Universitat Oberta de Catalunya

uoc.edu

La ciberseguridad como reto internacional:
La protección frente a las ciberamenazas

Autora: Anna Lourdes Ferrando Guillem

Director: Jorge Chinea López

Máster Interuniversitario de Seguridad en las Tecnologías de la Información y las Comunicaciones(Mistic)

Área del Trabajo Final de Máster: Ad Hoc INCIBE

FICHA DEL TRABAJO FINAL

Título del trabajo:	*La ciberseguridad como reto internacional: La protección frente a las ciberamenazas*
Nombre del autor:	*Anna Lourdes Ferrando Guillem*
Nombre del consultor/a:	*Jorge Chinea López*
Nombre del PRA:	*Víctor García Font*
Fecha de entrega (mm/aaaa):	12/2018
Titulación:	*Máster en Seguridad de las Tecnologías de la Información y de las Comunicaciones*
Área del Trabajo Final:	*TFM-Ad hoc*
Idioma del trabajo:	*Castellano*
Palabras clave	*Tecnologías de la información, Internet, Protección de datos*

Resumen del Trabajo:

Hay más de 4.000 millones de personas en el mundo conectadas a Internet y esa cifra aumenta diariamente. Ante este escenario, en el que cada día son más necesarias las tecnologías emergentes para realizar cualquier actividad cotidiana, la ciberseguridad se convierte en algo imprescindible para poder garantizar la seguridad de las Tecnologías de la Información y de la Comunicación.

En este Trabajo Final de Máster, se utilizará una metodología documental, para llevar a cabo un análisis en profundidad sobre la ciberseguridad en el ámbito internacional. Se estudiarán las ciberamenazas más relevantes en estos momentos y como existen leyes, normas, organismos y tratados de cooperación internacionales para hacer frente a estas ciberamenazas y a los ciberdelincuentes que intentan materializarlas. Además, se realizará un estudio exhaustivo de los principales ciberataques internacionales que han sucedido recientemente y de los posibles ataques que podrían ocurrir en un futuro.

Una vez llevado a cabo el análisis sobre la ciberseguridad en el ámbito internacional, se llega a la conclusión de que hay que seguir mejorando la ciberseguridad y que la bases para esa mejora se encuentra en dar formación a los usuarios y en aumentar la capacidad de cooperación internacional para formar un frente común en la lucha contra las ciberamenazas.

Abstract :

There are more than 4000 million people in the world connected to the Internet and that number increases daily. In the face of this scenario, where emerging technologies are essential for everyday activities, Cyber Security becomes indispensable in order to ensure the security of the Information and Communication Technologies.

In this Master's Final Project, the purpose is to analyse Cyber Security using a documentary research. This in-depth analysis will cover the most relevant cyber-threats and cyber-criminals that exist currently, as well as the laws, norms, agencies and International Cooperation Treaties created to deal with them. Furthermore, there will be a thorough study of the main international cyber-attacks in recent history and the possible ones that could occur in the future.

With the results of this analysis, the conclusion obtained is that Cyber Security must continue its development. And the basis for this consists in two key points: to provide the information needed to users and to improve international cooperation to form a united front in the fight against cyber-threats.

Índice

Lista de figuras

1. Introducción

1.1 Contexto y justificación del Trabajo

En un mundo en el que la tecnología de la información y las comunicaciones es de vital importancia, estamos a merced de los hackers que crean y buscan nuevas maneras de obtener beneficios a costa de provocar incidentes de seguridad internacionales. Según Gartner [1] el presupuesto mundial destinado a Seguridad en TI en 2018 será de aproximadamente 114 billones de $ y se estima que crezca en un 8,7% en 2019, siendo el gasto esperado de 124 billones de $. Aunque se aumenta la inversión anualmente, no es suficiente para frenar los ciberataques y sus devastadoras perdidas económicas. Deloitte estima que el ransomware “WannaCry”, que infecto unos 15 millones de equipos en 2017, podría haber provocado unas pérdidas de unos 200 millones de € en el mundo [2].

La entrada en vigor del Reglamento General de Protección de Datos(RGPD) en mayo de 2018, es un paso hacia delante en la protección de la información, pero hay que seguir profundizando en este tema y buscar la forma de mejorar las leyes existentes o incluso crear nuevas para salvaguardar los datos de usuarios y empresas.

En este Trabajo Final de Máster se pretende hacer un estudio exhaustivo de la ciberseguridad a escala mundial. Se mostrarán los fundamentos en los que se basa la ciberseguridad, se analizará la normativa existente a nivel internacional, que organizaciones velan por la ciberseguridad y si existen tratados de cooperación entre países y finalmente estudiaremos los ciberataques que se están produciendo globalmente, sus consecuencias y las soluciones que se pueden implementar para evitarlos o minimizar su impacto.

1.2 Objetivos del Trabajo

La finalidad del presente Trabajo Final de Máster es estudiar la ciberseguridad a nivel internacional y buscar posibles mejoras en la protección contra las ciberamenazas. Para lograr nuestro propósito tendremos que alcanzar los siguientes objetivos:

- Analizar los fundamentos de la ciberseguridad y estudiar y clasificar los tipos de ciberamenazas que existen actualmente.
- Documentarse sobre las normativas, tratados y leyes internacionales en seguridad de las TIC para así analizar los puntos débiles y fuertes que poseen cada una de ellas.
- Recabar información sobre los organismos y entidades dedicados a la seguridad de las TIC a nivel internacional. Estudiar las relaciones existentes entre dichas entidades y de qué forma gestionan la ciberseguridad en cada país.

- Estudiar los tratados de cooperación entre países para así poder establecer sus características fundamentales, sus similitudes y sus diferencias.
- Analizar ciberataques que hayan sucedido a escala global para conocer en profundidad como se han gestionado, que leyes o normas se han aplicado, que entidades han intervenido y si se ha utilizado algún tratado de cooperación para resolverlos.
- Realizar un análisis exhaustivo de toda la documentación recopilada y proponer mejoras en el sector de la ciberseguridad.
- Presentar las conclusiones que se han obtenido de la realización de este trabajo y su posible desarrollo futuro.

1.3 Enfoque y método seguido

La metodología que se seguirá para poder cumplir los objetivos establecidos será del tipo documental y se organizará en las siguientes fases:

- *Definición del plan de trabajo:* En esta primera fase se explicará el contexto y la justificación de este Trabajo Final de Máster. Se marcarán unos objetivos y una metodología para llevarlos a cabo. También se realizará una planificación aproximada de las tareas a realizar y una revisión general del estado del arte de la ciberseguridad.
- *Fundamentos de la Ciberseguridad y ciberamenazas*: Para esta fase se llevará a cabo una búsqueda de documentación relativa a la ciberseguridad y se analizará a fondo para poder ofrecer una clasificación de las amenazas existentes en la actualidad.
- *Leyes y Normas internacionales:* En esta etapa se estudiará la legislación internacional existente en ciberdelitos. Se profundizará en la legislación europea y española, ya que son las que nos afectan directamente y se mostraran las últimas propuestas legislativas que se han presentado en materia de ciberseguridad.
- *Organismos Internacionales de Ciberseguridad:* Esta fase es documental y se llevará a cabo buscando las principales entidades existentes en Seguridad de las Tecnologías de la Información. Se estudiará su funcionamiento, si hay relaciones entre ellas y como operan cuando se produce un incidente a escala mundial.
- *Tratados de Cooperación Internacionales:* Esta etapa se centrará en recabar información sobre los tratados de cooperación existentes. Se analizará la documentación obtenida y se compararan los distintos acuerdos internacionales para conocer las características más favorables que puede tener un tratado de cooperación en Ciberseguridad.
- *Ciberataques mundiales:* Esta fase será las más relevante del Trabajo Final de Máster. Se documentarán los ataques más importantes que han sucedido en los últimos años. Se buscarán similitudes y diferencias entre ellos con la finalidad de buscar patrones que puedan ayudar a prever futuros ataques.
- *Conclusiones y futuros trabajos:* Esta será la etapa final del trabajo y por tanto aquí mostraremos los resultados que hemos obtenido a lo largo de

toda la investigación. Se recopilarán las conclusiones obtenidas en el resto de los capítulos y finalmente se propondrán futuros trabajos que puedan seguir mejorando la Ciberseguridad.

1.4 Listado de tareas

Se va a detallar a continuación la lista de tareas necesarias para llevar a cabo la metodología expuesta en el apartado anterior.
Plan de trabajo:

- Contexto y justificación.
- Objetivos.
- Metodología.
- Listado de tareas.
- Planificación.
- Revisión del estado del arte.

Fundamentos de la Ciberseguridad y Ciberamenazas:

- Búsqueda de documentación de Ciberseguridad y Ciberamenazas existentes.
- Análisis de la documentación.
- Clasificación de Ciberamenazas.

Leyes y Normas internacionales:

- Investigación sobre leyes y normas internacionales.
- Análisis de las principales normas existentes en Ciberseguridad.

Organismos Internacionales en Ciberseguridad:

- Investigación para recabar información sobre las entidades internacionales existentes.
- Estudio de los diferentes tipos de organismos en Ciberseguridad existentes.

Tratados de Cooperación Internacionales:

- Búsqueda de documentación sobre Tratados de Cooperación en Ciberseguridad.
- Análisis comparativo de los diferentes tratados hallados.

Ciberataques mundiales:

- Investigación sobre ciberataques mundiales.
- Análisis de la tipología de los ataques.
- Conclusiones y mejoras para poder evitar futuros ataques.

Conclusiones y trabajo futuro

- Conclusiones del Trabajo Final de Máster.
- Trabajo futuro.
- Revisión de Memoria y documentación.

Realización de la presentación:

- Preparación de la presentación en PowerPoint.
- Realización del video de la exposición de la presentación.

Defensa del Trabajo Final de Máster:

- Periodo en el que el tribunal podrá presentar preguntas sobre el Trabajo Final de Máster y el alumno deberá contestarlas mediante correo electrónico.

1.5 Planificación del Trabajo

A continuación, mostraremos la planificación temporal de las tareas principales del listado del punto 1.4. No se ha asignado una planificación temporal a las subtareas ya que en muchas ocasiones se realizarán de forma simultánea. A cada entregable del proyecto se le han asignado sus tareas como se puede observar en la siguiente imagen:

Nombre	Fecha de inicio	
TFM	19/09/18	18/01/19
PEC1	19/09/18	8/10/18
Plan de trabajo	19/09/18	8/10/18
PEC 2	9/10/18	5/11/18
Fundamentos de la Ciberseguridad y Ciberamenazas	9/10/18	22/10/18
Leyes y Normas internacionales	23/10/18	5/11/18
PEC 3	6/11/18	3/12/18
Organismos Internacionales en Ciberseguridad	6/11/18	20/11/18
Tratados de Cooperación Internacionales	20/11/18	3/12/18
PEC 4	4/12/18	31/12/18
Ciberataques Mundiales	4/12/18	21/12/18
Conclusiones y Trabajo Futuro	24/12/18	27/12/18
Revisión de Memoria y Documentación	28/12/18	31/12/18
Realización Presentación	1/01/19	8/01/19
Preparación Presentación	1/01/19	2/01/19
Realización vídeo	3/01/19	8/01/19
Defensa TFM	14/01/19	18/01/19

Figura 1 : Listado de tareas realizado con Gantt project

En la figura que se muestra a continuación, se observa el diagrama de Gantt en el que se especifica la tarea a realizar y el periodo temporal en el que se llevará a cabo.

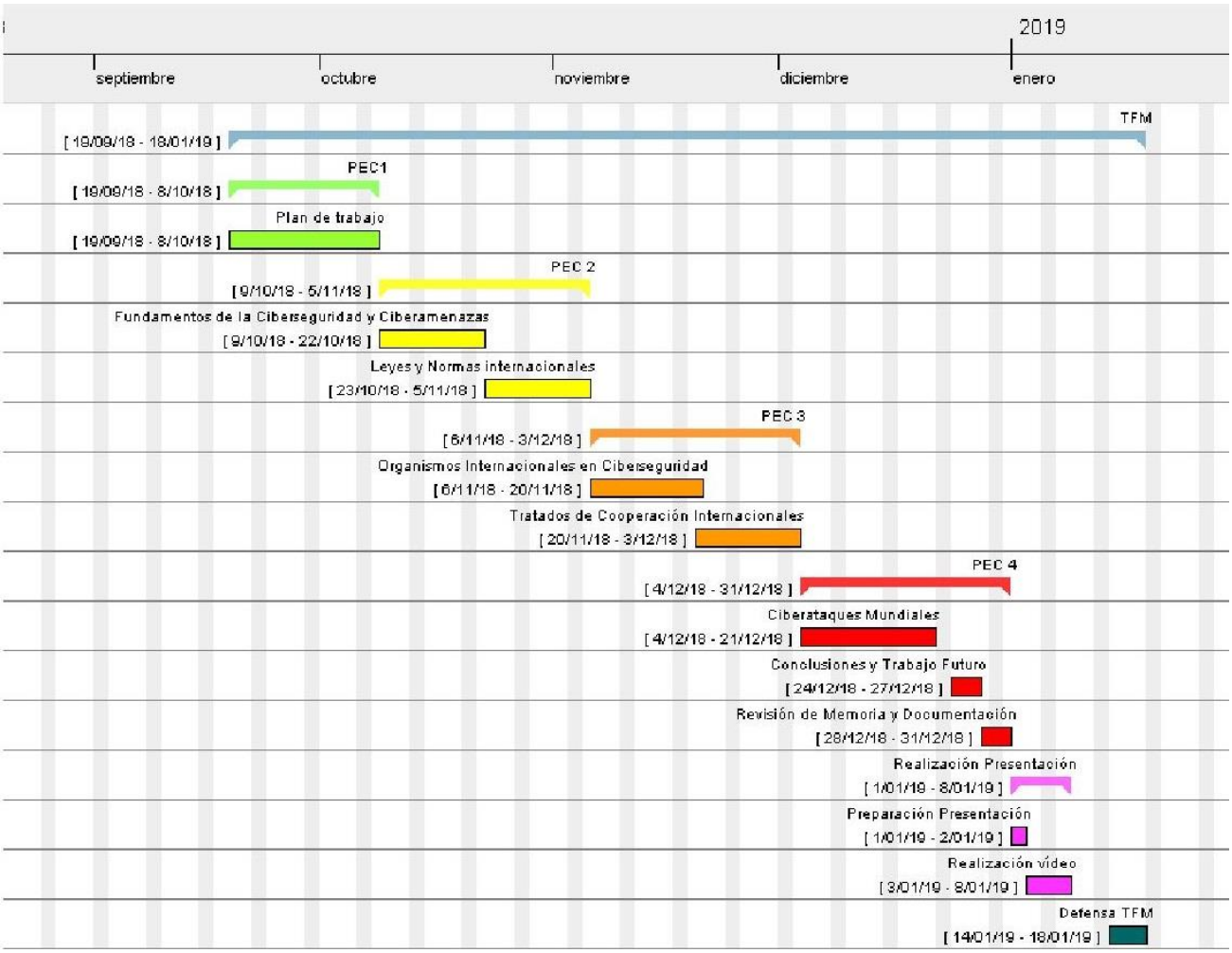


Figura 2: Diagrama de Gantt realizado con Gantt project

1.6 Revisión del Estado del Arte

Para la revisión del estado del arte en Ciberseguridad se ha obtenido información del "Gartner Forecasts Worldwide Information Security Spending to Exceed $124 Billion in 2019"[1] de Gartner, del "Reporte Anual de Ciberseguridad" [3] de Cisco, del documento "Tendencias en Ciberseguridad 2018: El costo de nuestro mundo Conectado" [4] de ESET, del artículo "Del año del ransomware al año del cryptojacking" [6] de Panda Security, y de noticias actuales en el mundo de la Seguridad en las TIC [5].

Vamos a presentar los puntos que se consideran más relevantes de los informes y artículos estudiados y que pueden darnos una visión de conjunto del estado actual de la Seguridad en la Tecnología de la Información y las Comunicaciones.

- Según el artículo de Gartner [1], este año el gasto mundial en ciberseguridad aumentará en un 12,4% respecto de 2017. Además,

también se indica que en 2017 la mayor parte de los gastos en ciberseguridad se destinaron a riesgos en seguridad en primer lugar, en segundo lugar, a las necesidades de negocio y en tercer lugar a los cambios en la industria. De este análisis se deprende que cada día se invierte más en seguridad y que las organizaciones van tomando conciencia de que la información es un activo fundamental y que hay que protegerlo y gestionar sus riesgos adecuadamente.

- El Reglamento General de Protección de Datos(RGPD) entra en vigor en mayo de 2018 con un consiguiente aumento de la protección de la privacidad para los usuarios. Después de escándalos como el de Facebook y su cesión de datos de carácter sensible a la empresa Cambridge Analytica [5], que se hizo sin consentimiento de los usuarios, se extreman las medidas de seguridad para proteger los datos de carácter personal y se aplican sanciones a las empresas que las incumplen, intentando así evitar la venta de datos personales que luego se utilizan para big data o con otras finalidades poco ortodoxas.
- Cloud Computing y el Internet of Things(IoT) son avances que han revolucionado el mercado y la forma de concebir nuestro entorno. Al estar aún en desarrollo, existen enormes brechas de seguridad que ayudan a que atacantes o “hackers” se lucren de estos agujeros para provocar ataques internacionales que repercuten en empresas y usuarios finales. También existen numerosas vulnerabilidades en los dispositivos de realidad aumentada, que cada vez son más demandados, y que como el IoT no disponen de un sistema de seguridad sofisticado.
- El ransomware está tomando nuevas formas y se adapta a nuevos entornos haciéndose más difícil su erradicación. En 2017 se produjo la aparición de los cryptoworms que atacan sin que sea necesaria la intervención humana. Esta nueva generación de ransomware se propaga a través de la red y han sido utilizados en dos de los ataques más importantes de 2017(WannaCry y Petya).
- Las criptomonedas llevan varios años en auge y la minería de criptomoneda produce cuantiosos beneficios a los mineros. En 2018 ha aumentado de forma desproporcionada el cryptojacking [6], que consiste en secuestrar dispositivos mediante malware para usar una parte de la capacidad de sus procesadores en el minado de criptomonedas. El atacante secuestras múltiples dispositivos y crea su propia botnet para el minado, obteniendo grandes ganancias a costa del uso de recursos ajenos.
- Se intensifican los ataques a infraestructuras críticas mediante ataques a Sistemas de Control Industrial(ICS). Desde el descubrimiento de Stuxnet en 2010, se ha ido desarrollando nuevo malware que infecta ICS dejando infraestructuras críticas como por ejemplo centrales eléctricas sin servicio. Con el aumento de estos ataques en 2018, hay que incrementar las medidas de protección y seguridad en todas las infraestructuras críticas para contrarrestar posibles ciberataques.

De lo expuesto en los puntos anteriores se extrae que este año hay numerosos frentes que abordar. Se tendrán que buscar formas de contratacar los nuevos ransomware que son más ágiles, hábiles y rápidos en propagación, aumentar las medidas de seguridad en las empresas, sobre todo en las infraestructuras críticas, proteger los dispositivos de posibles ataques de cryptojacking y principalmente seguir invirtiendo en mejorar la seguridad de la TIC.
Esta revisión del estudio del arte es un pequeño análisis previo del estado de la ciberseguridad en la actualidad. A lo largo del TFM se profundizará en estos y otros temas, que se consideran relevantes en la seguridad de la Tecnología de la Información y las Comunicaciones.

2. Fundamentos de la Ciberseguridad y Ciberamenazas

2.1 Introducción

En este capítulo vamos a abordar los conceptos de ciberseguridad y ciberamenazas. Empezaremos definiendo la ciberseguridad y las ciberamenazas. Analizaremos la historia de la seguridad en las TIC y sus fundamentos básicos. Una vez analizado el contexto existente en Seguridad de la Tecnología de la información y de la Comunicación, nos centraremos en las ciberamenazas existentes, en las vulnerabilidades que pueden aprovechar estas amenazas para atacar los sistemas de información y en las medidas de seguridad que se pueden llevar a cabo para evitar los ataques.

2.2 Definición de Ciberseguridad y Ciberamenazas

Es imposible separar los conceptos de ciberseguridad y ciberamenaza porque uno surge con el fin de evitar que se produzca el otro. A continuación, daremos dos definiciones de ciberseguridad para que quede más clara la relación existente entre los dos conceptos.
Isaca da la siguiente definición de ciberseguridad [7]: *protección de activos de información mediante el tratamiento de las amenazas existentes para la información que es procesada, almacenada y transportada por sistemas de información que se encuentran conectados con Internet*.
La definición de ITU es la siguiente [8]: *La ciberseguridad es 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 ciberentorno.*

La definición de Isaca nos da una perspectiva más general de la ciberseguridad y la de ITU concreta más, dando unas directrices para proteger los activos de la información. Analizando las dos definiciones se extrae que la ciberseguridad nace para proteger de las ciberamenazas a los activos de las organizaciones y a los usuarios que usan el ciberentorno. Por tanto, el concepto ciberamenaza va ligado estrechamente a la ciberseguridad. A continuación, definiremos que son los activos, las amenazas y las vulnerabilidades:
Según la ISO 55000[9] un activo es un elemento, cosa o entidad que tiene un valor potencial o materializado para la organización. En el caso de los Sistemas de Información serian todos los elementos del sistema o los que están relacionados de forma indirecta o directa con este, que ayudan a cumplir su actividad o función principal y a que su funcionamiento sea el correcto.
La UNE 71504[10] nos da la siguiente definición de amenaza: Causa potencial de un incidente que puede causar daños a un sistema de información o una organización. Las ciberamenazas utilizan las vulnerabilidades existentes en los activos para atacar y producir daños en los activos de información.
Vulnerabilidades: Son las debilidades de los activos de información que pueden ser aprovechadas para que las amenazas se materialicen.

En el siguiente esquema se muestran las relaciones existentes entre ellas:

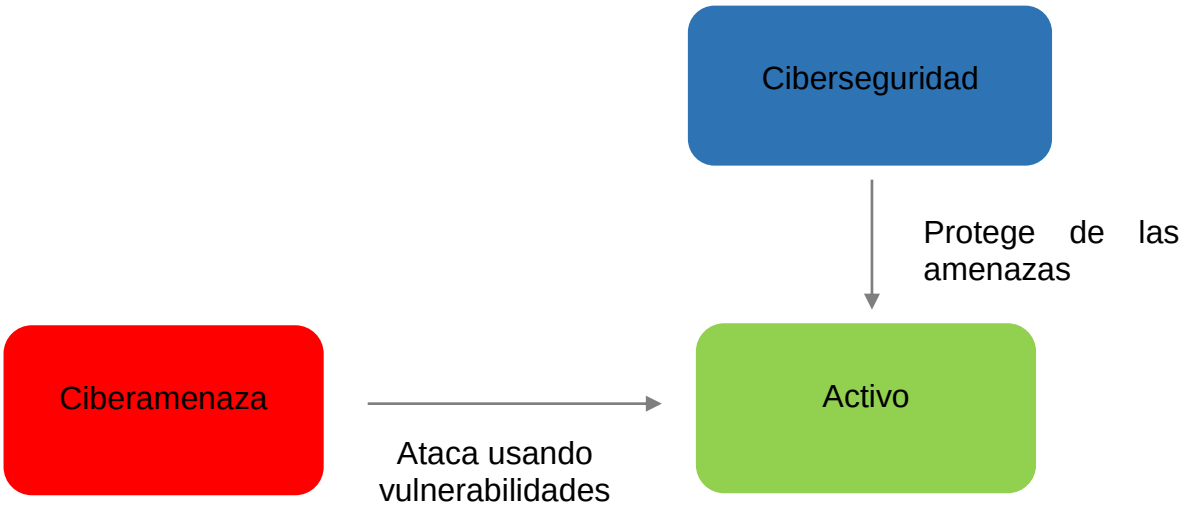


Figura 3: Esquema relacional ciberamenaza-ciberseguridad

En este esquema se explica a grandes rasgos la relación entre ciberseguridad, activo y amenaza. Se debería incluir el concepto riesgo y explicar cómo se analizan los riesgos, pero se ha considerado que esta fuera del alcance de este TFM. A lo largo del capítulo se ampliará información de estos conceptos y se incluirán otros nuevos.

2.2 Historia de la Ciberseguridad.

Para entender la ciberseguridad hay que remontarse a sus inicios y conocer el por qué y cómo ha ido evolucionando a lo largo de los años. La información es un bien valioso y se ha intentado siempre buscar medios para protegerla de las amenazas existente. Podemos remontarnos a la segunda guerra mundial para encontrar la máquina de cifrado alemana Enigma y como ya entonces ese sistema de protección de la información fue atacado y descifrado por los británicos. No se puede hablar en esa época de ciberseguridad o de ciberamenazas, ya que no existían aún los sistemas de información como hoy en día, pero sí que podemos ver como se utilizó una vulnerabilidad para materializar una amenaza y atacar un sistema y también podemos observar que no hubo una protección adecuada de la máquina de cifrado para evitar la materialización del ataque.

En 1972 se produce el primer ataque informático mediante lo que se conoce hoy como virus. Este ataque conocido como Creeper emitía periódicamente un mensaje en la pantalla de un ordenador IBM 360. Para solucionar el problema, se creó el primer antivirus conocido como the Reaper. No será hasta 1984 que los laboratorios Bell Labs y sus investigadores acuñarían esta denominación. Por tanto, podemos decir que con la creación de los virus surge la necesidad de protección y aparecen los antivirus, así que se puede considerar que está sería la primera etapa de la ciberseguridad.

En los 90 se va generalizando el uso de ordenadores y de internet y se hace necesaria la implantación de medidas de seguridad físicas y lógicas por parte de los usuarios y los proveedores. Podríamos considerar que en esta etapa es donde se empiezan a definir las medidas de protección de la red y se crean las bases para unas redes de comunicación seguras y eficientes.

La época de 2000 comienza con la amenaza del efecto 2000 en los sistemas informáticos, se cree que se producirá un apagado masivo de los sistemas de información debido a unos errores de programación existentes en ellos. Finalmente se soluciona con mínimas incidencias. En esta época las amenazas comienzan a aumentar y empiezan a producirse ataques internos y externos en redes corporativas. Con la aparición de las redes sociales y las compras online empiezan a producirse los primeros fraudes y delitos no contemplados en las legislaciones. Se empiezan a implementar medidas para asegurar la información y se busca adecuar las leyes para proteger a los usuarios y la información.

A partir de 2010 y la entrada en el mercado de los smartphones aparece un nuevo campo de acción para los ciberdelincuentes. No existe la suficiente protección en los dispositivos móviles y surgen nuevos ataques más sofisticados. Se aumenta la seguridad de la información fomentando el uso de programas de cifrado de la información y las empresas empiezan a implementar sistemas de gestión de la seguridad de la información. Un nuevo horizonte se va perfilando, donde la privacidad va cobrando cada vez más relevancia. Se busca la protección también de las infraestructuras críticas creando una legislación para su protección. Esta época consolida la ciberseguridad y abre el camino a nuevos desafíos como el Internet of things(IoT), las Vanets y otras nuevas infraestructuras en las que se deben aplicar medidas de protección y seguridad para evitar las nuevas ciberamenazas que van emergiendo.

A continuación, se muestra una imagen de un artículo de Incibe [11] donde se muestra la evolución de la seguridad de las empresas.

