Universidad de Buenos Aires
Facultades de Ciencias Económicas, Ciencias Exactas y Naturales e Ingeniería

Carrera de Especialización en Seguridad Informática

Trabajo Final

Línea de Investigación: Ciberseguridad

Análisis de los Ciberataques en las Infraestructuras Críticas de la Información y las Comunicaciones a nivel mundial dentro del periodo [2009 - 2019]

Autora: Ing. Andrea Vernaza Bedoya
Tutora: Mg. Marcia L. Maggiore

Año 2020
Cohorte 2012

DECLARACIÓN JURADA

Por medio de la presente, el autor manifiesta conocer y aceptar el Reglamento de Trabajos Finales Vigente (v. 8.7.3) y que se hace responsable que la totalidad de los contenidos del presente documento son originales y de su creación exclusiva, o bien pertenecen a terceros u otras fuentes, que han sido adecuadamente referenciados y cuya inclusión no infringe la legislación Nacional e Internacional de Propiedad Intelectual.

_____

FIRMADO

Andrea Vernaza Bedoya.

DNI 94.960.360

RESUMEN

Hoy en día, la ciberseguridad conforma uno de los puntos clave en las estrategias, programas y planes de Seguridad Nacional de muchos países. Es sabido que, desde el inicio de la historia de la civilización, se conocía de la existencia de cuatro elementos los cuales son Tierra, Agua, Fuego y Aire. En base a ello, los ejércitos se dividían en estos cuatro elementos para combatir durante las guerras de ese momento. A esos cuatro elementos se ha sumado un quinto elemento llamado Ciberespacio, donde las guerras ahora son virtuales y, por ende, se han desplazado desde las fronteras físicas hacia una esfera tecnológica y de las telecomunicaciones, manteniendo un campo de batalla constante por medio de las redes digitales. Debido a la extensa variedad de amenazas que concurren en el ciberespacio, los países están obligados a profundizar las medidas de protección de los activos informáticos, acción que quizá en otros tiempos no hubieran considerado realizar. Por ejemplo, reforzar tecnológicamente sus IC de manera de estar mejor preparados ante cualquier posible ciberataque protegiendo así a sus sectores/servicios críticos.

El presente trabajo pretende hacer una investigación y análisis sobre la presencia y ocurrencia de los ciberataques en las infraestructuras críticas a nivel mundial, evaluando las causas, tipos y consecuencias de los ciberataques, además de analizar la normativa aprobada, las estructuras creadas y la estrategia de ciberseguridad aplicada por cada país para la protección de los sectores críticos. Por otro lado, se plantea una investigación monográfica relevando información desde fuentes públicas y fidedignas con la intención de lograr en un solo documento la unificación de conceptos y que posteriormente sirva como material a utilizar por otras investigaciones en la materia.

En conclusión, se presenta un análisis investigativo en el cual se compila algunos de los tipos de ciberataques en las infraestructuras críticas, se expone las consecuencias obtenidas sobre cada ataque ocurrido durante los últimos 10 años y de esta forma poder plantear recomendaciónes sobre el correcto uso de un marco de trabajo de ciberseguridad y mantener los sistemas más protegidos ante cualquier potencial ataque.

Palabras Claves: ciberseguridad, infraestructuras críticas de la información, protección de la información, ciberataques.

TABLA DE CONTENIDOS

LISTA DE TABLAS

LISTA DE FIGURAS

PAG

AGRADECIMIENTOS

Agradezco primeramente a Dios, que siempre estuvo presente guiándome para sacar adelante los logros propuestos; a mis padres, porque gracias a su apoyo económico y emocional, además de su amor constante, pude lograr este tan importante desafío académico en mi carrera profesional; a mi tutora académica Mg. Marcia Maggiore gracias por el acompañamiento continuo que me brindó con la revisión y modificaciones para la mejora del documento; al Ingeniero y Dr. Juan Javier Sarell quien me dio un buen soporte académico con el seguimiento y corrección de mi trabajo y a una persona que jugó un rol muy importante durante todo este proceso el Dr. Pedro Hetch, ya que en el transcurso del posgrado fue un gran sostén para completar mi trabajo final, A los docentes y administrativos de la Universidad de Buenos Aires, quienes proporcionaron los medios necesarios para el continuo desarrollo de la Carrera de Especialización en Seguridad Informática. Y, por último, agradezco a todas aquellas personas que directa o indirectamente contribuyeron con sus esfuerzos para el logro de este objetivo.

NÓMINA DE ABREVIATURAS

ACSC *Australian Cyber Security Centre*

AFP *Australian Federal Police*

ARGUS *Sistema Europeo de Alerta Rápida*

ASIO *Australian Security Intelligence Organisation*

CCN *Centro Criptológico Nacional*

CERT *Computer Emergency Response Team*

CIAC *Critical Infrastructure Advisory Council*

CIP *Critical Information Protection*

CIIP *Critical Information Infrastructure Protection*

CIR *Critical Infrastructure Resilience*

CIWIN *Critical Infrastructure Warning Information Networking*

CNI *Centro Nacional de Inteligencia*

CNPI *Centre for the Protection of National Infrastructure*

CNPIC *Centro Nacional para la Protección de las Infraestructuras Críticas*

CSIRT *Computer Security Incident Response Team*

DoS *Denial of Service*

DDoS *Distributed Denial of Service*

EE. UU *Estados Unidos*

ENS *Esquema Nacional de Seguridad*

ENCS *Network for Cyber Security*

ENISA *European Union Agency for Network and Information Security*

EPCIP *European Programme for Critical Infrastructure Protection*

FERC *Federal Energy Regulatory Commission*

HTML *Hypertext Markup Language*

HTTP *Hypertext Transfer Protocol*

IC *Infraestructura Crítica*

ICE *Infraestructura Crítica Europea*

ICI *Infraestructura Crítica de la Información*

ICIC *Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad*

ICMP *Internet Control Messages Protocol*

IP *Internet Protocol*

ISACA *Systems Audit and Control Association*

ISO/IEC *International Organization for Standardization/International Electrotechnical Commission*

LPIC *Ley de Protección de Infraestructuras Críticas*

NCSC *Cyber Security Centre*

NERC *North American Electricity Reliability Corporation*

NIPP *National Infrastructure Protection Plan*

NIST *National Institute of Standards and Technology*

PEPIC *Programa Europeo de Protección de Infraestructuras Críticas*

PHP *Hypertext Preprocessor / Lenguaje de Programación Interpretado*

PIC *Protección de Infraestructura Crítica*

PLC *Programmable Logic Controller*

TCP/IP *Transmission Control Protocol / Internet Protocol*

TI *Tecnologías de Información*

TIC *Tecnología de información y comunicación*

TISN *Trusted Information Sharing Network*

UDP *User Datagram Protocol*

UK *United Kingdom*

UE *Unión Europea*

PARTE I - CUERPO INTRODUCTORIO

FUNDAMENTACIÓN DE LA INVESTIGACIÓN

INTRODUCCIÓN

Este trabajo de especialización está relacionado con el análisis de ciberataques en las ICI a nivel mundial dentro del periodo (2009 – 2019). Actualmente vivimos en un contexto interconectado y digitalizado, donde las TIC se han convertido en un foco importante dentro de la sociedad. En el mundo cibernético, existen múltiples formas de ejecutar ataques desde sitios remotos, en los cuales los agresores pueden ocultar su identidad y su ubicación, de acuerdo con la definición de ciberataque incluida en el Reglamento de Ciberseguridad de la UE 2019/796 del Consejo del 17 de mayo de 2019 [1] *"Los ciberataques son acciones que implican cualesquiera de los siguientes elementos, acceso a sistemas de información; intromisión en sistemas de información; intromisión en datos, o interceptación de datos o cuando dichas acciones no estén debidamente autorizadas por el propietario o por otro titular de derechos del sistema o de los datos, o de parte de los mismos, o no estén permitidas por el derecho de la Unión o de un Estado miembro."*

De allí nace la necesidad de estudiar más a fondo el papel que juega la ciberseguridad en los organismos gubernamentales y no-gubernamentales y los mecanismos de protección de la información confidencial, además de entender el gran impacto tecnológico, en mayor o menor magnitud, que tuvieron los ciberataques en las ICI.

Esta necesidad cobra mayor importancia debido a que las ICI son imprescindibles para el funcionamiento normal de los servicios básicos y los sistemas de producción de cualquier sociedad.

De tal manera que cualquier interrupción, ya sea debido a causas naturales o causas técnicas o a ataques deliberados, tendría graves consecuencias en los flujos de suministros vitales o en el funcionamiento de los servicios esenciales, además de suponer un riesgo de seguridad. Mediante un enfoque investigativo teórico del comportamiento de los ciberataques más relevantes ocurridos en los últimos diez años, se estudió la manera en la que fueron atacadas las ICI y sus consecuencias.

En base a lo anterior, se realizó un estudio investigativo sobre los tipos de ciberataques a las IC, se seleccionó los ciberataques más importantes ocurridos durante la década del 2009 - 2019 a nivel mundial, que marcaron un punto de partida en la historia de la ciberseguridad en los sistemas críticos de cada país; junto con la descripción de las consecuencias obtenidas después del ataque ocurrido.

A lo largo del desarrollo histórico, social y económico de las sociedades, han venido sucediendo ciberataques en las IC, muchos de ellos registrados a nivel mundial, que causaron desastres significativos, afectando muchos servicios básicos, vitales y necesarios para la supervivencia; existiendo casos que fueron relevantes y dejaron huella de las fallas en la protección de las ICI.

Identificación del problema

En la actualidad, las ICI de cada región se encuentran expuestas a sufrir algún tipo de ataque cibernético. Por ende, es importante profundizar en la investigación de estos, indagando cuáles fueron los más importantes a nivel mundial en los últimos diez años. De esta manera, se pretende tener un espectro mucho más amplio de la temática en cuestión y así presentar algunas conclusiones sobre la existencia de ciberataques que tienen como objetivo las IC, así como algunas recomendaciones para proteger adecuadamente los sectores críticos.

Existe una problemática adicional referente a que no todas las normativas que están relacionadas con la ciberseguridad no rigen adecuadamente en la región o no se encuentran formalizadas. Por esta razón, es fundamental definir cuáles son las normativas vigentes en las distintas regiones como América, Europa, África o Asia y de esta manera poder fortalecer en mayor dimensión el marco regulatorio en cuanto a la ciberseguridad de las IC de cada país.

Para lograr una correcta identificación del problema en cuestión es necesario plantearse nuevas interrogantes y así entender mejor cuál es el trasfondo de la investigación que se está realizando, ¿Cuáles fueron los ciberataques mundiales más importantes a las IC en los últimos diez años?, ¿Cuáles son las normativas vigentes relacionadas con la ciberseguridad en las IC en el mundo? o ¿Cuáles son las consecuencias de los ciberataques ocurridos en las IC a nivel mundial en el periodo 2009-2019?

Objetivo y Alcance

El objetivo de esta investigación es evaluar las consecuencias de los ciberataques en las IC del área de las TIC a nivel mundial en el período 2009-2019 y su alcance es de tipo teórico y documental, donde se profundiza en el análisis de las consecuencias de un ciberataque en una IC.

Si bien existen varias áreas estratégicas que conforman las IC, este trabajo solo se enfoca en una de ellas, la de las **Tecnologías de Información y Comunicación,** generalmente denominada **Infraestructura Crítica de la Información (ICI).** Las áreas restantes únicamente se citan y no fueron incluidas dentro de este proyecto. Ellas varían según el país de que se trate, pero, en general, se puede incluir las siguientes: Administración Pública, Salud, Seguridad Pública, Energía, Defensa, Servicios Financieros, Transporte, Tecnología de la Información y la Comunicación, Servicio de Agua, Espacio, Protección Civil, entre otras.

Por otra parte, se descartó profundizar en temas legales vinculados a la ciberseguridad y la protección de los datos; Cabe aclarar también que queda fuera del alcance de esta investigación, realizar un compendio de buenas prácticas, establecer políticas de ciberseguridad o controles definidos para proteger las IC, ya que estos tópicos se manejan de manera diferente en cada país, dependiendo de los recursos con los que cuente y las necesidades que tenga para proteger sus sectores y servicios críticos como también sus activos de información.

Estructura del Trabajo

El trabajo está compuesto por dos partes, el cuerpo introductorio y el cuerpo principal. El cuerpo introductorio comienza relatando la identificación, definición y planteamiento del problema, siguiendo con los objetivos a lograr, el alcance del proyecto y el enfoque de estudio junto con la justificación de la investigación a realizar. Continuando en la misma línea, se profundiza sobre el marco metodológico, el cual se separa en tres aspectos, a saber: el nivel de la investigación, el diseño de la investigación y las técnicas e instrumentos empleados durante la recolección de información. Finalmente, se muestra los resultados alcanzados y coincidentes con el objetivo planteado al inicio del trabajo. En el cuerpo principal del trabajo básicamente se desarrolla el estudio realizado y se encuentra dividido en cuatro capítulos: los dos primeros despliegan un marco teórico que presenta una vista completa de los conceptos correspondientes a la línea de investigación a desarrollar y los dos capítulos restantes exponen la parte más importante del trabajo, ya que muestran los resultados encontrados durante la investigación junto con las conclusiones realizadas. Finalmente, se encuentra el glosario, los anexos y la bibliografía correspondiente del trabajo.

Enfoque de Estudio

Esta investigación cuenta con un enfoque exploratorio, descriptivo y teórico [2] con un diseño de investigación documental, bibliográfica ya que se enfatizó en la recolección y análisis de información, tanto impresa como digitalizada. En referencia a esto, como aporte personal se desarrolló un análisis investigativo sobre los ciberataques en la ICI y se propuso una algunas recomendaciones sobre el uso adecuado de un marco de trabajo de Ciberseguridad con el fin de preservar las ICI.

Relevancia

Este proyecto investigativo es relevante en cuanto a poner de manifiesto el alto impacto que tienen los ciberataques sobre las IC y lo que están produciendo en los sistemas informáticos, industriales y de telecomunicaciones actuales. Es necesario profundizar en la recolección, el análisis y la evaluación de datos para poder encontrar las consecuencias que produjeron los ciberataques realizados en los últimos diez años a nivel mundial y de esta manera, poder tomar medidas necesarias a futuro para proteger dichos sistemas con el fin de minimizar sus ocurrencias.

Marco Metodológico

El marco metodológico empleado para realizar este trabajo incluye tres aspectos: *Nivel de investigación, Diseño de investigación y Técnicas de recolección de datos.*

El nivel de esta investigación es de tipo exploratorio ya que la temática elegida *“Ciberataques en las infraestructuras críticas de la información”* no ha sido muy estudiada ni desarrollada en trabajos académicos ni profesionales. Por esta razón, la información que sea recolectada e investigada servirá como base para próximas investigaciones en la materia y mediante el enfoque descriptivo-teórico se hace referencia a la información recopilada sobre las consecuencias de los ciberataques ocurridos en las IC.

El diseño de la investigación es documental porque se enfoca en la obtención de datos provenientes de materiales impresos y/o digitalizados, tales como revistas, libros, artículos, trabajos de grado y de tesis; obtenidos de páginas web y bases de datos académicas, entre otros. En el marco del diseño documental se utilizó específicamente la investigación bibliográfica para producir un informe narrativo de hallazgos con el fin de transmitir el estado del tema en la actualidad.

Las técnicas e instrumentos de recolección de datos que se emplearon para llevar a cabo el desarrollo del trabajo fue la búsqueda, recopilación y análisis de contenidos junto con la clasificación de fichas documentales relacionadas con la temática de investigación.

PARTE II - CUERPO PRINCIPAL

DESARROLLO DE LA INVESTIGACIÓN

CAPÍTULO 1. Ciberataques en las Infraestructuras Críticas

1.1. ¿Qué es un Ciberataque?

De acuerdo con la empresa Check Point Software Technologies ltd [3], un ciberataque es un asalto lanzado por ciberdelincuentes que usan una o más computadoras contra una o varias computadoras o redes, el cual puede inhabilitar maliciosamente las computadoras, robar datos o usar una computadora atacada como punto de partida para otros ataques.

De acuerdo con IBM [4], un ataque cibernético es la explotación deliberada de sistemas informáticos y redes que utilizan el *malware* o código maligno, para comprometer los datos o inhabilitar las operaciones. Los ataques cibernéticos permiten los delitos informáticos en el ciberespacio como el robo de información, el fraude y los esquemas de ransomware.

Según Cisco [5], el ciberataque es un intento malicioso y deliberado de un individuo o una organización, de violar el sistema de información de otro individuo u organización. Por lo general, el atacante busca algún tipo de beneficio al interrumpir la red de la víctima.

En base a las tres definiciones planteadas por grandes empresas tecnológicas, se toma como referencia la definición de IBM. [4]

1.2. ¿Qué es una Infraestructura Crítica?

Cada región a nivel mundial cuenta con una definición particular de este tipo de infraestructura dependiendo de los recursos y las necesidades con las que cuente y además difiriendo levemente en algunos criterios de criticidad de cada estructura.

Es importante saber que la seguridad nacional[1] de cada país tiene el deber de proteger dichas infraestructuras que resultan esenciales y vitales para la preservación de los sectores y/o servicios críticos de una sociedad. Su interrupción tendría graves consecuencias dentro de un territorio o de un país específico. A continuación, se presenta de manera gráfica las áreas estratégicas, entre otras, consideradas IC en los diferentes países.

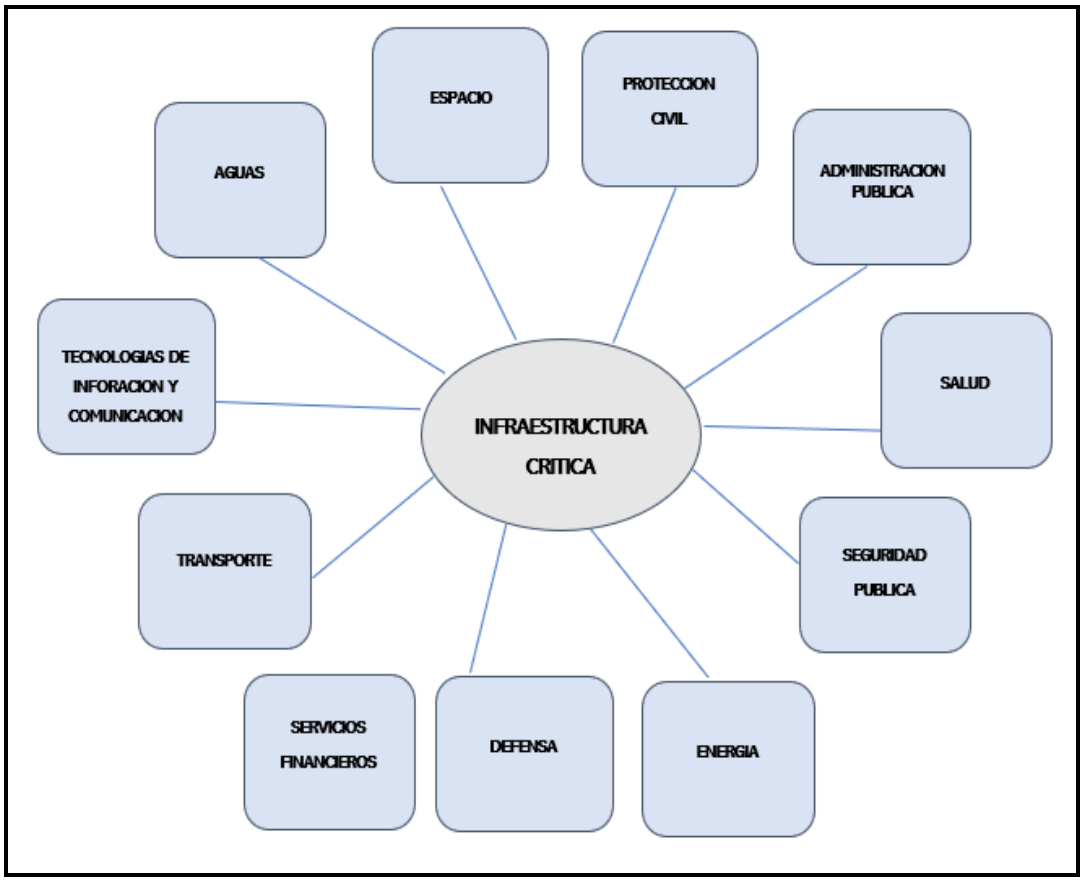


Figura N° 1 – Diagrama de clasificación de Infraestructuras críticas

Fuente: Elaboración Propia

En la siguiente tabla se realiza un breve resumen con las definiciones nacionales de IC en algunos de los países que han sido víctima de ciberataques en sus sectores críticos y han tenido que avanzar con mayor celeridad en la implementación de mecanismos de protección para estas infraestructuras.

[1] **Seguridad Nacional**: se refiere a la noción de relativa estabilidad, calma o predictibilidad que se supone beneficiosa para el desarrollo de un país; así como a los recursos y estrategias para conseguirla (principalmente a través de la defensa nacional).

PAIS	DEFINICION
Australia	Son aquellas instalaciones físicas, cadenas de suministro, tecnologías de la información y redes de comunicación, que, si se destruyen, se degradan o dejan de estar disponibles por un periodo de tiempo prolongado tendrán un impacto significativo en el bienestar social o económico de la nación, o afectara la capacidad del país para llevar a cabo la defensa nacional y garantizar la seguridad nacional. [6]
Canadá	Son procesos, sistemas, instalaciones, tecnologías, redes, activos y servicios esenciales para la salud, la seguridad y el bienestar económico de los ciudadanos como también para el funcionamiento efectivo del gobierno. La IC puede estar interconectada, puede ser independiente o ser interdependiente dentro y a través de las provincias, los territorios y las fronteras nacionales. Las interrupciones de la IC podrían ocasionar pérdidas catastróficas de vidas humanas, generar efectos económicos adversos y daños significativos a la confianza del público. [7]
Reino Unido	Son aquellas instalaciones, sistemas, sitios, información, personas, redes y procesos, necesarios para que un país funcione y de los cuales depende la vida diaria. [8]
Estados Unidos	Son los sistemas y activos físicos o virtuales con los que cuenta el país, dado que su incapacidad o destrucción de tales activos tendrían un impacto debilitante en la seguridad física y la seguridad económica nacional. [9]

PAIS	DEFINICION
Europa	Las Infraestructura Críticas son aquellas instalaciones, redes, servicios y equipos físicos y de tecnología de la información cuya interrupción o destrucción tendría un impacto mayor en la salud, la seguridad o el bienestar económico de los ciudadanos o en el eficaz funcionamiento de las instituciones del Estado y de las Administraciones Públicas. [10]
España	Son aquellas instalaciones que, por su actividad, resultan esenciales para el funcionamiento de un país. Su relevancia es tal, que incluso cuentan con una ley propia para garantizar que tanto operadores públicos como privados apliquen los máximos estándares de seguridad para la protección de IC. [11]
Estonia	Es un activo, sistema o parte del mismo, que es esencial para el mantenimiento de funciones sociales vitales y la salud, seguridad, bienestar económico o social de las personas y cuya interrupción o destrucción tendría un impacto significativo en una nación como resultado de la falta de mantenimiento de esas funciones. [12]

Tabla N° 1: Definición Nacional de una Infraestructura Critica en cada país
Fuente: Elaboración Propia

Concluyendo que todas las definiciones presentadas son parecidas y tienen el mismo objetivo, se puede unificar el concepto de una IC de la siguiente manera:

Una Infraestructura critica es aquella instalación, servicio y/o sistema de información que es tan esencial para las naciones que su interrupción o destrucción tendría un impacto negativo elevado en la seguridad nacional, la economía nacional, la salud pública, la seguridad o en las funciones de gobierno.

1.3. Tipos de Infraestructuras Críticas

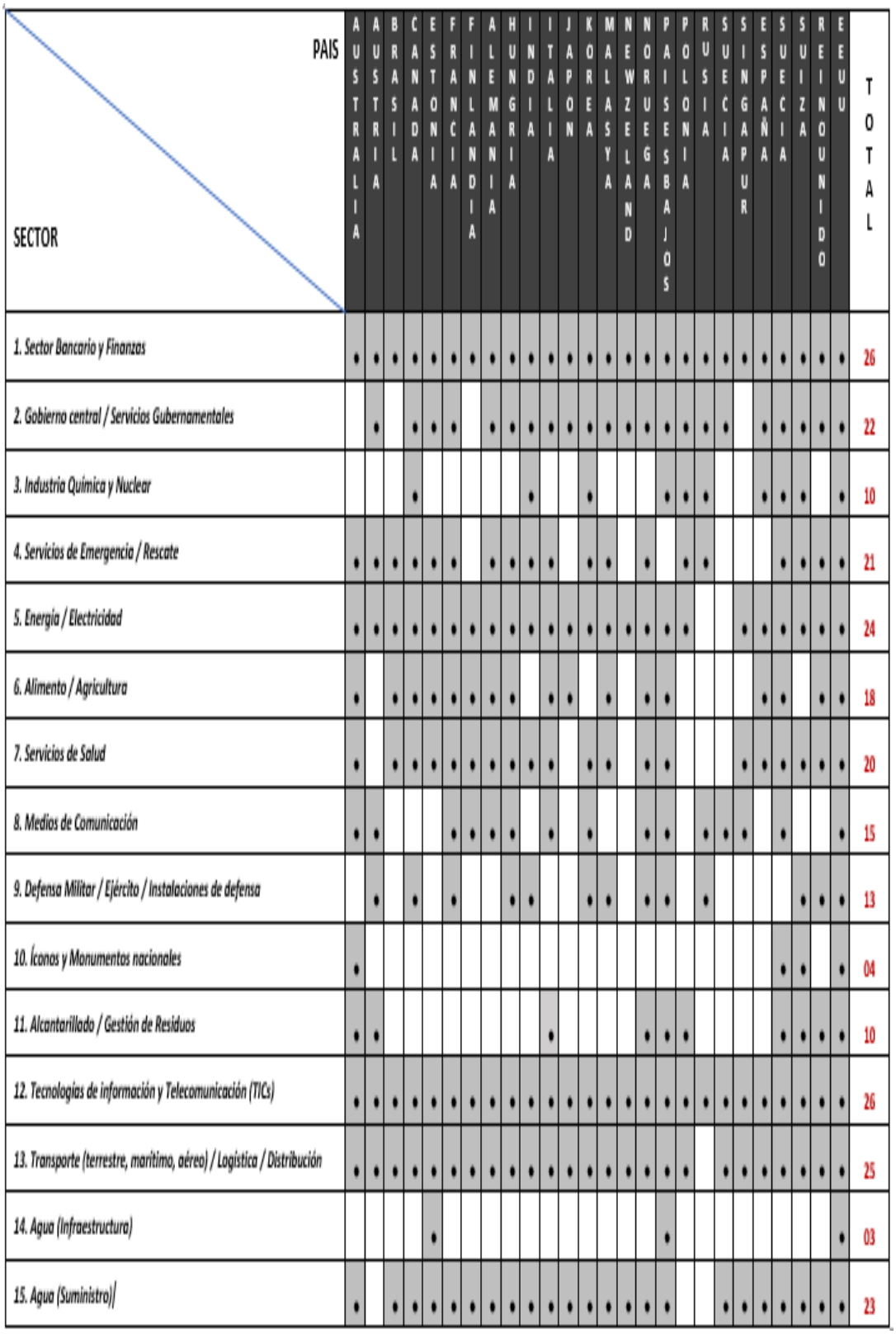
En cada región se pueden encontrar diversas cantidades de IC que son esenciales para el funcionamiento de una sociedad. Por ejemplo, en los EE.UU [13], de acuerdo con *Homeland Security*[2] cuenta con dieciséis sectores de IC cuyos activos, sistemas y redes físicas o virtuales, se consideran tan vitales para el país que su incapacidad o destrucción tendrían un efecto debilitante en la seguridad económica nacional, la salud o seguridad pública nacional, o cualquier combinación de estos[3]. En cuanto al Reino Unido [14], hay trece sectores de IC, cada uno de ellos tiene uno o más departamentos principales del gobierno responsable de su desempeño y de asegurar la protección de sus activos críticos. En lo que respecta a España [15], existen diez sectores de IC, los cuales se encargan de proteger los sectores críticos y estrategias de todo el país; continuando así, con los demás países, algunos tienen más que otros, pero necesariamente deben contar con las infraestructuras esenciales que hacen que un estado funcione correctamente con todos sus sectores y servicios críticos.

De acuerdo con el *Manual Internacional CIIP Handbook 2008/2009*[4], se muestra en la siguiente grafica un resumen de sectores y subsectores. Es importante tener en cuenta que, durante la investigación, se corroboró si los datos encontrados en el Manual CIIP del año 2009 fueron actualizados o permanecían iguales.

[2] **Homeland Security:** Departamento de Seguridad Nacional de los Estados Unidos (DHS) es una agencia federal diseñada para proteger a los Estados Unidos contra las amenazas. Sus amplias funciones incluyen seguridad de la aviación, control de fronteras, respuesta a emergencias y ciberseguridad, su función es prevenir el terrorismo y mejorar la seguridad. Asegure y administre las fronteras de Estados Unidos

[3] **Ver Anexo 1 -** Información adicional - Infraestructuras Criticas en Estados Unidos

[4] **Manual internacional CIIP 2008/2009:** El Manual CIIP se enfoca en los esfuerzos gubernamentales nacionales para proteger la infraestructura crítica de información (CII). El propósito general del manual es proporcionar una visión general de las prácticas de protección de CII en una gama cada vez más amplia de países



SECTOR \ PAIS	AUSTRALIA	AUSTRIA	BRASIL	CANADA	ESTONIA	FRANCIA	FINLANDIA	ALEMANIA	HUNGRIA	INDIA	ITALIA	JAPON	KOREA	MALASYA	NEWZEELAND	NORUEGA	PAISESBAJOS	POLONIA	RUSIA	SUECIA	SINGAPUR	ESPAÑA	SUECIA	SUIZA	REINOUNIDO	EEUU	TOTAL
1. Sector Bancario y Finanzas	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	26
2. Gobierno central / Servicios Gubernamentales		•		•	•	•		•	•	•	•	•	•	•	•	•	•	•	•	•		•	•	•	•	•	22
3. Industria Química y Nuclear				•						•			•				•	•	•			•	•	•		•	10
4. Servicios de Emergencia / Rescate	•	•	•	•	•	•		•	•	•	•		•	•		•		•	•				•	•	•	•	21
5. Energía / Electricidad	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•			•	•	•	•	•	•	24
6. Alimento / Agricultura	•		•	•	•	•	•	•	•		•	•		•		•	•					•	•		•	•	18
7. Servicios de Salud	•		•	•	•	•	•	•	•	•	•		•	•		•	•				•	•	•	•	•	•	20
8. Medios de Comunicación	•	•				•	•	•	•		•		•			•	•		•	•	•		•			•	15
9. Defensa Militar / Ejército / Instalaciones de defensa		•		•		•			•	•			•	•		•	•		•					•	•	•	13
10. Íconos y Monumentos nacionales	•																						•	•		•	04
11. Alcantarillado / Gestión de Residuos	•	•									•					•	•	•					•	•	•	•	10
12. Tecnologías de información y Telecomunicación (TICs)	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	26
13. Transporte (terrestre, marítimo, aéreo) / Logística / Distribución	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•	•		•	•	•	•	•	•	•	25
14. Agua (infraestructura)					•												•									•	03
15. Agua (Suministro)/	•		•	•	•	•	•	•	•	•	•	•	•	•	•	•	•			•	•	•	•	•	•	•	23

Figura N° 2: Clasificación por Sector/País –
Cantidad de Infraestructuras Críticas por sector [16]

1.4. Infraestructuras Críticas de la información

Como se expresó anteriormente, las infraestructuras críticas están subdividas en áreas estratégicas o sectores críticos que deben ser adecuadamente preservados por entidades públicas y/o privadas. Continuando con la misma línea de desarrollo, a continuación, se incluye, un breve resumen con las definiciones de ICI en algunos países con estructuras tecnológicas y de telecomunicaciones.

PAÍS	DEFINICIÓN
Estados Unidos	Es cualquier sistema de información físico o virtual que controla, procesa, transmite, recibe o almacena información electrónica en cualquier forma que incluya datos, voz o video y es vital que estas infraestructuras tengan un correcto funcionamiento ya que la incapacidad o destrucción de tales sistemas tendría un impacto debilitante en la seguridad Nacional, la seguridad económica y la seguridad pública. [17]
Uruguay	Son los activos de información crítica con los que cuenta el estado para garantizar y mantener el adecuado funcionamiento de los servicios esenciales para la operación del gobierno y la economía del país. [18]
China	La infraestructura de información clave nacional se refiere a las instalaciones de información y telecomunicación que se encuentran relacionadas con la seguridad y la economía Nacional como el sustento de las personas. Una vez que los datos se filtran, se dañan o pierden su función, pueden poner en peligro la seguridad nacional y los intereses públicos, incluyendo, entre otros, las comunicaciones públicas, los servicios de transmisión de radio y televisión, etc. [19]

PAÍS	DEFINICIÓN
Estonia	Es una red y un sistema de información cuya operación, confiabilidad y seguridad son críticas para la operación del país. [20]
Reino Unido	Es cualquier sistema de TI que soporta activos y servicios clave dentro de la Infraestructura nacional. [21]
India	Son aquellas instalaciones, sistemas o funciones cuya incapacidad o destrucción causaría un impacto debilitante en la seguridad nacional, la gobernanza, la economía y el bienestar social de una nación**.** [22]
España	La ley española de PIC no hace ningún tipo de distinción entre una IC y una ICI. Esta ley establece el concepto de un enfoque de seguridad integral que une la seguridad física y cibernética es una sola estrategia. De acuerdo al plan nacional de la PIC son aquellas instalaciones, redes, servicios y equipos físicos y de tecnología de la información cuya interrupción o destrucción tendría un gran impacto en la salud, la seguridad o el bienestar económico de los ciudadanos. [23]
Kosovo	Son las TIC que se consideran esenciales para la operación de un país ya sean las telecomunicaciones, las computadoras / software, Internet, satélites, etc. [24]

Tabla N° 2: Definición nacional de Infraestructura Crítica de la Información en c/país.

