamente cualquier fuente de la empresa con el fin de almacenarlos para diferentes casos de uso, como la gobernanza y el cumplimiento, la correspondencia de patrones basada en reglas, la detección heurística / de comportamiento de amenazas como UEBA, y la detección de indicadores de peligro (IoC) o indicadores atómicos en las fuentes de telemetría. [18]

Sin embargo, la implementación de las herramientas SIEM requiere muchos ajustes y esfuerzos. Los equipos de seguridad pueden verse superados por la gran cantidad de alertas procedentes de un SIEM, con lo que el centro de operaciones de seguridad (SOC) podría terminar pasando por alto alertas críticas. Además, aunque un SIEM capture datos de decenas de fuentes y sensores, sigue siendo una herramienta analítica pasiva que emite alertas.

3.9.7 Detección y respuesta de endpoints (EDR / XDR)

EDR proporciona a una organización la capacidad de supervisar los endpoints en busca de comportamientos sospechosos y registrar todas y cada una de las actividades y eventos. Acto seguido, relaciona la información para proporcionar un contexto crítico que permita detectar las amenazas

avanzadas y, por último, ejecuta una acción de respuesta automatizada, como aislar el endpoint infectado de la red prácticamente en tiempo real. [18, 19]

XDR es la evolución de EDR, la detección y respuesta para endpoints. Mientras que EDR recopila y correlaciona las actividades que se suceden en varios endpoints, XDR amplía el alcance de la detección con el fin de proporcionar detección, análisis y respuesta no solo en los endpoints, sino también en las redes, servidores, cargas de trabajo en la nube, SIEM y mucho más.

Esto proporciona una vista unificada de varias herramientas y vectores de ataque. Esta visibilidad mejorada contextualiza las amenazas para facilitar la clasificación, investigación y reparación.

XDR recopila y relaciona automáticamente los datos de diversos vectores de seguridad, favoreciendo así una detección más rápida de las amenazas para que los analistas de seguridad puedan responder rápidamente antes de que se amplíe el alcance de la amenaza. Las integraciones listas para usar y los mecanismos de detección preestablecidos en varios productos y plataformas diferentes ayudan a mejorar la productividad, la detección de amenazas y el análisis forense.

¿En qué se diferencia XDR de SIEM?

Cuando hablamos de XDR, hay quien piensa que estamos describiendo una herramienta de información de seguridad y gestión de eventos (SIEM) de una manera diferente. Pero XDR y SIEM son dos cosas distintas.

La plataforma XDR pretende resolver los retos que plantean las herramientas SIEM para una detección y respuesta eficaz a los ataques dirigidos e incluye análisis de comportamiento, inteligencia sobre amenazas, perfiles de comportamiento y análisis.

3.9.8 Infraestructura de Clave Pública o PKI

PKI son las siglas de *Public Key Infrastructure* (Infraestructura de clave pública). Esta herramienta admite la distribución e identificación de claves de cifrado públicas. Permite a los usuarios y sistemas informáticos intercambiar datos de forma segura a través de Internet y verificar la identidad de la otra parte. También es posible intercambiar información confidencial sin PKI pero, en ese caso, no habría garantía de autenticación de la otra parte [15]. En la figura 3-10 se ve el esquema de funcionamiento de la herramienta PKI.

Muchas personas asocian PKI con SSL o TLS. Esta es la tecnología que encripta la comunicación del servidor y se encarga de HTTPS y el candado que podemos ver en la barra de direcciones de nuestro navegador. PKI resuelve muchos problemas de ciberseguridad.

Se trata de un sistema de recursos, políticas y servicios que da soporte al uso de cifrado de claves públicas para autenticar a las partes que participan en una transacción. Proporciona los siguientes servicios:

- Emisión de certificados digitales
- Validación de certificados digitales
- Revocación de certificados digitales
- Distribución de claves públicas

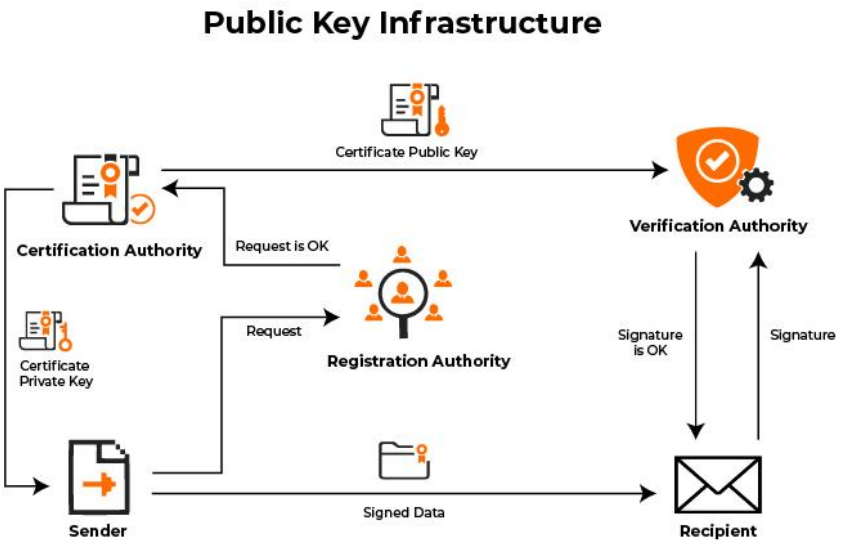


Figura 3-10 Esquema funcionamiento PKI. Fuente: [15]

3.9.9 Accesos seguros desde equipos externos VPN (SSL, iPSec)

Virtual Private Network (VPN) se emplean para crear túneles que usan la red pública para conectar distintas unidades organizativas, compartir información o conectar empleados en actividades remotas a plataformas corporativas. [20]

Los túneles VPN establecen conexiones para el tráfico de paquetes. Estos paquetes contienen formatos específicos para coincidir con el tipo de protocolo en uso. Es decir, un paquete que sale de una «red A» se encapsula en un formato que se fija al protocolo de transmisión, atraviesa el túnel entre redes y al final, cuando llega a su destino «red B» se desencapsula.

Si se piensa en Internet como la infraestructura básica para la transmisión, los paquetes a menudo están encapsulados por dos tipos de protocolos.

Los dos modelos de implementación de VPN más usuales actúan en diferentes capas de la estructura OSI. *Internet Protocol Security* (IPSec) trabaja en la capa de red, mientras que *Secure Sockets Layer* (SSL) opera en la capa de aplicación.

La implementación de IPSec se diseñó para brindar conexiones permanentes punto a punto, enlazando redes privadas a dispositivos fuera del perímetro de la empresa; por ejemplo, sucursales de oficina.

En ese caso, la transmisión de paquetes sigue una especificación estándar dentro del encabezado TCP / IP, por lo que es habitual encontrarla en fabricantes y sistemas operativos.

La implementación de SSL se ha mejorado frente a los retos de movilidad. A diferencia de IPSec, SSL VPN no brinda acceso a la red privada. El usuario remoto que usa este tipo de túnel puede ingresar de manera controlada a recursos perimetrales específicos.

Por ejemplo, si necesita mantener un acceso local permanente (sucursales), la implementación de IPSec es la mejor opción. Sin embargo, para conseguir más control de acceso por aplicación, es mejor adoptar la implementación de SSL, que también es más adecuada para el acceso de usuarios remotos (empleados en una reunión externa, por ejemplo).

3.9.10 Pentesting

El Pentesting o test de penetración es una de las mejores formas de evaluar los sistemas de seguridad de nuestra empresa y la seguridad de una infraestructura de TI, ya que intenta aprovechar las vulnerabilidades de forma segura. Estas vulnerabilidades existen en sistemas operativos, servicios y aplicaciones, configuraciones incorrectas o comportamientos de riesgo del usuario final. [15]

En las pruebas de penetración, los expertos en ciberseguridad utilizarán las mismas técnicas y procesos que usan los piratas informáticos para detectar posibles amenazas y áreas de debilidad.

En resumen, consiste en atacar diferentes entornos o sistemas con el objetivo de detectar y prevenir posibles fallos. Se trata de una técnica para encontrar aquellos errores en el sistema. Es una de las prácticas más demandadas actualmente, ya que gracias a este tipo de exámenes las empresas pueden poner remedio a sus debilidades antes de que lo hagan los ciberdelincuentes. Un pentester es un auditor de seguridad informática. Se dividen en dos:

- **Red team**, la parte más ofensiva
- **Blue team**, la parte defensiva

Son útiles por diferentes razones. En primer lugar, porque determinan qué posibilidad de éxito podría tener un ciberataque, qué vulnerabilidades de mayor y menor riesgo tiene la empresa, cuáles de ellas pueden poner en riesgo a la organización y cuáles son casi imposibles de detectar. También comprueban la capacidad y la eficiencia de los informáticos a la hora de responder a posibles ataques.

Figura 3-11 Fases de Pentesting. Fuente: [15]

3.9.11 Escáneres de vulnerabilidades

Un escáner de vulnerabilidades es una herramienta de seguridad que examina tus activos de TI en busca de fallas, debilidades o CVE (vulnerabilidades y exposiciones comunes) que pueden poner en riesgo la ciberseguridad de la organización. [21]

Estos escáneres ayudan a corregir vulnerabilidades y priorizar el proceso de acuerdo con su nivel de riesgo. Una vez que el software completa el análisis, produce una medida de riesgo asociado con las vulnerabilidades identificadas y sugiere una solución para mitigar los riesgos.