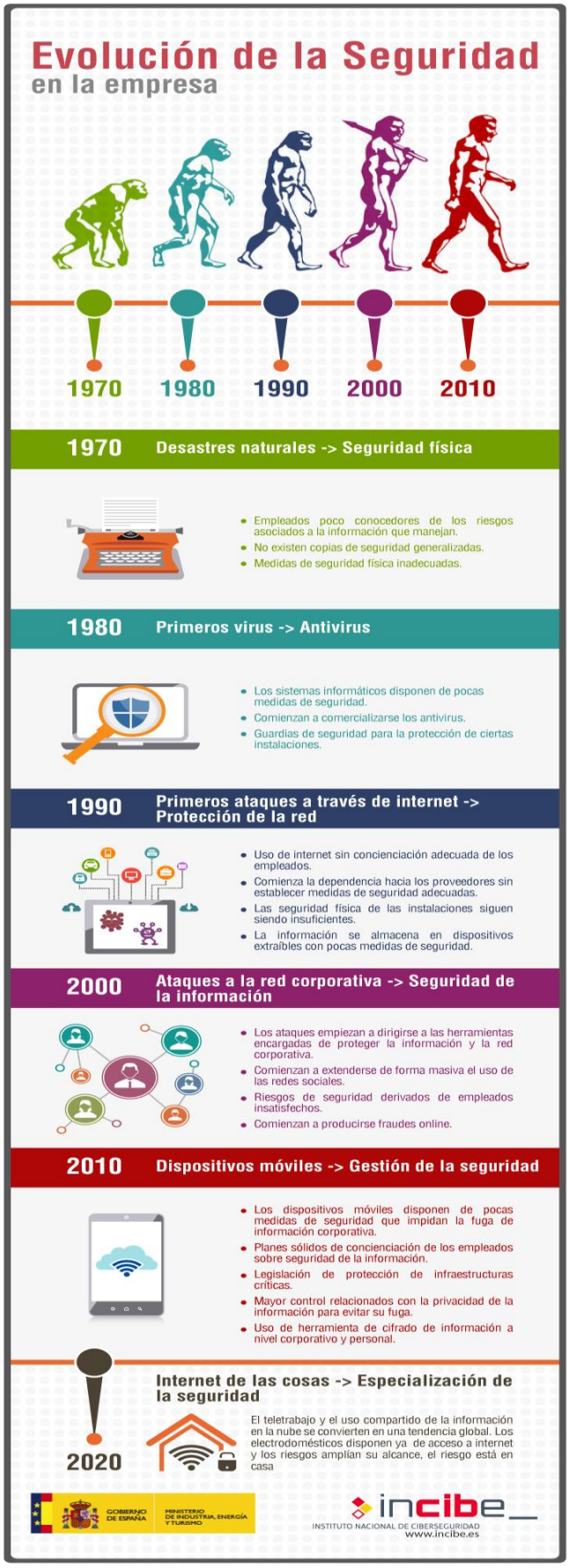


Figura 4: Evolución de la Seguridad en la empresa según Incibe[11]

2.3 Fundamentos de seguridad de la información

La seguridad de la información se fundamenta en tres pilares básicos conocidos como CIA [12] que se definen a continuación:

Confidencialidad: Esta propiedad nos garantiza que sólo podrán acceder a la información las personas que estén autorizadas para hacerlo.

Disponibilidad: La disponibilidad debe asegurarnos que si un usuario está autorizado podrá disponer de la información en cualquier momento que lo desee.

Cabe destacar que no en todas las empresas tienen la misma importancia los tres pilar básicos de la información. Por ejemplo, una empresa que vende tickets electrónicos para espectáculos debe garantizar por encima de todo la disponibilidad y la integridad de los tickets que vende. La confidencialidad tendría menos importancia en este caso, pero no dejaría de ser relevante.

Además de estas tres propiedades, existen dos propiedades complementarias que también son muy importantes para cumplir la seguridad de la información:

Autenticidad y no repudio: Se debe poder confirmar cuál es la identidad de los usuarios o de los procesos que utilizan la información y además no se debe poder negar la autoría de las acciones realizadas.

Trazabilidad: Es la propiedad que garantiza que se podrá reproducir una cronología de las acciones que se han producido en un proceso y quien las ha realizado.

La ciberseguridad por tanto tendrá que estudiar que propiedades de la seguridad de la información se pueden ver afectadas por una amenaza a un activo o a un sistema de la información, y ver de qué forma puede protegerse el activo o el sistema para que nunca lleguen a materializarse la amenazas.

2.4 Ciberamenazas

Las ciberamenazas intentan utilizar las vulnerabilidades existentes en los activos para atacar y producir daños a los sistemas de información. Por tanto, hay que combatir las vulnerabilidades existentes para que las amenazas no se puedan materializar.
A lo largo de la historia de la ciberseguridad han existido muchas amenazas que han ido desapareciendo con el aumento de la protección de los sistemas de seguridad de la información. A continuación, vamos a presentar un listado de las amenazas más relevantes en la actualidad, sus vulnerabilidades, ataques y las medidas de seguridad a aplicar para evitar dichos ataques.

- IoT y Fog computing: Esta amenaza se centra en los dispositivos del Internet of things y la arquitectura fog computing. Con la tendencia al aumento de los dispositivos IoT y la futura aparición de Smart cities la

posibilidad de ataques a los sistemas de IoT se eleva. Existen numerosas vulnerabilidades que pueden aprovechar los atacantes, ya que estos dispositivos no tienen implementadas medidas de seguridad, su firmware está obsoleto y si se accede a un nodo se puede ver comprometida la seguridad de toda la red de nodos. Si la amenaza se materializa se verán afectadas todas las dimensiones de la seguridad de la información.
Las vulnerabilidades que pueden afectar a los sistemas IoT y Fog Computing son [13]:

- Interfaces poco seguras.
- Software/Firmware inseguro.
- Falta de cifrado en el transporte.
- No exigir el uso de contraseñas.

Las medidas de seguridad que se pueden aplicar para minimizar los riesgos son [13]:

- Instalar actualizaciones de firmware y software.
- Establecer contraseñas seguras.
- Utilizar el cifrado para el transporte y las comunicaciones.
- Establecer la autenticación de dos factores.

- Ciberespionaje: Existen varios tipos de ciberespionaje, pero todos tienen en común la obtención de información confidencial o privilegiada y que el ciberespía obtiene cuantiosos beneficios por la realización de su trabajo. Desde hace unos años los ciberdelitos por espionaje aumentan y los sectores más afectados son el de la política, el de la industria y el militar.
  Los ciberespías suelen aprovechar vulnerabilidades de día cero para realizar los ataques o el uso de ataques phishing para obtener las credenciales de usuarios de alto nivel.
  Se pueden implementar las siguientes medidas de seguridad para evitar el ciberespionaje [14]:
  - Usar cuentas de correo electrónicas seguras que garanticen el cifrado de los mensajes.
  - Usar programas de cifrado para garantizar la seguridad de la información sensible.
  - Utilizar teléfonos que permitan las comunicaciones seguras o aplicaciones como redphone que evitan que programas como PRISM accedan a las comunicaciones.

- Robo información corporativa en dispositivos móviles: Esta amenaza se podría incluir como una parte del ciberespionaje, pero se ha considerado que era mejor darle un apartado específico. Hoy en día los dispositivos móviles se utilizan para uso personal y como herramienta de trabajo. La seguridad en este tipo de dispositivos va mejorando poco a poco, pero aún existen múltiples vulnerabilidades que son aprovechadas por los delincuentes para obtener información confidencial de las corporaciones e incluso privada de los usuarios. Algunas de las vulnerabilidades que pueden afectar a los dispositivos móviles son [15]:
  - Vulnerabilidades de las aplicaciones instaladas.
  - Vulnerabilidades de los Sistemas Operativos.
  - Configuración incorrecta de permisos que dan acceso a funciones que no son necesarias para el uso de la aplicación.

- Vulnerabilidades en las conexiones inalámbricas.

Las medidas de seguridad que se deberían aplicar a los dispositivos móviles corporativos son las siguientes [15]:

- No instalar aplicaciones que no sean corporativas.
- Actualizar los Sistemas Operativos.
- Revisar los permisos solicitados por las aplicaciones.
- Evitar las conexiones wifi que no sean las de la corporación.

- Crime-as-a-Service(CaaS): Grupos de cibercriminales crean kits y otros paquetes o servicios de ataque para usuarios inexpertos y los venden por la Deep Web. Estos kits proporcionan unas armas complejas y sofisticadas a criminales sin experiencia y aumentan así el número de ciberdelitos. Algunos de los kits más utilizados del CaaS son: Phishing kits, exploit kits, malware, criminal phone Banks, DDos-for-hire. Para luchar contra el CaaS se deberán aplicar herramientas para gestionar las vulnerabilidades, firewalls, antivirus, actualizaciones de Software…

- Business Email Compromise(BEC) o "fraude del CEO" es una amenaza que aumenta de forma exponencial cada año. Según datos de Trend Micro [16], en 2018 provocará unas pérdidas mundiales que superarán los 9 billones de dólares. A continuación, se muestra un gráfico del artículo de Trend Micro donde se muestran las perdidas acumulativas que provoca la materialización de esta amenaza.

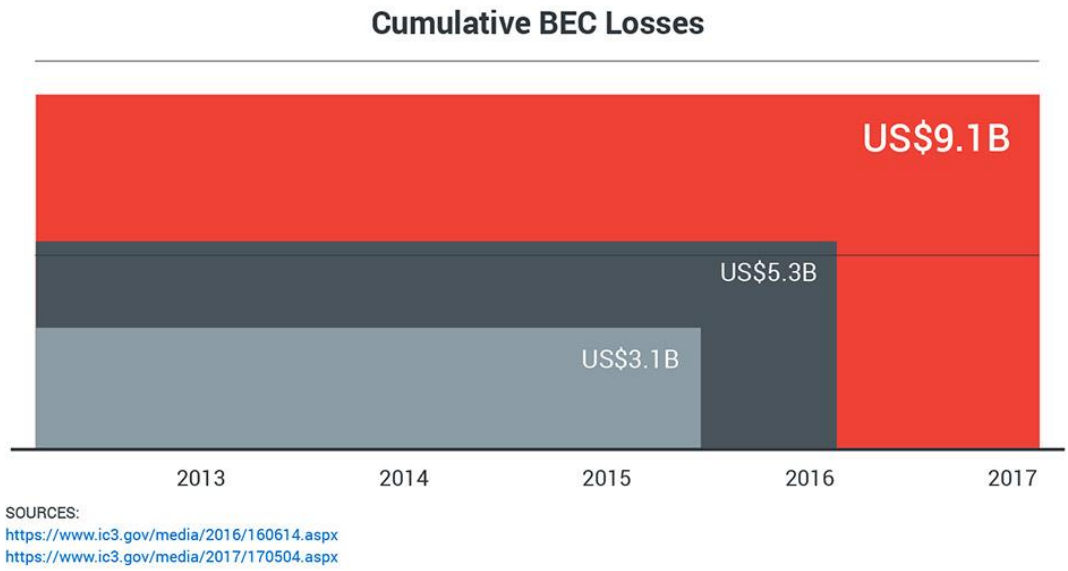


Figura 5: Gráfica de pérdidas BEC según TrendMicro [16]

El propósito del BCE es el robo de importantes sumas de dinero mediante el engaño a los departamentos de finanzas de las empresas. Para materializar esta amenaza se utilizan las técnicas de captura de credenciales y de correo electrónico, para llevarlas a cabo primero se utilizan vulnerabilidades de software o ingeniería social para obtener información de la empresa que después se aprovechará para realizar los ataques. Algunas medidas de seguridad que se pueden implementar son las siguientes [17]:

- Formar a la organización en Ciberseguridad

  - Definir políticas y procedimientos para evitar este ataque y darlos a conocer a todo el personal de la organización.
  - Crear formularios para reportar posibles incidentes al departamento de seguridad.
  - Diseñar o comprar herramientas específicas para evitar este tipo de ataques.

- Ransomware: Esta amenaza es una de las más peligrosas y con más relevancia en los últimos años. Puede afectar a grandes empresas, pymes e incluso a usuarios domésticos. Inicialmente la amenaza solo se podía materializar si existía una interactuación humana, pero se han ido mejorando los sistemas de ataque y en 2017 con la aparición de los cryptoworms ya se puede atacar de forma automática. El funcionamiento de esta amenaza es secuestrar el dispositivo y cifrar el contenido. Una vez secuestrado se pide un rescate para descifrar el contenido del ordenador y devolver el control al usuario. En algunas ocasiones estos ataques simplemente se realizan para dañar un activo tan importante como es la información. El Ransomware puede aprovechar las siguientes vulnerabilidades:
  - Vulnerabilidades de tipo humano al aceptar correos infectados o enlazar a webs maliciosas.
  - Vulnerabilidades de software que no han sido parcheadas o actualizadas.
  - Vulnerabilidades zero day.
  - Vulnerabilidades de hardware por no actualizar el firmware.

  En cuanto a las medidas de seguridad que se podrían aplicar están las siguientes [18]:
  - Utilizar medidas de seguridad avanzada en el correo electrónico.
  - Instalar un bloqueador de webs maliciosas.
  - Formar a los empleados en ciberseguridad.
  - Actualizar software y firmware.

- Cryptojacking: Debido al interés creciente en las criptomonedas y los beneficios que se obtienen al minarlas, los ciberdelincuentes están desarrollando nuevas formas de obtener el control parcial de ordenadores para crear botnets con el fin de obtener beneficios económicos utilizando los recursos de otros. Las técnicas que se utiliza para materializar esta amenaza son las de introducir código oculto en webs mediante herramientas como CoinHive o la instalación de software malicioso. Cuando el usuario visita la web o instala el software se comienzan a usar sus recursos para minar criptomonedas sin su consentimiento. Puede pasar mucho tiempo hasta que se perciba que hay un mal funcionamiento del dispositivo afectado. La vulnerabilidad que se utiliza es aprovechar la carencia de formación en ciberseguridad de los usuarios para que instalen el software malicioso a accedan a la web. Las medidas de seguridad que se pueden aplicar para evitar que se materialice la amenaza son [19]:
  - Utilizar bloqueadores de minería como por ejemplo No coin o MinerBlock.

- Actualizar las extensiones instaladas en los navegadores y eliminar las que no se utilicen.
- Realizar las actualizaciones de software correspondientes.
- No instalar software no confiable.

- Amenazas a Infraestructuras críticas: El ministerio del interior [20] informo que en el primer trimestre de 2018 se produjeron 125 incidentes en infraestructuras críticas. La materialización de estas amenazas puede suponer desde escanear las redes de la ICS hasta el robo de información crítica. Para los ciberdelincuentes es un ámbito de ataque cada vez más atractivo, ya que un ataque que dañe a un ICS como por ejemplo pueda ser el de una instalación eléctrica, provoca daños indirectamente a millones de usuarios y pérdidas millonarias a la empresa que gestiona la infraestructura crítica y a los usuarios que dependen de los servicios de ICS para realizar sus actividades diarias. Las vulnerabilidades típicas que suelen ser aprovechadas por los atacantes son la siguientes [21]:
  - Falta de autenticación o cifrado.
  - Almacenamiento de contraseñas frágil.
  - Software no actualizado.
  - Vulnerabilidades debidas a las redes de conexión.

  Algunas medidas que pueden aplicarse para evitar ataques son las que se muestran a continuación [21]:
  - Suprimir las conexiones a internet o realizarlas por VPN.
  - Suprimir las credenciales por defecto.
  - Habilitar medidas para poder bloquear cuentas.
  - Implementar el uso de contraseñas seguras.
  - Aplicar actualizaciones y parches de seguridad.

- Amenazas Avanzadas Persistentes(APTs): Según Wikipedia[22] la APT es un conjunto de procesos informáticos sigilosos y continuos, a menudo orquestados por humanos, dirigidos a penetrar la seguridad informática de una entidad específica. Una APT, generalmente, fija sus objetivos en organizaciones o naciones por motivos de negocios o políticos. Algunos de los grupos que actualmente operan son Sofacy, Sandworm, Lazarus/BlueNoroff, APT Scarcruff, APT LuckyMouse y OrangeWorn.
  Las APTs utilizan vulnerabilidades de día cero para introducirse en los sistemas o aplican técnicas de ingeniera social. Estos ataques son muy complejos, pero existen unas medidas de protección básicas que se pueden aplicar para evitar los ataques:
  - Gestionar los permisos de autorización para que los usuarios solo puedan acceder a la información necesaria.
  - Instalar firewall para evitar el acceso de atacantes a la red interna.
  - Actualizar firmware y software.
  - Instalar herramientas de seguridad en todos los dispositivos que tengan acceso a la red interna.

- Ciberterrorismo: La Jefatura de información de la Guardia Civil define el ciberterrorismo [89] como el empleo generalizado de las Tecnologías de la Información y la Comunicación(TIC), por parte de grupos terroristas u

organizaciones afines, para la consecución de sus objetivos; utilizando Internet (sistemas informáticos y contenidos) como instrumento de comisión del delito o como acción del delito. De esta definición se extrae que existen dos modalidades de ciberterrorismo, la primera que usa Internet como medio o instrumento para la realización de las actividades terroristas y la segunda, que tiene como acción del delito Internet (infraestructuras críticas, objetivos estratégicos). Algunas de las medidas propuestas por países europeos en la lucha contra el ciberterrorismo son [90]:

- Desarrollar procedimientos automatizados basados en la inteligencia artificial para poder descubrir que factores influyen en la radicalización y así poder evitar que se produzca o minimizar su alcance.
- Llevar a cabo análisis predictivos para aumentar la seguridad internacional.
- Utilizar el confinamiento algorítmico (contenido basado en preferencias) de las redes sociales y gestionarlo de forma que se elimine lo más rápidamente posible el contenido que publicite información terrorista.

2.5 Conclusiones

Después de evaluar toda la documentación recopilada se extraen las siguientes conclusiones de este capítulo:

- Existe una relación directa entre los conceptos de ciberamenaza y ciberseguridad y el concepto que las une son los activos de seguridad de la información.
- La creación de la ciberseguridad es muy reciente y aun se tiene que mejorar para minimizar el riesgo de materialización de las ciberamenazas existentes.
- La ciberseguridad se fundamenta en la Confidencialidad, Integridad y Disponibilidad. Estos pilares se complementan con dos propiedades más que son trazabilidad, no repudio y autenticidad.
- Existen multitud de amenazas que acechan a los sistemas de información en la actualidad. Se tiene que comprobar frecuentemente que los activos no tengan vulnerabilidades y si las tienen solucionarlas rápidamente.
- Es conveniente formar a los usuarios en materia de ciberseguridad para evitar que se produzcan ataques debidos a factores humanos.
- Se deberán aplicar todas las recomendaciones y medidas de seguridad con el fin de evitar posibles ataques a los sistemas de información.

3. Leyes y Normas internacionales

3.1 Introducción

En este capítulo vamos a hablar de las norma y leyes que existen en el ámbito de la seguridad en tecnología de la información y la comunicación. Comenzaremos analizando las directrices y normas existentes en EE. UU, después analizaremos las de China y Rusia, países conocidos por vulnerar los derechos de los usuarios. Una vez analizada la normativa anterior, nos centraremos en las leyes que rigen la Unión Europea para finalmente centrarnos en las leyes existentes en España.

3.2 Legislación sobre Ciberseguridad en EE. UU.

EE. UU implemento el Plan de Acción Nacional de Ciberseguridad (CNAP) en 2016 para aumentar la ciberseguridad del país y evitar ataques masivos. Este plan tiene tres objetivos estratégicos [23]:

- Aumentar el nivel de ciberseguridad en los sectores públicos, privados y consumidores.
- Establecer medidas preventivas en la lucha contra la actividad maliciosa en el ciberespacio que pueda afectar al país o a sus aliados.
- Crear un sistema de respuesta a incidentes efectivo y eficaz.

En el marco del CNAP la administración americana crea una Directiva de Política Nacional para la coordinación de incidentes cibernéticos y una metodología que valora la severidad de esos incidentes. La directiva se rige por los siguientes principios para establecer la respuesta a incidentes [24]:

- Responsabilidad Compartida: Las agencias gubernamentales, los consumidores y el sector privado tienen intereses comunes y tienen que compartir responsabilidades para manejar los incidentes de forma correcta y afrontar sus consecuencias.
- Respuesta basada en el riesgo: Se determinarán las acciones a llevar a cabo para responder a los incidentes y los recursos que se utilizaran en función de un análisis de riesgo que se realizará específicamente para cada caso.
- Respetar a las entidades afectadas: Se intentará proteger en la medida de los posible a las entidades afectadas para no exponerlas, pero en el caso que la gravedad del incidente lo requiera se emitirá una declaración pública sobre el incidente.
- Unidad de Esfuerzo Gubernamental: Se coordinarán los esfuerzos entre agencias federales y autoridades para responder de forma rápida y eficaz a los incidentes. En el caso que el incidente lo requiera se unirán a socios internacionales dando prioridad ante todo a la respuesta al incidente.
- Habilitar la Recuperación y la Restauración: Se priorizará el dar una respuesta al incidente que facilite la recuperación y restauración de las entidades que hayan sido víctimas de este.

En cuanto al tratamiento y la compartición de información surge la Ley de compartición de la Seguridad de la información(CISA). Esta ley que ha sido muy controvertida por su contenido tiene como finalidad crear un sistema de informantes corporativos que cedan datos personales de sus clientes al Departamento de Seguridad Nacional, que a su vez podrá ceder esta información a diferentes entidades gubernamentales como la Oficina del Director de Inteligencia Nacional, Defensa, el Tesoro… [25].

En 2017 EE. UU da un paso más en la gestión de la información confidencial y crea una nueva ley que consiente la venta de datos de usuarios a los proveedores de Internet. Estos podrán comerciar con historiales de búsqueda, localización, tiempo de navegación, aplicaciones descargadas y tipo de dispositivo utilizado y no será necesario que se obtenga el consentimiento de los usuarios para realizar la venta de sus datos, pero no se podrán vender en el caso de que un usuario lo solicite [26].

En febrero de 2018 se extiende el Acta de Vigilancia de Inteligencia Extranjera (FISA). FISA es un conglomerado de leyes que da poder a las agencias de seguridad estadounidense para recopilar y usar información procedente de otros países en el caso de sospecha de posible espionaje y terrorismo. En 2018 se ha ampliado la sección 702 y con ello se pretende facilitar que la NSA pueda obtener información de las comunicaciones de los usuarios a través de proveedores y grandes operadoras como Facebook. No será necesario que la información sea un objetivo sospechoso, se podrá recopilar información en masa que luego podrá ser cedida a agencias federales sin necesidad de orden judicial [27].

3.3 Legislación sobre Ciberseguridad en Rusia

En el caso de Rusia hay que destacar la ley que entró en vigor en octubre de 2017 y que tiene como fin acabar con las conexiones seguras y anónimas de los usuarios y empresas. El objetivo de la ley es prohibir los programas que se utilizan para acceder por VPN o de forma anónima a internet y da permiso a la agencia rusa de vigilancia de telecomunicaciones (Roskomnadzor) para hacer un listado de los servicios y programas que tienen esa finalidad y bloquearlos [28].

En 2013 el Consejo de Seguridad en colaboración con el Ministerio de Asuntos Exteriores, Defensa, Comunicaciones y justicia elaboran un documento llamado "*Principios de la política gubernamental de la Federación Rusa en el ámbito de la seguridad informática internacional hasta el 2020*". El documento cataloga las 4 principales ciberamenazas a las que se puede ver expuesta Rusia y que son las siguientes según un artículo del CSIRT-CV [29]:

- Utilizar las tecnologías de la información como arma para realizar actos hostiles y actos de agresión.
- Utilizar las tecnologías de la información con fines terroristas.
- Ataque cibernético, el cual incluye el acceso ilegal a información, la creación y distribución de programas nocivos.

- Utilizar la tecnología de internet para inmiscuirse en asuntos internos de los estados, la violación del orden establecido, la incitación a la hostilidad y la propaganda de ideas que inciten a la violencia.

En el documento también se considera que se hará frente a las amenazas con la cooperación de la OTSC (Organización del Tratado de Seguridad Colectiva), los BRICS (Asociación Económica que engloba a Brasil, Rusia, India, China y Sudáfrica) y la organización de Cooperación de Shanghái.

Cabe destacar que, en octubre de 2018 Rusia presenta un proyecto de protección cibernética [30] ante la ONU (Organización de Naciones Unidas) para desarrollar un sistema de ciberseguridad mundial. La intención de este proyecto es crear un grupo de seguridad internacional para verificar que se cumplen las normas relativas al buen uso de Internet, proteger la privacidad de los usuarios y proteger los datos confidenciales. Este proyecto deberá ser evaluado y votado por todos los miembros de la ONU.

3.4 Legislación sobre Ciberseguridad en China

En junio de 2017 entra en vigor la ley de Ciberseguridad de la República Popular China. Esta ley está formada por 79 artículos y no sigue la formulación habitual de las leyes de seguridad de otros países. A continuación, se muestran los capítulos que conforman la ley [31]:

- Capítulo 1: Provisiones Generales
- Capítulo 2: Soporte y Promoción de Seguridad en la red
- Capítulo 3: Seguridad de las operaciones en red
  Sección 1: Provisiones Generales
  Sección 2: Seguridad de operaciones para infraestructuras de información crítica
- Capítulo 4: Seguridad de la información en red
- Capítulo 5: Monitorización, alerta temprana y respuestas a incidentes
- Capítulo 6: Responsabilidad legal
- Capítulo 7: Provisiones suplementarias

Los expertos coinciden en que es una ley muy general y que crea muchas dudas a la hora de aplicarla. En la misma ley se identifican los delitos y las sanciones que se impondrán por su comisión.
El artículo 21 impone un sistema de monitorización para que los registros de actividad de red se guarden por un periodo de 6 meses por parte de los operadores. En cuanto a los datos de carácter personal se indica que deberán ser almacenados en China y también obliga a las operadoras de infraestructura de información crítica a localizar la información personal de los ciudadanos que son extranjeros y que viven en China [32].

3.5 Legislación sobre Ciberseguridad en la Comunidad Europea

Uno de los pilares fundamentales en materia de Ciberseguridad en la Unión Europea es la Directiva sobre la Seguridad de las redes y sistemas de Información (Directiva NIS) [33] que entró en vigor en 2016 y en la que sus requisitos y normas son jurídicamente vinculantes. Los Estados miembros

disponían de 21 meses para transponer la Directiva a las legislaciones nacionales y 6 meses más para identificar a los operadores. La finalidad de esta directiva es exigir a los operadores de servicios esenciales y a los proveedores de servicios digitales que gestionen los riesgos que provocan las amenazas en los sistemas de información que se usan para los servicios que prestan. También obligan a comunicar los incidentes más graves a las autoridades nacionales y a implantar las medidas necesarias para prevenir y reducir los riesgos de los incidentes.

Propuesta de ley del Reglamento de ciberseguridad de 2018. Se pretende crear un Reglamento de Ciberseguridad para hacer frente a las amenazas a las que se enfrenta la Unión Europea. Los puntos más destacables de esta propuesta son [34]:

- Dar a ENISA (Agencia de Seguridad de las Redes y de la Información de la Unión Europea) la función de agencia de ciberseguridad de la UE y relanzarla para que tenga un posicionamiento destacado en cuestiones de Ciberseguridad.
- Crear una certificación común a la UE en materia de Ciberseguridad de procesos, productos y servicios TIC específicos. Así se logrará tener unos servicios más confiables y unificados. En principio la certificación no será de carácter obligatorio. Se proponen tres niveles: básico, sustancial y elevado.
- Realizar una aplicación rápida de la Directiva NIS.

