

Universidad de Buenos Aires



**Facultades de Ciencias Económicas,
Ciencias Exactas y Naturales e Ingeniería**

**Carrera de Especialización en Seguridad
Informática**

Trabajo Final de Especialización

Tema

Ciberseguridad y Ciberdelitos

Título

**Estado situacional de la República Argentina en materia de
Ciberseguridad.-**

Autor: Ing. Juan Manuel Beltran

Tutor del Trabajo Final: Ing. Hugo Pagola

Año 2018

Cohorte 2013

Declaración Jurada:

Por medio de la presente, el autor manifiesta conocer y aceptar el Reglamento de Trabajos Finales vigente y 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

Juan Manuel Beltran
D.N.I. 18.580.646

Resumen

El presente trabajo pretende relevar e introducir la situación actual de la ciberseguridad y los ciberdelitos más frecuentes en nuestro país, a los fines de que las autoridades y facilitadores en seguridad informática puedan disponer la planificación de la estrategia e implementación de políticas específicas, a mediano y largo plazo, para el combate contra el ciberdelito y el aumento del nivel y calidad de la ciberseguridad.

En este orden de ideas, se plantea la situación actual, relevando fuentes públicas y homogeneizando los conceptos en un único documento con el objetivo que el mismo sea el disparador de otros trabajos e investigaciones en la materia.

El compromiso es la concientización de las autoridades en la situación actual, alcance y probables impactos de las acciones delictivas en tecnologías, a los efectos de que dichas autoridades posean la información necesaria para la toma de decisiones estratégicas e implementaciones tecnológicas, operativas, administrativas y elaboración de propuestas legislativas.

En esta inteligencia, y a fin de ahorrar espacio y tiempo, se evita todo tipo de introducción básica y terminología ampliamente conocida por los potenciales lectores (a excepción de la terminología mínima) con el objetivo de mostrar casos puntuales, desarrollo, conclusiones y propuestas.

En virtud de ello, las leyes, decretos, convenios, resoluciones y toda información aclaratoria o ampliatoria, se ha colocado aparte, en forma de “Anexos” al informe principal para facilitar y reducir al mínimo el contenido concreto del mismo.

Palabras clave: Ciberseguridad, Ciberdelito, Seguridad Informática en Argentina.

Índice

Introducción – Capítulo I	8
1.1 Definiciones necesarias para contextualizar el análisis pretendido	9
1.1.1 Ciberdelitos	9
Capítulo 2	11
2.1 Plataformas frecuentemente utilizadas para la comisión de ciberdelitos	11
2.1.1 Criptomonedas.....	11
2.2 Herramientas informáticas utilizadas por el ciberdelitos.....	20
2.2.1 Deep Web o web profunda	20
2.2.2 Navegadores Anónimos.....	24
2.2.3 Navegador TOR.....	24
2.2.3 Vulnerabilidad o Exploit ZERO DAY (día cero).....	26
2.3.1 Phishing	29
2.3.2 Botnets.....	29
2.3.3 Denegación de Servicios	30
2.3.4 Ataques de denegación de servicio distribuidos (DDoS)	30
2.3.5 Ransomware.....	31
2.3.6 BEC	34
2.4 Impactos de los Ciberdelitos más importantes realizados hasta el momento.....	38
2.5 Ataques desde Rusia a la campaña presidencial del partido demócrata de los Estados Unidos de Norteamérica.....	40
2.6 Delito Tecnológico de elevado daño estratégico - IMSI Catcher	43
Capítulo 3 - Marco Normativo	46
3.1 Legislación Argentina.....	46
3.2 Infraestructuras Críticas de Información y Ciberseguridad	47

Capítulo 4 - Indicadores Internacionales.....	50
4.1 Proyecto Índice Mundial de Ciberseguridad	50
4.2 Categorías e indicadores de rendimiento	54
4.3 Medidas jurídicas.....	54
4.5 Reglamento y conformidad	55
4.6 Medidas técnicas	56
4.7 CERT/CIRT/CSIRT	57
4.8 Normas	57
4.9 Certificación	58
4.10 Medidas organizativas	58
4.11 Política	59
4.12 Hoja de ruta para la gobernanza	60
4.13 Organismo responsable.....	60
4.14 Evaluación comparativa nacional.....	61
4.15 Creación de capacidades	61
4.16 Desarrollo de la normalización.....	62
4.17 Desarrollo laboral.....	62
4.18 Certificación profesional.....	63
4.19 Certificación del organismo.....	63
4.20 Cooperación	64
4.21 Cooperación interestatal	64
4.22 Cooperación entre organismos.....	65
4.23 Asociaciones entre los sectores público y privado.....	65
4.24 Cooperación internacional	66
4.25 Metodología del Índice de Ciberseguridad.....	66
4.26 Repercusión.....	68
Capítulo 5 - Respuestas o esfuerzos institucionales:	75

5.1 ICIC.....	75
5.2 Creación del Comité de Ciberseguridad	78
5.3 Comparativa de la Estrategia de otros países	79
5.3.1 Australia - Estrategia de Ciberseguridad de Australia (2016)	79
5.3.2 Canadá - Estrategia de Ciberseguridad de Canadá (2010)	80
5.3.3 Colombia - Política Nacional de Seguridad Digital (2016)	80
5.3.4 Estonia (alto índice de informatización y gobierno electrónico) - Estrategia de Ciberseguridad (2014–2017)	81
5.3.5 Los Países Bajos - Estrategia Nacional de Ciberseguridad (2013) ..	81
5.3.6 Estados Unidos - Estrategia de Ciberseguridad y Plan de Implementación 2015.....	82
5.3.7 España - Estrategia de Ciberseguridad Nacional (2013).....	83
Capítulo 6 - Contramedidas a difundir – “Evangelización”:	85
6.1 Simples medidas contra los ataques más implementados en la República Argentina durante 2016-2017	85
6.1.1 Phishing	85
6.1.2 Ransomware.....	86
6.1.3 Uso ilegal del Bitcoin.....	87
6.1.4 Pasos para evitar el uso de Bitcoin en el lavado de dinero.....	89
6.1.5 BEC	89
Capítulo 7 – Capítulo Final – Propuestas y Conclusiones	91
7.1 - Propuestas de Legislación y medidas tecnológicas, operativas y administrativas	91
7.1.1 Ciberpatrullaje Web Profunda (Deep Web).....	91
7.1.2 Adhesión al Convenio de Budapest	92
7.1.3 Proyecto de Ley sobre Pornografía Infantil.....	95
7.1.4 Explotación de Fuentes Abiertas	95

7.1.5 Registro por parte de las prestadoras de Telefonía Celular GSM, de la Señalización (especialmente afiliación) de los aparatos celulares a cada celda.	96
7.1.5.1 Utilización	98
7.2.1 Reformulación de la Ley 25.873 (El cual consta como Anexo III).....	99
7.3 Propuestas Tecnológicas-Operativas	99
7.3.1 Encriptación de las comunicaciones gubernamentales	100
7.4 Diseño de nuevas políticas	101
7.4.1 Propuestas de implementación de Políticas Públicas en Ciberseguridad	101
7.5 Creación de Capacidades y Propuestas Formativas	101
7.5.1 Universidad de Buenos Aires.....	101
7.5.2 Universidad de la Defensa Nacional (UNDEF)	102
7.5.3 Instituto Universitario de la Policía Federal Argentina.....	102
7.6 Conclusiones Finales.....	102
Glosario:	104
Bibliografía consultada y referenciada en el presente trabajo	105
ANEXOS.....	111

Introducción – Capítulo I

No existe una definición universal de ciberseguridad, no obstante luego de analizar la bibliografía existente, optamos por las dos más completas:

“La actividad o el proceso, habilidad o capacidad, referentes a los sistemas de información y comunicación y la información contenida en estos sistemas están protegidos contra el daño, el uso o la modificación no autorizados, o la explotación.”

“Estrategias, políticas y normas relativas a la seguridad de las operaciones en el ciberespacio, y abarca todos los tipos de reducción de amenazas, la reducción de la vulnerabilidad, la disuasión, la participación internacional, la respuesta a incidentes, resiliencia, y las políticas y actividades de recuperación, incluidas las operaciones de redes informáticas, integridad de la información, aplicación de la ley, la diplomacia, militares y misiones de inteligencia con respecto a su relación con la seguridad y la estabilidad de la infraestructura mundial de la información y las comunicaciones.¹”

Los objetivos generales de la ciberseguridad son: Disponibilidad, Integridad – la cual puede incluir autenticidad y no repudio – y Confidencialidad.

La ciberseguridad abarca la protección de la información, de los activos de las organizaciones y de los ciudadanos en el ciberespacio a fin de prevenir, detectar, y responder a potenciales ataques cibernéticos o a exposición de información sensible mediante la utilización de herramientas, políticas, normativa, directrices, métodos de gestión de riesgos, acciones, formación y prácticas idóneas que brinden el adecuado marco de acción para esta protección

¹ Adaptado de: CNSSI 4009, NIST SP 800-53 Rev. 4, NIPP, DHS National Preparedness Goal; White House Cyberspace Policy Review, Mayo 2009).

El presente Trabajo Final se desarrolla de la siguiente forma: marco teórico y normativo, principales herramientas y ciberdelitos actuales, principales amenazas, respuestas o esfuerzos institucionales actuales y propuestas de mejoras tecnológicas, operativas, administrativas y legislativas.

1.1 Definiciones necesarias para contextualizar el análisis pretendido

1.1.1 Ciberdelitos

Es un crimen facilitado por un sistema informático o directamente en contra un sistema informático. Además, el crimen cibernético también incluye delitos tradicionales realizados a través de Internet. Por ejemplo: fraude en Internet, el robo de cuentas de tarjetas de crédito, entre otros, son considerados como delitos cibernéticos cuando las actividades ilegales se comenten mediante el uso de la tecnología e internet

1.1.2 Infraestructuras Críticas

Son aquellas instalaciones, redes, servicios y equipos físicos y de tecnología de la información situado en los Estados u organismos privados que posibilitan una mejora del funcionamiento de las distintas áreas estratégicas de una sociedad y cuya interrupción o destrucción pueden tener una repercusión importante en la salud, la seguridad, la información, la integridad física o el bienestar económico y social de los ciudadanos o en el eficaz funcionamiento de las instituciones estatales y las administraciones públicas.

Las infraestructuras críticas están presentes en numerosos sectores como por ejemplo en las actividades bancarias y financieras, transporte y distribución, energía, servicios, salud, abastecimiento de alimentos, comunicaciones, administraciones públicas.

Algunos elementos críticos de estos sectores o áreas no son “infraestructuras” en el sentido estricto, sino que son redes o cadenas de suministro que contribuyen a la entrega de un producto o servicio esenciales. Por ejemplo, el suministro de alimentos y agua a las grandes zonas urbanas

depende de algunas instalaciones clave, pero también de una compleja red de productores, procesadores, fabricantes, distribuidores y minoristas e información que vincula a todos ellos.

En una sociedad en continuos avances como en la que vivimos cada vez son más los recursos e infraestructuras que adquieren la calificación de "fundamentales".

Asimismo, los desarrollos tecnológicos implican que en la actualidad casi la totalidad de éstas sean controladas y gestionadas gracias al desarrollo de sistemas y programas informáticos que se han convertido a su vez en críticos.

Normalmente, un componente o un sistema es calificado como crítico en razón a su posición dentro de toda la infraestructura y, en particular, debido a la interdependencia que éste tenga con otras infraestructuras.

Capítulo 2

2.1 Plataformas frecuentemente utilizadas para la comisión de ciberdelitos

2.1.1 Criptomonedas

Con las nuevas tecnologías, cada vez surgen nuevas formas de resolver situaciones cotidianas incorporando mejoras en el servicio prestado (en sus costos asociados, la facilidad de uso, etc.), por ejemplo, el uso de email en lugar de correo tradicional. Uno de los casos de más relevancia en la actualidad son los métodos de pago electrónico y, concretamente, las criptomonedas.

Una criptomoneda es una moneda virtual que actúa como dinero en efectivo en Internet. Esta moneda se transmite de persona a persona, a través de sistemas P2P², sin más intermediarios que los servidores (o mineros) que apuntan la transacción en un libro contable distribuido, denominado cadena de bloques pública o blockchain

Criptomonedas como Bitcoin, Ethereum y similares son una variante de moneda digital, basadas en la criptografía, que no tiene representación física, sino que se crea y almacena de forma electrónica. Estas monedas digitales se engloban a su vez en lo que se conoce como monedas virtuales, que se caracterizan por ser un tipo de dinero que se emite de forma digital y que, normalmente, está controlado por sus desarrolladores y es utilizado por los miembros de una comunidad virtual específica.

² P2P significa Peer To Peer. Una red peer-to-peer, red de pares, red entre iguales o red entre pares (P2P, por sus siglas en inglés) es una red de computadoras en la que todos o algunos aspectos funcionan sin clientes ni servidores fijos, sino una serie de nodos que se comportan como iguales entre sí. Es decir, actúan simultáneamente como clientes y servidores respecto a los demás nodos de la red. Las redes P2P permiten el intercambio directo de información, en cualquier formato, entre las computadoras interconectadas.

Los usuarios que forman parte de estos sistemas monetarios, que no están gestionados por empresas o estados, no tienen la necesidad de identificarse, lo que les permite disfrutar de un mayor grado de privacidad o, incluso, anonimato en sus transacciones.

También hay que destacar que las criptomonedas, al apoyarse en algoritmos matemáticos para su generación e intercambio, no están vinculadas a referentes usados por las monedas tradicionales, como podría ser el patrón oro.

Precisamente, una de las particularidades de este tipo de monedas es que cualquiera con una capacidad de cálculo aceptable, como la que proporcionan las tarjetas gráficas y microprocesadores actuales de gama media-alta, puede empezar a generarlas en un proceso que se conoce como minería.

La forma de gestionar las transacciones también es particular y es algo que ha despertado más interés incluso que las propias criptomonedas, principalmente por las múltiples aplicaciones en las que se puede utilizar. Este registro de contabilidad público conocido como blockchain o cadena de bloques anota todas y cada una de las operaciones realizadas pero manteniendo siempre el anonimato de sus usuarios.

Aunque Bitcoin fuera la primera moneda criptográfica en aparecer (2009) y sentara las bases para todas las que vinieron después, actualmente existen muchas otras disponibles.

Una de las monedas que más ha captado la atención de los usuarios recientemente es Ethereum, que en los últimos meses ha visto cómo su valor aumentaba considerablemente para, en fechas más recientes, volver a bajar de valor y estabilizarse.

2.1.2 Bitcoin

El Bitcoin se creó con el objetivo de ser una moneda descentralizada y que no sea supeditada por un regulador. Esto genera riesgos, ya que cuando se adquiere se realiza a través de una casa de cambio virtual y se establece un anonimato para la persona, la cual se registra con un seudónimo o correo electrónico.

Esta libertad de la cual hablan sus creadores del anonimato, también puede aprovecharse para realizar actividades ilícitas. No es que el Bitcoin sea la moneda de la legitimización de capitales o moneda del crimen, pero tiene cualidades que la hace susceptible para ser mal utilizada.

En pocas palabras, Bitcoin es un sistema de dinero electrónico. Las monedas electrónicas tienen generalmente dos implicaciones fundamentales, y es que combinan la comodidad de poder hacer pagos por Internet con el anonimato de los pagos en efectivo. Pero Bitcoin no es el primer sistema de dinero electrónico que existe. Esta idea es original de 1985, y fue propuesta por David Chaum en su artículo "Security without identification: transaction systems to make Big Brother obsolete".

Desde entonces, se han propuesto multitud de sistemas incorporando mejoras en diferentes aspectos, o sacrificando algunas características en pro de otras. La principal razón es que Bitcoin no es controlado por ninguna autoridad, sino que lo controlan sus usuarios. En este aspecto, Bitcoin ha sido pionero. Por ello y, por otras razones, ha ganado mucha popularidad.

A continuación haremos un breve repaso de los principales aspectos del sistema, con la intención de entender qué características ofrece con respecto a sus antecesores y muchos de sus competidores.

En el sistema Bitcoin, podemos encontrar dos tipos de participantes:

- Usuarios: compran y venden utilizando bitcoins, generando y publicando las transacciones correspondientes.

- Mineros: reciben transacciones de otros usuarios, las verifican, y trabajan para incluirlas en la cadena de bloques de transacciones aceptadas.

Estableciendo una analogía con cuentas bancarias, la clave pública (la dirección) sería el número de cuenta, y la clave privada sería la contraseña de la cuenta. Para hacer una transacción desde una dirección A hacia una dirección B, el propietario de A firmará con su clave privada tantas bitcoins como quiera transferir a B junto con la clave pública (dirección) de B.

Gracias a la arquitectura P2P, cuando se crea una transacción, esta difunde al resto de nodos de la red. En este punto, los mineros procederán a validar las nuevas transacciones.

Para validar transacciones nuevas, los mineros las combinan con transacciones ya validadas, añadiendo además un número aleatorio, aplicando al resultado una función hash criptográfica. No obstante, no será válido cualquier hash resultante, sino que deberá cumplir un requisito especial (normalmente comenzar con un número determinado de ceros).

Las funciones hash son funciones no invertibles, por lo que la única forma de conseguir un resultado válido es probar números aleatorios por ensayo y error hasta encontrar uno que produzca un hash válido. Este conjunto de datos se conoce como bloque de transacciones, y por su elevado costo de cómputo, se conocen como pruebas de trabajo (tras la idea original del Hashcash³).

El minero que genere un bloque válido, lo publica, y ese bloque queda añadido a la cadena de bloques existentes. Los usuarios de Bitcoin se

³ Hashcash es un método que agrega un string al encabezado de un correo electrónico que prueba que el emisor dedicó un poco de tiempo para calcular dicho string. La idea es que como el emisor le dedicó tiempo a calcular el string y enviar el correo, es improbable que éste sea spam. Por otro lado el receptor puede, con un costo computacional casi nulo, verificar que el string es válido.

descargan la cadena de bloques, y verifican que todos los bloques sean válidos.

La cadena válida de mayor longitud es la considerada como “legítima” bajo la premisa de que la potencia de cálculo controlada por cualquier atacante será menor que la del resto de usuarios, lo cual, gracias a las pruebas de trabajo, es muy difícil.

Brevemente, la seguridad de Bitcoin se basa fundamentalmente en que un atacante no podrá superar la potencia de cómputo de todos los usuarios honestos del sistema (y, obviamente, que no podrá romper las primitivas criptográficas subyacentes).

Primero, las funciones hash criptográficas no son invertibles, por lo que es necesario aplicar fuerza bruta hasta conseguir un hash válido. Por lo tanto, un atacante que quiera incluir una transacción ilegítima tendrá que computar el nuevo bloque más rápido que el resto de la red. Si el atacante tiene menos potencia de cómputo que el resto de mineros, ellos generarán un bloque nuevo (legítimo), y los cálculos realizados por el atacante serán automáticamente inservibles.

Este mecanismo de autorregulación es el principal aspecto técnico novedoso de Bitcoin: en los sistemas precedentes, para evitar double spending (pagar varias cosas con la misma moneda), se recurría a una entidad central, controlada por alguna autoridad, lo cual hacía al sistema en cuestión directamente dependiente de la fiabilidad de dicha autoridad. Pero no sirve sólo para evitar double spending, también es una forma de consensuar el protocolo “oficial” (por ejemplo, si un minero intentase aumentar su recompensa por encontrar un nuevo bloque, el resto de usuarios rechazarían dicho bloque por incluir una recompensa inválida).

Segundo, gracias a las propiedades de la criptografía asimétrica, sólo quien conozca la clave privada correspondiente a una clave pública (dirección) determinada, podrá gastar las bitcoins asociadas. Así, el sistema es ajeno a

los problemas de transacciones bancarias típicas, en las que el tráfico tiene que estar protegido mediante cifrado para evitar robos. Esto no es un problema en Bitcoin, donde por definición, las transacciones son públicas.

En resumen, desde el punto de vista técnico, el sistema Bitcoin ha puesto en marcha unos mecanismos de autorregulación distribuida en un campo en el que parecía complicado hacerlo. Desde el punto de vista económico y social, crea un escenario totalmente nuevo, donde es difícil predecir qué efectos tendrá o cómo será su adopción.

2.1.3 Blockchain

Blockchain nació con las criptomonedas, pero excede el mundo financiero y ya es utilizada por gobiernos para realizar ayuda humanitaria. Como mencionamos anteriormente en el presente proyecto, la más popular de ellas, el Bitcoin, pasó de cotizar un dólar o menos cuando la creó Satoshi Nakamoto, en 2008, y este año llegó a superar los US\$ 4600 por unidad, subiendo más de un 600% en menos de un año. Independientemente de la subida, las caídas también son abruptas. Siendo muy volátil.

La volatilidad extrema llevó a analistas financieros a hablar del "fin de una burbuja", a gobiernos (como el de Inglaterra) a prevenir a ahorristas sobre los riesgos de invertir en estas opciones y a diversos medios a advertir que las monedas virtuales y su tecnología de base (la red descentralizada blockchain) están sobrevaluadas.

Blockchain es una red global descentralizada, similar a un libro contable abierto, en donde se asientan todas las transacciones de bitcoins del mundo, pero los activos que se pueden certificar allí exceden a esta moneda virtual: pueden ser bienes, servicios, contratos legales y hasta personas que se asocian a un "bloque" de código que luego se encadena con otros (de ahí su nombre).

Es una de las tecnologías exponenciales que genera más entusiasmo y sus partidarios no se intimidan con las fluctuaciones de las criptomonedas,

a las que consideran aprendizajes propios de una etapa temprana de desarrollo, pero la tecnología subyacente abarca un abanico de aplicaciones que excede al campo financiero.

De hecho, blockchain tiene un motor extra al margen del mercado: se está convirtiendo en una "tecnología política"⁴ que los gobiernos comienzan a ver con un creciente interés para un sinfín de soluciones, desde la titularización de tierras y propiedades hasta la ayuda humanitaria, pasando por la protección de documentos públicos.