Cuando el análisis de vulnerabilidades se realiza con regularidad con una gestión adecuada de vulnerabilidades, ayuda a proteger la organización contra nuevas amenazas que emanan de actualizaciones frecuentes en el software. Además, la herramienta realiza una verificación cruzada con una o más bases de datos de vulnerabilidades para identificar si existen vulnerabilidades conocidas.

Los escáneres de vulnerabilidades permiten a las organizaciones cumplir con los estándares de seguridad en evolución al monitorizar y detectar vulnerabilidades y corregirlas para mantener la seguridad de la red. Además, el escaneo de vulnerabilidades es también uno de los primeros pasos en las pruebas de penetración.

¿Cuál es el propósito de los escáneres de vulnerabilidades?

- Detectar amenazas de seguridad
- Descubrir dispositivos no identificados.
- Verificar el inventario de dispositivos de red

Tipos de análisis de vulnerabilidades:

- Análisis de vulnerabilidades externas

  Los análisis de vulnerabilidades externas ayudan a las empresas a identificar y corregir las vulnerabilidades que exponen su red a los atacantes. Estos análisis se realizan desde fuera de la red de la organización, incluidos los activos de TI, las aplicaciones web, los puertos y más.

- Análisis de vulnerabilidades internas

  Estos análisis le ayudan a detectar las vulnerabilidades de seguridad que los piratas informáticos pueden utilizar para su beneficio una vez que han penetrado a través de los agujeros de seguridad o el marco de defensa externo. Estos análisis también ayudan a identificar la amenaza que representa el malware o las amenazas internas modeladas por empleados o contratistas descontentos.

- Análisis de vulnerabilidades no autenticados

  Los análisis de vulnerabilidades no autenticados exploran y detectan servicios abiertos en una computadora a través de una red enviando paquetes en sus puertos abiertos. Determina la versión del sistema operativo, la versión del software detrás de los respectivos servicios, archivos compartidos abiertos o cualquier otra información disponible sin autenticación.

- Análisis de vulnerabilidades autenticados

  Los análisis de vulnerabilidad autenticados acumulan información más detallada sobre la versión del sistema operativo y el software instalados mediante el uso de credenciales de inicio de sesión. Los análisis autenticados brindan información completa sobre las vulnerabilidades del sistema, ya que pueden acceder a aplicaciones y archivos.

- Análisis de vulnerabilidades completos

  Los análisis completos de vulnerabilidades exploran, examinan e identifican nuevas vulnerabilidades en todos los dispositivos administrados en la red. Estos incluyen servidores, computadoras de escritorio, computadoras portátiles, máquinas virtuales, teléfonos móviles, contenedores, impresoras, firewalls, conmutadores y más.

- Análisis de vulnerabilidades limitado

Los análisis de vulnerabilidad limitados se centran principalmente en dispositivos particulares como un servidor, una estación de trabajo o un software. Estos análisis se realizan para obtener una postura de seguridad muy específica de las herramientas y protegerlas mejor contra posibles riesgos.

3.9.12 Autenticación robusta con doble factor de autenticación

El doble factor es un sistema de verificación en dos pasos, que de manera general, funciona con una contraseña, que se puede enviar por diferentes métodos, a los cuales debería tener únicamente acceso el usuario, y permiten que el usuario verifique y se identifique de manera inequívoca. Las claves de este tipo de métodos de doble factor de autenticación son [22]:

- Contraseñas de un solo uso.
- Envío mediante un método de acceso único para el usuario.
- Envío por SMS, llamada telefónica, correo electrónico, app, etc.
- Límite temporal de uso de la contraseña.
- Sencillo de utilizar y rápido.

Para que un sistema sea realmente de doble factor, se deben cumplir una serie de requisitos, donde al menos encontremos dos capas de seguridad, las cuales identifiquen de manera inequívoca al usuario, por este motivo es necesario que un sistema doble factor al menos cumpla los siguientes requisitos:

- Una contraseña que sólo conozca el usuario.
- Desde un dispositivo o elemento que sólo posea el usuario.
- Con una característica propia del usuario (biométrica, una firma, voz, etc.)

3.9.13 Network Access Control (NAC)

También conocido como control de admisión de red, es el proceso de restringir el acceso de usuarios y dispositivos no autorizados a una red corporativa o privada. NAC garantiza que solo los usuarios autenticados y los dispositivos autorizados y compatibles con las políticas de seguridad puedan ingresar a la red. [23]

A medida que los puntos finales proliferan en una organización, generalmente impulsados por políticas BYOD (traiga su propio dispositivo) y una expansión en el uso de dispositivos de Internet de las cosas (IoT), se necesita más control. Incluso las organizaciones de TI más grandes no tienen los recursos para configurar manualmente todos los dispositivos en uso. Las características automatizadas de una solución NAC son un beneficio considerable, ya que reducen el tiempo y los costos asociados con la autenticación y autorización de usuarios y la determinación de que sus dispositivos son compatibles.

Además, los ciberdelincuentes son muy conscientes de este aumento en el uso de endpoints y continúan diseñando y lanzando campañas sofisticadas que explotan cualquier vulnerabilidad en las redes corporativas. Con más puntos finales, la superficie de ataque aumenta, lo que significa más oportunidades para que los estafadores obtengan acceso.

Las soluciones NAC se pueden configurar para detectar cualquier actividad de red inusual o sospechosa y responder con una acción inmediata, como aislar el dispositivo de la red para evitar la posible propagación del ataque.

¿Cuáles son las ventajas del control de acceso a la red?

El control de acceso a la red viene con una serie de beneficios para las organizaciones:

1. Controlar los usuarios que entran en la red corporativa
2. Controlar el acceso a las aplicaciones y recursos a los que los usuarios pretenden acceder
3. Permitir que los contratistas, socios e invitados ingresen a la red según sea necesario, pero restringiendo su acceso
4. Segmentar a los empleados en grupos en función de su función laboral y crear políticas de acceso basadas en roles
5. Proteger contra los ataques cibernéticos implementando sistemas y controles que detecten actividades inusuales o sospechosas
6. Automatizar la respuesta a incidentes
7. Generar informes e información sobre los intentos de acceso en toda la organización

3.9.14 Sandboxing

El sandboxing es una técnica de seguridad informática que se basa en la ejecución de programas o aplicaciones en un espacio virtual limitado, en el cual se pueden controlar todos los procesos sin que afecten al resto del equipo. [18, 24]

La traducción al español del término sandbox sería «caja de arena» haciendo un símil con los típicos espacios de juegos donde los niños pueden jugar sin correr peligro mientras son supervisados por sus padres.

La técnica del sandboxing funciona de forma similar a estos espacios cerrados de arena. Este mecanismo de aislamiento de procesos permite abrir programas o aplicaciones desde un contenedor virtual y aislarlas del resto del equipo. De este modo, se pueden controlar los recursos que solicita el programa y ejecutarlo desde un entorno controlado y aislado del resto de procesos que se ejecutan en el ordenador o en otros dispositivos externos conectados.

Es una técnica que puede ofrecer grandes beneficios en materia de ciberseguridad. No solo aísla programas para proteger el conjunto del sistema, sino que permite descubrir nuevas amenazas, analizarlas y estudiarlas dentro de un entorno de prueba. Imagina tener un malware aislado en ámbar para poder estudiarlo sin temor a que se escape. Pues sería algo parecido.

La información obtenida sobre el malware o programa malicioso en este entorno virtual se puede emplear para desarrollar técnicas aplicables al entorno real y que eviten los riesgos provocados por estas amenazas. Muchas empresas de seguridad informática emplean los entornos sandbox para desarrollar nuevos métodos de protección que luego acaban siendo de uso general. Por ello, el sandboxing es un gran aliado de las empresas frente al robo de información y otros ataques malintencionados.

3.9.15 Formación

Por último, aunque la formación del personal no sea una herramienta de ciberseguridad en sí, contar con empleados con conocimientos básicos en ciberseguridad es una de las formas más sólidas de defensa contra los ciberataques.

Existen muchas herramientas y formas de capacitación disponibles que pueden educar al personal de la empresa, sobre las mejores prácticas en ciberseguridad. Todas las empresas pueden llevar a cabo diversas técnicas de capacitación para educar a sus empleados para que estos puedan comprender su papel en la seguridad.

Si no lo hacen, pueden dejar a la organización en una posición en la que los piratas informáticos podrían atacar fácilmente el sistema de seguridad. Por lo tanto, el gasto de la inversión en estas herramientas de capacitación podría representar una recompensa para la organización empresarial con seguridad y protección a largo plazo.

3.10 Herramienta de gestión integral

Figura 3-12 Cuadro de Mando Integral. Fuente: [25]

Después de lo expuesto con anterioridad sobre la casuística de las múltiples herramientas en materia de ciberseguridad, y que estando disponibles en el mercado podrán ser elegidas o no para dar la mejor solución posible, atendiendo a las necesidades y capacidades de cada organización, el lector de este TFM podría haberse preguntado – y ¿Dónde está la herramienta maestra integradora? –, es decir esa herramienta que le permite gestionar y controlar todas las demás herramientas, y que puede implementarse una organización para atender a sus necesidades. La figura 3-12 muestra una imagen que publicita a alguna de las herramientas de mercado, que están empezando a desarrollarse para tal fin, en la que muestran la interconexión de un gran número de aplicaciones, utilidades o cuadros de control.