Reglamento General de Protección de Datos: El RGPD ofrece una serie de directrices y reglas para que las empresas puedan dar tratamiento a los datos personales de los usuarios, garantizando su privacidad y su protección. Impone sanciones económicas al incumplimiento de las directrices que se tienen que aplicar. Los puntos más destacables del RGPD son los siguientes [35]:

- Proporcionar un tratamiento legal, leal y transparente de los datos.
- Imponer limitaciones a la finalidad con que se tratan los datos, al almacenamiento que se hace de ellos y al tipo de datos que se recopila.
- Los interesados tendrán derecho a la corrección, oposición, eliminación y transferencia de los datos personales.
- Se deberá solicitar al usuario una autorización clara y explicita para el tratamiento de sus datos personales.
- Se realizará una Evaluación de Impacto de Protección de datos si se introduce un cambio en el tratamiento de los datos personales.
- Se deberá asignar un Delegado de Protección de Datos si se realiza un tratamiento significativo de los datos personales.
- Se formará y concienciará a los trabajadores en los requisitos más importantes del RGPD.

La Directiva 2013/40/UE sirve para equiparar las penas de los distintos códigos penales de los países miembros de la Unión Europea en materia de ciberseguridad y fomentar la cooperación entre países al poseer unos criterios unificados. Según un artículo que analiza la directiva [36] los puntos más importantes son:

- Ataques a infraestructuras críticas.
- Ataques a gran escala o masivos contra cualquier sistema u objetivo.
- Intromisión ilegal en los sistemas.
- Intercepción de la información.
- Robo, bloqueo o usurpación de identidad.
- La creación y comercialización de los programas o medios usados en la comisión de un delito.
- Se le otorga responsabilidad a las personas jurídicas cuando se lucren o propicien accesos ilegales a terceros.

3.6 Legislación sobre Ciberseguridad en España

En España se ha creado el Código de Derecho de la Ciberseguridad [37]. En este código se agrupan las normas y leyes principales para hacer frente a las amenazas que se ciernen sobre el ciberespacio. A continuación, se muestran las que se consideran más relevantes en materia de ciberseguridad:

Ley 34/2002 de servicios a la sociedad de la información y comercio electrónico(LSSI) [38]. Esta Ley nos ofrece un marco jurídico de aplicación a los servicios de las sociedades de información y al comercio electrónico. Legisla entre otros los siguientes aspectos:

- Comunicaciones comerciales por vía electrónica.
- Contratos electrónicos: que información es necesaria, validez de estos…
- Régimen sancionador de aplicación a los prestadores de los servicios de seguridad de la sociedad de la información y también sus obligaciones.

Ley 50/2003 de firma electrónica [39]: Según su artículo 1 en esta ley regula la firma electrónica, su eficacia jurídica y la prestación de servicios de certificación. Por tanto, esta ley es vital para garantizar la seguridad de la firma electrónica que es un aspecto clave en la gestión de documentos electrónicos.

Real Decreto 381/2015[40] por el que se establecen medidas contra el tráfico no permitido o irregular con fines fraudulentos en comunicaciones electrónicas. Este Real Decreto nace con los objetivos de proteger la integridad y la seguridad de las redes y servicios de comunicaciones electrónicas, asegurar los derechos de los usuarios y garantizar que se cumple con unos mínimos de calidad cuando se realiza la prestación de los servicios de comunicaciones electrónicas.

Ley 25/2007[41], de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones(LCD): En esta ley se establece la obligación para los prestadores de servicios de comunicaciones electrónicas de guardar datos generados por los usuarios en sus comunicaciones por un periodo de al menos 12 meses, para que puedan estar disponibles para investigaciones de delitos graves, siempre supeditado a una autorización judicial. Esta ley está en entredicho debido a las sentencias que dicto el Tribunal de Justicia de la Unión Europea(TJUE) y que declaran nula la Directiva 2006/24/CE en la que la LCD basa una parte de su contenido.

Hay que destacar también la transposición o aplicación directa de las siguientes directivas y reglamentos europeos que se han comentado en el punto 3.5:

- Directiva UE 2016/1148 (Directiva NIS) se transpone en septiembre de 2018 mediante el Real Decreto-Ley 12/2018.
- Reglamento General de Protección de Datos(RGPD) de aplicación directa, sin necesidad de transposición.
- Directiva 2013/40 UE que se transpone en la modificación del Código Penal de 2015 con la inclusión de nuevos artículos para el tratamiento de delitos informáticos.

Existen otras leyes que no son específicas de la ciberseguridad pero que también regulan algunos de sus aspectos. Algunas de estas leyes son la ley de propiedad intelectual y el derecho marcario.

3.7 Conclusiones

Del análisis de la normativa sobre Ciberseguridad Internacional se extraen las siguientes conclusiones:

- China y Rusia no respetan los derechos de los usuarios y proveedores y centran sus leyes en la protección gubernamental.
- EE. UU también centras sus esfuerzos en la protección gubernamental y aunque no limita los derechos de navegación de los usuarios, no respeta la privacidad de los usuarios en aras de la protección del país.
- La Comunidad Europea proporciona unas directivas y criterios a los estados miembros para facilitar la unificación de la legislación sobre ciberseguridad en la Unión Europea.
- En Europa se da más relevancia a la protección de la privacidad y el respeto de los derechos de los usuarios que en el resto de las normativas de los países que se han estudiado.
- En España se transponen o se aplican directamente las directivas de la Comunidad Europea relativas a Seguridad en las tecnologías de la Comunicación y la Información.
- Existen leyes y reales decretos de aplicación nacional para garantizar la seguridad legal de la tecnología de la información y la comunicación.

4. Organismos Internacionales en Ciberseguridad

4.1 Introducción

Ante el creciente aumento de los ciberataques a nivel internacional, la ciberseguridad toma cada día más importancia. Debido a esta nueva dimensión que ha adquirido la seguridad de las TIC es necesario establecer organismos y entidades que se dediquen exclusivamente a gestionar la seguridad en este ámbito.

A lo largo del capítulo, mostraremos asociaciones internacionales, continentales y nacionales que se dedican entre otros temas a gestionar la respuesta a incidentes, ciberdefensa, ciberdelitos, seguridad nacional, etc. Dado el gran número de organizaciones dedicadas a la ciberseguridad se han seleccionado las que se consideran más relevantes o las que son más controvertidas en este campo.

4.2 Foro de Respuesta de Incidentes y de Equipos de Seguridad(FIRST)

El **FIRST** se crea en 1990 para poder coordinar y mejorar la comunicación a nivel global entre Equipos de Respuesta de Incidentes. Está formada por 449 equipos de 90 países distintos. Los puntos clave de su misión son los siguientes [42]:

- Desarrollar y compartir información técnica, herramientas, metodologías y mejores prácticas.
- Promover el desarrollo de procesos, mejores prácticas y productos de seguridad con un alto nivel de calidad.
- Desarrollar y promulgar mejores prácticas de seguridad informática.
- Promover la creación y expansión de Equipos de Respuesta de Incidentes en el mundo.
- Instar a los miembros de la asociación a utilizar sus conocimientos, habilidades y experiencias de forma combinada para promover un medio electrónico seguro a nivel internacional.

Se estructura como se muestra a continuación [43]:

- Junta Directiva: Son los responsables de la política general operativa, de los procedimientos y de establecer comités permanentes y temporales para mejorar los objetivos del FIRST.
- Secretaria: Se encarga de todas las gestiones administrativas de la organización.
- Comités: Los gestiona y organiza la Junta Directiva. Hay dos tipos de comités, los permanentes y los temporales. Sus miembros son designados por la Junta Directiva.
- El Encuentro General Anual del FIRST: Es un encuentro anual en el que se debaten y se discuten los objetivos y metas a conseguir. En cada encuentro también se eligen 5 miembros de la junta directiva.

4.3 Organismos OTAN en Ciberseguridad

La Organización del Tratado del Atlántico Norte(OTAN) [44] es una alianza militar gubernamental basada en el tratado de Washington de 1949. Está formada por 29 países de Europa y Norteamérica, cuyo propósito es organizar una defensa colectiva ante cualquier ataque que reciba uno de sus miembros. En cuestión de ciberseguridad cuentan con un organismo propio denominado NCI Agency.

La **NCI Agency** (Agencia Nacional de Comunicaciones e Informaciones de la OTAN), se crea como parte de la reforma de la OTAN que se llevó a cabo en 2012 con la misión de gestionar sistemas de comunicación de la OTAN y luchar contra ciberamenazas y ciberataques coordinándose con gobiernos e industria. Algunos de los servicios y organizaciones más relevantes que la NCI ofrece en ciberseguridad según su web [45] son:

- **Escudo Cibernético de la OTAN**
- **Capacidad de respuesta a incidentes informáticos de la OTAN**(**NCIRC**) [46]: Tienen un equipo de 200 personas que gestiona la protección de las redes de la OTAN durante 24 horas al día, 7 días a la semana. Gestiona los incidentes y facilita información sobre ciberamenazas a sus miembros.
- **Asociación Cibernética de la Industria de la OTAN(NCIP)**: Sirve como nexo entre el sector privado y la OTAN para aunar esfuerzos en la lucha contra las ciberamenazas y en la prevención, respuesta y recuperación de ciberataques. Está formada por entidades de la OTAN, CERTs nacionales y representantes de la industria de los países miembros de la OTAN. Algunos de sus objetivos son [47]
  - Mejorar la ciberdefensa en la cadena de soporte de la OTAN.
  - Contribuir a la educación, entrenamiento y ejercicios de defensa cibernética de la OTAN.
  - Facilitar a la OTAN y sus aliados el aprendizaje de la industria.
  - Construir una relación de confianza entre la OTAN y el sector privado.
  - Obtener asistencia rápida, eficiente y adecuada si sucede algún ciberincidente.
  - Preparar una red de empresas de confianza para que puedan tener acceso los aliados.
  - Facilitar el intercambio de información sobre amenazas, vulnerabilidades y experiencias en ataques cibernéticos.
  - Intercambiar experiencias en prevención y recuperación y guías de mejores prácticas.
- **Equipo de Reacción Rápida** [48]: Nace en 2011 al revisar la política en ciberdefensa. Sus funciones son proporcionar asistencia a sus miembros y socios centrándose sobre todo en los países que aún no disponen de las habilidades y recursos necesarios en ciberdefensa. Sus principios se fundamentan en las bases de defensa colectiva y asistencia mutua.

4.4 Anti-Phishing Working Group (APWG)

APGW es una coalición internacional que integra una respuesta global al cibercrimen entre industria, gobierno, fuerzas de la ley y organizaciones no gubernamentales. Está formada por más de 1800 instituciones, entre las que se encuentran Europol EC3, Comisión Europea, ICANN, etc. La APWG se instituye en EE. UU y en 2013 se establece una división europea con sede en Barcelona.
La APWG tiene tres ejes fundamentales [49]:

- Centros de información APWG: Envían más de mil millones de registros sobre ciberdelitos mensualmente a sus miembros para informar sobre aplicaciones de ciberseguridad, técnicas forenses y programas de investigación. Mediante el intercambio de datos e información entre sus miembros y los centros de información internacionales se desarrollan recursos para unificar una respuesta global a los ciberdelitos.
- Simposio Anual sobre Investigación electrónica de delitos: Sus trabajos son publicados por IEEE y recopila artículos sobre ciberdelitos de investigadores destacados.
- APWG y NCSA's STOP. THINK. CONNECT. Es una campaña de concienciación sobre ciberseguridad que se lleva a cabo en 23 países.

La APWG proporciona los siguientes beneficios para sus miembros:

- Centros de intercambio de información sobre utilidades de respuesta al cibercrimen para profesionales del sector público, privado y organizaciones no gubernamentales que combatan el cibercrimen.
- Conferencias para profesionales de la gestión del cibercrimen, gobierno, fuerzas de la ley e investigadores pioneros a nivel internacional.
- Servicios públicos de educación para prevenir ciberdelitos y desarrollar programas y políticas en la lucha contra los delitos informáticos.

4.5 Corporación de Internet para la Asignación de Nombres y Números(ICANN)

ICANN [50] es una organización sin ánimo de lucro que nace en 1998 para asumir las funciones de IANA (Internet Assigned Number Authority). Su sede se establece en California. Se responsabilizan de asignar las direcciones del protocolo IP, sus identificadores, las funciones de gestión del sistema de dominio y la administración del sistema de servidores raíz.
Se estructura de la siguiente forma:

- Presidente: Nombrado por la junta de directores.
- Junta de directores: formada por 6 representantes de las organizaciones de apoyo y 8 representantes independientes de interés público seleccionados por un comité de nominaciones que representa a todas las circunscripciones de ICANN.
- Organizaciones de apoyo:
  GNSO (Generic Names Support Organization): Redacta políticas sobre dominios genéricos de nivel superior.
  CCNSO (Country Codes Names Support Organization) elabora políticas en relación con códigos de países de dominios de nivel superior.
  ASO (Address Supporting Organization): Es la organización responsable de elaborar las políticas de las direcciones IP.

- Comités consultivos: Se utilizan con el fin de obtener asesoramiento sobre los intereses de los miembros que no se encuentran en las organizaciones de apoyo. Como ejemplo de comités tenemos el GAC (Comité Asesor Gubernamental) que está formado por representantes de los gobiernos nacionales de múltiples países.

4.6 Organismos de América en Ciberseguridad

El **CSIRTamericas** aglutina los CSIRT (Computer security incident response teams) de América. Incluye los CSIRT nacionales, policiales, de defensa y gubernamentales. Los objetivos que se definen en su web son los siguientes [51]:

- Colaboración: Promover la colaboración e integración de los CSIRT americanos.
- Compartir: Facilitar que se pueda compartir información sobre incidentes, amenazas y herramientas de respuesta de incidentes entre los CSIRT.
- Promover: Dar soporte a la creación de CSIRT y asesorar a los que se acaban de crear.
- Proyectos Técnicos: Preparar proyectos para ayudar a mejorar los servicios existentes en los CSIRT.

4.7 Organismos de EE. UU en Ciberseguridad

EE. UU es uno de los países que centra más esfuerzos en gestionar la ciberseguridad. Existen diversos organismos de ciberseguridad en el país, pero los más relevantes en esta materia son los que se muestran a continuación:

NSA (National Security Agency): Agencia de inteligencia del gobierno de los EE. UU que se encarga de todo lo relativo a la seguridad de la información. Forma parte del departamento de defensa y fue creada en 1952, aunque se ocultó su existencia hasta 1970. Es una agencia muy controvertida ya que realiza tareas de espionaje y vigilancia masiva de las comunicaciones. LA NSA se centra en los dos objetivos siguientes que se reflejan en su misión:

- Facilitar las operaciones para supervisar y proteger las redes informáticas(CNO) propias de cualquier ciberataque y proteger la información privada del gobierno.
- Recopilar información de interés de las comunicaciones extranjeras(SIGINT) para proteger la seguridad del país y sus aliados.

En materia de Ciberseguridad llevan a cabo las siguientes tareas [52]:

- Defender la seguridad de la TIC durante 24 horas, 7 días a la semana para así prevenir las ciberamenazas mediante medidas de seguridad adecuadas. Además, proporciona información sobre ciberamenazas a los socios y aliados de EE. UU.
- Identificar vulnerabilidades, desarrollar soluciones y crear estándares para los Sistemas de Seguridad Nacional.
- Mediante el programa de transferencia tecnológica compartir información y tecnología.

- A través de la Iniciativa de Ciencia de Seguridad y Privacidad se deberá promover la ciberseguridad.
- Desarrollar y formar nuevos profesionales mediante la NSA CyberEjercicio (NCX) y los Centros de Excelencia Académica en Ciberseguridad.
- Ofrecer a los profesionales de la ciberseguridad consejos y mejores prácticas.

USCC (United States Cyber Command): Creado en junio 2009 bajo el control del Departamento de Defensa de los EE. UU. El USCC tiene como objetivo proteger los intereses de EE. UU y sus aliados mediante la utilización de técnicas informáticas. Dentro del documento "Achieve and Mantain Cyberspace Superiority: Command Vision for US Cyber Command" [53] se encuentran los siguientes imperativos u ordenes que están relacionados con la ciberseguridad y que se utilizan para conseguir los objetivos principales de la USCC:

- Alcanzar y superar las capacidades del adversario: Anticiparse a los avances tecnológicos y explotar tecnologías emergentes mejor y más deprisa que los adversarios. Transferir rápidamente las tecnologías con utilidad militar para poder escalar habilidades operacionales. Capacitar a los trabajadores para obtener ventajas en el ciberespacio y asegurar que las fuerzas están debidamente preparadas.
- Preparar mejoras en el ciberespacio para optimizar las operaciones en todos los dominios. Facilitar la integración de las habilidades y capacidades del ciberespacio en los planes y operaciones de todas las divisiones.
- Crear ventajas informativas para apoyar los resultados operativos y lograr impacto estratégico: Integrar y unificar las operaciones del ciberespacio con las de información.
- Hacer operativo el espacio de batalla para unas maniobras agiles: Suministrar rapidez y agilidad para las operaciones del ciberespacio en procesos de toma de decisiones, inversiones, conceptos de operaciones y políticas. Asegurar que todos los procesos se alinean con el medio operacional del ciberespacio.
- Ampliar, profundizar y hacer operativas las asociaciones: Aprovechar el talento, la experiencia y los recursos de otras agencias, aliados, servicios, etc. Identificar y comprender los avances que se producen en el ciberespacio, estudiar cuál es su origen y donde se encuentran. Incrementar el alcance y la velocidad para compartir la información de las amenazas con el sector privado, gestionando planes de operación, ejercicios conjuntos y desarrollando habilidades. Habilitar y reforzar a los socios y aliados.

CERT Coordination Center [54]: Se crea en 1988 como una división del SEI (Software Engineering Institute) y tiene relación directa con la Carnegie Mellon University. Está formado por un grupo de ingenieros de software, investigadores, analistas y especialistas en TI y su finalidad es investigar las vulnerabilidades de seguridad en software, contribuir a las mejoras de las redes y desarrollar mejores prácticas y capacitaciones en Ciberseguridad. Las áreas en las que trabaja este CERT son las siguientes:

- Cyber Center Development: Facilitar a CSIRTs y otras organizaciones operacionales de seguridad mejores prácticas y desarrollos medibles.
- Autonomía Segura y resiliencia: Crear mejores prácticas para el desarrollo y empleo de sistemas de machine learning.
- Ciberinteligencia: Identificar los métodos que utilizan los atacantes a través del estudio de su comportamiento y capacidades.
- Cyber Workforce Development: Ayudar a la cyber workforce a mantener la ciberseguridad en las organizaciones, desarrollando y manteniendo productos a su medida.
- Forense Digital: Contribuir a mejorar las prácticas de análisis y la respuesta a incidentes que utilizan las organizaciones paralelamente al desarrollo tecnológico y al aumento de las habilidades de los ciberdelincuentes.
- Gestión del Riesgo en empresas: Ayudar a las organizaciones a gestionar y mitigar riesgos mediante la creación de marcos de trabajo y controles adecuados.
- Amenazas internas: Colaborar con las empresas para ayudar a detectar y reducir el impacto de las amenazas internas.
- Conocer el estado de las redes: Estudiar el ciberespacio y los sistemas informáticos mientras evoluciona para poder caracterizar los activos en riesgo, medir la actividad de los ciberdelincuentes y establecer prioridades para resolver las ciberamenazas.
- Security-aware adquisition: Gestionar las vulnerabilidades y planificar la forma de abordar las amenazas de manera más eficaz durante el ciclo de vida de la adquisición.
- Desarrollo Seguro: Analizar el código fuente para asegurarse de que cumple con las mejores prácticas de seguridad y así poder obtener plataformas seguras.
- Evaluación de Sistemas y Plataformas: Buscar vulnerabilidades mediante la evaluación de software, dispositivos y plataformas para así poder crear estrategias para combatir futuros ataques.
- Threat-Aware Sustainment: Disminuir en los sistemas la exposición a vulnerabilidades.

4.8 Organismos de Rusia en Ciberseguridad

El principal organismo en Rusia es el **Servicio Federal de Supervisión de las Telecomunicaciones, Tecnologías de la Información y Medios de Comunicación(Roskomnadzor)** [55]. Este organismo realiza la vigilancia de los medios de comunicación (electrónicos y comunicaciones masivas), tecnologías de la información y telecomunicaciones. Además, también supervisa el cumplimiento de ley de confidencialidad de datos personales y gestiona el servicio de frecuencia de radio.

El Roskomnadzor es internacionalmente conocido por realizar en Rusia un bloqueo selectivo de webs desde 2013, que según ellos, se realiza para proteger a los usuarios del ciberespacio ruso. Estas medidas han sido muy criticadas por la comunidad internacional ya que privando a los ciudadanos de navegar por internet libremente.

4.9 Organismos de Asia en Ciberseguridad

En Asia existe el **APCERT** que es una coalición de CERTs (Computer Emergency Response Team) y CSIRTs (Computer Security Response Teams) de la región Asia-Pacífico. Está organización se estructura de la siguiente forma [56]:

- Presidente: La presidencia es adoptada por un equipo de algún país miembro. En la actualidad tiene el cargo la ACSC (Australian Cibersecurity Centre).
- Vicepresidente: El cargo lo ostenta la Malaysan Computer Emergency Response Team(MyCERT).
- Comité Directivo: Está formado por el presidente, vicepresidente, secretario y 4 miembros más. Son los encargados de las políticas operativas generales, procedimientos, guías y cualquier gestión relativa al APCERT.
- Secretario: Mantiene la web de APCERT y realiza tareas administrativas entre las que están gestionar la "APCERT anual" y orientar a los equipos que soliciten acceso a la organización.
- Equipos miembros: Existen dos categorías. La primera, es la de miembros operacionales que está formada por 30 miembros de 21 países y que deben cumplir la condición de ser CSIRT/CERT a tiempo completo. La segunda categoría son los miembros de soporte que en la actualidad cuenta con 3 equipos y su función es contribuir y respaldar las operaciones APCERT y las funciones CSIRT/CERT.
- Grupos de trabajo: Existen 9 grupos de trabajo que abordan diferentes temáticas como la mitigación de malware, seguridad en dispositivos IoT, pagos seguros digitales, etc.

Los objetivos que tiene el APCERT y que se muestran en su misión son los siguientes [57]:

- Mejorar la cooperación regional e internacional en materia de ciberseguridad de la Región Asia-Pacífico.
- Crear conjuntamente medidas para gestionar los incidentes de seguridad de redes regionales o a gran escala.
- Facilitar el intercambio entre sus miembros de información y tecnología que incluya la seguridad de la información, códigos maliciosos, etc.
- Promover entre sus miembros la búsqueda y el desarrollo colaborativo en temas de interés.
- Colaborar con otros CISRTs para que puedan llevar a cabo una respuesta de incidentes de forma eficiente y efectiva.
- Proporcionar en las fronteras regionales asistencia y recomendaciones legales relacionadas con la seguridad de la información y las respuestas a emergencias.

4.10 Organismos de China en Ciberseguridad

La **Administración del Ciberespacio de China(CAC)** [58] fue fundada en 2014 y depende de la Comisión de Asuntos Centrales del Ciberespacio del gobierno de la República Popular China. Su principal misión es controlar el ciberespacio

en China y evitar que se materialicen las ciberamenazas. Está estructurada en los siguientes departamentos:

- Centro de Comando de Emergencias de Seguridad en Internet.
- Agencia de Centros de Servicios.
- Centro de Comunicación de información ilegal y poco saludable.

Igual que en el caso de Rusia, está administración censura los contenidos web e incluso es más restrictiva que Roskomnadzor.

En dependencia de esta administración, se crea en 2016 la **Asociación de Seguridad Cibernética(ASC),** [59] cuyo propósito es unir al sector privado con el público para gestionar la ciberseguridad en China. Está asociación está dirigida por el científico Fang Binxing que fue el creador del firewall que censura las webs que no cumplen los estándares marcados por la República Popular China. Algunos de los miembros que conforman la ASC son empresas como Baidu, Alibaba, Tencet, China Mobile y China Unicom.

4.11 Organismos de la Unión Europea en Ciberseguridad

La Unión Europea cuenta con organizaciones para gestionar la ciberseguridad en Europa que colaboran y ayudan a las asociaciones y organizaciones de cada uno de los Estados Miembros. A continuación, presentaremos las más importantes:

ENISA (European Union Agency for Network and Information Security) [60] fue creada en 2004, su sede principal está en Heraklion(Grecia) y tiene una plantilla de 65 trabajadores. Es un centro de conocimiento especializado para la ciberseguridad en Europa. Las funciones de ENISA son las siguientes:

- Cooperar en el desarrollo de las estrategias nacionales de ciberseguridad.
- Preparar a nivel europeo ejercicios de crisis cibernéticas.
- Fomentar la cooperación entre los equipos de respuestas de emergencias informáticas.
- Redactar y publicar estudios sobre ciberseguridad.
- Preparar políticas y legislación para la Unión Europea sobre ciberseguridad.

Su composición se regula según los Reglamentos UE 460/2004 y UE 526/2013 y es la siguiente:

- Director Ejecutivo.
- Consejo de Administración.
- Comité Ejecutivo.
- Grupo Permanente de Partes Interesadas.

Anualmente se realizan consultas al Comité Ejecutivo y al Consejo de Administración y del resultado de dichas consultas se obtiene un programa de trabajo anual, que marcará el funcionamiento de la agencia durante todo el año.
Los objetivos de ENISA son:

- Conseguir experiencia mediante la anticipación de la aparición de problemas de seguridad en las TIC y en caso de que se produzca su aparición, hacerles frente con avances tecnológicos.
- Ayudar a los Estados miembros y a las instituciones de la UE a redactar, elaborar y aplicar políticas para cumplir la legislación relativa a Seguridad de la Información.
- Dotar a Europa de los medios más novedosos en ciberseguridad.
- Facilitar la cooperación entre los Estados miembros y las comunidades de Seguridad de Información Nacional.

ENISA también colabora con otras organizaciones europeas como Europol, el Centro Europeo de Ciberdelincuencia(EC3), Agencia Europea de Seguridad Aérea(AESA), etc.

Los beneficiarios de la labor de la agencia son las instituciones y gobiernos de la UE, la industria de las TIC, las pymes, los equipos de respuesta de emergencias informáticas, instituciones académicas y los ciberusuarios de Europa.

CERT-EU (Computer Emergency Response Team-Europe): Es una organización europea que coopera con los CERT y las organizaciones de ciberseguridad de los Estados Miembros para intercambiar información y enfrentarse conjuntamente a las ciberamenzas. Se crea en 2012 y su equipo está compuesto por 30 expertos en seguridad de las TIC de las Instituciones de la UE (Parlamento Europeo, Comité de las regiones, Comité Económico y Social…). Su alcance abarca la prevención, detección, respuesta y recuperación de incidentes. Según el documento RFC 2350[61] los valores clave que rigen el CERT-EU son:

- Orientación al servicio en un alto grado y disponibilidad operativa.
- Mantener los más altos estándares de integridad ética.
- En el caso de incidentes y emergencias responder con una alta capacidad efectiva y con un elevado compromiso para la resolución de problemas.
- Instituir y complementar las capacidades de sus miembros.
- Facilitar el intercambio de buenas prácticas entre miembros y entidades afines.
- Fomentar una cultura abierta, en un entorno protegido con la finalidad de obtener y aumentar el conocimiento.