Entre sus promotores más activos hoy están los gobiernos de las ex repúblicas soviéticas (Estonia, Georgia y Rusia) y algunos países petroleros.

Asimismo, organismos internacionales, como el BID, el Banco Mundial o las Naciones Unidas, la cual, a principios de junio de 2017, envió el 100% de la ayuda humanitaria a refugiados sirios en los campos de Jordania a través de la criptomoneda Ethereum.

La moneda virtual se saltea los intermediarios (elimina costos y posible corrupción) y llega mediante cupones (de comida, medicina) directamente a los más necesitados, que validan su identidad con una tecnología de escaneo del iris de los ojos. El terreno de la ayuda humanitaria es uno de los campos donde blockchain dejó de ser una promesa o una burbuja para transformarse en una herramienta de suma practicidad y en pleno crecimiento.

A los países y organismos internacionales se le suma un ecosistema de startups y emprendedores sociales (como AID tech o Disberse) que promueven e incentivan las donaciones "directas", sin costos de intermediación.

Ban Ki-moon, ex secretario general de la ONU, estimó en su momento que un 30% de la ayuda humanitaria se pierde en el camino hasta los

⁴ Sebastian Campanario – La Nación (Julio 2017)

destinatarios finales por costos de intermediación financiera, administrativos y de posible corrupción.

Los países que están promoviendo su uso lo hacen en buena medida para mejorar su reputación y transparencia, y por ende volverse más atractivos para la inversión extranjera y la recepción de inmigrantes.

Blockchain puede ser una herramienta muy potente para contribuir a agilizar la cooperación en situaciones de crisis humanitaria, como así también a reducir la informalidad en el mundo, a partir de la simplificación de los mecanismos de registro de bienes y personas.

La efervescencia por este fenómeno es tan intensa que no sólo se pronostica la decadencia de un sinfín de profesiones e instituciones que en la economía se dedican a "proveer confianza" (abogados, contadores, escribanos, auditores, managers de fondos de inversión, bancos, instituciones gubernamentales) sino el final, también, de empresas de la nueva economía, como Uber o Airbnb, porque esta nueva tecnología permite (en teoría) eliminar cualquier tipo de intermediario que se quede con una comisión en el medio de una operación.

La confianza surge de un esquema descentralizado, donde todos los "nodos" (usuarios o computadoras) comprueban que cada operación sea válida.

Los usos de esta "tecnología política" parecen infinitos y cada día aparece una nueva "startup"⁵ con una solución para algún problema social.

⁵ Empresas que buscan arrancar, emprender o montar un nuevo negocio, y aluden a ideas de negocios que están empezando o están en construcción, y generalmente se trata de empresas emergentes apoyadas en la tecnología. Son ideas que innovan el mercado y buscan facilitar los procesos complicados, enfocadas a diferentes temas y usos. Generalmente son empresas asociadas a la innovación, al desarrollo de tecnologías, al diseño web o al desarrollo web, y son empresas de capital-riesgo.

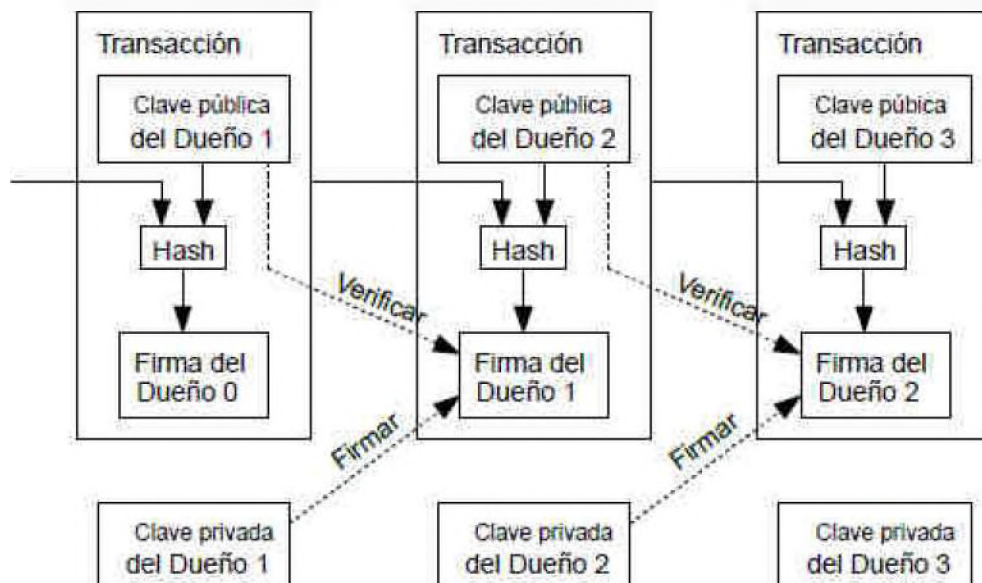
En el extremo utópico, hay quienes aseguran que la red detrás de las monedas virtuales podría usarse como un “per saltum” con el cual países de ingresos medios y bajos saltarán el proceso de construcción institucional que a los países más ricos les llevó décadas o siglos.

Aún persisten problemas tecnológicos a solucionar, pero se trata de una tecnología que avanza a pasos agigantados.

Los delincuentes también están al tanto y no solo usan estas monedas para tratar de camuflar sus operaciones delictivas, sino que también tienen a los mineros y otros usuarios en su punto de mira.

Es importante pues que si tenemos interés de adentrarnos en este mundo, lo hagamos de forma segura e informándonos de todos los riesgos y precauciones a adoptar.

Esquema Criptográfico para controlar la creación y la transferencia de dinero, en lugar de depender de las autoridades centrales



Fuente: <https://puntodevistaeconomico.wordpress.com/2014/04/28/bitcoin-un-sistema-de-efectivo-electronico-usuario-a-usuario-por-satoshi-nakamoto-en-espanol/>

2.2 Herramientas informáticas utilizadas por el cibercrimen

Antes de los tipos de ataques detectados en nuestro país, debemos hacer una introducción a los siguientes temas –en forma breve y concreta– directamente involucrados con el cibercrimen:

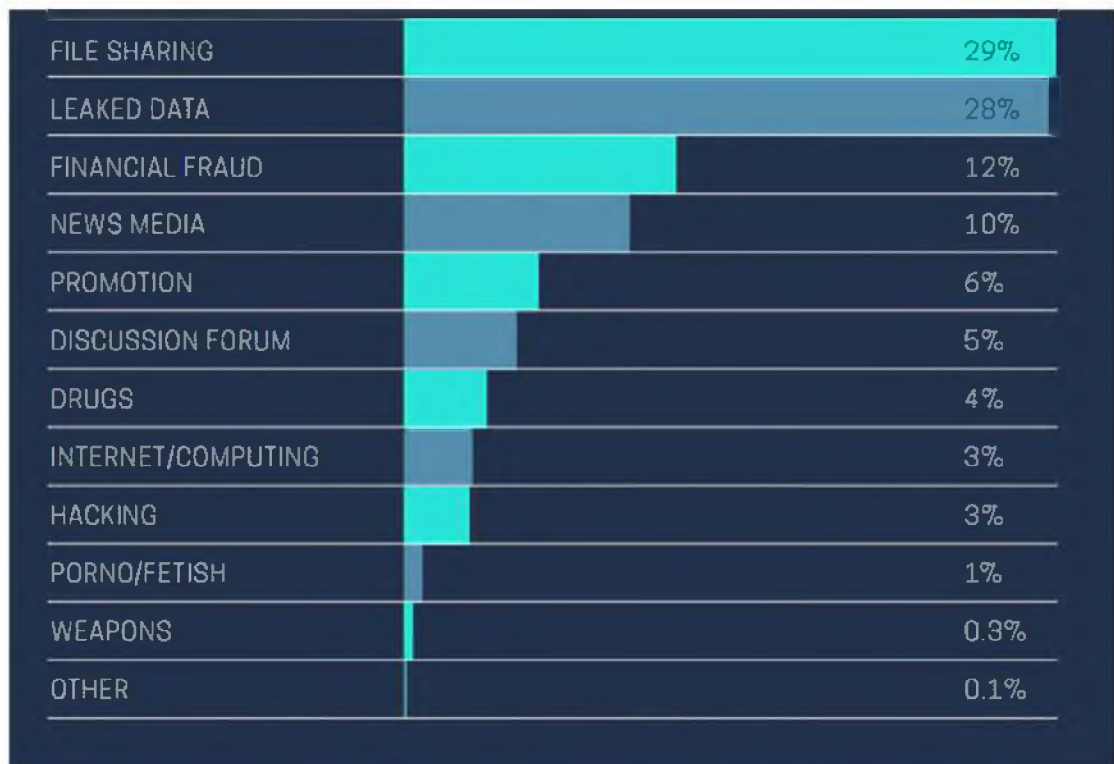
- **DEEP WEB** (web profunda)
- **Navegadores “anónimos”**
- **Vulnerabilidad ZERO DAY** (día cero)

2.2.1 Deep Web o web profunda

También denominada Dark Web (Internet profunda u oscura) es aquella que no está indexada en los buscadores tales como Google, Bing o Yahoo. Esta definición es muy amplia y, como tal, podría incluir aquellas publicaciones comerciales que, por motivos estratégicos, impiden o limitan que los buscadores comerciales indexen los contenidos que generan.

No obstante, se identifica la Deep Web con los usos más oscuros y criminales de Internet, un lugar en el cual es fácil comprar drogas, armas, o traficar con órganos. A un nivel más técnico, diremos que la Web Profunda es aquella en la que las páginas cambian constantemente de ubicación, de tal forma que incluso su dirección está encriptada, y una URL de esta parte de Internet no tiene el formato habitual de www.google.com.ar, sino que tiene más bien un aspecto como ***plc67asdt348bhjgdfyetyuhi5674.onion***.

Según el informe llamado "*Shinning a light on the dark web*" se pudo observar que las categorías más importantes relevadas de la dark web son: pornografía, medicamentos, armas, blogs, sitios de fraude financiero, drogas, servicio de documentación falsa, sitios de uso fraudulento de tarjetas de crédito.



Asimismo el informe indica que de un total del 29,532 sitios ".onion" detectados durante el periodo que duró la confección del informe, el 46% estaba accesible y el 54% inaccesible y los idiomas que prevalece es el Inglés

con un 76%, seguido por el Alemán y el Chino con un 4% y 3,7% respectivamente, detectando un total de 32 idiomas.



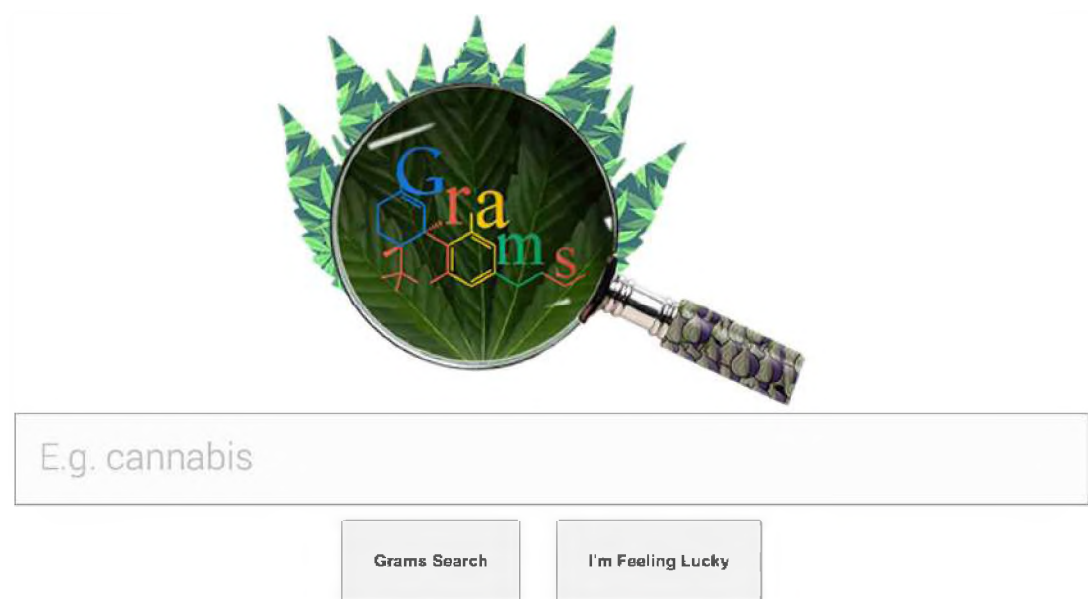
Según los sitios analizados, basándose en las leyes de USA y UK se puede observar que el 48% solamente viola alguna de las leyes, si se basan en la detección automática por medio de algoritmos y el mismo aumenta a un 68% utilizando un muestreo manual.

Se puede observar en la dark web mercados que permiten la comercialización de productos ilegales.

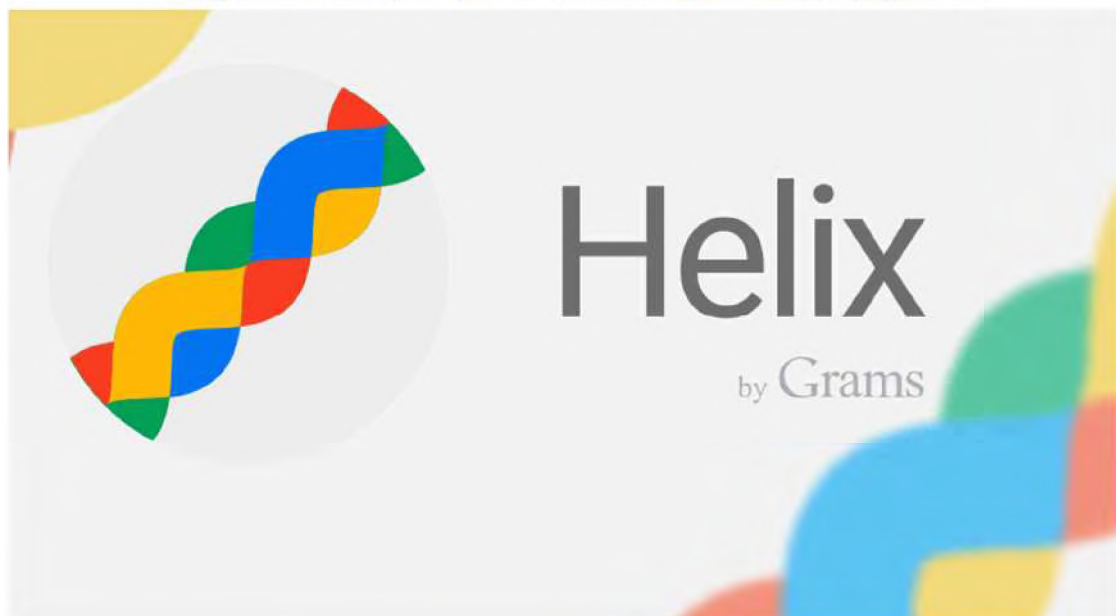
Es importante destacar que las diferentes fuerzas de seguridad de diversos países están intentando desactivar estos mercados.

Actualmente se está intentando identificar, no solo a los vendedores en dichos mercados, sino también a los compradores.

A modo de ejemplo se puede nombrar AlphaBay y Hansa donde los esfuerzos de las fuerzas de seguridad están dando frutos.



Búsqueda de navegador para comercialización de drogas peligrosas



Lavado de dinero mediante navegador específico

Como fácilmente se aprecia, se trata de un mercado negro virtual, sumado al pago mediante criptomonedas lo hace el medio anónimo para todo tipo de comisión de delitos, que ya exceden a los ciberdelitos, especialmente al tráfico de estupefacientes y drogas peligrosas. La estrategia local que consideramos más acertada se propone en las conclusiones del presente Trabajo Final de Especialización.

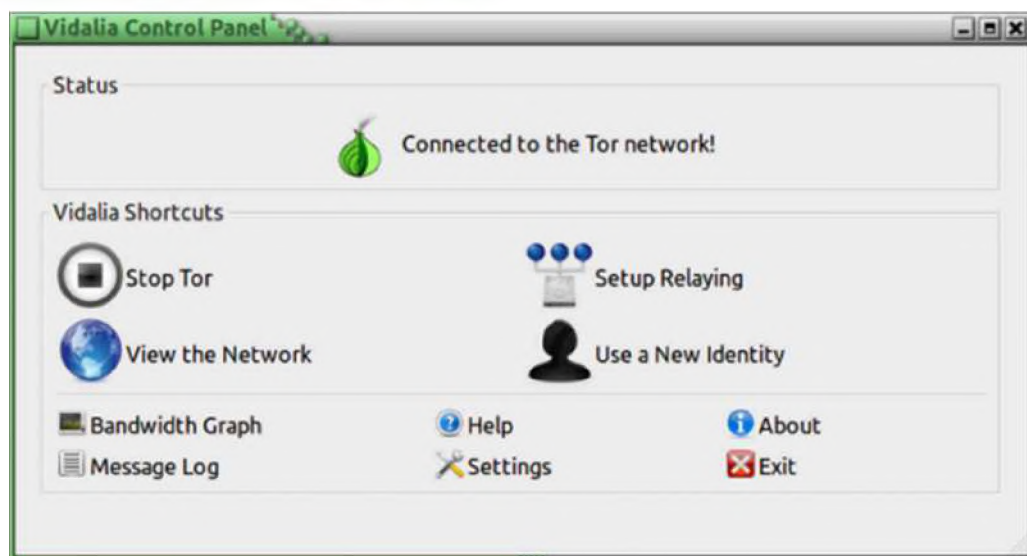
2.2.2 Navegadores Anónimos

Ante la necesidad de permanecer anónimos (que no se pueda, o al menos, que sea bastante dificultoso, identificar la dirección IP) los ciberdelincuentes optan por la utilización de navegadores que permiten tal circunstancia mediante medidas técnicas (saltos de servidores a nivel global, etc.) teniendo como desventaja que la velocidad de navegación, por ese tipo de procedimiento, se reduce sensiblemente. Por otro lado, para navegar en la Deep Web hacen falta navegadores específicos. Ejemplo de esto es TOR, que se debe usar un navegador modificado de Firefox para poder ser utilizado.

2.2.3 Navegador TOR

Tor es una aplicación que toma los datos que entran y salen a través de la conexión a Internet y los hace pasar a través de un circuito de servidores repartidos por todo el mundo. Eso consigue que el tráfico se vuelva totalmente anónimo.

La **red de Tor**, en la que cualquiera puede participar como nodo voluntario, consta de más de 4.000 máquinas repartidas por decenas de países de todo el mundo. Esta cantidad de nodos garantiza anonimato y conectividad para los usuarios de Tor.



El panel de control Vidalia para Tor, disponible para Windows, Mac y Linux

Para facilitar su uso, Tor se distribuye con Vidalia, una utilidad que permite iniciar, parar y controlar el funcionamiento de Tor. Existe una App⁶ similar para teléfonos Android llamada Orbot, e incluso una distribución Linux que usa exclusivamente Tor.

Tor es un acrónimo para *The Onion Router*, el “enrutador cebolla”. La referencia se debe a la estructura de la red usada por Tor, que consiste en varias capas de cifrado que protegen los datos.

El proyecto Onion Router fue financiado originalmente por el gobierno de los Estados Unidos, y se desarrolló en los laboratorios de investigación de la marina de los EEUU. A día de hoy, Tor recibe financiación de diversas fuentes, como empresas y ONGs.

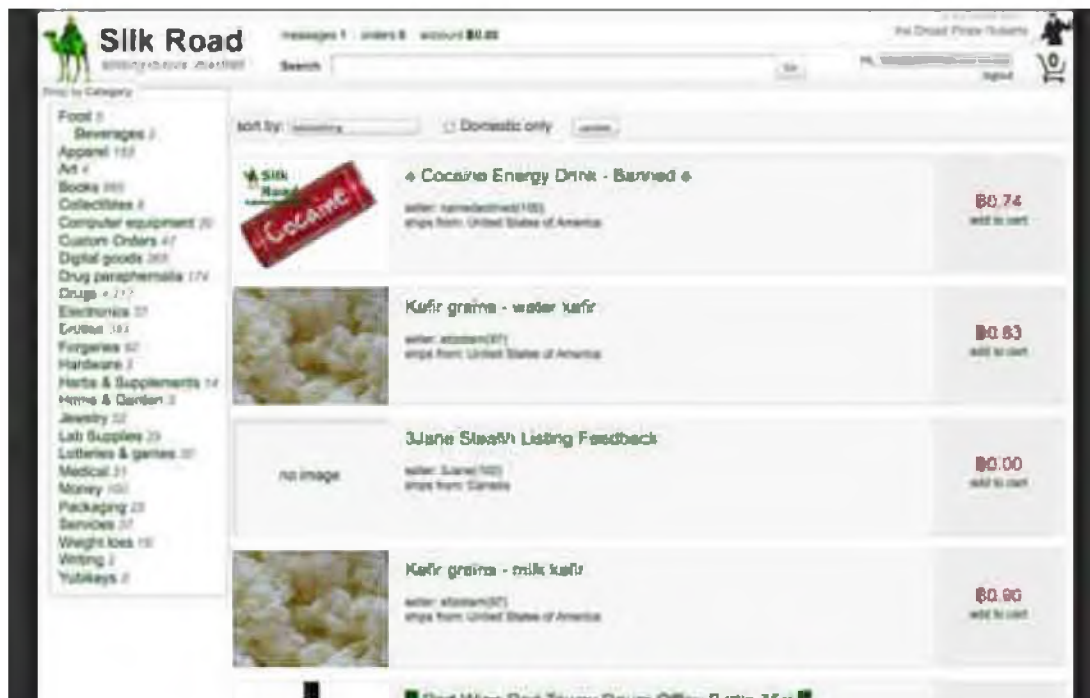
Tor se usa cuando se desea impedir que una actividad en Internet se pueda relacionar con la persona que la lleva a cabo. **Tor crea anonimato en la red.** Este anonimato puede ser aprovechado para las finalidades más diversas.



Grupos descentralizados como Anonymous usan regularmente Tor

Un uso ético de Tor es el que defienden instituciones como la EFF, que promociona Tor como una herramienta que protege a quien lucha por los derechos civiles en regímenes totalitarios, ya sean periodistas, informadores o disidentes políticos.