Esa herramienta permitiría reducir la complejidad de tener que gestionar múltiples soluciones, que aportarían resultados de manera independiente, pero que no aprovecharían las acciones realizadas por las demás herramientas, y que podría contribuir a mejorar el resultado final, además de reducir costes en personal y equipos necesarios para el mantenimiento, y explotación de las múltiples herramientas.

Sin esta herramienta, el automatismo en acciones y reacciones para mitigar un ciberataque o asegurar los activos de la organización no existiría, salvo que la solución para la ciberseguridad esté implementada por una única firma o fabricante, que integre un gran número de campos de actuación, pero con el *hándicap* de no poder abarcar todos, al menos en la actualidad.

La situación actual es que los diferentes fabricantes y proveedores de herramientas están intentando abarcar la mayor parte de los campos de acción, que se pueden identificar en la ciberseguridad de esta era. Y si bien es verdad que presentan posibles soluciones a modo cuadro de control integral, que controlan todas aquellas herramientas de su firma o empresa, además de asegurar que es totalmente compatible con la mayoría de las herramientas de la competencia, también es cierto que no existe ninguna que realmente sea compatible, y que pueda integrar al cien por cien las capacidades de todas las demás herramientas, que se elijan en una organización si estas son de múltiples fabricantes.

La gran mayoría defiende que se pueden interconectar mediante enlaces API de código abierto, pero la realidad es que luego resulta que no es así, sino que hay que pagar por el desarrollo si realmente se quiere que funcione a todo su potencial, y en muchos casos no siendo posible su propio desarrollo particularizado.

Es por ello que puede sentenciarse que a fecha de hoy no existe esa herramienta de gestión integral, pero que no cabe duda que a muy corto plazo habrá múltiples fabricantes que si la ofrezcan, midiéndose su éxito por el grado de integración de herramientas, y por su nivel de gestión ofrecido sin importar la marca o fabricante que deba integrarse.

A continuación se hará una breve síntesis de cuales se consideran deben ser los requisitos mínimos o capacidades fundamentales que debe presentar dicha herramienta.

- Debe ser capaz de presentar en un cuadro de mando completo, una selección de campos intercambiables, que midan las distintas métricas aportadas por las herramientas de ciberseguridad que reportan datos. Esos cuadros pueden ser gráficos, estadísticas, diagramas, paneles informativos que contengan numeraciones, datos o sistemas de colores, que presenten una visión clara e inequívoca de la situación general y particular por áreas de interés.
- Debe poder producir informes completos de dirección, y parciales técnicos, ajustables en periodos de tiempo, automatizados y siempre disponibles.
- Debe mostrar el inventario total de activos de la organización, diferenciándolos por categorías, sistemas y servicios, que estén totalmente interrelacionados, para poder abarcar todas las posibles concurrencias.
- Debe poder mostrar el nivel de los sistemas acorde al ENS y deben estar claramente registrados cada uno de los responsables del sistema (servicio, información seguridad, sistema).
- Debe mostrar un despliegue somero, de fácil comprensión sobre el despliegue general de los activos, que puedan ocasionar un mayor impacto en la organización en caso de ser atacados.
- Debe ser capaz de efectuar el análisis de riesgos, fruto de la multitud de datos recibidos de forma automática, y establecer un valor de criticidad de los activos, para que mediante un algoritmo se determine el impacto, que puede surtir en la organización la manifestación de los diferentes riesgos, a los que puede estar expuesta en cada momento.
- Debe recibir de forma automatizada de las herramientas y de fuentes abiertas, la máxima información posible de las CVE,s, que le permita calcular u mostrar el estado de riesgo de la organización, ante cada una de la CVE,s que se van publicando, y refrescar la situación cuando hayan sido mitigadas.
- Debe recibir inteligencia de herramientas que le permita calcular esa criticidad dinámica y esa medición del impacto, que varía en función de las posibles amenazas que no siendo solo las CVE,s, sino otros incidentes o brechas.
- Debe proporcionar soluciones automatizadas para mitigación de las CVE,s caso de que afecten a la organización, o a los demás incidentes que puedan ser reportados de forma manual o automática.
- Debe poder controlar de forma automática las soluciones aplicadas, y resetear la situación acorde a cada uno de los estados o acciones en las que se vaya encontrando la organización.

Para complementar esa herramienta en el caso de grandes corporaciones con despliegues en diferentes sedes y sobre todo con sedes internacionales, será necesario que pueda ingestar datos de plataformas que proporcionen juicios o partes de información o de inteligencia, que permita variar el nivel de riesgo calculado, atendiendo a condicionantes particulares como pueden ser posibles catástrofes naturales, zonas de conflicto armado, o bajo tensiones políticas desestabilizantes, etc.

De la misma forma debe proveer de parámetros o datos, a las plataformas que proporcionan un mapa de situación global de los activos y de las diferentes zonas en función del riesgo de la organización, que sirvan tanto para mantener controlada la ciberseguridad, como para la ciberdefensa en el ciberespacio.

3.11 Contratación de servicios y suministro de ciberseguridad

Como ya se ha ido señalando en los diferentes apartados anteriores, aunque si bien es verdad que depende del tipo de organización, es muy habitual el contratar todas las herramientas de ciberseguridad a proveedores y firmas disponibles en el mercado, pudiéndose desarrollar alguna de forma interna, de la misma forma que también se contratan los servicios que deberán atender en algún caso a toda la ciberseguridad de la organización, como puede ser un servicio de SOC 24x7 o 8x5, y en otros sólo a la explotación de determinadas herramientas contratadas.

Generalmente este tipo de servicios paralelo o no a las herramientas, se suelen contratar mediante contratos plurianuales que oscilan entre 2 y 3 años prorrogables a un 3º o 4º año, al objeto de no atarse de forma exclusiva a una única solución que pudiera quedar obsoleta en el plazo de la vigencia del contrato. Es fundamental realizar un estudio de mercado y tecnologías, para no contratar algo que ya no tiene futuro por estar superada su solución, o porque vaya a quedarse sin soporte a medio plazo, por muy barato que pudiera salir.

Por lo general muchas firmas de fabricantes que van asociadas a proveedores de servicios y partners, ofrecen su producto ligado a los proveedores de servicios, lo cual parece lógico, pero no es obligado para su contratación, si la propia organización dispone de personal cualificado para la explotación de las herramientas, pudiéndose en este último caso contratar solo el hardware o software, y adquiriendo las licencias que fuesen necesarias.

A continuación se expone a modo de ejemplo 8 de los servicios de ciberseguridad más demandados del mercado.

1. **Análisis de vulnerabilidades**

Es el servicio más básico e inicial que cualquier empresa debe hacer. Se trata de hacer un diagnóstico básico. Este servicio te va a permitir conocer todas las vulnerabilidades básicas que pueden aparecer en los sistemas de organización.

2. **Test de intrusión**

El test de intrusión incluye un escaneo de las vulnerabilidades manuales que realiza un especialista en ciberseguridad, estudiando el entorno y pudiendo identificar los fallos en seguridad donde no llegarían las herramientas automáticas.

3. **Web Hacking**

Este servicio se parece bastante al anterior, pero dedicado exclusivamente a la revisión de ciberseguridad de una aplicación web.

4. **Revisión wifi**

Las redes wifi es un sistema de entrada muy utilizado por los ciberdelincuentes, ya que físicamente, no están limitadas de la organización. Por este motivo, una revisión wifi es muy interesante ya que va a proporcionar una identificación de los puntos de acceso que están siendo controlados, así como la posible identificación de otros puntos de acceso.

Además, también va a ser posible identificar si los protocolos de cifrado y funciones que se han establecido son los suficientemente seguros, y no son explotables por un ciberdelincuente.

5. Monitorización continua

Este servicio evalúa de una forma continua cada uno de los puntos definidos para que, cuando se identifique alguno, se realice inmediatamente la corrección, evitando más ataques.

Además, este servicio también detecta si un atacante está intentando acceder o se ha conseguido meter en la compañía, ya que recoge y procesa la información que se ha recopilado en los diferentes sistemas.

6. Protección de pérdida de datos

Este servicio cuida los siguientes medios para evitar que pueda conseguir la información alguien que no debiera tener acceso:

- Transferir los datos a un disco duro o USB
- Enviar la información por una cuenta de correo personal
- Subir la información a las plataformas de almacenamiento en la nube

Los sistemas DLP son una herramienta que va a permitir establecer un control sobre la información sensible, y con ello, definir lo que puede o no hacer cada usuario con ella.

7. Formación

Es muy importante mantener formados a los empleados ya que es clave para que la empresa sea segura.

También se debe formar al equipo técnico para ayudarles a que identifiquen los ataques y las medidas que deben tomar para poder ponerles remedio.

8. Copias de seguridad

Este servicio va a ayudar a realizar una copia de toda la información, e incluso de todo el servidor o sistema. Estas copias pueden hacerse en un disco externo, en la nube, etc. Incluso se puede hacer una copia de la información en la nube y, en el caso de ataque, se restauren en un entorno virtual en la nube con el fin de que la empresa continúe su actividad en el menor tiempo posible.

Como ya se ha comentado también con anterioridad, existen organismos que se encargan de dar soporte en materia de ciberseguridad a las organizaciones privadas como es el caso del INCIBE-CERT, que es el centro de respuesta a incidentes de seguridad de referencia para los ciudadanos y entidades de derecho privado en España operado por el Instituto Nacional de Ciberseguridad (INCIBE), dependiente del Ministerio de Asuntos Económicos y Transformación Digital, a través de la Secretaría de Estado de Digitalización e Inteligencia Artificial.