Los servicios que ofrece el CERT-EU son los siguientes:

- Anuncios: Proporcionar información (vulnerabilidades publicadas, medidas de seguridad o protección, ciberamenazas…) para proteger los sistemas y las redes.
- Advertencias y alertas: Difundir información sobre interrupciones, ciberataques, alertas de intrusión, virus, vulnerabilidades y recomendaciones a los miembros de CERT-EU para abordar los problemas.
- Coordinación de Respuesta de Incidentes: Se encarga de coordinar la respuesta de incidentes en las instituciones y organismos de la UE, cooperando con proveedores y propietarios de las partes implicadas de la

infraestructura TI, CERTs y CSIRTs internacionales y europeos, operadores de telecomunicaciones y cuerpos públicos y privados según corresponda.

Centro Europeo de Ciberdelincuencia(EC3): Forma parte de la estructura de EUROPOL y se encuentra activo desde 2013. Surge en el marco de la Estrategia de Seguridad Interior de la UE de 2010 para disminuir el número de ciberdelitos de la Unión Europea.

Sus principales líneas de acción son los ciberataques de tipo financiero, la explotación sexual a través de medios electrónicos y los delitos a infraestructuras críticas y esenciales de la UE.

Según la Comisión Europea de 2012 el EC3 debe desarrollar los siguientes aspectos [62] [63]:

- Ser el eje central de información sobre delincuencia en Europa.
- Contribuir a la formación de los Estados miembros de la UE aunando el conocimiento sobre ciberdelitos europeos.
- Apoyar a los Estados Miembros en la investigación de ciberdelitos.
- Representar al colectivo de investigadores de ciberdelitos de Europa ante el Estamento Judicial y los Organismos de Orden Público.

Según la figura 6 que se ha obtenido de la página de EUROPOL [63], el EC3 se estructura en tres áreas diferenciadas que son:

Estrategias: Formada por dos equipos

- Divulgación y apoyo: crea asociaciones y coordina medidas preventivas y de sensibilización.
- Estrategias de desarrollo: Realiza el análisis estratégico, prepara medidas políticas y legislativas y desarrolla formación estandarizada.

Operaciones: Se centra en los ciberdelitos siguientes:

- Crímenes de alta tecnología.
- Pago fraudulento.
- Abuso sexual infantil online.

Pericia forense: Se distribuye en análisis forense digital y de documentos, cuya finalidad es dar soporte operativo y realizar investigaciones y desarrollo.

Todas las áreas son respaldadas por el J-CAT (Joint Cybercrime Action Taskforce) que gestiona los principales ciberdelitos de la Unión Europea y el CIT (Cyber Intelligence Team) que analiza, recoge y procesa información relacionada con ciberamenazas emergentes y patrones obtenida de fuentes públicas y privadas.

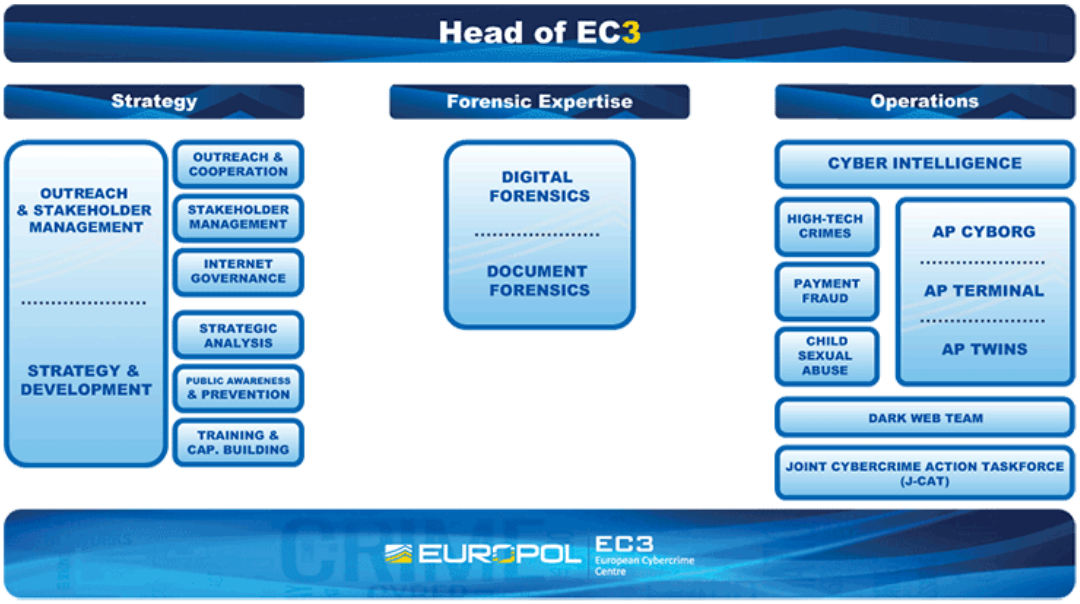


Figura 6: Estructura del EC3 obtenida de la web de Europol [63]

Para cada una de las tres categorías anteriores, el EC3 tiene que cumplir los siguientes objetivos que se indican en su web [63]:

- Servir como eje central para la información criminal e inteligencia.
- Apoyar las operaciones y las investigaciones de los Estados miembros mediante el análisis operativo, la coordinación y la experiencia.
- Proporcionar una variedad de productos de análisis estratégico que permitan la toma de decisiones basadas en información a nivel táctico y estratégico para combatir y prevenir los ciberdelitos.
- Proveer una función de divulgación integral que conecte a las autoridades policiales y judiciales que se ocupan del cibercrimen con el sector privado, las instituciones académicas y otros miembros.
- Apoyar la capacitación y la creación de habilidades en particular para las autoridades pertinentes de los Estados miembros.
- Proporcionar especialización técnica en soporte forense digital y técnico para investigaciones y operaciones.
- Representar a las entidades policiales de la UE en áreas de interés común (requisitos de investigación y desarrollo, gobierno de internet y desarrollo de políticas).

4.12 Organismos de España en Ciberseguridad

En este apartado analizaremos las organizaciones que abordan la ciberseguridad en España. Como el ámbito de la ciberseguridad es tan amplio, estudiaremos las organizaciones gubernamentales, las militares, las que se dedican a ciberdelitos e incluso las que centran su actividad en la protección de datos.

Consejo de Seguridad Nacional(CSN): La Ciberseguridad cada día tiene más relevancia y las pérdidas económicas debidas a ciberataques aumentan de forma desproporcionada anualmente. Ante esta realidad y para alinearse con las

propuestas de la Unión Europea en ciberseguridad se crea la Estrategia de Ciberseguridad Nacional [64] que tiene como objetivo general conseguir que España haga un uso seguro de los Sistemas de Información y Telecomunicaciones, fortaleciendo las capacidades de prevención, defensa, detección y respuesta a los ciberataques. Según la citada estrategia, este objetivo general se puede desglosar en los seis objetivos siguientes [64]:

- Garantizar que los Sistemas de Información y Telecomunicaciones de las Administraciones Públicas tengan el nivel correcto de resiliencia y ciberseguridad.
- Impulsar la resiliencia y seguridad de los Sistemas de Información y Telecomunicaciones que se utilizan en el sector empresarial y más concretamente en los operadores de Infraestructuras Críticas
- Potenciar las capacidades de prevención, detección, reacción, análisis, recuperación, respuesta, investigación y coordinación frente a las actividades del terrorismo y la delincuencia en el ciberespacio.
- Sensibilizar a los ciudadanos, profesionales, empresas y Administraciones Públicas de los riesgos derivados del ciberespacio.
- Alcanzar y mantener los conocimientos, habilidades, experiencia y capacidades tecnológicas que necesita España para sustentar todos los objetivos de ciberseguridad.
- Contribuir a la mejora de la ciberseguridad en el ámbito internacional.

Para poder cumplir esos objetivos la estructura orgánica que establece el gobierno es la que mostramos en la siguiente imagen:

Figura 7: Estructura orgánica de la ciberseguridad Nacional
Fuente: Estrategia de Ciberseguridad Nacional 2013[64]

El Consejo de Seguridad Nacional(CSN): Se crea como una Comisión Delegada del Gobierno para la Seguridad Nacional. Su función es asistir al presidente dirigiendo la Política de Seguridad Nacional. Bajo su mando se establecen dos comités especializados en Ciberseguridad que analizaremos a continuación:

- **Consejo Nacional de Ciberseguridad:** Es el comité especializado en Ciberseguridad y se creó el 5 de diciembre de 2013 por acuerdo del Consejo de Seguridad Nacional. Se compone de departamentos, organismos y agencias de las Administraciones Públicas en materia de

ciberseguridad y miembros del sector privado y especialistas cuya contribución se considere necesaria. En la siguiente imagen obtenida de la web del Departamento de Seguridad Nacional [65] se muestra la estructura organizativa:

Figura 8: Estructura Consejo Nacional de Ciberseguridad de la web del DSN [65]

Se reúne a petición del presidente al menos de forma semestral y cuantas veces se estime oportuno dependiendo de las necesidades en materia de ciberseguridad. Entre sus funciones se encuentran la de dar apoyo en la toma de decisiones del Consejo de Seguridad Nacional en temas de ciberseguridad, mejorar y reforzar las relaciones de colaboración y cooperación entre las Administraciones Públicas que se dedican a la Ciberseguridad y también entre los sectores privados y públicos, preparar propuestas de normativas en ciberseguridad para elevarlas al CSN, verificar el cumplimiento de la Estrategia de Ciberseguridad Nacional y valorar los riesgos y amenazas para crear planes de respuesta y ejercicios de gestión de crisis.

- **Comité Especializado de Situación:** Actuará para gestionar situaciones de crisis en el ámbito de ciberseguridad, que por su dimensión o impacto no puedan ser controladas por los medios habituales.

Instituto Nacional de Ciberseguridad(INCIBE): Adquiere su actual denominación en 2014, ya que con anterioridad era conocido como Instituto Nacional de Tecnologías de la Comunicación, S.A.(INTECO). Depende del Ministerio de Economía y Empresa a través de la Secretaría de Estado para el Avance Digital. Su misión según su web [66] es reforzar la ciberseguridad, la confianza y la protección de la información y privacidad en los servicios de la

Sociedad de la Información, aportando valor a ciudadanos, empresas, Administración, red académica y de investigación española, sector de las tecnologías de la información y las comunicaciones y sectores estratégicos en general.
Su visión se centra en conseguir sus objetivos mediante:

- El compromiso de profesionales excepcionalmente cualificados que mediante sus proyectos y dedicación aportan valor e innovación de forma continua.
- Dinamizar el sector de las TIC, facilitando la creación de negocios y oportunidades para clientes, proveedores y profesionales siempre respetando el principio de igualdad.
- Dar soporte a ciudadanos, empresas, administraciones, RedIRIS y sus afiliados.
- Generar inteligencia en ciberseguridad para así poder desarrollar tecnologías y conocimiento que se podrá utilizar en nuevas estrategias y herramientas.

Algunos de sus valores fundamentales son la transparencia, la búsqueda de la excelencia, la vocación de servicio público, la sostenibilidad, etc.

El INCIBE tiene 4 divisiones o líneas de acción que explicaremos a continuación:

- Oficina Segura del Internauta(OSI) [67]: nace para dar apoyo e informar a los usuarios en temas relacionados con la navegación por internet. Tienen como objetivo reforzar la confianza en el ámbito digital mediante la formación en ciberseguridad. Dispone de herramientas, documentos y guías para la navegación segura, soporte técnico y un canal de avisos.
- Internet Segura for Kids(IS4K): Se crea para alinearse con la estrategia europea BIK (Better Internet for Kids). Es un Centro de Seguridad en Internet para menores que tiene como objetivo promover el uso responsable y seguro de las nuevas tecnologías e internet entre menores de edad. Sus funciones son [68]:
    - Sensibilizar y formar a menores y a las personas relacionadas con ellos, a través de programas, iniciativas y campañas a nivel nacional.
    - Ofrecer un servicio online de ayuda para asesorar a los menores y a su entorno para que puedan afrontar los riesgos de Internet (conductas inapropiadas, contactos dañinos y contenidos perjudiciales).
    - Organizar en España el Día de la Internet Segura.
    - Disminuir la disponibilidad de contenido criminal en Internet, centrándose en contenidos de abuso infantil para dar soporte a las FFCCSE (Fuerzas y Cuerpos de Seguridad del Estado).
- INCIBE-CERT [69]: Es el centro de respuesta a incidentes de seguridad del INCIBE, el cual da apoyo a los ciudadanos y al sector privado. Su función es coordinarse con equipos de incidentes nacionales e internacionales para gestionar incidentes y delitos relacionados con las redes y sistemas de información. Si el incidente que se produce afecta a infraestructuras críticas tendrá que gestionarlo con el CNPIC (Centro Nacional de Infraestructuras y Ciberseguridad).

- Protege tu empresa [70]: Es una sección dentro de la web de INCIBE en la que se asesora a empresas en materia de ciberseguridad mediante guías, herramientas, kits, formación, avisos y un blog especializado.

CCN-CERT: Se crea en 2006 y forma parte del Centro Criptológico Nacional(CCN). Su misión según su web [71] es la de 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. Su competencia se centra en gestionar los incidentes en ciberseguridad que afecten a los organismos o empresas de tipo público. En el caso de operadores críticos públicos el incidente se gestionará en coordinación con el CNPIC (Centro Nacional de Infraestructuras y Ciberseguridad).

Mando Conjunto de Ciberdefensa(MCCD): Nace en 2013, subordinado al Jefe de Estado Mayor de la Defensa(JEMAD). Es el encargado de planificar y ejecutar todas las acciones de ciberdefensa en los sistemas de información y redes del Ministerio de Defensa. Sus funciones principales según su web son [72]:

- Garantizar el acceso de forma libre al ciberespacio, para poder cumplir las misiones y cometidos asignados a las Fuerzas Armadas, a través de los medios y procedimientos necesarios.
- Garantizar la disponibilidad, integridad y confidencialidad de la información, así como la integridad y disponibilidad de las redes y sistemas que la gestionan.
- Garantizar la operatividad de los servicios críticos de los sistemas de información y telecomunicaciones de las Fuerzas Armadas cuando se produzcan incidentes, accidentes o ataques y el ambiente donde se encuentren estos sistemas este degradado.
- Obtener, analizar y explotar la información sobre ciberataques e incidentes en las redes y sistemas que operen bajo su tutela.
- Ante amenazas o agresiones que comprometan la Defensa Nacional, llevar a cabo una respuesta oportuna, legítima y proporcionada en el espacio cibernético.
- Administrar y organizar, en el ámbito de Ciberdefensa, la actividad de los centros de respuesta a incidentes de seguridad de la información de los Ejércitos y Armada y el de operaciones de seguridad de la información del Ministerio de Defensa.
- Ejercer la representación del Ministerio de Defensa en cuestiones de ciberdefensa militar a escala nacional e internacional.
- Colaborar, en el ámbito de ciberdefensa, con los centros nacionales de respuesta a incidentes de seguridad de la información, en concordancia con lo que determinen las estrategias y políticas nacionales de ciberseguridad en vigor, así como con otros CERTs militares en el ámbito internacional.
- Delimitar, administrar y coordinar la concienciación, la formación y la instrucción especializada en el ámbito de ciberdefensa.

Posee un CERT propio denominado ESP DEF CERT, cuya función es gestionar los incidentes en ciberseguridad de las Fuerzas Armadas y los que puedan afectar a Defensa Nacional.

Centro Nacional de Infraestructuras y Ciberseguridad(CNPIC) [73]: Nace en 2002 de un acuerdo del Consejo de Ministros para la protección de infraestructuras críticas. Posee competencias para la gestionar los ciberincidentes producidos en las infraestructuras críticas. Ha suscrito un acuerdo de colaboración con INCIBE mediante el cual se ha creado un CERT especializado en gestión de incidentes nacionales en las infraestructuras críticas. Cualquier tipo de problema de seguridad cibernética en infraestructuras críticas se le debe notificar para que pueda gestionarlo adecuadamente.

Agencia Española de Protección de Datos(AEPD): Es una autoridad estatal independiente que nace en 1992 y empieza su actividad en 1994 y que se encarga del cumplimiento de la normativa sobre protección de datos. Tiene personalidad jurídica propia y su relación con el Gobierno es a través del Ministerio de Justicia. En la siguiente imagen que se ha obtenido de su web [74] se muestra su organigrama:

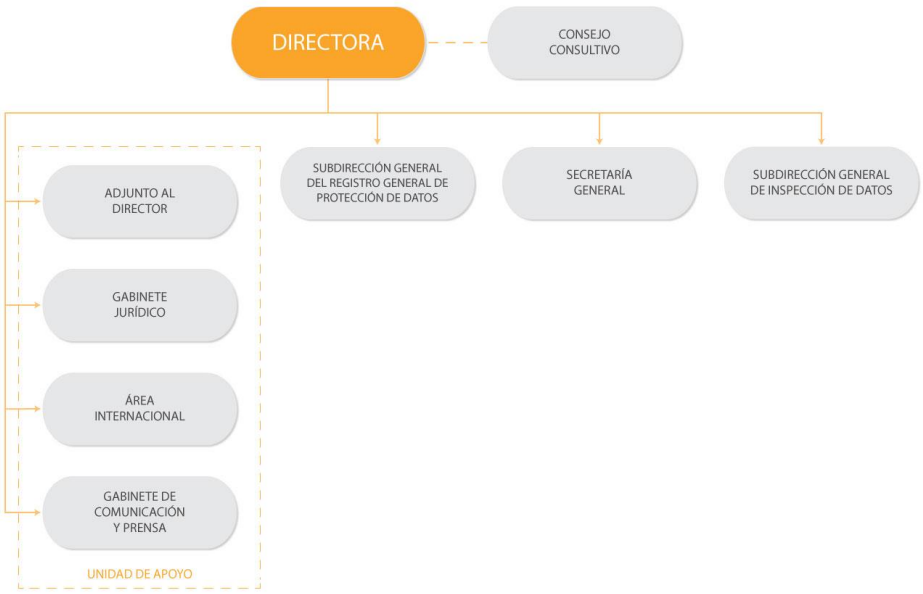


Figura 9: Organigrama AEPD obtenido de la web de la AEPD [74]

Como se observa en la imagen, su máximo representante es la directora que es asesorada por un Consejo Consultivo formado por 9 miembros y la propia directora, que se reúnen como mínimo cada seis meses. En dependencia de la dirección está la subdirección general del registro general de protección de datos, la secretaria general, la subdirección general de inspección de datos y la unidad de apoyo que está compuesta por diversas áreas.
Los programas e iniciativas que lleva a cabo se basan en los 5 ejes centrales del plan estratégico 2015-2019 que se muestran a continuación [75]:

- Prevención para una protección más eficaz: Algunas de las líneas a desarrollar en este eje son la creación de herramientas y guías para concienciar sobre los derechos y garantías de los ciudadanos en materia

de protección de datos, focalizando su atención en proteger a los ciudadanos en las actividades que desarrollan en internet y en garantizar la privacidad de los menores de edad.

- Innovación y protección de datos: factor de confianza y garantía de calidad: En este sentido algunos de los puntos a desarrollar son el estudio y análisis de productos tecnológicos para verificar que se da el tratamiento correcto y adecuado a los datos personales y que se da cumplimiento a lo especificado en el RGPD.
- Una agencia colaboradora, transparente y participativa: Este eje centrará sus líneas de actuación en la mejora de los canales de información existentes y además pretende poner en marcha un servicio específico de atención a menores, docentes y padres y otros servicios a pymes y responsables de ficheros.
- Una agencia cercana a los responsables y a los profesionales de la privacidad: Se pretende promover la figura de los delegados de protección de datos (DPO) y establecer una colaboración permanente con ellos.
- Una agencia más ágil y eficiente: En este punto se pretende llevar a cabo la digitalización y automatización de los procesos internos de gestión y de las herramientas de comunicación con los usuarios. Se quiere también implementar medidas para incentivar la productividad y la calidad del trabajo y se establecerán métricas para realizar la evaluación objetiva de los trabajadores.

Grupo de Delitos Telemáticos(GDT): El grupo de delitos informáticos fue creado en 1996, bajo la tutela de la Unidad Central Operativa de la Guardia Civil con el nombre de Grupo de Delitos Informáticos(GDI). Su misión es investigar todas las conductas delictivas que se producen contra los sistemas de información o a través de ellos. Para ayudar al GDT se crea un Equipo de Investigación Tecnológica (EDITE, s) en cada provincia española. Los objetivos del GDT y los EDITEs son [76]:

- Investigar los cibercrímenes.
- Fomentar el uso seguro de las nuevas tecnologías para poder reducir el impacto de la ciberdelincuencia.
- Asistir a seminarios y conferencias internacionales para poder crear una red de contactos internacionales que les ayuden a resolver crímenes a escala global.
- Participar activamente en los Grupos de la Interpol de Europa y Latinoamérica y en el Grupo Europol.

Grupo de Ciberterrorismo [91]: Este grupo pertenece al Servicio de Información de la Guardia Civil. Su función es luchar contra las amenazas terroristas a través de Internet y colaborar con otros grupos del Servicio de Información en lo referente a las Tecnologías de la Información(TI). Algunas de las tareas que lleva a cabo este grupo son:

- Acciones preventivas que se centran en monitorizar los sistemas y detectar vulnerabilidades en red.
- Vigilar las actividades en red de grupos terroristas.
- Realizar actividades formativas sobre seguridad en las TIC.

Brigada Central de Investigación Tecnológica(BCIT): Encuadrada en la Unidad de Delincuencia Económica y Fiscal(UDEF) de la Policía Nacional se encarga de la investigación ciberdelitos. Su misión consiste en recabar pruebas y perseguir delincuentes para poder ponerlos a disposición judicial. Su ámbito de actuación es el siguiente [77]:

- Amenazas, injurias y calumnias por medios digitales.
- Pornografía infantil y protección del menor en la utilización de nuevas tecnologías.
- Fraudes en el uso de las comunicaciones.
- Fraudes y estafas en internet.
- Seguridad lógica, ataques DDoS, hacking, descubrimiento y revelación de secretos, suplantación de identidad…
- Piratería de software, música y productos cinematográficos.

Las funciones que lleva a cabo para cumplir su misión son [78]:

- Gestionar de forma directa las investigaciones más complejas.
- Coordinar las operaciones que involucren a varias Jefaturas Superiores
- Formar al personal del Cuerpo Nacional de Policía y a otros cuerpos de Policía extranjeros.
- Ejecutar y/o coordinar investigaciones que se originen en otros países y para las que se solicite la intervención del BCIT.

4.13 Conclusiones

A lo largo de este capítulo se han analizado distintos tipos de organizaciones cuya finalidad es ayudar a garantizar la ciberseguridad y evitar o mitigar los daños producidos por los ciberataques. A continuación, se presentan las conclusiones que se han obtenido del análisis realizado:

- Las organizaciones de tipo militar centran sus estrategias en la ciberdefensa y suelen aliarse con otros países u organizaciones afines para proteger sus intereses.
- Cada país suele contar con un CERT propio para poder gestionar los incidentes de seguridad que sucedan. También existen CERTs a nivel continental o incluso el FIRST, que trabaja a nivel internacional ayudando a gestionar los incidentes y facilitando la cooperación y comunicación entre los CERTs que lo forman.
- Existen también departamentos dentro de los cuerpos policiales dedicados a luchar contra la ciberdelincuencia. EL EC3 surge en la Europol con esa finalidad y coopera con los cuerpos policiales de los Estados Miembros y con otros estamentos policiales a nivel internacional para luchar contra la ciberdelincuencia.
- La función de ICANN es asignar las direcciones IP y verificar los DNS. Aunque parece no tener una relación directa con la ciberseguridad es muy importante ya que, si no realizase su labor, todas las bases del funcionamiento de Internet se desmoronarían. Por tanto, está asociación es crucial para mantener la ciberseguridad.
- En EE. UU existen organizaciones como la NSA que espían comunicaciones de ciudadanos de otros países para proteger la

seguridad de su país y de sus aliados. Esta forma de gestionar las comunicaciones es muy criticada ya que se violan los derechos de privacidad de los ciudadanos.

- Rusia y China utilizan sus organizaciones dedicadas a la ciberseguridad para intervenir y censurar las comunicaciones de los ciudadanos. Ambas poseen listas negras para incluir las webs que ellos consideran que son nocivas para sus ciudadanos y evitar así que puedan acceder a ellas, vulnerando los derechos fundamentales de los ciberusuarios.
- La Unión Europea tiene como organismo principal de la ciberseguridad a ENISA. Esta organización ayuda a gestionar la ciberseguridad de las instituciones y órganos de la Unión Europea y de los Estados Miembros.
- España posee un sistema de organizaciones en ciberseguridad muy bien estructurado. La base de la seguridad en las TIC se establece en el plan estratégico de ciberseguridad y se lleva a cabo mediante la gestión que realizan esos organismos y asociaciones.
- No existe un modelo perfecto de organización para gestionar la ciberseguridad. Cada una de ellas aporta su propio valor y se dedica a realizar la misión para la que se ha creado. El valor fundamental que poseen todas ellas es el espíritu de cooperación nacional e internacional para poder gestionar la ciberseguridad, evitar ciberataques y luchar contra los ciberdelincuentes de forma organizada.

5. Tratados de Cooperación Internacionales en Ciberseguridad

5.1 Introducción

Los usuarios de Internet aumentan día a día, y en un mundo cada vez más globalizado y dependiente de las tecnologías emergentes se hace más difícil gestionar de forma adecuada la ciberseguridad. Cuando se produce un ciberataque no suele afectar a un solo país y aunque suceda así, en muchas ocasiones el ataque se ha lanzado desde otro lugar del mundo. Ante esta situación, se empiezan a establecer convenios y acuerdos internacionales para poder hacer frente al ciberterrorismo, la ciberdelincuencia y los ciberataques de forma coordinada.

En este capítulo analizaremos los convenios y tratados más relevantes en ciberseguridad. Se empezará presentando las declaraciones conjuntas entre UE y OTAN, se revisarán a continuación acuerdos entre asociaciones de la UE, declaraciones conjuntas internacionales y acuerdos entre empresas tecnológicas. Se analizará en profundidad el Convenio de Budapest y finalmente se hablará de forma general de los acuerdos suscritos por el Gobierno de España en el ámbito de la Ciberseguridad.

5.2 Acuerdo de Colaboración UE y OTAN

La OTAN y la UE han firmado varios acuerdos de cooperación en seguridad. Entre los puntos de esos acuerdos se encuentra la ciberseguridad, ya que hoy en día es uno los puntos clave para garantizar la seguridad internacional. A continuación, hablaremos de la declaración conjunta de 2018 y del acuerdo técnico de 2016 y como en ellos, la UE y la OTAN se comprometen a cooperar para mejorar la ciberseguridad.

El 10 de junio de 2018, la UE y la OTAN firman una declaración conjunta para abordar las amenazas comunes. Dentro de este acuerdo menciona la cooperación que deberá existir para hacer frente a las ciberamenazas. El punto 6 del acuerdo [79] nos dice lo siguiente:" Los múltiples y cambiantes desafíos de seguridad que enfrentan nuestros Estados Miembros y Aliados del Este y del Sur hacen que nuestra cooperación continua sea esencial, incluyendo la respuesta a híbridos y amenazas cibernéticas en las operaciones y ayudando a nuestros socios comunes". No se dan directrices para gestionar la colaboración en ciberseguridad, pero posiblemente se presenten unas conclusiones complementarias para ejecutar la Declaración Conjunta como sucedió con la Declaración conjunta UE-OTAN de julio de 2016.