⁶ El término App es una abreviatura de la palabra en inglés application. Es decir, una App es un programa. Se refieren sobre todo a aplicaciones destinadas a tablets (como el iPad o equipos Android) o a teléfonos del tipo smartphone (como el iPhone o el Samsung Galaxy)



Silk Road, una página de comercio electrónico donde los usuarios pagan con bitcoins. (Silk Road 2.0 fue desarticulado por el FBI y Europol)

Pero la sombra que Tor ofrece también es usada para **finés más turbios**, como la compra-venta de moneda virtual (Bitcoin), la distribución de contenidos ilegales, el comercio ilegal, el espionaje y la comunicación entre grupos criminales.

2.2.3 Vulnerabilidad o Exploit ZERO DAY (día cero)

Lamentablemente, además de las medidas que podamos tomar y la concientización sobre las personas para evitar maniobras como el phishing, existen vulnerabilidades no descubiertas por las firmas proveedoras de hardware y software (generalmente este último), mientras que miles de individuos, usualmente hackers, se dedican en el mundo a descubrirlas.

Un ataque de Exploit de día cero (ZETA, por sus siglas en inglés) tiene lugar cuando se descubre una debilidad en el software.

En ese momento, el ataque se produce antes de que el creador del software o producto encuentre una solución al problema.

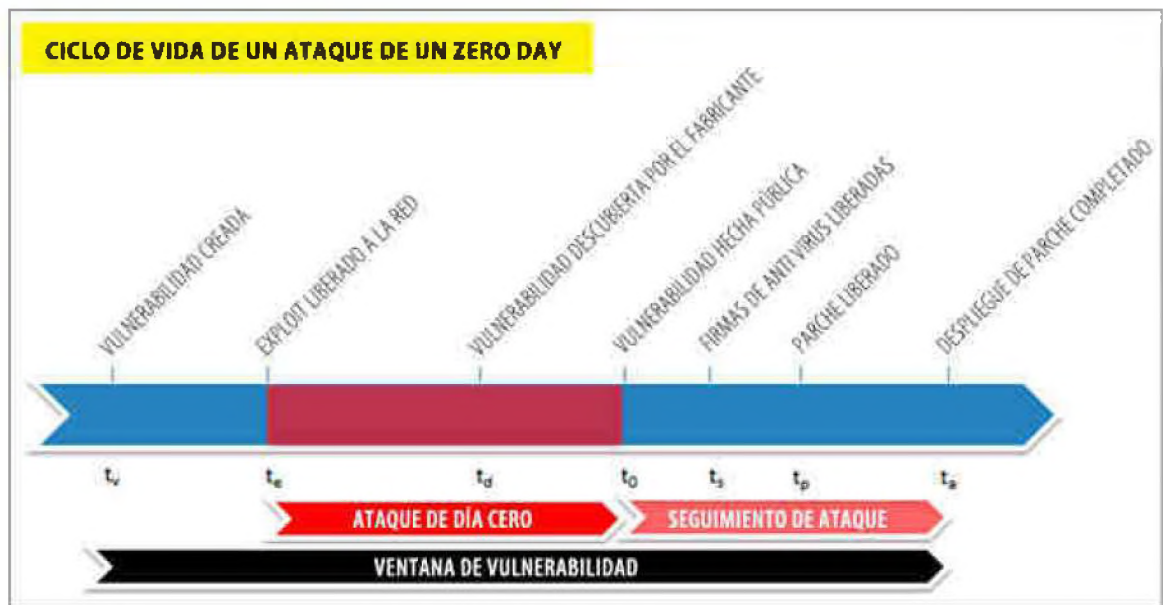
En un principio, cuando un usuario descubre que hay un riesgo para la seguridad en un programa, puede comunicarlo a la empresa fabricante del software que, de forma inmediata, desarrollará un parche de seguridad para solucionar el defecto.

Este mismo usuario también podría advertir a otros usuarios del defecto a través de Internet. Por lo general, los creadores del programa dan rápidamente con una solución que mejora la protección del sistema.

Sin embargo, a veces los hackers se enteran de ese defecto antes y lo explotan con rapidez. Cuando sucede esto, la protección frente a un ataque es mínima porque el defecto de software es demasiado reciente.



Fuente: <https://henryraul.wordpress.com/2016/07/19/como-combatir-los-ataque-de-dia-cero/>



Fuente: <http://www.emb.cl/channelnews/articulo.mvc?xid=2521>

2.3 Descripción de los ataques y herramientas maliciosas más utilizadas

Antes de comenzar la clasificación, debemos mencionar lo referenciado -en forma extraoficial- por los jefes de Seguridad Informática de entidades bancarias que fueron entrevistados por el autor del presente, revelando que los intentos de ataques a sus servidores, no solo son a diario, sino en forma casi constante, es decir, verifican a través de sus sistemas de monitoreo, en una periodicidad de prácticamente minuto a minuto, intentos de penetración a la red interna o ataques informáticos similares, y relevando -en la medida de lo posible- el origen de las IP (en gran parte gracias al anonimato que permiten los navegadores TOR y similares) estas varían desde Rusia hasta la propia Ciudad de Buenos Aires.

Esto refiere a que los ataques son transnacionales y gracias a la globalización y las transferencias o compras internacionales el obtener cualquier tipo de dato para realizar una maniobra fraudulenta, "sirve" para todo tipo de delincuente informático proveniente de cualquier parte del mundo.

2.3.1 Phishing

Debido al aumento de correos electrónicos en los que se solicitan datos personales de manera maliciosa y con el objeto de evitar que esta técnica de engaño tenga éxito se ha elaborado esta recomendación.

Phishing es una forma de engaño mediante la cual los atacantes envían un mensaje (anzuelo), por distintos medios, a una o varias personas, intentando convencerlas para que revelen sus datos personales. Es posible que luego, esa información sea utilizada para realizar acciones fraudulentas, como transferencias de fondos de su cuenta bancaria, robo de identidad, compras con sus tarjetas de crédito u otras acciones fraudulentas. A modo de ejemplo, una entidad bancaria nunca pedirá que se ingresen todos los dígitos de su tarjeta de coordenadas, situación que se ha detectado en diversos phishing y que lamentablemente muchas veces los usuarios, por desconocimiento ingresan esos datos.

2.3.2 Botnets

Los usuarios empezaron a conocer este programa malicioso a partir del año 2000 cuando un adolescente de Canadá lanzó una serie de ataques de denegación de servicio contra páginas web muy populares. El joven, cuyo apodo era "Mafiaboy", atacó Yahoo, ETrade, Dell, eBay, Amazon, entre otros, durante varios días, sobrecargando los sitios web hasta que los servidores se colapsaron. Mafia Boy, o su nombre real Michael Cale, no usó un botnet para su ataque, pero los expertos en seguridad avisaron, después de este episodio, que los botnets (grandes redes de computadoras infectadas con una variedad de malware) y los ataques DDoS eran una gran amenaza para la estabilidad e integridad de Internet. Por supuesto, los profesionales no se equivocaron en absoluto.

Además, los botnets también se utilizan para otras operaciones como envío masivo de spam o fraudes de tarjetas de crédito a gran escala.

2.3.3 Denegación de Servicios

Es un ataque a un sistema de computadoras o red que causa que un servicio o recurso sea inaccesible a los usuarios legítimos. Normalmente provoca la pérdida de la conectividad con la red por el consumo del ancho de banda de la red de la víctima o sobrecarga de los recursos computacionales del sistema atacado.

Existen diferentes tipos de ataques DDoS, pero el objetivo siempre es el mismo: colapsar una web. Los atacantes usaban esta táctica para “derribar” las páginas de sus enemigos.

No obstante, empezaron a utilizar este método para atacar portales como Yahoo, Microsoft, tiendas online, bancos o web gubernamentales. Los grupos como Anonymous y LulzSec utilizaron los ataques DDoS contra este tipo de organizaciones.

Por otro lado, los ciberdelincuentes usaban este tipo de ataque contra páginas bancarias para ocultar otros ataques más importantes en entidades bancarias.

Existen diferentes formas de defensa frente a los ataques DDoS, pero casi todas ellas operan a nivel de servidor o ISP.

Para los usuarios, la defensa frente a un botnet empieza actualizando todo el software de su equipo y evitando ingresar (“hacer click”) en enlaces sospechosos.

Los hackers se aprovechan de la ingenuidad de los usuarios a la hora de abrir archivos maliciosos o hacer click en enlaces que esconden un malware.

2.3.4 Ataques de denegación de servicio distribuidos (DDoS)

El ataque de tipo DDoS desde una Botnet, dada la dispersión geográfica de las computadoras que la componen, es casi imposible encontrar

a las máquinas que están atacando y dado el alto número de ellas que lo estarán haciendo al mismo tiempo, no se puede contemplar el filtrado de paquetes como una solución real que funcione. No obstante, puede ayudar a mitigar el problema hacer un escaneo pasivo de los paquetes para reconfigurar y adaptar el firewall.

Una de las alternativas más utilizadas hoy en día es la contratación de ancho de banda dinámico (elástico) que permite ampliarse transitoriamente cuando existe este tipo de ataques, hasta tanto pueda detectarse y mitigarse y de esta manera evitar la denegación de servicio.

Envío de Spam: Lo más frecuente es que una botnet se utilice para enviar spam a direcciones de correo electrónico. Normalmente los creadores de estas Botnets venden sus servicios a los "spammers".

Por lo menos en un caso una investigación (la red Rustock) consiguió averiguar que un solo hacker había conseguido el control de un millón de computadoras, utilizándolas como plataforma para sus ataques, con los que era capaz de enviar 30 millones de spam por día.

Minería de Bitcoins: Con la aparición de criptomonedas, ya en 2011 había reportes de un nuevo uso para las botnets: usar el procesamiento de las computadoras para generar bitcoins. De esta forma los criminales pueden obtener recursos sin gastar en hardware ni en consumo de energía. Se espera que este uso siga aumentando en el futuro. Un ejemplo de estas redes es Zero Access botnet.

Robo de Bitcoins: Una variante adicional es el robo de bitcoins usando botnets. Es el caso de la red Pony, que robaba información de los equipos infectados. Se estima que con esta red se obtuvieron credenciales (usuario/password) de, al menos, 2 millones de equipos.

2.3.5 Ransomware

Es un software malicioso que bloquea el acceso de la víctima del ataque a sus datos hasta que efectúe el pago de un rescate (ransom), es

decir, secuestra su información para extorsionar a las víctimas, solicitando el pago de una suma de dinero para recuperar esos datos.

Las versiones modernas por lo general encriptan fuertemente los datos de los archivos de la persona o entidad afectada y exigen un pago en bitcoins, una moneda virtual, a cambio de la clave que permitirá descryptar dicha información.

La información secuestrada es cifrada utilizando procedimientos criptográficos.

En los últimos dos años, el ransomware ha cobrado una mayor relevancia en el panorama de la seguridad de la información y ha infectado tanto a usuarios como empresas. Las extensiones más perjudicadas son las de archivos de ofimática y multimedia:

- Procesadores de texto
- Hojas de cálculo
- Diapositivas
- Imágenes
- Correos electrónicos

Puede ejecutarse de múltiples maneras, ya sea a través de un enlace malicioso en una página web o en un correo electrónico, un archivo adjunto, un pendrive USB o una red local.

La particularidad del ransomware es que aunque pueda eliminarse el programa que bloqueó el acceso a los datos, estos ya están encriptados y es prácticamente imposible recuperarlos sin la clave de descifrado, que no está en la computadora de la víctima. Por este motivo lo que se puede lograr es eliminar el programa para evitar que se siga propagando, pero no se recuperan los datos.

Actualmente algunas versiones más antiguas de ransomware pueden ser descryptadas.

Explotación del sistema

Propagación por correo, pendrive u otros.

Instalación

En la mayoría de los casos, tras abrir un archivo adjunto infectado en un correo electrónico.

Identificación de archivos a cifrar

Cifrado de Datos

Las últimas variantes de Filecoder usan RSA de 2048 bits.

Notificación al usuario

Puede usar trucos como hacerse pasar por un organismo estatal para asustar a la víctima.

Espera por el pago

Los métodos aceptados van desde tarjetas prepagas hasta bitcoins o cupones de MoneyPak, Ukash y cashU, para otorgar anonimato.

Entrega de las claves de descifrado

Nada asegura que el atacante devuelva el control del equipo infectado.

La modalidad de Ransomware que cifra los archivos:

- Se comunica con el atacante a través de Tor mientras exige la transferencia de dinero. Cryptolocker, CTB-Locker y TorrentLocker son los más resonantes.

La modalidad de Ransomware que bloquea la pantalla:

- No es posible usar el equipo hasta haber pagado el rescate. W32/Reveton es una de las familias más encontradas en entornos virtuales.

Las mismas amenazas llegan a nuevas plataformas. En Android encontramos a Simplocker, en iOS a WireLurker y, además, nuevas variantes del “Virus de la Policía”.

Algunas estadísticas recolectadas:

2.500 dólares le costó a una compañía argentina recuperar sus datos.

15% de las detecciones de CTB-Locker fueron en países hispanoparlantes.

500.000 es el número estimado de víctimas de Cryptolocker.

1,44 % de las víctimas de TorrentLocker terminó pagando el rescate.

Numerosas compañías en todo el mundo se han visto afectadas por un nuevo ataque de ransomware que afectó a equipos con sistemas Windows y el valor de rescate que se pidió bitcoins para recuperar los datos no superaban los 500 dólares.

Al promediar la realización del presente Trabajo Final de Especialización, se produjo un ataque a nivel global (150 países) mediante Ransomware, de la variedad WannaCry (en inglés WannaCry ransomware attack o Wanna Cry Doble Pulsar Attack), que usan el criptogusano conocido como WannaCry (también denominado WannaCrypt, WanaCrypt0r 2.0, Wanna Decryptor) dirigidos al sistema operativo Windows de Microsoft.

El 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 son 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 también fueron afectadas; junto con muchos otros blancos a nivel mundial.

2.3.6 BEC

Son las siglas de "Business Email Compromise", es decir, el compromiso de los correos electrónicos corporativos es una estafa sofisticada dirigida a las empresas que trabajan con proveedores extranjeros y las empresas que realizan periódicamente los pagos de transferencia electrónica.

Anteriormente conocidos como estafas de Man-in-the-Email, estos esquemas comprometen las cuentas oficiales de correo electrónico para llevar a cabo transferencias de fondos no autorizadas.

Según el FBI, las víctimas perdieron cerca de 750 millones de dólares y afectaron a más de 7.000 personas entre octubre de 2013 y agosto de 2015. Globalmente, los ciberdelincuentes robaron más de 50 millones de dólares de víctimas en países fuera de Norteamérica.

Las estafas BEC a menudo empiezan con un atacante comprometiendo la cuenta de correo electrónico de un ejecutivo de negocios o cualquier correo electrónico públicamente listado.

Normalmente, esto se hace utilizando métodos de phishing, donde los atacantes crean un dominio similar al de la empresa a la que apuntan o un correo electrónico falsificado que engaña al objetivo para proporcionar detalles de la cuenta.

Al supervisar la cuenta de correo electrónico comprometida, el estafador tratará de determinar quién inicia los pedidos y quién los solicita. Los autores suelen realizar una buena cantidad de investigación, buscando una empresa que ha tenido un cambio en sus autoridades, las empresas donde los ejecutivos están viajando, o por la conducción de una conferencia telefónica con inversionistas. Ellos usan estos como oportunidades para ejecutar el esquema.

Las estafas BEC tienen tres versiones:

Versión 1: El esquema de factura Bogus

Esta versión, que también se ha denominado "El esquema de factura Bogus", "La estafa del proveedor" y "Esquema de modificación de la factura", normalmente implica una empresa que tiene una relación establecida con un proveedor. El estafador pide transferir fondos para el pago de facturas a una cuenta fraudulenta alternativa a través de correo electrónico, teléfono o facsímil falsificados.

Versión 2: Fraude del CEO

En esta versión, los defraudadores se identifican como ejecutivos de alto nivel (CFO, CEO, CTO, etc.), abogados u otros tipos de representantes legales y pretenden manejar asuntos confidenciales o sensibles al tiempo e iniciar una transferencia bancaria a una cuenta que controlan. En algunos casos, la solicitud fraudulenta de transferencia bancaria se envía directamente a la institución financiera con instrucciones para enviar urgentemente fondos a un banco. Esta estafa también se conoce como "Fraude CEO", "Business Scam Ejecutivo", "Masquerading", y "Financial Industry Wire Fraudes".

Versión 3: Compromiso de la cuenta

De forma similar a las otras dos versiones, una cuenta de correo electrónico de un empleado es hackeada y luego se utiliza para realizar solicitudes de pago de facturas a cuentas bancarias controladas por el fraude. Los mensajes se envían a varios proveedores identificados de la lista de contactos del empleado. Es posible que la empresa no se dé cuenta del esquema hasta que sus proveedores lo sigan para verificar el estado del pago de la factura.

Versión 4: Representación del Fiscal

En esta versión, el ciberdelincuente se pone en contacto con los empleados y / o el CEO de la empresa y se identifican como abogados, alegando tratar asuntos confidenciales y sensibles al tiempo. Este contacto, normalmente hecho por teléfono o por correo electrónico, presiona a la parte contactada para que actúe rápida o secretamente en el manejo de la transferencia de fondos. Este tipo de régimen BEC puede ser programado para ocurrir al final del día hábil o semana laboral, cuando los empleados se están preparando para descansar y por lo tanto son vulnerables al pánico.

Versión 5: Robo de datos

Este esquema involucra el correo electrónico de los empleados específicos de rol (normalmente los recursos humanos) en la empresa comprometida y luego se utiliza para enviar solicitudes - no para las

transferencias de fondos, sino para la información de identificación personal de otros empleados y ejecutivos. Esto por lo tanto puede servir como un punto de salto para los ataques BEC más perjudiciales contra la propia empresa.

La estafa se basa principalmente en ingeniería social y, por lo general, no necesita una penetración sofisticada del sistema. A diferencia de las estafas de phishing, los correos electrónicos utilizados en las estafas BEC no se envían por correo electrónico masivo para evitar ser marcados como spam. Además, en las estafas BEC, las víctimas son engañadas a hacer las transferencias para ellos, por lo general instruyendo a las víctimas a actuar con rapidez o confianza en la transferencia de fondos.

En el 2016, se descubrió que una creciente línea de empresas y negocios han caído en esquemas similares. Empresas como Seagate, Snapchat y Sprouts Farmer's Market se encontraban entre las empresas que fueron víctimas de estafas de correo electrónico que utilizan el mismo modus. Pivotal Software, una compañía de software y servicios con sede en San Francisco, fue violada a través de un esquema de phishing que filtró un número no revelado de información de impuestos de los empleados.

El incumplimiento fue iniciado por un correo electrónico que parecía ser del CEO de la compañía Rob Mee, solicitando información sobre el personal de la compañía. Esto dio lugar a la entrega de la información del legajo del empleado que incluyó nombres, direcciones, detalles del rédito 2015, números del seguro social, y números individuales de la identificación del contribuyente a un destinatario no autorizado.

No mucho después de este incidente, se utilizaron esquemas similares para lograr información personal del sector educativo. Después de la exposición de la información del legajo de 3.000 empleados del Tidewater Community College de Virginia, un correo electrónico similar que se presentó como una solicitud del presidente de la Universidad Estatal de Kentucky, Raymond Burse, fue enviado a uno de los miembros del personal de la

escuela. Lista de empleados y estudiantes junto con la información de sus respectivos legajos fue vulnerada.

Las estafas que involucran el robo de información personal a través de correos electrónicos de phishing han demostrado ser un valioso material, ya que los datos robados podrían ser vendidos en mercados secundarios y también ser usados para organizar futuros ataques. Como se ve en las estafas de fraudes fiscales recientes y anteriores, las estafas de correo electrónico se han convertido en uno de los métodos más rápidos para engañar a los usuarios que no conocen.

2.4 Impactos de los Ciberdelitos más importantes realizados hasta el momento

Este ranking se establece teniendo en cuenta criterios de impacto económico, dimensión de las fugas o robos de información en cuanto a usuarios, empresas o instituciones afectadas, daño a la reputación o efectos causados en el ciberespacio a nivel mundial.

En total, se han registrado “sucesos” de Ciberseguridad, principalmente ataques con robo de información, perpetración de ciberdelitos, infecciones por malware, incidentes que afectaron a Operadores Críticos no nacionales, ciberespionaje e incidentes relacionados con el cifrado de información.

El ranking de los principales “sucesos” de ciberseguridad, que vuelve a poner de manifiesto que ningún sector es inmune a los ataques y que es importante seguir los procedimientos de seguridad, lo encabeza el robo de 81 millones de dólares al Banco Central de Bangladés perpetrado por piratas informáticos que lograron acceder a los sistemas informáticos del Banco y transferir esa cantidad de dinero a varios casinos de Filipinas. Un error ortográfico en el nombre de uno de los destinatarios levantó las alarmas evitando así el mayor robo de la historia, puesto que en realidad se habían realizado 35 peticiones para obtener casi 1.000 millones de dólares.

El segundo puesto lo ocupa el robo de unos 64 millones de dólares en bitcoins a la plataforma de intercambio Bitfinex de Hong Kong, el mayor operador mundial de intercambio de Bitcoin basado en dólares, lo que provocó una caída de la cotización del Bitcoin superior al 23 por ciento.

La tercera posición del ranking es para la publicación de datos de 154 millones de votantes de Estados Unidos. Los datos incluían información personal como dirección, correo electrónico, número de teléfono o enlaces a redes sociales.

En cuarto lugar, encontramos la publicación de datos personales de 93 millones de ciudadanos de México, debido a la defectuosa configuración de la base de datos MongoDB utilizada por el Instituto Nacional Electoral de México. Este hecho, en el que quedaron expuestos detalles como la dirección postal y la fecha de nacimiento, levantó un gran revuelo en un país donde los secuestros son un crimen habitual.