Figura 3-13 Logotipo del CESTIC

En el caso de la administración pública, esta seguridad la proporcionan centros de ciberseguridad propios especializados, como es el caso del MINISDEF y su red I3D (Infraestructura Intregral de Información para la Defensa), que dispone del COS-I3D, desplegado por el CESTIC en su emplazamiento en Arturo Soria 289 (Madrid). Este centro opera 24x7 dando seguridad tanto en territorio Nacional como en operaciones en el exterior a la red I3D. Otro ejemplo sería el COCS de la Guardia Civil desplegado en la Dirección de Telecomunicaciones de la Guardia Civil en Guzmán el Bueno (Madrid), que asegura las redes corporativas del Benemérito Instituto. Y para el caso de la administración civil, se dispone del COCS de la SGAD (secretaria general de la administración digital) de la AGE, cuyos servicios se describen en el punto 3.3.

Es importante señalar que muchos de los proveedores de servicios de ciberseguridad contratados, verán condicionada su posible contratación por las empresas españolas y fundamentalmente por la administración civil española y prácticamente europea, en función de los estándares o requisitos que cumplan, referentes a normas ISO, CCN-STIC, ENS, y fundamentalmente por donde alojen los datos o información que extraen de los sistemas a proteger, necesaria para alimentar su procesos de análisis, computación, tratamiento y almacenamiento.

Por lo general y para cumplir con la legislación, ese cómputo y almacenamiento e IA (inteligencia artificial) aplicada, se realizará en nubes privadas de las propias firmas, o subcontratadas a proveedores generalmente de renombre, que cumplan con la legislación vigente, que deben ser desplegadas dentro de territorio europeo, y bajo unas condiciones de cifra, encriptado y eliminación claramente definidas para el contratante.

3.12 Las auditorias de seguridad como herramienta de ciberseguridad

Las auditorias de seguridad, son análisis de las redes, sistemas, servicios aplicaciones y procedimientos que suelen aplicarse en determinados momentos o situaciones en una organización buscando diferentes objetivos, entre los que están:

- Adecuación al ENS, de los servicios, sistemas, aplicaciones y procedimientos que se emplean en la organización.

- Análisis de las vulnerabilidades, de riesgos y determinación del posible impacto en los activos, las redes, sistemas y servicios de una organización.
- Análisis de las vulnerabilidades de un determinado software o hardware antes de ser implementado.
- Análisis forense tras haber sufrido un ciberincidente, para buscar la resolución al mismo, mediante búsquedas de TTP (técnicas, tácticas y procedimientos) de ataque empleados.
- Auditoria para reacreditar la adecuación al ENS o el cumplimiento adecuado del plan de ciberseguridad aprobado en la organización.

Por lo general las auditorias de ciberseguridad, suelen contratarse como servicio a entidades o empresas que dispongan de estos servicios, dado que es poco probable que las organizaciones o empresas cuenten con su propio órgano de auditorías.

Siendo necesario además que en algunos tipos de procesos, como el de adecuación al ENS dicho órgano debe ser independiente a la propia organización, para asegurar la imparcialidad en los intereses, además que debe ser reconocido por el CCN y disponer de la certificación correspondiente.

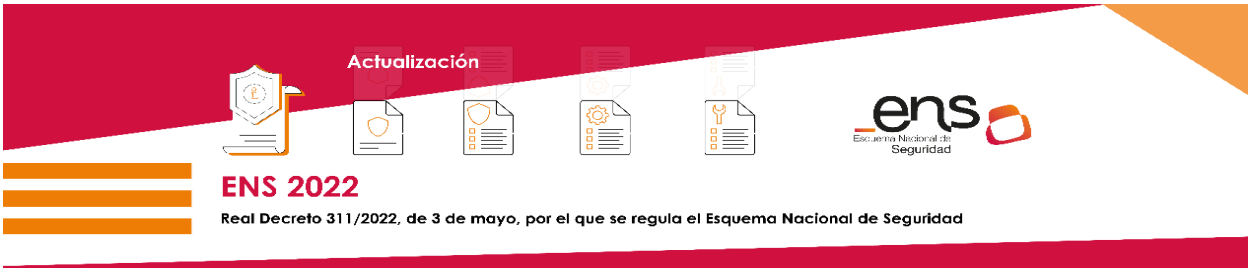


Figura 3-14 Logotipo del ENS. Fuente: [26]

4 CONCLUSIONES

4.1 Conclusiones del TFM

Como parte final o colofón de este trabajo, se considera necesario exponer que el grado de consecución de los objetivos marcados al inicio del mismo, es a criterio del autor más que aceptable y satisfactorio, toda vez que la finalidad pretendida en este trabajo es totalmente didáctica, no requiriéndose por ello demostrar ninguna hipótesis, sino solamente divulgar conocimiento. Ello es así porque claramente de han mostrado los requerimientos de ciberseguridad de una gran corporación y analizado los motivos de los que emanan, así como se ha mostrado la organización y la documentación a generar, todo ello perseguido en el objetivo primero.

Del mismo modo lo señalado para el objetivo número dos relativo a la exposición, análisis y diseño de las herramientas necesarias a desplegar para implementar la ciberseguridad, ha quedado claramente conseguido, con numerosos argumentos y datos aportados en la elaboración del cuerpo propiamente dicho del TFM.

Por último el objetivo número tres en el que se fijaba el revisar las diferentes estrategias a nivel del Estado, así como la revisión de parte de la legislación que en materia de ciberseguridad se está generando, igualmente parece más que acertado señalar que el objetivo ha sido cumplido, dado que se han recogido múltiples casos y se han analizado alguno de los más relevantes como el caso del reglamento europeo. A continuación se desarrollan las concusiones más reseñables a las que se ha llegado en el desarrollo del presente TFM, no queriendo con ello denotar que éstas sean la únicas posibles, pero si las más relevantes a modo de ver del autor, y sobre las cuales quiere que se preste una mayor atención.

La ciberseguridad en una organización, va mucho más allá de la mera implementación de ciertas herramientas o aplicaciones contratadas a proveedores o fabricantes, que podrán estar más o menos actualizadas y serán más o menos compatibles entre sí. Sino que **abarca también a la propia articulación del personal de la organización**, que deben organizarse en órganos de dirección, comités de crisis, centros y grupos de control y respuesta, que además deberán diseñar e implementar una serie de políticas, guías y planes de ciberseguridad, para la resolución de posibles crisis o incidente de ciberseguridad.

Una herramienta de ciberseguridad, que si ahora no lo es, ya queda claramente demostrado que en el futuro será **fundamental** tenerla desplegada, **es la herramienta de gestión integral**. Dicha herramienta se hace indispensable si se quiere tener una política de ciberseguridad que contemple la mayor parte de las soluciones disponibles en el mercado, atendiendo a las diferentes áreas de actuación, con la intención de disminuir al máximo las posibles vulnerabilidades de la superficie de exposición, de las redes y activos de la propia organización. Dicha herramienta es además un gestor de las propias vulnerabilidades y ciberincidentes, es a la vez un cuadro de mando integral, que permite conocer el estado de ciberseguridad en todo momento y que además permite un gran ahorro económico, si se tiene en cuenta que elimina la dependencia perpetua de fabricantes y proveedores, sobre una determinada área de ciberseguridad y herramienta contratada, pudiendo hacerse el cambio hacia otro tipo de fabricante o tecnología, gracias a la compatibilidad total como requisito indispensable, mediante conexiones API de dicha herramienta.

La ciberseguridad y la ciberdefensa en una organización, deben actuar de forma conjunta y coordinada sin fisuras o divergencias. Ninguna de ellas es autosuficiente en sí misma y el éxito de cada una está intrínsecamente ligado al de la otra. Independientemente de si se ejecutan una u otra, o ambas, o ninguna en el seno de la propia organización, empleando sus propios recursos, su diseño, organización, despliegue y aplicación, debe ser coordinado y dirigido por la propia organización

internamente. Del mismo modo las diferentes herramientas que se apliquen para proporcionar ciberseguridad y ciberdefensa, dado que muchas servirán para ambas y algunas otras no, deberán elegirse de forma coordinada y con un objetivo único, acorde a la propia política de ciberseguridad.

La legislación existente y la que está aún por desarrollarse ya sea Nacional o Internacional**, es un factor primordial para el éxito de la ciberseguridad** y debe ser tenido en consideración, ya que mucha normativa es de obligado cumplimiento en la definición y aplicación de la ciberseguridad en la organización. Tan importante es este hecho en sí, que en la actualidad se están realizado numerosos foros y grupos de trabajo para regular y legislar en este aspecto, en organizaciones como la OTAN y la UE. Y tambien se están dotado de partidas económicas muy cuantiosas, los numerosos planes de actuación, tanto en el seno de esas grandes organizaciones como en planes del ámbito Nacional. Dichos planes definen tanto las cantidades asignadas, como las pautas o ejes a seguir a corto y medio plazo, al igual que identifican las posibles carencias o necesidades de personal y planes de formación, que deban identificarse y suplirse cara al futuro.