El 10 de febrero de 2016 la UE y la OTAN firmaron un acuerdo técnico [80] para aumentar su cooperación en la lucha contra los ciberataques, facilitando así el intercambio de información y mejores prácticas en el ámbito de ciberseguridad entre el CERT-EU y el NCIRC que son sus respectivos equipos de respuesta a incidentes.

Por último, otra medida de cooperación entre el Gobierno Europeo y la OTAN es la participación de la UE en el ejercicio de ciberseguridad anual de la OTAN denominado Cyber Coallition.

5.3 Memorando de Cooperación entre ENISA, EDA, Europol y CERT-EU

El 23 de mayo de 2018 se firma en Bruselas el Memorando de Cooperación entre ENISA (European Union Agency for Network and Information Security), EDA (European Defence Agency), Europol's European Cybercrime Centre(EC3) y CERT-EU (Computer Emergency Response Team-European Union) para cumplir con las medidas acordadas en el paquete de estrategias de seguridad cibernética de la Unión Europea. En el memorando se acuerda la cooperación entre las agencias, pero en ninguna circunstancia es legalmente vinculante. En el caso de que algún aspecto de cooperación no esté cubierto por alguna de las partes, la cooperación tendrá lugar entre el resto de los firmantes del memorando. El mandato lo llevará a cabo una de las agencias y se renovará anualmente de forma rotativa. Las áreas de cooperación y algunas de sus líneas de acción son [81]:

- Intercambio de información: Las partes acuerdan intercambiar información recogida, procesada y analizada y mejores prácticas que mejoren el entendimiento de la ciberseguridad, la ciberdefensa y el cibercrimen.
- Formación educativa y ciberejercicios: Se podrán desarrollar plataformas coordinadas para llevar a cabo formación, intercambio de documentación y ejercicios de ciberseguridad y ciberdefensa que ayudarán a promover sinergias y a evitar la duplicación de esfuerzos.
- Cooperación Técnica: Se intentará aumentar la cooperación entre las partes para poder mejorar la respuesta a los incidentes de seguridad y crisis.
- Cuestiones estratégicas y administrativas: Las partes realizarán consultas entre ellas cuando preparen sus estrategias y planes de acción en las áreas de cooperación definidas en el memorando. Además, también se acuerda cooperar en cuestiones administrativas para compartir experiencias y mejores prácticas en el campo de los Recursos Humanos, auditorías internas y externas, calidad y gestión de riesgos, finanzas, etc.

5.4 Paris Call For Trust and Security in CyberSpace

La Paris Call For Trust and Security in CyberSpace se firma el 12 de noviembre de 2018 en el Paris Peace Forum y es una declaración de alto nivel en la que se desarrollan principios comunes en ciberseguridad para obtener una estabilidad digital en el mundo y respetar los derechos humanos en entornos digitales. Está declaración está respaldada por 370 firmantes entre los que se encuentran gobiernos, representantes de la industria, comunidad técnica, investigadores, organizaciones no gubernamentales y ciudadanos. Para cumplir con los principios de la declaración, los firmantes deberán trabajar juntos y cooperar en los siguientes puntos citados en el acuerdo [82]:

- Tomar medidas de prevención y recuperación de actividades maliciosas que amenacen o causen daños significativos, indiscriminados o sistémicos a usuarios e infraestructuras críticas.

- Proteger la disponibilidad y la integridad en internet.
- Cooperar para evitar interferencias en procesos electorales.
- Trabajar en la prevención del robo de la propiedad intelectual mediante internet, incluidos secretos comerciales u otra información comercial confidencial, con la intención de proporcionar ventajas competitivas.
- Prevenir la difusión de herramientas y prácticas maliciosas online.
- Fortalecer la seguridad de los procesos, productos y servicios digitales, a lo largo de su ciclo de vida y cadena de suministro.
- Promover una higiene cibernética avanzada para todos los actores.
- Tomar medidas para evitar que los actores no estatales, incluido el sector privado, pirateen, para sus propios fines o los de otros actores no estatales.
- Cooperar para llevar a cabo una aceptación e implementación generalizada de las normas internacionales de comportamiento responsable, así como las medidas de fomento de la confianza en el ciberespacio.

Se programarán reuniones en 2019 para verificar el progreso de los objetivos definidos en la declaración.

5.5 Cybersecurity Tech Accord

Es un acuerdo que surge entre empresas tecnológicas y de seguridad para luchar contra cibercriminales. Algunas de las empresas que han firmado este acuerdo son: ABB, Arm, Avast, Bitdefender, BT, CA Technologies, Cisco, Cloudflare, DataStax, Dell, DocuSign, Facebook, Fastly, FireEye, F-Secure, GitHub, Guardtime, HP Inc., HPE, Intuit, Juniper Networks, LinkedIn, Microsoft, Nielsen, Nokia, Oracle, RSA, SAP, Stripe, Symantec, Telefónica, Tenable, Trend Micro y VMware.

Los principios que se adoptan en el acuerdo según su web [83] son:

- Proteger a los usuarios y clientes en todo el mundo: Las empresas firmantes se esforzarán por proteger a los usuarios y clientes de los ciberataques. Se comprometen a desarrollar y diseñar productos y servicios en los que se dé prioridad a la seguridad, privacidad, integridad y confidencialidad y que minimicen la gravedad, probabilidad, frecuencia y explotación de vulnerabilidades.
- Oponerse a los ciberataques a ciudadanos inocentes y empresas del mundo: Se protegerá de la manipulación y explotación de productos y servicios durante su desarrollo, diseño, distribución y uso.
  No se colaborará en ninguna circunstancia con el lanzamiento de ciberataques de los gobiernos.
- Ayudar a empoderar a usuarios, clientes y desarrolladores para que fortalezcan la protección en ciberseguridad: Se facilitaran a los clientes, desarrolladores y usuarios información y herramientas para conocer las ciberamenazas existentes y futuras y que se puedan proteger de ellas.
  Se apoyará a gobiernos, organizaciones internacionales y ciudadanos para que se promueva la ciberseguridad y se desarrollen equitativamente capacidades de ciberseguridad en países desarrollados y emergentes.

- Se trabajará la cooperación entre los firmantes y grupos afines para mejorar la ciberseguridad: Se crearán grupos formales e informales con investigadores, empresas y ciudadanos en los que se mejorará la colaboración técnica, la divulgación de vulnerabilidades y amenazas y la minimización de código malicioso mediante tecnologías patentadas y código abierto.
  Se fomentarán intercambios de información global para prevenir, detectar, identificar y responder a los ciberataques.

5.6 Convenio sobre ciberdelincuencia

El convenio sobre ciberdelincuencia o convenio de Budapest se firma en Budapest en 2001 por parte de los miembros del Consejo Europeo. Podríamos considerarlo como el convenio más importante en el ámbito de la ciberdelincuencia. Hoy en día, ha sido firmado por más de 56 países y algunos más se encuentran a la espera de ser aceptados.

El objetivo del convenio es crear una política penal común para los ciberdelitos y fomentar la cooperación internacional. Para lograr este objetivo se establecen tres ejes centrales que se distribuyen a lo largo de los cuatro capítulos que posee el convenio y que son las siguientes [84], [85]:

- Definir y clasificar los delitos informáticos: Esta clasificación se distribuye en las cuatro categorías que se muestran a continuación:
  - Tecnología como fin: Estos delitos dañan la confidencialidad, disponibilidad e integridad. Dentro de esta categoría se encuentran el acceso ilícito, la interceptación ilícita, ataques a la integridad de datos, ataques a la integridad del sistema y abuso de los dispositivos.
  - Delitos informáticos o delitos que utilizan los sistemas informáticos como medio. Dentro de esta categoría se encuentran la falsificación informática y el fraude informático.
  - Delitos relacionados con el contenido: Se encuadran toda la tipología de delitos de pornografía infantil.
  - Delitos relacionados con infracciones de la propiedad intelectual y derechos afines: Se refiere a delitos vinculados con la vulneración de la propiedad intelectual y que utilizan como medio internet o sistemas informáticos.
- Normas procesales: En esta sección se instauran los procedimientos para proteger y salvaguardar la prueba o evidencia digital. Estos procedimientos son aplicables a cualquier delito en el que exista una evidencia digital o se haya cometido por algún medio o sistema electrónico. Establece la forma de recoger, asegurar, y conservar las evidencias digitales para que puedan utilizarse como pruebas en un proceso judicial.
- Normas de cooperación internacional: Facilitan unas directrices y reglas de cooperación para poder investigar internacionalmente delitos que incluyan evidencias digitales. Incluye disposiciones sobre los procesos de extradición, los envíos y recogidas de evidencias digitales para que se mantenga la cadena de custodia y la localización de sospechosos.

Cuando un país es aceptado y ha firmado el convenio de Budapest ha de adecuar sus normas y legislaciones en materia de ciberseguridad a lo marcado en el convenio y además según el artículo 35 debe designar un punto de contacto para la red que este operativo 24 horas durante 7 días a la semana.

5.7 Acuerdos bilaterales y multilaterales españoles en Ciberseguridad

El Gobierno de España para dar cumplimiento al objetivo de mejora de la ciberseguridad que se incluye en la Estrategia de Ciberseguridad Nacional subscribe acuerdos y memorandos internacionales para cooperar con diversos países y organizaciones en materia de ciberseguridad.

- Memorandos de Entendimiento: España ha suscrito memorandos o declaraciones de intenciones para garantizar la ciberseguridad con los países que se mencionan a continuación [86]:
  - Túnez: Firmado el 11 de abril de 2017 y que circunscribe las tareas comunes en organizaciones internacionales, regionales y con socios y aliados comunes en materia de ciberseguridad.
  - Argentina: Suscrito el 23 de febrero de 2013 para cooperar en la lucha contra la ciberdelincuencia y el ciberterrorismo.
  - Perú: Suscrito el 8 de Julio de 2015 para proporcionar colaboración bilateral en cuestiones de ciberseguridad.
  - Paraguay: Firmado el 27 de octubre de 2015 para llevar a cabo una colaboración directa entre los países firmantes en cuestiones de ciberseguridad.
  - Chile: Suscrito el 28 de agosto de 2018. En lo referente a ciberseguridad propone cooperar para afrontar la materialización de riesgos derivados de ciberataques en organismos oficiales y sistemas informáticos y financieros.
  - Marruecos: se firma el 27 de octubre de 2015 y tiene como objetivo llevar a cabo actuaciones preparadas bilaterales en el Magreb y la Liga Árabe en ciberseguridad.
  - India: suscrito el 31 de mayo de 2017 y que tiene como finalidad acercar posturas y cooperar para evitar ciberataques y establecer medidas que aumenten la seguridad en las TIC en India y España.
- Acuerdo Multilateral con la Organización de Estados Americanos(OEA) [87]. Se firma el 17 de noviembre de 2015 y establece las bases para que los países que la suscriben cooperen en ciberseguridad intercambiando información, buenas prácticas y realizando actividades conjuntas de formación, congresos, seminarios, etc. La OEA aportará cooperación policial para luchar contra el ciberterrorismo y el cibercrimen y se coordinará con el Gobierno de España en la lucha contra las ciberamenazas.
- Acuerdo entre España y Rusia para la creación de un foro de ciberseguridad contra la desinformación [88]: El 6 de noviembre de 2018 en el encuentro que tuvo lugar en Madrid entre los Ministros de Asuntos Exteriores ruso y español, Rusia realiza una propuesta de creación de un foro para evitar la propagación de noticias falsas en medio cibernéticos. Esta propuesta aún no se ha materializado y ha recibido numerosas críticas de países europeos y de la OTAN debido a que todos los problemas de desinformación existentes se atribuyen a Rusia.

5.8 Conclusiones

Después de estudiar los convenios y declaraciones más relevantes en el ámbito de la ciberseguridad se ha llegado a las siguientes conclusiones:

- El convenio sobre ciberdelincuencia es de los más importantes y respetados en ciberseguridad. Dicta unas bases para que todos los países firmantes legislen de forma similar y consideren los mismos tipos de ciberdelitos. Al contar con 56 miembros, forma una red de muy amplia de países que cooperan en la lucha contra los ciberdelitos.
- Los acuerdos entre la Unión Europea y la OTAN centran sus esfuerzos en garantizar la ciberdefensa y en aunar esfuerzos de sus respectivos CERTs para gestionar de forma conjunta los incidentes que les afecten. Suelen ser acuerdos de alto nivel y con posterioridad se desarrollan propuestas específicas para abordarlos.
- El Memorando de Cooperación entre ENISA, EDA, Europol y CERT-EU se firma para cumplir con uno de los puntos de la Estrategia de Seguridad Cibernética de la Unión Europea. Este memorando establece directrices para que las organizaciones de la Unión Europea puedan cooperar en el ámbito de la Ciberseguridad. Es un acuerdo muy positivo que posiciona a la Unión Europea como uno de los principales referentes en ciberseguridad.
- La declaración Paris Call For Trust and Security in CyberSpace es un acuerdo de alto nivel por lo que nos marca unos puntos generales para cooperar. No entra en el nivel de detalle del Convenio de Budapest, pero es una declaración refrendada por 360 firmantes que coordina una voluntad común de gobiernos, ciudadanos, organizaciones no gubernamentales y empresas tecnológicas para conseguir una sociedad tecnológica pacífica y libre de ciberataques.
- El Cybersecurity Tech Accord destaca por ser un acuerdo entre empresas tecnológicas con una voluntad común para mantener la ciberseguridad y evitar los ciberataques. Uno de los puntos más relevantes del acuerdo es que se compromete a no cooperar en los ciberataques realizados por los gobiernos.
- El Gobierno de España siguiendo su Estrategia de Ciberseguridad Nacional ha firmado 8 convenios bilaterales y uno multilateral para garantizar la ciberseguridad. Dichos acuerdos son a alto nivel y marcan unos principios generales para asegurar la cooperación internacional ante posibles ciberataques. De entre todos los acuerdos, destaca el firmado con la Organización de los Estados Americanos, ya que al firmar este acuerdo se está garantizando la cooperación de 35 países americanos con España.
- El acuerdo de España con Rusia para crear un foro de ciberseguridad contra la desinformación de momento no se ha materializado, y posiblemente no lo haga debido a las presiones que pueda ejercer la Unión Europea y la OTAN para que España no participe en ningún foro con Rusia.
- La conclusión general a la que se llega es que no hay un acuerdo que se pueda usar como modelo a seguir pero que todos tienen en común una

declaración de principios, un alcance internacional y la voluntad de cooperación de los firmantes para luchar por un ciberespacio seguro y libre de ciberataques.

6. Ciberataques mundiales

6.1 Introducción

A lo largo de este tema se hará un análisis de los ciberataques a escala global más relevantes de los últimos tiempos. Los ataques se clasificarán según las características que mejor los definan. Los tipos de ataques que se estudiarán son:

- Ataques relacionados con criptomonedas: En 2018 ha aumentado este tipo de ataques exponencialmente. Hay diversos tipos de ataque relacionados con criptomonedas que se pueden clasificar en función de donde se centre el foco del ataque y los resultados que se esperen obtener.
- Ransomware: Estos ataques se suelen producir a escala global y suelen provocar daños multimillonarios, dado que conllevan pérdidas de información y daños en los sistemas informáticos.
- Ataques de ciberespionaje y fugas de información: Con la entrada en vigor del RGPD las fugas de información han cobrado más relevancia y en 2018 se han convertido en el centro de atención de los atacantes. Por otro lado, el ciberespionaje se mantiene latente y sigue cobrándose víctimas este año.
- Ataques a infraestructuras críticas: Estos ataques son muy importantes ya que dañan los sistemas de infraestructuras críticas como empresas eléctricas, centrales nucleares, etc.
- Ataques DDoS y botnets: Con el creciente aumento de los dispositivo IoT las redes zombies aumentan su sofisticación y cada día se incrementan en número.
- Ciberatracos: En estos últimos años, los ciberdelincuentes están cometiendo este tipo de ciberdelitos que les permiten obtener beneficios de forma rápida aprovechando vulnerabilidades existentes en los sistemas financieros.
- Posibles escenarios ciberterroristas: En este apartado se estudian algunos ataques ciberterroristas que se han intentado realizar sin éxito y otros que se podrían llevar a cabo en un futuro.

6.2 Ataques relacionados con criptomonedas

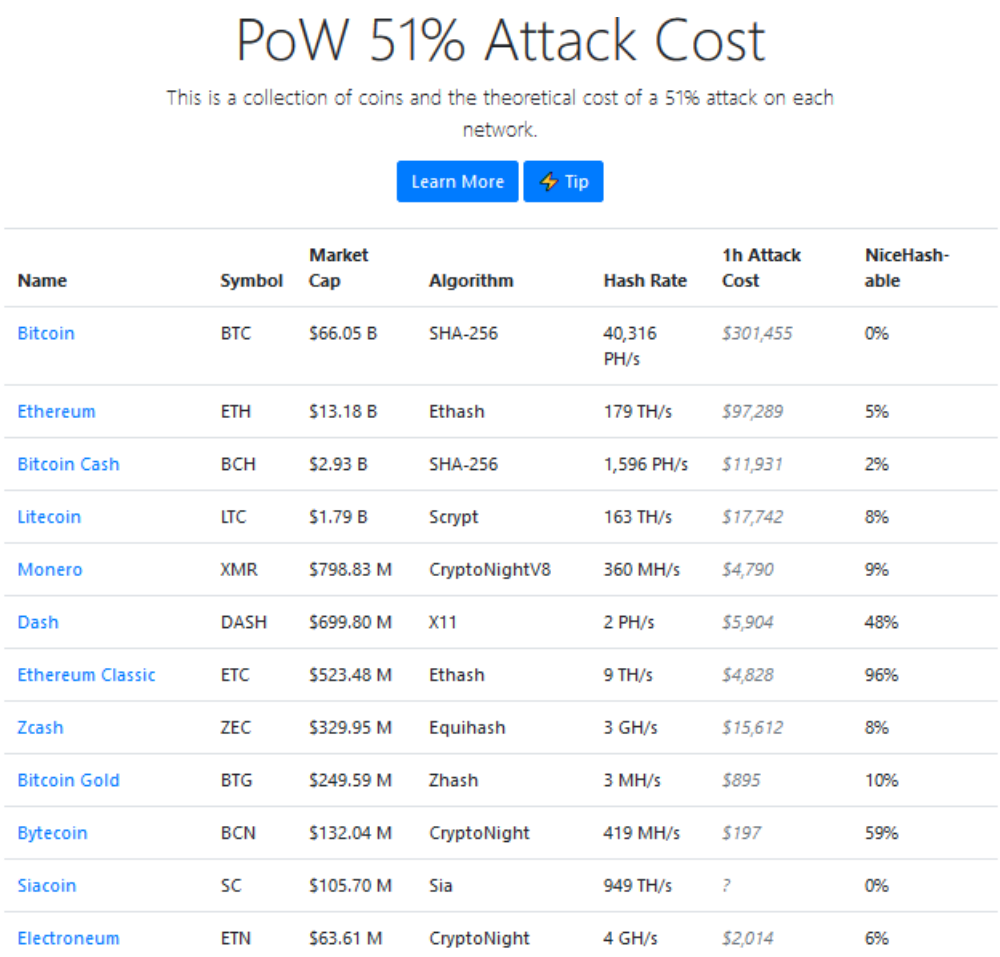
Las criptomonedas se han convertido en un elemento imprescindible en los últimos tiempos. Su anonimización y difícil rastreo las han convertido en foco de atención de los ciberatacantes, que han encontrado diversos sistemas de ataque para obtener beneficios de las criptomonedas. A continuación, se analizan los tipos de ciberataque relacionados con criptomonedas [92] más comunes y algunos de los casos más relevantes que se han llevado a cabo.

- Ataques blockchain: Los ataques de retención de bloques o del 51% son unos ataques muy complejos y suponen un coste económico muy elevado para el atacante. Estos ataques se centran en controlar la capacidad de procesar de la blockchain para evitar que se confirmen las

transacciones o alterar su historial. Para conseguir que el ataque sea exitoso, se tiene que controlar la "tasa de hash" para poder usar los mismos fondos por duplicado y así hacer una división de la blockchain en dos, con la consecuente creación de diferentes registros. El funcionamiento de la blockchain se basa en nodos distribuidos que procesan las transacciones y las registran en la cadena de bloques mediante los sistemas PoW (prueba de trabajo) o PoS (prueba de participación). Si el atacante consigue concentrar más del 50% del poder de procesamiento de la cadena de bloques, se hará con el control y podrá alterar los registros en su propio beneficio. Algunos de los ataques de este tipo que han tenido más repercusión son los que se muestran a continuación [93]:

- Monacoin: Esta criptomoneda sufrió múltiples ataques desde mayo de 2018 que ocasionaron la pérdida de confianza de sus inversores y el robo de 90.000$ en criptomonedas.
- Electroneum sufrió un ataque en mayo de 2018 pero fue neutralizado antes de que se produjesen pérdidas económicas.
- Bitcoin Gold fue atacada en mayo de 2018, como las criptomonedas anteriores, y sufrió una pérdida de confianza que provocó la cancelación de sus transacciones en las casas de cambio más importantes a escala mundial
- Verge sufrió tres ataques entre abril y junio, ya que los desarrolladores no modificaron sus problemas de seguridad después del primer incidente. En el primer ataque los hackers se hicieron con 1.400.000$.
- Zencash: Este ataque se realizó en junio de 2018 y fue el último incidente utilizando la técnica de retención de bloques que se ha notificado este año. Supuso unas pérdidas de 550.000$.

Se ha creado una web llamada crypto51[94] donde se hace un análisis del coste económico de alquilar los recursos para realizar un ataque del 51% durante una hora a diversas criptomonedas. Esta web, según sus creadores, tiene como finalidad concienciar a la gente de la problemática de este tipo de ataques y de que se deben encontrar soluciones para evitarlos. A continuación, se muestra una imagen de la lista [94]:



PoW 51% Attack Cost

This is a collection of coins and the theoretical cost of a 51% attack on each network.

Learn More | ⚡ Tip

Name	Symbol	Market Cap	Algorithm	Hash Rate	1h Attack Cost	NiceHash-able
Bitcoin	BTC	$66.05 B	SHA-256	40,316 PH/s	*$301,455*	0%
Ethereum	ETH	$13.18 B	Ethash	179 TH/s	*$97,289*	5%
Bitcoin Cash	BCH	$2.93 B	SHA-256	1,596 PH/s	*$11,931*	2%
Litecoin	LTC	$1.79 B	Scrypt	163 TH/s	*$17,742*	8%
Monero	XMR	$798.83 M	CryptoNightV8	360 MH/s	*$4,790*	9%
Dash	DASH	$699.80 M	X11	2 PH/s	*$5,904*	48%
Ethereum Classic	ETC	$523.48 M	Ethash	9 TH/s	*$4,828*	96%
Zcash	ZEC	$329.95 M	Equihash	3 GH/s	*$15,612*	8%
Bitcoin Gold	BTG	$249.59 M	Zhash	3 MH/s	*$895*	10%
Bytecoin	BCN	$132.04 M	CryptoNight	419 MH/s	*$197*	59%
Siacoin	SC	$105.70 M	Sia	949 TH/s	*?*	0%
Electroneum	ETN	$63.61 M	CryptoNight	4 GH/s	*$2,014*	6%

Figura 10: ***Lista del coste de un ataque del 51% por crypto51 [94]***

- Hackeos en casas de cambio: Las casas de cambio operan online mediante el movimiento constante de criptomonedas. Debido a este funcionamiento están expuestas a vulnerabilidades de forma habitual. Para realizar sus operaciones poseen carteras calientes y frías. Las carteras calientes son las que guardan las criptomonedas online y por tanto son un blanco fácil para los atacantes. Por otro lado, las carteras frías no se encuentran en red y son más seguras. Algunos de los ataques que se han cometido a las casas de cambio en 2018 son los siguientes:

    - Coincheck: Esta casa de cambios es una de las principales en Japón y en el continente asiático. Debido a fallos en sus medidas de seguridad y una mala gestión de los monederos en caliente, unos atacantes robaron unos 330 millones de euros en criptomonedas NEM (New Economic Movement). Este ataque perjudicó a 260.000 usuarios y coincheck tuvo que realizar compensaciones económicas a los afectados de sus propios fondos y someterse a investigaciones y controles por parte del gobierno japonés.
    - Bitgrail: La casa de cambio italiana sufrió a principios de 2018 el robo de 192 millones de dólares en criptomonedas XRB. Se

suspendieron actividades de la casa de cambio para realizar investigaciones y restaurar los sistemas.

- Coinrail: Un 30% de sus fondos fueron robados en junio de 2018 debido a una intrusión informática en sus sistemas. Inmediatamente se trasladaron sus fondos a una bóveda fría y se suspendieron sus actividades. Se estimaron unas pérdidas de unos 37.2 millones de dólares. Además de las pérdidas directas que sufrió la casa de cambio, se produjeron perdidas indirectas ya que hubo una caída del precio del bitcoin.

Como se observa en el análisis de los ataques, el problema reside en fallos de seguridad del sistema y en no guardar las criptomonedas en carteras frías para protegerlas de posibles ataques. Si se tomasen esas medidas de seguridad posiblemente el número de ataques a las casas de cambio podría disminuir significativamente.