Fuente: Elaboración Propia

1.5. Ciberataque en una Infraestructura Crítica

La red es la puerta de entrada elegida por los ciberdelincuentes, quienes buscan métodos de entrada a la red con la finalidad de llevar a cabo un ataque cibernético. Uno de ellos es usar algunas técnicas de acceso a los sistemas y a la red buscando vulnerabilidades en los equipos o introduciendo algún tipo de *malware* a los sistemas, con el objetivo de tomar el control de la IC, de algún sector o área estratégica.

1.6. Casos más relevantes de los ciberataques ocurridos en los últimos diez años

PAÍS	CIBERATAQUE	AÑO	DESCRIPCIÓN
Estonia	Ciberataque de DDoS [5]	**2007**	La relocalización de una estatua de bronce que representaba a un soldado ruso en Tallin (Estonia) generó una confrontación nacionalista entre Rusia y Estonia. Esto conllevó a masivas protestas, tanto en Tallin como en la sede de Embajada de Estonia en Moscú, trasladándose este escenario de confrontación al mundo digital a través de las acciones desplegadas por hacktivistas. Los ciberataques hicieron que temporalmente se bajaran sitios web y redes de tecnología de instituciones estatales del despacho del presidente, el parlamento y la policía e igualmente se presentaron ataques masivos a bancos y medios de comunicación (prensa y televisión).[6]

[5] Es importante tener en cuenta que este ciberataque no entra dentro del rango de fechas a estudiar en la investigación, pero fue un ataque cibernético que tuvo un alto impacto dentro del país el cual afecto los sectores y servicios críticos dentro de Estonia

[6] **Ver Anexo 2** - Información adicional - Ciberataque de DDoS a Estonia

PAÍS	CIBERATAQUE	AÑO	DESCRIPCIÓN
Irán	Primer ataque a nivel industrial	**2010**	En junio de 2010, el gusano informático *Stuxnet* sacudió el mundo informático. Este ataque destruyó 1000 máquinas en la central nuclear de Natanz (Irán). Era el primer virus que podía reprogramar procesos industriales. Las centrales nucleares iraníes, el New York Times y la BBC rastrearon el origen de *Stuxnet* hasta los gobiernos de EE.UU e Israel, aunque ambos luego rechazaron la acusación.[7]
Estados Unidos	The New York Times: Represalia a un Diario	**2012**	Tras publicar una investigación sobre la prosperidad económica de la familia del Primer Ministro chino, decenas de piezas diferentes de código maligno fueron usadas para robar las claves de empleados del diario y acceder a sus computadoras. Sobre todo, para ingresar discretamente a la información del periodista David Barboza, quien había encabezado la investigación, el diario contrató a *Mandiant,* una empresa de Seguridad Informática, a fin de corroborar el ataque y encontrar su raíz. El informe concluyó que inequívocamente el origen fue China.

[7] **Ver Anexo 3** - Información adicional - Ciberataque Stuxnet a Iran y Sistemas SCADA

PAÍS	CIBERATAQUE	AÑO	DESCRIPCIÓN
Taiwán	Acción sostenida en el tiempo	**2013**	Taiwán recibe sistemáticamente ataques cibernéticos de su par chino, tal y como las autoridades lo han declarado públicamente. Hace algunos años, un troyano se introdujo en 30 agencias gubernamentales y en 50 compañías privadas, generando ataques de denegación de servicio. Estos ataques dejaron sin servicio a infraestructuras como hospitales, la Bolsa y algunos sistemas de control de tráfico.
Holanda	Ciberataque Mundial de Denegación de Servicio Distribuido	**2013**	La agresión se basó en la modalidad de denegación de servicio, que consiste en el bloqueo del portal debido a una avalancha de solicitudes sin permitir que los ciudadanos puedan acceder a pagar sus cuentas. Diez millones de holandeses se quedaron sin firma digital y no pudieron acceder a la declaración de renta muy popular para pagar impuestos. Después se aclaró que la seguridad de las cuentas no se había visto comprometida y los clientes podían sacar dinero de los cajeros automáticos sin ningún inconveniente.

PAÍS	CIBERATAQUE	AÑO	DESCRIPCIÓN
Estados Unidos	SONY Pictures Entertainment	**2014**	Sony Pictures Entertainment tres años después de las afectaciones a *Play Station Network*, los reflectores se pusieron sobre Sony nuevamente, cuando información confidencial de Sony fue filtrada. El autodenominado grupo *"Guardianes de la paz"* se adjudicó el ciberataque, alegando que habían logrado tener acceso a las computadoras un año antes de que éste se hiciera público. Los hackers tuvieron acceso a información sobre los empleados de Sony y sus familiares, obteniendo así e-mails, direcciones e información financiera. Otra información obtenida incluía guiones para próximas producciones, así como registros médicos de diversos actores famosos. El gobierno de EE.UU responsabilizó a Corea del Norte por los ataques, aunque el país asiático lo negó. [8]
Ucrania	BlackEnergy	**2015**	El gobierno de Ucrania señala a Rusia como responsable del apagón que sufrieron diversas centrales eléctricas del país, en un ataque con virus informáticos. Unas 80.000 personas se quedaron sin electricidad durante 6 largas horas, abandonadas al frío diciembre. BlackEnergy fue el primer ciberataque en la historia que se supo que estuvo involucrado en un apagón eléctrico generalizado.[9]

[8] **Ver Anexo 4 -** Información adicional - Ciberataque a Sony Pictures Entertainment en Estados Unidos
[9] **Ver Anexo 5 -** Información adicional - Ciberataque BlackEnergy en Ucrania

PAÍS	CIBERATAQUE	AÑO	DESCRIPCIÓN
Mundial	WannaCry	**2017**	Este ciberataque informático *Ransomware* Wannacry bloqueaba computadoras pidiendo un rescate económico a cambio de desbloquearlos. Se registraron ataques a más de diez mil organizaciones y más de doscientos mil usuarios finales en 150 países, que infectó sistemas Windows de diversas organizaciones y empresas como Telefónica y también afecto a computadoras de medio planeta y a redes tales como el Sistema Sanitario Británico, compañías de China, de Rusia, de toda Europa, entre otras.[10]

Tabla N° 3: Ciberataques más conocidos entre los años 2009 y 2019
Fuente: Elaboración Propia

[10] **Ver Anexo 6 -** Información adicional - Ciberataque de Ransomware “Wannacry” a nivel mundial

En comparación con otras regiones del mundo es poca la documentación que se ha obtenido sobre ciberataques a las ICI en América Latina; Sin embargo, no por ello se puede afirmar que no hayan ocurrido. Cabe aclarar que continuamente hay ciberataques en la mayoría de los países latinoamericanos, pero no tienen como objetivo los sectores críticos de cada país. Es decir, el ciberataque pudo haber existido, pero quizá no tuvo gran impacto a nivel nacional o internacional, o no fue reportado por falta de conocimiento o para no despertar algún tipo de pánico entre los ciudadanos.

CAPÍTULO 2. Normativa internacional y nacional para la protección de las Infraestructuras Criticas

2.1. Organismos, legislaciones, aportes y estrategias internacionales para la protección de las infraestructuras críticas.

Las medidas que las organizaciones y los gobiernos internacionales toman para asegurar la protección de las IC no siempre son similares, pero existen muchas fuentes de información disponibles las cuales muestran que, en países de Norteamérica, Unión Europea, Australia y Latinoamérica, es donde se han ejecutado en gran parte los avances más importantes respecto a la planeación e implementación de los mecanismos de protección de las IC. Por esta razón, se listan algunos países indicando la normativa aplicable y las organizaciones involucradas junto con las estrategias de ciberseguridad respectivas.

REGIÓN	AÑO	LEGISLACIÓN – PROGRAMA – ESTRATEGIA
Estados Unidos	**2001**	**Ley USA Patriot (Act de 2001)**[11] es una ley federal de los EE.UU que tiene por objeto ampliar la capacidad de control del estado pudiendo así combatir el terrorismo, mejorando la capacidad de las distintas agencias de seguridad, realizando actividades de coordinación y dotándolas de mayores poderes de vigilancia contra los mencionados delitos. [25]
	2002	**Ley CCI -** *Ley de información de Infraestructura Critica (Act 2002)* tiene por objeto facilitar un mayor intercambio de información sobre las IC entre los propietarios/operadores y entidades gubernamentales con responsabilidades en la protección de dichas Infraestructuras. [26]

[11] **USA PATRIOT** – **U**niting and **S**trengthening **A**mérica by **P**roviding **A**ppropriate **T**ools **R**equired to **I**ntercept and **O**bstruct **T**errorism | (Traducción al castellano) - Unir y Fortalecer a los Estados Unidos al Proporcionar las Herramientas Apropiadas Necesarias para Interceptar y Obstruir el Terrorismo)

REGIÓN	AÑO	LEGISLACIÓN – PROGRAMA – ESTRATEGIA
Estados Unidos	2003	**Directiva Presidencial de Seguridad Nacional-7 (HSPD-7),** titulada como *la Identificación, Priorización y Protección de Infraestructuras Críticas.* Establece la política nacional para identificar y dar prioridad a infraestructuras esenciales y protegerlos de los ataques terroristas. Estas declaraciones de política definen lo que cubre la directiva y los roles que desempeñan varias agencias federales, estatales y locales en su cumplimiento. [27]
		Estrategia Nacional para la Protección Física de las Infraestructuras Criticas y Activos Clave [12] identifica los objetivos nacionales y expone los principios básicos que sustentan las infraestructuras y los recursos vitales para la seguridad nacional. [28]
	2006	**NIPP** *Plan Nacional de Protección de Infraestructuras de Estados Unidos* este documento fue solicitado por la Directiva Presidencial de Seguridad Nacional - 7, su objetivo principal fue crear un programa para las Infraestructuras esenciales en EE.UU que proporciona un marco global y unificado para la protección de las IC y KR[13] a través de entidades federales, estatales, locales y el sector privado, incluidos los sectores específicos, el estado y los socios del sector privado en materia de seguridad. La versión inicial de NIPP se publicó en 2006 y se revisó en 2009 y 2013. [29]

[12] Strategy for Physical Protection of Critical Infrastructure and Key Assets
[13] **KR** – Key Resources ≡ Recursos Clave

REGIÓN	AÑO	LEGISLACIÓN – PROGRAMA – ESTRATEGIA
Estados Unidos	2006	**FERC** *Comisión Regulatoria de Energía Federal* es una agencia independiente que regula el intercambio interestatal de energía eléctrica en los EE UU Dado que la red eléctrica se ha convertido en uno de los principales objetivos del ciberterrorismo, el gobierno estableció la necesidad de desarrollar medidas de seguridad que protejan a estas Infraestructuras. [30]
		NERC *Organización de Confiabilidad Eléctrica* es el organismo responsable de establecer los estándares de seguridad para la red eléctrica en Norteamérica, es una parte importante de los esfuerzos y recursos dedicados en los EE.UU a la protección de IC. [31]
	2013	**Directiva de Política Presidencial 21 (PPD-21),** Seguridad y Resiliencia de la Infraestructura Crítica, emitida por el Presidente Barak Obama que pide explícitamente una actualización del NIPP. Esta directiva PPD-21 es una política que establece cómo el gobierno federal construye asociaciones confiables y promueve una unidad nacional de esfuerzo para fortalecer y mantener una infraestructura crítica segura, funcional y resistente. [32]
	2018	**Estrategia Nacional de Ciberseguridad de los Estados Unidos** se trata de un documento que contiene aspectos que van desde la seguridad de las redes federales y las IC hasta aspectos relacionados con el cibercrimen, para luego tratar el desarrollo de una fuerza especial y de aspectos esenciales como la resiliencia y las conductas en el ciberespacio, entre otros aspectos tratados. [33]

REGIÓN	AÑO	LEGISLACIÓN – PROGRAMA – ESTRATEGIA
	2004	**ENISA** *Agencia de la Unión Europea para la Ciberseguridad* es la agencia dedicada a lograr un alto nivel común de ciberseguridad en toda Europa. Se estableció en el año 2004 y se reforzó por la Ley de Ciberseguridad de la UE, también contribuye a la política cibernética de la UE, mejora la confiabilidad de los productos, servicios y procesos de TIC con esquemas de certificación de ciberseguridad, coopera con los estados miembros y los organismos de la UE y la ayuda a Europa a prepararse para los desafíos cibernéticos del futuro. [34]
Europa	**2005**	**Libro Verde**[14] GREEN PAPER es un *Programa Europeo para la Protección de Infraestructuras Críticas* cuyo objetivo principal fue recabar los distintos puntos de vista en torno a las posibles opciones para el PEPIC gracias a una amplia participación de los agentes interesados. Una protección eficaz de las IC requiere la comunicación, coordinación y cooperación, tanto en el ámbito nacional como en el de la UE, entre todas las partes interesadas: como propietarios y operadores de infraestructuras, reguladores, asociaciones profesionales y empresariales en cooperación con todos los niveles de la administración y el público en general. [35]

[14] **Libro Verde -** Green Paper on a European Programme for Critical Infrastructure Protection

REGIÓN	AÑO	LEGISLACIÓN – PROGRAMA – ESTRATEGIA
Europa	**2006**	**PEPIC** *Programa Europeo de Protección de Infraestructuras Críticas* tiene como objetivo la mejora de la protección de las IC en la UE frente a las amenazas a las mismas, especialmente contra el terrorismo. Su ejecución requiere la adopción de medidas diseñadas para facilitar la aplicación del programa el cual incluye un plan de acción del PEPIC, de la CIWIN, el uso de grupos de expertos en PIC a nivel de la UE, los procedimientos para compartir la información sobre PIC y la identificación y análisis de interdependencias y el ARGUS, el cual permite la conexión de todos los sistemas de emergencia de Europa mandando información para que lleven a cabo las medidas pertinentes en caso de amenaza. [36]
	2008	**La Comisión Europea aprobó la Directiva el 8 de diciembre de 2008**, sobre la identificación y designación de las ICE y la evaluación de la necesidad de mejorar su protección, mediante la cual se puso en marcha el programa PEPIC con el objetivo de mejorar la protección de las IC de la UE. [37]
	2012	**ENCS** *Red Europea para la Ciberseguridad Europea***,** es una organización sin ánimo de lucro, fundada por empresas holandesas de los sectores eléctricos, energéticos y de telecomunicaciones, cuya misión es mejorar la seguridad cibernética de las ICE. [38]

REGIÓN	AÑO	LEGISLACIÓN – PROGRAMA – ESTRATEGIA
Europa	**2019**	**Reglamento sobre la Ley de la Ciberseguridad de la Unión Europea** *o Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo.* Tiene como objetivo poder alcanzar un alto nivel de ciberseguridad, ciberresiliencia y confianza en la UE por medio del establecimiento de objetivos, tareas y aspectos organizativos para ENISA, redenominada y fortalecida con un nuevo mandato permanente y un marco para esquemas europeos voluntarios de certificación de productos, servicios y procesos de tecnologías de la información y de la comunicación. [39]
España	**2004**	**Real Decreto 421/2004** *del 12 de marzo* reguló y definió el ámbito y funciones del CCN, adscrito al CNI. Se hace necesaria la participación de un organismo que partiendo de un conocimiento de las tecnologías de la información y de las amenazas y vulnerabilidades que existen, proporcione una garantía razonable sobre la seguridad de productos y sistemas. A partir de esa garantía, los responsables de los sistemas de información pueden implementar los productos y sistemas que satisfagan los requisitos de seguridad de la información. [40]
	2006	**CCN-CERT** es la capacidad de respuesta a incidentes de seguridad de la Información del CCN, adscrito al CNI. Este servicio se creó en el año 2006 como CERT Gubernamental Nacional español.

REGIÓN	AÑO	LEGISLACIÓN – PROGRAMA – ESTRATEGIA
	2006	Su misión es contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas, incluyendo la coordinación a nivel público estatal de las distintas capacidades de respuesta a incidentes o centros de operaciones de ciberseguridad existentes. [41]
España	**2007**	**CNPIC** *Centro Nacional de Protección de Infraestructuras Críticas* es el organismo responsable del desarrollo, coordinación y supervisión de todas las políticas y actividades relacionadas con la protección de las IC españolas y con la ciberseguridad en el seno del Ministerio del Interior. Dentro de la estructura orgánica del CNPIC se encuentra la Oficina de Coordinación Cibernética que desempeña la coordinación técnica y la comunicación con los CSIRT nacionales de referencia: CERTSI y CCN-CERT. Estos se ocupan de la resolución técnica de incidentes de ciberseguridad que puedan afectar a operadores privados de IC. [42]
	2011	**Ley 8/2011** tiene por objeto establecer las estrategias y las estructuras adecuadas que permitan dirigir y coordinar las actuaciones de los distintos órganos de las administraciones públicas en materia de protección de las IC, previa identificación y designación de estas, para mejorar la prevención, preparación y respuesta de la nación frente a atentados terroristas u otras amenazas que afecten a las IC. [43]

REGIÓN	AÑO	LEGISLACIÓN – PROGRAMA – ESTRATEGIA
España	2013	**Estrategia de Ciberseguridad Nacional Española** es un documento estratégico que sirve de fundamento al Gobierno de España para desarrollar las previsiones de la Estrategia de Seguridad Nacional en materia de protección del ciberespacio con el fin de implantar de forma coherente y estructurada acciones de prevención, defensa, detección, respuesta y recuperación frente a las ciberamenazas. [44]
	2014	**INCIBE** es una sociedad dependiente del Ministerio de Asuntos Económicos y Transformación Digital a través de la Secretaría de Estado de Digitalización e Inteligencia Artificial y consolidada como entidad de referencia para el desarrollo de la ciberseguridad y de la confianza digital de ciudadanos, red académica y de investigación, profesionales, empresas y especialmente para sectores estratégicos. Con una actividad basada en la investigación, la prestación de servicios y la coordinación con los agentes con competencias en la materia, INCIBE contribuye a construir ciberseguridad a nivel nacional e internacional. Desde el 28 de octubre de 2014, el Instituto Nacional de Tecnologías de la Comunicación, S.A. (INTECO) pasa a llamarse Instituto Nacional de Ciberseguridad de España M.P., S.A. (INCIBE), según el acuerdo adoptado en Junta General del 27 de Octubre de 2014. Con dicho cambio de denominación e imagen, INCIBE proyecta una identidad acorde con su orientación estratégica y posicionamiento como centro nacional de referencia en ciber seguridad. [45]

REGIÓN	AÑO	LEGISLACIÓN – PROGRAMA – ESTRATEGIA
Reino Unido	**2007**	**CPNI** *Centro para la Protección de la Infraestructura Nacional del Reino Unido*, tiene como objetivo proteger la seguridad nacional proporcionando apoyo y asesoramiento sobre seguridad física, seguridad personal y seguridad de la información. CPNI es una organización interdepartamental con recursos de la industria, la academia y una serie de departamentos y organismos oficiales. [46]
	2016	**NCSC** *Centro Nacional de Ciberseguridad de Reino Unido* es una organización del gobierno de UK que se encarga de brindar asesoramiento y soporte tanto a los sectores públicos como privados sobre como poder reducir riesgos y evitar amenazas de la seguridad cibernética al Reino Unido. [47]
Australia	**1960**	**ASIO** *Organización de inteligencia de seguridad australiana* colabora estrechamente con el Gobierno con la AFP, con los operadores y propietarios de las IC, en la prevención y respuesta a los ataques terroristas que se puedan producir sobre una IC. ASIO tiene claro que el espionaje puede implicar el robo de información confidencial, privilegiada o clasificada que daña los intereses nacionales de Australia por esta razón trabaja en la industria gubernamental y privada para aumentar la conciencia de la amenaza y desarrollar contramedidas efectivas. [48]
	2004	**TISN** *Red de Intercambio de Información Confiable* es el principal mecanismo de participación del gobierno para el intercambio de información del gobierno empresarial y las iniciativas de creación de resiliencia en las IC.

REGIÓN	AÑO	LEGISLACIÓN – PROGRAMA – ESTRATEGIA
		El TISN conecta a representantes de la industria y el gobierno para garantizar el funcionamiento continuo de la IC frente a todos los peligros. Al compartir información sobre las amenazas y vulnerabilidades actuales y de mediano a largo plazo, la industria y el gobierno pueden colaborar en las medidas apropiadas para mitigar el riesgo y mejorar la capacidad de recuperación de la IC de Australia. [49]
Australia	**2004**	**CIAC** *Consejo Asesor de Infraestructura Critica* perteneciente al Departamento del Gobierno Federal de Australia[15] es un órgano consultivo del gobierno cuya misión es el liderazgo de la protección de las IC además de estar presidido por dicho departamento realiza labores de secretaría y asesoría en materias de recuperación de las IC. El CIAC australiano asemeja sus funciones al CNPIC español. [50]
	2014	**ACSC** *Centro de Ciberseguridad Australiano* brinda asesoramiento oportuno y personalizado a los socios de las IC, ayuda a los propietarios de activos a identificar y evaluar las vulnerabilidades de seguridad y brinda asistencia a los operadores de activos en la implementación de estrategias sólidas de mitigación y reducción de riesgos. [51]

[15] Departamento del Gobierno Federal de Australia ≡ Attorney General´s Department

REGIÓN	AÑO	LEGISLACIÓN – PROGRAMA – ESTRATEGIA
Australia	**2017**	**CiCentre** *Centro de Infraestructura Crítica Australiano* reúne experiencia y capacidad de todo el gobierno australiano para gestionar los riesgos complejos para la seguridad nacional de sabotaje, espionaje y coacción, además se centra en ayudar a los propietarios y los operadores a comprender y gestionar mejor los riesgos y desarrollar resiliencia, realizan evaluaciones de riesgos y brindan asesoramiento para reducir la posibilidad de que los actores malintencionados obtener acceso y control de los principales infraestructuras mediante propiedad, deslocalización, acuerdos de subcontratación y cadena de suministro. [52]
	2018	**Ley de Seguridad de la Infraestructura Critica del 2018** busca gestionar los complejos y cambiantes riesgos de seguridad nacional del sabotaje, el espionaje y la coerción que plantea la participación extranjera en la infraestructura crítica de Australia. La Ley se aplica a aproximadamente 200 activos en los sectores de electricidad, gas, agua y puertos. [53]
Canadá	**2003**	*Seguridad Publica de Canada* legalmente incorporado como el Departamento de Seguridad Pública y Preparación para Emergencias, es el departamento del gobierno federal de Canadá responsable para proteger a los ciudadanos canadienses, ayudar a mantener una sociedad pacífica y segura además de brindar asesoramento de apoyo al ministro de seguridad publica en asuntos relacionados con politicas de seguridad publica incluida la seguridad nacional y la gestión de emergencias, la politica y la aplicación de la ley, la interoperabilidad y el intercambio de información, la gestión de fronteras y la prevencion del delito. [54]

REGIÓN	AÑO	LEGISLACIÓN – PROGRAMA – ESTRATEGIA
Canadá	**2010**	**Estrategia de Protección a la Infraestructura Crítica Nacional de Canadá** el sistema canadiense de protección de las IC se desarrolla en la *National Strategy for Critical Infrastructure* y el *Action Plan for Critical Infrastructure* que establecen una colaboración a nivel federal, provincial, territorial y de los sectores de las IC con el fin de fortalecer su capacidad de recuperación. [55]
	2018	**Centro Canadiense de Ciberseguridad** CCIRC coordina la respuesta federal a los eventos cibernéticos y difunde avisos e informes a los departamentos federales, gobiernos provinciales y sectores críticos de la infraestructura. Para crear credibilidad, el departamento de ciberseguridad se involucra con las partes interesadas nacionales e internacionales como un socio confiable que comparte inteligencia procesable para defenderse de las amenazas cibernéticas. Para promover la conciencia pública, se realizan actividades de participación y promoción con otros niveles de gobierno, industria, academia y canadienses para impulsar un cambio de comportamiento duradero. [56]
Estonia	**2006**	**CERT- EE** es la organización responsable de la gestión de incidentes de seguridad en redes informáticas en Estonia, también es un punto de contacto nacional para la cooperación internacional en el campo de la seguridad informática, su deber es ayudar a los usuarios de Internet de Estonia en la implementación de medidas preventivas para reducir los posibles daños causados por incidentes de seguridad y ayudarlos a responder a las amenazas a la seguridad. [57]

REGIÓN	AÑO	LEGISLACIÓN – PROGRAMA – ESTRATEGIA
Estonia	**2014**	**Estrategia de Ciberseguridad de Estonia (2014-2018)** es el documento básico se centra en garantizar la seguridad de los servicios vitales, mejorar la lucha contra el delito cibernético y desarrollar las capacidades de defensa nacional. Uno de los principales objetivos de la estrategia es describir las medidas para el funcionamiento ininterrumpido y la durabilidad de los servicios básicos y la protección de la infraestructura de información crítica contra las amenazas cibernéticas. Es importante saber que Estonia es uno de los pocos estados del mundo que ha lanzado una estrategia nacional de ciberseguridad de tercera generación (2019-2022) destacando la naturaleza global de las amenazas en el ciberespacio y la necesidad de una acción internacional y multilateral. [58]
	2018	**Ley de Ciberseguridad de Estonia** establece las obligaciones de los proveedores de servicios para garantizar la seguridad cibernética de la red y los sistemas de información y la base para las notificaciones de incidentes cibernéticos. [59]

Tabla N° 4: Programas de protección de Infraestructuras críticas
Fuente: Elaboración Propia

Entre las principales iniciativas de los países latinoamericanos se encuentra la organización de grupos de trabajo adscritos al Ministerio de Defensa, en países como Brasil y Colombia, pioneros en la implementación de estrategias contra ataques informáticos.

Los equipos de respuesta a incidentes de seguridad cibernética *CSIRT* existen en varios países de América Latina y como referencia se tiene a: ArCERT (Argentina), posteriormente daría lugar al ICIC), ClCERT (Chile), CERT.Br (Brasil), VenCERT (Venezuela), ColCERT (Colombia), CERT.Uy (Uruguay), CGII (Bolivia), entre otros. De esta manera han ido surgiendo diferentes foros y organismos que coordinan los diferentes CSIRTS de todos los países del mundo compartiendo información específica sobre vulnerabilidades y ciberataques, divulgando medidas tecnológicas que se encargan de mitigar el riesgo de ataques a los sistemas y usuarios que se encuentren conectados a Internet que dan servicio a sus respectivas comunidades.

2.2. Organismos, legislaciones, aportes y estrategias nacionales (Caso Argentina) para la protección de las Infraestructuras Críticas.

► **ArCERT** se creó en 1999 mediante Resolución SFP Nº 81/99 y se llamó Coordinación de Emergencia en Redes Teleinformáticas de la Administración Pública Argentina y funcionó en el ámbito de la entonces denominada Subsecretaria de las Tecnologías Informáticas de la Secretaría de la Función Pública de la Jefatura de Gabinete de Ministros. ArCERT era un centro de respuesta de incidentes de seguridad el cual se encargaba de realizar la difusión de información a fin de neutralizar incidentes de seguridad en forma preventiva y correctiva, capacitaba al personal técnico que estaba a cargo de las redes de los organismos del sector público nacional y a la vez los asistía técnicamente para prevenir, detectar, manejar y superar dichos incidentes. [60]

A partir de 2013, ArCERT fue reemplazado por ICIC-CERT [61], el cual se define como una unidad de respuesta de incidentes de redes, teniendo como objetivo principal centralizar y coordinar los esfuerzos para el manejo de los incidentes de seguridad, que afecten los recursos informáticos de la administración pública nacional.

► **Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad (ICIC).** De acuerdo con la Resolución 580/2011 [62] se creó en el ámbito de la Oficina Nacional de Tecnologías de Información (ONTI) de la Subsecretaría de Tecnologías de Gestión, Secretaría de Gabinete, Jefatura de Gabinete de Ministros, con el fin de impulsar la creación y adopción de un marco regulatorio especifico que respalde la identificación y protección de las infraestructuras estratégicas y críticas del sector público nacional y del sector privado con miras al desarrollo de nuevas estrategias y la correcta implementación de tecnologías acertadas y útiles para su funcionamiento.

En el marco de este programa, al crear el ICIC, se conformaron cuatro grupos de trabajo. [63]

1) Grupo de trabajo ICIC-CERT: Administra la información sobre reportes de incidentes de seguridad, ayuda a encausar posibles soluciones de forma organizada brindando el asesoramiento técnico, promueve la centralización de reportes sobre incidentes de seguridad ocurridos en redes informáticas.

2) Grupo de trabajo ICIC-GAP: (Grupo de Acción Preventiva) Investiga nuevas herramientas e incorpora tecnologías de última generación en materia de ciberseguridad, para minimizar todas las posibles vulnerabilidades de la infraestructura digital del sector público nacional y monitorea los sistemas y servicios críticos de la infraestructura para prevenir posibles fallas de seguridad.

3) Grupo de trabajo ICIC-GICI: (Grupo de ICI) Se encarga de proponer normas de gestión de la seguridad documentarlas y actualizarlas; elaborar políticas de resguardo de seguridad digital con el fin de fortalecer alianzas entre los sectores público y privado; establecer prioridades y planes estratégicos para liderar el abordaje de la ciberseguridad asegurando la implementación de los últimos avances en tecnología para la protección de las IC, de los datos y de los sistemas, coordinando la implementación de ejercicios de respuesta; definir a estas infraestructuras como instalaciones,

redes, servicios y equipos físicos y de TI, cuyo funcionamiento es indispensable para brindar servicios a los ciudadanos y a las instituciones; alertar a los organismos que se adhieran al programa sobre casos de detección de intentos de vulneración de infraestructura critica, sean estos reales o no; coordinar la implementación de ejercicios de respuesta ante la eventualidad de un intento de vulneración de las IC del sector público nacional.

4) Grupo de trabajo ICIC-INTERNET SANO: Promueve la concientización de los riesgos respecto al uso de los medios digitales tanto en el sector público como privado.

► **El Decreto N° 1067/2015** creó la SUBSECRETARIA DE PROTECCION DE INFRAESTRUCTURAS CRITICAS DE INFORMACIÓN Y CIBESEGURIDAD [64] en el ámbito de la Secretaria de Gabinete de la Jefatura de Gabinete de Ministros. Esta subsecretaría tiene como objetivo principal la elaboración de la Estrategia Nacional de Protección de Infraestructuras Críticas de Información y Ciberseguridad además de otros objetivos como entender los procesos relativos al accionar del equipo de respuesta a emergencias informáticas a nivel nacional y entender las acciones de supervisión, monitoreo, análisis y detección de los activos críticos de la información. Para ello se transfirió el Programa Nacional ICIC a la esfera de la DIRECCION NACIONAL DE INFRAESTRUCTURAS CRITICAS DE INFORMACIÓN Y CIBERSEGURIDAD dependiente de la subsecretaría recién creada.

►En el año 2017, por el **Decreto N° 577/17**, el gobierno creó el **Comité de Ciberseguridad** [65], en la órbita del entonces Ministerio de Modernización ahora llamado Subsecretaria del Ministerio de Modernización, integrado por representantes de dicho Ministerio, Ministerio de Defensa y de Seguridad.

El Comité de Ciberseguridad debía cumplir con las siguientes tareas específicas como son el desarrollo de la Estrategia Nacional de Ciberseguridad, en coordinación con las áreas competentes de la Administración Pública Nacional, elaboración de un plan de acción necesario para la implementación de la Estrategia Nacional de Ciberseguridad, convocar a otros organismos para que participen en la implementación de medidas en el marco del plan de acción elaborado conforme, impulsar el dictado de un marco normativo en materia de ciberseguridad, fijar los lineamientos y criterios para la definición, identificación y protección de las IC nacionales, participar en el desarrollo de acciones inherentes a la ciberseguridad nacional que se le encomienden.

►**Estrategia Nacional de Ciberseguridad.** [66] La Secretaría de Gobierno de Modernización en el año **2019** emitió la **Resolución N° 829/19**, a través de la cual establece la Estrategia de Ciberseguridad, crea la Unidad Ejecutiva del Comité de Ciberseguridad y establece los objetivos a lograr:

- Concientización del uso seguro del ciberespacio;
- Capacitación y educación en el uso seguro del ciberespacio;
- Desarrollo del marco normativo;
- Fortalecimiento de capacidades de prevención, detección y respuesta;
- Protección y recuperación de los sistemas de información del sector público;
- Fomento de la industria de la ciberseguridad;
- Cooperación internacional;
- Protección de las infraestructuras nacionales de información críticas.

► **Ley de Delitos Informáticos, Ley 26.388.** [67] En el año 2008 se incorporan al código penal aspectos tecnológicos vinculados a delitos actuales y modifica varios artículos del código penal para contemplar delitos que utilicen como medio a las TIC En esta ley se incorporan sanciones en los siguientes casos: posesión de pornografía infantil con la finalidad de distribuirla por Internet o a través de otros medios electrónicos, la apropiación, violación y difusión de comunicaciones electrónicas, la interceptación de cualquier tipo de comunicaciones electrónicas, la suspensión de las comunicaciones electrónicas, el acceso ilícito a sistemas informáticos, el acceso a bases de datos personales, la comunicación de información almacenada en bases de datos personales, la producción de daños informáticos y la propagación de virus, la introducción de datos falsos en un archivo de datos personales, el fraude informático, el daño o sabotaje informático.

►**Ley de Protección de Datos Personales, Ley 25.236.** [68] Tiene como objetivo la protección integral de los datos personales recogidos en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean estos públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, se caracteriza por definir principios generales relativos a la protección de datos. Esto abarca desde derechos de los titulares hasta las figuras de usuarios y responsables de archivos, registros y bancos de datos, el control, sanciones, acción de protección de los datos personales e inclusive el spam están vinculados a esta Ley.

► **Ley de Firma Digital, Ley 25.506.** [69] Con esta ley se admite y se fijan las condiciones para el uso de la firma electrónica y de la firma digital reconociendo su eficacia jurídica. También se instaura la Infraestructura de Firma Digital de la República Argentina.