En la quinta posición aparece el robo de 1.000 millones de cuentas a Yahoo!. Además de fechas de nacimiento, direcciones de correo electrónico, números de teléfono, contraseñas en MD5, la información robada también contenía preguntas y respuestas de seguridad sin cifrar.

Otro suceso relacionado con la misma compañía ocupa el puesto sexto. Concretamente el robo de 500 millones de cuentas en un ataque que de acuerdo a la información publicada podría estar respaldado por un país extranjero, ocurrido en finales de 2014. Entre los datos robados, de nuevo se encontraban preguntas y respuestas de seguridad sin cifrar.

Continuando con este ranking, en séptima posición aparece el robo de 400 millones de cuentas de Friend Finder Network Inc., compañía que gestiona diferentes páginas de citas. La información robada incluía datos personales, como correo electrónico, patrones de navegación, patrones de compra y orientación sexual de los usuarios.

El octavo puesto es para el mayor ataque de Denegación de Servicio (DDoS) producido hasta la fecha con dispositivos de Internet de las cosas (IoT). Producido por la botnet Mirai, compuesta por cientos de miles de cámaras IP junto a otros dispositivos IoT, dejó fuera de juego a múltiples servicios de Internet, llegando a afectar a PlayStation Network y Twitter, entre otros. Además, se sospecha que este ciberataque ***habría sido también una prueba de concepto para afectar al funcionamiento de los sistemas de voto electrónico de EE.UU.*** previamente a las ***elecciones presidenciales*** del 8 de noviembre.

El noveno lugar de esta clasificación lo ocupa el fallo en la implementación de la stack TCP en sistemas Linux posteriores a la versión de Kernel 3.6. Este fallo, que permitía la infección de malware de forma remota o incluso el secuestro del tráfico de los usuarios, afectaba a todos los dispositivos móviles con sistema operativo Android y a las televisiones inteligentes, además de degradar las conexiones mediante el protocolo Https y redirigir el tráfico.

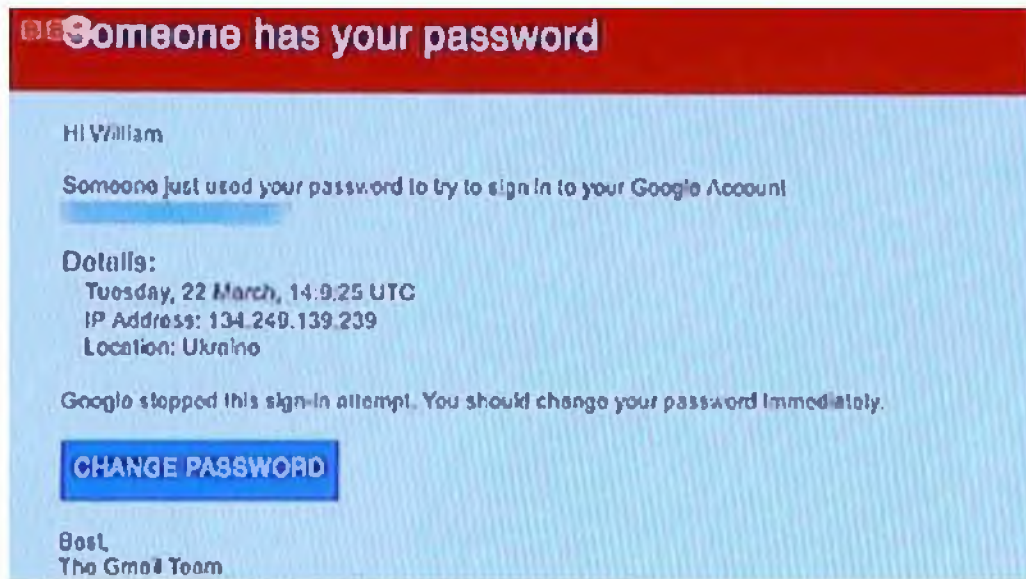
Cierra este ranking el fallo en los procesadores Qualcomm que permitía acceder a la información cifrada sin que se activaran los mecanismos de borrado. Esta vulnerabilidad en la generación de las claves de cifrado afectó aproximadamente al 60% de los teléfonos Android del mercado

2.5 Ataques desde Rusia a la campaña presidencial del partido demócrata de los Estados Unidos de Norteamérica

Se trató de una Ataque mediante Phishing al Comité Nacional del Partido Demócrata de los Estados Unidos y a la organización de la campaña y esto ocurrió mediante la obtención de la clave del mail Google (Gmail), que un integrante del equipo de campaña ingresó, “actualizando” su clave, cayendo en el engaño. El horario de los hackeos coincide con la zona de Rusia, así como también se detectaron códigos alfabetos del idioma ruso.

Salió publicado en GUCCIFER 2.0 luego se publicó en Wikileaks, unos 19.252 correos electrónicos. La campaña de Clinton y el Partido Demócrata fueron objeto de múltiples ataques que causaron el robo de información, pero el que se describe fue el de mayor relevancia.

John Podesta era el jefe de la campaña de Hillary Clinton, un antiguo asesor del presidente Barack Obama y parte del equipo de la Casa Blanca. En marzo pasado, cuando estaba en marcha la campaña de las primarias demócratas, Podesta recibió la siguiente alerta de correo electrónico:



Era totalmente similar al que recibe cualquier usuario del correo de Google recibe cuando ocurre un inicio de sesión sospechoso, desde un lugar inusual o en un dispositivo desconocido.

Para proteger la seguridad de la cuenta, pide que el usuario cambie la contraseña inmediatamente y de esa manera quede bloqueado cualquier nuevo intento de ingreso cuando la clave fue robada.

Podestá no hizo click al instante, sino que envió ese mensaje a su equipo de soporte técnico y ciberseguridad para que se encargaran de comprobar la veracidad de la alerta.

"Este es un correo legítimo", fue el diagnóstico de Charles Delavan, del equipo técnico de Clinton, el 19 de marzo pasado, según una investigación de The New York Times.

Podestá no era el único que había recibido el correo, sino que se trataba de una oleada de correos dirigidos a miembros del Comité Nacional Demócrata y los miembros de la campaña de Clinton.

Los correos de "phishing" fueron enviados a múltiples empleados de la campaña demócrata, en la que también fueron "hackeados" computadoras.

Hacer clic en el botón "cambiar contraseña" de ese correo fue quizás el error que desencadenó uno de los mayores golpes a la campaña de Hillary Clinton.

John Podestá acababa de entregar su contraseña genuina gracias al método de hackeo "phishing" o suplantación de identidad.

El Comité Nacional Demócrata hizo público en junio el hackeo, pero desde abril el partido tuvo conocimiento de que las computadoras habían sido infiltradas, correos electrónicos intervenidos y los chats espiados.

Desde junio, Schultz denunció la intromisión, pues dijo que la firma de seguridad CrowdStrike, contratada por los demócratas. La firma identificó dos grupos de atacantes, uno llamado "Fancy Bear" que acababa de entrar al sistema, y otro que llevaba allí casi un año y se denomina "Cozy Bear".

Ambos son nombres utilizados por un grupo de ciberespionaje vinculado al gobierno ruso que los investigadores del FBI han llamado The Dukes (los duques). No obstante, el gobierno de Vladimir Putin ha descalificado las acusaciones de EE.UU. sobre ataques cibernéticos a EE.UU.

Lo que también coincidió con los ataques, eran los husos horarios de los mismos, y los días laborales de Rusia.

Nerea Tunden fue una de las asesoras de Hillary Clinton cuyos correos electrónicos fueron publicados en internet. No solo los correos de Tunden, sino múltiples correos de Podesta y otros demócratas de alto rango fueron publicados, sino que miles de correos publicados por WikiLeaks, antes y después de la Convención Nacional Demócrata que nominó a Clinton, y cuyo origen se ha negado a revelar su fundador, Julian Assange.

Pero quizás este "compromete" pudo haberse evitado si el asesor de seguridad de los demócratas no hubiera cometido el error que reconoció en una entrevista al diario The New York Times, esto es haber olvidado escribir un "no" en su respuesta en inglés a John Podesta. Es decir, no haberle escrito "This is 'not' a legitimate email", en español: "Este 'no' es un correo legítimo".

Estos grupos rusos vienen trabajando hace años. Como antecedente, en el año 2007, se produjo un ataque a todas las infraestructuras críticas del país de Estonia, incluyendo a la banca electrónica, principalmente con ataques DoS (Denegación de Servicios).

2.6 Delito Tecnológico de elevado daño estratégico - IMSI Catcher

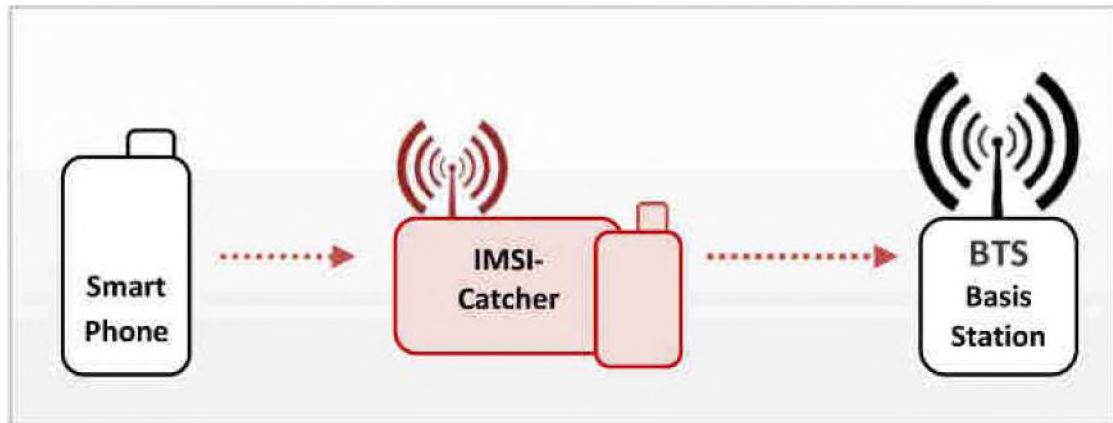
Un IMSI Catcher es una falsa estación base que actúa entre el teléfono móvil objetivo y las verdaderas torres de proveedores de servicio, de esta manera intercepta las informaciones que transitan entre ambos, haciéndose pasar por una antena de telefonía móvil.

Este sistema puede ser instalado en un vehículo tipo camioneta y su peligrosidad radica en la capacidad de irradiar con más potencia que la estación base y conseguir que el móvil se enganche a él.

Características:

Puede identificar todos los dispositivos que están a su alrededor e interactuar con los mismos, haciendo que suenen mediante una llamada, enviarles un mensaje de cualquier contacto, interceptar sus llamadas, el

tráfico de datos (man in the Middle) y por ende todas las claves que se escriban y los mensajes de texto e incluso tomar el control del dispositivo.



Fuente: <http://sujeet.bambawale.com/2016/01/20/what-is-an-imsi-catcher/>



Fuente: <http://www.army-technology.com/>

En nuestro país⁷ como en muchos otros, no se lo utiliza legalmente (aunque existen agencias de determinados países que lo utilizan con orden

⁷ Como es sabido, la interceptación legal de los celulares se realiza a través de la Corte Suprema de Justicia de la Nación y tecnológicamente, existen conexiones de fibra óptica a las centrales de las Compañías Celulares las cuales conectan los abonados intervenidos a dichos vínculos.

judicial o autorización legal) pero también existen equipos por todo el mundo y en cualquier mano, mientras que en algunos países directamente es un equipo ilegal.

Con una mínima logística (un vehículo o utilitario chico cerca del "objetivo") se puede interceptar cualquier celular y grabar su tráfico de voz y mensajes de texto. Con ciertos modelos de celulares y equipos interceptores se puede provocar una llamada y registrar lo que se habla desde el propio micrófono del celular intervenido.

Cuando es atacado un celular de una alta autoridad nacional, el impacto estratégico del daño puede ser muy elevado.

Capítulo 3 - Marco Normativo

3.1 Legislación Argentina

A continuación, se detallan la normativa vigente relacionada con la ciberseguridad en la República Argentina, cuyos textos completos se adjuntan como Anexos al presente Trabajo Final de Especialización:

- Ley 25.326 - PROTECCION DE LOS DATOS PERSONALES. Principios generales relativos a la protección de datos. Derechos de los titulares de datos. Usuarios y responsables de archivos, registros y bancos de datos. Control. Sanciones. Acción de protección de los datos personales.
- Ley 25.506 - FIRMA DIGITAL. Certificados digitales. Certificador licenciado. Titular de un certificado digital. Organización institucional. Autoridad de aplicación. Sistema de auditoría. Comisión Asesora para la Infraestructura de Firma Digital. Responsabilidad. Sanciones.
- Ley 25.520 - LEY DE INTELIGENCIA NACIONAL. Bases jurídicas, orgánicas y funcionales del Sistema de Inteligencia de la Nación. Principios generales. Protección de los derechos y garantías de los habitantes. Organismos de Inteligencia. Política de Inteligencia Nacional. Clasificación de la información. Interceptación y Captación de Comunicaciones. Personal y capacitación. Control parlamentario. Disposiciones penales.
- Ley 25.873 – MODIFICACIÓN DE LA LEY NACIONAL DE TELECOMUNICACIONES (LEY 19.798) Establece responsabilidad de los prestadores respecto de la captación y derivación de comunicaciones para su observación remota por parte del Poder Judicial o Ministerio Público

- Ley 26.388 – Modificación del CÓDIGO PENAL a fin de incorporar los “Delitos Informáticos”
- Ley 26.904 - Modificación del CÓDIGO PENAL a fin de incorporar el delito de delito contra la integridad sexual de la misma (Ciber-acoso o “Grooming”)
- Ley 27.078 – LEY DE ARGENTINA DIGITAL
- Ley 27.126 - AGENCIA FEDERAL DE INTELIGENCIA. Creación. Ley N° 25.520. Modificación.
- Decreto 256/2015 - CORTE SUPREMA DE JUSTICIA DE LA NACIÓN. Transfiérase el Departamento de Interceptación y Captación de las Comunicaciones.

3.2 Infraestructuras Críticas de Información y Ciberseguridad

El “Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad” (ICIC), creado mediante la Resolución JGM N° 580/2011, tiene como finalidad impulsar la creación y adopción de un marco regulatorio específico que propicie la identificación y protección de las infraestructuras estratégicas y críticas del Sector Público Nacional, los organismos interjurisdiccionales y las organizaciones civiles y del sector privado que así lo requieran, y la colaboración de los mencionados sectores con miras al desarrollo de estrategias y estructuras adecuadas para un accionar coordinado hacia la implementación de las pertinentes tecnologías, entre otras acciones.

El ICIC funciona en el ámbito de la Oficina Nacional de Tecnologías de Información (ONTI), la cual coordinará las actividades vinculadas al programa con las entidades y jurisdicciones definidas en el artículo 8° de la Ley N° 24.156 y sus modificatorias, los organismos interjurisdiccionales y las organizaciones civiles y del sector privado que adhieran al mismo.

Las tecnologías de la información, y especialmente Internet, han sido paulatinamente incorporadas en la gestión de los organismos públicos. Esto ha significado un avance importante en términos de eficiencia, productividad y comunicación. Sin embargo, la misma interconectividad que permite transmitir en un instante información a cualquier lugar del planeta con sólo presionar una tecla, también crea oportunidades desconocidas hasta hoy, para quienes se proponen causar un daño, obtener una ventaja económica o simplemente acceder a un recurso o a una información sin la debida autorización.

La protección de los recursos informáticos de la Administración Pública Nacional representa un verdadero desafío, y al mismo tiempo, un objetivo que no debe ni puede pasarse por alto.

Oportunamente la Subsecretaría de la Gestión Pública de la Jefatura de Gabinete de Ministros dispuso la creación de ArCERT, en la actualidad llamado ICIC CERT, unidad de respuesta ante incidentes en redes que centraliza y coordina los esfuerzos para el manejo de los incidentes de seguridad que afecten los recursos informáticos de la Administración Pública Nacional, es decir cualquier ataque o intento de penetración a través de sus redes de información.

También difunde información con el fin de neutralizar dichos incidentes, en forma preventiva o correctiva, y capacita al personal técnico afectado a las redes de los organismos del Sector Público Nacional. ArCERT comenzó a funcionar en mayo de 1999 en el ámbito de la Subsecretaría de la Gestión Pública, siendo sus principales funciones: Centralizar los reportes sobre incidentes de seguridad ocurridos en la APN y facilitar el intercambio de información para afrontarlos.

ICIC CERT es una unidad de respuesta ante incidentes en redes que centraliza y coordina los esfuerzos para el manejo de los incidentes de seguridad que afecten los recursos informáticos de la Administración Pública

Nacional, es decir cualquier ataque o intento de penetración a través de sus redes de información. También difunde información con el fin de neutralizarlos y facilitar el intercambio de información para afrontarlos.

ICIC CERT tiene como funciones el recibir reportes de incidentes de seguridad que los distintos organismos reporten, y brindar una respuesta a los mismos, coordinando acciones para solucionar el problema que dio origen al incidente.

ICIC CERT está en contacto con los demás equipos de seguridad existentes en el mundo, y con las organizaciones que agrupan a los equipos de seguridad como, por ejemplo, la organización FIRST (Forum of Incident Response and Security Teams), que nuclea a CERT's de todo el mundo, actúa como repositorio de información y centro de intercambio de experiencias.

Proveer un servicio especializado de asesoramiento en seguridad de redes. Promover la coordinación entre los organismos de la APN para prevenir, detectar, manejar y recuperar incidentes de seguridad.

Actuar como repositorio de toda la información sobre incidentes de seguridad, herramientas y técnicas de defensa

Capítulo 4 - Indicadores Internacionales

4.1 Proyecto Índice Mundial de Ciberseguridad

A los efectos de este Trabajo Final de Especialización, se contemplaron tanto los datos internacionales como nacionales, siendo que estos últimos, son muy pocos debido a que no está unificado y/o coordinado el esfuerzo del Estado en el relevamiento, vigilancia, prevención, investigación y conjuración o represión de esta **modalidad delictiva**, la cual atraviesa todos los estamentos de nuestra sociedad y tiende inexorablemente a crecer exponencialmente, de tal manera, que en un futuro próximo, algunos delitos “físicos” serán reemplazados **por delitos con el uso de tecnologías o en tecnologías**.

El principal obstáculo consiste en que la admisión de vulnerabilidades podría llegar a considerarse una debilidad, lo que obstaculizaría el debate sobre ciberamenazas y prácticas óptimas y el intercambio de información sobre éstas. Sin embargo, la seguridad “oscurantista” no es un modelo de defensa viable frente a las ciberamenazas modernas.

La solución consiste en implementar mecanismos de ciberseguridad en todos los estratos de la sociedad. No obstante, la motivación y el incentivo para proceder de este modo son inadecuados, ya sea por las limitaciones de índole económica o sencillamente por **falta de la adecuada concientización**.

Un primer paso para remediar esta situación sería la comparación de las capacidades de seguridad de los Estados nación y la publicación de una clasificación efectiva de su situación.⁸

Un sistema de clasificación revelaría las deficiencias existentes y serviría de acicate para que los Estados intensificasen sus esfuerzos en

⁸ El Índice Mundial de Ciberseguridad (IMC) surge de la asociación de colaboración entre el sector privado (ABI Research) y la Unión Internacional de Telecomunicaciones, que contribuye a una mejor comprensión del compromiso de los estados soberanos con la ciberseguridad.

materia de ciberseguridad. Sólo puede sopesarse el valor real de la capacidad de ciberseguridad de un país, por comparación.

El proyecto de Índice Mundial de Ciberseguridad (IMC) tiene por objeto medir efectivamente el nivel de compromiso con la ciberseguridad de cada Estado nación.

La meta en última instancia es contribuir al fomento de una cultura mundial de la ciberseguridad y a su integración como componente fundamental de las tecnologías de la información y la comunicación.

Este proyecto lo han puesto en marcha la Unión Internacional de Telecomunicaciones (UIT) y la empresa del sector privado ABI Research.

El proyecto del IMC se fundamenta en el mandato actual de la UIT y en los proyectos y actividades afines de la Oficina de Desarrollo de las Telecomunicaciones (BDT) de la UIT.

La UIT es el facilitador principal para la Línea de Acción C5 de la CMSI (Cumbre Mundial sobre la Sociedad de la Información) para ayudar a las partes interesadas a crear confianza y seguridad en la utilización de las TIC a nivel nacional, regional e internacional.

El mandato de la UIT sobre ciberseguridad queda además confirmado por la Resolución 69 sobre “Creación de equipos nacionales de intervención en caso de accidente informático, especialmente para los países en desarrollo, y cooperación entre los mismos” adoptada en la quinta Conferencia Mundial de Desarrollo de las Telecomunicaciones (CMDT-10) y en virtud de la Resolución 130 (Busán, 2014) sobre “Fortalecimiento del papel de la UIT en la creación de confianza y seguridad en la utilización de las tecnologías de la información y la comunicación”.

En este contexto, el Secretario General presentó la Agenda sobre Ciberseguridad Global (GCA), como marco de la UIT para la cooperación

entre todas las partes interesadas en la construcción de una sociedad de la información más segura, centrándose en las siguientes áreas de trabajo:

- Medidas jurídicas
- Medidas técnicas
- Medidas organizativas
- Creación de capacidades
- Cooperación.

Estas cinco áreas designadas constituirán la base de los indicadores para el IMC. Estos cinco indicadores son críticos para medir las capacidades nacionales de ciberseguridad, debido a que forman los elementos constructivos intrínsecos de cada cultura nacional. La ciberseguridad tiene un ámbito de aplicación que alcanza a todas las industrias y a todos los sectores, tanto vertical como horizontalmente.

Por este motivo, para poder desarrollar las capacidades nacionales es preciso que las fuerzas políticas, económicas y sociales realicen inversiones. Esto puede ser competencia de los departamentos de justicia y orden público, las instituciones educativas y los ministerios, los operadores del sector privado, y los desarrolladores de tecnología, las asociaciones público-privadas y la cooperación interestatal.