- Ataques a monederos: El monedero o wallet podríamos decir que es similar a una cuenta bancaria y es utilizado para almacenar criptomonedas. Existen monederos online y monederos hardware. Los primeros suelen ser más fáciles de atacar que los segundos, aunque se están observando nuevas tendencias para clonar o alterar los dispositivos hardware y así poder tener acceso a las criptomonedas almacenadas en ellos. En 2018 ha habido hackeos de carteras en línea y se ha utilizado el phishing para suplantar aplicaciones y obtener las credenciales de los usuarios. A continuación, se van a mostrar los casos que más repercusión han tenido:

  - Blackwallet: En enero de 2018 unos ciberdelincuentes secuestraron su dominio y así consiguieron sustraer 400.000$ en criptomoneda XLM.
  - MyEtherWallet se vio afectada en abril por un ataque de secuestro de DNS y redireccionamiento a un sitio de phishing. No se robaron grandes cantidades, pero sí que se vio comprometida la confianza de los usuarios, ya que en diciembre del 2017 se había producido otro ataque de phishing con una app falsa en la tienda apple. Después de estos incidentes y cuando parecía que MyEtherWallet volvía a la normalidad, unos hackers atacaron la VPN hola (extensión de Chrome) que muchos clientes utilizan para acceder a su monedero, debido a esto sus fondos se vieron comprometidos y los usuarios tuvieron que redireccionar los fondos a otras carteras.
  - Samourai Wallet: En octubre de 2018 se produjo un “ataque de polvo” para desanonimizar las direcciones que poseen los usuarios en Bitcoin. Este tipo de ataques se centra en hacer movimientos de cantidades mínimas de bitcoins para seguir su rastro y así conseguir finalmente las direcciones de los usuarios que han recibido esas transferencias. El ataque fue neutralizado sin consecuencias y se informó a los usuarios de la opción que debían activar en su billetera para no sufrir ese tipo de ataque. En la

imagen siguiente se muestra el contenido de la comunicación de Samourai Wallet:

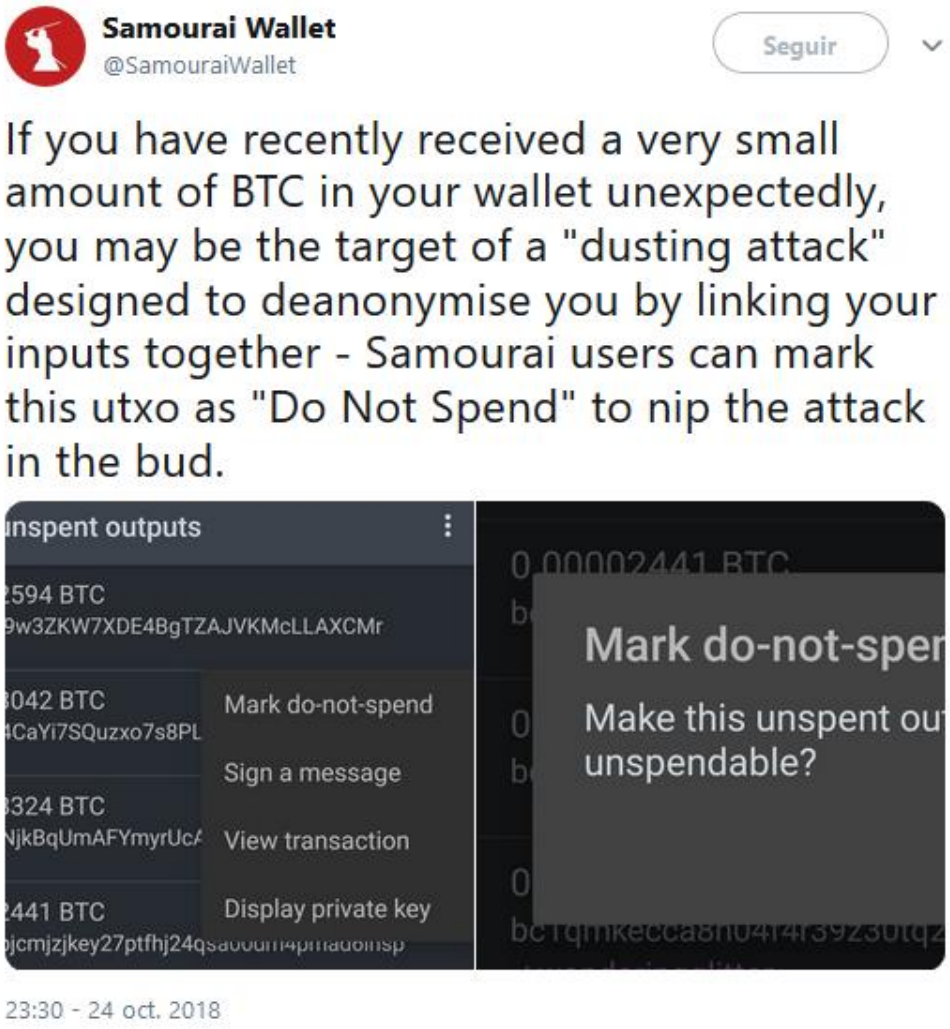


Figura 11: Twitter de Samourai Wallet para avisar a los usuarios del ataque

- LocalBitCoins y Metamask [95]: Estas dos carteras en línea fueron atacadas mediante phishing creando aplicaciones falsas en la tienda Google Play. Una vez fue descubierto el ataque se retiraron las aplicaciones, pero algunos usuarios ya habían sufrido el robo de sus fondos. La forma de ejecutarse la aplicación denotaba que no era legítima, ya que no tenía ni clave pública, ni privada y solo utilizaba un código QR habilitado para realizar las transacciones. A continuación, se muestra una imagen de la aplicación falsa LocalBitCoins.

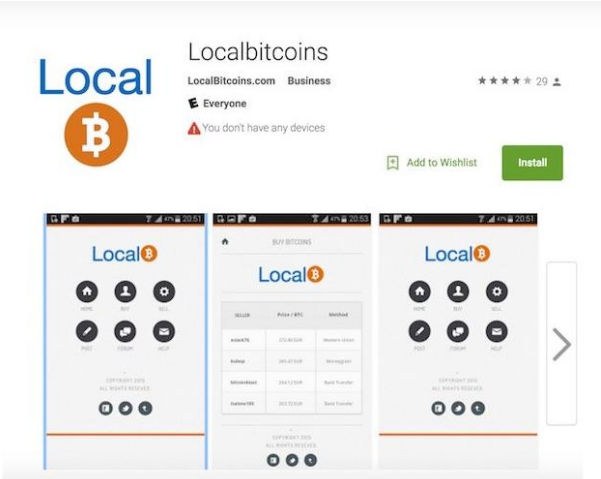


Figura 12: Phishing Localbitcoins[95]

Respecto a los monederos fríos, se han reportado vulnerabilidades en los monederos Nano y Trezor [96] que los hace vulnerables a ataques y que hace que ofrezcan menos resiliencia de la esperada. Aun así, ofrecen más seguridad que los monederos calientes y es preferible depositar los fondos en este tipo de carteras. Como las vulnerabilidades han sido expuestas públicamente, se espera que las empresas afectadas realicen las mejoras oportunas para solucionar dichas vulnerabilidades.

- Cryptojacking

  El cryptojacking o minería encubierta es un ataque en el que se utiliza la capacidad de procesamiento del dispositivo infectado para minar criptomonedas. Una de las técnicas que utilizan los atacantes consiste en introducir un minero como coinhive o similar en el código javascript de páginas de descargas ilegales o páginas de pornografía. Una vez el usuario ha accedido a las webs comprometidas, el atacante puede minar las criptomonedas sin que el usuario sea consciente. Otra alternativa que utilizan los ciberdelincuentes es ocultar los mineros en software como adobe flash de forma encubierta y prácticamente indetectable. Lo que comenzó como ataques a ordenadores personales, se ha convertido también en ataques a empresas, consiguiendo así una capacidad de procesamiento mayor que les ayuda a obtener beneficios de forma rápida. A continuación, se muestran varios casos de empresas que han sido afectadas por el cryptojacking:

  - Tesla y Amazon web [97]: En febrero de 2018 la firma de seguridad RedLock descubrió que se había accedido de forma ilegal a uno de los servidores de Tesla que se almacenaba en Amazon web. Dicho servidor, no tenía contraseña y era el servidor encargado de la distribución y gestión de las aplicaciones para los coches. Los atacantes aprovecharon el fallo de seguridad para usar el poder computacional del servidor para minar criptomonedas.
  - Youtube [98], [99]: En enero de 2018 se detectó que la plataforma de anuncios DoubleClick, que inserta anuncios en YouTube, había

sido atacada y que en el código de inserción de los anuncios se había añadido el cliente coinhive. Debido a esto, los usuarios de YouTube que visualizaban los anuncios comprometidos minaban la criptodivisa Monero(XMR) sin ser conscientes de ello. Los países que se vieron más afectados fueron Japón, Francia, Taiwán, Italia y España.

- Aviva, Gemalto y Amazon web [100]: Este caso se detectó a finales de 2017 y es similar al caso de Tesla. Mediante una vulnerabilidad existente en kubernetes que consistía en la falta de contraseña en sus contenedores, se accedió a ellos y mediante un comando minero se utilizó el poder computacional de los contenedores para minar altcoins.
- Telecom Egypt [101]: Según un estudio realizado por Citizen Lab en la Universidad de Toronto en marzo de 2018[102], Telecom Egypt habría estado redirigiendo a los usuarios de la empresa de telecomunicaciones a sitios de minería a través de middleboxes. Según el mismo estudio, se usaron como métodos de redireccionamiento el "spray mode" y el "trickle mode". En el primer método se producía el redireccionamiento de los usuarios de forma generalizada cuando hacían una petición de acceso a una página web. En el segundo, solo se producían los redireccionamientos al acceder a las webs CopticPope.org (web del Papa ortodoxo de la iglesia de Alexandria) y Babylon-X.com (web de pornografía).

6.3 Ransomware

El año 2017 fue el año del ransomware con ataques a nivel internacional devastadores y con pérdidas económicas inafrontables para muchas empresas. La finalidad de estos ataques consistía en obtener criptomonedas y para ello se procedió a cifrar toda la información de los dispositivos afectados por el ransomware y se solicitó un rescate para su devolución. El ransomware suele estar asociado a correos phishing que llevan adjunto el malware y por tanto es necesaria la intervención humana para su propagación, aunque esta forma de ataque está evolucionando hacia la autopropagación mediante gusanos que se replican y se van distribuyendo a lo largo de la red. Se muestran a continuación los ataques más relevantes a nivel internacional que han sucedido y que están relacionados con este malware.

- WannaCry: El 12 de mayo de 2017 se produce la mayor infección por ransomware vista hasta el momento. Según estadísticas de Kaspersky [103] afectó a 200.000 sistemas en más de 150 países y los más afectados fueron Rusia con un 33,64% de las empresas infectadas, Vietnam con un 12,45%, Ucrania e India con un 6,95%. Empresas multinacionales como Renault, Telefónica, Deutsche Banh, FedEx, Bengala Occidental, Hitachi e incluso servicios públicos como los hospitales de Reino Unido y el Ministerio Interior Ruso fueron afectados por el ataque.

  El vector de infección que se usó y que permitió que no se necesitase la intervención humana para su propagación fue el exploit EternalBlue. Este

exploit, aprovechaba la vulnerabilidad CVE-2017-0144 en la implementación del protocolo SMB versión 1 de Windows y valiéndose de ella instalaba un backdoor conocido como "DoublePulsar", que se utilizaba para inyectar código malicioso. Cuando sucedieron los ataques ya existía un parche creado por Windows y disponible para los sistemas operativos afectados, pero muchos usuarios y organizaciones no habían procedido a realizar las actualizaciones pertinentes y por tanto eran vulnerables a ataques.

A continuación, se muestra una imagen de la pantalla que veía el usuario una vez se había producido la infección en su dispositivo:

Figura 13:Rescate solicitado en la infección WannaCry

Después de ese primer ataque se produjeron ataques similares, debido a que las empresas seguían sin aplicar el parche ofrecido por Microsoft. Algunas de las organizaciones que se han visto afectadas por ataques posteriores han sido LG, los radares de tráfico de Australia y la empresa Boeing que se infectó en marzo de 2018.
Según las estadísticas de Kasperky Lab [103], el 65% de las empresas que fueron infectadas en 2017 perdieron gran parte de sus datos o incluso todos. Por otro lado, una de cada 6 empresas de las que pagaron el rescate no pudieron recuperar la información secuestrada.

- NotPetya [104], [105]: Este ataque fue enmascarado como un ataque ransomware similar a Petya, pero en realidad era un ataque wiper. La diferencia entre ransomware y wiper es que el primero puede restaurar las modificaciones en el sistema y recuperar los archivos cifrados una vez

pagado el rescate, mientras que el segundo no busca obtener un rescate económico, sino destruir todos los archivos mediante un borrado seguro y evitar la restauración del sistema. En el caso de NotPetya se pensó en un primer momento que era un ransomware porque pedía un rescate, pero en realidad era solo un señuelo, ya que lo que se quería era dañar los sistemas de información. A continuación, se muestra una imagen de lo que se veía en las pantallas de los dispositivos después de la infección:

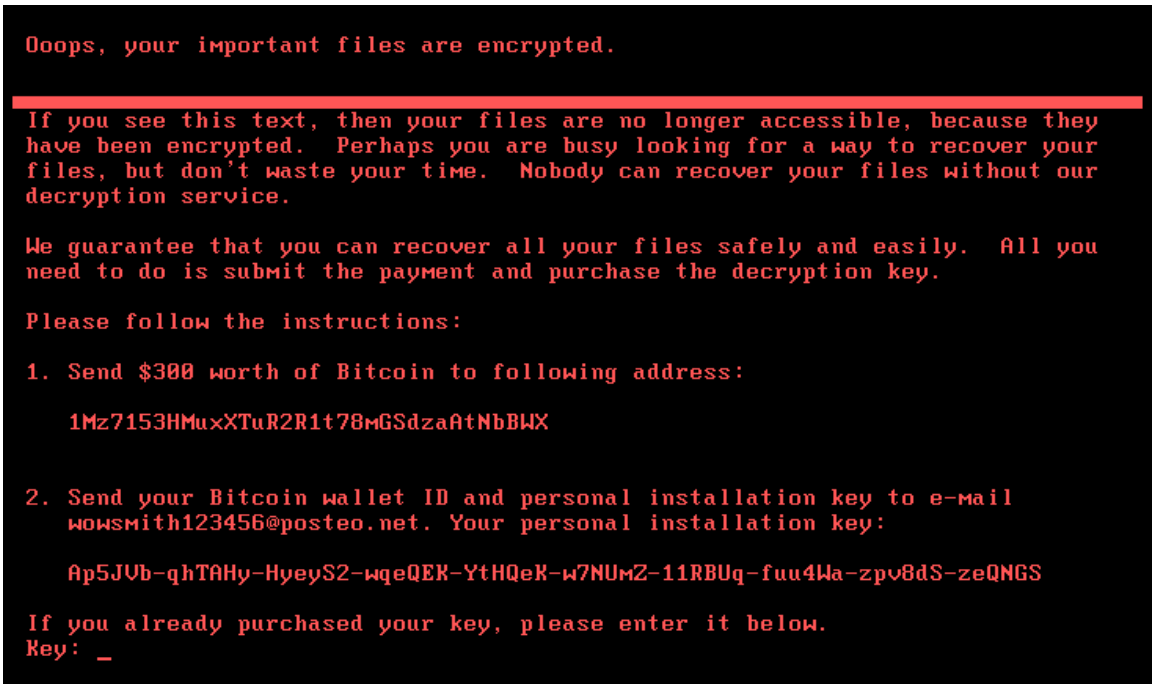


Figura 14: :Rescate solicitado en el ataque NotPetya [104]

El ataque se produjo en junio de 2017 y afectó a unas 2.000 organizaciones. El punto central del ataque fue Ucrania con un 60% de los dispositivos afectados y más concretamente MeDoc, que es una empresa que desarrolla software de aplicaciones contables. Según Roman Boyarchuk, que es el director del centro de ciberseguridad ucraniano, el ataque fue perpetrado por el gobierno ruso para dañar a Ucrania.
El vector de ataque que se uso es el mismo que el del ataque WannaCry y además se utilizó el exploit EternalBlue y otro similar llamado EternalRomance que usa el puerto TCP 445 o herramientas como psexec para poder ejecutar comandos de las máquinas a las que se conecta. El cifrado de los archivos se producía entre 10 y 60 minutos después de la infección, cuando se solicitaba al usuario que reiniciase el sistema y después del reinicio aparecía una pantalla similar al CHKDSK. Si no se apagaba el dispositivo cuando aparecía esa pantalla, quedaba totalmente inutilizado.

- KeyPass: Este Ransomware comenzó a distribuirse en agosto de 2018. Es similar a otros ransomware, pero tiene una nueva funcionalidad que permite personalizar los ataques. Según Kaspersky esta funcionalidad sería un indicador de que se pretenden realizar ataques manuales personalizados con este malware. Esta función esta oculta por defecto en

la interfaz, pero si se aprieta un botón específico del teclado se muestra y nos ofrece la posibilidad de personalizar los siguientes aspectos [106]:

- Clave de cifrado
- Nombre y texto de la nota de rescate
- ID de la víctima
- Extensión de los archivos cifrados
- Lista de direcciones excluidas del ataque

A continuación, se muestra una imagen de la interfaz gráfica obtenida de la web genbeta [107]:

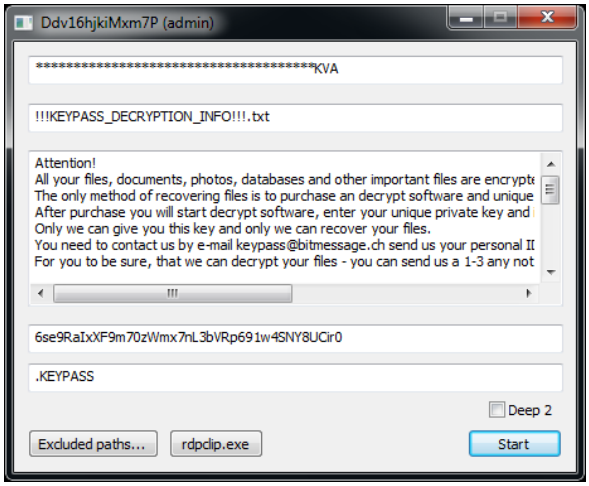


Figura 15: Interfaz KeyPass[107]

Este troyano hasta el momento ha producido infecciones en 20 países y se han visto afectados centenares de usuarios, sobre todo en países en vías de desarrollo. La propagación del ransomware ha sido a través de un troyano integrado en instaladores de software falsos.

- Ryuk [108]: En agosto de 2018 se produjeron ataques con el ransomware Ryuk a grandes empresas. Check point informó de que eran ataques de ransomware dirigidos para operar a pequeña escala y que la infección solo afectaba a recursos cruciales de las redes objetivo y que la distribución se realizaba de forma manual. Para poder realizar un ataque de esas características los hackers previamente debieron realizar un mapeo de redes y recopilar credenciales.
  La similitud con el ataque del ransomware HERMES al banco FEIB de Taiwán ha hecho creer a los expertos que este ataque fue llevado a cabo por Lazarous Group. Se tiene constancia de que el ataque ha afectado al menos a 3 multinacionales y que se han pagado hasta el momento 640.000$ de rescate para recuperar información secuestrada.

- Bad Rabbit [109]: Este ransomware atacó en octubre de 2017 y se centró en los medios de comunicación de Rusia y en el sector de transportes de Ucrania, aunque también se reportaron ataques en EE. UU, Alemania y Japón de menor magnitud. Para acceder a los sistemas informáticos se utilizó un instalador falso de Adobe Flash, una vez infectados los dispositivos se hacía un escaneado de red con el fin de obtener

credenciales para acceder a otros dispositivos escalando privilegios y procediendo al cifrado de archivos y a la solicitud de rescate.
Según Kaspersky Lab, Bad Rabbit podría tener relación con el wiper NotPetya dada la similitud del código de ambos.

6.4 Ciberespionaje y fugas de datos

Con la entrada en vigor del RGPD el ciberespionaje y las fugas de información se convierten en objetivo prioritario para los ciberdelincuentes en 2018.
El ciberespionaje pretende obtener información confidencial y privilegiada de gobiernos, empresas o entidades para venderlas por grandes sumas de dinero a competidores. A continuación, se muestra un caso que ha tenido repercusión global y que ha sucedido a finales de 2018.

- Operación OceanSalt [110]: La operación OceanSalt consistía en una operación de ciberespionaje que tenía como objetivos Corea del Sur, EE. UU y Canadá. Para realizar el espionaje se usaba un implante de reconocimiento de datos como el que uso el grupo chino paramilitar Comment Crew para atacar entre 2006 y 2010 a 141 empresas estadounidenses. Este implante, da control total a los ciberdelincuentes sobre todos los sistemas infectados y la red a la que están conectados dichos sistemas.
  Según McAffe, que fue la empresa de seguridad que descubrió la operación, el ataque se realizó en 5 fases y cada una de ellas se adaptó a un objetivo distinto. Las dos primeras fases dirigidas a Corea del Sur se realizaron por spearfishing, mediante documentos maliciosos que actuaban descargando el implante. Los documentos utilizados tenían relación con infraestructuras críticas de Corea. El tercer ataque, que también tenía como objetivo Corea del Sur, se realizó mediante un documento malicioso de Microsoft Word que contenía información falsa del Fondo de Cooperación Intercoreano. La cuarta y quinta fase iban dirigidas a EE. UU y Canadá por lo que se puede intuir que los atacantes pretendían realizar un ataque más amplio a escala global.

En cuanto a las fugas de datos, este 2018 se han producido numerosos ataques a organizaciones para obtener datos personales de sus usuarios. Se van a mostrar los casos que más importancia han tenido y que han afectado a más usuarios [111]:

- Facebook: Después del escándalo de Cambridge Analytica y la consiguiente multa de 565.000 € por violar la privacidad de sus usuarios, en septiembre de 2018 se produce una fuga de datos que afectó a 50.000 usuarios. Los atacantes aprovecharon una vulnerabilidad existente en la opción “ver cómo” y consiguieron robar los tokens de acceso para así poder acceder a las cuentas sin necesidad de contraseña. Aunque la vulnerabilidad ya ha sido solucionada se ha producido una pérdida de confianza en la red social, que ha hecho que muchos usuarios del mercado europeo se hayan dado de baja y que no se haya obtenido la cantidad de nuevas altas esperada.

- Jobandtalent: En junio de 2018 la empresa de búsqueda de empleo vio comprometida la seguridad de la información de los datos personales de sus 10.000.000 de usuarios. Los datos personales incluían email, nombre, apellidos y el hash de la contraseña. La organización procedió a resolver el fallo de seguridad, reiniciar las contraseñas de todos los usuarios y notificarles el ataque, y cumpliendo lo estipulado en el RGPD notificó a la Agencia Española de Protección de Datos el incidente para que se investigase.
- BritishAirways: La empresa británica sufrió un ataque mediante un malware que transfirió la información de 380.000 tarjetas de crédito de sus clientes a servidores ubicados en Rumania. Los datos se robaron utilizando una brecha de seguridad existente en la web y la aplicación móvil. La empresa comunicó el incidente y emitió un comunicado en el que se comprometía a compensar económicamente a sus clientes afectados.
- Ticketmaster [112]: La empresa de venta de entradas sufrió un ataque a un producto de soporte del cliente, gestionado por Inbenta Technologies, con la consiguiente filtración de los datos de 40.000 usuarios. El ataque solo afectó a Reino Unido y no se vieron comprometidas las bases de datos, pero mientras duró el incidente los ciberdelincuentes pudieron obtener los datos de los usuarios que estaban realizando compras en ticketmaster. Inbenta soluciono la vulnerabilidad y Ticketmaster notificó a sus usuarios para que cambiasen su contraseña y les ofreció asistencia para hacer seguimiento online de su identidad durante 12 meses.
- Equifax [113]: Este ataque sucedió entre mayo y julio de 2017 y dejo al descubierto la información de 143.000.000 de personas. La información a la que tuvieron acceso los atacantes fueron datos identificativos, datos de la seguridad social del usuario, tarjetas de crédito y domicilios. Este ataque destaca porque Equifax es una compañía que realiza informes crediticios en EE. UU y por tanto la mayoría de los afectados no sabían que sus datos personales estaban guardados en dicha organización.
- T-Mobile [114]: Esta empresa sufrió una filtración que afecto a 2.300.000 de usuarios de EE. UU. Los datos que se vieron comprometidos fueron nombre de usuario, números de teléfono, email y números y tipos de cuenta. Los ciberatacantes accedieron a los servidores mediante una API desde un país que no ha sido revelado y los desarrolladores de T-Mobile solucionaron la vulnerabilidad de forma inmediata una vez detectada. La compañía informó a sus clientes mediante correos electrónicos.

6.5 Ataques a Infraestructuras Críticas

En España entre enero y febrero de 2018 se duplicaron el número de incidentes que se habían producido en todo el 2014. Según los datos ofrecidos por el Ministerio del Interior [115] en enero se produjeron 53 incidentes y en febrero 72 y en todo el año 2014 se produjeron 63. Estos datos son alarmantes dado que las infraestructuras críticas deberían ser un objetivo prioritario en la seguridad de cualquier país. El problema de dichas infraestructuras, son sus sistemas industriales que están expuestos a numerosas vulnerabilidades que son aprovechadas por los atacantes. En los siguientes puntos se mostrarán ataques a infraestructuras críticas que han sido internacionalmente conocidos:

- Stuxnet [117]: Conocido como la primera ciberarma, tuvo como objetivo principal el ataque a la central nuclear de Natanz(Irán) en 2010. La organización de seguridad Langner lo analizo en profundidad y ofreció un informe de su funcionamiento [116] y de cómo consiguió evitar todos los sistemas de seguridad para introducirse en la central.
  Según el análisis de Langner la finalidad de Stuxnet era retrasar el programa nuclear que se estaba llevando a cabo en Irán. En la central nuclear se enriquecía uranio empobrecido mediante centrifugadoras, estas máquinas tenían debilidades en los controladores de las válvulas de presión y de los rotores que fueron aprovechadas por Stuxnet. A continuación, se muestra una imagen del esquema del ataque del informe que realizó Langner [116]:

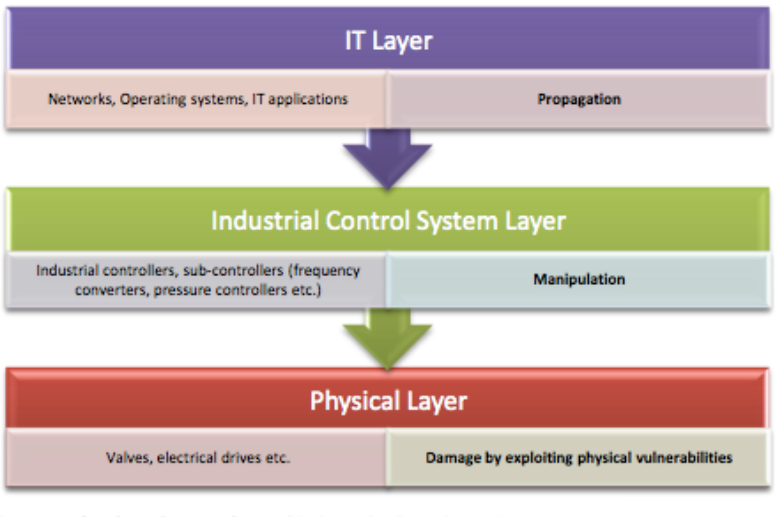


Figura 16: Esquema de ataque Stuxnet por Langner [116]

En el ataque se usaron dos versiones de Stuxnet. La primera, que se atribuye por Langner a expertos en sistemas industriales y programadores, tenía como objetivo los controladores Siemens S7-417 que se encargaban de controlar las válvulas y los sensores de presión de las centrifugadoras. Stuxnet se introdujo en los sistemas mediante un archivo falso de configuración de Siemens y en esos momentos era incapaz de autopropagarse. Una vez introducido en el sistema se hacía con el control y reemplazaba funciones del sistema de forma discreta para no alertar de la infección. Cuando se daban una serie de condiciones concretas, Stuxnet grababa 21 segundos de lecturas de los sensores y creaba un bucle en el que se reproducían repetidamente. Así cuando el sistema SCADA pedía las lecturas de los controladores no se observaba nada anómalo. Mientras las lecturas aparecían como correctas, lo que en realidad sucedía en la centrifugadora era que Stuxnet aumentaba la presión y evitaba que las válvulas se abriesen y aliviasen ese exceso de presión, provocando que el sistema trabajase al límite hasta que decidía restaurar las condiciones normales de funcionamiento. Esto provocaba un desgaste del sistema debido a un mal funcionamiento que no podía ser detectado por culpa de Stuxnet.