►**Ley de Grooming, Ley 26.904.** [70] Fue sancionada en el año 2013 y a partir de ese año el *Grooming* se volvió un delito que muestra un alarmante crecimiento de casos. Según su Artículo 1°, que se incorporó como artículo 131 al Código Penal: "*Será penado con prisión de seis (6) meses a cuatro (4) años el que, por medio de comunicaciones electrónicas, telecomunicaciones o cualquier otra tecnología de transmisión de datos, contactare a una persona menor de edad, con el propósito de cometer cualquier delito contra la integridad sexual de la misma"*.

►**Ley de Inteligencia Nacional, Ley 27.126.** [71] Define el marco jurídico dentro del que deben llevarse a cabo las actuaciones de inteligencia del Estado. Esta ley también establece que esas actuaciones tendrán que realizarse conforme la Constitución Nacional, los tratados de derechos humanos y cualquier otra ley que recoja derechos y garantías. Además, en esta ley se crea la Agencia Federal de Inteligencia, dependiente del Poder Ejecutivo Nacional. Se considera el órgano superior del Sistema de Inteligencia Nacional. A este órgano se le atribuyen funciones relacionadas con la creación de inteligencia nacional y la producción de inteligencia criminal.

CAPÍTULO 3. Resultados del Anáisis Realizado

3.1. Tipos de ciberataque de infraestructuras criticas[16]

Uno de los primeros resultados de la investigación es mostrar algunos de los tipos más relevantes de ciberataques a las IC, además de ser los más comunes en las páginas visitadas. En la siguiente figura se puede visualizar un claro ejemplo de los tipos de ciberataques más conocidos, de los cuales a continuación, se hará una breve descripción.

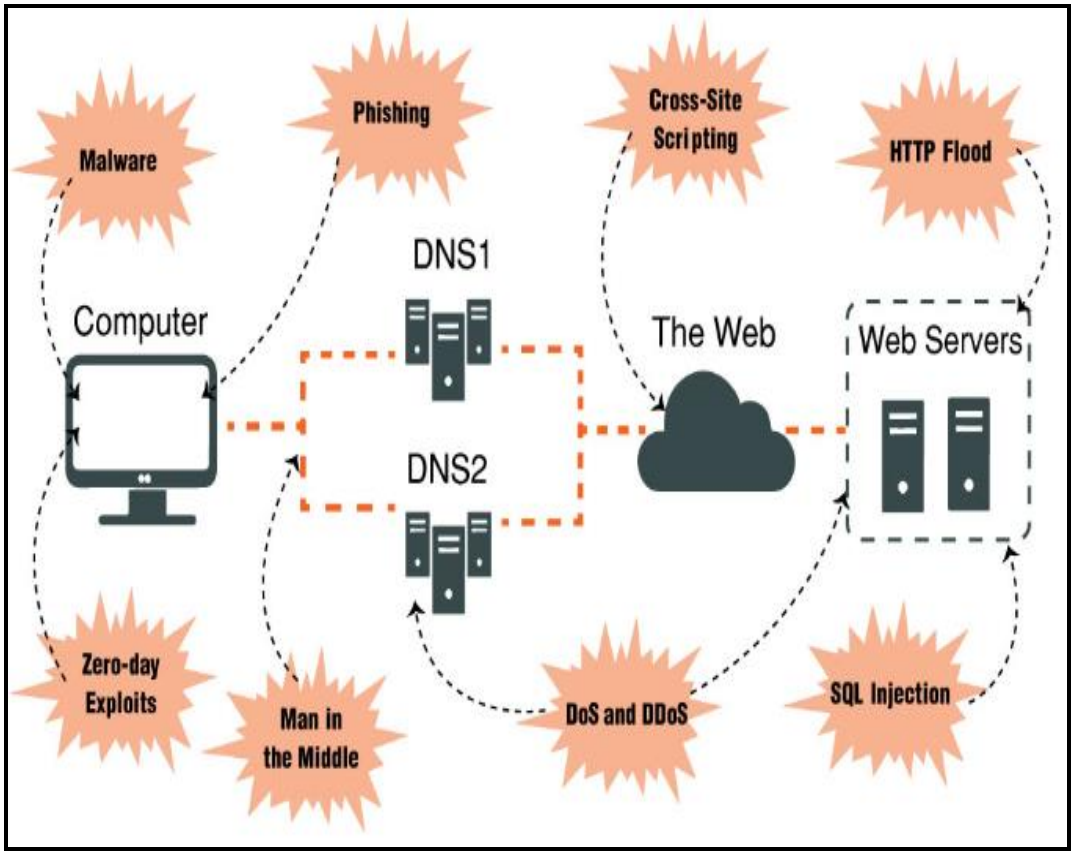


Figura N° 3: Ciberataques más comunes en las Infraestructuras críticas [72]

[16] **Ver Anexo 7 –** Información adicional - Tipos de ciberataques de las infraestructuras críticas.

► Ataques de Denegación de Servicio (DoS/DDoS)

Un ataque de Denegación de Servicio se encarga de saturar los recursos de un sistema para que éste no pueda responder a las solicitudes de servicio mientras que un ataque de Denegación de servicio Distribuido también es un ataque a los recursos del sistema, pero se inicia desde una gran cantidad de otras máquinas host que están infectadas por el software malicioso controlado por el atacante. Existen algunos tipos de ciberataque DoS y DDoS y son los siguientes: [73]

- Ataque SYN o Inundación TCP/SYN

Consiste en saturar el tráfico de la red para aprovechar el mecanismo de negociación de tres vías del protocolo TCP. [74]

- Ataque de ping de la muerte – (Ping of Death Attack o PoD)

Es un tipo de ataque de DoS en el que un atacante intenta bloquear, desestabilizar o congelar la computadora o el servicio objetivo mediante el envío de paquetes de gran tamaño con un simple comando *ping*, mientras que los ataques PoD explotan las debilidades heredadas que pueden haber sido parcheadas en los sistemas de destino. [75]

- Ataque Pitufo – (Smurf attack)

Es un tipo de ataque de DDoS que deja las redes informáticas inoperativas. El ataque *smurf* logra atacar aprovechando las vulnerabilidades del protocolo de Internet y de los protocolos de mensajes de control de Internet. [76]

- Ataque de lágrima – (Teardrop Attack)

Es un ataque de denegación de servicio que implica enviar paquetes fragmentados a una máquina de destino. Dado que la máquina que recibe dichos paquetes no puede volver a ensamblarlos debido a un error en el reensamblaje de fragmentación TCP/IP, los paquetes se superponen entre sí, lo que bloquea el dispositivo de red de destino. [77]

- Botnets

Se refiere a un grupo de computadoras que han sido infectadas por *malware* y quedan bajo el control de un actor malicioso. Los botnets pueden diseñarse para realizar tareas ilegales o maliciosas, incluido el envío de spam, el robo de datos, el *ransomware*, hacer click de manera fraudulenta en anuncios o ataques de DDoS. [78]

► Ataque del Hombre del Medio – (Man in the Middle - (MitM))

Un ataque de MitM ocurre cuando un hacker se inserta entre las comunicaciones de un cliente y un servidor. Estos son algunos tipos comunes de ataques de MitM: [79]

- Secuestro de sesión (Session hijacking)

El atacante secuestra una sesión entre un cliente de confianza y un servidor de red. La computadora atacante sustituye su dirección IP por el cliente de confianza mientras el servidor continúa la sesión, creyendo que se está comunicando con el cliente. [80]

- Suplantación de IP *(IP Spoofing)*

La suplantación de IP es utilizada por un atacante para convencer a un sistema de que se está comunicando con una entidad conocida y confiable y, en consecuencia, proporcionarle acceso.

El atacante envía un paquete con la dirección de origen IP de un host conocido y confiable en lugar de su propia dirección de origen IP. El host de destino puede aceptar el paquete y actuar sobre él. [81]

► El Ataque de Phishing

Es la práctica de enviar correos electrónicos que parecen provenir de fuentes confiables con el objetivo de obtener información personal o influir en los usuarios para que ejecuten alguna acción en particular. Podría implicar un archivo adjunto a un correo electrónico que carga *malware* en su computadora o también podría ser un enlace a un sitio web ilegítimo que puede engañarlo para que descargue código malicioso o entregue su información personal.

Existe un tipo muy específico de phishing llamado *Ataque Spear Phishing* donde los atacantes se toman el tiempo para investigar el target (objetivo) a atacar y de esta forma crear mensajes personales y relevantes. Debido a esto, la suplantación de identidad puede ser muy difícil de identificar e incluso más difícil de defender. [82]

► Ataque de Conducción – (Drive-By Attack)

Los ataques de descarga drive-by son un método común para propagar *malware*. Los hackers buscan sitios web inseguros y plantan un script malicioso en el código HTTP o PHP en una de las páginas. Este script puede instalar *malware* directamente en la computadora de alguien que visita el sitio o puede redirigir a la víctima a un sitio controlado por los hackers. [83]

► Ataque de Contraseña – (Password Attack)

Debido a que las contraseñas representan el mecanismo más utilizado para autenticar a los usuarios en un sistema de información, obtener contraseñas es un enfoque de ataque común y efectivo.

El acceso a la contraseña de una persona se puede obtener mirando alrededor del escritorio de la persona, "Olfateando o Sniffeando" la conexión a la red para adquirir contraseñas sin cifrar, utilizando ingeniería social, obteniendo acceso a una base de datos de contraseñas o adivinando directamente. [84]

Existen dos tipos de ataque de contraseña, ya sea por fuerza bruta o ataque de diccionario o de manera aleatoria o manera sistemática:

- Ataque por Fuerza Bruta

Para adivinar la contraseña se usa este ataque siendo un enfoque aleatorio probando diferentes contraseñas y esperando que funcione. Se puede aplicar cierta lógica probando contraseñas relacionadas con el nombre de la persona, el cargo, los pasatiempos o elementos similares. [85]

- Ataque de Diccionario

Se utiliza un diccionario de contraseñas comunes para intentar obtener acceso a la computadora y la red de un usuario. Un enfoque aplicado es copiar un archivo cifrado que contiene las contraseñas, aplicar el mismo cifrado a un diccionario de contraseñas de uso común y comparar los resultados. [86]

► Ataque de Cumpleaños – (Birthday Attack)

Los ataques de cumpleaños se realizan contra algoritmos hash que se usan para verificar la integridad de un mensaje, software o firma digital. Un mensaje procesado por una función hash produce un Resumen de Mensaje o MD de longitud fija, independiente de la longitud del mensaje de entrada, este MD caracteriza de manera única el mensaje. El ataque de cumpleaños se refiere a la probabilidad de encontrar dos mensajes aleatorios que generan el mismo MD cuando es procesado por una función hash. Si un atacante calcula el mismo MD para su mensaje que el usuario, puede reemplazar con seguridad el mensaje del usuario con el suyo y el receptor no podrá detectar el reemplazo incluso si compara los MD. [87]

► **Ataque de Inyección de SQL – (SQL Injection Attack)**

El lenguaje de consulta estructurado SQL se utiliza para consultar, operar y administrar sistemas de bases de datos como Microsoft SQL Server, Oracle o MySQL. SQL es consistente en todos los sistemas de bases de datos que lo admiten; sin embargo, hay complejidades que son particulares de cada sistema. Un ataque de inyección SQL es un ataque que tiene como objetivo alterar la intención original de la aplicación mediante el envío de declaraciones SQL proporcionadas por el atacante directamente a la base de datos del backend, dependiendo de la aplicación web y de cómo procesa los datos suministrados por el atacante antes de crear una declaración SQL. Un ataque de inyección SQL exitoso puede tener implicaciones de largo alcance. [88]

► **Ataque XSS – (Cross-Site Scripting XSS Attack)**

XSS es el proceso de agregar código malicioso a un sitio web legítimo para recopilar información del usuario con un propósito delictivo. Los ataques XSS se realizan gracias a las vulnerabilidades de seguridad que se encuentran en las aplicaciones web y se explotan comúnmente mediante la inyección de un script del lado del cliente. Por ejemplo, se podría enviar la cookie de la víctima al servidor del atacante, el atacante puede extraerla y usarla para el secuestro de sesión. Las consecuencias más peligrosas se producen cuando el XSS se utiliza para explotar vulnerabilidades adicionales. Estas vulnerabilidades pueden permitir a un atacante no solo robar cookies, sino también registrar pulsaciones de teclas, hacer capturas de pantallas, descubrir y recopilar información de red, y acceder y controlar de forma remota la máquina de la víctima. [89]

► **Ataque de Espionaje – (Eavesdropping Attack)**

Los ataques de espionaje ocurren a través de la intercepción del tráfico de la red. Al escuchar a escondidas, un atacante puede obtener contraseñas, números de tarjetas de crédito y otra información confidencial que un usuario podría estar enviando a través de la red.

Las escuchas pueden ser pasivas cuando un atacante detecta la información escuchando la transmisión de mensajes en la red o activas cuando un atacante capta activamente la información disfrazándose de unidad amiga y enviando consultas a los transmisores. Esto se llama sondeo, escaneo o manipulación. [90]

► Infecciones por Malware – (Malware Attack)

Malware o software malicioso, que incluye bots de spyware, *ransomware*, virus, gusanos, adware, errores y rootkits.

El *malware* infringe una red a través de una vulnerabilidad, generalmente es cuando un usuario hace click en algún enlace o archivo adjunto de un correo electrónico, de esta forma instala el software maligno, una vez este dentro del sistema, el *malware* puede hacer las siguientes acciones: bloquear el acceso a componentes clave de la red, instalar algún software peligroso adicional, obtener información de forma encubierta transmitiendo datos desde un disco duro, alterar ciertos componentes y dejar el sistema inoperable. [91]

3.2. Consecuencias de los ciberataques en análisis

Como resultado del proceso de análisis investigativo realizado sobre los casos de ciberataques tratados en este trabajo fue posible visualizar, tal como se ha explicado previamente, que el impacto de la interrupción del servicio de una IC llega a la sociedad en su conjunto, o bien a algunos sectores sociales, produciendo daños económicos, de imagen, y también en el desarrollo de la vida habitual de cualquier persona.

A continuación, se muestran las consecuencias producidas por cada uno de los ciberataques:

- **(2010) Irán - Primer ataque a nivel industrial**

Stuxnet definitivamente marcó un giro evidente en la historia de la ciberseguridad y de la historia militar, ya no es recordado como un golpe representativo contra el programa nuclear iraní, sino que será recordado como el punto de partida hacia una ciberguerra.

Stuxnet lanzó una nueva era rediseñando conceptos de guerra y definiendo que de ahora en más dejara de ser física para convertirse en digital, es decir que una nación puede atacar a otra sin declaración de disputas ni reconocimiento oficial de algún tipo de embestida, aun así, habiendo arrasado con parte de sus infraestructuras.

Hoy en día, muchas naciones llevan a cabo operaciones de guerra virtual a espaldas de sus ciudadanos y de la opinión pública.

Stuxnet tuvo una alta significancia ya que fue una pieza de *malware* de nueva generación que se introdujo, se propagó y pudo ocasionar daños en los sistemas industriales que no estaban conectados a Internet.

El objetivo básico del *Stuxnet* fue explotar una vulnerabilidad física que en este caso eran los rotores de centrífuga de la planta nuclear de Natanz y de esta forma ejercer mayor presión sobre las centrifugadoras y manipular las velocidades del rotor.

Asimismo, el Presidente Iraní de ese momento *Mahmud Ahmadineyad*, reconoció públicamente que, luego del incidente, la planta central había sido cerrada temporalmente y culpó a EE.UU e Israel por haber desarrollado el *malware Stuxnet.*

Todas las investigaciones iniciadas fueron suspendidas sin arrojar ningún resultado positivo. Hasta el momento de la emisión de los informes emitidos, no se había logrado conocer a ciencia cierta cuál fue el origen de este virus. Lo que, si se pudo confirmar con total certeza, después de algunos estudios, que *Stuxnet* había sido creado para afectar las centrífugas nucleares y afectar sus sistemas industriales.

A raíz del ciberataque ocurrido en la Planta de Natanz, dos meses después del ataque, se conoció que las infecciones del *malware* se habían propagado hacia otros países.

De acuerdo con algunas empresas de Seguridad Informática, se pudo rastrear aproximadamente 60.000 máquinas infectadas en torno a los países que fueron víctimas del Stuxnet, de esta manera, se logró determinar la gran trayectoria con que el gusano cibernético se expandió infectando muchas computadoras a nivel mundial.

A pesar de que los iraníes a finales del 2010 dijeron públicamente que el gusano *Stuxnet* tuvo un impacto mínimo en sus operaciones nucleares, los expertos de seguridad que siguieron la investigación afirmaron que el *malware* atrasó dos años el programa nuclear de Irán.

- **(2012-2013) EE UU - The New York Times: Represalia a un Diario**

La primera intrusión en los sistemas del diario fue el 13 de septiembre del 2012, justo cuando el artículo de investigación sobre *Wen Jiabao,* el primer Ministro Chino, estaba casi terminado. El ataque se ejecutó por medio de la creación de tres puertas traseras las cuales pudieron llegar hasta las computadoras de los usuarios. El artículo en cuestión trataba sobre los familiares del ministro y de la fortuna de varios millones de dólares que habrían acumulado ilegalmente.

Cuando *The New York Times* se enteró de las advertencias que los funcionarios del gobierno de China les habían hecho sobre el articulo próximo a publicar, ya que bajo ningún modo les convenia que los manejos de dinero y los negocios ilícitos salieran a la luz, los ejecutivos del diario solicitaron a la multinacional de tecnología y telecomunicaciones *AT&T,* un día antes de la publicación, que monitoreara la red informática y que estuviese atenta ante cualquier actividad inusual.

El 25 de octubre del 2012, el mismo día en que se publicó el artículo en línea, la empresa *AT&T* informó al diario *The New York Times*, que se había notado un comportamiento que era parecido a otros ataques y se creía que había sido perpetrado por el ejército chino.

Más adelante, el 31 de enero del 2013 se ejecutó el ataque principal al diario, el cual básicamente consistía en la utilización de un *malware* que les permitió a los atacantes chinos infiltrarse en los sistemas informáticos de la empresa durante cuatro meses a pesar de tener activado un software de seguridad, apropiándose de las contraseñas corporativas y robando correos electrónicos, contactos y documentación privada de algunos periodistas; además de lograr instalar cuarenta y cinco programas de *malwar*e en la red y siendo uno solo de estos detectado por el software de seguridad, el resto del *malware* se ejecutó en el sistema sin activar alarma alguna.

Después de rastrear bajo cuerda a los intrusos y así estudiar sus movimientos con el fin de ayudar a tener las mejores defensas para bloquearlos, *The New York Times* y los expertos en seguridad informática expulsaron a los hackers y evitaron que volvieran a acceder.

Según las investigaciones realizadas sobre este ciberataque, es posible que los atacantes hayan usado técnicas de ataque de *phishing*, en el que envían correos electrónicos a los empleados que contienen enlaces o archivos adjuntos maliciosos. Todo lo que se necesita es un click en el correo electrónico de un empleado para que los piratas informáticos instalen herramientas de acceso remoto.

Se tuvo conocimiento que los hackers chinos cambiaban continuamente de una dirección IP a otra; una dirección IP y el uso de computadoras de la universidad como proxy con el objetivo de ocultar las fuentes de los ataques. *The New York Times* bloqueó las computadoras externas comprometidas, eliminó todas las puertas traseras de su red, cambió la contraseña de cada empleado y agregó seguridad adicional en sus sistemas.

Se pudo conocer con exactitud las acciones que fueron realizadas en este ataque, de acuerdo con las investigaciones hechas post - incidente, llegando incluso a determinar que los ataques coincidían con el horario relativo a una jornada laboral convencional en China, ya que la actividad maliciosa de cada día se iniciaba coincidiendo con las 8 AM en Beijing.

El creciente número de ataques que se han rastreado hasta China sugiere que los piratas informáticos están detrás de una campaña de espionaje de gran alcance dirigida a un conjunto de objetivos en expansión que incluye corporaciones, agencias gubernamentales, grupos de activistas y organizaciones de medios dentro de los EE.UU.

La campaña de espionaje de China hacia los EE.UU trata de controlar la imagen pública de China, tanto a nivel nacional como en el exterior, así como de robar secretos comerciales.

El ataque al *New York Times* tiene un perceptible componente político, por las condiciones en las que se ha producido. Casos como el del *New York Times* demuestran una realidad cada vez más cierta acerca de las acciones y/o decisiones que se toman en el mundo real y pueden tener su impacto a través del mundo virtual.

- **(2013) Holanda - Ciberataque mundial de DDoS**

En el 2013, existió el llamado *Mayor Ciberataque de Denegación de Servicio de la Historia*, ya que en marzo de ese año Internet colapso en todo el mundo e interrumpió los servicios globales por un lapso de tiempo determinado. El ataque DDOS provocó una sobrecarga de los recursos del sistema informático hasta que la red se ralentizó por los accesos masivos a la misma.

En ese mismo mes de marzo del 2013, Holanda detecto un ataque a sus Sistemas de Identificación Electrónica Nacional conocido como **DigiD** que sirve para identificarse en sitios web de la administración pública, en las instituciones sanitarias y en los fondos de pensiones, ya que este sistema les permite a los ciudadanos presentar por internet la declaración de renta. Se trató de restablecer la conectividad con ligereza, pero no fue posible; muchos de los sitios que fueron atacados permanecieron inaccesibles por unos días. Este ataque cibernético dejó a más de 10 millones de holandeses sin firma digital aproximadamente por 72 horas y con gran cantidad de portales web del gobierno caídos.

- **(2014) Estados Unidos - Sony Pictures Entertainment**

El 24 de Noviembre de 2014, un grupo de hackers se encargó de atacar los servidores de una de las más prestigiosas productoras cinematográficas y de televisión de los EE.UU, *SONY Pictures*.

El ataque bloqueó los sistemas críticos de la compañía mediante un *malware* y pudo acceder a la información privada de los empleados como también a la información confidencial de la organización en lo que respecta a las próximas películas que iban a estrenar. *SONY* sufrió grandes daños económicos después del hackeo, como también se vio afectada por la caída de sus acciones en la bolsa, además del dinero perdido en relación a los costos de producción de los films que no se pudo estrenar, se estimó pérdidas de hasta 200 millones de dólares y la compañía sufrió demandas por parte de los actores por no saber proteger debidamente sus datos personales y privados.

Al mes siguiente del ciberataque, el día 2 de diciembre, se empezó a difundir toda esa información en Internet, causando un daño incalculable a la reputación y las finanzas de una multinacional. El Departamento de Justicia de Estados Unidos emitió cargos formales relacionados con el hackeo de *SONY* contra el ciudadano norcoreano Park Jin-hyok el 6 de Septiembre de 2018 y ordenó el arresto de *Park* por orden del tribunal del Distrito Central de California.

- **(2015) Ucrania – BlackEnergy**

En diciembre del 2015, ocurrió un apagón sorpresivo en Ucrania, el cual estaba relacionado con el *malware* destructivo llamado *BlackEnergy*. Este *malware* cuenta con un componente capaz de apagar los sistemas eléctricos de cualquier región.

El objetivo del ataque en la localidad ucraniana cerca a Kiev, la capital de Ucrania principalmente fue el sabotaje de los sistemas de control de red eléctrica interrumpiendo el suministro eléctrico a millones de residentes de la localidad, y dicho objetivo fue logrado exitosamente.

El día del ataque, aproximadamente 1.5 millones de habitantes se quedaron sin electricidad durante seis largas horas. En primera instancia, los intrusos cortaron la electricidad, luego intentaron dañar la configuración de los sistemas SCADA de manera de entorpecer la reactivación del sistema eléctrico, ejecutaron el troyano llamado *KillDisk* el cual está programado principalmente para destruir archivos importantes de cualquier central eléctrica, después bloquearon todas las comunicaciones entre los clientes y el sistema de control, a fin de poder dificultar las acciones de las compañías para descubrir que se había producido un ataque de esas características y semejante magnitud y luego lanzaron el ataque de denegación de servicio en sitios web y centrales telefónicas de tal forma que los clientes no podían llamar a la misma ni ser informados por medio virtual sobre lo que había ocurrido; concluyendo, este *malware* después de haberse propagado por la gran mayoría de las computadoras de la compañía eléctrica destruyo los discos duros dejándolos inservibles, borrando de esta manera cualquier huella o evidencia posible dentro de los sistemas.

- **(2017) Mundial - Ransomware Wannacry**

Este ataque empezó el viernes 12 de mayo de 2017 infectando más de 10.000 organizaciones y 230.000 computadoras en más de 150 países.

El *malware* se propagó a nivel global por países de Asia como China y Rusia los cuales fueron altamente golpeados afectando indiscriminadamente tanto al sector público como al sector privado; países europeos como Ucrania y Francia fueron víctimas del ataque en sus sistemas de control y de información, además de gran parte del Servicio Nacional de Gran Bretaña, también resultaron afectados.

La empresa de Tecnología y Telecomunicaciones *Telefónica de España* fue una de las primeras afectadas por Wannacry y también una de las primeras entre las que tomaron estado público. Asimismo, fueron afectados numerosos equipos de la compañía estadounidense de transporte FedEx y fabricantes de vehículos como Nissan y Renault, entre otras. En cuanto a Latinoamérica, los países que sufrieron mayor impacto fueron Argentina, Chile, México, Brasil, Colombia y Ecuador.

Para ejecutar el *ransomware* “*WannaCry*” o “QUIERO LLORAR" sólo hacía falta que uno de sus archivos llegase a una computadora o red de computadoras para poder secuestrar un sistema por completo. Una vez se encontraba dentro, el *ransomware* bloqueaba el acceso al administrador y a los usuarios reales, pidiendo una recompensa a cambio de la devolución del acceso. Habitualmente ésta recompensa se exige en *Bitcoins*, una criptomoneda prácticamente imposible de rastrear.

El impacto de este ataque fue tal que *Microsoft,* decidió lanzar especialmente parches post-ataque para Windows XP, Windows 8 y Windows Server 2003, a pesar de ser versiones sin soporte oficial de esta forma y por la severidad de este caso ameritó que se hiciera la excepción de publicar actualizaciones incluso para los sistemas obsoletos. La multinacional de software de seguridad *Check Point* afirma que las empresas afectadas por el virus *WannaCry* a nivel mundial pagaron rescates por valor de 43,30 bitcoins, equivalentes a más de 70.000 euros.

Los expertos señalan el severo impacto del virus informático que se propagó a gran escala pese al silencio de las numerosas compañías que se han visto afectadas.

3.3. Recomendaciones

Si bien el alcance de esta investigación es de tipo teórico y documental, siendo su objetivo evaluar las consecuencias de los ciberataques más relevantes a nivel mundial en el período 2009-2019 a las IC es importante complementarlo con la propuesta de algunas recomendaciones para mejorar sus procesos de ciberseguridad.

En principio, dada la complejidad del problema, es una buena práctica tomar como base algún estándar internacional, porque ellos definen y comunican acciones que fueron convenientemente probadas por otras organizaciones. Existen varios marcos de trabajo, estándares y guías de ciberseguridad. Uno de los más conocidos a nivel mundial, es el Framework de Ciberseguridad del NIST [92].

De acuerdo con el NIST: "*El marco de trabajo es una guía voluntaria, basada en estándares, directrices y prácticas existentes para que las organizaciones de infraestructura crítica gestionen mejor y reduzcan el riesgo de ciberseguridad. Además, se diseñó para fomentar las comunicaciones de gestión del riesgo y la seguridad cibernética entre los interesados internos y externos de la organización*".

Este proporciona una clasificación y un mecanismo común para que las organizaciones describan su situación actual en materia de ciberseguridad y su estado objetivo; identifiquen y prioricen oportunidades de mejora dentro del contexto de un proceso continuo y repetible; evalúen el progreso hacia el estado objetivo y comuniquen a las partes interesadas internas y externas sobre el riesgo de ciberseguridad. Las organizaciones deben decidir qué directivas del marco implementarán y cómo lo harán.

A continuación, se detallan las cinco funciones fundamentales definidas por el mencionado marco:

- **Identificar**: Comprender el contexto empresarial, los recursos que respaldan las funciones críticas y los riesgos de ciberseguridad relacionados permite a una organización enfocar y priorizar sus esfuerzos, de acuerdo con su estrategia de gestión de riesgos y sus necesidades comerciales. Gestionar el riesgo de ciberseguridad para los sistemas, las personas, los activos, los datos y las capacidades. Elaborar y compartir una política de ciberseguridad que contengan, entre otros, las funciones y responsabilidades de los empleados, proveedores y todo aquel que tenga acceso a datos críticos o sensibles, así como las acciones a ejecutar para protegerse frente a un ataque o limitar el daño si se produce uno.

- **Proteger:** Implementar los controles adecuados para garantizar la prestación de servicios críticos. Hacer uso de las buenas prácticas desarrolladas por otros estándares como los ISO/IEC 27001, 27002 del 2013 y el 27032:2012 [93], el cual define las directrices de la ciberseguridad.

- **Detectar:** Desarrollar e implementar las actividades apropiadas para identificar la ocurrencia de un evento de ciberseguridad a través de la monitorización continua.

- **Responder:** Permite la definición y despliegue de actividades para reaccionar frente a un evento de ciberseguridad identificado y mitigar su impacto.

- **Recuperar:** Desarrollar e implementar actividades apropiadas para mantener planes de resiliencia y restaurar cualquier capacidad o servicio que se haya visto afectado debido a un incidente de ciberseguridad. La función de recuperación admite la recuperación oportuna de las operaciones normales para reducir el impacto de un incidente de ciberseguridad.

El desarrollo y puesta en práctica de estas funciones llevará a una cadena, y abultada cantidad, de acciones tanto tecnológicas como de gestión.

Estas funciones debieran enmarcarse en un sistema de gestión de seguridad de la información que incluya las particularidades de la ciberseguridad, dirigido y supervisado por el cuerpo de gobierno de la organización.

Dicho sistema debiera contar con una política de seguridad de la información corporativa, con el intercambio de información entre los Equipos de Respuesta ante Ciberincidentes (*CERT*), con procesos de gestión de los recursos humanos, con la asignación de responsabilidades, con planes de continuidad del negocio y con la gestión del cumplimiento de la legislación, regulaciones y normativas externas e internas vigentes.

El gobierno de cada país debiera fomentar la actualización de la legislación respecto de la ciberseguridad, crear los organismos necesarios, y dotarlos de recursos, para la aplicación de las leyes y el control de las IC, así como el trabajo conjunto con otros países para proteger estas infraestructuras que son las que brindan los servicios básicos y esenciales a sus ciudadanos y cuya interrupción acarrea peligrosas consecuencias para la sociedad.

CAPÍTULO 4. Conclusiones

Según indican las empresas de seguridad de la información a nivel mundial, los ciberataques a las IC aumentan año a año, siendo los más habituales los producidos por *ransomware*, *phishing*, denegación de servicio y ataque por *malware*.

También surge de dicha información que los sectores más atacados en el año 2020 fueron los de energía, logística y automoción.

De algunas encuestas se desprende que más de la mitad de los operadores de IC reconocen haber sufrido ciberataques.

Por lo tanto, el panorama se presenta más complejo día a día.

Países como EE.UU, Australia, Reino Unido, algunos de la Unión Europea y otros de Asia, a través de los años han sido víctimas de ciberataques en sus sectores críticos de forma frecuente, por ello se han visto obligados a acelerar su preparación y protección frente a estos tipos de ataque.

En cuanto a los países latinoamericanos, si bien los ciberataques han ocurrido con menor periodicidad, criticidad y cantidad de consecuencias han ido mejorando la tecnología y sus procesos de seguridad con el fin de contar con un escenario más sólido, estructurado y estable.

En marzo de 2019 la Unión Europea adoptó un nuevo protocolo de respuesta de emergencia a los ciberataques. Dice la Oficina Europea de Policía que el protocolo sirve “como una herramienta para ayudar a las autoridades policiales de la UE a proporcionar una respuesta inmediata a los principales ciberataques transfronterizos a través de una evaluación rápida, el intercambio seguro y oportuno de información crítica y la coordinación efectiva de los aspectos internacionales de sus investigaciones”.

Seguramente cada país o comunidad de países tendrá que comenzar a delinear, o a reforzar en todo caso, las acciones tendientes a proteger sus infraestructuras críticas frente a amenazas cada vez más complejas y variables.

GLOSARIO DE TERMINOS

Activo de información: conocimiento o datos que tienen un valor para un individuo u organización.

Activo físico: activo que tiene una existencia tangible o material.

Algoritmo: proceso matemático claramente especificado para el cálculo; un conjunto de reglas que, si se siguen, darán un resultado prescrito.

Aplicación Web: es una herramienta en la que un usuario puede acceder a un servidor web a través de internet o de una intranet mediante un navegador.

A

Amenaza: es toda acción que aprovecha una vulnerabilidad para atentar contra la seguridad de un sistema de información.

Adware: es un tipo de software dañino que bombardea la computadora o dispositivo móvil con incesantes anuncios emergentes.

Awareness (Concientización): es capacitar a los usuarios con programas de sensibilización sobre la seguridad de la información y enseñarles a tomar conciencia sobre cómo proteger sus sistemas informáticos.

Backend: es la parte del desarrollo web que se encarga de que toda la lógica de una página web funcione.

Backdoor (Puerta Trasera): es un tipo de troyano que permite el acceso al sistema infectado y tomar el control remoto. El atacante puede entonces eliminar o modificar archivos, ejecutar programas, enviar correos masivamente o instalar herramientas maliciosas.

B

Bitcoin: Es un tipo de dinero completamente virtual, es una versión online de las monedas o billetes tradicionales y se puede usar para comprar productos y servicios.

B

Bot: es un software preparado para realizar tareas repetitivas a través de Internet como si fuese un humano y con cierta inteligencia de forma malicioso.

Botnet: es un conjunto o red de robots informáticos o *bots*, que se ejecutan de manera autónoma y automática. la botnet puede controlar todas las computadoras o servidores infectados de forma remota.

Ciberamenaza (Cyber-Threat): cualquier circunstancia o evento con el potencial de impactar negativamente las operaciones organizacionales (incluyendo misión, funciones, imagen o reputación), activos organizacionales, individuos, otras organizaciones o la Nación a través de un sistema de información a través del acceso no autorizado, destrucción, divulgación, modificación de información y / o denegación de servicio.