Por ultimo cabría destacar que **una acción fundamental en materia de ciberseguridad** que no debe pasada por alto, **es la concienciación o formación del personal en dicha materia**. Se ha demostrado que gran parte de los posibles ataques o incidentes sufridos, no habrían tenido lugar si el personal que los ha sufrido o facilitado, hubiera estado correctamente formado o al menos concienciado sobre la importancia de la ciberseguridad. Es por ello que en la actualidad existen numerosos planes de concienciación en el seno de las organizaciones, a la vez que existen empresas especializadas y dedicadas en la provisión de los mismos, o incluso organizaciones nacionales como el CN-CERT que ofrecen portales que pueden ser accedidos para la formación del personal, véase así la herramienta ángeles del CN-CERT, de libre acceso.

4.2 Consideraciones de futuro

Todo lo descrito en el presente trabajo, son acciones del presente y que sin lugar a dudas tienen mucho de desarrollo, transformación y aplicación en el futuro, pero a modo de inquietud personal o de motivación de los posibles lectores, cabría la posibilidad de preguntarse o de tratar de exponer en este apartado alguna reflexiones, sobre cómo afectará la ciberseguridad a los sistemas clasificados, o como afectara a sistemas desplegados en la nube versus a los que lo hagan onpremise, sin olvidarnos tampoco que posibles consecuencias tendrá en las redes 5G, o en los prometedores sistemas que empleen la tecnología cuántica, aun relativamente en pañales.

En la actualidad no son muchas las empresas que necesitan la implementación de **sistemas clasificados**, dado que son aquellos que contengan información de carácter reservado o secreto, acorde a lo establecido por la ley de secretos oficiales (ley 9 /1969 de 5 de abril), ley española aprobada en 1968 por las Cortes Generales que tiene por objeto regular aquella información sensible cuyo conocimiento público podría suponer un riesgo para la seguridad y defensa del Estado y que posee un reglamento de desarrollo, el Decreto 242/1969. Aunque si bien es cierto que esta ley previsiblemente cambiará en breve, por una actualizada que contemplará las categorías de Uso Oficial, Difusión Limitada y Confidencial, como novedades de información que deba contar con una especial protección.

En estos sistemas la ciberseguridad debe seguir exactamente los mismos patrones que en los sistemas sin clasificar, siendo posible incluso la misma articulación del personal, pero que presentará dos diferencias fundamentales. La primera es que los sistemas no estarán conectados a redes externas, siendo dichas redes unas burbujas en sí mismas, lo cual les confieren una mayor seguridad frente a la mayor parte de los ciberincidentes actuales, pero sin descuidar la posible fuga de información premeditada como principal vector de ataque. Y la segunda diferencia, será que la información disponible en ellos debe contar con una protección reforzada en materia de confidencialidad, e integridad de la misma, dada

su especial protección requerida legalmente, lo cual significa que deberán contar con sistemas que cifren y descifren dicha información, además de canales criptográficamente seguros.

En relación a la ciberseguridad en sistemas desplegados en la **nube versus**, a los desplegados ***onpremise***, no parece observarse que haya ninguna diferencia significativa en su diseño o aplicación en líneas generales, salvo la mera cuestión de la ubicación física de los sistemas y activos a ciberproteger y la propia naturaleza de la contratación de las herramientas y servicios. En definitiva, en la modalidad *onpremise* se mantendrán los activos en instalaciones propias, pero la estructura organizativa debe centrarse en la organización, contratando las herramientas y o servicios de ciberseguridad en proveedores externos, frente a la nube, donde además de externalizar herramientas y servicios, se externalizan las aplicaciones, y gran parte de los activos. Pero a modo de conclusión la ciberseguridad siempre debe reposar en su concepción y control en los órganos directivos de la propia organización, independientemente de lo que se delegue o transfiera a proveedores externos mediante contrato. No hay que olvidar que tanto la protección de la información manejada regulado por ley, independientemente de su clasificación, como del negocio de la propia empresa, son dos de los activos fundamentales que deben ser protegidos, y que mejor forma de ser controlados que desde los más altos niveles de cualquier organización.

Figura 4-15 Operadores con redes 5G en España en 2022

En el caso de **las redes 5G** la ciberseguridad aún está por definir, sobre todo por la falta de análisis que aún no han permitido concretar, cuales son los vectores posibles de ataque y las TTP (técnicas táctica y procedimiento) empleados para perpetrar los mismos. En la figura 3-15 se muestran los logotipos de los cinco únicos operadores autorizados para el despliegue de redes 5G en España.

Dado que el despliegue de redes 5G es muy limitado, centrándose sobre todo a los núcleos de las grandes ciudades, a priori se podría pensar que esta ciberseguridad tendrá muchas similitudes con las aplicadas sobre las redes WIFI, WIMAX o 4G. De igual forma que en las redes inalámbricas actuales, mucha influencia la tendrá el tipo de cifrado que se emplee para securizar los canales empleados, al igual que los protocolos que se establezcan en los diferentes procesos o niveles. En este caso es previsible que

el ancho de banda ya no sea un problema, para emplear un protocolo u otro, pero si lo será que todas las comunicaciones salen al espectro electromagnético, en lugar de viajar encapsuladas en fibra óptica o cables de cobre, lo cual le confería cierta seguridad al menos física.

Habrá que espera a que los grandes operadores desplieguen esta tecnología, pero lo que no tiene sentido es no progresar en la propuesta de soluciones que la aseguren, tanto es así que ya existen proyectos a nivel privado y a nivel de la administración estatal, donde se licitan contratos para desarrollar laboratorios 5G que avancen en la ciberseguridad y ciberdefensa, así como la Inteligencia Artificial.

Atendiendo a las **tecnologías cuánticas** y a su apasionante y prometedor futuro, si ya en el 5G la ciberseguridad parece algo del futuro, en el caso del mundo cuántico está todavía parece inabordable o difícil de orientar. Esto es debido principalmente a que el desarrollo de la informática cuántica, se limita en la actualidad a un número muy reducido de supercomputadoras en manos de grandes corporaciones o gobiernos, cuya única utilidad por el momento, a parte del propio análisis y desarrollo de dicha tecnología, se basa en lograr un aumento exponencial de la capacidad de cálculo, al objeto de realizar operaciones complejas o inabordables por la informática de nuestros días.

Es por ello que pensar en desarrollar una ciberseguridad para estos supercomputadores, no parece algo necesario a corto o medio plazo, lo cual previsiblemente cambiará cuando ya haya un número de computadores interconectados, y lo será mucho más si de alguna forma se consigue que esta tecnología descienda incluso a nivel usuario doméstico.

Si por el contrario abordamos el tema de la cuántica, como el caso particular de buscar una solución para la problemática de muchas organizaciones, de tener que emplear circuitos seguros para enviar información clasificada como secreto, reservada o confidencial, este hecho ya es algo más tangible y alcanzable, dado que ya existen proyectos que lo están abordando.

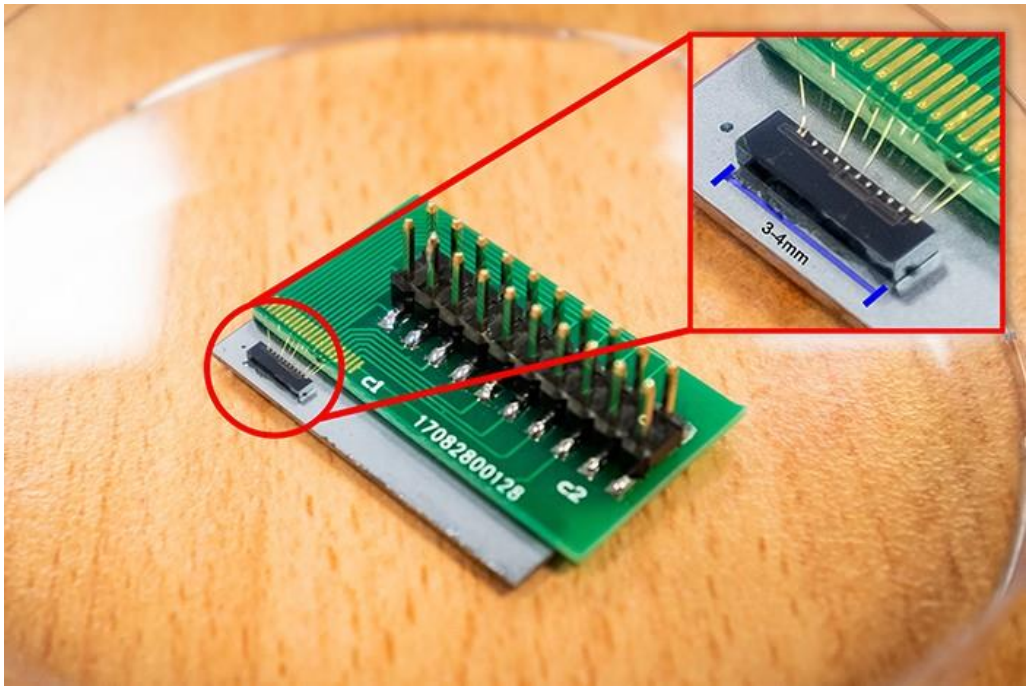
En este caso la propia cuántica, ya sería parte de la ciberseguridad en sí misma, ya que el proyecto contempla en su objetivo final último, el desarrollo de un dispositivo cifrador cuántico, que permita enviar esta información clasificada, de forma cifrada y por un canal no seguro, pero que en su fase inicial dado el desarrollo actual de esta tecnología, presumiblemente es solo un dispositivo transmisor de claves, que emplee propiedades de la mecánica cuántica en la fase de intercambió de claves, para evitar que la claves sea interceptadas por un atacante, sin que ese hecho pueda ser percibido por emisor y receptor.