El objetivo a largo plazo es impulsar más esfuerzos para la adopción e integración de la ciberseguridad a escala mundial. La comparación de las estrategias de ciberseguridad nacionales pondrá de manifiesto qué Estados ocupan los lugares más altos de la clasificación en ámbitos específicos y, por consiguiente, expondrá estrategias de ciberseguridad menos conocidas que otras, aunque igualmente acertadas.

Esto puede provocar además un aumento del intercambio de información sobre el despliegue de la ciberseguridad en aquellos Estados con distintos niveles de desarrollo. Al medir el nivel de preparación para la ciberseguridad en diversos ámbitos, este índice permitirá a los Estados

determinar en qué punto de la escala de desarrollo se encuentran, los aspectos en los que necesitan mejorar y lo lejos que se encuentran de implementar un nivel de ciberseguridad aceptable.

Todos los Estados progresan hacia un entorno más digital y conectado, por lo que la adopción temprana de la ciberseguridad podrá facilitar el despliegue de una infraestructura más segura y con mayor capacidad de recuperación a largo plazo.

El proyecto del IMC será una labor conjunta entre la BDT, específicamente la División de ciberseguridad y aplicaciones TIC (CYB) y ABI Research. La CYB actuará como coordinadora y propietaria del proyecto, mientras que ABI Research aportará sus conocimientos fundamentales en desarrollo de estrategias, inteligencia competitiva, planificación de negocios, evaluación tecnológica y evaluación comparativa de las industrias, para la realización del proyecto. ABI Research es una empresa de información sobre el mercado, especializada en la predicción cuantitativa y el análisis de las tendencias y métricas clave de los mercados tecnológicos mundiales. ABI Research, que sobresale en el suministro de información orientada hacia el futuro y elementos de datos del mundo real, fundamentados y oportunos, sobre el sector tecnológico, aportará sus conocimientos especializados para el desarrollo puntual y la producción de un índice fiable.

En virtud de este acuerdo, la UIT y ABI Research:

- han definido una métrica del rendimiento;
- han elaborado un mecanismo de clasificación mundial;
- han investigado y recopilado datos sobre las capacidades de los Estados nación en materia de ciberseguridad;
- han establecido contacto y se han coordinado con los Estados nación y las organizaciones pertinentes;

- han identificado los datos pertinentes y los han incorporado al índice;
- han publicado un índice mundial de ciberseguridad.

4.2 Categorías e indicadores de rendimiento

El IMC es una clasificación de evaluaciones comparativas en la que se midan las capacidades de desarrollo de la ciberseguridad de los Estados nación soberanos. Este índice es esencialmente un indicador compuesto, en el que se agregan varios indicadores individuales.

El proceso del desarrollo de la ciberseguridad puede analizarse en cinco amplias categorías de importancia. Se han definido los indicadores y subgrupos que se indican a continuación, que permitirán clasificar a las naciones con arreglo a la evaluación comparativa correspondiente a cada indicador.

4.3 Medidas jurídicas

La legislación es una medida crítica para la habilitación de un marco armónico que permita a las entidades alinearse de acuerdo con una base de reglamentación común, ya sea en materia de prohibición de una conducta delictiva específica o de requisitos mínimos de reglamentación.

Las medidas jurídicas permiten además que un Estado nación establezca los mecanismos básicos de respuesta a las infracciones: mediante la investigación y la persecución de los delitos y la imposición de sanciones por falta de conformidad o incumplimiento de la ley.

El marco legislativo establece las normas de comportamiento mínimas con carácter general, aplicables a todos, y sobre las que pueden construirse mayores capacidades de ciberseguridad.

En última instancia, el objetivo es conseguir que todos los Estados nación dispongan de una legislación adecuada a fin de armonizar

supranacionalmente las prácticas y ofrecer un marco de medidas interoperables que facilite la lucha internacional contra la ciberdelincuencia.

El entorno legal puede medirse a partir de la existencia de varias instituciones y marcos jurídicos competentes en materia de ciberseguridad y ciberdelincuencia. Este subgrupo consta de los siguientes indicadores de rendimiento:

4.4 Legislación penal

La legislación de la ciberdelincuencia abarca las leyes sobre el acceso, la interferencia, la interceptación de computadoras, sistemas y datos, sin autorización (sin derecho).

Estas leyes pueden clasificarse por su nivel: ninguna, parcial o de amplio alcance.

La legislación parcial se refiere a la simple inserción de texto alusivo a la informática en una ley o código penal existente, cuyo enunciado se limite a extender al ciberespacio, por ejemplo, el fraude o la falsificación, o la vigilancia y el robo.

La legislación de amplio alcance se refiere a la promulgación de legislación específica o de una ley que aborde los aspectos específicos del delito informático (por ejemplo, la Ley de Utilización Indebida de la Informática del Reino Unido de 1990). Esta categoría puede incluir legislación parcial cuando exista un amplio desarrollo de la legislación consuetudinaria o jurisprudencia. Sírvanse indicar los tipos de leyes y reglamentos, así como su ausencia, o su carácter parcial o de amplio alcance.

4.5 Reglamento y conformidad

La reglamentación de la ciberseguridad comprende las leyes que tratan de la protección de datos, la notificación de infracciones y los requisitos de certificación/normalización.

Estas leyes pueden clasificarse por su nivel: ninguna, parcial o de amplio alcance. La reglamentación parcial se refiere a la inserción de un texto alusivo a la informática en el derecho penal o civil, de modo que se extienda al ciberespacio la aplicabilidad de una reglamentación que no está relacionada específicamente o exclusivamente con la ciberseguridad (por ejemplo, la Directiva de la UE 95/46/EC sobre protección de los individuos con respecto al procesamiento de datos personales y sobre el libre movimiento de dichos datos).

La reglamentación de amplio alcance se refiere a la promulgación de legislación específica, ley o directiva que exija la conformidad con la ciberseguridad (por ejemplo, la Ley Federal de Gestión de la Seguridad de la Información de EE.UU., de 2002). Sírvanse indicar los tipos de leyes y reglamentos, así como su ausencia, o su carácter parcial o de amplio alcance.

4.6 Medidas técnicas

La tecnología es la primera línea defensiva frente a las ciberamenazas y los agentes malintencionados en línea.

Sin las medidas técnicas adecuadas ni las capacidades para detectar y responder a los ciberataques, los Estados nación y sus entidades respectivas son vulnerables a las ciberamenazas.

La proliferación y el éxito de las TIC⁹ sólo pueden ser verdaderamente viables en un clima de confianza y seguridad. Por este motivo, es necesario que los Estados nación sean capaces de preparar estrategias para el establecimiento de criterios mínimos de seguridad aceptables y regímenes de acreditación de las aplicaciones de software y de los sistemas. Es necesario que esta labor venga acompañada de la creación de una entidad nacional dedicada especialmente a resolver los incidentes informáticos a nivel nacional, como mínimo con un organismo gubernamental responsable y un

⁹ Tecnologías de la Información y Comunicaciones

marco nacional concomitante para la vigilancia, la alerta y la respuesta ante incidentes.

Pueden llevarse a cabo medidas técnicas tomando como base la existencia y el número de instituciones técnicas y marcos relacionados con la ciberseguridad respaldados o creados por el Estado nación. Este subgrupo se compone de los siguientes indicadores de rendimiento:

4.7 CERT/CIRT/CSIRT

El establecimiento de un CIRT (Equipo de Respuesta ante Incidentes Informáticos), CERT (Equipo de Respuesta ante Emergencias Informáticas) o CSIRT (Equipo de Respuesta ante Incidentes de Seguridad Informática) que ofrezca las capacidades de identificar las ciberamenazas, defenderse de ellas, ofrecer una respuesta a las mismas y gestionirlas, además de mejorar la seguridad en el espacio del Estado nación.

Es necesario que esta capacidad se combine con la de recopilación de su propia información en vez de depender de fuentes de información de incidentes de seguridad secundarias, ya sea procedentes de las circunscripciones de los CIRT o de otras fuentes.

Sírvanse indicar el número y los nombres de los equipos CERT y CSIRT nacionales o específicos de algún sector, que cuenten con la aprobación oficial, así como si obedecen a un mandato legal o no. El nivel de desarrollo se clasificará con arreglo a la existencia de estos equipos nacionales y al hecho de que obedezcan a un mandato legal o no.

4.8 Normas

Este indicador mide la existencia de uno o varios marcos aprobados (o respaldados) por el Gobierno para la implementación de normas de ciberseguridad internacionalmente reconocidas en el ámbito del sector público (en el caso de organismos gubernamentales) y en el seno de las infraestructuras críticas (aunque sean explotadas por el sector privado).

Entre estas normas, se pueden mencionar las desarrolladas por los siguientes organismos: ISO, UIT, IETF, IEEE, ATIS, OASIS, 3GPP, 3GPP2, IAB, ISOC, ISG, ISI, ETSI, ISF, RFC, ISA, CEI, NERC, NIST, FIPS, PCI DSS, etc. Sírvanse indicar si cuentan con marcos nacionales (y específicos de los sectores), que cuenten con la aprobación oficial para implantar normas de ciberseguridad reconocidas internacionalmente.

4.9 Certificación

Este indicador mide la existencia de uno o varios marcos aprobados (o respaldados) por el Gobierno para la certificación y acreditación de organismos (gubernamentales) nacionales y profesionales del sector público con arreglo a normas de ciberseguridad reconocidas internacionalmente.

Entre estas certificaciones, acreditaciones y normas, cabe citar las siguientes: Conocimientos sobre seguridad en la nube (Cloud Security Alliance), CISSP, SSCP, CSSLP CBK, Analista Forense de Ciberseguridad (ISC²), GIAC, GIAC GSSP (SANS), CISM, CISA, CRISC (ISACA), CompTIA, C|CISO, CEH, ECSA, CHFI (Consejo de la CE), OSSTMM (ISECOM), PCIP/CCISP (Critical Infrastructure Institute), Certificación (sin más), Q/ISP, Certificación en Ingeniería de Seguridad de Software (Security University), CPP, PSP, PCI (ASIS), LPQ, LPC (Loss Prevention Institute), CFE (Association of Certified Fraud Examiners), Técnico certificado en incidentes de seguridad informática-CERT (SEI), CITRMS (Institute of Consumer Financial Education), CSFA (Cybersecurity Institute), CIPP (IAPP), ABCP, CBCP, MBCP (DRI), BCCP, BCCS, BCCE, DRCS, DRCE (BCM), CIA, CCSA (Institute of Internal Auditors), (Professional Risk Managers International Association), PMP (Project Management Institute), etc.

4.10 Medidas organizativas

Las medidas organizativas y procedimentales son necesarias para la adecuada implantación de cualquier tipo de iniciativa nacional. Es necesario que el Estado nación defina un objetivo estratégico general, con un plan de amplio alcance en ejecución, entrega y medición.

Es necesario habilitar estructuras tales como organismos nacionales que pongan en marcha la estrategia y evalúen el éxito o fracaso del plan.

Sin una estrategia nacional, un modelo de gobernanza y un organismo supervisor, la labor de los diferentes sectores e industrias se dispersa y queda inconexa, frustrando el intento de lograr la armonización nacional del desarrollo de la capacidad de ciberseguridad.

Las estructuras organizativas pueden medirse con arreglo a la existencia y número de instituciones y estrategias que organizan el desarrollo de la ciberseguridad a nivel nacional.

La creación de estructuras organizativas eficaces es necesaria para la promoción de la ciberseguridad, la lucha contra la delincuencia y el fomento del papel de la vigilancia, alerta y respuesta ante incidentes, a fin de lograr la coordinación entre organismos, entre sectores y transfronteriza entre las nuevas iniciativas y las previamente existentes. Este subgrupo consta de los siguientes indicadores de rendimiento:

4.11 Política

El desarrollo de una política de promoción de la ciberseguridad se reconoce como máxima prioridad. Una estrategia nacional para la seguridad de la red y de los sistemas de información debe mantener una infraestructura fiable y con capacidad de recuperación, y fijarse el objetivo de garantizar la seguridad de los ciudadanos; proteger los activos materiales e intelectuales de los ciudadanos, las organizaciones y el Estado; evitar los ciberataques a las infraestructuras críticas; y reducir al mínimo los daños producidos por los ciberataques y el tiempo de recuperación de éstos.

Las políticas sobre **Estrategias de Ciberseguridad Nacional** o Planes Nacionales para la Protección de las Infraestructuras de la Información son las definidas oficialmente y respaldadas por un Estado nación, y pueden comprender los siguientes compromisos: establecer responsabilidades claras sobre la ciberseguridad a todos los niveles gubernamentales (local, regional y

federal o nacional), con competencias y responsabilidades claramente definidas; establecer un claro compromiso con la ciberseguridad, que sea público y transparente; y fomentar la implicación del sector privado y su asociación con las iniciativas lideradas por el Gobierno para promover la ciberseguridad.

4.12 Hoja de ruta para la gobernanza

La hoja de ruta para la gobernanza en materia de ciberseguridad se establece por lo general mediante una estrategia/política nacional de ciberseguridad y por la identificación de los interesados clave.

El desarrollo de un marco de política nacional es una de las máximas prioridades en el desarrollo de la gobernanza de alto nivel para la ciberseguridad. El marco de política nacional debe tener en cuenta las necesidades de protección de las infraestructuras de información críticas para el país. También debe procurar fomentar el intercambio de información en el seno del sector público, así como entre el sector público y el privado.

La gobernanza de la ciberseguridad debe construirse sobre un marco nacional que contemple los retos y demás problemas de seguridad de la información y seguridad de la red a nivel nacional, pudiendo comprender: la estrategia y política nacionales, los fundamentos jurídicos de la adaptación de la legislación de seguridad a los entornos en red y en línea; la implicación de todas las partes interesadas; el desarrollo de una cultura para la ciberseguridad; los procedimientos para hacer frente a las infracciones de seguridad de las TIC y la gestión de los incidentes (denuncia, intercambio de información, gestión de las alertas, colaboración de la justicia y la policía); la implementación efectiva de la política de ciberseguridad nacional; y el control, evaluación, validación y optimización del programa de ciberseguridad. .

4.13 Organismo responsable

El organismo responsable de la implementación de una estrategia/política de ciberseguridad nacional puede estar integrado por

comités permanentes, grupos de trabajo oficiales, consejos asesores y centros interdisciplinarios.

La mayor parte de los organismos nacionales serán directamente responsables de los sistemas de vigilancia y alerta, y de la respuesta a los incidentes, así como del desarrollo de las estructuras organizativas necesarias para coordinar las respuestas a los ciberataques.

4.14 Evaluación comparativa nacional

Este indicador mide la existencia de los ejercicios de evaluación comparativa nacionales o específicos de algún sector, que cuenten con el reconocimiento oficial, o las referencias utilizadas para medir el desarrollo de la ciberseguridad.

Por ejemplo, una norma de seguridad nacional inspirada en ISO/CEI 27002-2005 (Referencia NCSec) puede ayudar a que los Estados nación respondan a las necesidades específicas de la ciberseguridad.

Esta referencia se divide en cinco dominios: Políticas y estrategias de la NCSec; Estructuras organizativas de la NCSec; Implementación de la NCSec; Coordinación nacional de la NCSec; y Actividades de sensibilización de la NCSec. Sírvanse indicar los ejercicios de evaluación comparativa o referencias, nacionales o específicos de algún sector, que cuenten con el reconocimiento oficial para medir el desarrollo de la ciberseguridad.

4.15 Creación de capacidades

La creación de capacidades es intrínseca a las tres primeras medidas (jurídicas, técnicas y organizativas). La comprensión de la tecnología, el riesgo y las implicaciones puede contribuir a mejorar la legislación, las políticas y las estrategias, así como las organizaciones en cuanto a sus diversas competencias y responsabilidades.

La ciberseguridad **es un área relativamente nueva**, no mucho más antigua que Internet.

Esta área de estudio suele acometerse desde una perspectiva tecnológica; sin embargo, existen muchas implicaciones socioeconómicas y políticas que tienen aplicabilidad en esta área.

La creación de capacidades humanas e institucionales es necesaria para mejorar el conocimiento y la preparación técnica de todos los sectores, a fin de aplicar las soluciones idóneas y promover el desarrollo de los profesionales más competentes.

Un marco de creación de capacidades para promover la ciberseguridad debe comprender la sensibilización y la disponibilidad de recursos. La creación de capacidades puede medirse con arreglo a la existencia de varios programas de investigación y desarrollo, educación y formación, y de organismos profesionales en el sector público certificados.

4.16 Desarrollo de la normalización

La normalización constituye un buen indicador del grado de madurez de una tecnología. La aparición de nuevas normas en áreas clave destaca la importancia vital de dichas normas.

Aunque la ciberseguridad siempre ha sido un problema para la seguridad nacional que se ha tratado de forma diferente en los diversos países, hay planteamientos comunes que están respaldados por normas comúnmente reconocidas. Entre estas normas cabe citar las desarrolladas por los siguientes organismos: ISO, UIT, IETF, IEEE, ATIS, OASIS, 3GPP, 3GPP2, IAB, ISOC, ISG, ISI, ETSI, ISF, RFC, ISA, CEI, NERC, NIST, FIPS, PCI DSS, etc.

4.17 Desarrollo laboral

El desarrollo laboral debe comprender la labor de los Estados nación orientada a la promoción de campañas de publicidad de amplia difusión, con el fin de lograr la mayor audiencia posible, así como el recurso a las ONG, instituciones, organizaciones, ISP, bibliotecas, cámaras de comercio, centros

comunitarios, tiendas de informática, centros de estudios superiores y programas de educación de adultos, colegios y organizaciones y asociaciones de padres de alumnos para transmitir el mensaje del “cibercomportamiento” seguro en línea.

Esto comprende medidas tales como la creación de portales y sitios web para promover la sensibilización, distribuir el material de apoyo a los educadores e impartir cursos de capacitación profesional y programas educativos (o incentivar la asistencia a los mismos), la promoción de los cursos sobre ciberseguridad en la educación superior (enseñanzas técnicas, ciencias sociales, etc.) y el fomento de la certificación de los profesionales, tanto en el sector público como en el privado.

4.18 Certificación profesional

Este indicador de rendimiento puede medirse a partir del número de profesionales del sector público certificados con arreglo a normas de los programas de certificación internacionalmente reconocidos, entre los que cabe citar los siguientes: Conocimiento sobre seguridad en la nube (Cloud Security Alliance), CISSP, SSCP, CSSLP CBK, Analista Forense de Ciberseguridad (ISC²), GIAC, GIAC GSSP (SANS), CISM, CISA, CRISC (ISACA), CompTIA, C|CISO, CEH, ECSA, CHFI (Consejo de la CE), OSSTMM (ISECOM), PCIP/CCISP (Critical Infrastructure Institute), Certificación, Q/ISP, Certificación en Ingeniería de Seguridad de Software (Security University), CPP, PSP, PCI (ASIS), LPQ, LPC (Loss Prevention Institute), CFE (Association of Certified Fraud Examiners), Técnico certificado en incidentes de seguridad informática-CERT (SEI), CITRMS (Institute of Consumer Financial Education), CSFA (Cybersecurity Institute), CIPP (IAPP), ABCP, CBCP, MBCP (DRI), BCCP, BCCS, BCCE, DRCS, DRCE (BCM), CIA, CCSA (Institute of Internal Auditors), (Professional Risk Managers International Association), PMP (Project Management Institute), etc.

4.19 Certificación del organismo

Este indicador de rendimiento puede medirse a partir del número de organismos gubernamentales y del sector público certificados con arreglo a

normas reconocidas internacionalmente. Entre estas normas cabe citar las desarrolladas por los siguientes organismos: ISO, UIT, IETF, IEEE, ATIS, OASIS, 3GPP, 3GPP2, IAB, ISOC, ISG, ISI, ETSI, ISF, RFC, ISA, CEI, NERC, NIST, FIPS, PCI DSS, etc.

4.20 Cooperación

La ciberseguridad necesita la contribución de todos los sectores y disciplinas, y por este motivo es necesario que se acometa con arreglo a un planteamiento de múltiples partes interesadas. La cooperación mejora el diálogo y la coordinación, lo que hace posible la creación de un ámbito de aplicación de la ciberseguridad de mayor alcance.

El intercambio de información es difícil, en el mejor de los casos, entre las diversas disciplinas y entre los operadores del sector privado. Este problema se agudiza a nivel internacional. No obstante, el problema de la ciberdelincuencia tiene carácter mundial y no le afectan ni las fronteras nacionales ni las distinciones entre sectores. La cooperación permite el intercambio de información sobre amenazas, casuística de los ataques y las prácticas óptimas de respuesta y defensa ante éstos.

La intensificación de las iniciativas de colaboración puede hacer posible el desarrollo de capacidades de ciberseguridad mucho más fuertes, lo que contribuirá a evitar la reiteración y persistencia de las amenazas en línea, mejorando la investigación, captura y procesamiento de los agentes malintencionados.

La cooperación nacional e internacional puede medirse con arreglo a la existencia de varias alianzas, marcos de colaboración y redes de intercambio de información.

4.21 Cooperación interestatal

La cooperación interestatal se refiere a las asociaciones nacionales o específicas de los sectores reconocidas oficialmente para el intercambio de activos de ciberseguridad transfronterizo con otros Estados nación (es decir,

firmando asociaciones bilaterales o multilaterales para la cooperación o el intercambio de información, conocimientos técnicos especializados, tecnología y/o recursos).

La cooperación interestatal también comprende las iniciativas a nivel regional, tales como las emprendidas por la Unión Europea, el Consejo de Europa, el Grupo de Estados del G8, el Foro de Cooperación Económica de Asia-Pacífico (APEC), la Organización de Estados Americanos (OEA), la Asociación de Naciones del Sudeste Asiático (ASEAN), la Liga Árabe, la Unión Africana, la Organización de Cooperación de Shanghái (SCO) y los Grupos de Operaciones de Red (NOG), etc. Sirvanse indicar si existen asociaciones nacionales o específicas de algún sector, que cuenten con el reconocimiento oficial para el intercambio de activos de seguridad a través de las fronteras con otros Estados nación.