C

Ciberataque (Cyberspace-Attack): acciones del ciberespacio que crean varios efectos directos de negación (es decir, degradación, interrupción o destrucción) y manipulación que conduce a una negación que está oculta o que se manifiesta en los dominios físicos.

Ciberespacio (Cyber-Space*):* es un dominio global dentro del entorno de información que consiste en la red interdependiente de infraestructuras de sistemas de información que incluyen Internet, redes de telecomunicaciones, sistemas informáticos y procesadores y controladores integrados.

Ciberincidente (Cyber-Incident): son acciones tomadas a través del uso de un sistema o red de información que resultan en un efecto adverso real o potencial en un sistema de información, red y/o la información que reside en ellos.

Ciberresiliencia (Cyber-Resiliency): capacidad de anticipar, resistir, recuperarse y adaptarse a condiciones adversas, tensiones, ataques o compromisos en sistemas que usan o están habilitados por recursos cibernéticos.

Ciberseguridad (Cyber-Security): La capacidad de proteger o defender el uso del ciberespacio de los ataques cibernéticos.

CERT: es un equipo de personas dedicado a la implantación y gestión de medidas preventivas, reactivas y de gestión de la seguridad con el objetivo de mitigar el riesgo de ataques contra las redes y sistemas de la comunidad a la que se proporciona el servicio y ofrecer soluciones para la mitigación de cualquier incidente y sus efectos, en el menor tiempo posible.

C

Código PHP: es un lenguaje de código abierto muy popular especialmente adecuado para el desarrollo web y que puede ser incrustado en HTML.

Código HTTP: Los códigos de estado de respuesta HTTP indican si se ha completado satisfactoriamente una solicitud HTTP específica.

Código HTTP: Los códigos de estado de respuesta HTTP indican si se ha completado satisfactoriamente una solicitud HTTP específica.

Colisión: es un evento en el que dos mensajes diferentes tienen el mismo resumen de mensajes.

C

Confidencialidad: la información no está a disposición ni debe ser revelada a ciertos individuos, entidades o procesos que no se encuentren autorizados.

Código Fuente: al conjunto de líneas de texto que expresan, en un lenguaje de programación determinado, los pasos que debe seguir el computador para la correcta ejecución de un programa específico.

Cookies: es la información proporcionada por un servidor web a un navegador, en respuesta a un recurso solicitado, para que el navegador la almacene temporalmente y vuelva al servidor en cualquier visita o solicitud posterior.

CSIRT: es un grupo de expertos responsables del desarrollo de medidas preventivas y reactivas ante incidencias de seguridad en los sistemas de información.

D

Denegación de servicio: su objetivo de este ataque es degradar la calidad de un servicio, por ejemplo, una página web, y dejarlo en un estado no funcional. Para lograrlo, se saturan los recursos del sistema que aloja el servicio que se quiere interrumpir, enviándoles una avalancha de peticiones que no son capaces de atender.

Denegación de servicio distribuido: estos ataques son intentos maliciosos para conseguir que un sitio web o una aplicación web no estén disponibles para los usuarios saturando el sitio con una enorme cantidad de tráfico, lo que provocará que se bloquee o funcione de forma muy lenta.

Disponibilidad: garantizar el acceso oportuno y confiable y el uso de la información.

E

Exploit: es un código que se aprovecha de una vulnerabilidad de software o una falla de seguridad, Los exploits permiten que un intruso acceda de forma remota a una red y obtenga privilegios elevados o se adentre más en la red.

Firma Digital es un mecanismo criptográfico que permite al receptor de un mensaje firmado digitalmente determinar la entidad originadora de dicho mensaje (autenticación de origen y no repudio) y confirmar que el mensaje no ha sido alterado desde que fue firmado por el originador (integridad).

F

Firma Electrónica: es el conjunto de datos electrónicos integrados, ligados o asociados de manera lógica a otros datos electrónicos, utilizado por el signatario como su medio de identificación, que carezca de alguno de los requisitos legales para ser considerada firma digital. En caso de ser desconocida la firma electrónica corresponde a quien la invoca acreditar su validez

Función Hash: función criptográfica hash es un algoritmo matemático que transforma cualquier bloque arbitrario de datos en una nueva serie de caracteres con una longitud fija. Independientemente de la longitud de los datos de entrada, el valor hash de salida tendrá siempre la misma longitud.

G

Grooming: es la acción deliberada de un adulto de acosar sexualmente a un niño, niña o adolescente mediante el uso de Internet, a través de comunicaciones electrónicas, telecomunicaciones o cualquier otra tecnología de transmisión de datos (redes sociales, páginas web, aplicaciones de mensajerías como WhatsApp, Facebook, Instagram etc.)

H

Hacker (Pirata informático, Atacante, Cibercriminal): es un usuario no autorizado que intenta u obtiene acceso a un sistema de información.

Hacktivistas: son personas que usan técnicas informáticas para luchar por una causa especifica. Los hacktivistas buscan protestas y actos políticos a través de la irrupción, legal e ilegal, a sistemas informáticos para la difusión de información.

Handshake: Protocolo de diálogo entre dos sistemas para identificarse y autenticarse entre sí, o para sincronizar sus operaciones entre sí.

H

Hash: es una cadena de texto codificada, formada por número y letras de longitud fija y en un orden único e irrepetible que representan a una serie de datos.

Host (Anfitrión): se refiere a las computadoras u otros dispositivos móviles que se encuentran conectados a una red que provee servicios de la maquina host.

I

ICMP: es un protocolo de mensajes de control de internet y permite administrar información relacionada con errores a través de la generación y envío de mensajes a la dirección IP de origen cuando hay problemas de red que son encontrados por el sistema.

Infraestructuras Críticas: son aquellos sistemas físicos y virtuales que proporcionan funciones y servicios esenciales para dar respaldo a los sistemas sociales, económicos y ambientales de un país de esta forma no permite soluciones alternativas, por lo que su perturbación o destrucción tendría un grave impacto sobre los servicios esenciales.

Infraestructuras Críticas de la información: son aquellas tecnologías, instalaciones, servicios, redes, información y equipos físicos esenciales para las funciones sociales vitales como la salud, la seguridad, el bienestar social y la economía de los ciudadanos de un país.

Ingeniería Social: es un conjunto de técnicas que usan los cibercriminales para engañar a los usuarios ingenuos para que les envíen datos confidenciales, infecten sus computadoras con malware o abran enlaces que los redirigen a sitios infectados.

I	**Integridad:** es protegerse contra la modificación o destrucción indebida de la información, e incluye garantizar el no repudio y la autenticidad de la información.
J	**Java script (JS):** es un lenguaje de programación orientado a objetos. se utiliza principalmente del lado del cliente, implementado como parte de un navegador web permitiendo mejoras en la interfaz de usuario y páginas webs dinámicas.
L	**Linux:** Es un sistema operativo open source con una plataforma de infraestructura de TI, debido a que Linux es de fuente abierta tiene licencia de uso público, lo que significa que todos pueden ejecutar, estudiar, compartir y modificar el software. El código modificado también se puede redistribuir e incluso vender, pero todo esto se debe hacer con la misma licencia.
M	**Malware (programa malicioso):** es un software diseñado para causarle daño una computadora, a los dispositivos móviles o cualquier información almacenada en los equipos. **MYSQL:** es un sistema de gestión de bases de datos relacionales de código abierto con un modelo cliente-servidor.
O	**Oracle:** es una herramienta para la gestión de bases de datos, usada principalmente poder controlar y gestionar una gran cantidad de contenidos desde un solo archivo.
P	**PLC (Programmable Logic Controller):** es un controlador lógico programable o un equipo electrónico programable en lenguaje no informático, diseñado para controlar en tiempo real y en ambiente de tipo industrial, procesos secuenciales.

R

Ransomware (Secuestro de datos): es un programa de software malicioso que infecta la computadora y muestra mensajes que exigen el pago de dinero para restablecer el funcionamiento del sistema. El ransomware tiene la capacidad de bloquear la pantalla de una computadora o cifrar archivos importantes predeterminados con una contraseña.

Rootkit: es un conjunto de herramientas usadas por los atacantes que consiguen acceder ilícitamente a un sistema informático. Estas herramientas sirven para esconder los procesos y archivos que permiten al intruso mantener el acceso al sistema, la mayoría de las veces se hace con fines delictivos.

S

SCADA (Control de supervisión y adquisición de datos): son sistemas que tienen como finalidad supervisar y controlar remotamente una instalación, pudiendo integrar datos recogidos desde diferentes sensores autómatas como PLCs y equipos mediante diferentes protocolos en un solo lugar.

SQL (Structured Query Language): Lenguaje de consulta estructurada, es un lenguaje de base de datos estándar la cual se utiliza para crear, mantener y recuperar la base de datos relacional.

Software: son programas informáticos y datos asociados que pueden escribirse o modificarse dinámicamente durante la ejecución.

Sistema Operativo: es el software principal o conjunto de programas de un sistema informático que gestiona los recursos de hardware y provee servicios a los programas de aplicación de software, ejecutándose en modo privilegiado respecto de los restantes.

Script: es una secuencia de instrucciones, que van desde una simple lista de comandos del sistema operativo hasta declaraciones completas del lenguaje de programación, que un intérprete puede ejecutar automáticamente.

S

Spyware (Software espía): es un software que se instala de forma secreta en un sistema informático para recopilar información sobre personas u organizaciones sin su conocimiento, es un tipo de código malicioso.

Spam (Correo no deseado): es un correo electrónico basura o abuso de sistemas de mensajería electrónica para enviar indiscriminadamente mensajes masivos no solicitados.

Target: es el objetivo en el cual se realizará el ataque (puede ser la información, las computadoras, las redes, etc.)

TIC (Tecnologías de Información y Telecomunicaciones): son todos aquellos recursos, herramientas y programas que se utilizan para procesar, administrar y compartir la información mediante diversos soportes tecnológicos, tales como: computadoras,

T

celulares, televisores, reproductores portátiles de audio y video o consolas de juego, etc.

Troyano (Caballo de Troya o Troyano): es un programa informático que parece tener una función útil, pero también tiene una función oculta y potencialmente maliciosa que evade los mecanismos de seguridad, a veces mediante la explotación de autorizaciones legítimas de una entidad del sistema que invoca el programa.

U	**Unix:** es un sistema operativo multiusuario y multitarea, cuenta con un conjunto de programas bastante amplio y va enfocado a compilar en lenguaje de programación, comunicación por correos electrónicos, comunicaciones telefónicas, conexión a redes y su acceso, editar texto, interpretar comandos, manejar archivos.
V	**Vulnerabilidad:** es la debilidad en un sistema de información, por ejemplo, procedimientos de seguridad del sistema, controles internos o implementación que podrían ser explotados o desencadenados por una fuente de amenaza.
W	**Windows:** es un sistema operativo que facilita la administración de los recursos de una computadora, puede gestionar todos los componentes hardware y software. El sistema operativo es un intermediario entre el usuario y el hardware, ya que el sistema es quien permite el acceso a los recursos y periféricos, así como también asegura su correcto funcionamiento y asigna la cantidad de memoria respectiva en función de sus necesidades.

ANEXOS

ANEXO 1 – Infraestructuras Criticas según el Homeland Security en Estados Unidos

CISA (Cybersecurity & Infrastructure Security Agency)

CISA es la Dirección de Ciberseguridad de los Estados Unidos, es el asesor de riesgos de la nación, trabaja con socios para defenderse de las amenazas del hoy y colabora para construir una infraestructura más segura y resistente para el futuro.

El papel de CISA en la ciberseguridad

El ciberespacio y su infraestructura subyacente son vulnerables a una amplia gama de riesgos derivados de amenazas y peligros tanto físicos como digitales. Los actores cibernéticos sofisticados y el estado-nación aprovechan las vulnerabilidades para robar información y dinero y están desarrollando capacidades para interrumpir, destruir o amenazar la prestación de servicios esenciales. El ciberespacio es particularmente difícil de proteger debido a una serie de factores: la capacidad de los actores malintencionados para operar desde cualquier parte del mundo, los vínculos entre el ciberespacio y los sistemas físicos, y la dificultad de reducir las vulnerabilidades y las consecuencias en las redes cibernéticas complejas. La creciente preocupación es la amenaza cibernética a la infraestructura crítica, que está cada vez más sujeta a intrusiones cibernéticas sofisticadas que plantean nuevos riesgos. A medida que la tecnología de la información se integra cada vez más con las operaciones de la infraestructura física, existe un mayor riesgo de eventos de gran escala o de grandes consecuencias que podrían dañar o interrumpir los servicios de los que depende nuestra economía y la vida diaria de millones de estadounidenses. A la luz del riesgo y las posibles consecuencias de los eventos cibernéticos, el fortalecimiento de la seguridad y la resiliencia del ciberespacio se ha convertido en una importante misión de seguridad nacional.

Servicios de ciberseguridad CISA

Los servicios de ciberseguridad que ofrece el CISA y su catálogo de servicios esta todo en un solo lugar: un recurso único que brinda a los usuarios acceso a información sobre servicios en todas las áreas de misión de CISA que están disponibles para el gobierno federal; gobierno estatal, local, tribal y territorial; la Industria privada; Academia; ONG y organizaciones sin fines de lucro y partes interesadas del público en general. Como parte del Plan Nacional de Protección de Infraestructura, los socios del sector público y privado en cada uno de los 16 sectores de infraestructura crítica y la comunidad de gobierno estatal, local, tribal y territorial han desarrollado un Plan Sectorial Específico que se enfoca en las condiciones operativas únicas y panorama de riesgo dentro de ese sector. Desarrollados en estrecha colaboración con agencias federales y socios del sector privado, los planes específicos del sector se actualizan cada cuatro años para garantizar que cada sector se adapte al panorama de riesgos en constante evolución.

Los planes sectoriales de 2015 establecen metas y prioridades para el sector que abordan su entorno de riesgo actual, como el nexo entre la ciberseguridad y la seguridad física y la interdependencia entre varios sectores, riesgos asociados con el cambio climático, la infraestructura obsoleta y envejecida y la necesidad de asegurar la continuidad en una fuerza laboral que se acerca rápidamente a la jubilación.

Estos sectores que representan aspectos clave de la seguridad económica y física nacional, incluyen servicios de los que las personas dependen todos los días, tales como el transporte, las comunicaciones, la energía, el agua, los alimentos y la agricultura, los químicos, los financieros, la atención médica y otros servicios esenciales que sostienen la vitalidad económica y alto nivel de vida para los estadounidenses.

Las empresas y los socios gubernamentales en cada sector de infraestructura crítica pueden usar su respectivo **Plan Específico del Sector 2015** para desarrollar caminos individuales a medida que abordan desafíos de seguridad y construyen resiliencia dentro de las perspectivas, prioridades y recursos únicos de gestión de riesgos distintos de su sector.

Los planes también sugieren formas para desarrollar métricas significativas donde los sectores puedan medir su progreso a medida que optimizan la seguridad y la resistencia de su infraestructura crítica.

Al aplicar las acciones descritas en los planes, los participantes del sector deberían poder crear productos y herramientas que respalden las jurisdicciones locales y regionales donde se ubican las instalaciones y los sistemas y se llevan a cabo los eventos. Los planes también proporcionan un lenguaje y una taxonomía comunes, así como una mirada a ejemplos prometedores de cómo la coordinación y otras actividades a nivel nacional pueden ser aplicables a los niveles local y regional.

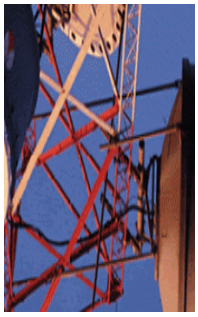
CISA trabaja con empresas, comunidades y gobiernos de todos los niveles para ayudar a que la infraestructura crítica de la nación sea más resistente a las amenazas físicas y cibernéticas. Todos tienen un papel en la protección de la infraestructura crítica de la nación. Es importante tener en cuenta que este Plan Específico de cada Sector citado a continuación es el Plan Nacional de Protección de Infraestructura (NIPP) de 2010 y se actualizó en el 2015**.**

Hay 16 sectores de infraestructura crítica "*cuyos activos, sistemas y redes, ya sean físicos o virtuales, se consideran tan vitales para los Estados Unidos que su incapacitación o destrucción tendría un efecto debilitante en la seguridad, la seguridad económica nacional, la salud pública o la seguridad nacional o cualquier combinación de los mismos*".

De acuerdo a la Directiva de Política Presidencial 21 (PPD-21) la seguridad y resiliencia de la infraestructura crítica promueve una política nacional para fortalecer y mantener una infraestructura crítica segura, funcional y resistente. Esta directiva reemplaza a la Directiva presidencial 7 de Seguridad Nacional.

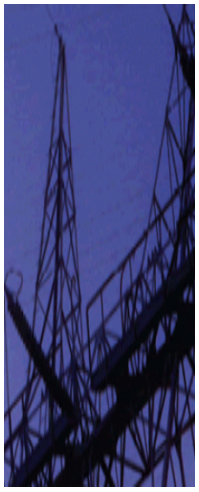
En el siguiente cuadro, se puede ver a detalle de que consta cada sector perteneciente a las Infraestructuras Criticas de los Estados Unidos con sus respectivos departamentos o agencias a los que pertenecen:

	SECTOR	DETALLE	DEPAR-TAMENTO
1	**Quimico** 	El sector químico es un componente integral de la economía de los EE UU que fabrica, almacena, utiliza y transporta productos químicos potencialmente peligrosos de los que depende una amplia gama de otros sectores de infraestructura crítica, ademas de proteger estos productos químicos contra amenazas crecientes y en evolución requiere la vigilancia tanto del sector público como del privado.	Seguridad Nacional
2	**Instalaciones Comerciales** 	Este sector incluye una amplia gama de sitios que atraen a grandes multitudes de personas para realizar compras, negocios, entretenimiento o alojamiento. Las instalaciones dentro del sector operan según el principio de acceso público abierto lo que significa que el público en general puede moverse libremente sin la disuasión de barreras de seguridad muy visibles. La mayoría de estas instalaciones son de propiedad y operación privadas con una interacción mínima con el gobierno federal y otras entidades reguladoras.	Seguridad Nacional

	SECTOR	DETALLE	DEPAR-TAMENTO
3	**Comunicaciones** 	El sector privado como propietario y operador de la mayoría de la infraestructura de comunicaciones, es la entidad principal responsable de proteger la infraestructura y los activos del sector. Al trabajar con el gobierno federal, el sector privado puede predecir, anticipar y responder a las interrupciones del sector y comprender cómo podrían afectar la capacidad del liderazgo nacional para comunicarse durante tiempos de crisis, impactar las operaciones de otros sectores y afectar la respuesta y esfuerzos de recuperación.	Seguridad Nacional
4	**Manufacturero Critico** 	El sector manufacturero crítico es crucial para la prosperidad económica y la continuidad de los EE UU el sector de fabricación crítica se centra en la identificación, evaluación, priorización y protección de las industrias manufactureras de importancia nacional dentro del sector que pueden ser susceptibles a desastres naturales y provocados por el hombre.	Seguridad Nacional

	SECTOR	DETALLE	DEPAR-TAMENTO
5	**Represas** 	El Sector de Represas brinda servicios críticos de retención y control de agua en los EE UU que incluyen generación de energía hidroeléctrica, suministros de agua municipales e industriales, riego agrícola, control de sedimentos e inundaciones, navegación fluvial para el transporte terrestre de graneles, manejo de desechos industriales y recreación. Sus servicios clave dan soporte a múltiples sectores e industrias de infraestructura crítica**.**	Seguridad Nacional
6	**Base Industrial de Defensa** 	El Sector de base industrial de defensa es el complejo industrial mundial que permite la investigación y el desarrollo, así como el diseño, la producción, la entrega y el mantenimiento de sistemas, subsistemas y componentes o piezas de armas militares para cumplir con los requisitos militares de EE. UU El sector proporciona productos y servicios que son esenciales para movilizar, desplegar y sostener operaciones militares. El Sector de Base Industrial de Defensa no incluye la infraestructura comercial de proveedores de servicios tales como energía, comunicaciones, transporte o servicios públicos que el Departamento de Defensa utiliza para cumplir con los requisitos operativos militares.	Defensa

	SECTOR	DETALLE	DEPAR-TAMENTO
7	**Servicios de Emergencia** 	El Sector de Servicios de Emergencia (ESS) es una comunidad de millones de personal altamente calificado y capacitado, junto con los recursos físicos y cibernéticos, que brindan una amplia gama de servicios de prevención, preparación, respuesta y recuperación durante el día a día operaciones y respuesta a incidentes. El *ESS* incluye instalaciones y equipos distribuidos geográficamente en capacidades pagadas y voluntarias, organizadas principalmente en niveles del gobierno federal, estatal, local, tribal y territorial, tales como Departamentos de Policía de la Ciudad y Estaciones de Bomberos, Oficinas del Alguacil del Condado, Policía del Departamento de Defensa y Departamentos de obras públicas de la ciudad. El ESS también incluye recursos del sector privado, como departamentos de bomberos industriales, organizaciones de seguridad privada y proveedores privados de servicios médicos de emergencia.	Seguridad Nacional

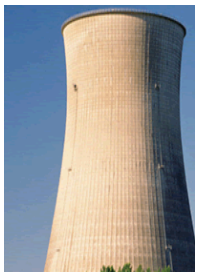
	SECTOR	DETALLE	DEPAR-TAMENTO
8	**Energia** 	La infraestructura energética de EE UU impulsa la economía del siglo XXI. Sin un suministro de energía estable, la salud y el bienestar se ven amenazados y la economía estadounidense no puede funcionar. *La Directiva PPD-21*, identifica al sector energético como **excepcionalmente crítico** porque proporciona una **"Función Habilitadora"** en todos los sectores de infraestructura crítica. Más del 80% de la infraestructura energética del país es propiedad del sector privado, que suministra combustibles a la industria del transporte, electricidad a hogares y empresas y otras fuentes de energía que son parte integral del crecimiento y la producción en todo el país. La infraestructura energética se divide en tres segmentos interrelacionados que son: Electricidad, Petróleo y Gas Natural.	Energia

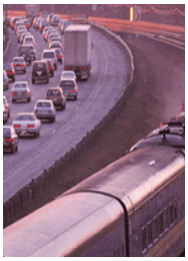
	SECTOR	DETALLE	DEPAR-TAMENTO
9	**Servicios Financieros** 	El Sector de Servicios Financieros representa un componente vital de la infraestructura crítica de EE UU los cortes de energía a gran escala, los desastres naturales y el aumento en el número y sofisticación de los ciberataques demuestran la amplia gama de riesgos potenciales que enfrenta el sector. Este sector incluye miles de instituciones de depósitos, proveedores de productos de inversión, compañías de seguros, otras organizaciones crediticias y financieras, proveedores de servicios y utilidades financieras críticas que respaldan estas funciones.	Tesoro
10	**Agroalimentario** 	El sector de la alimentación y la agricultura es casi en su totalidad de propiedad privada y se compone de aproximadamente 2,1 millones de granjas, 935.000 restaurantes y más de 200.000 instalaciones registradas de fabricación, procesamiento y almacenamiento de alimentos. Este sector representa aproximadamente una quinta parte de la actividad económica del país y tiene dependencias críticas con los siguientes sectores: Sistemas de agua y Aguas Residuales, Sistemas de Transporte, Energía y Químico.	Agricultura y Salud y Servicios Humanos

	SECTOR	DETALLE	DEPAR-TAMENTO
11	**Instalaciones Gubernamentales** 	El Sector de Instalaciones Gubernamentales incluye una amplia variedad de edificios, ubicados en los EE UU y en el extranjero, que son propiedad o están alquilados por gobiernos federales, estatales, locales y tribales. Muchas instalaciones gubernamentales están abiertas al público para actividades comerciales, transacciones comerciales o actividades recreativas, mientras que otras que no están abiertas al público ya que contienen información, materiales, procesos y equipos altamente sensibles. Estas instalaciones incluyen edificios de oficinas de uso general e instalaciones militares de uso especial, embajadas, juzgados, laboratorios nacionales y estructuras que pueden albergar equipos, sistemas, redes y funciones críticas. Además de las estructuras físicas, el sector incluye elementos cibernéticos que contribuyen a la protección de los activos del sector.	Seguridad Nacional y Administración de Servicios Generales

	SECTOR	DETALLE	DEPAR-TAMENTO
12	**Sanitario y Salud Publica** 	Este sector protege a todos los sectores de la economía de peligros como el terrorismo, brotes de enfermedades infecciosas y desastres naturales. Debido a que la gran mayoría de los activos del sector son de propiedad y operación privada, la colaboración y el intercambio de información entre los sectores público y privado es esencial para aumentar la resiliencia de la infraestructura crítica de atención médica y salud pública del país. Con operaciones en todos los estados, territorios y áreas tribales de EE UU. El sector juega un papel importante en la respuesta y recuperación en todos los demás sectores en caso de un desastre natural o provocado por el hombre. Si bien la atención médica tiende a brindarse y administrarse localmente, el componente de salud pública del sector, centrado principalmente en la salud de la población, se administra en todos los niveles de gobierno: nacional, estatal, regional, local, tribal. El Sector de la Salud Salud Pública y depende de los demás sectores de la continuidad de las operaciones y la prestación de servicios, incluidos altamente	Salud y Servicios Humanos

	SECTOR	DETALLE	DEPAR-TAMENTO
		Comunicaciones, Servicios de Emergencia, Energía, Agricultura y la Alimentación, Tecnología de la Información, Sistemas de Transporte y Sistemas de Agua y Aguas Residuales.	
13	**Tecnologias de información** 	El sector de Tecnología de la Información es fundamental para la seguridad, la economía y la salud pública y la seguridad de la nación, ya que las empresas, los gobiernos, el mundo académico y los ciudadanos dependen cada vez más de las funciones del sector de tecnología de la información. Estas funciones virtuales y distribuidas producen y proporcionan Hardware, Software y Sistemas y Servicios de tecnología de la información y en colaboración con el sector de Comunicaciones e Internet. El entorno complejo y dinámico del sector dificulta la identificación de amenazas y la evaluación de vulnerabilidades y requiere que estas tareas se aborden de manera colaborativa y creativa.	Seguridad Nacional

	SECTOR	DETALLE	DEPAR-TAMENTO
		Las funciones del Sector de Tecnología de la Información son operadas por una combinación de entidades a menudo propietarios y operadores y sus respectivas asociaciones, que mantienen y reconstituyen la red, incluida Internet. Si bien la infraestructura de tecnología de la información tiene un cierto nivel de resiliencia inherente, su estructura interdependiente e interconectada presenta desafíos y oportunidades para coordinar las actividades de preparación y protección de los sectores público y privado.	
14	**Reactores Nucleares, Materiales y Desechos** 	Desde los reactores de potencia que proporcionan electricidad a millones de estadounidenses hasta los isótopos médicos utilizados para tratar a los pacientes con cáncer, el sector de reactores nucleares, materiales y desechos cubre la mayoría de los aspectos de la infraestructura nuclear civil de EE UU.	Seguridad Nacional

	SECTOR	DETALLE	DEPAR-TAMENTO
15	**Sistemas de Transporte** 	El sistema de transporte de la nación mueve personas y mercancías de manera rápida y segura a través del país y hacia el extranjero. El sector de sistemas de transporte consta de siete subsectores: Aereo, Terrestre, Marítimo, Ferroviario, Sistemas de Tuberías, Trenes de carga, y Mensajeria.	Seguridad Nacional y Transporte
16	**Sector de Agua y Aguas Residuales** 	El agua potable es un requisito previo para proteger la salud pública y toda la actividad humana. Las aguas residuales tratadas adecuadamente son vitales para prevenir enfermedades y proteger el medio ambiente. Por lo tanto, asegurar el suministro de agua potable y tratamiento y servicio de aguas residuales es fundamental para la vida moderna y la economía de la Nación.	Agencia de proteccion ambiental

ANEXO 2 – Ciberataque de Denegación de Servicio Distribuido a Estonia

Las estatuas de bronce simbolizan mucho para los rusos, ya que tenían un significado representativo para aquellos que fueron "Liberados" pero ese significado era algo completamente diferente. Las estatuas, los muertos y los cuerpos de los soldados del **Ejército Rojo** debajo de ellos eran alegóricamente pararrayos. En Tallin, la estatua también atrajo relámpagos cibernéticos. Las tensiones entre los rusos étnicos que vivían en Estonia y los propios estonios nativos habían sido una construcción desde que la pequeña nación había vuelto a declarar su independencia al final de la Guerra Fría. La mayoría de los estonios trataron de eliminar cualquier símbolo de las cinco décadas opresivas durante las cuales se había visto obligado a formar parte de la Unión Soviética.

En **febrero del 2007,** la legislatura aprobó una Ley de Estructuras Prohibidas que hubiera provocado la eliminación de cualquier cosa que denotara la ocupación, incluyendo el soldado de bronce gigante. Los estonios todavía estaban resentidos por la profanación de las tumbas de sus propios veteranos que habían seguido la aparición del Ejército Rojo. Moscú se quejó de mover al soldado de bronce y difamaría a los heroicos muertos soviéticos, incluidos los enterrados alrededor del gigante de bronce. Buscando evitar un incidente, el Presidente de Estonia vetó la ley, pero la presión pública para quitar la estatua creció, al igual que un grupo étnico ruso dedicado a proteger el monumento y un grupo nacionalista estonio que amenaza con destruirlo se volvió cada vez más militante. A medida que el invierno báltico se convirtió en primavera, la política se trasladó a la calle.

En **abril del 2007,** ahora conocido como Bronze Night (Noche de Bronce), estalló un motín entre radicales de ambas facciones étnicas, con la policía y la estatua atrapadas en el medio. Las autoridades intervinieron rápidamente y trasladó la estatua a una nueva ubicación protegida en el cementerio militar.

Lejos de sofocar la disputa, la medida encendió respuestas nacionalistas indignadas en los medios de comunicación de Moscú y en la legislatura de Rusia. Fue entonces cuando el ***conflicto se trasladó al ciberespacio***. Estonia, curiosamente, es una de las naciones más conectadas en el mundo, ubicándose, junto con Corea del Sur muy por delante de Estados Unidos en el alcance de su penetración de la banda ancha y su utilización de aplicaciones de Internet en la vida cotidiana. Esos avances lo convirtieron en un objetivo perfecto para ataques cibernéticos.

Después de la *Bronze Night*, de repente, las luces se apagan, las líneas de comunicación se quedan en silencio, se pierden las conexiones a Internet, los estonios no podían utilizar su banca en línea, los sitios web de los periódicos o los servicios electrónicos de su gobierno no respondían, las personas que se aventuran en las calles congestionadas descubren que los bancos están cerrados, los cajeros automáticos no funcionan correctamente, los semáforos están atascados, las estaciones de radio y televisión no pueden transmitir, los aeropuertos y estaciones de tren están cerrados, la producción de alimentos se detiene y el suministro de agua comienza a disminuir rápidamente a medida que las bombas dejan de funcionar, los saqueadores están alborotados, el pánico se apodera del público, la policía no puede mantener el orden.

Los servidores que soportan las páginas web que se utilizan con frecuencia en Estonia se inundaron con solicitudes de acceso cibernético, tan inundadas que algunas de los servidores colapsaron bajo la carga y se apagaron. Otros servidores estaban tan atascados con hacer ping que eran esencialmente inaccesibles.

Lo que había afectado a Estonia era un **DDoS**, un ataque ***Distribuido de Denegación de Servicio***, básicamente este tipo de ataque es una inundación pre-programada de tráfico de Internet diseñada para colapsar o bloquear redes, se distribuye en cientos de miles de computadoras que están comprometidas al hacer ping a un puñado de ubicaciones específicas en Internet. Las computadoras atacantes se denominan "Botnet" una red robótica de "Zombies", las computadoras que están bajo control remoto.

Los zombies atacantes estaban siguiendo instrucciones que se les habían cargado sin el conocimiento de sus dueños. En efecto, los propietarios por lo general ni siquiera pueden saber cuándo sus computadoras se han convertido en zombies o están involucrados en un ataque de DDOS. Un usuario puede notar que la computadora portátil funciona un poco lenta o que el acceso a las páginas web es tardando un poco más de lo normal, pero ese es el único indicador. La actividad maliciosa está funcionando en segundo plano y tratando de no aparecer en la pantalla del usuario.

Lo que ha sucedido, a menudo semanas o meses antes de que una botnet pasara a la ofensiva, es que el usuario de la computadora fue a una página web de apariencia inocente y esa página descargó en secreto el software que convirtió su computadora en un zombi o se abrió un correo electrónico, quizá alguien que conocía y descargó el software zombie; A veces, la computadora zombi espera pacientemente órdenes, otras veces empieza a buscar otras computadoras para atacar, cuando una computadora transmite su infección a otras y ellas a su vez tienen el fenómeno conocido como un "Gusano", la infección se propaga desde una computadora a través de miles a millones. Una infección puede extenderse por todo el mundo en cuestión de horas.

En Estonia, “El **DDoS** fue el más grande jamás visto” parecía que varias botnets diferentes cada una con decenas de miles de máquinas infectadas habían estado durmiendo y ahora estaban en funcionamiento. Al principio, los estonios pensaron que la eliminación de algunas de sus páginas web era solo una molestia que se les envió de los rusos indignados. Luego, las botnets comenzaron a apuntar a direcciones de los servidores que se ejecutaban en partes del teléfono, en la red, en el sistema de verificación de tarjetas de crédito y en el directorio de Internet.

Cientos de sitios clave en el país fueron atacados semana tras semana, sin poder volver a levantarse, mientras los expertos en seguridad de Internet viajaban hacia Tallin (*Capital de Estonia*) desde Europa y América del Norte, Estonia llevó el asunto ante el Consejo del Atlántico Norte, el máximo órgano de la alianza militar de la OTAN, los equipos de respuesta a cargo de analizar el incidente concluyeron que las maquinas zombies se adaptaron y probablemente fueron reprogramadas por la computadora maestro.