En la actualidad ya existen protocolos que se han creado para esa finalidad como son BB84, B92 o en el de Artur Ekert (E91 o ERP) y el proyecto consiste groso modo en que los sistemas una vez implementados y en funcionamiento, se utilizarían para crear un cifrado perfecto del tipo One time Pad, sin el problema de tener que intercambiar la clave necesariamente en un canal seguro.

En su fase inicial permitirán el intercambio de claves seguro, claves que luego serán procesadas por un cifrador para cifrar el mensaje y trasmitirlo por ese mismo canal. Pero que en un futuro ese mismo dispositivo además de generar y transmitir esas claves, deberá poder cifrar los mensajes, por canales no seguros.

Este sistema supondría una evolución mayúscula en la seguridad, y cambiaría el paradigma de la trasmisión de información clasificada, abaratando costes al ser necesarios menor número de, equipos, sistemas y circuitos.

En la figura 3-16 se muestra un chip de solo 3 mm desarrollado por científicos de NTU, que utiliza algoritmos de computación cuántica.



Con un tamaño aproximado de 3 mm, el pequeño chip desarrollado por los científicos de NTU utiliza algoritmos de comunicación cuántica para una mejor seguridad que los estándares existentes de la industria.

También abre puertas para tecnologías de comunicación más seguras que se pueden implementar en dispositivos compactos como teléfonos inteligentes, tabletas y dispositivos portátiles.

Figura 4-16 Chip cuántico. Fuente: [27]

5 BIBLIOGRAFÍA

[1] **José Francisco García Gil** y **Pablo Francisco García de Zúñiga Hernández**, Ciberespacio, ciberterrorismo y ciberdefensa, Ejército de Tierra, dicembre 2020.

[2] **José Francisco García Gil y Panblo Francisco García de Zúñiga Hernández**, Técnicas de ciberataque y ciberdefensa, Ejército de Tierra, dicembre 2020

[3] BOE (Boletín Oficial del Estado), Real decreto 311/2022. de 3 de mayo, por el que se regurla el ENS (Esquem Nacional de Seguridad), publicación 4 mayo 2022

Páginas web

[4] «Web Microsoft Bing,» [En línea]. Available: https://www.bing.com. [Último acceso: 04 noviembre 2022].

[5] «Web de www.itu.int,» [En línea]. Available: https://www.itu.int [Último acceso: 29 noviembre 2022].

[6] «Web de Nextibs,» [En línea]. Available: https://www.nextibs [Último acceso: 07 noviembre 2022].

[7] «Web de La RAE,» [En línea]. Available: https://www.rae.es. [Último acceso: 04 noviembreo 2022].

[8] «Web de Respuestasabia,» [En línea]. Available: https://www.respuestasabia.com [Último acceso: 07 noviembre 2022].

[9] «Web de Wikipedia,» [En línea]. Available: https://es.wikipedia.org. [Último acceso: 04 de noviembre 2022].

[10] «Web de Protección de datos,» [En línea]. Available: https://protecciondatos-lopd.com. [Último acceso: 13 enero 2020

[11] «Web del Departamento de Seguridad Nacional,» [En línea]. Available: https://www.dsn.gob.es. [Último acceso: 04 noviembre 2022].

[12] «Web de Digitales,» [En línea]. Available: https://www.digitales.es [Último acceso: 04 noviembre 2022].

[13] «Web de Cuadernos de seguridad,» [En línea]. Available: https://cuadernosdeseguridad.com. [Último acceso: 04 noviembre 2022].

[14] «Web del CCN-CERT,» [En línea]. Available: https://www.ccn-cert.cni.es. [Último acceso: 04 noviembre 2022].

[15] «Web de IEBS,» [En línea]. Available: https://www.iebschool.co. [Último acceso: 04 noviembre 2022].

[16] «Web de F5,» [En línea]. Available: https://www.f5.com. [Último acceso: 04 noviembre 2022].

[17] «Web de Clavei,» [En línea]. Available: https://www.clavei.es. [Último acceso: 04 noviembre 2022].

[18] «Web de Sentinelone,» [En línea]. Available: https://es.sentinelone.com. [Último acceso: 04 noviembre 2022].

[19] «Web de Asiami,» [En línea]. Available: https://www.asiami.com [Último acceso: 07 noviembre 2022].

[20] «Web de Blockbit,» [En línea]. Available: https://www.blockbit.com. [Último acceso: 04 noviembre 2022].

[21] «Web de ciberseguridad.com,» [En línea]. Available: https://ciberseguridad.com. [Último acceso: 4 noviembre 2022].

[22] «Web de Firmadocumentos,» [En línea]. Available: https://firmadocumentos.es. [Último acceso: 04 noviembre 2022].

[23] «Web de Fortinet,» [En línea]. Available: https://www.fortinet.com [Último acceso: 11 noviembre 2022].

[24] «Web de Ayudaleyprotecciondatos,» [En línea]. Available: https://ayudaleyprotecciondatos.es. [Último acceso: 04 noviembre 2022].

[25] «Web de Google,» [En línea]. Available: https://www.google.es. [Último acceso: 04 noviembre 2022].

[26] «Web del Centro Criptlógico Nacional,» [En línea]. Available: https://www.ccn.cni.es. [Último acceso: 04 noviembre 2022].

[27] «Web de Código oculto,» [En línea]. Available: https://www.codigooculto.com [Último acceso: 04 noviembre 2022].

[28] «Web de Kaspersky,» [En línea]. Available: https://latam.kaspersky.com. [Último acceso: 04 noviembre 2022].

[29] «Web de Invgate,» [En línea]. Available: https://www.invgate.com [Último acceso: 11 noviembre 2022].

[30] «Web de Deloite,» [En línea]. Available: https://www.deloitte.com [Último acceso: 11 noviembre 2022].

[31] «Web de websiterating.com,» [En línea]. Available: https://www.websitersting.com [Último acceso: 11 noviembre 2022].

[32] «Web de Newtral,» [En línea]. Available: https://www.newtral.es. [Último acceso: 04 noviembre 2022].

[33] «Web de INCIBE,» [En línea]. Available: https://www.incibe-cert.es. [Último acceso: 04 noviembre 2022].

[34] «Web del Equipos de Ciberseguridad y Gestión de Incidentes españoles CSIRT,» [En línea]. Available: https://www.csirt.es [Último acceso: 04 noviembre 2022].

[35] «Web del Portal de Adminsitración Electrónica,» [En línea]. Available: https://administracionelectronica.gob.es [Último acceso: 04 noviembre 2022]

[36] «Web Ehe Data Driven Company,» [En línea]. Available: https://artyco.com [Último acceso: 04 noviembre 2022].

[37] «Web de Comunicare,» [En línea]. Available: https://www.comunicare.es. [Último acceso: 04 noviembre 2022].

[38] «Web de Checkpoint,» [En línea]. Available: https:// www.checkpoint.com [Último acceso: 04 noviembre 2022].

[39] «Web de Incopyme,» [En línea]. Available: https://www.incopyme.com. [Último acceso: 04 noviembre 2022].

[40] «Web de Cisco,» [En línea]. Available: https://www.cisco.com [Último acceso: 07 noviembre 2022].

ANEXO I: CIBERAMENAZAS EN EL MUNDO

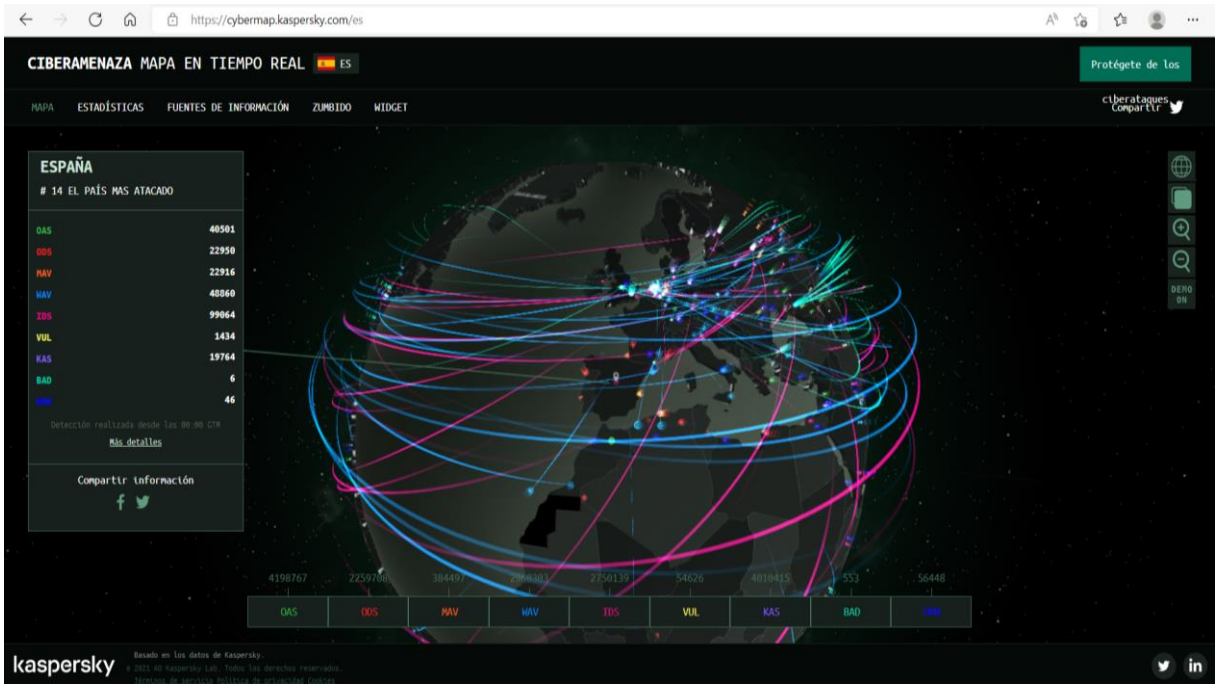


Figura A1-1 Web que muestra las ciberamenazas en el mundo en tiempo real. Fuente: [28]

El día en el que se realiza la consulta fue el 04 de noviembre de 2022 sobre la página web de Kaspersky.com. [28]

	MUNDO	**ESPAÑA (puesto 14)**
OAS On-Access Scan	4.198.767	40.501
ODS: On Demand Scan	2.259.768	22.950
MAV: Mail Anti-virus	384.497	22.916
WAV: Web Anti-virus	2.968.303	48.860
IDS: Intrusion Detection Scan	2.750.139	99.064
VUL: Vulnerability Scan	54.626	1.434
KAS: Kaspersky Anti-Spam	4.010.415	19.764
BAD: Botnet Activity Detection	553	6
RMN: Ransomware	56.448	46

OAS (On-Access Scan).