La versión 2 de Stuxnet según Langner habría sido realizada por algún grupo experto en ciberseguridad como la NSA. En este caso, el método de propagación no es directo como en el primer caso. Para llevarlo a cabo se usaron 4 vulnerabilidades de día cero mediante las cuales se infectaban dispositivos USB para poder propagar Stuxnet entre sistemas y además se usó una vulnerabilidad de Windows para así acceder a los ordenadores de la red privada. Para no levantar sospechas se habían incluido certificados digitales robados para que Windows detectase el archivo como legítimo. Se cree que el origen de entrada al sistema fue los ordenadores portátiles de contratistas externos y que a partir de ahí entraron en funcionamiento los métodos de propagación explicados anteriormente. En este caso, el ataque fue dirigido a los controladores Siemens S7-315 que se encargaban de controlar los rotores de las centrifugadoras. La función de Stuxnet consistía en que una vez al mes disminuía la velocidad de los rotores al mínimo y luego la elevaba hasta valores normales, provocando así que trabajasen a distintas velocidades críticas y acortando por tanto su vida útil. Como los rotores suelen trabajar a velocidad constante, las lecturas de SCADA no son directas de los controladores, así que no era necesario alterarlas, ya que se producían directamente de la memoria y allí estaba guardado un valor constante y adecuado a las condiciones de funcionamiento normal.
Stuxnet no poseía ningún interruptor de apagado y por tanto se podía ejecutar de forma autónoma. Una vez comprometidos todos los sistemas de la central, se expandió a través de contratistas hasta que empresas de seguridad lo detectaron y lo sacaron a la luz. A continuación, se muestra un esquema de las dos versiones de Stuxnet que descubrió Langner:

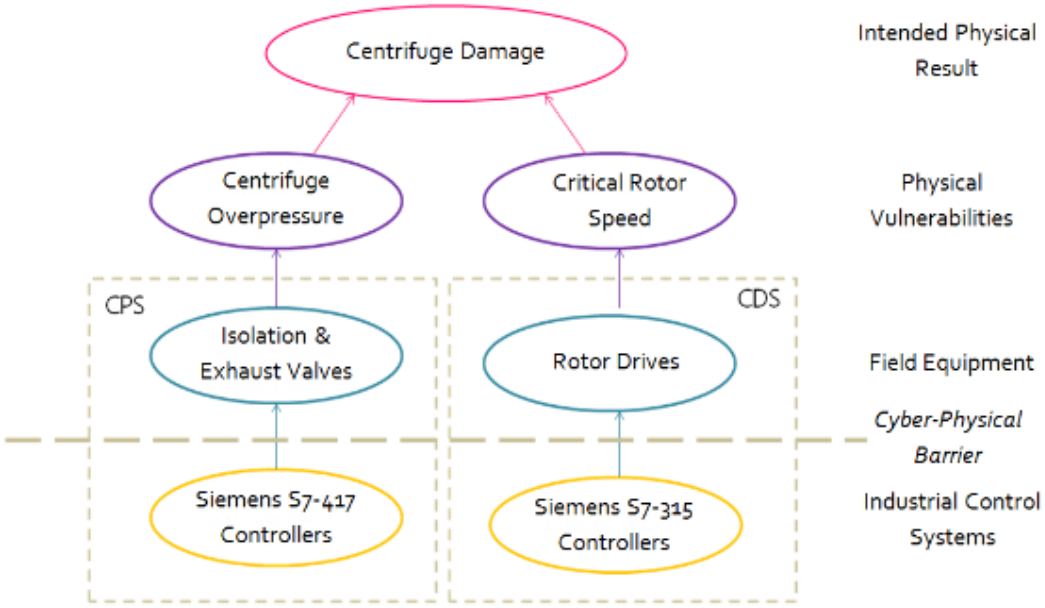


Figura 17: Esquema versiones de Stuxnet obtenida de Informe Langner[116]

Con este ataque se demostró lo vulnerables que son las infraestructuras críticas y fue un punto de inflexión para que las organizaciones de infraestructuras críticas comenzasen a preocuparse por la seguridad de sus sistemas e invirtiesen en realizar las mejoras necesarias.

- Industroyer: Según la empresa de seguridad Eset [118] este malware es del tipo modular y ofrece la posibilidad de personalizarlo, por tanto, se puede adaptar a cualquier tipo de infraestructura crítica. Este malware fue utilizado en 2016 para atacar la central eléctrica de Kiev y dejó sin suministro eléctrico a sus habitantes durante 1 hora. Eset cree que el esquema de funcionamiento del ataque en Kiev fue el siguiente:

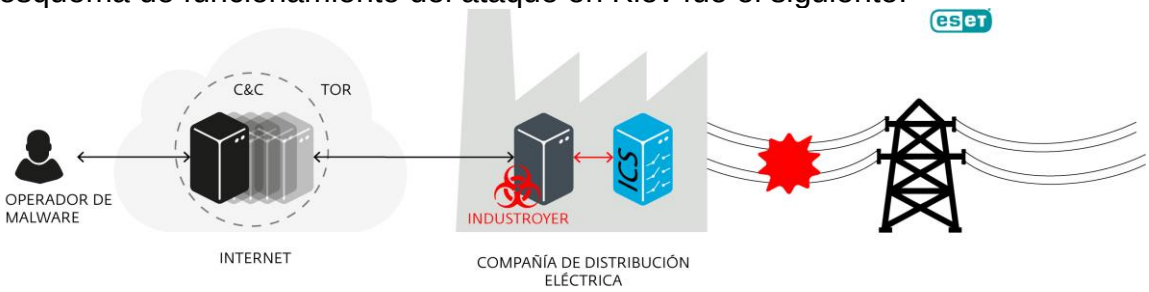


Figura 18: Ataque a central eléctrica de Kiev. Imagen obtenida de informe de Eset [118]

Según informe de Eset, industroyer era capaz de controlar los interruptores de una subestación eléctrica utilizando los protocolos de comunicación industrial. Se puede decir que industroyer utilizaba el mismo lenguaje para el que están diseñados los protocolos y por tanto no necesita buscar, ni explotar ninguna vulnerabilidad en los protocolos.
El análisis de la estructura y funcionalidad de industroyer, hecho por Eset, muestra que el componente central es un backdoor que instala y gestiona otros componentes y que se conecta a un servidor remoto desde el que los atacantes envían comandos y al que el sistema envía reportes. Además de esto, se incluyen cuatro payloads que atacan a protocolos concretos para poder así obtener el control total de los interruptores y disyuntores de la subestación. Por último, también posee funcionalidades adicionales para no ser detectado y borrar su rastro, y un backdoor adicional, que se camufla como un archivo .txt y que se utiliza si el backdoor principal es descubierto, además también tiene su propio escáner de puertos. A continuación, se muestra una imagen del informe de Eset donde se muestra el esquema de funcionamiento:

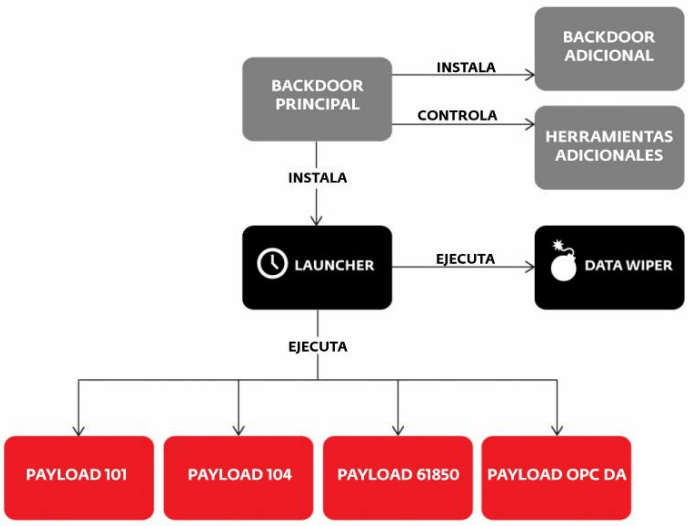


Figura 19: Esquema de industroyer de informe Eset[118]

Este malware al ser altamente personalizable puede adaptarse a todo tipo de infraestructuras críticas y se deberá seguir de cerca su evolución, para impedir o minimizar el riesgo de futuros ataques.

- BlackEnergy [119]: Estamos ante otro malware de tipo modular que fue responsable de los apagones provocados en Ucrania en las navidades de 2015. El ataque lo sufrieron varias empresas energéticas de Ucrania, aunque la parte más visible del ataque fue el apagón que dejó sin suministro eléctrico a 1.400.000 personas de la región Ivano-Frankovsk y que duró varias horas.
  Este tipo de malware pertenece a la familia de troyanos dropper y su finalidad en este ataque era infectar los ICS (Sistemas de control industrial) SCADA. El medio de ataque eran unos correos phishing que suplantaban la identidad del Parlamento ucraniano(RADA), los correos llevaban adjunto un fichero Excel con unas macros maliciosas. Una vez la víctima habilitaba las macros se descargaba BlackEnergy e inmediatamente se producía la descarga de otro troyano denominado KillDisk. La finalidad habitual de KillDisk es la de borrar archivos del sistema para evitar que pueda ser arrancado, pero en el caso del ataque de 2015 tenía funcionalidades adicionales para sabotear los sistemas industriales. Las funcionalidades consistían en finalizar los procesos komut.exe y sec_service.exe, que son procesos propios de algunos Sistemas de Control Industrial. Si el troyano detectaba esos procesos los finalizaba y además sobrescribía esos archivos ejecutables con datos aleatorios.
  Los ataques con BlackEnergy no solo han sido a infraestructuras críticas, ya que en 2015 también se reportaron ataques a medios de comunicación ucranianos.
- Triton: A finales de 2017 se produjo una parada y el cierre de las instalaciones en una planta industrial debida a un ataque con Triton [120], el nombre y la ubicación de la empresa no ha sido revelado pero el modus operandi del ataque sí que se ha dado a conocer. El malware se camufla como una aplicación legitima y una vez instalado, toma el control y modifica el comportamiento de sistemas instrumentados de seguridad para poder manipular los controladores que se encargan de detectar fallos en el sistema. En el caso del ataque a la planta industrial se modificó la programación de algunos controladores y entraron en modo a prueba de fallos provocando el apagado generalizado y el cierre de las instalaciones por seguridad.
  Según la empresa de seguridad FireEye, dadas las características del malware y del ataque, podría haber sido realizado por un Estado-nación con recursos elevados y con la intención de provocar daños a una infraestructura concreta.

6.6 Ataques DDoS y Botnets

La definición de botnets nos dice que son un grupo de ordenadores que han sido infectados y que un ciberdelincuente gestiona de forma remota para utilizarlos en ataques de denegación de servicio distribuido(DDoS) o en otros tipos de ataques que necesiten un gran poder computacional para ser llevados a

cabo. Este concepto se ha ampliado desde que ha aumentado el número de dispositivos IoT, ya que los ciberdelincuentes también están creando botnets de este tipo de dispositivos para lucrarse y realizar ataques masivos. A continuación, vamos a hablar de las botnets más conocidas a nivel internacional.

- Mirai: En octubre de 2016 se dio a conocer Mirai [122] después de que ocurriesen varios ataques de denegación de servicio distribuido(DDoS) relacionados con la empresa Dyn, que es proveedora de servicios DNS. Este ataque afecto a empresas como Paypal, Github, Spotify, Whatsapp, Twitter y muchas más que vieron como su servicio fue interrumpido temporalmente.
  Mirai estaba formada por dispositivos IoT como cámaras IP de vigilancia y routers que habían sido infectados por el malware Mirai, y afectó a 164 países y a 380.000 dispositivos. A continuación, se muestra el mapa de infección que presentó la empresa de seguridad Imperva [121]:

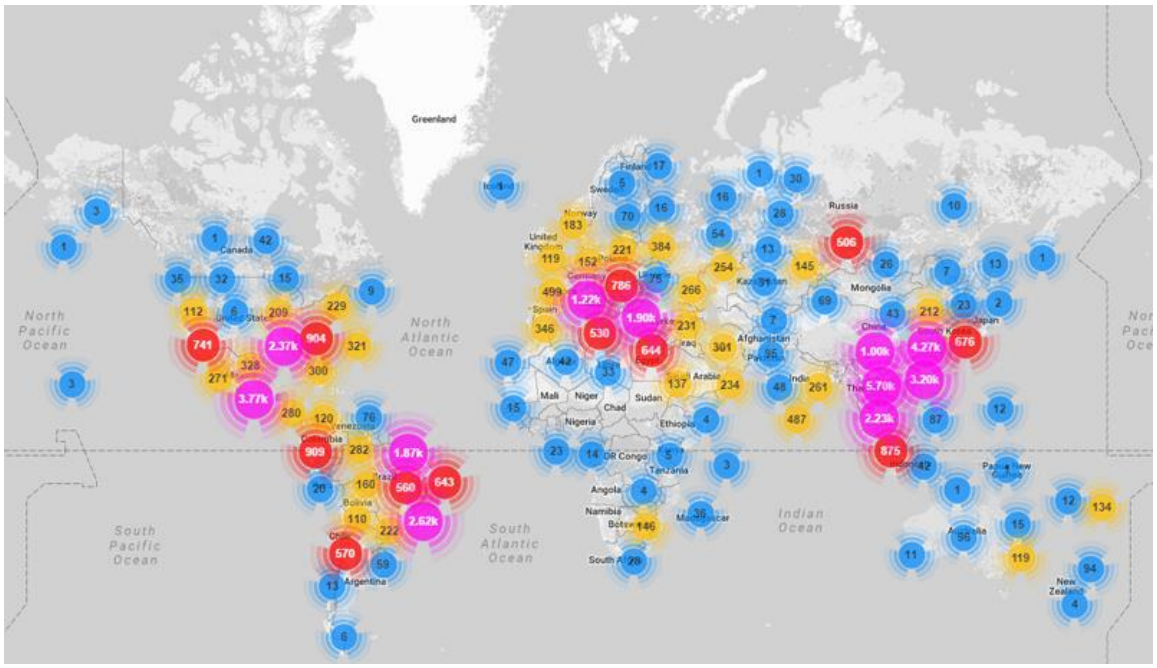


Figura 20: Mapa de Equipos infectados detectados por Imperva[121]

El método que utiliza Mirai para infectar los dispositivos es intentar robar las credenciales probando un listado de 62 contraseñas y usuarios que se suelen usar por defecto. Si consigue acceder al dispositivo lo añade a la botnet y posteriormente se comunica con el centro de comando y control(C&C) para recibir órdenes de las tareas que debe realizar y que pueden consistir en ataques de DDoS o en escanear un gran rango de IPs del puerto 48101/TCP para detectar otras posibles víctimas que infectar.
Las medidas de seguridad que propone el CERT-PY [122] para evitar infecciones son: cambiar contraseñas existentes por defecto, actualizar el firmware y aplicar parches a los dispositivos, realizar escaneos de puertos de los dispositivos y si no es necesario el acceso remoto, mantener cerrados dichos puertos y desactivar el Universal Plug and Play de los dispositivos.

- Satori [123]: La botnet IoT apareció a finales de 2017 y es una modificación de la botnet Mirai que aprovechaba una vulnerabilidad de día cero (CVE-2017-17215) existente en los routers Huawei HG532. Satori usó dos exploits que se conectaban con los puertos 37215 y 52869 para así infectar dispositivos móviles de forma masiva sin necesidad de utilizar un escáner para buscar posibles dispositivos víctimas. La botnet alcanzó los 700.000 nodos en cuatro días. Los dispositivos afectados se encontraban mayoritariamente en Egipto y en América latina. La botnet finalmente fue interrumpida por los proveedores de servicios de Internet (ISP) de las áreas afectadas al bloquear el tráfico del servidor de comando y control(C&C) mientras se parcheaban los routers afectados.
  Posteriormente se descubrió que una variante de Satori [124] tenía un tercer exploit y que aprovechaba una vulnerabilidad en el programa Claymore Miner para cambiar la dirección donde el minero recibe las criptomonedas por una dirección perteneciente al atacante. Si el minero no revisaba la configuración no era capaz de detectar el robo de las criptomonedas.

- Masuta [125]: Esta botnet está basada también en el código de Mirai, pero introduce un nuevo sistema de cifrado para iniciar los ataques. El dominio que se utiliza como C&C es Soluciones Nexius IO y eso hace pensar a los expertos, que esta botnet puede haber sido gestionada por Nexus Zeta, que son los responsables de Satori. En 2018 se estima que fueron infectados unas 2.400 IP.
  Se han identificado dos variantes distintas que se explican a continuación:
  - Masuta Botnet: Funciona de la misma forma que Mirai intentando penetrar en los dispositivos utilizando un listado de usuarios y contraseñas predeterminadas.
  - Pure Masuta: Está versión mejora las funcionalidades de Masuta, ya que aprovecha una vulnerabilidad existente en los routers más antiguos y que afecta al protocolo HNAP (Home Network Administration Protocol). Al atacar esta vulnerabilidad el malware es capaz de eludir la autenticación de seguridad.

  Una vez el atacante accede al dispositivo se ejecuta un script desde el centro de comando y control y se añade el dispositivo a la botnet. Masuta también puede utilizar ataques que aprovechan vulnerabilidades como la CVE-2014-8361 y la CVE-2017-17215 que afectan a diversos tipos de dispositivos.
  Se recomienda como en las botnets anteriores mantener los dispositivos actualizados y evitar las contraseñas débiles.

- Hidden'n Seek [126]: Heredera de Mirai, esta botnet IoT proporciona dos funcionalidades, la primera es utilizar el escáner del malware Mirai para atacar direcciones IP de forma aleatoria y explotar vulnerabilidades conocidas, y si así no se consigue el acceso se usa un listado de usuarios y contraseñas predeterminadas. La segunda funcionalidad que aporta es utilizar un protocolo P2P(peer-to-peer) mediante el cual filtra

archivos de los dispositivos infectados, distribuye archivos binarios, comparte archivos e incluso mina altcoins Monero.
Podemos analizar la evolución de Hidde'n Seek por fases. La primera es su detección en enero de 2018 por la empresa de seguridad Bitdefender y la comprobación de que más de 32.000 dispositivos estaban infectados. Unos meses después, la bonet explota dos nuevas vulnerabilidades que afectan a cámaras IP. En julio de 2018, la empresa 360 Netlab descubrió dos exploits adicionales y un programa para minado de criptomonedas que era usado por los dispositivos infectados. Finalmente, en octubre de 2018, Hidde'n Seek da el salto y consigue añadir una nueva funcionalidad que permite al malware explotar el puerto ADB (Android Debug Bridge) que se utiliza para programar y depurar aplicaciones en los dispositivo Android.
Como medidas de seguridad para evitar la infección se mantienen las explicadas para las botnets anteriores y se añade la de comprobar si el puerto ADB está activado en los dispositivos móviles y si es así proceder a desactivarlo.

6.7 Ciberatracos

Una de las últimas tendencias en ciberdelitos son los ciberatracos a entidades financieras. Este método proporciona a los atacantes grandes cantidades de dinero de forma rápida si se aprovechan de forma correcta las vulnerabilidades de los sistemas de las entidades bancarias. A continuación, se van a estudiar algunos de los ciberatracos globales que se han producido los últimos años.

- Bancos rusos [127]: En 2015 se produjo un ciberataque sin precedentes a entidades financiares rusas y que posteriormente se fue ampliando a bancos de otros países como Bielorrusia, Kazajistán, Azerbaiyán y Taiwán. Se calcula que los ciberdelincuentes se hicieron con 800 millones de euros.
  El método de infección era a través de unos correos phishing que suplantaban la identidad de las propias entidades y que tenían adjunto un fichero malware. Cuando se descargaba el fichero, se realizaba una escalada de privilegios para controlar el sistema, además también se tomaba el control de las cámaras IP para poder obtener contraseñas y capturar los movimientos realizados por los trabajadores. En algunos de los robos se hackearon los cajeros para que personas de la banda delictiva pudiesen obtener el dinero en efectivo a una hora programada, pero en general el dinero se blanqueaba usando criptomonedas.
  Los ciberatracadores actuaron entre 2013 y 2015 y desarrollaron tres tipos de virus para infectar los sistemas. El primero fue anunak que era el más básico de los tres, a medida que se aumentaba el nivel de seguridad de los bancos se empezó a utilizar Carberp que era más destructivo. Finalmente, se creó Cobalt Strike y se amplió el campo de actuación de los atracadores a otros países.
  En marzo de 2018 se detiene a Denis K., líder de la banda criminal de atracadores, en Alicante. Entre sus posesiones se descubre un nuevo virus que mejoraba las funcionalidades de los anteriores y que se iba a

utilizar para realizar atracos a gran escala. El dinero robado por Denis K. no se ha recuperado por el momento.

- Bancos Mexicanos [128]: El 27 de abril de 2018 se produjeron ciberatracos en varias entidades bancarias de México. Se estima que los atracadores obtuvieron entre 15 y 20 millones de $. Los ciberdelincuentes accedieron a los sistemas bancarios y realizaron transferencias a cuentas fantasmas, según informó Reuters. Se cree que los hackers fueron ayudados por trabajadores de las entidades. Se verificó en el Sistema de Pagos Electrónicos Interbancarios(SPEI), que opera el Banco de México, que se estaban realizando transferencias sospechosas y parece ser que el punto donde actuaron los atacantes estaba en los proveedores que tienen contratados los bancos para operar y enlazar las operaciones con el SPEI. Una vez detectado el ataque el Banco de México activo el plan de contingencia y las operaciones para realizar transferencias en el SPEI comenzaron a migrarse, provocando que el sistema se volviese más lento, pero evitando así que se robasen más fondos.

- Banco de Chile [129]: Este caso se produjo el 24 de mayo de 2018. Lo que inicialmente parecía un virus que estaba atacando los sistemas informáticos del banco, en realidad se trataba de un robo que sustrajo la cantidad de 10 millones de dólares de los fondos del propio banco.
  Swapq es el malware que infectó el sistema y se encargó del robo y hasta el día de la infección no se conocía su existencia. Como métodos de distracción utilizaron Killdisk o KillMBR para forzar la activación del plan de contingencia y que se dirigiesen los esfuerzos a la restauración de los sistemas informáticos. Mientras esto sucedía se producía un ataque a la red SWIFT aprovechando una vulnerabilidad de día cero y se realizaban transferencias a cuentas fantasma. Se barajan tres posibilidades distintas como método de la infección:
  - Correo phishing a empleados del banco con archivo adjunto infectado.
  - Empleados del banco actúan como infiltrados y ayudan a los atacantes.
  - Se realiza un hackeo del servidor Web y a través de ahí se accede a la red SWIFT.

  Aún se desconoce el método de infección, pero lo que está claro es que la red SWIFT tiene que ser actualizada y reparar las vulnerabilidades que posee para que las entidades financieras puedan operar de manera segura.

6.8 Posibles escenarios de ataques ciberterroristas

Cada día se producen avances en la tecnología que mejoran la vida diaria de las personas, pero estos dispositivos y sistemas suelen carecer de medidas de seguridad en sus primeras fases de incorporación al mercado. Los grupos de ciberterroristas, cuya finalidad es sembrar el caos y el miedo entre la población, pueden aprovechar estos dispositivos, que poseen tantas vulnerabilidades, para perpetrar incidentes de distintos tipos. A continuación, se muestran posibles

ataques que podrían suceder en un futuro y algunos que se han intentado llevar a cabo sin éxito.

- Ataques con drones: Los drones cada vez están más instaurados en las actividades cotidianas, pero aún no poseen las medidas adecuadas de protección contra ciberataques. En marzo de 2018, el grupo terrorista ISIS lanzó una amenaza [130] en la cual decía que se iba a realizar un ataque en el que drones lanzarían explosivos contra el público del festival Lollapalooza de Argentina. Una vez conocida la amenaza se enviaron 1.500 efectivos de la Unidad e Investigación Antiterrorista. Después de estudiarse la amenaza, se terminó descartando y finalmente se celebró el festival sin incidencias.
  Otro incidente relacionado con drones se produjo el 20 de diciembre de 2018 en el aeropuerto internacional de Gatwick [131]. Esa noche, aparecieron dos drones en una pista de aterrizaje. Se produjo un caos generalizado que obligó a suspender los vuelos durante 45 minutos. Algunos de los vuelos que tenían que aterrizar fueron desviados a aeropuertos próximos y unos 10.000 pasajeros se vieron afectados. Unas horas más tarde, cuando ya se operaba de forma normal, los drones volvieron a las pistas y se tuvieron que volver a paralizar las operaciones del aeropuerto. Aún se está investigando quien ha podido llevar acabó este ataque.
  Otro posible ataque con drones consistiría en hackear los sistemas que evitan que los drones choquen con el suelo y contra personas. Una vez desactivados estos sistemas se podrían llevar a cabo ataques en autopistas o grandes superficies para sembrar el caos.
- Ataques yihadistas: Los yihadistas utilizan Internet como medio de difusión propagandística de sus acciones y también para captar nuevos militantes. A parte de usar Internet como medio también han centrado sus objetivos en atacar los sistemas informáticos para producir daños a la población. En octubre de 2018 se revela un intento de ataque ciberterrorista a una infraestructura crítica del Reino Unido que sucedió entre 2015 y 2016[132]. El ataque tenía como objetivo atacar una depuradora y alterar los valores de la composición del agua para envenenar a la población. Finalmente, el ataque fue frustrado sin ninguna víctima.
  Otro caso de ciberterrorismo yihadista del que se tiene constancia sucedió durante los ataques terroristas que se llevaron a cabo en París en 2015 [132] y que se cobraron la vida de 130 personas. Los islamistas de Daesh lanzaron un ataque contra los sistemas de las fuerzas de Seguridad y Servicios de Información, en el que alteraron los relojes de los sistemas de información adelantándolos o atrasándolos. Este ataque provoco descoordinación y lentitud a la hora de gestionar los ataques terroristas que habían sucedido.
  Aunque las capacidades económicas de los grupos yihadistas no son muy grandes por el momento, no se descarta que cometan ciberatracos para aumentar su financiación y que comiencen a realizar operaciones de ciberterrorismo de mayor envergadura, que tendrían como objetivo infraestructuras críticas y ataques contra aviones.

- Ataques a torres de control y aviones: Se pueden producir ataques a los sistemas de las torres de control con el consiguiente choque de aviones. Para producir este tipo de ataque se usaría BlindRadars [133] que es una técnica que genera una interferencia electrónica en los radares de las torres de control y los sistemas de seguimiento. Si se comprometen estos sistemas los controladores aéreos serían incapaces de guiar a los aviones a las pistas de aterrizaje y podrían producirse impactos.

6.9 Conclusiones

A lo largo de este capítulo se han analizado distintos ciberataques que han sucedido en estos últimos años y que han tenido consecuencias importantes a nivel internacional. Las conclusiones a las que se ha llegado son las que se muestran a continuación:

- Las criptomonedas son un mercado en alza y cada vez se producen más ciberataques relacionados con ellas. Se deben guardar los fondos en carteras frías y evitar webs que puedan utilizar nuestros dispositivos para el minado de criptomonedas.
- Los ciberdelincuentes suelen usar las criptomonedas para blanquear el dinero o como forma de recibir los rescates, ya que ofrecen anonimización y son difíciles de rastrear.
- Aunque este año han disminuido las infecciones por ransomware, se ha de seguir de cerca la evolución de este tipo de malware, ya que sus ataques suelen ser masivos y dejan innumerables pérdidas económicas.
- Las fugas de datos cada vez tienen más relevancia debido a la entrada en vigor del RGPD. En 2018 se han producido numerosos ataques ya que las organizaciones no aplican las medidas de seguridad necesarias para proteger la información y los sistemas tienen vulnerabilidades que aprovechan los atacantes.
- Se deberían actualizar los sistemas de control industrial, ya que se encuentran obsoletos y los ciberdelincuentes pueden aprovechar sus vulnerabilidades para atacar infraestructuras críticas.
- Con el aumento de dispositivos IoT se ha producido un aumento de las redes zombies o botnets que tienen como objetivo provocar ataques DDoS o incluso el minado de criptomonedas.
- Se deben revisar los sistemas SWIFT de pagos e implementar mejoras para evitar los ciberatracos.
- Los gobiernos y las unidades especializadas en terrorismo deberán seguir de cerca las actividades de los grupos ciberterroristas y prepararse para luchar contra posibles ataques de ciberterrorismo.