Estonia afirmó que el máximo control de las máquinas estaba en Rusia y que el código de la computadora involucrada había sido escrito en alfabeto cirílico (ruso). El gobierno ruso negó indignado que estuviera involucrado en una guerra cibernética contra Estonia y rechazó la solicitud diplomática formal de Estonia de asistencia para localizar a los atacantes, aunque el acuerdo bilateral permanente requería que Moscú cooperara informando que los ataques habían sido rastreados, de regreso a Rusia algunos funcionarios del gobierno admitieron que tal vez habían sido los patrióticos los rusos, indignados por lo que había hecho Estonia y se estaban tomando el asunto en sus propias manos.

Desde entonces, el episodio ha sido denominado la ***"Primera Guerra Cibernética del mundo"***, porque fue la primera vez que se lanzó un ataque electrónico sostenido, generalizado y políticamente motivado para causar estragos en toda la infraestructura digital de un país. Hasta entonces la "Ciberseguridad" se había limitado en la práctica a lidiar con intrusiones de piratería limitadas y con objetivos específicos a menudo como parte de una operación clandestina, para investigar o interrumpir el comando militar y los sistemas de comunicaciones incluido el Pentágono.

Los países occidentales han dado los primeros pasos para implementar acuerdos atrasados que definen los ataques cibernéticos como un posible acto de guerra, construyendo defensas más sólidas y acordando protocolos para la cooperación aliada.

Una iniciativa clave ha sido la creación del **"Centro de Excelencia para la Ciberdefensa"** de la OTAN que se une a la lista de instalaciones de la alianza que desarrollan las mejores prácticas para tipos especiales de guerra; este centro estará ubicado en Estonia y otros países de la OTAN ya se comprometieron a participar.

La batalla para frustrar los ataques de Rusia fue liderada por un expolicía, *Hillar Aarelaid*, director del CERT de Estonia que había estado combatiendo el ciberdelito durante más de diez años cuando estalló esta batalla en Abril. En todo momento, estuvo en su puesto de comando del **CERT** todos los días al amanecer inspeccionaba los sistemas de TI del país para asegurarse de que estuvieran trabajando antes de que otros ciudadanos llegaran a sus oficinas, *Aarelaid* contaba con un pequeño grupo de amigos de la tecnología de la información de los sectores privado y gubernamental que trabajaron en estrecha colaboración durante tres semanas, al pasar de los años habían formado una estrecha red social, frecuentando los mismos pubs y saunas familiares, durante la crisis, formaron un equipo de amigos que incluía a los principales expertos en seguridad cibernética de Estonia de los proveedores de servicios de Internet, medios de comunicación, bancos y agencias gubernamentales. Este grupo de talentos se fusionó en una fuerza informal de reacción rápida para contrarrestar los ataques.

A medida que se desarrolló la campaña por parte del equipo CERT de Estonia, con la ayuda de expertos internacionales, se diseñó y se implementó una respuesta estratégica de tres frentes:

- Reforzar rápidamente la capacidad del servidor del país.

- Encontrar formas de distinguir electrónicamente el tráfico de correo electrónico auténtico del "tráfico de ataque" zombi y evitar que llegue a los servidores de Estonia localizando y neutralizando a los bots y zombies.

- Contraatacar a los asaltantes, el apoyo decisivo provino de un cuadro de élite internacional de los mejores y más confiables técnicos en el sistema de gobierno de Internet.

En resumen, la guerra cibernética contra Estonia ofrece una visión inquietante del caos potencial y la devastación que podría sobrevenir a las naciones cuyos líderes no se anticipan ni se preparan para los ciberataques del futuro. Por cierto, también, los eventos ofrecen un recordatorio aleccionador de los métodos de mano dura que parecen gozar de una creciente influencia en Rusia, sin embargo, la consecuencia más profunda de la ***Primera Guerra Cibernética*** puede ser que los atacantes, tal vez sin darse cuenta, lanzaron una campaña de concienciación en Occidente, dando una llamada de atención a los gobiernos individuales y organizaciones internacionales por igual sobre las vulnerabilidades de sus infraestructuras esenciales.

ANEXO 3 – Ciberataque Stuxnet a IRAN y Sistemas SCADA

- Ciberataque Stuxnet a la planta Nuclear Iraní

Stuxnet fue un gusano descubierto por la Compañía de Seguridad de TI Bielorrusa llamada *VirusBlokAda,* el 17 de junio de 2010 este *malware* tuvo un papel central en lo que se considera el ciberataque más sofisticado de la historia una operación contra el Programa Nuclear de Natanz (Irán). A pesar de algunos inconvenientes en el ataque y unos pocos errores en el propio Stuxnet, se logró ralentizar el proceso de enriquecimiento de uranio en *Natanz*, una instalación nuclear iraní y eventualmente demorar el proceso de creación de armas nucleares por parte del país. Fue el primer gusano conocido que espía y reprograma sistemas industriales en concreto sistemas SCADA de control y monitorización de procesos, pudiendo afectar a infraestructuras críticas como *Centrales Nucleares*. Stuxnet es capaz de reprogramar controladores lógicos programables y ocultar los cambios realizados, también es el primer gusano conocido que incluye un Rootkit para sistemas reprogramables PLC, en el caso de Stuxnet, esta técnica fue capaz de camuflar su interferencia con la velocidad de rotación del motor de los sistemas de monitoreo. Los atacantes lograron que la presión en las centrífugas sea mucho más alta de lo normal.

Este gusano informático logró dañar físicamente 1.000 máquinas de la planta nuclear, este ataque se logró hacer por medio de cuatro pasos:

1) Stuxnet penetró en la red: Stuxnet llegó al programa nuclear de *Natanz* en una memoria USB infectada. Alguien habría tenido que insertar físicamente el USB a una computadora conectada a la red. El gusano penetró así en el sistema informático de la planta, para luego aprovechar otros agujeros y contaminar otros equipos con WinCC *(Sistema SCADA de Siemens)* conectados en red. Una vez lograda la entrada al sistema Stuxnet emplea las contraseñas por defecto para obtener el control.

2) El gusano se propagó a través de las computadoras: Una vez se está dentro del sistema informático, Stuxnet buscó el software que controla las máquinas llamadas centrifugadoras. Las centrífugas giran a altas velocidades para separar componentes. En la planta de *Natanz*, las centrifugadoras estaban separando los diferentes tipos de uranio, para aislar el uranio enriquecido que es fundamental tanto para la energía como para las armas nucleares. El gusano en sí mismo se propagó de manera indiscriminada a través de redes atacando equipos Windows explotando cuatro vulnerabilidades desconocidas, llamadas Zero-Day en ese sistema operativo, liberaba un payload especializado *(carga que se ejecuta en esa vulnerabilidad)* que apuntaba a sistemas SCADA específicos, el cual era capaces de reprogramar los dispositivos

3) Stuxnet reprogramó las centrifugadoras: El gusano encontró el software que controlaba las centrifugadoras y se insertó en él, tomando el control de las máquinas. En primer lugar, hizo que las centrifugadoras giraran peligrosamente rápido durante unos 15 minutos, antes de volver a la velocidad normal, aproximadamente un mes después, desaceleró las centrifugadoras durante unos 50 minutos. Esto se repitió en distintas ocasiones durante varios meses.

4) Destrucción de las máquinas: Con el tiempo, la tensión provocada por las velocidades excesivas causó que 1000 de las máquinas infectadas se desintegraran. Durante el ataque cibernético, alrededor del 20% de las centrifugadoras en la Planta de Natanz quedaron fuera de servicio. Es bien sabido que la operación Stuxnet dañó las centrífugas usadas en el proceso de enriquecimiento de uranio alterando la velocidad de su rotor. Las vibraciones y distorsiones causadas por cambios grandes y repentinos en la velocidad destruyeron. Como los iraníes no pudieron reemplazarlas rápidamente, terminaron produciendo menos uranio enriquecido que el que hubieran producido.

Antes de que los atacantes recurrieran a alterar la velocidad de las centrífugas, habían tratado de dañar sus rotores mediante sobrepresión.

Las centrifugadoras de gas para el enriquecimiento de uranio son extremadamente sensibles a la presión del proceso. Normalmente, operan bajo una presión cercana al vacío. Cualquier aumento disminuye la eficiencia del enriquecimiento y los aumentos mayores conducen a cambios en el proceso que pone una mayor tensión mecánica en el rotor.

- Sistemas SCADA (Supervisory Control and Data Acquisition)

→ *¿Qué es un sistema SCADA?*

El **sistema SCADA** es una herramienta de **Automatización y Control Industrial** utilizada en los procesos productivos que puede **controlar, supervisar, recopilar datos, analizar datos y generar informes** a distancia mediante una aplicación informática. Su principal función es la de evaluar los datos con el propósito de corregir posibles errores.

En consecuencia, su definición es la de una agrupación de aplicaciones informáticas instaladas en una computadora Máster o MTU, destinada al control automático de una actividad productiva a distancia que está interconectada con otros instrumentos llamados de campo como son los Controladores Lógicos Programables (PLCs) y las Unidades Terminales Remotas (RTUs).

Los sistemas SCADA se han convertido en la actualidad en elementos fundamentales en las *plantas industriales* ya que ayudan a mantener la eficiencia, procesan los datos para tomar decisiones más inteligentes y comunican los problemas del sistema para ayudar a disminuir el tiempo de parada o inactividad.

→ *¿Cuál es la función de un sistema SCADA?*

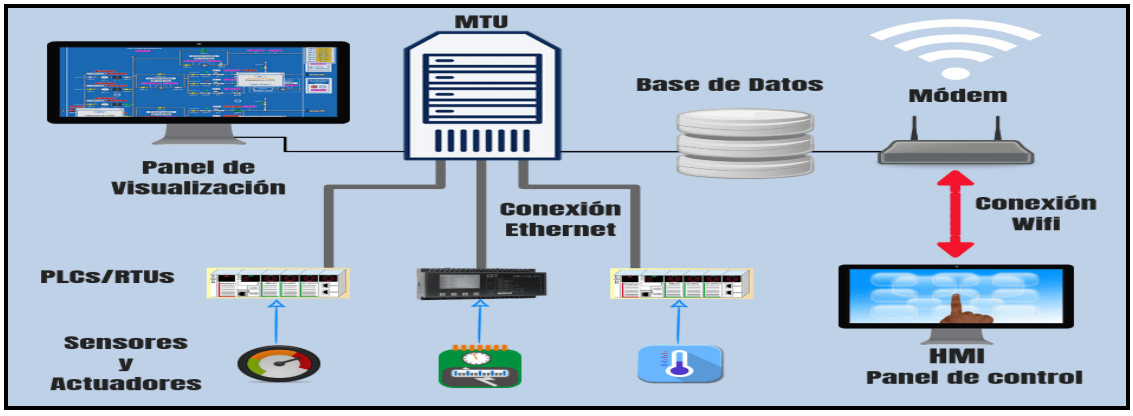
Es un **Sistema de Control de Supervisión y Adquisión de Datos** se encuentra formado por software y hardware que les permite a las empresas ejecutar algunas tareas como controlar los procesos industriales de forma local o remota, monitorear, recopilar y procesar datos en tiempo real, interactuar directamente con dispositivos como sensores, válvulas, motores y la interfaz HMI, grabar secuencialmente en un archivo o base de datos acontecimientos que se producen en un proceso productivo, crear paneles de alarma en fallas de máquinas por problemas de funcionamiento y el control de calidad mediante los datos recolectados.

→ *Componentes de un sistema SCADA*

HMI	*HMI* es una *Interfaz Humano-Máquina* en inglés es *Human-Machine Interface*. Es decir, es la interfaz entre el proceso y los operarios de una fábrica, una línea de producción, una empresa o cualquier sistema donde sea necesaria la operación por parte de un humano. En sí, es un panel de instrumentos que el operario puede manipular para controlar un proceso. Es la principal herramienta que utilizan los operarios y los supervisores de línea para coordinar y controlar procesos industriales y de fabricación.
Unidades Terminales Remotas (RTU)	Son microprocesadores (Computadoras Remotas) que obtienen señales independientes de una acción para enviar la información obtenida remotamente para que se procese. Se conectan a sensores que convierten las señales recibidas en datos digitales que lo envían a la computadora o al sistema de supervisión (MTU)

Sistema de supervisión o MTU (Computadora)	MTU Unidades Terminales Maestras que tiene la función de recopilar los datos del proceso y enviar las instrucciones mediante una línea de comandos.
PLCs	Comúnmente se denominan Autómatas Programables y son utilizados en el sistema como dispositivos de campo debido a que son más económicos, versátiles, flexibles y configurables que las RTUs.
Red o sistema de comunicación	Se encarga de establecer la conectividad de la computadora (MTU) a las RTUs y PLCs. Para ello utiliza conexiones vía Modem, Ethernet, Wifi o Fibra óptica.
Sensores	Son dispositivos que actúan como detectores de magnitudes físicas o químicas, denominadas variables de instrumentación y las convierten en variables o señales eléctricas.
Actuadores	Es un dispositivo mecánico que se utiliza para *actuar* u ofrecer movimiento sobre otro dispositivo mecánico.

→ *Cómo funciona un Sistema SCADA (Diagrama Básico)*



→ *Arquitectura básica de un sistema SCADA*

Está compuesta por **controladores lógicos programables (PLCs**) y unidades terminales remotas (RTUs). Los PLCs y RTUs son microprocesadores que se comunican con una serie de instrumentos, tales como maquinaria de fabricación, HMIs, sensores y dispositivos finales. A posterior, dirigen la información de esos objetos a computadoras con **software SCADA**. Este mismo **procesa, distribuye y muestra los datos**, ayudando a los operarios y a los técnicos de mantenimiento a analizar los datos y a tomar decisiones importantes.

Por ejemplo, el sistema notifica rápidamente a un operario que una partida de un producto muestra una alta incidencia de errores. En este caso, el operario hace una parada en la producción y visualiza los datos del sistema SCADA, a través de una HMI, para determinar la causa del problema. De esta manera, el técnico de mantenimiento revisa los datos y descubre que la máquina X estaba funcionando mal en el proceso Z. Por esta razón, la capacidad del sistema SCADA para notificar a los técnicos un problema, error o incidencia le ayuda a resolverlo y a prevenir más pérdidas de producto en el futuro, y en esta fase de la producción en concreto.

→ *¿Quién utiliza sistemas SCADA?*

Los sistemas SCADA son utilizados por organizaciones industriales y empresas de los sectores público y privado para controlar y mantener la eficiencia, distribuir datos para tomar decisiones más inteligentes y comunicar problemas del sistema para ayudar a mitigar el tiempo de inactividad.

Estos sistemas funcionan bien en diferentes tipos de empresas porque pueden ir desde configuraciones simples hasta instalaciones grandes y complejas. Así pues, son la columna vertebral de muchas industrias modernas, incluyendo: Energía, Alimentación y bebidas, Fabricación, Petróleo y gas, Potencia, Reciclaje, Transporte, Agua y aguas residuales, Entre otras muchas más.

Prácticamente en cualquier lugar del mundo actual, hay algún tipo de sistema SCADA que funciona entre bastidores: manteniendo los sistemas de refrigeración en el supermercado local, asegurando la **producción** y la **seguridad** en una refinería, alcanzando **estándares de calidad** en una planta de tratamiento de aguas residuales o incluso haciendo un **seguimiento de su uso de energía** en casa, por dar algunos ejemplos. Los sistemas SCADA efectivos pueden producir ahorros significativos de tiempo y dinero. Se han publicado numerosos estudios de casos que destacan los beneficios y ahorros de usar una solución de software SCADA moderna cómo WinCC.

→ *Historia de los sistemas SCADA*

En la década de 1930 los primeros sistemas SCADA se utilizaban para ahorrar personal operario y mejorar la visualización de los procesos industriales. Una vez que los sistemas SCADA fueron avanzando y la cantidad de datos adquiridos fue aumentando, en la década de 1960 y 1970 se hizo necesario gestionar una gran cantidad de datos, mejorar el rendimiento y manejar la gran complejidad de los sistemas.

En aquel tiempo, la toma de información se hacía en el campo y no existía aún una alta automatización a través de sistemas computacionales y no se contaba con redes de IT(Information Technology) y OT(Operation Technology) convergentes.

→ *Actualidad de los Sistemas SCADA*

Hoy en día los sistemas SCADA son más grandes y complejos ya que no dependen de simples redes punto a punto. *Una red de control industrial moderna* se puede dividir en tres segmentos como son la Red SCADA, La Red de ICS (Industrial Control Systems) y la Red IT de datos, los segmentos pueden operar interconectados para mejorar las funcionalidades propias del negocio, facilitando la comunicación entre distintas áreas de una organización y proporcionando información en tiempo real para la toma de decisiones.

La seguridad en los sistemas SCADA anteriormente se mantenía físicamente, es decir, solo las personas con permisos de acceso a las instalaciones podían obtener los datos, por lo tanto, la seguridad computacional no era preocupante. La convergencia de las redes de datos industriales con las redes de datos de TI ha proporcionado nuevas vías de acceso a estos sistemas, lo que involucra que los riesgos de seguridad asociados históricamente a las redes IT ahora también son de preocupación de las redes operacionales (OT).

Actualmente en los sistemas SCADA existen vulnerabilidades que pueden ser explotadas a través de distintos vectores de ataque comunes:

► Puertas traseras y agujeros en el perímetro de la red.

► Vulnerabilidades en protocolos comunes.

► Ataques a dispositivos de campo, remotos (ej. PLC).

► Ataques a Bases de Datos.

► Secuestros de sesiones y ataques de hombre en el medio “Man in the middle”.

Existen algunos posibles ataques que pueden agruparse en las siguientes categorías:

► Manipulación de datos de entrada introducidos a través de sensores comprometidos y/o exploit de enlaces de red entre sensores y controladores.

► Manipulación de datos de salida de sensores y controladores.

► Controlar archivos históricos.

► Ataques de Denegación de Servicio (DoS).

Los problemas de seguridad en sistemas SCADA más comunes incluyen una inadecuada o la falta absoluta de políticas de seguridad organizacional que incluya los sistemas SCADA, falta de segregación de redes, ausencia de logs de acceso, acceso a internet desde estaciones de trabajo de operadores, software no relacionado en las estaciones de trabajo y falta de revisión en los sistemas de control por parte de los fabricantes.

ANEXO 4 – Ciberataque a SONY Pictures Entertainment en Estados Unidos

El 24 de noviembre de 2014, un grupo de hackers autodenominados GPO "Guardianes de la paz" atacó los servidores de Sony, bloqueó sistemas críticos y borró información. Este grupo se encargó de paralizar los sistemas informáticos de la compañía y derivó en grandes filtraciones de datos, de registros financieros y de correos electrónicos privados de ejecutivos de Hollywood, los datos incluían información personal sobre los empleados de la compañía y sus familias, correos electrónicos entre empleados, información sobre salarios ejecutivos en la empresa, copias de películas inéditas y planes para futuras películas de Sony, guiones de ciertas películas y otra información.

Los criminales emplearon una variante de software malicioso llamado ***Shamoon,*** el cual es un virus que se encargó de infectar la computadora haciéndola inutilizable para borrar gran parte de la infraestructura informática de Sony. Los componentes del ataque incluyeron un implante de escucha, una puerta trasera, una herramienta de proxy, una herramienta de disco duro destructiva y una herramienta de limpieza de objetivos destructiva. Los componentes sugieren claramente la intención de obtener entradas repetidas, extraer información y ser destructivo, así como eliminar la evidencia del ataque.

En cuanto a daños económicos la compañía se vio afectada por el hackeo, tanto por la caída de sus acciones en la bolsa como por el dinero perdido en relación a los costos de producción del film que no se pudo llegar a estrenar exitosamente; además de eso, la compañía también sufrió demandas por parte de los actores por no saber proteger adecuadamente sus datos. Al mes siguiente del ciberataque, el 2 de diciembre, se empezó a difundir toda esa información en Internet, causando un daño incalculable a la reputación y las finanzas de una multinacional.

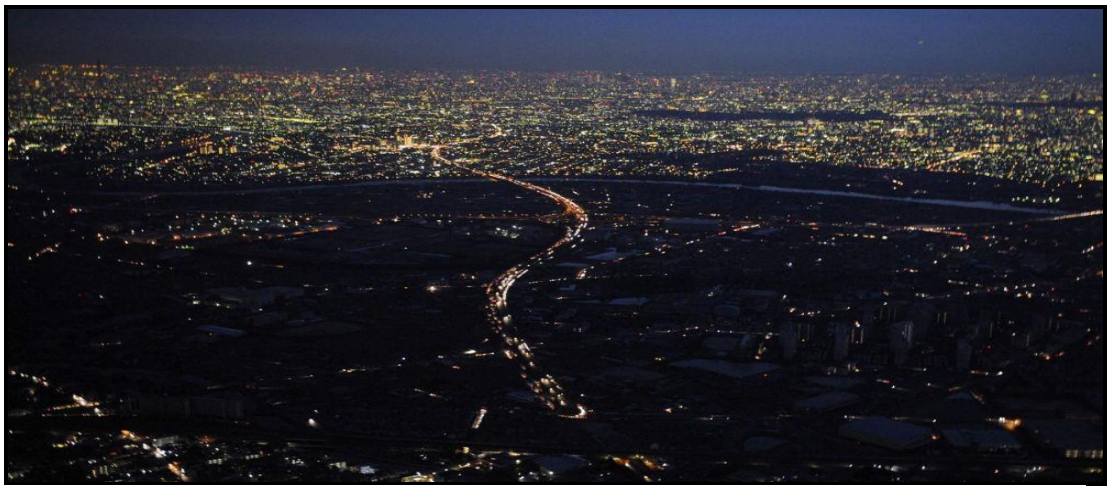
Durante el hackeo, el grupo exigió a SONY que retirara su próxima película The Interview, una comedia sobre un complot para asesinar al líder norcoreano *Kim Jong-un* y amenazó con realizar ataques terroristas en los cines que proyectaran dicha película. Después de que muchas de las principales cadenas de cines de EE UU optaron por no proyectar La entrevista en respuesta a algunas amenazas, de esta forma Sony decidió cancelar el estreno formal y el lanzamiento general de la película, optando por pasar directamente a un lanzamiento digital descargable seguido de un lanzamiento en cines limitado al día siguiente. Los funcionarios de inteligencia de Estados Unidos, después de evaluar el software, las técnicas y las fuentes de red utilizadas en el ataque, fundamentaron que el ataque fue patrocinado por el gobierno de Corea del Norte que desde entonces ha negado toda responsabilidad.

El FBI confirmó que Corea del Norte se encuentra detrás del ataque afirmando en un comunicado, ya que cuentan con información suficiente para concluir que el Gobierno norcoreano es el responsable de estos actos ocurridos. Las acciones de Corea del Norte tenían la intención de infligir un daño significativo a una empresa de EE UU y censurar el derecho de los ciudadanos americanos a expresarse, entre las pruebas que se mencionan expresamente, los investigadores han hallado direcciones IP asociadas a Corea del Norte comunicadas con las computadoras que efectuaron el ataque.

El Departamento de Justicia de EE. UU. emitió cargos formales relacionados con el hackeo de SONY contra el ciudadano norcoreano Park Jin-hyok el 6 de septiembre de 2018. El Departamento de Justicia afirmó que *Park* era un pirata informático norcoreano que trabajaba para la Oficina General de Reconocimiento del país, el equivalente de la *Agencia Central de Inteligencia*. El Departamento de Justicia había identificado previamente a Park y lo había estado monitoreando durante algún tiempo, pero no pudo acusarlo de inmediato ya que gran parte de la información a su alrededor estaba clasificada. La denuncia penal fue recientemente sin sellar.

ANEXO 5 – Ciberataque BlackEnergy en Ucrania

Los apagones en Ucrania están directamente relacionados con el troyano *BlackEnergy* un *malware* destructivo con un componente capaz de apagar sistemas críticos. El 23 de diciembre de 2015, aproximadamente 80.000 personas, residentes en la región ucraniana llamada ***Ivano-Frankivsk*** se quedaron sin electricidad durante seis largas horas en pleno invierno ucraniano. En la siguiente foto se puede ver la foto panorámica del gran apagón eléctrico ocurrido.



El gobierno de Ucrania señaló a Rusia como responsable del apagón que sufrieron diversas centrales eléctricas del país por medio de un ataque con un software dañino. El virus se llama ***BlackEnergy*** y es el primero en la historia de conocimiento público que está involucrado en un apagón eléctrico generalizado.

El virus BlackEnergy es de factoría rusa y ucraniana, después de dos años de guerra con Rusia, no cabe ninguna duda en señalar a este país como culpable, los expertos no lo confirmaron ni desmintieron porque los atacantes han tapado muy bien sus huellas.

BlackEnergy es un backdoor que se utilizó para instalar un componente llamado *KillDisk* en los equipos de destino cuya función era impedir que arranquen los sistemas informáticos críticos. BlackEnergy fue un elemento crucial en el sabotaje coordinado a diferentes empresas de servicio eléctrico de Ucrania al dar acceso a los atacantes. Una vez adquirido el acceso, los atacantes procedieron a cortar la electricidad, lanzaron un ataque de denegación de servicio para impedir que llegaran los reportes de los usuarios e intentaron dañar la configuración de los sistemas SCADA de manera de entorpecer la reactivación del sistema eléctrico.

De acuerdo al informe presentado por el equipo de respuestas ante incidentes de seguridad ucraniano CERT, *los ciberdelincuentes habían atacado a una serie de empresas de medios de prensa en la época de elecciones locales ucranianas del 2015 y como resultado se encontró que un gran número de* **materiales de vídeo y varios documentos** *quedaron destruidos como resultado del ataque.*

El troyano ***BlackEnergy*** es **modular** y emplea diversos componentes descargables para llevar a cabo tareas específicas. En el caso del ataque a Ucrania, se descubrió que el malware ***Win32/KillDisk*** estaba presente en el sistema infectado. KillDisk borro los archivos del sistema para que el equipo no arranque y saboteo específicamente sistemas críticos industriales esa fue la variante detectada en las compañías eléctricas.

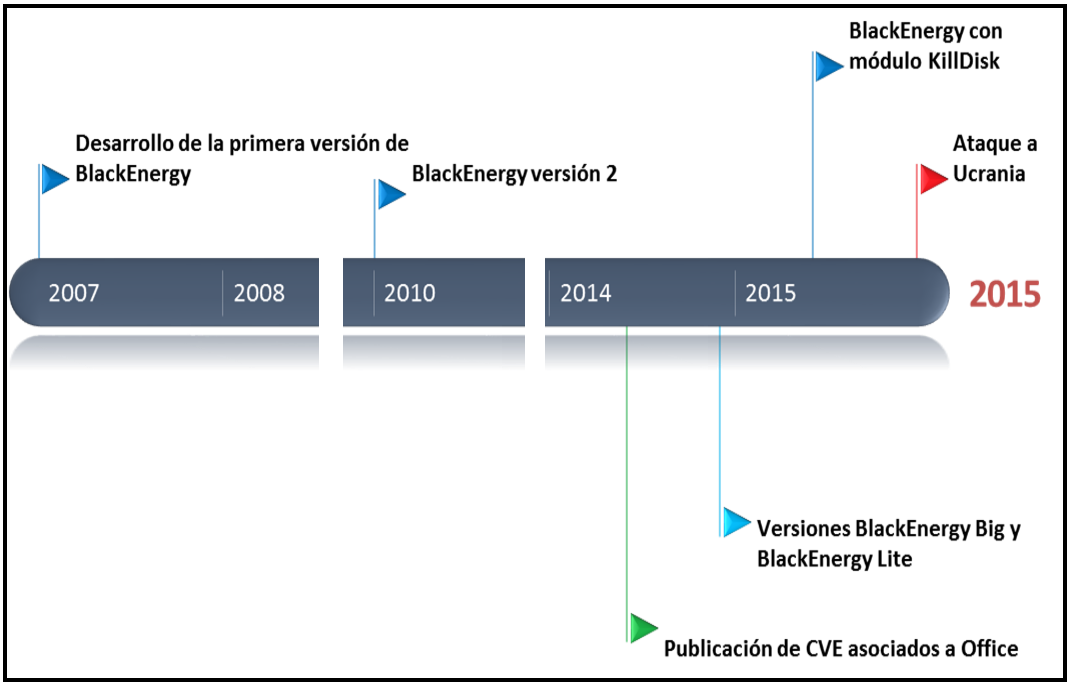
BlackEnergy al igual que un backdoor SSH por sí mismo les proporciona a los atacantes **acceso remoto** a los sistemas infectados. Tras infiltrarse exitosamente en un sistema crítico con cualquiera de estos troyanos, el atacante debería ser capaz de apagarlo. En tal caso, el troyano destructivo *KillDisk* instalado actuaría como un medio para dificultar aún más la recuperación del sistema.

Normalmente los sectores que sufren estos tipos de ciberataques son los siguientes tales como: energía, organismos gubernamentales y medios de comunicación en Ucrania, empresas ICS/SCADA de todo el mundo y empresas de energía de todo el mundo.

Las funciones principales de KillDisk tienen como objetivo:

- ► Borrar archivos de sistema para que el re-arranque sea lo más difícil posible.
- ► Borrar los eventos en el log de Windows.
- ► Agregar la opción de introducir un retraso (Delay) en la activación de una carga maliciosa (payload) destructiva.

BlackEnergy ha evolucionado de ser un troyano para convertirse en una Amenaza Persistente Avanzada *(APT - Advanced Persistent Threat).* No se trata de una muestra de malware reciente; de hecho, su primera detección fue ya en el año 2007.



Línea temporal de BlackEnergy

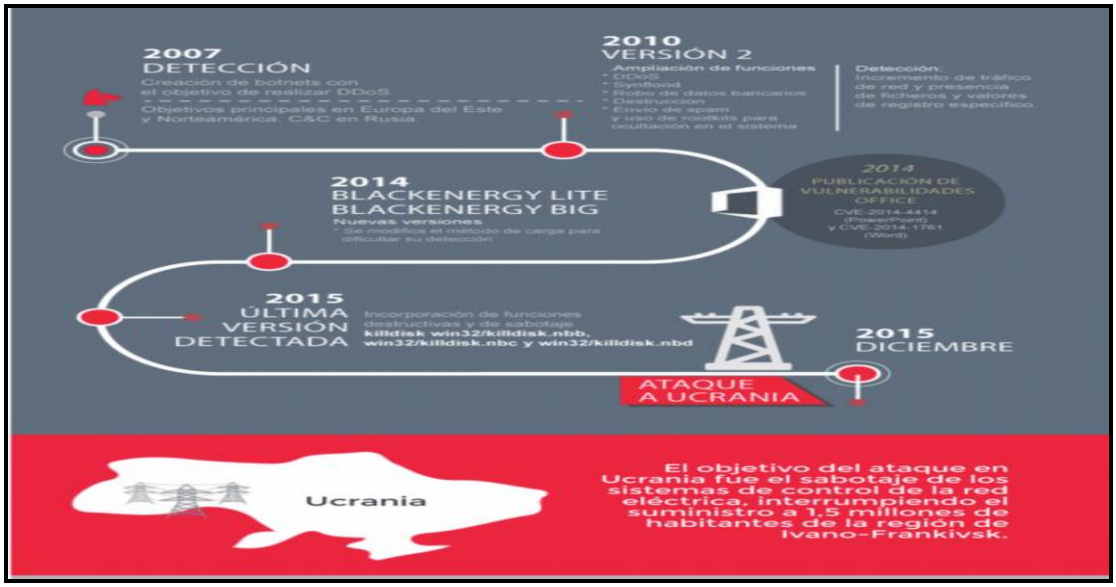
Originariamente se diseñó como una herramienta para crear botnets con el objetivo de realizar ataques DDoS. El troyano consta de una aplicación que genera los clientes que el atacante usa para infectar las máquinas de sus víctimas.

También provee scripts para llevar a cabo las DDoS que el atacante configura desde el servidor C&C (Command and Control), así como una interfaz para controlar los equipos infectados.

En el año 2014 surgen variaciones que limitan el modo kernel únicamente para la realización de la carga maliciosa o que directamente lo inhabilitan cargándolo mediante el proceso **rundl32.exe**, versión denominada BlackEnergy Lite. El uso en modo kernel dificultaba el proceso de ataque al tener que contrarrestar nuevas contramedidas de los sistemas operativas, como la firma de controladores o el arranque seguro, haciendo demasiado costosos este tipo de ataques. En el año 2015, BlackEnergy agrega las variaciones: ***Win32/KillDisk.NBB - Win32/KillDisk.NBC - Win32/KillDisk.NBD***

Detectados por el CERT- UA *(CERT Ucrania),* que incluyen el componente KilDisk. Esta es la versión utilizada en el ataque.

BlackEnergy ha evolucionado hasta adoptar un sofisticas diseño modular que incorpora un Rootkit y avanzadas funcionalidades para posibilitar ataques de spam, fraude bancario y ataques dirigidos. en el 2015 demostró capacitad de APT para infectar sistemas SCADA con un ataque a una Central eléctrica en Ucrania.



ANEXO 6 – Ciberataque Ransomware “Wannacry” a Nivel Mundial

- ¿Qué es un ransomware?

Es un tipo de *malware* o software malicioso que los cibercriminales utilizan para obligar a las personas o empresas a pagar un rescate. Un ataque de ransomware es aquel cuyo objetivo es una persona u organización se puede propagar a las computadoras a través de archivos adjuntos o enlaces incluidos en correos electrónicos de phishing, a través de sitios web infectados mediante una descarga oculta o a través de dispositivos USB infectados. Una vez que una computadora o una red están infectados con el ransomware, el *malware* bloquea el acceso al sistema o cifra los datos de dicho sistema. Los cibercriminales exigen que las víctimas paguen un rescate para recuperar el acceso a su computadora o a sus datos.

- Modos de Ataque de ransomware

Existen dos modalidades de ransomware:

→ Ransomware de Cifrado: cifra los archivos valiosos de una computadora para que el usuario no pueda acceder a ellos. Los cibercriminales que llevan a cabo los ataques de ransomware de cifrado ganan dinero exigiendo a las víctimas que paguen un rescate para recuperar sus archivos.

→ Ransomware de Bloqueo: no cifra los archivos, sino que bloquea a la víctima el acceso al dispositivo para que no pueda utilizarlos. Una vez bloqueado el acceso, los cibercriminales que llevan a cabo los ataques de ransomware piden un rescate para desbloquear el dispositivo.