Muestra el flujo de detección de malware durante el escaneo On- Access, por ejemplo, cuando los objetos son accedidos durante las operaciones abrir, copiar, ejecutar o guardar operaciones.

ODS (On Demand Scanner).

Muestra el flujo de detección de malware durante el análisis bajo pedido, cuando el usuario selecciona manualmente la opción "Buscar virus" en el menú de contexto.

MAV (Mail Anti-virus).

Muestra el flujo de detección de malware durante el escaneo MAV cuando aparecen nuevos objetos en una aplicación de email (Outlook, The Bat, Thunderbird).MAV escanea los mensajes entrantes y llama a OAS cuando guarda los adjuntos a un disco.

WAV (Web Anti-virus).

Muestra el flujo de detección de malware durante el análisis Web Anti-Virus donde la página html de un sitio web se abre o un archivo es descargado.

DS (Sistema de Detección de Intrusos).

Muestra el flujo de detección de los ataques a las redes.

VUL (Vulnerability Scan).

Muestra el flujo de la detección de vulnerabilidades.

RMW (Ransomware).

Muestra el flujo de detección del ransomware

KAS (Kaspersky Anti-Spam).

Muestra el tráfico sospechoso y no deseado descubierto por las tecnologías de Filtrado de Reputación de Kaspersky.

BAD (Detección de Actividad Botnet).

Muestra estadísticas sobre direcciones IP de víctimas de ataques DDoS y servidores botnet C&C.

ANEXO II: 14 TIPOS DE CIBERATAQUE

A continuación se muestran los 14 tipos de ciberataque más comunes según el blog la página web: INVGATE.COM. https://blog.invgate.com/es/tipos-de-ciberataque [29]

1 Malware

El primer tipo de ciberataque que nombramos aquí seguramente ya lo conoces. El **malware** es un término amplio que contempla diferentes clases de software malicioso, incluyendo virus, gusanos y spyware. Estos ataques aprovechan una vulnerabilidad y se introducen en la red para plantar el código nocivo.

2 Phishing

Otro de los tipos de ciberataque es el **phishing**, que se refiere a estafas orientadas a engañar a los usuarios para que revelen sus credenciales o cualquier otra forma de información confidencial. Esta **clase de ciberamenaza** recurre a la tecnología y a la ingeniería social para que las personas entreguen datos sensibles que luego serán utilizados con fines fraudulentos.

El atacante puede llamar, enviar un correo electrónico o WhatsApp a la víctima diciéndole que una determinada organización se pone en contacto con ella para actualizar información, y así le pide un PIN o una contraseña, por ejemplo. El phishing es un ejemplo de ingeniería social.

Como parte de un ataque de phishing, el hacker manda a la víctima un mensaje con un archivo adjunto malicioso o un enlace que la redirige a un sitio web engañoso donde descarga el malware.

Incluso puede ser una web falsa que emula a una legítima, como las propias redes sociales, en la que se pide al usuario que inicie sesión. Cuando la ejecuta, el atacante se hace con su nombre de usuario y contraseña.

Estos últimos ejemplos de phishing combinan la ingeniería social con la tecnología (código malicioso) diseñada para engañar a la persona con la finalidad de que revele datos sensibles.

3 Ataque de día cero

Un **ataque de día cero** es una vulnerabilidad que no fue revelada públicamente. Los hackers aprovechan ese momento antes de que el proveedor tenga la oportunidad de solucionarlo. Suele ser muy peligroso porque no hay protección hasta que se publica el parche.

Este tipo de ataques puede afectar a cualquier empresa y proveedor, sin importar el tamaño o la precaución tomada sobre el asunto. Por ejemplo, Google informó de seis vulnerabilidades de día cero en 2022. La empresa tuvo que lanzar actualizaciones de emergencia para solucionar los inconvenientes, las cuales tienen que instalarse rápidamente por los usuarios y las organizaciones. Es parte del proceso de gestión de parches.

4 Ramsomware

El **ransomware** incluye un código malicioso que cifra los datos para hacerlos inaccesibles a la víctima. Este programa suele utilizarse para exigir el pago de un rescate para que la víctima pueda descifrar los archivos, carpetas y sistemas cautivos.

El procedimiento consiste en que la víctima descarga (sin saberlo) el código malicioso desde un sitio web o un archivo adjunto. Luego, este software aprovecha una vulnerabilidad del sistema y encripta la información.

5 Ataque con contraseña

Los **ciberdelincuentes** se hacen con las contraseñas de la víctima de varias maneras. Una de ellas es probando diferentes combinaciones hasta conseguir la correcta. Obviamente que este método es más simple cuando la víctima utiliza palabras como "contraseña" o combinaciones como "12345" en lugar de un gestor de contraseñas.

Otra vía utilizada es recurrir a un software que permite probar en forma automatizada todas las combinaciones posibles del diccionario: de hecho se la conoce como **ataque de diccionario**.

Dentro del **ataque con contraseña** también es frecuente usar una web falsa donde el usuario escribe sus credenciales. O le proporciona los passwords a un ciberdelincuente -que se hace pasar por un banco, una empresa o alguna otra organización- por teléfono o mensaje. Se trata de un ataque con contraseña realizado mediante phishing.

A veces los delincuentes prueban combinaciones de nombres de usuario y contraseñas obtenidas en la web oscura. Son listas de datos comprometidos que provienen de filtraciones o ataques.

6 Ataque DoS y DDoS

Un **ataque de denegación de servicio o Denial of Service (DoS)** apunta a colapsar una red inundándola de tráfico. Lo hace mediante el envío de muchas peticiones, por lo que los recursos se ven desbordados, el sitio no puede responder, se apaga y se vuelve inaccesible para los usuarios.

Por su parte, un ataque de denegación de servicio distribuido o Distributed Denial of Service (DDoS) es un **ataque DoS** que utiliza múltiples máquinas (dispositivos remotos, bots o zombis) para que la red objetivo se vea desbordada. En consecuencia, el servidor se sobrecarga -más rápidamente que en un ataque DoS normal-.

7 Spoofing de DNS

Otro de los tipos de ciberataque es el **spoofing del Domain Name Server (DNS)** o servidor de nombres de dominio, que consiste en alterar el DNS para redirigir el tráfico a un sitio web falso que emula a uno legítimo.

En este **tipo de ciberataque**, la víctima introduce su nombre de usuario y contraseña para iniciar la sesión, facilitando estos datos a los hackers.

8 Ataques MitM o Man-in-the middle

En un **ataque de Man in the Middle** u hombre en el Medio (MitM), el delincuente intercepta la comunicación entre dos personas en forma secreta e incluso puede alterarla.

Este procedimiento es posible llevarlo adelante cuando la conexión se realiza desde un punto de acceso wi-fi no cifrado. Obviamente que las personas que participan de la conversación no saben que el atacante está espiando o modificando la información compartida.

9 Ataque de troyanos

Un **ataque de troyanos** recurre a un malware que se esconde dentro de un archivo o aplicación para engañar al usuario. Están diseñados para infligir diferentes tipos de daños a la red, dependiendo la acción que se pretende realizar.

En la mayoría de los casos, se utilizan para establecer una puerta trasera en la red. De este modo, el atacante puede robar datos sensibles o instalar otro malware en el sistema. A diferencia de un virus, un troyano no se replica.

10 Ataques de inyección SQL

Una inyección de lenguaje de consulta estructurado o Structured Query Language (SQL) -**inyección SQL**- es una amenaza de ciberseguridad que tiene como objetivo los sitios que utilizan bases de datos para servir a los usuarios.

El atacante obtiene acceso no autorizado a la base de datos de una aplicación web añadiendo una cadena de código malicioso a una consulta. Esta manipulación del código SQL permite al delincuente obtener información confidencial y sensible, como la correspondiente a las tarjetas de crédito.

11 Cross-site scripting

El **cross-site scripting** hace que un sitio vulnerable devuelva al usuario un JavaScript malicioso para que el código se ejecute en su navegador. Cuando esto ocurre, el atacante obtiene el control y compromete la interacción con la aplicación, accediendo a cualquier acción que desee ejecutar.

Incluso si la víctima tiene un ingreso privilegiado a los datos críticos, los atacantes podrían obtener el control total de esa información.