4.22 Cooperación entre organismos

La cooperación entre organismos se refiere a la existencia de programas nacionales o específicos de algún sector que cuenten con el reconocimiento oficial para el intercambio de activos de ciberseguridad (personas, procesos o herramientas) en el seno del sector público (por ejemplo, asociaciones oficiales para la cooperación o el intercambio de información, conocimientos especializados, tecnología y/o recursos entre departamentos y agencias y organismos). Esto comprende las iniciativas y programas entre sectores diferentes (fuerzas de orden público, defensa, atención sanitaria, transporte, energía, residuos y gestión del agua, etc.), así como en el seno de los departamentos/ministerios (gobiernos federales/locales, recursos humanos, servicio de atención TI, relaciones públicas, etc.).

4.23 Asociaciones entre los sectores público y privado

Las asociaciones público-privadas (PPP) son empresas entre el sector público y el privado. Este indicador de rendimiento puede medirse por el número de PPP nacionales o de algún sector específico, que cuenten con el

reconocimiento oficial para el intercambio de activos (personas, procesos y herramientas), conocimientos especializados, tecnología y/o recursos).

4.24 Cooperación internacional

Este indicador de rendimiento se refiere a la participación en plataformas y foros internacionales sobre ciberseguridad que cuenten con el reconocimiento oficial.

Entre estas iniciativas de colaboración se encuentran las emprendidas por: la Asamblea General de las Naciones Unidas; la Unión Internacional de Telecomunicaciones (UIT); Interpol/Europol; la Organización para la Cooperación y el Desarrollo Económico (OCDE); la Oficina de las Naciones Unidas contra la Droga y el Delito (ONUDD); el Instituto Interregional de las Naciones Unidas para Investigaciones sobre la Delincuencia y la Justicia (UNICRI); la Corporación de Internet para la Asignación de Nombres y Números (ICANN); la Organización Internacional de Normalización (ISO); la Comisión Electrotécnica Internacional (CEI); el Grupo de Tareas Especiales sobre Ingeniería de Internet; FIRST (Foro sobre los Equipos de Seguridad y Respuesta ante Incidentes).

4.25 Metodología del Índice de Ciberseguridad

El modelo estadístico utilizado se inspirará en el análisis multi-criterios (MCA). El MCA establece la preferencia entre alternativas por referencia a un conjunto explícito de objetivos identificados para los que se han definidos criterios de evaluación del grado en el que se han alcanzado dichos objetivos. Se aplicará un simple modelo de evaluación lineal aditiva. La matriz de rendimiento del MCA describe las alternativas, mientras que cada columna describe el rendimiento de las alternativas en relación con cada uno de los criterios. La evaluación individual del rendimiento es numérica. La puntuación de la evaluación comparativa se apoyará en los indicadores siguientes, cada uno de los cuales se pondera igualmente (aunque la ponderación de algunas subcategorías será ligeramente superior a las otras, dado que algunas contienen más subgrupos).

Se otorgan 0 puntos cuando no haya actividades; 1 punto cuando la medida tenga carácter parcial; y 2 puntos para las medidas de más amplio alcance.

La puntuación total atribuida a cada una de las categorías es la siguiente:

1. Medidas jurídicas 4

- A. Legislación penal 2
- B. Reglamentación y conformidad. 2

2. Medidas técnicas 6

- A. CERT/CIRT/CSIRT 2
- B. Normas 2
- C. Certificación 2

3. Medidas organizativas 8

- A. Política 2
- B. Hoja de ruta de gobernanza 2
- C. Organismo responsable 2
- D. Evaluación comparativa nacional 2

4. Creación de capacidades 8

- A. Desarrollo de normas 2
- B. Desarrollo laboral 2
- C. Certificación profesional 2
- D. Certificación del organismo 2

5. Cooperación 8

- A. Cooperación interestatal 2
- B. Cooperación entre organismos 2
- C. Asociaciones entre los sectores público y privado 2
- D. Cooperación internacional 2

Notación:

x_{qc} Valor del indicador individual q para el país c, siendo $q=1,..., Q$ y $c=1,..., M$.

I_{qc} Valor normalizado del indicador individual q para el país c

CI_c Valor del indicador compuesto para el país c

La referencia utilizada será la puntuación del país hipotético que maximice la puntuación global de la preparación (34). El índice compuesto resultante variará entre cero (correspondiente a la peor preparación posible) y 1 (la referencia):

$$CI_c = I_{qc} / 34$$

La técnica de normalización utilizará el método de clasificación:

$$I_{qc} = Rank(x_{qc})$$

4.26 Repercusión

El objetivo a largo plazo del IMC es seguir impulsando la labor de adopción e integración de la ciberseguridad a escala mundial.

La comparación de las estrategias nacionales de ciberseguridad pondrá de manifiesto aquellos Estados que se clasifiquen en los primeros lugares en áreas específicas, y por consiguiente expondrá estrategias de ciberseguridad, menos conocidas que otras aunque igualmente acertadas.

Esto puede provocar además un aumento del intercambio de información sobre el despliegue de la ciberseguridad, entre Estados con diferentes niveles de desarrollo.

Midiendo el nivel de preparación en ciberseguridad en diversas áreas, el índice permitirá a los Estados evaluar su situación en una escala de desarrollo, si necesitan mejorar o no, y lo lejos que se encuentran de implementar un nivel aceptable de ciberseguridad.

Todos los Estados progresan hacia un entorno más digitalizado y conectado, por lo que la adopción de la ciberseguridad en una fase temprana puede facilitar el despliegue de una infraestructura más segura y con mayor capacidad de recuperación.

<i>País / Índice</i>	<i>Clasificación mundial</i>
Estados Unidos de América* 0,824	1
Canadá* 0,794	2
Australia* 0,765	3
Malasia 0,765	3
Omán 0,765	3
Nueva Zelanda* 0,735	4
Noruega* 0,735	4
Brasil 0,706	5
Estonia* 0,706	5
Alemania* 0,706	5
India* 0,706	5
Japón* 0,706	5
República de Corea 0,706	5
Reino Unido 0,706	5
Austria* 0,676	6
Hungría* 0,676	6
Israel* 0,676	6
Países Bajos* 0,676	6
Singapur 0,676	6
Letonia* 0,647	7
Suecia* 0,647	7
Turquía 0,647	7
Hong Kong 0,618	8
Finlandia 0,618	8
Qatar 0,618	8
Eslovaquia 0,618	8
Uruguay 0,618	8
Colombia 0,588	9
Dinamarca* 0,588	9

<i>País / Índice</i>	<i>Clasificación mundial</i>
Egipto 0,588	9
Francia* 0,588	9
Mauricio 0,588	9
España* 0,588	9
Italia 0,559	10
Marruecos 0,559	10
Uganda 0,559	10
Azerbaiyán 0,529	11
Polonia* 0,529	11
Rwanda 0,529	11
Túnez 0,529	11
República Checa 0,500	12
Georgia 0,500	12
Rusia* 0,500	12
Indonesia 0,471	13
Luxemburgo* 0,471	13
Rumanía 0,471	13
Bélgica* 0,441	14
Bulgaria 0,441	14
China* 0,441	14
Lituania 0,441	14
Nigeria 0,441	14
Sudán 0,441	14
Argentina* 0,412	15
Camerún 0,412	15
Croacia 0,412	15
Kenya 0,412	15
Mongolia 0,412	15
Sri Lanka 0,412	15
Tailandia* 0,412	15
Brunei Darussalam 0,382	16
Chile* 0,382	16
Moldova* 0,382	16

<i>País / Índice</i>	<i>Clasificación mundial</i>
Montenegro 0,382	16
Myanmar 0,382	16
Sudáfrica 0,382	16
Costa Rica* 0,353	17
Ecuador 0,353	17
Malta* 0,353	17
Filipinas 0,353	17
Suiza 0,353	17
Ucrania* 0,353	17
Emiratos Árabes Unidos* 0,353	17
Burkina Faso 0,324	18
México* 0,324	18
Perú* 0,324	18
Viet Nam* 0,324	18
Bahrein 0,294	19
Bangladesh 0,294	19
Chipre* 0,294	19
Ghana* 0,294	19
Irán * 0,294	19
Libia 0,294	19
Panamá 0,294	19
Portugal* 0,294	19
Arabia Saudita* 0,294	19
Afganistán 0,265	20
Serbia 0,265	20
Togo 0,265	20
Côte d'Ivoire 0,235	21
Jamaica* 0,235	21
Albania 0,206	22
El Salvador* 0,206	22
Grecia* 0,206	22
Guatemala 0,206	22
Islandia* 0,206	22

<i>País / Índice</i>	<i>Clasificación mundial</i>
Irlanda* 0,206	22
Jordania 0,206	22
Liberia 0,206	22
Paraguay* 0,206	22
Tanzania 0,206	22
Trinidad y Tabago 0,206	22
Venezuela 0,206	22
Argelia 0,176	23
Armenia 0,176	23
Barbados 0,176	23
Belarús* 0,176	23
Belice* 0,176	23
Benin* 0,176	23
Bosnia y Herzegovina 0,176	23
Botswana 0,176	23
Kazajstán* 0,176	23
Malawi 0,176	23
Pakistán* 0,176	23
Samoa 0,176	23
Senegal* 0,176	23
Eslovenia* 0,176	23
Siria 0,176	23
Bahamas* 0,147	24
Mauritania* 0,147	24
Nicaragua* 0,147	24
Saint Kitts y Nevis 0,147	24
Estado de Palestina* 0,147	24
Tayikistán* 0,147	24
Macedonia* 0,147	24
Uzbekistán* 0,147	24
Vanuatu 0,147	24
Zambia 0,147	24
Antigua y Barbuda* 0,118	25

<i>País / Índice</i>	<i>Clasificación mundial</i>
Bhután 0,118	25
Bolivia * 0,118	25
Burundi 0,118	25
Camboya 0,118	25
República Dominicana 0,118	25
Granada 0,118	25
Guyana* 0,118	25
Kirguistán* 0,118	25
Liechtenstein* 0,118	25
Micronesia 0,118	25
Nepal* 0,118	25
Papua Nueva Guinea 0,118	25
Santa Lucía* 0,118	25
Seychelles* 0,118	25
Suriname* 0,118	25
San Marino 0,118	25
Angola* 0,088	26
Gambia 0,088	26
Kiribati 0,088	26
Líbano 0,088	26
Madagascar 0,088	26
Maldivas 0,088	26
Mali 0,088	26
Mónaco* 0,088	26
Niger* 0,088	26
Sudán del Sur* 0,088	26
Tonga 0,088	26
Turkmenistán* 0,088	26
Zimbabwe 0,088	26
Andorra* 0,059	27
Congo 0,059	27
Djibouti 0,059	27
Dominica* 0,059	27

<i>País / Índice</i>	<i>Clasificación mundial</i>
Fiji 0,059	27
Haití* 0,059	27
Kuwait* 0,059	27
Lao 0,059	27
Mozambique* 0,059	27
Santo Tomé y Príncipe 0,059	27
Sierra Leona 0,059	27
Swazilandia 0,059	27
Tuvalu 0,059	27
Yemen* 0,059	27
Cabo Verde 0,029	28
Chad* 0,029	28
Comoros 0,029	28
Cuba* 0,029	28
República Democrática del Congo 0,029	28
Eritrea* 0,029	28
Etiopia* 0,029	28
Gabón 0,029	28
Guinea 0,029	28
Guinea-Bissau* 0,029	28
Iraq* 0,029	28
Nauru 0,029	28
Palau* 0,029	28
Islas Salomón 0,029	28
Somalia 0,029	28
República Centroafricana* 0,000	29
República Popular Democrática de Corea* 0,000	29
Guinea Ecuatorial* 0,000	29
Honduras* 0,000	29
Lesotho 0,000	29
Namibia 0,000	29
San Vicente y las Granadinas 0,000	29

** A partir de datos secundarios (Fuente: ABI Research)*

Capítulo 5 - Respuestas o esfuerzos institucionales:

5.1 ICIC

En nuestro país existe el Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad (ICIC) dependiente de la Secretaría de Gobierno de Modernización.

La investigación de los delitos cibernéticos y las actividades conexas es llevada a cabo principalmente por la Policía Federal Argentina (PFA), a través del Departamento Ciberdelito¹⁰.

El Gobierno de Argentina también ha desarrollado políticas nacionales de seguridad de la información, y su estrategia nacional de ciberseguridad va a desarrollarse a través del Comité de Ciberseguridad, creado recientemente.

Dentro del marco del ICIC (www.icic.gov.ar) se fundó el primer CERT (equipo de respuesta a emergencias informáticas) a nivel nacional en 1994, y en 2011, se lo designó formalmente como parte de la Oficina Nacional de Tecnología de la Información (ONTI), en donde se expandió para brindar servicios adicionales. Actualmente, los cuatro objetivos principales de ICIC-CERT son los siguientes:

- Servir como repositorio de información relevante relacionada con los incidentes, herramientas y técnicas de seguridad cibernética;
- Promover la coordinación entre los administradores de redes para todas las instituciones públicas a nivel nacional, a fin de prevenir, detectar, gestionar y recuperarse de los incidentes relacionados con la seguridad que afecten sus redes

¹⁰ -Ex – Departamento CIBERCRIMEN, actualizada a la denominación Departamento CIBERDELITO con fecha 11/12/2018

- Centralizar la generación de informes respecto a incidentes que afecten las redes gubernamentales y facilitar el intercambio de información a fin de abordarlos de manera más eficaz
- Interactuar con otros equipos de respuesta ante incidentes en el país y la región

El Departamento CIBERDELITO de la PFA es la unidad responsable de las investigaciones referentes a delitos cibernéticos.

Las empresas del sector privado no están obligadas por ley a proporcionar información relacionada con los incidentes a las autoridades nacionales.

No obstante, las autoridades han informado que existen mecanismos establecidos para facilitar el intercambio de información por parte de las empresas privadas, como los proveedores de Internet (ISP) o de servicios de correo electrónico, cuando existe una clara base legal y judicial para la investigación. La actual legislación relacionada con los delitos informáticos se aprobó en el año 2008 y ha permitido realizar investigaciones y procesamientos exitosos en varios casos de importancia.

No obstante, las autoridades indicaron que sus esfuerzos para hacer pleno uso de la ley al combatir los delitos cibernéticos han sido obstaculizados, en cierto modo, por los desafíos que surgen de la naturaleza de muchos delitos informáticos, que no tienen fronteras y están en constante evolución.

Las iniciativas lideradas por el gobierno para crear conciencia respecto a las diversas cuestiones y los desafíos relacionados con la seguridad cibernética se han centrado, en gran medida, en debates y conversaciones mantenidos en zonas densamente pobladas. A su vez, los esfuerzos a nivel de autoridades locales se han centrado en el desarrollo de centros de capacitación y unidades operativas equipadas correctamente.

El ICIC también ha desarrollado una iniciativa llamada “Internet Sano”, que apunta a promover el uso responsable de las TIC e Internet. Y la Dirección Nacional de Protección de Datos Personales, dependiente del Ministerio de Justicia y Derechos Humanos, ha desarrollado un segundo programa de concientización denominado “Contigo en la web”.

En la actualidad, varias instituciones de educación superior en Argentina ofrecen programas de certificación y de posgrado en una amplia variedad de aspectos relacionados con la seguridad cibernética, incluyendo el análisis forense digital.

Asimismo, el Instituto Nacional de Administración Pública (INAP) ofrece capacitación y cursos sobre temas relacionados con seguridad cibernética.

Aunque no se cuenta con registros detallados y cifras concretas disponibles para su distribución pública, se ha observado durante este último año un aumento en determinados delitos informáticos y otras actividades informáticas maliciosas, entre los que se incluyen:

- Suplantación de identidad y fraudes por medio de las redes sociales, el correo electrónico o la banca electrónica, mediante el uso de ingeniería social o keylogger (registrador de pulsaciones de teclas) y otro malware (programas maliciosos)
- Vandalismo de sitios web
- Amenazas persistentes avanzadas (APT)

Sin embargo, no existe información disponible que indique qué sector de la población ha sido el más afectado o perjudicado.

El Gobierno argentino se entrena de forma continua con el propósito de prepararse ante las amenazas cibernéticas emergentes.

Desde el 2012 se han llevado a cabo Ejercicios Nacionales de Respuesta a Incidentes Cibernéticos (ENRIC), los cuales se realizan de forma anual. En el 2014 se realizó un ejercicio conjuntamente por la ONTI/ICIC, el Ministerio de Defensa y la Armada Argentina.

Otros talleres sobre tecnologías emergentes de seguridad cibernética se llevan a cabo de forma regular para garantizar que los técnicos argentinos permanezcan al día sobre las últimas tendencias.

Se identificaron tres impedimentos principales y estos son: la falta constante de concientización entre las partes interesadas en todos los niveles, problemas y cuestiones relacionados con la privacidad, y financiación insuficiente.

5.2 Creación del Comité de Ciberseguridad

Con fecha 31 de julio del 2017 se publicó en el Boletín Oficial de la República Argentina la creación del Comité de Ciberseguridad, bajo la órbita de la Secretaría de Gobierno de Modernización (Ex-Ministerio de Modernización), y el cual estará integrado por representantes de la citada Secretaría, del Ministerio de Defensa y del Ministerio de Seguridad.

El Comité tendrá por objetivo la elaboración de la Estrategia Nacional de Ciberseguridad, punto de partida de una real política de ciberseguridad a nivel País.

A continuación, se citan las tareas del Comité, las cuales son referenciadas y citadas, como propuestas concretas, en las conclusiones del presente Trabajo Final de Especialización:

- a) Desarrollar la Estrategia Nacional de Ciberseguridad, en coordinación con las áreas competentes de la Administración Pública Nacional.

b) Elaborar el plan de acción necesario para la implementación de la Estrategia Nacional de Ciberseguridad.

c) Convocar a otros organismos para que participen en la implementación de medidas en el marco del plan de acción elaborado conforme lo establecido en el punto b) precedente.

d) Impulsar el dictado de un marco normativo en materia de Ciberseguridad.

e) Fijar los lineamientos y criterios para la definición, identificación y protección de las infraestructuras críticas nacionales.

f) Participar en el desarrollo de acciones inherentes a la Ciberseguridad nacional que se le encomienden.

5.3 Comparativa de la Estrategia de otros países

En esta inteligencia, a los efectos de comparar las estrategias nacionales de ciberseguridad adoptadas por otros países, se describe a continuación un breve resumen de las mismas:

5.3.1 Australia - Estrategia de Ciberseguridad de Australia (2016)

Coordinación de Políticas:

Asesor Especial del Primer Ministro en Ciberseguridad: lidera la aplicación de la Estrategia de Ciberseguridad y fomenta la creación y el fortalecimiento de asociaciones entre el gobierno australiano, el sector privado, las organizaciones no gubernamentales y el mundo académico para proporcionar capacidades nacionales en ciberseguridad.

Órganos Operacionales:

CERT Australia: principal punto de contacto para las cuestiones de ciberseguridad que afectan a las principales empresas australianas, incluidos los propietarios y operadores de la infraestructura crítica de Australia y otros sistemas de interés nacional.

Centro de Crimen de Alta Tecnología de Australia:
Responsable de investigar crímenes de tecnología.

5.3.2 Canadá - Estrategia de Ciberseguridad de Canadá (2010)

Coordinación de Políticas:

Seguridad Pública Canadá: coordina la implementación de la Estrategia

Órganos Operacionales:

Centro de Respuesta a Incidentes Cibernéticos (Seguridad Pública): punto focal para monitorear y brindar asesoramiento para mitigar las amenazas cibernéticas y dirigir la respuesta nacional.

Servicio Canadiense de Inteligencia de Seguridad: investiga las amenazas nacionales e internacionales.

Policía Montada Real de Canadá: investiga los actos delictivos contra redes canadienses e infraestructuras críticas.

Secretaría del Consejo del Tesoro: fortalecer las capacidades de gestión de incidentes cibernéticos mediante el desarrollo de políticas, normas y herramientas de evaluación; Responsable del Gobierno de Canadá IT.

5.3.3 Colombia - Política Nacional de Seguridad Digital (2016)

Coordinación de Políticas:

Coordinador nacional de seguridad digital: El coordinador nacional de seguridad digital tendrá a su cargo un equipo de apoyo operativo intersectorial, el cual estará conformado por representantes de, al menos, las siguientes entidades: Ministerio de Tecnologías de la Información y las Comunicaciones, Ministerio de Defensa Nacional y la Dirección Nacional de Inteligencia.

Órganos Operacionales:

Centro Cibernético Policial (CCP): responsable de garantizar la integridad de las redes policiales y de la sociedad civil.

Comando Conjunto Cibernético (CCOC) o el Comando Cibernético Conjunto: responde a ataques contra los activos militares de la nación.

ColCERT: Entidad de coordinación a nivel nacional que afronta todos los aspectos de la ciberseguridad y la ciberdefensa.

5.3.4 Estonia (alto índice de informatización y gobierno electrónico) - Estrategia de Ciberseguridad (2014–2017)

Coordinación de Políticas:

Consejo de Seguridad Cibernética del Comité de Seguridad del Gobierno de la República: apoyar la cooperación interinstitucional de nivel estratégico y supervisar la aplicación de los objetivos de la Estrategia de Seguridad Cibernética mediante el seguimiento del progreso de la implementación de los objetivos establecidos en el Plan de Implementación.

Órganos Operacionales:

Autoridad del Sistema de Información de Estonia (RIA): desarrollar estándares para la implementación de la seguridad de la información y supervisar su implementación, enfocándose principalmente en asegurar la ciberseguridad de los proveedores de servicios vitales.

Ministerio del Interior y el Ministerio de Asuntos Económicos y Comunicaciones: cooperar con otros ministerios responsables de los diferentes sectores de infraestructuras críticas para implementar medidas de seguridad.

CERT-EE: responsable de la gestión de incidentes de seguridad en redes informáticas

5.3.5 Los Países Bajos - Estrategia Nacional de Ciberseguridad (2013)

Coordinación de Políticas:

El Consejo de Seguridad Cibernética: proporciona asesoramiento solicitado y no solicitado al gobierno, y también tiene como tarea garantizar el cumplimiento de la Estrategia Nacional de Ciberseguridad.