Existen algunos ejemplos de ransomware famosos, principalmente para entender lo diferentes y peligrosos que pueden llegar a ser cada uno en su categoría propia.

►**CryptoLocker** es un ransomware que apareció por primera vez en 2007 y que se propagó a través de archivos adjuntos de correo electrónico infectados. Una vez en la computadora, buscaba archivos valiosos y los cifraba para pedir un rescate. Se calcula que afectó a unas 500.000 computadoras, la policía y las empresas de seguridad finalmente consiguieron detectar una red mundial de computadoras domésticas secuestradas que se utilizaban para propagar el ransomware CryptoLocker. Esto les permitió controlar parte de la red cibercriminal y capturar los datos en el momento en que se enviaban sin que los cibercriminales lo supieran. Esta acción posteriormente desembocó en el desarrollo de un portal online en el que las víctimas podían obtener una clave para desbloquear y liberar sus datos de forma gratuita sin necesidad de pagar a los criminales.

►**Troldesh** El ataque del ransomware Troldesh se produjo en 2015 y se propagó a través de correos electrónicos de spam con enlaces o archivos adjuntos infectados. Curiosamente, los atacantes de Troldesh se pusieron en contacto con las víctimas directamente por correo electrónico para solicitar los rescates. Los cibercriminales incluso negociaron descuentos para las víctimas con las que entablaron una buena relación, algo muy poco común.

►**Locky** es un tipo de ransomware que fue usado por primera vez en 2016 en un ataque lanzado por un grupo organizado de hackers, con la capacidad de cifrar más de *160 tipos de archivos,* Locky se propaga engañando a las víctimas para que lo instalen mediante correos electrónicos falsos con archivos adjuntos infectados. Este método de transmisión se denomina *phishing* y es una forma de ingeniería social. Locky tiene como objetivo una amplia gama de tipos de archivos usados por diseñadores, desarrolladores, ingenieros y evaluadores.

►**Jigsaw** es un ataque de ransomware que comenzó en 2016. Tenía este nombre porque incluía una imagen de la marioneta de la película *Juego del miedo*. Jigsaw iba eliminando gradualmente más y más archivos de la víctima cada hora que pasaba sin pagarse el rescate exigido. El uso de imágenes de una película de terror en este ataque causaba aún más angustia a las víctimas.

►**Petya** *(no debe confundirse con ExPetr)* es un ataque de ransomware que se lanzó por primera vez en 2016 y que resurgió en 2017 como GoldenEye. En lugar de cifrar archivos específicos, este despiadado ransomware cifra todo el disco duro de la víctima. Para ello, cifra la tabla maestra de archivos *(MFT, del inglés "Master File Table")* lo que impide el acceso a los archivos del disco. Petya se propagaba por los departamentos de Recursos Humanos de las empresas a través de un correo electrónico de solicitud de empleo falsa con un enlace a Dropbox infectado.

►**WannaCry** es un ataque de ransomware que se propagó por 150 países en 2017. Diseñado para explotar una vulnerabilidad en Windows, fue creado por la *Agencia de Seguridad Nacional de Estados Unidos* y filtrado por el grupo *The Shadow Brokers*. WannaCry afectó a 230.000 computadoras en todo el mundo. El ataque alcanzó a un tercio de los centros hospitalarios del Reino Unido y le costó al NHS unos 92 millones de libras. Quedó bloqueado el acceso a los usuarios y los delincuentes exigían un rescate en bitcoins. El ataque puso de relieve los problemas que puede causar el uso de sistemas obsoletos que hace vulnerable a los ataques a los servicios de salud básicos. El impacto financiero global de WannaCry fue sustancial, se estima que el cibercrimen provocó pérdidas financieras por valor de 4.000 millones de dólares en todo el mundo.

► **Bad Rabbit** es un ataque de ransomware realizado en 2017 que se propagó mediante un método denominado *ataque "drive-by",* que hace uso de sitios web sin protección para llevar a cabo un ataque. Durante un ataque drive-by de ransomware un usuario visita un sitio web legítimo sin saber que un hacker lo ha vulnerado. A menudo, los ataques drive-by no necesitan interacción por parte de la víctima, aparte de navegar a la página vulnerada. Sin embargo, en este caso se infectan cuando hacen click para instalar algo que en realidad es *malware* disfrazado. Este elemento se conoce como instalador ***"dropper"*** de *malware*. Bad Rabbit solicitaba instalar *Adobe Flash*, pero lo que en realidad instalaba era un instalador de *malware* para propagar su infección.

►**Ryuk** El ransomware Ryuk, que se propagó en agosto de 2018, desactivaba la opción de restauración del sistema de Windows lo que impedía la restauración de los archivos cifrados si el usuario no contaba con una copia de seguridad. Ryuk también cifraba las unidades de red, los efectos fueron devastadores y muchas de las organizaciones que sufrieron el ataque en Estados Unidos pagaron los rescates exigidos. En los informes de agosto de 2018 se estimó que los fondos recaudados con el ataque superaban los 640 000 dólares.

►**GoldenEye:** El resurgimiento de Petya, conocido como GoldenEye, culminó en un ataque de ransomware global que tuvo lugar en 2017. Bautizado como el ***hermano devastador de WannaCry***, GoldenEye afectó a más de 2000 objetivos, entre ellos importantes productores de petróleo en Rusia y varios bancos. Lo más espantoso de todo es que GoldenEye incluso obligó a los trabajadores de la *central nuclear de Chernóbil* a comprobar de forma manual los niveles de radiación ya que se les había bloqueado el acceso a sus equipos Windows.

►**GandCrab** es un ataque de ransomware bastante desagradable que amenazaba con revelar los hábitos de visualización de pornografía de la víctima. Los cibercriminales de GandCrab afirmaban haber secuestrado la webcam de los usuarios, exigían un rescate y amenazaban a las víctimas con publicar el vergonzoso material si no se les pagaba. Tras su primer lanzamiento en enero de 2018, GandCrab evolucionó pasando por varias versiones.

Contextualizando mejor lo que es ransomware y los daños que genera se continuara específicamente con el ransomware WANNACRY o "QUIERO LLORAR" ocurrido en el año 2017 que corresponde a la investigación realizada.

Este ciberataque masivo del ransomware *WannaCry* el cual fue a nivel global, no paraban de aparecer actualizaciones, boletines, consejos, mensajes alarmantes que hablan de un "virus" que provocó un "hackeo mundial".

El culpable era **WannaCryptor** (también llamado WannaCry o Wcrypt), detectado por ESET como ***Win32/Filecoder.WannaCryptor.D***, que se aprovechó de una vulnerabilidad en Windows y también se valió del cifrado **AES y RSA** para tomar "de rehén" información contenida en el sistema infectado

Lo que convirtió al ataque en algo realmente escandaloso fue su capacidad de propagarse por sí mismo de manera similar a un gusano, por las redes de los equipos infectados. Así, naturalmente, escaló en cuestión de horas**.**

Esta es la captura de pantalla que veían los usuarios que estaban infectados con la versión en español o inglés:

Todo comenzó en el sector de telecomunicaciones de España, cuando el **85%** de los equipos de la Empresa Telefónica se infectaron y escaló rápidamente a nivel nacional e internacional. A este reporte se sumaron casos en organizaciones del sector de la salud, sitios comerciales y todo tipo de redes.

Este ataque empezó el viernes 12 de mayo de 2017 y ha sido descrito como sin precedentes en tamaño, infectando más de 230.000 computadoras en más de 150 países.

Los países más afectados que han sido reportados fueron en Europa se destacaron Rusia, Ucrania, India y Taiwán, pero partes del servicio nacional de salud de Gran Bretaña (NHS), Telefónica de España FedEx, Deutsche Bahn y las aerolíneas LATAM y en Latinoamérica se destacaron Argentina, Chile, México, Brasil, Colombia y Ecuador que también fueron afectadas junto con muchos otros blancos a nivel mundial.

En la siguiente imagen, se puede visualizar el mapa a nivel mundial en tiempo real de los países que fueron víctimas del ciberataque masico WannaCry ese 12 de mayo del 2017

El software secuestra las computadoras al congelarlas, mostrando una ventana roja con el mensaje *"¡Ups, sus archivos han sido cifrados!"* que reclama dinero en *bitcoins,* una moneda virtual, de 300 dólares al principio y 600 dólares más tarde para que no borre los archivos horas después. Basta que una persona de una organización haga clic en un archivo adjunto infectado o un enlace afectado para que todas las computadoras de la red se infecten.

El costo de rescate que pide *WannaCryptor* es de 300 dólares en bitcoins un monto similar al de otros casos de ransomware, pero lejos de ser el más alto, de todas formas, a este monto hay que sumarle el costo de la pérdida de productividad ocasionada por la infección y el daño a la reputación de la compañía que resulte víctima.

En la siguiente captura de pantalla se muestra como fue el WannaCry, el ransomware del ciberataque a Telefónica:

Este tipo de virus informático es el protagonista del hasta ahora ciberataque más peligroso acontecido en España, con consecuencias que se ramifican a varios niveles. Según el CNI, el protagonista del **ciberataque** a **Telefónica** es una versión del **ransomware WannaCry**. Es un tipo de *malware* que lleva circulando bastante tiempo y que ataca especialmente a sistemas con Windows.

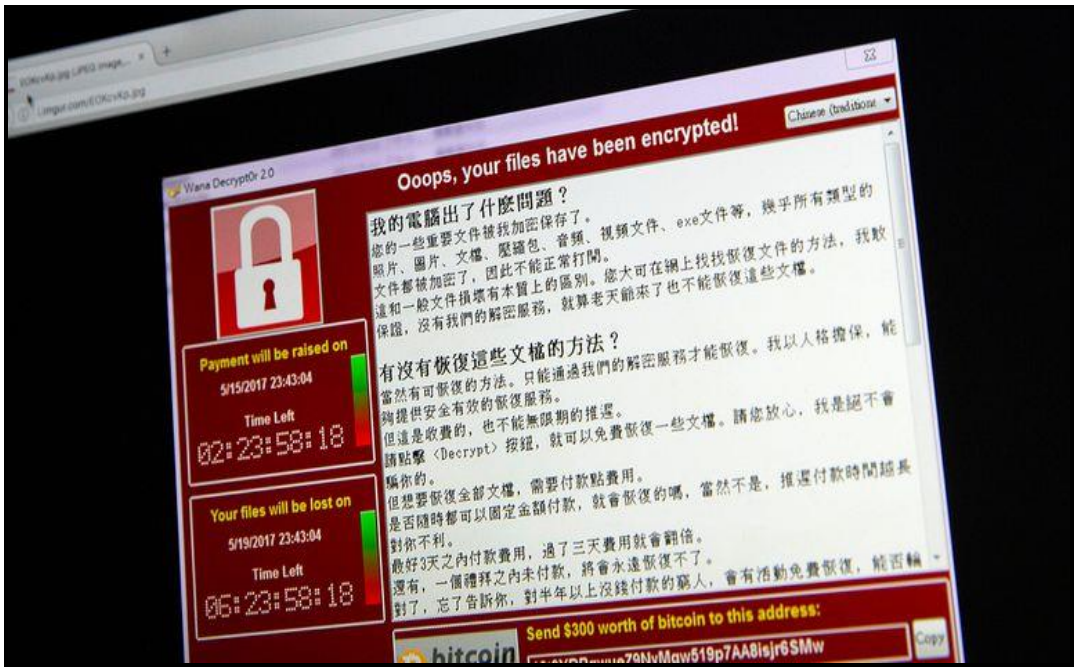
El funcionamiento del virus que ha atacado a **Telefónica** ya hizo saltar las alarmas en Microsoft en marzo. La compañía creadora de Windows detectó una vulnerabilidad crítica en sus sistemas operativos que permite a un hacker ejecutar código de forma remota. Gracias a esta circunstancia, el atacante puede concederse privilegios de administrador para ejecutar cualquier cambio en el sistema.

Así es cómo funciona WannaCry, sólo hace falta que uno de sus archivos llegue a la computadora o red de computadoras afectadas para poder secuestrar un sistema al completo. Una vez dentro, el ransomware bloquea el acceso al administrador y los usuarios reales, pidiendo una recompensa a cambio. Normalmente ésta se exige en Bitcoins, una criptomoneda prácticamente imposible de rastrear.

El impacto de este ataque fue tal que Microsoft lanzó especialmente parches para Windows XP, Windows 8 y Windows Server 2003, que no los habían tenido originalmente en marzo por ser versiones ya sin soporte oficial. Pero la severidad de este caso ameritó que se hiciera la excepción de publicar actualizaciones **incluso para los sistemas obsoletos.**

El *Centro Criptológico Nacional de España*, esta amenaza se vale de la vulnerabilidad *EternalBlue/DoblePulsar* incluida en el **boletín de seguridad MS17-010 de Microsoft**, para poder infectar a otros equipos Windows que estén conectados a una misma red. Según el *CCN-CERT*, la explotación de esa vulnerabilidad permite la **ejecución remota de comandos** a través de Samba.

En una segunda oleada, el virus que infecta computadores y roba información de todo el mundo golpeó Asia tal y como se puede ver en la siguiente captura de pantalla.



El ciberataque a nivel internacional que se produjo en China y afecto unas 30.000 organizaciones y empresas. Más de 20.000 gasolineras del gigante petrolero chino se quedaron sin conexión a Internet por lo que los clientes solo podían pagar en efectivo. Además, universidades y otras instituciones educativas estaban entre las más golpeadas, con en torno al 15% de las direcciones IP atacadas, según la *agencia oficial Xinhua News*

Agency estaciones de tren, servicios postales, hospitales, edificios, centros comerciales y servicios del gobierno se vieron involucrados.

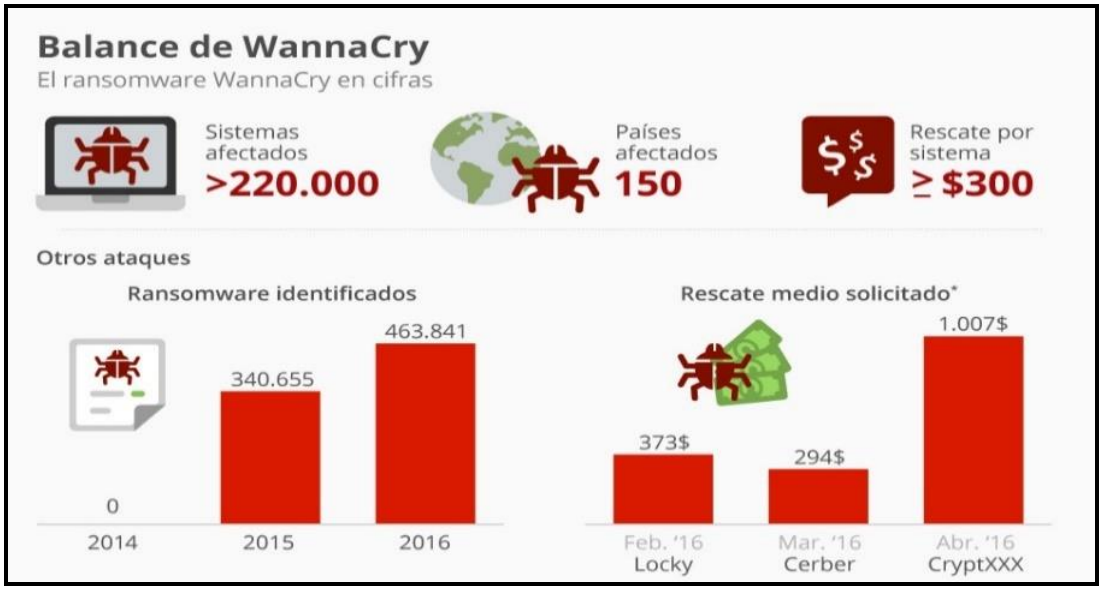
A su vez, en Japón la *empresa tecnológica Hitachi* informó hoy que como consecuencia del ciberataque había problemas con el envío y recepción de emails y la apertura de archivos adjuntos. Aún se investiga cuántas computadoras se vieron afectadas, pero parte de los sistemas paralizados ya fueron recuperados. El gobierno no encontró impacto entre agencias del gobierno, aunque empresas como *Hitachi* y *Nissan Motor Co*. reportaron problemas que no habían afectado de forma grave sus operaciones.

Indonesia llamó a sus autoridades y empresas a tomar medidas de protección. "En vista de este ataque mundial hay que actuar rápido", dijo el *ministro de Comunicaciones y Tecnología de la Información en Yakarta*. En la capital se vieron afectados dos hospitales. Por su parte, Tailandia informó que el ataque no tuvo grandes consecuencias en el país pero que, en la capital, Bangkok no funcionaban varios carteles digitales, que en vez de la publicidad programaba mostraban otras cosas.

Una vez instalado el *malware* WannaCry, este utiliza un exploit llamado ***EternalBlue***, desarrollado por la *Agencia de Seguridad Nacional de los Estados Unidos (NSA),* para extenderse a través de redes locales y anfitriones remotos que no hayan recibido la actualización de seguridad más reciente y de esta manera infecta directamente cualquier sistema expuesto.

Un **“parche”** crítico habría sido emitido por Microsoft el 14 de marzo de 2017 para eliminar la vulnerabilidad subyacente para sistemas soportados por Microsoft en la actualidad, lo cual se dio casi dos meses antes del ataque, sin embargo, muchas organizaciones no llegaron a aplicarlas. Varias horas después de la liberación inicial del ransomware, el 12 de mayo de 2017, mientras intentaba establecer la escala del ataque, *Marcus Hutchins*, un investigador quien bloguea bajo el seudónimo *@MalwareTech*, accidentalmente descubrió lo que en la práctica resulta ser un **"botón de apagado**" del malware, incluido como hardcode en el código del mismo. Registrando un nombre de dominio correspondiente a un

sinkhole DNS, logró detener la propagación del gusano, porque el ransomware sólo encriptaba los archivos de la computadora si era incapaz de conectarse a dicho dominio. Mientras esto no ayudó a los sistemas que ya habían sido infectados, retrasó severamente la propagación de la infección inicial y dio tiempo para que se desplegaran medidas defensivas en todo el mundo, particularmente en América del Norte y Asia, en donde el ataque no había alcanzado la misma extensión que en otras zonas. Se ha sugerido que el propósito de este "botón de apagado" incluía hacer el programa más difícil de analizar Algunas configuraciones de red pueden impedir la efectividad de este método. En la siguiente figura, se puede visualizar claramente como fue el ciberataque ransomware Wannacry



ANEXO 7 – Tipos de ciberataques en infraestructuras críticas

A continuación, se describen los tipos de ciberataques en las infraestructuras críticas.

►Ataques de Denegación de Servicio (DoS/DDoS)

Un ataque de **Denegación de Servicio** se encarga de saturar los recursos de un sistema para que éste no pueda responder a las solicitudes de servicio mientras que un ataque de **Denegación de servicio Distribuido** también es un ataque a los recursos del sistema, pero se inicia desde una gran cantidad de otras máquinas host que están infectadas por el software malicioso controlado por el atacante. Un ataque DDoS tiene consecuencias drásticas para los sistemas afectados que, por lo general, tienen pocas probabilidades de identificar la fuente real del ataque. Esto se debe principalmente a que, para construir estas redes de bots, los atacantes operan agentes especiales de software que a través de Internet y sin el consentimiento del operador, se colocan en los equipos que no cuenten con el sistema de protección adecuado y allí se controlan de forma central.

Los ataques de denegación de servicio se pueden dividir en dos clases:

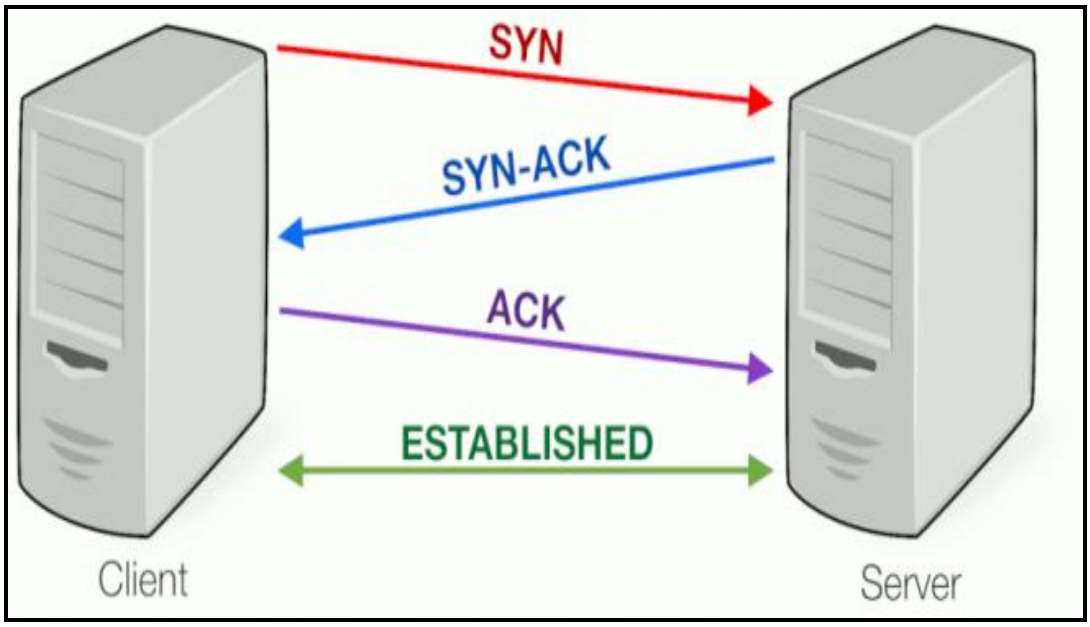
- Las *denegaciones de servicio por saturación*, que saturan un equipo con solicitudes para que no pueda responder a las solicitudes reales.

- Las *denegaciones de servicio por explotación de vulnerabilidades*, que aprovechan la vulnerabilidad en el sistema para volverlo inestable.

Existen algunos tipos de ciberataque DoS y DDoS y son los siguientes:

- **Ataque SYN o Inundación TCP/SYN**

Consiste en saturar el tráfico de la red para aprovechar el mecanismo de negociación de tres vías del protocolo TCP. El objetivo principal de este tipo de ataque es cuando los hosts corren como procesos de TCP, de esta forma se explota la vulnerabilidad del proceso TCP *Three-way-handshake* o "Apretón de manos por tres vías". Dicho proceso está diseñado de forma tal que dos computadoras puedan negociar los parámetros de conexión socket TCP, antes de la transmisión de datos como solicitudes SSH y HTTP. A continuación, se muestra un claro ejemplo de ataque de inundación SYN



Cuando un cliente establece una conexión con un servidor, envía una solicitud SYN; el servidor responde con un paquete SYN/ACK y el cliente valida la conexión con un paquete ACK (reconocimiento).

No es posible establecer una conexión TCP hasta haber finalizado estas tres vías. El ataque SYN consiste en enviar una gran cantidad de solicitudes SYN a través de una computadora con una dirección IP inexistente o no válida. En consecuencia, el equipo de destino no puede recibir un paquete ACK.

Los equipos vulnerables a los ataques SYN dejan las conexiones abiertas en cola dentro de una estructura de memoria de datos y aguardan la recepción de un paquete ACK.

Existe un mecanismo de caducidad que posibilita rechazar los paquetes una vez transcurrido un determinado período de tiempo. No obstante, cuando la cantidad de paquetes SYN es bastante considerable, si el equipo de destino utiliza todos los recursos para almacenar las solicitudes en cola, corre el riesgo de volverse inestable, lo que puede provocar la caída o el reinicio del sistema.

- **Ataque de Inundación de Ping – (Ping Flood Attacks o inundación ICMP)**

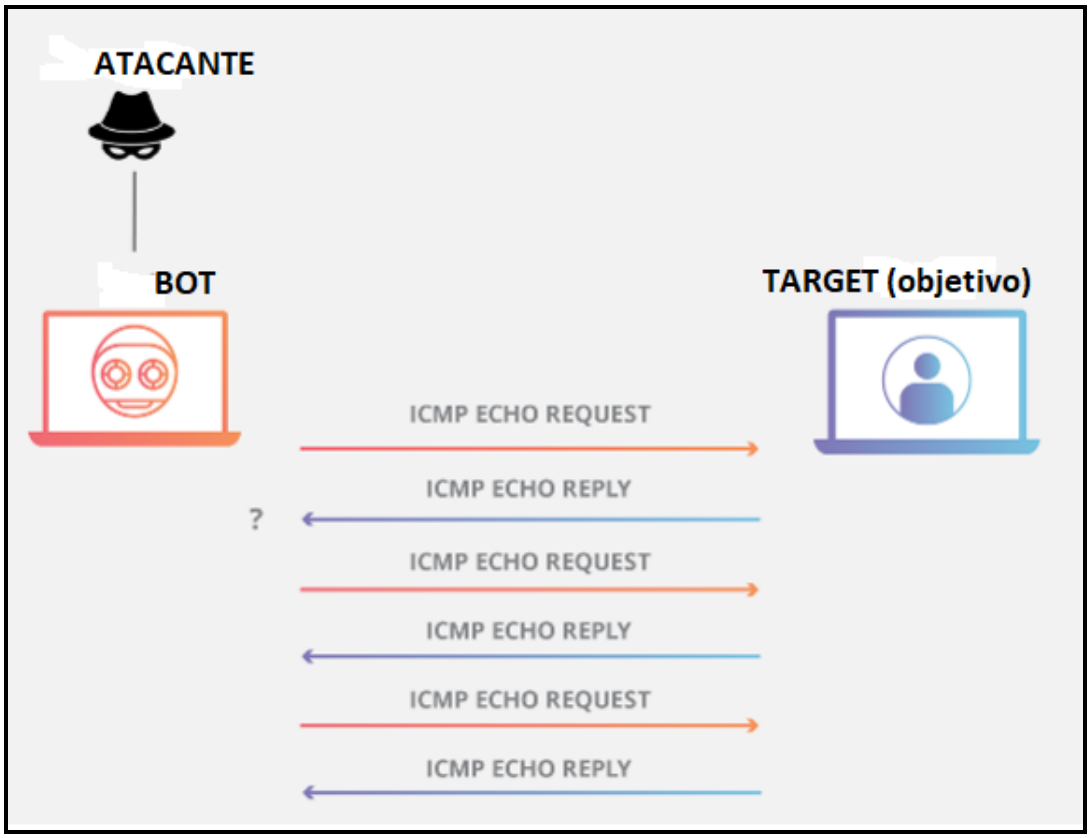
Es un ataque común de DoS en el que un atacante derriba la computadora de una víctima abrumando con solicitudes de eco ICMP, también conocidas como *pings*. El ataque implica inundar la red de la víctima con paquetes de solicitud, sabiendo que la red responderá con un número igual de paquetes de respuesta. Los métodos adicionales para derribar un objetivo con solicitudes ICMP incluyen el uso de herramientas o códigos personalizados, como *Hping y Scapy, e*sto agota los canales entrantes y salientes de la red, consume un ancho de banda significativo y da como resultado una denegación de servicio.

La forma para realizar este tipo de ataque de inundación de ping (ICMP) se divide en 2 pasos repetidos:

- El atacante envía muchos paquetes de solicitud de eco ICMP al servidor de destino utilizando varios dispositivos.

- El servidor de destino luego envía un paquete de respuesta de eco ICMP a la dirección IP de cada dispositivo solicitante como respuesta.

En el siguiente gráfico, se puede entender mejor como funciona dicho ataque:



- Ataque de ping de la muerte – (Ping of Death Attack o PoD)

Es un tipo de ataque de DoS en el que un atacante intenta bloquear, desestabilizar la computadora o el servicio objetivo mediante el envío de paquetes de datos por encima del límite máximo (65,536 bytes) que TCP / IP permite con un simple comando *ping*. La fragmentación de TCP / IP divide los paquetes en pequeños fragmentos que se envían al servidor. Dado que los paquetes de datos enviados son más grandes de lo que el servidor puede manejar, el servidor puede congelarse, reiniciarse o bloquearse. Sin embargo, en un sistema sin parches, el ataque sigue siendo relevante y peligroso.

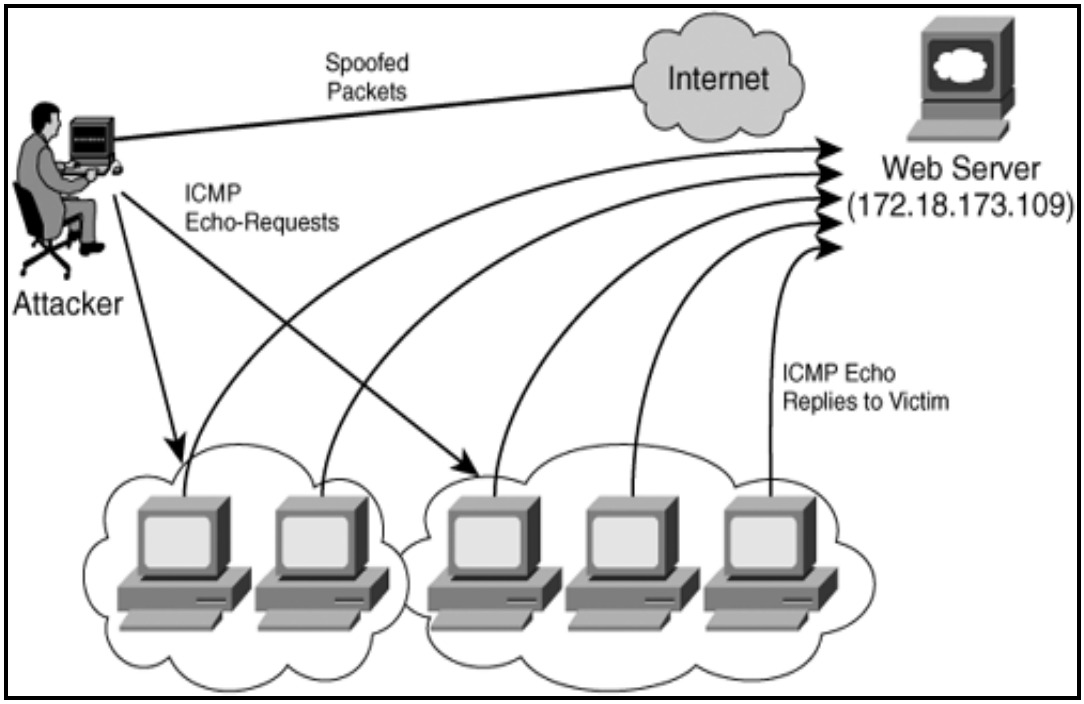
- Ataque Pitufo – (Smurf attack)

Es un tipo de ataque de DDoS que deja las redes informáticas inoperativas. El ataque *smurf* logra atacar aprovechando las vulnerabilidades del protocolo de Internet y de los protocolos de mensajes de control de Internet.

Este tipo de ataque se encarga de amplificar considerablemente los efectos de un ataque ICMP. Existen tres partes del ataque pitufo o Smurf, El atacante, el intermediario y la víctima.

En el ataque Smurf, el atacante dirige paquetes ICMP tipo *"echo request"* (ping) a una dirección IP de broadcast, usando como dirección IP origen, la dirección de la víctima (Spoofing). Se espera que los equipos conectados respondan a la petición, usando *Echo Reply*, a la máquina origen (víctima). Se dice que el efecto es **amplificado**, debido a que la cantidad de respuestas obtenidas corresponde a la cantidad de equipos en la red que puedan responder. Todas estas respuestas son dirigidas a la víctima intentando colapsar sus recursos de red.

En el siguiente grafico se explica cómo es un ataque pitufo o smurf:



- Ataque de lágrima – (Teardrop Attack)

Es un ataque de denegación de servicio que implica enviar paquetes fragmentados a una máquina de destino. Dado que la máquina que recibe dichos paquetes no puede volver a ensamblarlos debido a un error en el reensamblaje de fragmentación TCP/IP, los paquetes se superponen entre sí, lo que bloquea el dispositivo de red de destino.

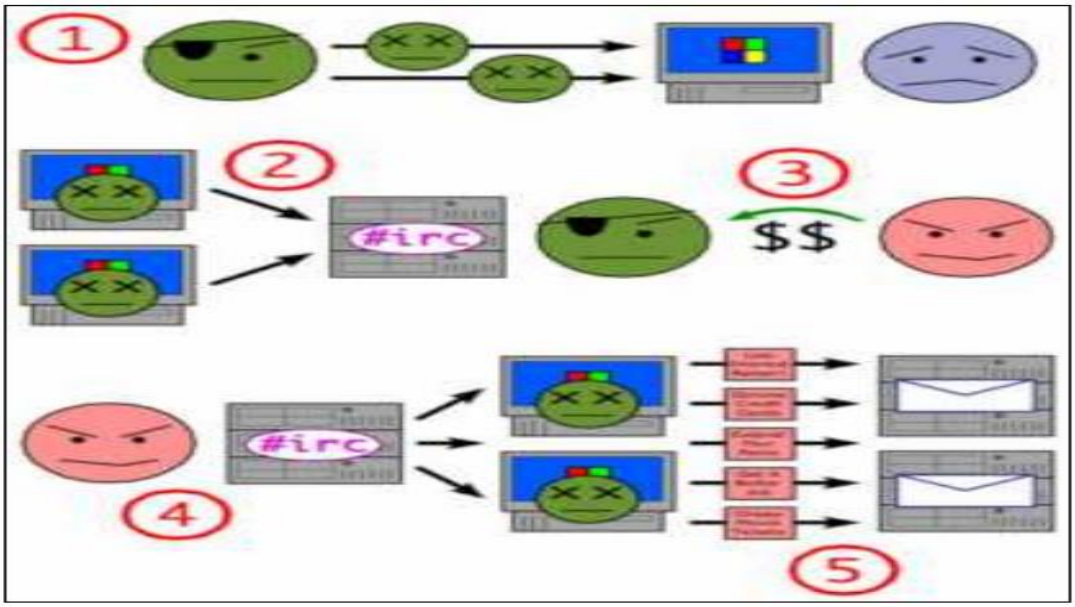
Cuando se ejecuta este tipo de ataque, las implementaciones de TCP / IP difieren ligeramente de una plataforma a otra. Algunos sistemas operativos, especialmente las versiones anteriores de Windows y Linux contienen un error de reensamblaje de fragmentación de TCP / IP. Los ataques en forma de lágrima están diseñados para aprovechar esta debilidad. Dado que los paquetes se superponen, se produce un error cuando el dispositivo intenta volver a ensamblar el paquete. El ataque se aprovecha de ese error para provocar un bloqueo fatal en el sistema operativo o aplicación que maneja el paquete.