12 Ataque de cumpleaños

Un **ataque de cumpleaños** es un tipo de ataque criptográfico en el que el ciberdelincuente tiene como objetivo los algoritmos hash, que son firmas digitales destinadas a verificar la autenticidad de las comunicaciones.

Si un delincuente crea un hash idéntico al enviado, puede sustituir el mensaje original por el suyo, por lo que la parte receptora lo recibirá sin sospechar que el contenido fue alterado.

Este tipo de **ciberataque de fuerza bruta** explota las matemáticas que hay detrás de la paradoja del cumpleaños -que dice que en un grupo aleatorio de 23 personas, hay un 50% de posibilidades de que dos de ellas cumplan el mismo día- en una teoría de la probabilidad.

13 Rootkits

Los **rootkits** se refieren a un grupo de herramientas de software que permiten a los delincuentes obtener acceso no autorizado a un sistema sin ser detectados.

Un rootkit esconde programas maliciosos que llegan a los dispositivos a través del spam o de otras formas.

Cuando el rootkit se activa, se crea una puerta trasera y los delincuentes pueden instalar otras formas de malware como ransomware o troyanos.

14 Amenaza interna

Para cerrar los **tipos de ciberataque,** la amenaza interna involucra a las personas que trabajan dentro de una organización y que utilizan el acceso autorizado o sus conocimientos sobre la entidad para lanzar un ataque.

El **ataque de amenaza interna** puede provocar daños y pérdidas de datos y afectar a la reputación de la empresa.

ANEXO III: LOS 5 MAYORES CIBERATAQUES DE LA HISTORIA

A continuación se muestran los 5 mayores ciberataques de la historia según la página web: WWW2.DELOITTE.COM.

https://www2.deloitte.com/es/es/pages/risk/articles/los-cinco-mayores-ciberataques-de-la-historia.htm). [30]

WANNACRY

12 de mayo de 2017, ordenadores en toda Europa ven afectados sus sistemas, encriptados sus archivos y bloqueados los accesos de administrador a sus usuarios.

Cunde el pánico.

Miles de empresas quedan paralizadas en cuestión de minutos debido a un ransomware distribuido en la red llamado WannaCryptor (conocido como WannaCry). El que, probablemente, por alcance a sistemas afectados y pérdidas económicas, ha sido el virus más destructor de la época actual. El malware se coló por una vulnerabilidad de un parche de seguridad instaurado semanas antes que infectó a más de 360.000 equipos. Se calcula que el impacto en pérdidas directas e indirectas alcanzó la suma de 4.000 millones de euros.

WannaCry ha supuesto un antes y un después en el mundo de la seguridad cibernética.

CONFICKER

Octubre de 2008, un complejo gusano se infiltra aprovechando una grieta explotable de Windows server, los sistemas vulnerables son Windows 2000, Windows XP, Windows Vista, Windows Server 2003 y Windows server 2008.

El ataque se vuelve masivo.

Su complejidad hace saltar las alarmas. Se esparce a tal velocidad que se le cataloga como una amenaza a nivel militar. Departamentos de Seguridad del Estado de todo el mundo, Fuerzas Armadas, hospitales, y un gran número de entidades privadas no escaparon a sus garras. En pocas semanas infectó a más de 10 millones de equipos en 190 países.

La empresa Microsoft ofreció una suma de 250.000 dólares para quien les facilitase información que desenmascarase a los creadores del Gusano Conficker.

STUXNET

Verano de 2010, el espía más sofisticado de nuestros días hace su aparición con un objetivo: Infraestructuras críticas y entornos industriales en Irán, como centrales nucleares o plantas de energía. El virus Stuxnet se instalaba en los sistemas, robaba su información y más tarde les ordenaba que se autodestruyeran.

Este malware es catalogado como el más desarrollado e innovador hasta la fecha. Analistas y expertos afirman que Stuxnet retrasó el progama nuclear Iraní provocando grandes daños físicos. Los datos de impacto oficiales nunca fueron revelados por ese gobierno.

Está comprobado que para desarrollar un virus tan sofisticado hacen falta meses de trabajo y un gran fondo económico detrás.

PETYA

2016, aparece un ransomware que infecta los ordenadores, encripta los datos haciendo imposible su uso para el usuario y pide un rescate a cambio.

Este virus, que afectaba a los sistemas Windows, accedía a través de un PDF ejecutable que la víctima abría para así dar comienzo a la fatalidad. A continuación, las pantallas de los equipos exhibían una calavera negra en fondo rojo y mostraban el mensaje de rescate. Petya le costó a la naviera danesa Maersk alrededor de unos 250 millones de euros. Pero lo peor estaba aún por venir…

En marzo de 2017 una nueva versión de este virus aparece, su nombre: NotPetya. Esta mutación es aparentemente similar a su fuente, sin embargo, este no necesita de la aceptación del usuario para introducirse en el equipo y por mucho que se pagase el rescate los archivos no se recuperaban. NotPetya no necesitaba de gestión humana, el virús actuaba por su cuenta infectando miles de sistemas diarios. Estaba fuera de control.

Su impacto a nivel económico todavía hoy no ha sido calculado.

ILoveYOU

Principios de milenio, alrededor de 60 millones de equipos son infectados a través de un correo electrónico spam con asunto LoveLetter4YOU. El motivo por el que esta campaña de phishing fue tan efectiva fue porque, por aquel entonces, no había tanta información sobre ciberseguridad y los usuarios abrían sus emails sin dudarlo. I HATE GOING TO SCHOOL es el texto que aparecía al abrir el correo, era el indicador de que el ataque había comenzado.

ILoveYOU se instalaba en el ordenador y borraba todos los ficheros con extensiones JPG, JPEG y MP3 y los sustituía por un troyano que intentaba recabar información confidencial.

Impacto total en coste económico: 1200 millones de dólares.

ANEXO IV: ESTADÍSTICAS DE CIBERSEGURIDAD

A continuación se muestran estadísticas y datos relevantes sobre ciberseguridad conocidos hasta 2020 en todo el mundo según la página www.websiterating.com.
https://www.websiterating.com/es/research/cybersecurity-statistics-facts/ [31]

- El 85% de las infracciones de seguridad cibernética son causadas por errores humanos.
- El 94% de todo el malware se envía por correo electrónico. (CSO en línea).
- Los ataques de ransomware ocurren cada 10 segundos.
- El 71% de todos los ataques cibernéticos están motivados económicamente (seguidos por el robo de propiedad intelectual y luego el espionaje).
- 445 millones de ciberataques ocurrieron en 2020 a nivel mundial.
- Se estima que el costo global anual de la ciberdelincuencia será de $ 10.5 billones para 2025.
- Se estima que la industria de la ciberseguridad tendrá un valor de más de $ 400 mil millones para 2027.
- En 2021 la industria de la ciberseguridad tuvo una tasa de desempleo del 0%.
- Más del 80% de los eventos de ciberseguridad involucran ataques de phishing.
- Google descubrió más de 2.1 millones de sitios de phishing en enero de 2020.
- Hubo un ataque de ransomware cada 10 segundos en 2020.
- Durante la próxima década, el costo de los ataques de ransomware superará los $ 265 mil millones.
- 2020 vio la primera muerte conocida por un ciberataque relacionado con ransomware.
- En 2020, en promedio, se necesitaron 207 días para identificar las brechas de seguridad informática.
- Marriott admite que una violación de seguridad en 2020 expuso los datos de al menos 5.2 millones de huéspedes.
- Más del 90% del malware llega a través del correo electrónico.
- 1 de cada 36 teléfonos inteligentes Android tiene instaladas aplicaciones peligrosas.
- Hay 2,244 ciberataques por día y 164 ciberdelitos denunciados todos los días.
- Casi la mitad de todos los ciberataques se dirigen a pequeñas empresas.
- Las violaciones de datos expusieron 36 mil millones de registros a fines del tercer trimestre de 2020.
- Las brechas de ciberseguridad reducen el valor de las empresas públicas en un 8.6% estimado.
- Una de las firmas de seguridad más grandes del mundo admite que fue víctima de un hackeo sofisticado en 2020.
- El 66% de las empresas estuvieron expuestas al phishing en 2020.
- El 43% de las pequeñas y medianas empresas (PYMES) aún no han adoptado planes de mitigación y evaluación de la ciberseguridad.
- El 20% de las pequeñas empresas permiten el trabajo remoto sin tener un plan de ciberseguridad.
- Los piratas informáticos robaron más de 9 millones de registros médicos en septiembre de 2020.
- Aproximadamente el 30% de los trabajadores de la educación no aprobaron una prueba de phishing.
- Más del 40% de los casos de ciberseguridad en la educación son causados por tácticas de ingeniería social.
- El 32% de las empresas pagan un rescate para recuperar sus datos.
- Alrededor de 60 millones de estadounidenses han sido afectados por el robo de identidad.

- Estados Unidos sufre la mayor cantidad de violaciones de datos por ubicación.
- 2244 ataques ocurrieron todos los días que es casi 1 ciberataque cada 39 segundos.
- Rusia, Brasil y China son los tres principales países donde se originan los ciberataques.
- En promedio, toma alrededor de 280 días para detectar y detener un ciberataque.
- Hoy en día, las mejores técnicas de seguridad disponibles son el cifrado, antivirus, firewall, firmas digitales y autenticación de dos factores.
- Los aviones de combate F-35 enfrentan mayores amenazas de ciberataques que de misiles enemigos.