Enviado Especial para la Ciberpolicía Internacional: con especial énfasis en un Internet libre, abierto y seguro, así como un ciberespacio seguro y estable.

Órganos Operacionales:

Centro Nacional de Seguridad Cibernética (CCSN): asesora a las partes privadas y públicas, tanto cuando se les solicita como por iniciativa propia, cuando se detectan vulnerabilidades importantes o en caso de situaciones de crisis (inminentes).

5.3.6 Estados Unidos - Estrategia de Ciberseguridad y Plan de Implementación 2015

Coordinación de Políticas:

Coordinador de Seguridad Cibernética de la Casa Blanca: responsable de coordinar todas las actividades de seguridad cibernética en todo el gobierno.

Órganos Operacionales:

Equipo Federal de Operaciones de Seguridad Cibernética de los Estados Unidos: Departamento de Justicia (DOJ) - Líder en investigación y aplicación de la ley.

Departamento de Estado (Departamento de Estado) - Oficina del Coordinador de Asuntos Cibernéticos: encargada de coordinar todo el espectro de cuestiones relacionadas con el ciberespacio, incluyendo la seguridad, las cuestiones económicas, la libertad de expresión y el libre flujo de información en Internet.

Departamento de Seguridad Nacional (DHS, por sus siglas en inglés): responsable por actividades centradas en cuestiones nacionales de ciberseguridad e interactuar con operadores privados de infraestructuras críticas y recursos claves del país. El DHS es la agencia federal responsable por coordinar los esfuerzos de infraestructura crítica.

Departamento de Defensa (DoD) – responsable por defender las redes, sistemas e información del Departamento de Defensa, defender el país contra ataques cibernéticos de impacto significativo, y por proporcionar apoyo cibernético a los planes operacionales militares.

5.3.7 España - Estrategia de Ciberseguridad Nacional (2013)

Coordinación de Políticas:

Consejo Nacional de Ciberseguridad: Es un órgano colegiado de apoyo al Consejo de Seguridad Nacional en su condición de Comisión Delegada del Gobierno para la Seguridad Nacional, en el marco de la Ley 50/1997, de 27 de noviembre, del Gobierno. El Consejo Nacional de Ciberseguridad se crea por Acuerdo del Consejo de Seguridad Nacional del 5 de diciembre de 2013.

Órganos Operacionales:

INCIBE: El Instituto Nacional de Ciberseguridad de España (INCIBE), 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.

Respuesta nacional a incidentes proporcionada por CNN-CERT and CERTSI (entre otros).

Como corolario de este capítulo podemos arribar a las siguientes estrategias para avanzar en Ciberseguridad, a nivel país:

- I. Enfoque Basado en el Riesgo: se recomienda abordar la ciberseguridad mediante un enfoque basado en el riesgo, en el cual se gestiona el riesgo, lo que significa que se reduce a un nivel aceptable de acuerdo con el contexto y los objetivos establecidos en la estrategia nacional. En tal sentido, es importante establecer las infraestructuras críticas del país, a modo de identificar sus vulnerabilidades.
- II. Gobernanza: es fundamental que la estrategia de ciberseguridad tenga un marco de gobernanza claro que defina las funciones y las responsabilidades de los distintos actores. El modelo de gobernanza

también debe proporcionar un marco para el diálogo entre los distintos actores y la coordinación de diversas actividades emprendidas en el ciclo de vida de la estrategia.

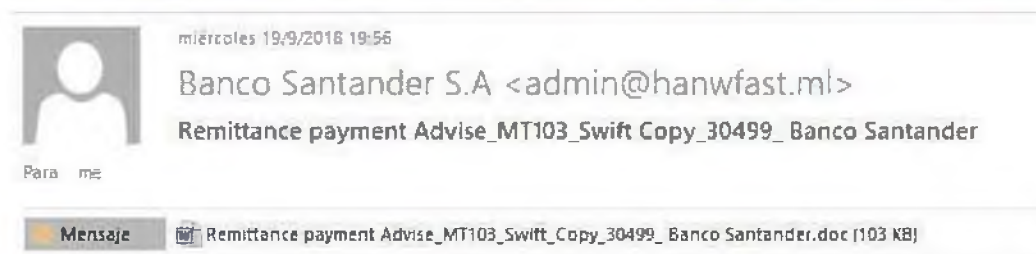
- III. Implementación (Plan de Acción): es recomendable definir acciones concretas, identificando explícitamente las entidades (o actores) responsables, un presupuesto estimado y el horizonte de tiempo para su ejecución.

Capítulo 6 - Contramedidas a difundir – “Evangelización”:

6.1 Simples medidas contra los ataques más implementados en la República Argentina durante 2016-2017

6.1.1 Phishing

No responder ningún mensaje que resulte sospechoso, ni hacer clic en los enlaces recibidos. Hay que concientizarse que el correo electrónico no es un medio seguro para enviar información personal o confidencial si no se emplea encriptación, conforme se desarrolla en las conclusiones del presente.



Greetings,

Please find attached the payment advice copy at maturity for your invoices that our client has paid to Santander Confirming.

Best regards,

Banco Santander SA, with head offices at 2-4 Pintor Sorolla Street, 46002 Valencia, will process your challenge your personal data by contacting us at e-mail at accionista@santander.com, or by post:

This is an automatic email auto, DO NOT REPLY. Any replies to this mail will be disregarded.

Ejemplos de phishing recibidos durante la elaboración del presente



miércoles 05/07/2017 06:38 a. m.

administrador del sistema <info@coesanet.com.ar>

advertencia

Para undisclosed-recipients:

Su buzón ha superado el límite de almacenamiento de [2.GB](#)
Establecido por el administrador esta actualmente 2,30 GB, no puede
enviar o recibir nuevos mensajes hasta que vuelva a validar su dirección de e-mail

Haga clic en el siguiente enlace para validar tu e-mail

<http://emailservice12301.tripod.com/servic/>

gracias
administrador del sistema



jueves 5/7/2018 11:14

Administrador de sistema

la advertencia de actualización de su cuenta

Para Recipientes

Querido Usuario

Nuestro registro indica que su cuenta no está actualizada, lo que puede llevar al cierre de su cuenta. Si n
para mejorar las Conversaciones, Contactos y Anexos.

Tómese un minuto para actualizar su cuenta y obtener una experiencia de correo más completa y rápida

Haga [clic aquí para](#) iniciar sesión / verificar cuenta.

Nota: El hecho de no actualizar su buzón dará lugar a la desactivación permanente de su cuenta.

Gracias,
El equipo de seguridad.

6.1.2 Ransomware

Siempre hay que verificar que el remitente sea conocido y que el
mensaje sea pertinente y razonable. Ante la mínima duda, se recomienda no
descargar el adjunto ni hacer clic en el enlace.

Si el mensaje parece provenir de una entidad con la que tenemos relación ya sea un banco, nuestro proveedor de correo electrónico, u otro, y nos indica hacer clic en un enlace para continuar una acción, **NO HACERLO**, por el contrario, ingresar directamente al sitio web del proveedor para buscar la información, **hacer el cambio de clave** o aquello que haya sido solicitado.

A partir de todo lo anterior, se desprende que la mejor acción es la prevención por parte de los usuarios para evitar ser víctima de un ataque y proteger la información en los dispositivos de este tipo de software malicioso.

Al igual que otros tipos de software malicioso como virus y troyano, entre otros, el ransomware se previene manteniendo las actualizaciones del sistema operativo con los parches de seguridad provistos por el proveedor, con un antivirus también actualizado y teniendo especial cuidado con los archivos adjuntos y/o enlaces en correos electrónicos, pero principalmente por la difusión constante (“evangelización”) de la cultura de la ciberseguridad, a todo el personal que maneje sistemas informáticos y cuentas de correo (en la actualidad, prácticamente todo el personal).

Política a difundir: Si bien es posible que se restituya el acceso a los archivos una vez pagado el rescate, hay que desalentar que la víctima acceda. Los cibercriminales pueden aun así dejar malware en el equipo y ahora saben que la víctima está dispuesta a pagar dinero, por lo que podría ser blanco de otro ataque. Además, hacer el pago motivaría a otros cibercriminales a continuar con este tipo de operaciones, y no hay garantía de que “cumplan su parte” del trato y realmente devuelvan los archivos.

6.1.3 Uso ilegal del Bitcoin

Varios países están emitiendo regulaciones al Bitcoin, adoptando mecanismos para evitar el lavado de dinero a través de esta vía.

Se estima que en poco tiempo dichas normas se estandarizaran, por lo cual es altamente conveniente adherirse como país a las mismas, en forma ejecutiva y eficiente.

En los Estados Unidos se estableció un control a los “cambiadores”, es decir, a las personas que reciben las monedas de uso en el mundo como el dólar o el euro por Bitcoin, exigiendo que estas personas estén registradas ante la autoridad competente.

Asimismo se exige que se cumpla que ese usuario anónimo tenga un registro al llenarse un formulario virtual con todos sus datos y, están obligados a llevar un reporte de actividades sospechosas. La regulación debería enfocarse en los ‘cambiadores’ (casas de cambio virtuales) para que en el momento en que una persona abra una cuenta, quede registrada. De esta manera, se puede hacer seguimiento a la ruta de actividades sospechosas al momento de iniciarse una investigación.

Alemania ha realizado esfuerzos en esta materia. Luego de reconocer al Bitcoin como una moneda, fijó un pago de impuesto, por lo que todos los registros que tenga una empresa por este tipo de operaciones deben ser reportados.

Canadá y Japón han adoptado ideas similares de protección a las EEUU y en Latinoamérica, México y Brasil también han establecido ciertas regulaciones.

El hecho de que el Bitcoin sea una “moneda transfronteriza” y de operación instantánea, hace difícil seguir la pista en caso de una investigación.

En resumen: el Bitcoin es una moneda digital que tiene las mismas características a la moneda física. Son transadas en Internet y tiene la bondad de que la transacción se realiza de inmediato. No tiene fronteras, la transacción se puede tardar 10 minutos, aproximadamente, y se puede hacer

desde cualquier parte del mundo y a cualquier hora. Se ejecuta a través de programas encriptados por lo que se hace difícil que la cadena de operación sea vulnerada.

6.1.4 Pasos para evitar el uso de Bitcoin en el lavado de dinero

“Los reguladores exigen que las operaciones con Bitcoin deben estar registradas ante la autoridad competente para así evitar el lavado de dinero”¹¹.

Para evitar que sean utilizadas en transacciones ilícitas, ya varios países han comenzado a adoptar normas que permitan disminuir este riesgo.

Las bondades y características de los Bitcoin, convierten las operaciones de estas monedas digitales en un alto riesgo para realizar operaciones vinculadas al lavado de dinero y demás operaciones características del crimen organizado.

El anonimato que existe en las operaciones mediante Bitcoin, es un elemento positivo porque ofrece seguridad para los participantes y obviamente existe el riesgo de aprovechar esta bondad para cometer lavado de dinero con la compra de bienes de alto valor como joyas y obras de arte e inclusive la compra-venta de droga.

6.1.5 BEC

Es altamente conveniente difundir simples instrucciones, creando las bases de una cultura de ciberseguridad, a todo integrante de los organismos estatales y público en general, sobre cómo evitar ser víctimas de estafas BEC y otros ataques similares.

Es importante saber que los ciberdelincuentes no se preocupan por el tamaño del objetivo ni necesitan ser altamente técnicos, ya que pueden

¹¹ José Antonio Gil - Asesoramiento financiero y estratégico. Corporate Finance. M&A (2016)

encontrar herramientas y servicios que atienden a todos los niveles de experiencia técnica en la deep web.

A medida que el mundo se basa cada vez más en los servicios web como el webmail, una única cuenta comprometida es todo lo que podría tomar para ingresar e interactuar en el Organismo atacado, con independencia del uso de la doble autenticación, que de hecho, desalienta y desbarata en gran medida estos tipos de ataques.

Capítulo 7 – Capítulo Final – Propuestas y Conclusiones

7.1 - Propuestas de Legislación y medidas tecnológicas, operativas y administrativas

Este Capítulo tiene como objetivo no sólo la elaboración de las conclusiones pertinentes sino, a manera de productividad, propuestas de diversas medidas de distinta índole como proyectos de legislación normativa específica, tendientes a elevar, aún más, el índice de Ciberseguridad de la República Argentina, que no se encuentra tan desprotegido como se podría llegar a prejuzgar partiendo de la base del desarrollo pendiente del mismo, especialmente en industria y tecnología,

Una de las razones de que ocurra esto es que globalidad tanto del ciberdelito como de las herramientas en seguridad informática para combatirlos, sumado el excelente nivel de profesionales con que cuenta el país.

En esta inteligencia, se describen a continuación las propuestas referidas y la conclusión final del presente trabajo.

7.1.1 Ciberpatrullaje Web Profunda (Deep Web)

Si bien la ley 27319, en los artículos 5 y 6 contempla la figura del agente revelador. Se estima imprescindible analizar jurídicamente, y en el caso de corresponder, ampliar el alcance con el objetivo de lograr un **Ciberpatrullaje de la web y especialmente de la Deep web**, pudiendo el personal de las Fuerzas de Seguridad Federales, intervenir y “participar” de la acción que se pretende anónima, como por ejemplo la compra de drogas peligrosas a través de la Deep web y pagando con Bitcoin (como ejemplo) con el fin de desbaratar la banda que se encuentra operando de esta manera.

Por otra en parte, tanto en virtud de los reiterados operativos exitosos contra el narcotráfico como por el avance de la tecnología, el comercio ilegal se desplazará y aumentará sobre dicha plataforma tecnológica, con lo cual

esta figura legal debería contarse con antelación al aumento de maniobras delictivas por la Deep Web.

7.1.2 Adhesión al Convenio de Budapest

A través de la aprobación del Convenio sobre Ciberdelito del Consejo de Europa (Convención de Budapest) se busca darle herramientas a la Justicia para investigar delitos en la web como la distribución de pornografía infantil, las infracciones vinculadas a la propiedad intelectual, los atentados contra la integridad del sistema hasta las estafas o los fraudes informáticos. El convenio sobre ciberdelito, aprobado el 23 de noviembre de 2001, consta de 48 artículos, y es el único instrumento internacional vigente sobre delitos informáticos y evidencia digital.

A dicho convenio mundial sobre ciberdelitos, ya adhirieron más de 50 países. El tratado busca consensuar las investigaciones de los delitos informáticos e impulsar la cooperación internacional.

Al comienzo de la elaboración del presente Trabajo Final, el Convenio de Budapest (Anexo II) encontraba a la espera que sea refrendado por la Cámara de Diputados, ya que la Cámara alta dio media sanción, a fines de abril del 2017, lo cual fue realizado por la dicha Cámara, con fecha 15 de diciembre de 2017 mediante la promulgación de la Ley 27.411.

Este es el único tratado de cooperación internacional vigente sobre esta materia y que desde el 2001 hasta la actualidad sumó la adhesión de países como España, Italia, Alemania, Francia, Portugal, Estados Unidos y Canadá, entre otros.

El proyecto aprobado marca los lineamientos procesales que habría que realizar a nivel nacional y provincial para que este pacto internacional constituya un paso fundamental en la lucha contra los delitos informáticos. También ayuda a mejorar la eficiencia del Estado en la investigación de delitos que requieren obtener evidencia digital alojada en países extranjeros,

situación cada vez más común en los casos de delincuencia transnacional y delitos complejos.

En los artículos 2 a 11¹² del proyecto se mencionan los tipos de “infracciones contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos”. Entre ellos se destaca el “acceso ilícito a un sistema cibernético, la interceptación dolosa y sin autorización, los atentados contra la integridad de los datos o del sistema en sí”, así como el “abuso de equipos e instrumentos técnicos” para cometer los delitos mencionados anteriormente. En tanto, penaliza según su derecho “interno” la estafa y la falsedad informática.

En lo que refiere a “infracciones” relativas a la “pornografía infantil” el proyecto lo deja sujeto a lo establecido en los códigos penales de cada país, así como la adecuación a lo que estipula el organismo mundial en cuanto a los delitos contra la propiedad intelectual. Mientas que en el artículo 11 explica los alcances penales para los “cómplices” de los ciberdelitos cuando sea considerada “dolosa” o con intención su actuación.

En cuanto al ámbito de aplicación del derecho procesal, es decir, como se realizará el procedimiento judicial necesario para el correcto juzgamiento de los causas, el convenio de Budapest manifiesta que se deberán “adoptar las medidas necesarias legislativas para instaurar los procedimientos y poderes a los efectos de la investigación o de los procedimientos penales mencionados en los artículo 2 a 11, a cualquier otra infracción penal cometida a través de un sistema informático o a la recopilación de las pruebas electrónicas de cualquier infracción penal”.

El artículo 16¹³ del acuerdo celebrado en Hungría hace 16 años, destaca que los países que firmaron su adhesión deberán realizar la

¹² ANEXO II

¹³ ANEXO II

“conservación inmediata de los datos informáticos almacenados”, para que “no sean objeto de pérdida o modificación”.

En esa línea, el Estado tiene el mandato para obligar y solicitarle al ciudadano que por 90 días tenga disponibles los datos para que las “autoridades competentes obtengan su comunicación”, según la legislación vigente y el respeto por las garantías individuales.

Así como el artículo 17 estipula, primero, la “conservación inmediata de los datos de tráfico cuando uno o más prestadores de servicio hayan participado de dicha comunicación” y, segundo, la de “asegurar la comunicación inmediata” de los datos de tráfico suficientes para “permitir la identificación de los prestadores del servicio y la vía” de comunicación. Así como su “recopilación en tiempo real”. El artículo 19 manifiesta la posibilidad de la “autoridades” sea el Poder Judicial y demás al “registro y decomiso de datos informáticos almacenados” y a un soporte de almacenamiento.

El convenio europeo de 2001 al que adhirió la Argentina establece que la cooperación internacional implicará la extradición de los implicados en los delitos mencionados y que tenga una pena prevista de una duración mínima de un año. Así como que en ambos Estados resulten punibles estos delitos on line.

En el caso de las medidas cautelares, se deberá disponer la “conservación inmediata de los datos almacenados en sistemas informáticos que se encuentren” en territorio argentino para su “fácil acceso” al país que los requiera.

En tanto, se deberá presentar una “demanda de conservación con los datos identificatorios” de la infracción que será objeto de investigación, así como de los datos informáticos almacenados que desean conservarse. Estos datos de tráfico, con excepciones de información netamente “política que podría poner en peligro su soberanía, seguridad, orden público u otro interés esencial”, debe ser “comunicada inmediatamente”.

7.1.3 Proyecto de Ley sobre Pornografía Infantil

Se estima conveniente elaborar un proyecto de ley de pocos artículos para el agregado en el Código Penal de la Nación de artículos que sancionen **la tenencia de pornografía infantil** (actualmente no penada) a los fines de complementar las acciones ya perseguidas, desalentando o, al menos, previniendo aquellas conductas más graves, desde su génesis. (***Promulgada mediante la ley 27.436 al momento de la finalización del presente trabajo***).

7.1.4 Explotación de Fuentes Abiertas

En los últimos años, la explosión de las redes sociales ha influido notablemente en el auge de la explotación de fuente abierta, al proporcionar una cantidad ingente de contenido generado por todas las personas, que a posteriori, se pueden estar dentro de una investigación penal, por tanto, se estima totalmente necesario que las Fuerzas de Seguridad Federales cuenten con las herramientas de explotación de fuentes abiertas. A tal efecto, se consideran abiertas fuentes de información tan diferentes como la web o cualquier un repositorio de información.

El principal objetivo de la explotación de fuente abierta es reducir el tiempo de investigación y los recursos volcados a la misma, construir líneas de tiempo con aplicación en investigaciones complejas (líneas de tiempo hacia atrás, cómo sucedieron las cosas) y con quienes estuvo conectado el victimario y/o la víctima de un delito (cualquier tipo de delito con o sin el uso de tecnologías).

Si bien, con dicha herramienta se consigue con informaciones no clasificadas (abiertas al público), su difusión debe ser segura ya que su verdadero valor radica en el producto obtenido al comparar y clasificar una cantidad impresionante de datos en poco tiempo.

Habiendo que el mercado existen diversas herramientas, hemos detectado que muchas de las mismas se han realizado por emprendimientos

de programadores, con poca capacidad para el manejo de grandes datos de información como lo requiere la seguridad pública e investigaciones judiciales, con lo cual es aconsejable evaluar productos de firmas que específicamente se dediquen a este segmento específico de la ciberseguridad.

7.1.5 Registro por parte de las prestadoras de Telefonía Celular GSM, de la Señalización (especialmente afiliación) de los aparatos celulares a cada celda.

Como introducción, debe tenerse en cuenta que los sistemas de telefonía celular, más precisamente su infraestructura a través de las celdas, poseen una comunicación fluida con los terminales móviles, que excede las llamadas, mediante el canal de control de cada celda.

Además del uso para llamadas del espectro, reservando para ello los canales precisos mientras se estén usando, el estándar GSM prevé que el terminal envíe y reciba datos para una serie de usos de señalización, como por ejemplo el registro inicial en la red al encender el terminal, la salida de la red al apagarlo, el canal en que va a establecerse la comunicación si entra o sale una llamada, la información del número de la llamada entrante.

Asimismo, prevé además que cada cierto tiempo el terminal avise a la red de que se encuentra encendido para optimizar el uso del espectro y no reservar capacidad para terminales apagados o fuera de cobertura (esto se denomina el estado de afiliación, el cual ocupa muy poco "peso" de información, unas decenas de bytes)

Este uso de señalización ocupa muy poca capacidad de red y se utiliza también para enviar y recibir los mensajes cortos SMS sin necesidad de asignar un canal de radio. Es sencillo escuchar una ráfaga de señalización si el teléfono se encuentra cerca de un aparato susceptible de captar interferencias, como un aparato de radio, televisión, un aparato telefónico de línea o inclusive un parlante de computador, (suena como una ráfaga

intermitente) y el terminal celular aparentemente no está haciendo nada (ninguna llamada y ni siquiera enciende su pantalla).