- Botnets

→ *Que es una botnet*

Se refiere a un grupo de computadoras que han sido infectadas por *malware* y quedan bajo el control de un actor malicioso. El término Botnet es un acrónimo de las palabras *robot* y *red*, y cada dispositivo infectado se llama *bot*. Los botnets pueden diseñarse para realizar tareas ilegales o maliciosas, incluido el envío de spam, el robo de datos, el *ransomware*, hacer click de manera fraudulenta en anuncios o ataques de DDoS. Si bien algunos programas maliciosos, como el *ransomware*, tendrán un impacto directo en el propietario del dispositivo de este modo el *malware* de la botnet puede tener diferentes niveles de visibilidad. Algunos programas maliciosos están diseñados para tomar el control total de un dispositivo, mientras que otros programas maliciosos se ejecutan como un proceso en segundo plano mientras esperan silenciosamente las instrucciones del atacante.

→ *Funcionamiento de la botnet*



Como bien indica el gráfico, se deben ejecutar cinco pasos básicos los cuales se listan a continuación:

1. El operador de la botnet manda virus/gusanos/etc a los usuarios.

2. Las PCs entran en el IRC o se usa otro medio de comunicación.

3. El spammer le compra acceso al operador de la Botnet.

4. El Spammer manda instrucciones vía un servidor de IRC u otro canal a las PC infectadas.

5. Causando que éstos envíen Spam a los servidores de correo.

El primer objetivo es distribuir el *malware* suficiente para lograr la mayor cantidad de equipos infectados con el troyano - cliente que conecta a los usuarios con el o los responsables/s de la botnet. Esta distribución se realiza mediante mensajes masivos con el fin de engañar a los usuarios, cuando estos mensajes se han propagado por miles de equipos y han sido infectados es el momento en que comienzan a servir de base para nuevas olas de ataques.

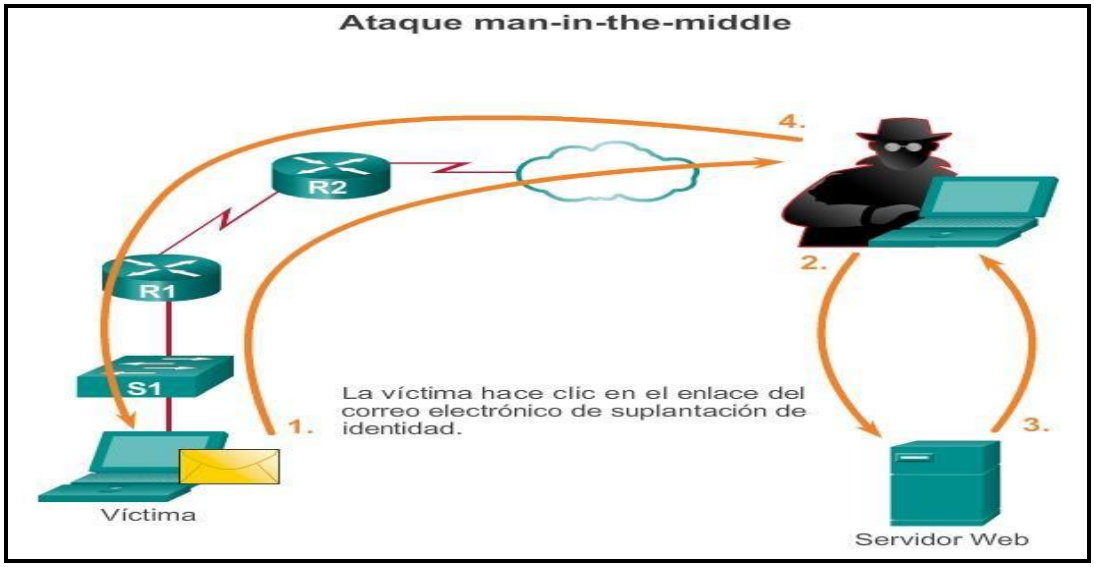
Una vez que la red ha sido convenientemente armada con millones de equipos , el responsable de la red que se construido, puede decidir con total libertad, remotamente y en cualquier parte del mundo qué hacer con la misma pudiendo, por ejemplo: Enviar spam, realizar ataques de denegación de servicio distribuido, crackear seriales, construir servidores web para alojar material de pornografía y pedofilia, construir servidores web para ataques de phishing, redes privadas de intercambio de material ilegal, snifeo de tráfico web para robo de datos confidenciales, distribución e instalación de nuevo *malware*, abuso de publicidad online, manipulación de juegos online, etc. El control de la red puede llevarse a cabo de diversas maneras: puede controlarse la red totalmente o en forma segmentada por canales de IRC, depender de DNS gratuitos que aseguran su movimiento permanente, cifrar el canal para evitar su rastreo, identificación o intromisiones de otras personas ajenas a la red.

→*¿Cómo infectar al equipo con una botnet?*

Los atacantes usan dos métodos para infectar las computadoras y estos forman parte de una botnet: *Ataques drive-by downloads* el proceso requiere de diferentes pasos y el atacante debe encontrar una página web con una vulnerabilidad que pueda explotar. Entonces, el atacante carga su código malicioso en la página y explota la vulnerabilidad en un navegador web como Google Chrome o Internet Explorer. El código redirige el navegador del usuario a otro sitio web controlado por el delincuente donde el código bot se descarga e instala en el equipo, y el segundo caso es vía email y claramente el proceso es más simple, es decir el atacante envía una gran cantidad de spam, donde se adjunta un archivo Word o PDF con un código malicioso o un enlace a la página que aloja el código. Una vez el código está en el equipo, la computadora se convierte en parte del botnet. El atacante puede manejar los comandos de forma remota, cargar datos en la maquina o hacer lo que realmente desee con el equipo.

►Ataque del Hombre del Medio – (Man in the Middle - (MitM))

Un ataque de MitM ocurre cuando un hacker se inserta entre las comunicaciones de un cliente y un servidor. Estos son algunos tipos comunes de ataques de MitM:



- Secuestro de sesión (Session Hijacking)

El atacante secuestra una sesión entre un cliente de confianza y un servidor de red. La computadora atacante sustituye su dirección IP por el cliente de confianza mientras el servidor continúa la sesión, creyendo que se está comunicando con el cliente.

Por ejemplo, el ataque podría desarrollarse así:

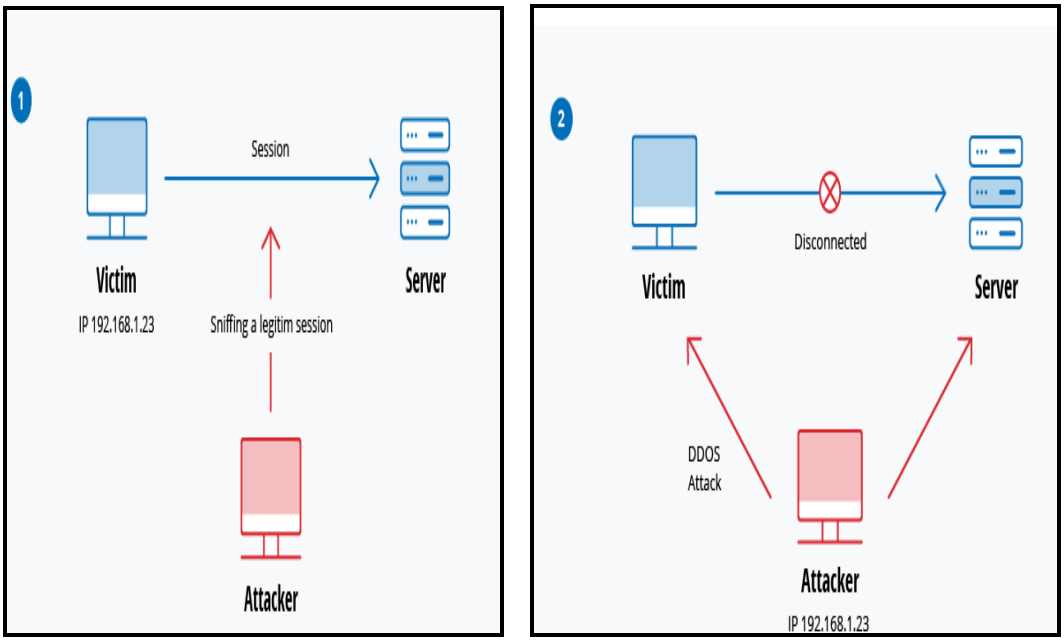
- Un cliente se conecta a un servidor.

- La computadora del atacante obtiene el control del cliente.

- La computadora del atacante desconecta al cliente del servidor.

- La computadora del atacante reemplaza la dirección IP del cliente con su propia dirección IP y falsifica los números de secuencia del cliente.

- La computadora del atacante continúa el diálogo con el servidor y el servidor cree que todavía se está comunicando con el cliente. A continuación, se muestra un ejemplo grafico de un ataque de MitM por secuestro de sesión.



- Suplantación de IP – (IP Spoofing)

La suplantación de IP es utilizada por un atacante para convencer a un sistema de que se está comunicando con una entidad conocida y confiable y proporcionarle al atacante acceso al sistema. El atacante envía un paquete con la dirección de origen IP de un host conocido y confiable en lugar de su propia dirección de origen IP a un host de destino. El host de destino puede aceptar el paquete y actuar sobre él.

Suplantar la dirección IP es posible gracias a que la dirección de origen y de destino que cada paquete IP contiene en su encabezado no están lo suficientemente protegidas contra la manipulación. Desafortunadamente no hay mecanismos para cifrar esta información ni para comprobar su veracidad. Sin embargo, con un simple ataque de IP spoofing el atacante no obtiene acceso al tráfico de datos. Es decir, este solo puede cambiar la dirección en el paquete correspondiente, mientras que **la dirección IP real se mantiene sin cambios**. Así, la respuesta con los datos emitidos no llegará al atacante, sino a la dirección del equipo que este introdujo.

El sistema que recibe la solicitud no tiene forma de saber que un tercero sin autorización se encuentra detrás del paquete IP, lo que hace que el IP spoofing sea de gran utilidad para los mencionados **ataques DoS y DDoS**. En particular, los dos siguientes escenarios son posibles:

1. Basándose en la dirección de origen, el atacante envía **muchos paquetes de datos a varios sistemas** dentro de la respectiva red. Estos responden enviando un paquete de datos a la computadora cuya dirección fue usurpada.

2. Un host de destino recibe, al mismo tiempo, **muchos paquetes de datos por parte de varias direcciones IP suplantadas** y, por lo tanto, se sobrecarga.

En ambos casos, debido a que los paquetes enviados parecen provenir oficialmente de parte de las computadoras cuyas IP fueron suplantadas, no es posible identificar a los atacantes**.**

►Suplantación de identidad Phishing

- ¿Qué es Phishing?

Phishing es el *robo datos y de identidad* realizado vía *correo electrónico y teléfono*, en el que el estafador se hace pasar por una entidad o una empresa prestataria de servicios al individuo en cuestión, de manera que este último le confíe al primero información personal sobre cuentas bancarias, contraseñas, y datos similares. El término *Phishing* proviene de la palabra inglesa *Fishing* que significa en español Pesca haciendo alusión al intento de hacer que los usuarios *"Piquen en el anzuelo".*

- Historia del Phishing

En los **años 70**, se formó una subcultura en torno a los ataques de baja tecnología para explotar el sistema telefónico. Estos primeros hackers se llamaban *“phreaks”,* una combinación de las palabras inglesas “Phone” (teléfono) y “Freak” (raro, friqui).

En una época en la que no había demasiadas computadoras en la red para hackear, el *phreaking* era una forma común de hacer llamadas gratuitas de larga distancia o llegar a números que no salían en los diarios.

La creación del término se atribuyó a un conocido *Spammer y Hacker* de mediados de los **años 90**, *Khan C Smith.* Asimismo, según los registros de Internet, la primera vez que se utilizó públicamente la palabra *Phishing* y quedó registrado fue el 2 de enero de 1996. La mención ocurrió en un grupo de noticias denominado *AOHell*. En ese momento, América Online (AOL) era el proveedor número uno de acceso a Internet, con millones de conexiones diarias.

Naturalmente, la popularidad de AOL la convirtió en blanco de los estafadores. Los hackers y piratas informáticos la utilizaron para comunicarse entre sí, así como para realizar ataques de *Phishing* contra usuarios legítimos. Cuando AOL adoptó medidas para cerrar AOHell, los atacantes recurrieron a otras técnicas.

Enviaban mensajes a los usuarios de AOL afirmando ser empleados de esta compañía y les pedían que verificaran sus cuentas y facilitaran la información de facturación. Con el tiempo, el problema creció tanto que AOL añadió advertencias en todos los programas cliente de correo electrónico y mensajería instantánea indicando que nadie que trabaje en AOL le pedirá su contraseña o información de facturación.

En la década de 2000, el *Phishing* dirigió su atención a explotar los Sistemas de Pago Online. Se hizo común que los *Phishers* dirigieran sus ataques a los clientes de servicios de pago bancario y online, algunos de los cuales, según investigaciones posteriores, fueron identificados correctamente y asociados al banco que verdaderamente utilizaban.

De igual forma, los sitios de redes sociales se convirtieron en un objetivo principal del *Phishing*, que era atractivo para los estafadores porque los detalles personales registrados en dichos sitios eran de utilidad para el robo de identidad. Los delincuentes registraron docenas de dominios que se hacían pasar por *eBay* y *PayPal* imitándolos tan bien que parecían reales si no se prestaba la suficiente atención.

Los clientes de *PayPal* recibieron entonces correos electrónicos de Phishing (con enlaces al sitio web falso), pidiéndoles que actualicen los números de su tarjeta de crédito y otra información personal. *The Banker* (una publicación propiedad de The Financial Times Ltd.) informó del primer ataque conocido de *Phishing* contra un banco en septiembre de 2003.

A **mediados de la década de 2000,** un software **"*Llave en mano*"** de *Phishing* estaba disponible en el mercado negro. Al mismo tiempo, grupos de hackers empezaron a organizarse para elaborar sofisticadas campañas de *Phishing*.

Las estimaciones de pérdidas debido al éxito de los ataques de P*hishing* durante este período varían con un informe de la empresa consultora de investigación de las tecnologías de información "*Gartner"* indica que entre Agosto del 2006 y Agosto del 2007 3,6 millón de adultos perdieron 3.200 millones de dólares.

En el **2011**, el *Phishing* encontró patrocinadores estatales cuando una presunta campaña china de Phishing atacó cuentas de Gmail de altos cargos políticos y mandos militares de los Estados Unidos y Corea del Sur, así como de activistas políticos chinos.

En el **2013**, en el evento posiblemente más famoso, se robaron 110 millones de registros de clientes y tarjetas de crédito de los clientes de *target*, por medio de la cuenta de una subcontratista suplantada con *Phishing*.

En el **primer trimestre del 2016**, se hizo una campaña de phishing lanzada por *Fancy Bear* (un grupo de ciberespionaje asociado con el departamento central de inteligencia ruso) contra las direcciones de correo electrónico asociadas con el comité nacional demócrata, por ejemplo la cuenta de Gmail del director de la campaña de Hillary Clinton en las elecciones presidenciales de 2016, John Podesta, fue hackeada con las filtraciones subsiguientes después de caer en el truco más antiguo: un ataque de Phishing que afirmaba que su contraseña de correo electrónico se había visto comprometida.

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

- Tipos de ataques de Phishing

A pesar de sus muchas variedades, el denominador común de todos los ataques de *Phishing* es el uso de un pretexto fraudulento para adquirir datos valiosos. Algunas categorías principales incluyen:

→ *Spear Phishing*

Mientras la mayoría de las campañas de Phishing envían correos electrónicos masivos al mayor número posible de personas, el **Spear Phishing** es un ataque dirigido, es decir ataca a una persona u organización específica, a menudo con contenido personalizado para la o las víctimas. Este tipo de ataque requiere un reconocimiento previo al ataque para descubrir nombres, cargos, direcciones de correo electrónico, etc. Los hackers buscan en Internet para relacionar esta información con lo que han averiguado sobre los colegas profesionales del objetivo, junto con los nombres y las relaciones profesionales de los empleados clave en sus organizaciones.

Con esto, el autor del Phishing crea un correo electrónico creíble. Por ejemplo, un estafador podría crear un ataque de Spear Phishing a un empleado cuyas responsabilidades incluyen la capacidad de autorizar pagos. El correo electrónico aparenta proceder de un ejecutivo en la organización, que exige al empleado que envíe un pago sustancial al ejecutivo o a un proveedor de la empresa (cuando en realidad el enlace del pago malicioso lo envía al atacante).

El objetivo final es el mismo, engañar al destinatario para que haga click en un enlace, URL o un archivo adjunto malicioso; pero, en este caso, el mensaje contiene el nombre, la empresa o el cargo de la víctima, o se mencionan a sus compañeros de trabajo y contactos.

Estos detalles personales hacen mucho más probable que el usuario abra o ejecute el contenido malicioso. Además, dada la proliferación de redes sociales y sitios web para hacer contactos profesionales a los ciberdelincuentes les resulta relativamente sencillo reunir la información personal necesaria para redactar un mensaje convincente.

→ *Whale Phishing*

Es el fraude dirigido a directores ejecutivos o ataques de correos electrónicos de empresa**.** Este tipo de phishing se dirige al equipo ejecutivo de una empresa con el fin de recopilar las credenciales de inicio de sesión de una *"Ballena"* **("Whale")**, es decir, un alto ejecutivo.

Una vez robados estos datos, los ciberdelincuentes pueden suplantar su identidad, llevando a cabo lo que se conoce como fraude dirigido a directores ejecutivos a través de correos electrónicos de empresa y autorizar transferencias bancarias u otras acciones de gran impacto. Un ejemplo de esto sería un **correo urgente** enviado **"desde"** la dirección de una directora ejecutiva al equipo de finanzas en el que autoriza una *transferencia de fondos,* porque está en china por negocios y necesita pagar urgentemente una factura a un proveedor del país.

→ *Phishing Telefónico*

Con los intentos de Phishing a través del teléfono, a veces llamados Phishing de Voz o **“Vishing**” que utiliza el protocolo voz sobre IP (VoIP), el Phisher llama afirmando representar a su banco local, la policía o incluso la agencia tributaria, lo asustan con algún tipo de problema e insisten en que lo solucione inmediatamente facilitando su información de cuenta o pagando una multa.

Normalmente le piden que pague con una transferencia bancaria o con tarjetas prepago, porque son imposibles de rastrear. Phishing vía SMS, o **“Smishing”** es el gemelo del vishing, que realiza el mismo tipo de estafa (algunas veces con un enlace malicioso incorporado en el que hacer click) por medio de un mensaje de texto SMS de esta forma los atacantes usan trucos de Ingeniería Social para crear algún tipo de alarma en los receptores de los mensajes, con indicaciones de urgencia, alarma y diferentes llamadas a la acción. La idea es que el usuario actúe de inmediato ante el estímulo y no se detenga a analizar los riesgos de su acción.

→ *Phishing Engañoso*

Este es el método de Phishing más frecuente, por el que los ciberdelincuentes suplantan la identidad de una empresa o dominio legítimos e intentan robar información de identificación personal o credenciales de inicio de sesión. Esta forma de Phishing a menudo carece de personalización y se difunde sin centrarse en un objetivo concreto. El atacante espera que si el volumen de mensajes es muy alto acabará abriéndolos el número de usuarios suficiente para lograr su objetivo.

Un ejemplo de este tipo de estafa sería un correo electrónico de Phishing de un "banco" que se envía a un gran número de personas, esperando que algunos de los destinatarios resulten ser clientes del banco suplantado. El asunto del correo electrónico suele escribirse de manera que genere una sensación de urgencia; por ejemplo, ***"Han robado su cuenta bancaria, actualice su contraseña inmediatamente"*** o ***"Factura vencida adjunta, páguela ahora para evitar acciones legales"***. Como se ha descrito anteriormente, una vez que se hace clic en el enlace y se envía la información, o se abre el archivo adjunto, el daño ya está hecho.

Siempre es recomendable acceder a las páginas web escribiendo la dirección directamente en el navegador y que contenga el protocolo seguro http(s). La mayoría de los ataques de Phishing comienzan con la recepción de un correo electrónico o un mensaje directo en el que el remitente se hace pasar por un banco o cualquier otra organización real con el fin de engañar al destinatario.

Este correo electrónico incluye links a un sitio web preparado por los criminales que imita al de la empresa legítima y en el que se invita a la víctima a introducir sus datos personales.

Un Ataque de Phishing usualmente incluye los siguientes cinco pasos:

1 - Identificar y seleccionar a las víctimas: Puede ser una campaña masiva o bien un ataque dirigido en el que se selecciona un grupo específico de destinatarios.

2 - Configurar el emisor del mensaje: Elegir una marca, crear un sitio de igual apariencia, armar un correo electrónico que parezca legítimo y finalmente, hacer parecer que el emisor del mensaje es legítimo (un contacto de la víctima, una dirección de correo de la marca).

3 - Distribución del ataque: Se envían los correos con enlaces a los sitios Phishing y se generan publicidades y participaciones en foros que también lleven al sitio ficticio. Esto se realiza acorde al público seleccionado en el primer paso, en términos de idioma, tipo de invitación, intereses, etc.

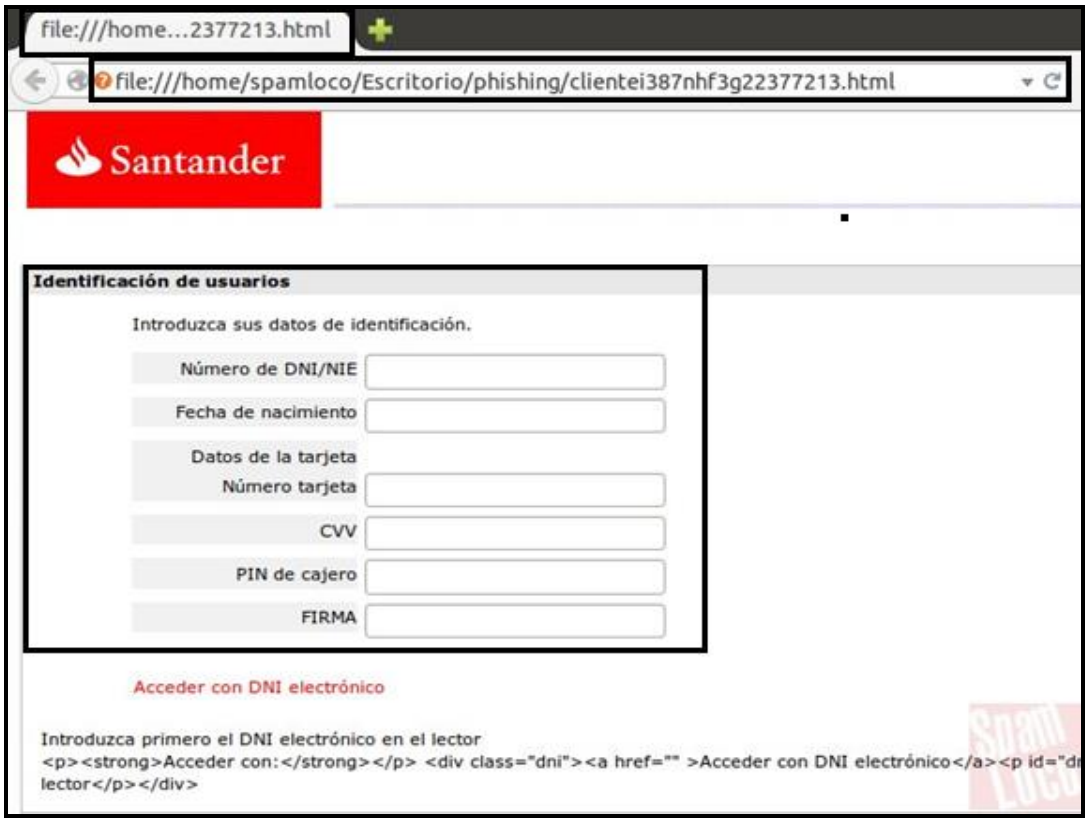
4 – Las víctimas caen en el engaño: Ingresan a enlaces fraudulentos y completan sus datos o responden los correos entregando la información.

5 - Monetizar el ataque → Se busca ganancia financiera vendiendo las credenciales obtenidas y accediendo a cuentas de pago de las víctimas. La información obtenida puede ser también el punto de partida para nuevos ataques o fases subsiguientes del mismo.

A continuación, se muestra un claro ejemplo de ataque de Phishing en forma gráfica para un mayor entendimiento.

Se ejecuto en conocido Banco Santander, el cual la victima recibe un e-mail con el siguiente asunto: ***¡SE HA LIMITADO SU TARJETA DE BANCO! Informa que por seguridad la tarjeta se ha desactivado e incluye un enlace para reactivarla***. El enlace en realidad lo redirecciona hacia una página falsa con solo pasar el cursor sobre el link es fácil detectarlo, teniendo un conocimiento previo sobre la operatoria del ataque de phishing.

El correo falso además incluye como adjunto un archivo **.html** que al ser abierto en el navegador carga un formulario que solicita los datos copiando el diseño web del Banco. Si la víctima piensa que se trata de algo real, terminará enviando sus datos al ciberdelincuente:



Generalmente este tipo de correos falsos terminan en las *bandejas de spam y son ignorados*, pero a veces pueden filtrarse dependiendo del servicio de correo que utilicemos o los usuarios abrirlos creyendo que son legítimos. Así que, no está de más comentarlos y compartir las capturas para alertar o reportarlos como correo no deseado o suplantación de identidad o phishing.

Siempre que reciba un correo de su banco procure analizar el contexto en el cual se envía. Si es algo inesperado no confíe en los enlaces ni adjuntos, lo ideal es llamar a la entidad o ir personalmente para hacer cualquier consulta sobre el estado de la tarjeta o la cuenta. También puede ingresar directamente al home Banking desde la página del banco para verificar el estado, pero es importante que lo haga escribiendo la URL letra por letra en el navegador y se asegure de que es la correcta.

Podría citar muchos otros ejemplos de *Phishing* que ocurren a diario, pero con la idea de materializar el concepto de una manera visible sobre la ejecución de este tipo de ataque, a modo ejemplo se explica en la siguiente Figura.

Se trata de un caso muy común que se llevó a cabo en Argentina, el cual, como dato no menor, según el informe presentado en la *8° Cumbre de Analistas de Seguridad para América latina*, este país se encuentra en un tercer lugar a nivel de países latinoamericanos con más víctimas de phishing detrás de países como Brasil y Venezuela. Este hecho ocurrió en la muy conocida plataforma de video llamada NETFLIX, donde el usuario recibía un email en su casilla de correo, solicitando que actualice su método de pago de su supuesta membresía, cuando el usuario presionaba el enlace adjunto al cual llevaba el mail para verificar los datos no correspondía a ninguna dirección oficial de la plataforma, ni tampoco aparecía el nombre de la misma en la composición del link.

►Ataque de Conducción – (Drive-By Attack)

→ *Que es el ataque de Conducción*

Los ataques de descarga drive-by son un método común para propagar *malware*. Los hackers buscan sitios web inseguros y plantan un script malicioso en el código HTTP o PHP en una de las páginas.

Este script puede instalar *malware* directamente en la computadora de alguien que visita el sitio o puede redirigir a la víctima a un sitio controlado por los hackers. Las descargas automáticas pueden ocurrir al visitar un sitio web, al ver un mensaje de correo electrónico o una ventana/mensaje emergente. Un *Drive-By* no depende de que un usuario haga nada para habilitar activamente el ataque: no tiene que hacer clic en un botón de descarga o abrir un archivo adjunto de correo electrónico malicioso para infectarse; una descarga no autorizada puede aprovechar una aplicación, sistema operativo o navegador web que contiene fallas de seguridad debido a actualizaciones fallidas o falta de actualizaciones.

→ *¿Como funciona el ataque de conducción?*

Este tipo de ataques explotan vulnerabilidades en navegadores web, complementos o bien otros componentes de los navegadores y pueden adoptar múltiples formas.

Por poner un ejemplo, puede estar navegando ingenuamente por la Web y llegar a un sitio que descarga *malware* en su máquina. El sitio podría haber sido creado por ciberdelincuentes, con el propósito de infectar las computadoras de las personas, o bien podría ser un sitio lícito que los ciberdelincuentes pusieron en riesgo mediante las vulnerabilidades existentes en el lugar.

Otra forma común en que las descargas drive-by se distribuyen es mediante redes promocionales. Otro ejemplo es cuando visitamos una página y de pronto aparezca una ventana emergente que parece la de un programa antivirus lícito, que avisa de la detección de un virus y solicita que haga click para conseguir un análisis de virus gratis.

Aunque el software antivirus malicioso y los exploits como este son un riesgo real, no son la mayor amenaza pues desde los departamentos de TI pueden dar instrucciones a los usuarios finales a fin de que no caigan en esta trampa.

►Ataque de Contraseña – (Password Attack)

Debido a que las contraseñas representan el mecanismo más utilizado para autenticar a los usuarios en un sistema de información, obtener contraseñas es un enfoque de ataque común y efectivo. El acceso a la contraseña de una persona se puede obtener mirando alrededor del escritorio de la persona, "Olfateando o Sniffeando" la conexión a la red para adquirir contraseñas sin cifrar, utilizando ingeniería social, obteniendo acceso a una base de datos de contraseñas o adivinando directamente. Existen dos tipos de ataque de contraseña, ya sea por fuerza bruta o ataque de diccionario o de manera aleatoria o manera sistemática:

- Ataque por Fuerza Bruta

Para adivinar la contraseña se usa este ataque siendo un enfoque aleatorio probando diferentes contraseñas y esperando que funcione. Se puede aplicar cierta lógica probando contraseñas relacionadas con el nombre de la persona, el cargo, los pasatiempos o elementos similares.

Generalmente, los ataques de fuerza bruta tienen mayor éxito en los casos en los que se utilizan contraseñas débiles o relativamente fáciles de predecir.

El término “fuerza bruta” relacionado con incidentes de seguridad informática está asociado a los intentos por conseguir averiguar una o varias contraseñas. Estas pueden estar vinculadas a accesos a servicios online o a ficheros y mensajes cifrados. En cualquier caso, el atacante va probando diversas combinaciones hasta dar con la correcta. Para ello se apoya en el uso de software, hardware, así como también en algoritmos y diccionarios de palabras. En cuanto al hardware que se utiliza, cuanta más potencia se tenga más combinaciones por segundo se podrán evaluar, mientras que en lo que respecta el software, existen programas que son utilizados desde hace tiempo para aplicar la fuerza bruta en el descifrado de contraseña. Un software clásico sería John the Ripper, que permite ser usado para tratar de romper varios algoritmos de cifrado o hash como **DES SHA-1** y otros.

También son muy usadas las herramientas que permiten averiguar contraseñas de redes Wi-Fi como Aircrack-ng.

Aprovechando los millones de credenciales filtradas a lo largo del tiempo, se prueban en distintos servicios online combinación de diferentes nombres de usuarios y contraseñas hasta dar con alguna combinación que permita un acceso.

Otro tipo de ataque de fuerza bruta es el que se conoce como *"credential stuffing"* o relleno de credenciales. Si bien es similar al de fuerza bruta inverso, la diferencia es que, en estos casos, con el objetivo de acceder a un sistema el atacante utiliza combinaciones de nombres de usuario/contraseña que tiene en su poder y que se filtraron en alguna brecha, sobre todo teniendo en cuenta que muchos usuarios suelen reutilizar las contraseñas en más de una cuenta; una práctica no recomendada.

- Ataque de Diccionario

Se utiliza un diccionario de contraseñas comunes para intentar obtener acceso a la computadora y la red de un usuario.

Un enfoque aplicado es copiar un archivo cifrado que contiene las contraseñas, aplicar el mismo cifrado a un diccionario de contraseñas de uso común y comparar los resultados.

►Ataque de Cumpleaños – (Birthday Attack)

Los ataques de cumpleaños se realizan contra algoritmos hash que se usan para verificar la integridad de un mensaje, software o firma digital. Un mensaje procesado por una función hash produce un Resumen de Mensaje o MD de longitud fija, independiente de la longitud del mensaje de entrada, este MD caracteriza de manera única el mensaje. El ataque de cumpleaños se refiere a la probabilidad de encontrar dos mensajes aleatorios que generan el mismo MD cuando es procesado por una función hash. Si un atacante calcula el mismo MD para su mensaje que el usuario, puede reemplazar con seguridad el mensaje del usuario con el suyo y el receptor no podrá detectar el reemplazo incluso si compara los MD.

Este es un tipo de tipo de ataque criptográfico que pertenece a una clase de ataque de fuerza bruta. El éxito de este ataque depende en gran medida de la mayor probabilidad de colisiones encontradas entre los intentos de ataque aleatorio y un grado fijo de permutaciones.