7. Conclusiones y futuros trabajos

Las conclusiones a las que se ha llegado y los futuros trabajos que se pueden plantear después de realizar este Trabajo Final de Máster son los siguientes:

- Las empresas y organizaciones cada vez son más conscientes de la necesidad de invertir en ciberseguridad. Cada año aumenta el presupuesto dedicado a ello, aunque los ciberatacantes siguen buscando nuevas formas de sorprender en sus ataques y nuevos objetivos para atacar.
- Los países cada día son más conscientes de que deben existir normas, leyes y documentos para gestionar la ciberseguridad y los ciberdelitos. Algunos países como China, Rusia y EE. UU incluyen en sus legislaciones medidas que no respetan la privacidad de sus ciudadanos. Sin embargo, la Unión Europea intenta con sus reglamentos y normativas que la privacidad se respete y no haya brechas de seguridad que puedan violar la seguridad de la información de su población.
- Existen numerosos organismos internacionales que velan por la seguridad de los cibernautas. Estas entidades tienen distintas finalidades y muchas de ellas trabajan de forma conjunta para evitar que se produzcan ciberataques.
- Los países, estados, empresas y organizaciones no gubernamentales son conscientes de que hay que actuar de forma conjunta para abordar las ciberamenazas y para ellos suscriben acuerdos de cooperación y tratados internacionales.
- Las empresas deberían realizar revisiones de los sistemas de forma programada e instalar parches y actualizaciones para evitar que se produzcan ataques debidos a vulnerabilidades para las que existen soluciones.
- Con la creciente aparición de dispositivos nuevos aumentan los posibles escenarios para realizar ciberataques. Se deben extremar las medidas de seguridad y en caso de que se produzca un ataque aplicar planes de contingencia.
- Si se producen ataques internacionales debe existir cooperación entre los países para gestionar los incidentes de forma rápida y uniforme. Las autoridades de los países deberán trabajar unidas para investigar los ciberdelitos y castigar a los ciberdelincuentes.
- Se deberá seguir documentando todo el proceso relacionado con la ciberseguridad a nivel internacional para encontrar nuevas formas de cooperación internacional que ayuden a mejorar las existentes.
- La ciberseguridad evoluciona constantemente y los ciberataques plantean nuevos retos a los profesionales de la seguridad. Se seguirán de cerca las investigaciones de ciberataques para encontrar soluciones que se puedan implementar para intentar garantizar la seguridad de los usuarios y sus dispositivos.
- Se deberían facilitar guías con las medidas básicas que deben adoptar los usuarios para evitar que sus dispositivos y su información se vean

comprometidos. Invertir en formación y documentación a la larga disminuiría las pérdidas provocadas en los ciberataques.

- En un futuro se podría plantear una acción conjunta entre varios países para realizar formación sobre ciberseguridad destinada a usuarios y empresas.

8. Glosario

8.1 Glosario

- Altcoin: Es un acrónimo de alternative y coin. Se refiere a los tipos de monedas alternativas a Bitcoin
- Amenazas Persistentes Avanzadas: Según Wikipedia[22] la APT es un conjunto de procesos informáticos sigilosos y continuos, a menudo orquestados por humanos, dirigidos a penetrar la seguridad informática de una entidad específica.
- Botnet o redes zombies: son un grupo de ordenadores o dispositivos IoT que han sido infectados y que un ciberdelincuente gestiona de forma remota para utilizarlos en ataques de denegación de servicio(DDoS) o en otros tipos de ataques que necesiten un gran poder computacional para ser llevados a cabo.
- Ciberataque: Ataques que aprovechan vulnerabilidades existentes en los sistemas de información para dañarlos.
- Ciberamenaza: Según La UNE 71504[10] las ciberamenazas son la causa potencial de un incidente que puede causar daños a un sistema de información o una organización.
- Ciberatracos: Atracos que usan como medio los sistemas de información.
- Ciberdelitos: Son los delitos en los que se utilizan como medio o como fin las tecnologías de la información y las comunicaciones.
- Ciberespionaje: Según Wikipedia [134], el ciberespionaje es el acto o practica 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 malicioso incluyendo Troyanos y spyware.
- Ciberseguridad: La definición de ITU [8] nos dice que La ciberseguridad es 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 ciberentorno.
- Ciberterrorismo: La Jefatura de información de la Guardia Civil define el ciberterrorismo [89] como el empleo generalizado de las Tecnologías de la Información y la Comunicación(TIC), por parte de grupos terroristas u organizaciones afines, para la consecución de sus objetivos; utilizando Internet (sistemas informáticos y contenidos) como instrumento de comisión del delito o como acción del delito
- Criptomonedas: Son la alternativa digital a las monedas físicas. Lo más destacable de este sistema es su anonimización y difícil rastreo por lo que se suelen utilizar en el blanqueo de capitales.
- Cryptojacking: Técnicas utilizadas para minar criptomonedas sin el consentimiento del usuario.

- Exploit: Son unas instrucciones o un trozo de código que se utiliza para aprovechar una vulnerabilidad de un sistema de información y forzarlo para que se comporte de forma anómala.
- Infraestructuras críticas: Son infraestructuras que ayudan a mantener los servicios básicos para el funcionamiento de un país. Algunos ejemplos de este tipo de infraestructuras son las centrales eléctricas, depuradoras de agua, etc.
- Internet of Things: Se puede definir como la interrelación entre diferentes dispositivos que ayudan a realizar las tareas cotidianas y a crear hogares inteligentes.
- Phishing: Es un tipo de ataque de suplantación de identidad que puede llevarse a cabo mediante correos electrónicos, páginas web o aplicaciones que imitan a las originales y cuya finalidad es engañar al usuario.
- Ransomware: Es un tipo de malware cuya finalidad es cifrar la información de los sistemas infectados para que los ciberatacantes obtengan un rescate económico a cambio de facilitar la clave para poder desencriptar la información que ha sido cifrada.
- Spam o correo basura: Es el correo electrónico no solicitado y que se envía con objetivos publicitarios o comerciales de forma masiva.
- Troyano: Es un tipo de malware que cuando se ejecuta permite al atacante acceso remoto al sistema infectado.
- Vulnerabilidad: Son las debilidades de los activos de información que pueden ser aprovechadas para que las amenazas se materialicen.
- Wiper: Es un tipo de malware cuya finalidad es destruir los sistemas infectados sobrescribiendo los archivos con datos aleatorios y dejando los dispositivos inoperativos.

8.2 Acrónimos

- AEPD: Agencia Española de Protección de Datos
- APWG: Anti-Phishing Working Group
- ASC: Asociación de Seguridad Cibernética
- BCIT: Brigada Central de Investigación Tecnológica
- CaaS: Crime as a Service
- CAC: Administración del Ciberespacio de China
- CERT: Computer Emergency Response Team
- CNPIC: Centro Nacional de Infraestructuras y Ciberseguridad
- CSIRT: Computer security incident response teams
- CSN: Consejo de Seguridad Nacional
- C&C: Centro de Comando y Control
- DDoS: ataques de denegación de servicio distribuido
- EC3: Centro Europeo de Ciberdelincuencia
- ENISA: European Union Agency for Network and Information Security
- FIRST: Foro de Respuesta de Incidentes y de Equipos de Seguridad
- GDT: Grupo de Delitos Telemáticos
- ICANN: Corporación de Internet para la Asignación de Nombres y Números:
- INCIBE: Instituto Nacional de Ciberseguridad

- IoT: Internet of Things
- MCCD: Mando Conjunto de Ciberdefensa
- ONU: Organización de Naciones Unidas
- OTAN: Organización del Tratado del Atlántico Norte
- RGPD: Reglamento General de Protección de Datos
- TIC: Tecnologías de la Información y la Comunicación
- UE: Unión Europea
- USCC: United States Cyber Command

9. Bibliografía

- [1] https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019 visitada el 30/09/2018
- [2] http://perspectivas.deloitte.com/hubfs/Campanas/WannaCry/Deloitte-ES-informe-WannaCry.pdf visitada el 30/9/2018
- [3] https://www.cisco.com/c/es_es/products/security/security-reports.html#~stickynav=3 visitada el 03/10/2018
- [4] https://www.welivesecurity.com/wp-content/uploads/2017/12/Tendencias_2018_ESET.pdf visitada el 03/10/2018
- [5] https://www.xataka.com/legislacion-y-derechos/que-ha-pasado-con-facebook-del-caso-cambridge-analytica-al-resto-de-polemicas-mas-recientes visitada el 04/10/2018
- [6] https://www.pandasecurity.com/spain/mediacenter/seguridad/del-ransomware-al-cryptojacking/ visitada el 05/10/2018
- [7] http://www.isaca.org/knowledge-center/documents/glossary/cybersecurity_fundamentals_glossary.pdf visitada el 25/10/2018
- [8] https://www.itu.int/net/itunews/issues/2010/09/pdf/201009_20-es.pdf visitada el 28/10/2018
- [9] ISO 55001:2015 Certificación de sistemas de gestión de activos
- [10] UNE 71504 Metodología de análisis y gestión de riesgos para los sistemas de información.
- [11] https://www.incibe.es/protege-tu-empresa/blog/seguridad-desde-inicio visitada el 25/10/2018
- [12] Silvia Garre Gui, Antonio José Segovia Henares i Arsenio Tortajada Gallego; Introducció a la seguretat de la informació
- [13] https://ciberseguridad.blog/recomendaciones-de-ciberseguridad-en-iot/ visitada el 28/10/2018
- [14]https://www.elmundo.es/tecnologia/2013/12/05/529f1cf861fd3da3058b4589.html visitada el 28/10/2018
- [15] https://www.isaca.org/Journal/archives/2016/volume-4/Pages/mobile-computing-device-threats-vulnerabilities-and-risk-are-ubiquitous-spanish.aspx visitada el 28/10/2018
- [16] https://www.trendmicro.com/vinfo/us/security/research-and-analysis/predictions/2018 visitada el 28/10/2018 visitada el 28/10/2018
- [17] https://bitlifemedia.com/2018/07/ciberataques-a-la-alta-direccion-el-fraude-del-ceo/ visitada el 30/10/2018
- [18] http://www.cobdc.net/programarilliure/vulnerabilidades-seguridad/ visitada el 30/10/2018
- [19] https://www.coincrispy.com/2018/03/08/cryptojacking/ visitada el 30/10/2018
  [20] https://www.securityartwork.es/2014/05/30/ics-cert-vulnerabilidades-de-sistemas-de-control-industrial/ visitada el 30/10/2018

[21] http://www.redseguridad.com/sectores-tic/infraestructuras-criticas/proteccion-de-infraestructuras-criticas-contra-ciberataques visitada el 30/10/2018

- [22] https://www.welivesecurity.com/la-es/2014/08/29/guia-definitiva-entender-protegerte-apt/ visitada el 30/10/2018
- [23] http://www.dsn.gob.es/es/actualidad/sala-prensa/directiva-estados-unidos-para-coordinacion-ciberincidentes visitada el 01/11/2018
- [24] https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan visitada el 01/1/2018

[25] https://www.alainet.org/es/articulo/181849 visitada el 01/11/2018

[26]https://elpais.com/internacional/2017/03/28/estados_unidos/1490738196_593249.html visitada el 01/11/2018

- [27]https://www.elmundo.es/tecnologia/2018/02/05/5a78333ae2704e2f0f8b45b6.html visitada el 02/11/2018
- [28] https://www.eluniverso.com/noticias/2017/10/31/nota/6459805/rusia-quiere-acabar-conexiones-seguras-anonimas-internet visitada el 02/11/2018
- [29] https://www.csirtcv.gva.es/es/noticias/rusia-aprueba-un-documento-de-ciberseguridad.html visitada el 02/11/2018
- [30] https://www.telesurtv.net/news/rusia-onu-presenta-proyecto-internacional-ciberseguridad-20181026-0045.html visitada el 02/11/2018
- [31]http://www.ieee.es/en/Galerias/fichero/docs_informativos/2017/DIEEEI01-2017_CyberChina_DRM.pdf visitada el 02/11/2018
- [32]http://www.ieee.es/en/Galerias/fichero/docs_informativos/2017/DIEEEI01-2017_CyberChina_DRM.pdf visitada el 02/11/2018
- [33]https://www.welivesecurity.com/la-es/2016/07/22/nis-que-es-nueva-legislacion-seguridad/ visitada el 02/11/2018
- [34] https://www.consilium.europa.eu/es/policies/cyber-security/ visitada el 02/11/2018
- [35] https://advisera.com/eugdpracademy/es/knowledgebase/un-resumen-de-10-requisitos-clave-del-rgpd/ visitada el 02/11/2018
- [36] https://peritoit.com/2014/06/12/directiva-201340eu-relativa-a-los-ataques-contra-sistemas-de-informacion-y-el-peritaje-informatico/ visitada el 02/11/2018
- [37]https://www.boe.es/legislacion/codigos/codigo.php?id=173_Codigo_de_Derecho__de_la_Ciberseguridad visitada el 03/11/2018
- [38]https://es.wikipedia.org/wiki/Ley_de_Servicios_de_la_Sociedad_de_la_Informaci%C3%B3n visitada el 03/11/2018
- [39] http://noticias.juridicas.com/base_datos/Admin/l59-2003.t1.html visitada el 03/11/2018
- [40] https://www.ecixgroup.com/publicado-el-real-decreto-3812015-de-14-de-mayo-por-el-que-se-establecen-medidas-contra-el-trafico-no-permitido-y-el-trafico-irregular-con-fines-fraudulentos-en-comunicaciones-electronicas/ visitada el 03/11/2018
- [41] http://www.legaltoday.com/blogs/nuevas-tecnologias/blog-ecija-2-0/el-tjue-hace-tambalear-los-cimientos-de-la-ley-de-conservacion-de-datos visitada el 03/11/2018
- [42] https://www.first.org/about/mission visitada el 25/11/2018

- [43] https://www.first.org/about/organization/ visitada el 25/11/2018
- [44] https://es.wikipedia.org/wiki/OTAN#Estados_miembros visitada el 25/11/2018
- [45] https://www.ncia.nato.int/About/Pages/Organization.aspx visitada el 25/11/2018
- [46]https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2017_05/20170515_1705-factsheet-cyber-defence-en.pdf visitada el 25/11/2018
- [47] https://www.ncia.nato.int/Industry/Pages/NATO-Industry-Cyber-Partnership.aspx visitada el 25/11/2018
- [48]http://www.ieee.es/Galerias/fichero/docs_informativos/2012/DIEEEI16-2012_NatoRapidReactionTeam_MJCaro.pdf visitada el 25/11/2018
- [49] https://www.apwg.org/about-APWG/ visitada el 27/11/2018
- [50]https://es.wikipedia.org/wiki/Corporaci%C3%B3n_de_Internet_para_la_Asignaci%C3%B3n_de_Nombres_y_N%C3%BAmeros visitada el 27/11/2018
- [51]https://csirtamericas.org/ visitada el 28/11/2003
- [52] https://www.nsa.gov/what-we-do/cybersecurity/ visitada el 25/11/2008
- [53]https://www.cybercom.mil/Portals/56/Documents/USCYBERCOM%20Vision%20April%202018.pdf?ver=2018-06-14-152556-010 visitada el 27/11/2018
- [54] https://www.sei.cmu.edu/about/divisions/cert/index.cfm#cert-division-what-we-do visitada el 27/11/2018
- [55]https://es.wikipedia.org/wiki/Servicio_Federal_de_Supervisi%C3%B3n_de_las_Telecomunicaciones,_Tecnolog%C3%ADas_de_la_Informaci%C3%B3n_y_Medios_de_Comunicaci%C3%B3n visitada 27/11/2018
- [56] http://www.apcert.org/about/structure/index.html visitada 27/11/2018
- [57] http://www.apcert.org/about/mission/index.html visitada 28/11/2018
- [58] https://en.wikipedia.org/wiki/Cyberspace_Administration_of_China visitada 27/11/2018
- [59]https://www.elmundo.es/tecnologia/2016/03/30/56fbb74f22601db61c8b45c8.html visitada el 27/11/2018
- [60] https://europa.eu/european-union/about-eu/agencies/enisa_es visitada el 27/11/2018
- [61] http://cert.europa.eu/static/RFC2350/RFC2350.pdf visitada el 28/11/2018
- [62] http://www.seguridadinternacional.es/?q=es/content/europol-centros-de-especializaci%C3%B3n-ec3-ectc-emsc visitada el 28/11/2018
- [63] https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3 visitada el 28/11/2018
- [64]http://www.dsn.gob.es/sites/dsn/files/estrategia%20de%20ciberseguridad%20nacional.pdf visitada el 28/11/2018
- [65] http://www.dsn.gob.es/sistema-seguridad-nacional/comit%C3%A9s-especializados/consejo-nacional-ciberseguridad#collapseTwo visitada el 28/11/2018
- [66] https://www.incibe.es/que-es-incibe visitada el 29/11/2018
- [67] https://www.osi.es/es/quienes-somos visitada el 29/11/2018
- [68] https://www.is4k.es/sobre-nosotros visitada el 29/11/2018
- [69] https://www.incibe-cert.es/sobre-incibe-cert/que-es-incibe-cert visitada el 29/11/2018

- [70] https://www.incibe.es/protege-tu-empresa visitada el 30/11/2018
- [71] https://www.ccn-cert.cni.es/sobre-nosotros/mision-y-objetivos.html visitada el 30/11/2018
- [72] http://www.emad.mde.es/CIBERDEFENSA/cometidos/ visitada el 30/11/2018
- [73] http://www.cnpic.es/Presentacion/index.html visitada el 30/11/2018
- [74] https://www.aepd.es/agencia/transparencia/organigrama/index.html visitada el 30/11/2018
- [75] https://www.aepd.es/agencia/transparencia/common/plan-estrategico/plan-estrategico-AEPD.pdf visitada el 30/11/2018
- [76] https://www.gdt.guardiacivil.es/webgdt/la_unidad.php visitada el 30/11/2018
- [77] https://www.policia.es/org_central/judicial/udef/bit_actuaciones.html visitada el 30/11/2018
- [78] https://www.policia.es/org_central/judicial/udef/bit_funciones.html visitada el 30/11/2018
- [79] https://www.consilium.europa.eu/media/36096/nato_eu_final_eng.pdf visitada el 30/11/2018
- [80] http://www.dsn.gob.es/es/actualidad/sala-prensa/otan-ue-aumentan-cooperaci%C3%B3n-ciberseguridad visitada el 30/11/2018
- [81] https://www.eda.europa.eu/docs/default-source/documents/mou---eda-enisa-cert-eu-ec3---23-05-18.pdf visitada el 01/12/2018
- [82] https://www.diplomatie.gouv.fr/IMG/pdf/paris_call_text_-_en_cle06f918.pdf visitada el 01/12/2018
- [83] https://cybertechaccord.org/accord/ visitada el 01/12/2018
- [84] https://www.oas.org/juridico/english/cyb_pry_convenio.pdf visitada el 01/12/2018
- [85] https://www.welivesecurity.com/la-es/2017/12/06/convenio-budapest-beneficios-implicaciones-seguridad-informatica/ visitada el 01/12/2018
- [86] https://thediplomatinspain.com/2017/05/espana-firmara-con-india-su-septimo-acuerdo-sobre-ciberseguridad-desde-2015/ visitada el 01/12/2018
- [87]http://www.oas.org/es/centro_noticias/comunicado_prensa.asp?sCodigo=C-340/15 visitada el 01/12/2018
- [88]https://elpais.com/politica/2018/11/06/actualidad/1541514798_739002.html visitada el 01/12/2018
- [89]http://www.dintel.org/web/Eventos/CongresosEspana/Profesionales/2010/ponencias/hernandez.pdf visitada el 22/12/2018
- [90] https://vanguardia.com.mx/articulo/se-alian-tres-paises-de-europa-para-combatir-ciberterrorismo visitada el 22/12/2018
- [91] https://www.computerworld.es/archive/la-guardia-civil-se-prepara-contra-el-ciberterrorismo visitada el 22/12/2018
- [92] https://www.criptonoticias.com/seguridad/ataques-blockchains-mineria-encubierta-robos-casas-cambio-2018/ visitada el 22/12/2018
- [93] https://www.criptonoticias.com/colecciones/ataques-retencion-51-dos-meses-dificultades-criptomonedas/ visitada el 22/12/2018
- [94] https://www.crypto51.app/ visitada el 22/12/2018

- [95] https://www.criptonoticias.com/seguridad/aplicacion-falsa-de-localbitcoins-usada-para-robar-las-criptomonedas-de-sus-usuarios/ visitada el 22/12/2018
- [96] https://www.criptonoticias.com/seguridad/asociado-consensys-destaca-vulnerabilidades-carteras-frias/ visitada el 22/12/2018
- [97] https://es.gizmodo.com/hackers-invaden-los-servidores-en-la-nube-de-tesla-y-lo-1823157065 visitada el 22/12/2018
- [98] https://es.cointelegraph.com/news/the-ethics-of-cryptojacking-rampant-malware-or-ad-free-internet visitada el 22/12/2018
- [99] https://www.xataka.com/seguridad/cuidado-con-los-anuncios-de-youtube-algunos-aprovechan-tu-cpu-para-hacer-mineria-de-criptomonedas visitada el 22/12/2018
- [100] https://es.cointelegraph.com/news/hackers-delight-bitcoin-mining-comes-to-aviva-due-to-lack-of-passwords visitada el 22/12/2018
- [101] https://es.cointelegraph.com/news/telecom-egypt-covertly-redirecting-internet-users-to-crypto-mining-sites-report-says visitada el 22/12/2018
- [102] https://citizenlab.ca/2018/03/bad-traffic-sandvines-packetlogic-devices-deploy-government-spyware-turkey-syria/ visitada el 23/12/2018
- [103] https://latam.kaspersky.com/blog/a-un-ano-de-wannacry-el-exploit-eternalblue-sigue-siendo-un-vector-de-infeccion/12952/ visitada el 23/12/2018
- [104] https://www.eldiario.es/tecnologia/objetivo-ultimo-ciberataque-dinero_0_659684380.html visitada el 23/12/2018
- [105] https://www.xataka.com/seguridad/notpetya-asi-actua-el-nuevo-ransomware-que-esta-causando-el-caos-y-asi-puedes-detener-su-avance visitada el 23/12/2018
- [106] https://losvirus.es/hackers-emplean-el-ransomware-keypass-para-realizar-ataques-manuales/ visitada el 23/12/2018
- [107] https://www.genbeta.com/seguridad/descubierto-nuevo-ransomware-funciones-ocultas-que-permiten-personalizar-ataques visitada el 23/12/2018
- [108] https://www.checkpoint.com/es/press/2018/ryuk-la-ultima-amenaza-creada-por-profesionales-del-ransomware/ visitada el 23/12/2018
- [109] https://cnnespanol.cnn.com/2017/10/26/bad-rabbit-ataque-hackers-adobe-virus-ransomware-malware/ visitada el 23/12/2018
- [110]https://www.eleconomista.es/tecnologia/noticias/9463604/10/18/Operacion-Oceansalt-la-campana-de-ciberespionaje-que-usa-el-codigo-fuente-de-hackers-chinos.html visitada el 23/12/2018
- [111] https://computerhoy.com/noticias/tecnologia/2018-ano-fugas-datos-estos-han-sido-ataques-mas-sonados-313185 visitada el 24/12/2018
- [112] https://www.xataka.com/seguridad/ticketmaster-sufre-fallo-seguridad-que-compromete-datos-miles-usuarios visitada el 24/12/2018
- [113] https://www.univision.com/noticias/delitos-ciberneticos/un-ciberataque-a-la-gigante-medidora-de-credito-equifax-pudo-haber-afectado-a-143-millones-de-personas visitada el 24/12/2018
- [114] https://www.tekcrispy.com/2018/08/24/hackers-roban-datos-t-mobile/ visitada el 24/12/2018

- [115] https://cuadernosdeseguridad.com/2018/04/los-ciberataques-a-infraestructuras-criticas-se-duplican-en-los-dos-primeros-meses-del-ano/# visitada el 24/12/2018
- [116] https://www.langner.com/wp-content/uploads/2017/03/to-kill-a-centrifuge.pdf visitada el 24/12/2018
- [117] https://www.genbeta.com/seguridad/stuxnet-historia-del-primer-arma-de-la-ciberguerra visitada el 24/12/2018
- [118] https://www.welivesecurity.com/la-es/2017/06/12/industroyer-amenaza-control-industrial/ visitada el 25/12/2018
- [119] https://www.welivesecurity.com/la-es/2016/01/05/troyano-blackenergy-ataca-planta-energia-electrica-ucrania/ visitada el 25/12/2018
- [120] https://www.genbeta.com/seguridad/triton-un-malware-disenado-para-atacar-industrias-e-infraestructuras-criticas-ha-causado-el-cierre-de-una-planta visitada el 25/12/2018
- [121] https://www.incapsula.com/blog/malware-analysis-mirai-ddos-botnet.html visitada el 25/12/2018
- [122] https://www.cert.gov.py/index.php/noticias/botnet-mirai-y-otras-amenazas-dispositivos-conectados-internet-iot visitada el 25/12/2018
- [123] https://www.silicon.es/se-publico-codigo-utilizado-la-botnet-satori-iot-explotar-routers-huawei-2368286?inf_by=5bb10b99671db8a4608b496d visitada el 26/12/2018
- [124] https://www.redeszone.net/2018/01/17/una-nueva-variante-satori-botnet-ataca-plataformas-ethereum/ visitada el 26/12/2018
- [125] https://sensorstechforum.com/es/mirai-based-masuta-iot-botnet-worldwide-attack/ visitada el 26/12/2018
- [126] https://www.itdigitalsecurity.es/endpoint/2018/12/la-botnet-hide-n-seek-continua-creciendo-infectando-dispositivos-iot visitada el 27/12/2018
- [127]https://elpais.com/economia/2018/03/26/actualidad/1522056458_237222.html visitada el 28/12/2018
- [128]https://elpais.com/economia/2018/05/14/actualidad/1526325508_023221.html visitada el 28/12/2018
- [129] https://blog.segu-info.com.ar/2018/06/banco-de-chile-malware-para-distraer-y.html visitada el 28/12/2018
- [130] https://www.minutouno.com/notas/3066142-explosivos-drones-la-amenaza-isis-el-lollapalooza visitada el 28/12/2018
- [131] https://www.clarin.com/mundo/londres-suspenden-vuelos-aeropuerto-gatwick-drones-cerca-pista-miles-pasajeros-afectados_0_NzufiPUKT.html visitada el 28/12/2018
- [132] https://www.larazon.es/espana/el-estado-islamico-intento-hackear-una-depuradora-y-envenenar-el-agua-de-miles-de-personas-en-inglaterra-CH20148208 visitada el 28/12/2018
- [133] http://www.ieee.es/Galerias/fichero/docs_opinion/2015/DIEEEO09-2015_AmenazaCiberataques_Fco.Uruena.pdf visitada el 28/12/2018
- [134] https://es.wikipedia.org/wiki/Ciberespionaje visitada el 28/12/2018