►Ataque de Inyección de SQL – (SQL Injection Attack)

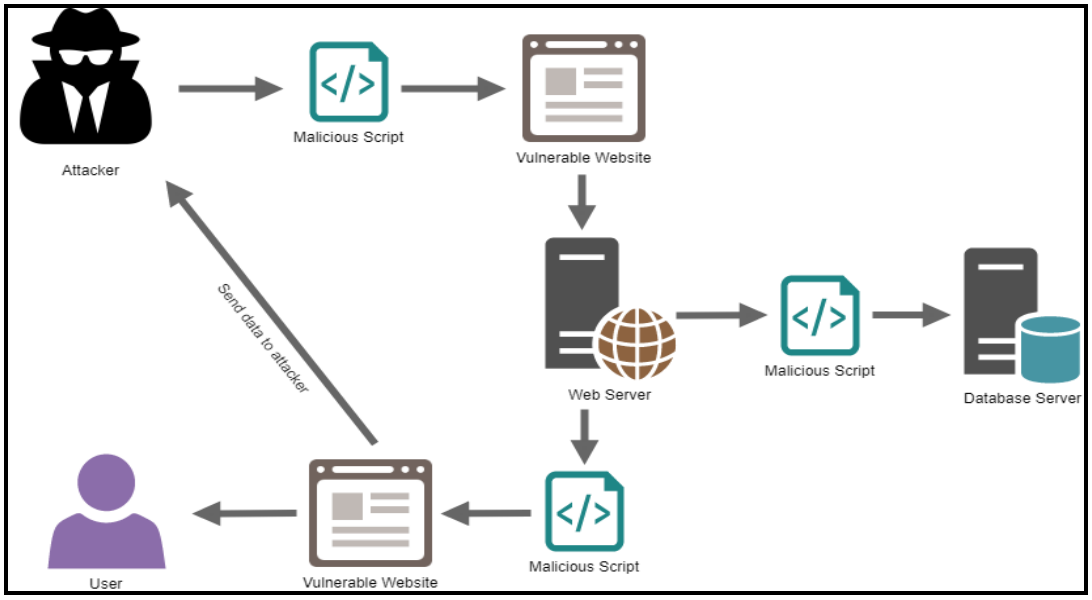
El lenguaje de consulta estructurado SQL se utiliza para consultar, operar y administrar sistemas de bases de datos como Microsoft SQL Server, Oracle o MySQL. SQL es consistente en todos los sistemas de bases de datos que lo admiten; sin embargo, hay complejidades que son particulares de cada sistema.

Un ataque de inyección SQL es un ataque que tiene como objetivo alterar la intención original de la aplicación mediante el envío de declaraciones SQL proporcionadas por el atacante directamente a la base de datos del backend, dependiendo de la aplicación web y de cómo procesa los datos suministrados por el atacante antes de crear una declaración SQL. Un ataque de inyección SQL exitoso puede tener implicaciones de largo alcance.

►Ataque XSS – (Cross-Site Scripting XSS Attack)

XSS es el proceso de agregar código malicioso a un sitio web legítimo para recopilar información del usuario con un propósito delictivo. Los ataques XSS se realizan gracias a las vulnerabilidades de seguridad que se encuentran en las aplicaciones web y se explotan comúnmente mediante la inyección de un script del lado del cliente. Por ejemplo, se podría enviar la cookie de la víctima al servidor del atacante, el atacante puede extraerla y usarla para el secuestro de sesión. Las consecuencias más peligrosas se producen cuando el XSS se utiliza para explotar vulnerabilidades adicionales. Estas vulnerabilidades pueden permitir a un atacante no solo robar cookies, sino también registrar pulsaciones de teclas, hacer capturas de pantallas, descubrir y recopilar información de red, y acceder y controlar de forma remota la máquina de la víctima.

En el siguiente grafico se visualiza un ejemplo de un ataque XSS



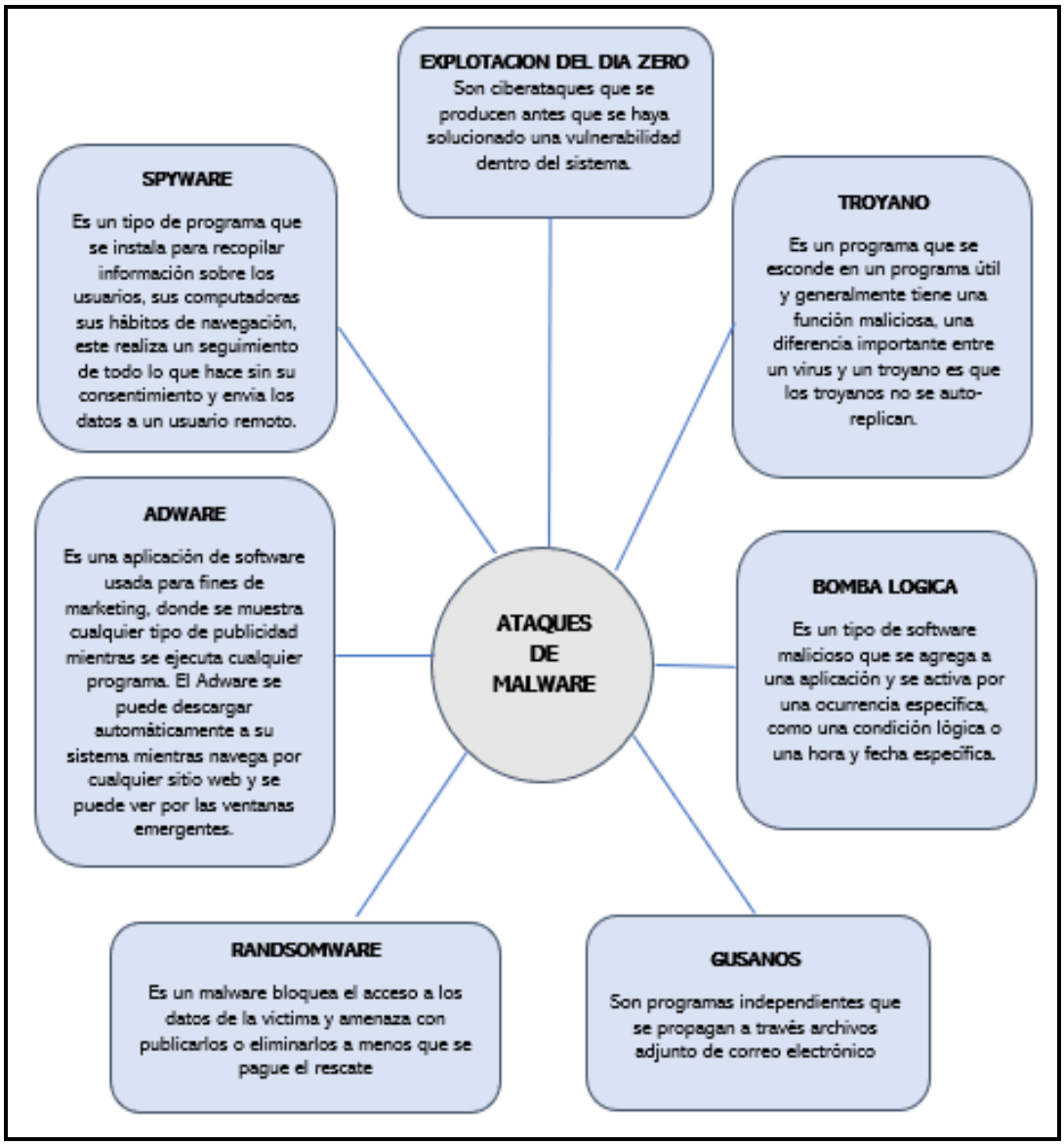
►Ataque de Espionaje – (Eavesdropping Attack)

Los ataques de espionaje ocurren a través de la intercepción del tráfico de la red. Al escuchar a escondidas, un atacante puede obtener contraseñas, números de tarjetas de crédito y otra información confidencial que un usuario podría estar enviando a través de la red. Las escuchas pueden ser *pasivas* cuando un atacante detecta la información escuchando la transmisión de mensajes en la red o *activas* cuando un atacante capta activamente la información disfrazándose de unidad amiga y enviando consultas a los transmisores, Esto se llama sondeo, escaneo o manipulación.

► Infecciones por Malware – (Malware Attack)

Malware o software malicioso, que incluye bots de *spyware*, *ransomware*, virus, gusanos, adware, errores y rootkits. El *malware* infringe una red a través de una vulnerabilidad, generalmente es cuando un usuario hace click en algún enlace o archivo adjunto de un correo electrónico, de esta forma instala el software maligno, una vez este dentro del sistema, el *malware* puede hacer las siguientes acciones: bloquear el acceso a componentes clave de la red, instalar algún software peligroso adicional, obtener información de forma encubierta transmitiendo datos desde un

disco duro, alterar ciertos componentes y dejar el sistema inoperable. En la siguiente grafica se detalla algunos de los tipos más comunes de *malware*:



BIBLIOGRAFIA

[1] Legislación oficial de la Unión Europea, Concepto de ciberataque a un Infraestructura Crítica Europea, https://www.boe.es/doue/2019/129/L01001-01012.pdf (Consultada el 02/08/2020).

[2] Arias, Fidias, G., Proyecto de investigación, Introducción a la Metodología Científica, Editorial Episteme, Caracas, 2012.

[3] Empresa de tecnología Check Point Software Technologies ltd, ¿Que es un Ciberataque?, https://www.checkpoint.com/cyber-hub/cyber-security/what-is-cyber-attack/ (Consultada el 13/04/2019).

[4] Empresa de Tecnología IBM, ¿Qué es un Ciberataque?, https://www.ibm.com/services/business-continuity/cyber-attack (Consultada el 01/03/2018).

[5] Empresa de Tecnología Cisco, ¿Qué es un Ciberataque?, https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html (Consultada el 15/06/2019).

[6] Agencia Gubernamental Australiana, Infraestructura Critica de Australia, https://www.homeaffairs.gov.au/nat-security/files/cic-factsheet-what-is-critical-infrastructure-centre.pdf (Consultada el 10/10/2018).

[7] Seguridad Publica de Canadá, Infraestructura Critica en Canadá. https://www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/index-en.aspx (Consultada el 20/11/2019).

[8] Centro de Protección Nacional de Infraestructura de Reino Unido, Infraestructura Critica en UK, https://www.cpni.gov.uk/critical-national-infrastructure-0 (Consultada el 25/07/2018).

[9] Departamento de Seguridad Nacional de los Estados Unidos, Infraestructura Critica en Estados Unidos, https://www.dhs.gov/topic/critical-infrastructure-security# (Consultada el 10/05/2020).

[10] Dirección General de la Comisión Europea, Infraestructura Critica en Europa. https://ec.europa.eu/home-affairs/tags/critical-infrastructure_en (Consultada el 12/12/2019).

[11] Empresa de seguridad digital internacional ThalesGroup, Infraestructura Critica en España, https://www.thalesgroup.com/es/espana/magazine/como-se-protegen-las-infraestructuras-criticas (Consultada el 10/02/2020).

[12] Sitio web oficial de la Autoridad del sistema de información de Estonia, Infraestructuras Críticas en Estonia, https://www.ria.ee/en/cyber-security/critical-information-infrastructure-protection-ciip.html (Consultado el 01/08/2020).

[13] Departamento de Seguridad Nacional de los Estados Unidos, Cantidad de Infraestructuras Criticas en EE.UU, https://www.dhs.gov/cisa/critical-infrastructure-sectors (Consultada el 10/05/2020).

[14] Parlamento del Reino Unido, Cantidad de Infraestructura Critica en Reino Unido, https://www.parliament.uk/documents/post/postpn389_cyber-security-in-the-UK.pdf (Consultada el 12/04/2020).

[15] Blog del Consultor Internacional de Seguridad Pública y Privada y socio-consejero del circuito de inteligencia Manuel Sánchez Gómez - Merelo, Infraestructuras Críticas y Ciberseguridad en España Cantidad de IC en España, https://manuelsanchez.com/2018/02/06/infraestructuras-criticas-en-latinoamerica-asignatura-de-seguridad-nacional/ (Consultado el 01/08/2020).

[16] Manual Internacional de Protección de Infraestructuras Críticas, Clasificación por País/Cantidad de IC - 2008/2009 (Ultima Actualización), https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CIIP-HB-08-09.pdf (Consultado el 01/08/2018).

[17] Cantidad de Infraestructuras Críticas en los Estados Unidos, IC de los EE.UU, https://websites.fraunhofer.de/CIPedia/index.php/Critical_Information_Infrastructure#United_States (Consultado el 10/09/2020).

[18] Sitio web oficial del Centro Nacional de Respuesta a incidentes de Seguridad Informática, ICI en Uruguay, https://www.gub.uy/centro-nacional-respuesta-incidentes-seguridad-informatica/?MOD=AJPERES (Consultada el 01/03/2018).

[19] Estrategia Nacional de Seguridad del Ciberespacio, ICI en China, http://politics.people.com.cn/n1/2016/1227/c1001-28980829.html (Consultada el 24/11/2019).

[20] Protección de la Infraestructura de Información Crítica, ICI en Estonia, https://www.ria.ee/et/kuberturvalisus/kriitilise-informatsiooni-infrastruktuuri-kaitse.html (Consultada el 15/06/2019).

[21] Sitio web oficial del Departamento del Gobierno de Reino Unido. Sector de Seguridad y Planes de Resiliencia, ICI en UK, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/678927/Public_Summary_of_Sector_Security_and_Resilience_Plans_2017__FINAL_pdf__002_.pdf (Consultada el 18/10/2018).

[22] Centro Nacional de Protección de Infraestructura de Información Crítica de la India, ICI de la India, https://www.nciipc.gov.in (Consultada el 28/09/2018).

[23] Blog del Consultor Internacional de Seguridad Pública y Privada y socio-consejero del circuito de inteligencia Manuel Sánchez Gómez - Merelo, Infraestructuras Críticas y Ciberseguridad en España Cantidad de IC en España, Definición de las ICI en España. https://manuelsanchez.com/2011/07/06/infraestructuras-criticas-y-ciberseguridad/ (Consultada el 19/12/2019).

[24] Sitio web oficial del gobierno de Kosovo - Estrategia de Ciberseguridad Nacional de Kosovo (2016 – 2019), ICI en Kosovo.http://www.kryeministri-ks.net/repository/docs/National_Cyber_Security_Strategy_and_Action_Plan_2016-2019_per_publikim_1202.pdf (Consultada el 25/10/2019).

[25] Sitio Web Gobierno Estadounidense, USA Patriot Act de 2001 – EEUU, https://www.congress.gov/107/plaws/publ56/PLAW-107publ56.pdf (Consultada el 16/06/2019).

[26] Sitio web oficial del Departamento de Seguridad Nacional de los Estados Unidos, Critical Infrastructure Information Act of 2002, https://www.dhs.gov/sites/default/files/publications/CII-Act_508_0.pdf (Consultada el 01/07/2020).

[27] Sitio web oficial de la Agencia de seguridad de infraestructura y ciberseguridad de los Estados Unidos, Directiva Presidencial 7 de Seguridad Nacional, https://www.cisa.gov/homeland-security-presidential-directive-7 (Consultada el 21/10/2019).

[28] Departamento de Seguridad Nacional de los Estados Unidos, Estrategia Nacional para la Protección Física de Infraestructuras Críticas y Activos Clave, http://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf (Consultada el 01/09/2019).

[29] Documento Expuesto para presentación como fuente confiable del Homeland Security, NIPP – EEUU, https://www.slideserve.com/nigel-west/national-infrastructure-protection-plan-nipp-powerpoint-ppt-presentation (Consultada el 02/05/2020).

[30] Sitio web oficial de la Comisión Reguladora Federal de Energía en los Estados Unidos, ¿Que es FERC?, https://www.ferc.gov/about/what-ferc (Consultada el 20/02/2020).

[31] Sitio web oficial de la Autoridad Reguladora Internacional de América del Norte, ¿Que es NERC?, https://www.nerc.com/AboutNERC/Pages/default.aspx (Consultada el 21/02/2020).

[32] Sitio web oficial the White House President Barack Obama, Directiva de Política Presidencial PPD-21: Seguridad y Resiliencia de la Infraestructura Crítica, https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil (Consultada el 25/10/2019).

[33] Sitio web oficial de la casa blanca de EE.UU, Estrategia Nacional de Ciberseguridad de los Estados Unidos. https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf (Consultada el 16/08/2020).

[34] Sitio web oficial de ENISA, ¿Que hace ENISA?, https://www.enisa.europa.eu/about-enisa (Consultada el 19/06/2020).

[35] Legislación oficial de la Unión Europea, Libro Verde o Green Paper on a European Programme for Critical Infrastructure Protection. https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:52005DC0576 (Consultada el 22/06/2019).

[36] Legislación oficial de la Unión Europea, - PEPIC - Programa Europeo de Protección de Infraestructuras Críticas, https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=legissum:l33260 (Consultada el 15/12/2019).

[37] Oficina de Publicaciones de la Unión Europea, Directiva 2008/114/CE del Consejo de 8 de diciembre de 2008 sobre la Identificación y Designación de Infraestructuras Críticas Europeas y la Evaluación de la Necesidad de Mejorar su Protección, La Comisión Europea aprobó la Directiva el 8 de diciembre de 2008, https://op.europa.eu/es/publication-detail/-/publication/ba51b03f-66f4-4807-bf7d-c66244414b10/language-es (Consultada el 10/09/2019).

[38] Sitio web oficial de la Red Europea de Ciberseguridad, ¿Que es ENCS?, https://encs.eu/ (Consultada el 29/03/2020).

[39] Legislación oficial de la Unión Europea, Reglamento sobre la Ciberseguridad de la Unión Europea, https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=LEGISSUM:4398780 (Consultada el 02/08/2020).

[40] Sitio web del Boletín Oficial del Estado Español, Real Decreto 421/2004 del 12 de Marzo, https://www.boe.es/eli/es/rd/2004/03/12/421/con (Consultada el 10/12/2019).

[41] Centro Criptológico Nacional - CERT España, ¿Que hace el CCN-CERT?, https://www.ccn-cert.cni.es/sobre-nosotros/mision-y-objetivos.html (Consultada el 02/04/2020).

[42] Sitio web oficial del Centro Nacional de Protección de Infraestructuras y Ciberseguridad Español, ¿Que hace CNPIC en España?. http://www.cnpic.es/en/ (Consultada el 29/07/2019).

[43] Boletín Oficial del Estado Español, Ley 8/2011 Medidas para la Protección de IC. https://www.boe.es/buscar/pdf/2011/BOE-A-2011-7630-consolidado.pdf (Consultada el 20/12/2018).

[44] Sitio web oficial del Departamento de Seguridad Nacional de España, Estrategia de Ciberseguridad Nacional Española, https://www.dsn.gob.es/sites/dsn/files/estrategia%20de%20ciberseguridad%20nacional.pdf (Consultada el 11/08/2020).

[45] Sitio web oficial del Instituto Nacional de Ciberseguridad Español, ¿Que es el INCIBE?, https://www.incibe.es/que-es-incibe (Consultada el 06/08/2020).

[46] Sitio web oficial del Centro de protección de la Infraestructura Nacional de Reino Unido, ¿Cuál es la función del CPNI?, https://www.cpni.gov.uk/about (Consultada el 02/09/2019).

[47] Sitio web oficial del Centro Nacional de Ciberseguridad del Reino Unido, ¿Que hace el NCSC?, https://www.ncsc.gov.uk/section/about-ncsc/what-we-do (Consultada el 10/06/2020).

[48] Sitio web oficial del Departamento Australiano de Inteligencia de Seguridad, ¿Cuál es la función de la organización ASIO?, https://www.asio.gov.au/what-we-do.html (Consultada el 16/08/2019).

[49] Centro de Infraestructura Critica Australiano, Red de intercambio de información confiable (TISN), https://cicentre.gov.au/tisn (Consultada el (10/08/2020).

[50] Sitio web oficial del Gobierno Australiano, Consejo Asesor de Infraestructura Critica de Australia (CIAC), https://www.directory.gov.au/portfolios/home-affairs/trusted-information-sharing-network-critical-infrastructure-resilience (Consultada el 26/12/2018).

[51] Sitio web oficial de Centro de Ciberseguridad Australiano, Función del ACSC, https://www.cyber.gov.au/acsc/large-organisations-and-infrastructure/critical-infrastructure (Consultada el 01/09/2020).

[52] Sitio web oficial de Centro de Infraestructura Critica Australiana, ¿Que función tiene el CiCentre?, https://cicentre.gov.au/ (Consultada el 01/08/2019).

[53] Sitio web oficial de la Agencia Gubernamental Australiana, Ley de seguridad de infraestructura crítica 2018. https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/security-coordination/security-of-critical-infrastructure-act-2018 (Consultada el 14/09/2019).

[54] Sitio web oficial del Gobierno Canadiense, Departamento de Seguridad Pública de Canadá, https://www.publicsafety.gc.ca/cnt/ntnl-scrt/index-en.aspx (Consultada el 16/03/2020).

[55] Sitio web oficial del Gobierno Canadiense, Estrategia Nacional Canadiense de Infraestructura Critica, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/index-en.aspx (Consultada el 29/11/2019).

[56] Sitio web oficial del Gobierno Canadiense, Centro Canadiense de Respuestas a incidentes cibernéticos (CCIRC), https://www.publicsafety.gc.ca/cnt/trnsprnc/ccss-nfrmtn-prvc/prvc-mpct-ssssmnt/cndn-cbr-ncdnt-en.aspx (Consultada el 14/07/2020).

[57] Sitio web oficial de la Autoridad del sistema de información de Estonia, Función del CERT.EE en Estonia, https://www.ria.ee/en/cyber-security/cert-ee.html (Consultada el 12/08/2020).

[58] Sitio web oficial de la Autoridad del Sistema de información de Estonia, Estrategia Nacional de Estonia para la Protección de las ICI. https://www.ria.ee/en/cyber-security/critical-information-infrastructure-protection-ciip.html (Consultada el 12/08/2020).

[59] Sitio web oficial de la Autoridad del Sistema de información de Estonia, Ley de Ciberseguridad de Estonia, https://www.mkm.ee/sites/default/files/cyber_security_strategy_2014-2017_public_version.pdf (Consultada el 12/08/2020).

[60] Sitio web INFOLEG Información Legislativa avalado por el Ministerio de Justicia y Derechos Humanos Presidencia de la Nación, Reglamento de Operación del ArCERT Argentina. http://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/61122/norma.htm (Consultada el 19/09/2018).

[61] Sitio web INFOLEG Información Legislativa avalado por el Ministerio de Justicia y Derechos Humanos Presidencia de la Nación, ICIC - CERT [Argentina] (Articulo1°) http://servicios.infoleg.gob.ar/infolegInternet/anexos/215000-219999/219212/norma.htm (Consultado el 29/09/2019).

[62] Sitio web INFOLEG Información Legislativa avalado por el Ministerio de Justicia y Derechos Humanos Presidencia de la Nación, Creación de Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad (ICIC). [Argentina], Resolución 580/211. http://servicios.infoleg.gob.ar/infolegInternet/anexos/185000-189999/185055/norma.htm (Consultado el 29/09/2019).

[63] Sitio web INFOLEG Información Legislativa avalado por el Ministerio de Justicia y Derechos Humanos Presidencia de la Nación, Grupos de Trabajo ICIC - Argentina. http://servicios.infoleg.gob.ar/infolegInternet/anexos/215000-219999/219212/norma.htm (Consultado el 20/10/2020).

[64] Sitio web AFIP – Biblioteca Electrónica. Decreto N° 1067/2015, Creación de Subsecretaria de Protección de Infraestructuras Criticas de la información y Ciberseguridad. – Argentina. http://biblioteca.afip.gob.ar/dcp/DEC_C_001067_2015_06_10 (Consultado el 15/09/2020)

[65] Sitio web oficial de Argentina Presidencia**,** Boletín Oficial de la Republica de Argentina**,** Decreto N° 577/17, Comité de Ciberseguridad https://www.boletinoficial.gob.ar/detalleAviso/primera/211277/20190712 (Consultado el 24/08/2020).

[66] Consultora Argentina – Marval- Estrategia Nacional de Ciberseguridad de la Republica Argentina, https://marval.com/publicacion/estrategia-nacional-de-ciberseguridad-de-la-republica-argentina-13372 (Consultado el 25/08/2020).

[67] Sitio web INFOLEG Información Legislativa avalado por el Ministerio de Justicia y Derechos Humanos Presidencia de la Nación, Código penal Argentino Ley 26.388 de Delitos Informáticos. http://servicios.infoleg.gob.ar/infolegInternet/anexos/140000-144999/141790/norma.htm (Consultada el 09/09/2018).

[68] Sitio web INFOLEG Información Legislativa avalado por el Ministerio de Justicia y Derechos Humanos Presidencia de la Nación, Código penal Argentino Ley 25.326 de Protección de Datos Personales http://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/norma.htm (Consultada el 28/08/2020).

[69] Sitio web INFOLEG Información Legislativa avalado por el Ministerio de Justicia y Derechos Humanos Presidencia de la Nación, Código penal Argentino Ley 25.506 de Firma Digital http://servicios.infoleg.gob.ar/infolegInternet/anexos/70000-74999/70749/texact.htm (Consultada el 28/08/2020).

[70] Sitio web INFOLEG Información Legislativa avalado por el Ministerio de Justicia y Derechos Humanos Presidencia de la Nación, Código penal Argentino Ley 26.904 de Grooming http://servicios.infoleg.gob.ar/infolegInternet/anexos/220000-224999/223586/norma.htm (Consultada el 26/08/2020).

[71] Sitio web INFOLEG Información Legislativa avalado por el Ministerio de Justicia y Derechos Humanos Presidencia de la Nación, Código penal Argentino Ley 27.126 de Inteligencia Nacional http://servicios.i4nfoleg.gob.ar/infolegInternet/anexos/240000-244999/243821/norma.htm (Consultada el 20/08/2020).

[72] Repositorio/Foro de Seguridad, Grafico de tipos de ciberataques más comunes en las Infraestructuras críticas. https://www.pcwdld.com/cyber-attacks (Consultada el 13/03/2020)

[73] Repositorio/Foro de Seguridad, Ataques de Denegación de Servicio (DoS/DDoS), https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/ (Consultada el 05/01/2020).

[74] Blog Tecnología HighTech, Ataque inundación SYN o Inundación TCP/SYN, https://es.ccm.net/contents/14-ataque-syn (Consultada el 05/01/2020).

[75] Blog de seguridad Netwrix, Tipo de ciberataque de DDoS, Ping de la Muerte, https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/ (Consultada el 05/01/2020).

[76] Empresa Internacional de Seguridad Kaspersky, Ataque Smurf, https://latam.kaspersky.com/resource-center/definitions/what-is-a-smurf-attack (Consultada el 02/02/2020).

[77] Empresa de Ciberseguridad Internacional, Ataque Teardrop, https://security.radware.com/ddos-knowledge-center/ddospedia/teardrop-attack (Consultada el 05/07/2019).

[78] Empresa internacional Estadounidense de infraestructura web y seguridad de sitios web, Botnets. https://www.cloudflare.com/learning/ddos/what-is-a-ddos-botnet/ (Consultada el 11/12/2019).

[79] Blog de seguridad Netwrix, Ataque de MitM, https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/#Man-in-the-middle%20(MitM)%20attack (Consultada el 18/11/2020).

[80] Blog de seguridad Netwrix, Ataque de MitM - Secuestro de sesión, https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/#Man-in-the-middle%20(MitM)%20attack (Consultada el 05/10/2020).

[81] Empresa internacional (USA) de infraestructura web y seguridad de sitios web, Suplantación de IP – (IP Spoofing), https://www.cloudflare.com/es-es/learning/ddos/glossary/ip-spoofing/ (Consultada el 05/01/2020).

[82] Sitio oficial Panda Security (Empresa Española especializada en Seguridad Informática), Suplantación de Identidad Phishing, www.pandasecurity.com/es/security-info/phishing/ (Consultada el 25/10/2020).

[83] Sitio Oficial Kaspersky (Compañía Internacional de Seguridad Informática), Ataque de Conducción – (Drive-By Attack) https://www.kaspersky.com/resource-center/definitions/drive-by-download (Consultada el 16/01/2020).

[84] Blog de Seguridad Netwrix, Ataque por contraseña, https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/#Man-in-the-middle%20(MitM)%20attack (Consultada el 20/07/2020).

[85] Comunidad de investigación de la Compañía Internacional de Seguridad Informática ESET, Ataque de Fuerza Bruta. https://www.welivesecurity.com/la-es/2020/06/24/que-es-ataque-fuerza-bruta-como-funciona/ (Consultada el 20/08/2020).

[86] Sitio oficial Diccionario de informática y tecnología, Ataque de Diccionario, https://www.alegsa.com.ar/Dic/ataque_por_diccionario.php (Consultada el 25/06/2020).

[87] Blog de Seguridad Informática HostDime, Ataque de Cumpleaños, https://www.hostdime.com.pe/blog/tipos-mas-comunes-de-ataques-ciberneticos/ (Consultada el 15/07/2020).

[88] Blog de Seguridad Informática HostDime, Ataque de Inyección de SQL, https://www.hostdime.com.pe/blog/tipos-mas-comunes-de-ataques-ciberneticos/ (Consultada el 15/07/2020).

[89] Blog de Tecnología e información sobre Seguridad informática, ¿Como se hace un ataque XSS?, https://pc-solucion.es/2018/09/05/cross-site-xss (Consultada el 15/05/2020).

[90] Blog de Seguridad Informática HostDime, Ataque de Espionaje, https://www.hostdime.com.pe/blog/tipos-mas-comunes-de-ataques-ciberneticos/ (Consultada el 05/02/2020).

[91] Blog de Seguridad Informática HostDime, Ataque de Malware, https://www.hostdime.com.pe/blog/tipos-mas-comunes-de-ataques-ciberneticos/ (Consultada el 05/01/2020).

[92] Instituto Nacional de Estándares y Tecnología, (CSF-Cybersecurity Framework) o Marco de Trabajo de Ciberseguridad del NIST Versión1.1,https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf (Consultada el 04/10/2020).

[93] Estándar ISO/IEC 27032:2012. Tecnologías de la información - Técnicas de seguridad - Directrices para la Ciberseguridad, https://www.isecauditors.com/consultoria-csf-iso-27032 (Consultada el 04/10/2020).

BIBLIOGRAFIA GENERAL

- https://www.cisa.gov/critical-infrastructure-sectors
- https://es.malwarebytes.com/phishing/
- https://es.wikipedia.org/wiki/Botnet
- https://www.kaspersky.es/blog/que-es-un-botnet/755/
- https://www.kaspersky.es/blog/five-most-notorious-cyberattacks/17277/
- https://es.mailjet.com/blog/news/que-es-phishing/
- https://es.slideshare.net/nestorcusco/sistema-scada-249022
- https://core.ac.uk/download/pdf/226164978.pdf
- https://es.qaz.wiki/wiki/Bronze_Night
- https://www.magazcitum.com.mx/?p=3034#.X5Sh2s5KiM-
- https://www.youtube.com/watch?v=UgaD8Hrcp6Y
- https://es.ccm.net/contents/15-ataque-teardrop
- http://news.bbc.co.uk/2/hi/europe/6665195.stm
- https://www.hsdl.org/?abstract&did=473297
- https://www.crowe.com/es/insights/top3-ciberataques
- https://threatmap.checkpoint.com/
- https://www.redeszone.net/tutoriales/seguridad/ataque-syn-que-es/
- https://www.muycomputerpro.com/2015/01/05/ataque-sony-pictures
- https://www.redeszone.net/tutoriales/seguridad/tipos-ataques-phishing/
- https://cybermap.kaspersky.com/es/stats
- https://www.incibe-cert.es/blog/blackenergy-sistemas-criticos
- https://www.cursosaula21.com/que-es-un-sistema-scada/

► https://es.qaz.wiki/wiki/2007_cyberattacks_on_Estonia

► https://www.nato.int/docu/review/2013/Cyber/timeline/ES/index.htm

► https://es.qaz.wiki/wiki/Homeland_Security_Presidential_Directive_7

► https://uss.com.ar/corporativo/phishing-en-argentina/

► https://www.cloudflare.com/es-la/learning/ddos/ping-icmp-flood-ddos-attack/

► https://revista.une.org/15/ciberataques-dirigidos-a-infraestructuras-criticas.html

► https://www.elladodelmal.com/2016/10/ataques-ddos-con-amplificacion-via.html

► https://cursoslared.com/archivos/1529/tutorial-ataque-denegacion-servicio-dos

► https://www.spamloco.net/2014/05/dos-ejemplos-de-phishing- bancario-para-alertar.html

► https://www.smh.com.au/national/estonia-urges-firm-eu-nato-response-to-new-form-of-warfare-cyber-attacks-20070516-gdq5iu.html

► https://cronicaseguridad.com/2018/05/16/stuxnet-primera-ciberarma-historia

► https://observatorio.cisde.es/archivo/stuxnet-la-primera-batalla-de-la-guerra-de-iran/

► https://cnnespanol.cnn.com/2014/12/25/quien-causo-realmente-el-ataque-a-sony/

► https://arstechnica.com/information-technology/2016/01/analysis-confirms-coordinated-hack-attack-caused-ukrainian-power-outage/

►https://www.computing.es/seguridad/noticias/1108306002501/grupo-cibercriminal-blackenergy-vuelve-al-ataque.1.html

► https://www.elconfidencial.com/tecnologia/2016-01-21/amenazas-en-la-oscuridad-como-los-hackers-pueden-provocar-un-apagon-en-tu-ciudad_1138837/

► https://www.enigmasoftware.com/wannacryptorransomware-removal/?gclid=CjwKCAjwwab7BRBAEiwAapgpTKyw4WA-5tK4d-AHKpPwHda7CAdTU-MXUARNeE61UwHGpDjIGmkJ9xoCPbMQAvD_BwE

► https://www.lanacion.com.ar/el-mundo/ciberataque-ransomware-china-japon-tailandia-indonesia-nid2023961/

► http://repositoriouba.sisbi.uba.ar/gsdl/cgi-bin/library.cgi?e=p-10000-00---off-0--00-----0-10-0---0---0direct-10----4-------0-1l--10-es-Zz-1---20-biblioteca---0--1-00-00--4----0-0-01-00-0utfZz-8-00&a=p&p=about&c=tesuba

►https://books.google.com.ar/books?id=1n16CgAAQBAJ&printsec=frontcover&dq=ciberataques+en+la+infraestructuras+criticas+de+la+informacion&hl=es-419&sa=X&redir_esc=y#v=onepage&q&f=false

► https://www.technologyreview.es/s/7413/los-20-ciberataques-mas-perversos-del-siglo-xxi

► https://www.pandasecurity.com/es/mediacenter/noticias/ciberataques-hasta-la-fecha/

► https://www.ccn-cert.cni.es/eu/segurtasun-eguneratua/gaurkotasunari-buruzko-berriak/122-amenazas-mas-destacadas-de-septiembre-segun-eset.html

►https://www.ticpymes.es/tecnologia/noticias/1115836049504/protagonistas-del-cibercrimen-2019-ransomware-phishing-infraestructuras-criticas.1.html