En GSM se definen una serie de canales para establecer la comunicación, que agrupan la información a transmitir entre la estación base y el teléfono. Se definen los siguientes tipos de canal:

- *Canales de tráfico (Traffic Channels, TCH): albergan las llamadas en proceso que soporta la estación base.*
- *Canales de control o señalización:*
- *Canales de difusión (Broadcast Channels, BCH).*
- *Canal de control broadcast (Broadcast Control Channel, BCCH): comunica desde la estación base al móvil la información básica y los parámetros del sistema.*
- *Canal de control de frecuencia (Frequency Control Channel, FCCH): comunica al móvil (desde la BS) la frecuencia portadora de la estación base -celda-.*
- *Canal de control de sincronismo (Synchronization Control Channel, SCCH): informa al móvil sobre la secuencia de entrenamiento (training) vigente en la estación base, para que el móvil la incorpore a sus ráfagas.*
- *Canales de control dedicado (Dedicated Control Channels, DCCH).*
- *Canal de control asociado lento (Slow Associated Control Channel, SACCH).*
- *Canal de control asociado rápido (Fast Associated Control Channel, FACCH).*
- *Canal de control dedicado entre estación base y móvil (Stand-Alone Dedicated Control Channel, SDCCH).*
- *Canales de control común (Common Control Channels, CCCH).*
- *Canal de aviso de llamadas (Paging Channel, PCH): permite a la estación base avisar al móvil de que hay una llamada entrante hacia el terminal.*
- *Canal de acceso aleatorio (Random Access Channel, RACH): alberga las peticiones de acceso a la red del móvil a la estación base -celda-.*

- *Canal de reconocimiento de acceso (Access-Grant Channel, AGCH): procesa la aceptación, o no, de la estación base -celda- de la petición de acceso del móvil.*
- *Canales de Difusión Celular (Cell Broadcast Channels, CBC).*

7.1.5.1 Utilización

Se estima de fundamental importancia, a la hora de investigar un delito grave. Por ejemplo, en el caso del homicidio de una joven en la Ciudad de Buenos Aires, años atrás, que si bien, a la fecha, se encuentra esclarecido, se podría haber determinado más rápidamente o incluso detectar complicidad o encubrimiento, ya que en el lugar donde fue arrojado el cuaderno de la víctima con posterioridad al hecho, no existían cámaras disponibles (o no fueron encontradas por falta de registro de los sistemas –siguiente punto-) y las actividades de las CELDAS de TELEFONÍA CELULAR no se registran, es decir, si los teléfonos investigados no realizaron o recibieron una llamada, pueden haber estado en la zona del hecho sin que quede registrada esa información, que sí existió.

Un caso distinto es si el teléfono celular es investigado e intervenido judicialmente, a partir de ese momento se podría solicitar a las prestadoras ese tipo de información, pero también es un tema tecnológico y de inversión de cada prestadora.

En resumen, que un Fiscal o un Juez puedan solicitar el dato “crudo” de las afiliaciones de teléfonos celulares por las celdas de interés, y luego filtrarse los teléfonos investigados, es como “volver el tiempo atrás” y obtener datos muy valiosos de donde estuvo cada celular investigado o si estuvieron en el lugar del hecho o en camino con los horarios, ya que también se pueden concluir –a grandes rasgos- sus trayectos, siempre que esté encendido (sin hacer llamados, porque en este caso sí se registra todo, dado que lo tienen que facturar).

Las prestadoras pueden esgrimir que en celdas urbanas son millones de registros y si bien es así, son millones de registros de muy poco tamaño,

los cuales, con la tecnología de “storage” (almacenamiento) actual, pueden registrarse.

Otra objeción, la privacidad, deviene en abstracto, en virtud que esto ya ocurre con el registro de llamados (los cuales quedan registrados pero hasta que una autoridad judicial no lo solicita solo están en poder de la prestadora, por el término que fija una ley, hoy suspendida –ANEXO III-)

7.2 Propuestas Legislativas

7.2.1 Reformulación de la Ley 25.873 (El cual consta como Anexo III)

A los efectos de subsanar los vicios de inconstitucionalidad que pudiera tener, ya que el espíritu de la misma otorgaba herramientas técnico-administrativas con el fin de salvaguardar la vida de las personas.

Dicha ley fue reglamentada por el Decreto 1573/2004 y luego fue suspendida su aplicación mediante mismo instrumento, Decreto 357/2005.

Transcurridos unos 14 años de la promulgación de la ley, 13 del decreto reglamentario y 12 del decreto que suspendía el anterior, con el ritmo de la evolución tecnológica, esta falta de normativa tiene alto impacto en la Ciberseguridad y el Cibercrimen en virtud de la convergencia de los smartphones y su amplia conectividad.

Actualmente, los casos y las medidas quedan a criterio de los magistrados y fiscales intervinientes, generando una disparidad de medidas y resultados en la utilización de las herramientas tecnológicas y la información obrante en las compañías prestadoras, para afrontar los delitos cometidos y en muchos de los casos salvaguardar la vida de las personas (como cuando ocurre una privación ilegítima de la libertad, es decir, los secuestros)

7.3 Propuestas Tecnológicas-Operativas

Se propone, independientemente de la utilización de doble autenticación, la adopción de Programas Criptográficos para la encriptación -

protección- de **correos electrónicos oficiales**, reservados y confidenciales y toda documentación sensible. De esta manera se evita filtración de información y los daños que conlleva tal penetración, cuando el phishing sea exitoso, **ya que siempre existe el factor humano**, que puede ser víctima de engaños en su buena fe.

Asimismo, esta protección se podrá adquirir a nivel internacional pero habida cuenta lo sensible del tema y que contempla información estratégica nacional, se puede encarar un desarrollo nacional y/o implementación local, para lo cual nuestro país cuenta con expertos a nivel internacional de primera línea como por ejemplo, el Dr. Hugo Scolnik y el Dr. Pedro Hecht.

7.3.1 Encriptación de las comunicaciones gubernamentales

Como se citó, en el Capítulo 2, la interceptación ilegal de celulares GSM hoy es posible y realizable con relativamente bajo costo.

Tal como lo hacen algunos países más avanzados tecnológicamente, se debería proporcionar, al menos, a los miembros del gabinete nacional de celulares específicos con Criptografía por Hardware y protocolos robustos que no estén debilitados a la fecha, como por ejemplo el protocolo de encriptación AES 256 bits. De esta manera se evita la “intercepción por celda falsa” (ver “IMSI Catcher”).

También podrá estudiarse una encriptación por software, si el desarrollo es nacional, no obstante, todos los desarrollos de software implican llamadas de **VoIP** (Voz sobre IP), es decir, llamadas realizadas a través de la transmisión de datos y no a través del sistema **GSM** -celular propiamente dicho- siendo la llamada de este tipo más usual aquella que se realizan por **Whatsapp, Telegram**, etc.

7.4 Diseño de nuevas políticas

Estudio de implementación de la Firma Digital para todos los correos oficiales de los tres poderes de la República y, en una segunda etapa, ejecutar la encriptación del contenido de dichos correos electrónicos.

7.4.1 Propuestas de implementación de Políticas Públicas en Ciberseguridad

Implementación de una Política Nacional de Ciberseguridad, a través de:

- Puesta en marcha inmediata del Comité de Ciberseguridad
- Alcance de la Estrategia Nacional de Ciberseguridad

Se estima muy conveniente definir el alcance de la estrategia nacional de ciberseguridad no sólo en términos de contenido, sino también de actores impactados.

En caso de ser un documento será una estrategia para el ciberespacio, ciberseguridad o mismo la seguridad de la información. Además, la estrategia enfoca en el gobierno Nacional/Federal, y poco se discute sobre el rol de los gobiernos locales.

7.5 Creación de Capacidades y Propuestas Formativas

En nuestro país, existen las siguientes carreras de posgrado relacionadas o directamente abocadas a la Seguridad Informática:

7.5.1 Universidad de Buenos Aires

Organizado en forma conjunta por las facultades de Ciencias Económicas, Ciencias Exactas y Naturales e Ingeniería de la Universidad de Buenos Aires.

ESPECIALISTA Y MAGÍSTER EN SEGURIDAD INFORMÁTICA de la Universidad de Buenos Aires.

7.5.2 Universidad de la Defensa Nacional (UNDEF)

Facultad de Ingeniería del Ejército

ESPECIALIZACIÓN EN CRIPTOGRAFÍA Y SEGURIDAD
TELEINFORMÁTICA

7.5.3 Instituto Universitario de la Policía Federal Argentina

Se dicta la Licenciatura en SEGURIDAD EN TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES, siendo actualmente la única carrera de grado que se ocupa de la Seguridad Informática, Electrónica y de Telecomunicaciones.

La primera cohorte (2014) se encuentra en la realización de su Tesina, y las cohortes 2016 y 2017 cuentan con alumnos tanto de la comunidad como de las fuerzas de seguridad y policiales.

Sus características y fundamentación se encuentran adjuntos en el ANEXO VI. El hecho de contar con una carrera de grado (casi inexistentes en Latinoamérica) ha subido el puntaje del índice de Ciberseguridad que lleva adelante la OEA, conforme lo plasmado en el presente en el punto Indicadores Internacionales (Pág. 26).

En pleno proyecto de elaboración se encuentra la carrera de TÉCNICO UNIVERSITARIO EN INFORMATICA FORENSE, con el objetivo de dictarse también en el Instituto Universitario de la Policía Federal Argentina, con el objetivo de formar no solo peritos sino especialistas en la investigación informática para suplir las necesidades actuales de estos profesionales.

7.6 Conclusiones Finales

Por todo lo expuesto, se arriba a una conclusión que es contraria a la percepción que se tenía sobre la situación de nuestro país no era tan favorable con relación al nivel de Ciberseguridad.

El fiel reflejo es que en el índice de Ciberseguridad que lleva adelante la OEA, la posición de Argentina es elevada, y teniendo en cuenta que es uno de los pocos países que cuenta con carrera de grado en seguridad en tecnologías de la información y comunicaciones, lo que también contribuye a la calificación.

Si bien organismos públicos y fuerzas de seguridad fueron víctimas de ciberataques, siempre fueron aprovechando que aún no se implementaron en forma total las políticas de seguridad de la información ni nos hemos concientizado plenamente sobre la “cultura de la ciberseguridad” (sencillamente podemos decir que nadie deja las llaves puestas de su casa del lado de afuera de la puerta o dejar abierto un automóvil, situaciones que sí ocurren todavía a nivel informático, por falta de información e instrucción específica).

No obstante, lo expuesto, si tenemos en cuenta que el propio comité de campaña del partido demócrata, de los Estados Unidos, fue ciberatacado con éxito y con herramientas básicas de phishing, y aún están evaluando el daño alcanzado a la elección presidencial de dicho país, no podemos concluir rápidamente que estamos a fojas cero, si bien, no estamos en una posición fuerte, la tendencia es exponencialmente favorable a alcanzarla.

El presente trabajo final refleja que tanto la infraestructura, la legislación y especialmente los recursos humanos no se encuentran tan atrás en el marco global de este flagelo de las últimas décadas: el ciberdelito y sus derivaciones.

Si se detectó, que se carece de una efectiva articulación entre todos los actores y organismos de base inherentes a la Ciberseguridad de nuestro país, como el faltante de una legislación más específica y la implementación de medidas tecnológicas y administrativas, cuyas correcciones y articulaciones se pretendieron proponer con la elaboración del presente Trabajo Final de Especialización.

Glosario:

CSA (Cloud Security Alliance)

CHFI (Consejo de la CE)

PCIP/CCISP (Critical Infrastructure Institute)

LPC (Loss Prevention Institute)

CFE (Association of Certified Fraud Examiners)

CITRMS (Institute of Consumer Financial Education),

CSFA (Cybersecurity Institute),

CCSA (Institute of Internal Auditors)

PMP (Project Management Institute)

ICIC (Infraestructuras Críticas de Información y Ciberseguridad)

ONTI (Oficina Nacional de Tecnologías de la Información)

CERT (Equipo de Respuesta ante Emergencias Informáticas)

CIRT (Equipo de Respuesta ante Incidentes Informáticos), CERT

CSIRT (Equipo de Respuesta ante Incidentes de Seguridad Informática)

P2P (Peer to Peer)

ONU (Organización de las Naciones Unidas)

UIT (Unión Internacional de Telecomunicaciones)

BDT (Oficina de Desarrollo de las Telecomunicaciones – UIT)

CMSI (Cumbre Mundial sobre la Sociedad de la Información)

GSA (Agenda sobre Ciberseguridad Global)

UE (Unión Europea)

IMC (Índice Mundial de Ciberseguridad)

Bibliografía consultada y referenciada en el presente trabajo

<http://www.redseguridad.com/actualidad/info-tic/los-10-principales-incidentes-de-ciberseguridad-en-2016>

<http://www.vocesporlajusticia.gob.ar/avance-la-adhesion-argentina-convenio-cibercrimen/>

<http://ist-technet.blogspot.com/2017/04/el-senado-acaba-de-darle-media-sancion.html>

<https://haddensecurity.wordpress.com/2014/07/29/bitcoin-funcionamiento-y-aspectos-destacables/>

http://www.publiz.es/blog/961_Incidentes-de-ciberseguridad-en-2016.html

<http://www.lanuevacronica.com/incibe-enumera-los-principales-incidentes-de-ciberseguridad-a-nivel-mundial>

<http://www.ejercitos.org/2017/02/13/incibe-publica-ranking-los-10-principales-incidentes-ciberseguridad-nivel-mundial-2016/>

<https://haddensecurity.wordpress.com/category/economia-2/page/2/>

<http://lawyerpress.com/2017/02/13/incibe-publica-el-ranking-de-los-10-principales-incidentes-de-ciberseguridad-a-nivel-mundial-de-2016/>

<http://cso.computerworld.es/actualidad/ranking-de-los-10-principales-incidentes-de-ciberseguridad-en-2016>

<http://www.taringa.net/posts/info/17009788/Navega-sin-dejar-rastros.html>

http://www.uv.mx/infosegura/general/conocimientos_tor/

<http://www.taringa.net/comunidades/chapines/8109970/Info-Que-es-Tor-y-como-funciona.html>

<http://noticiasdehacking.com/2017/07/11/una-tecnologia-politica-que-crece-al-margen-del-mercado-noticias-hacking/>

<https://haddensecurity.wordpress.com/tag/inteco/>

<https://noticias.eset.es/aggregator/sources/1>

<https://laopinion.com/2016/12/17/como-fue-el-hackeo-de-ciberpiratas-de-rusia-en-las-elecciones-de-eeuu/>

<https://haddensecurity.wordpress.com/tag/silk-road/>

<http://jsk-sde.blogspot.com/2016/12/el-phishing-tras-uno-de-los-mayores.html>

<http://notihoy.com/como-fue-el-hackeo-de-los-rusos-durante-las-elecciones-de-ee-uu/>

<http://www.animalpolitico.com/2016/12/hackeo-rusia-elecciones-eu/>
<http://reyquirarezas.blogspot.com/2017/02/ranking-de-los-10-principales.html>
<http://jaquematweb.com/confirmado-los-rusos-si-hackearon-elecciones-presidenciales-de-eeuu/>
<https://haddensecurity.wordpress.com/2017/01/13/como-fue-el-hackeo-de-piratas-informaticos-de-rusia-durante-las-elecciones-de-eeuu/>
<http://www.lostiempos.com/oh/actualidad/20170116/hackers-rusos-votaron-trump>
<http://www.seguritecnia.es/actualidad/al-dia/los-10-principales-incidentes-de-ciberseguridad-en-2016>
<http://www.negocioscastillayleon.com/el-robo-de-81-millones-de-dolares-al-banco-central-de-banglades-lidera-el-ranking-mundial-de-los-incidentes-de-ciberseguridad/>
<http://www.taringa.net/posts/info/17043696/Borra-tu-identidad-con-un-click-Conexion-anonima.html>
<https://noticiasdehoy.co/una-tecnologia-politica-que-crece-al-margen-del-mercado/>
<https://juanmaperezmicroinformatica.wordpress.com/2016/01/21/programas-de-interes-informatico/>
<http://defensanacional.argentinaforo.net/t4847-ciberespacio-hipotesis-de-conflicto>
<http://www.entornointeligente.com/articulo/10255556/ARGENTINA-Una-tecnologia-politica-que-crece-al-margen-del-mercado-09072017>
<http://wtcradio.net/blockchain-una-tecnologia-politica-crece-al-margen-del-mercado/>
<http://www.chismesmundo.com/que-es-tor-y-como-funciona/>
<https://nic.ar/Enterate/Noticias/como-evitar-ransomware>
<https://sistemasayala.wordpress.com/2017/03/01/los-diez-principales-incidentes-en-ciberseguridad-de-2016-sistemas-ayala/>
<http://www.hoylosangeles.com/noticias/estadosunidos/hoyla-eeuu-como-fue-el-hackeo-de-piratas-informaticos-de-rusia-durante-las-elecciones-de-estados-unidos-20161229-story.html>
<https://www.softonic.com/articulos/que-es-tor-uso-seguridad-y-alternativas>
<http://www.bbc.com/mundo/noticias-internacional-38350244>

https://es.wikipedia.org/wiki/Sistema_global_para_las_comunicaciones_m%C3%B3viles

<https://www.efe.com/efe/castillayleon/tecnologias/un-robo-al-banco-central-banglades-principal-incidente-ciberseguridad-en-2016/50000476-3177893>

<https://www.pablofain.com/como-funciona-la-red-gsm/>

<http://www.elsalvador.com/entretenimiento/tecnologia/349940/wannacry-un-robo-cibernetico/>

<https://empresas.eset-la.com/archivos/novedades/34/ESET-Ransomware-final.pdf>

<http://liacolombia.com/2016/10/ransomware-que-es-como-funciona-y-como-protegerse/>

<https://es.slideshare.net/ESETLA/infografa-ransomware>

<https://blogs.protegerse.com/2017/07/21/que-esta-pasando-con-las-criptomonedas-incidentes-recientes-con-ethereum-y-el-futuro-de-bitcoin/>

<http://www.esacademic.com/dic.nsf/eswiki/513084>

http://www.tecnonews.info/noticias/diez_principales_incidentes_de_ciberseguridad_producidos_en_2016

<http://conocimientoswirelessnetworkdesign.blogspot.com/2011/03/>

<https://www.incibe.es/sala-prensa/notas-prensa/incibe-publica-el-ranking-los-10-principales-incidentes-ciberseguridad>

<https://www.kaspersky.es/blog/que-es-un-botnet/755/>

<http://www.efefuturo.com/noticia/peores-ciberdelitos-2016/>

<http://noticiasseguridad.com/seguridad-informatica/que-esta-pasando-con-las-criptomonedas-incidentes-recientes-con-ethereum-y-el-futuro-de-bitcoin/>

<https://articulosblog.wordpress.com/2013/11/20/que-es-tor-y-como-funciona/>

<http://www.lanacion.com.ar/2040823-una-tecnologia-politica-que-crece-al-margen-del-mercado>

<http://estandaresdetelefoniamovil.blogspot.com/2007/03/canales-lgicos-gsm.html>

<https://seguridadeinformaticabrm.wordpress.com/2017/03/08/botnet/>

<http://www.lavanguardia.com/vida/20170213/414294473364/un-robo-al-banco-central-bangladesprincipal-incidente-ciberseguridad-en-2016.html>

<https://www.scribd.com/document/39399415/SENALIZACION-GSM>

http://mp3killdownload.com/mp3/Tpb_FChZP5l2/nos-conocemos-protecci%C3%B3n-de-meno.html

http://www.youtube.com/watch?v=Tpb_FChZP5l

<https://es-us.noticias.yahoo.com/tecnolog%C3%ADa-pol%C3%ADtica-crece-margen-mercado-000000336.html>

<https://www.certs.es/blog/bitcoin-funcionamiento>

<https://cienciaytecnologia.wordpress.com/category/amenazas-informaticas/>

<https://www.diariolibre.com/ciencia-y-tecnologia/tecnologia/los-ciberdelitos-en-el-2016-causaron-perdidas-por-miles-de-millones-dolares-CJ6281756>

http://www.economiadigital.es/redirect/mayores-ciberataques-2016_188964_102.html

<https://avidaecambiosite.wordpress.com/tag/botnet/>

<https://sistemasayala.wordpress.com/tag/internet/>

https://es.wikipedia.org/wiki/WannaCry_ransomware_attack

<http://www.spiquers.com/sebastian-campanario-fenomeno-blockchain-la-red-transacciones-online/>

<https://www.scribd.com/presentation/294255262/GSM>

<https://www.slideshare.net/ObservatorioCCD/informe-final-seguridad-en-las-comunicaciones>

<http://www.lanacion.com.ar/1987882-confianza-ciega-el-codigo-magico-que-enamora-a-los-innovadores>

<http://www.periodismo.com/link/blockchain-una-tecnologia-politica-que-crece-al-margen-del-mercado/>

<http://www.redgealc.net/arcert/contenido/4371/es/>

<http://www.sisonline.com/noticias/noticias.asp?id=8065>

<http://elcomercio.pe/mundo/actualidad/bbc-hackeo-ruso-elecciones-ee-uu-230395>

<https://es.wikipedia.org/wiki/Botnet>

<http://estandaresdetelefoniamovil.blogspot.com/>

https://es.wikipedia.org/wiki/Ataque_inform%C3%A1tico

http://www.oas.org/juridico/PDFs/arg_ley25326.pdf

<http://www.ambito.com/891870-el-gobierno-creo-un-comite-de-ciberseguridad>

<http://seguridadinformaticabancaria2.blogspot.com.es/>

<http://redgealc.org/arcert/contenido/4371/es/>

https://www.economiadigital.es/tecnologia-y-tendencias/los-diez-mayores-ataques-informaticos-de-2016_188964_102.html

<https://prezi.com/lzjqjbxpmnrd/gsm/>

<https://vidateleco.wordpress.com/2009/02/25/canales-y-tramas-de-las-comunicaciones-moviles-parte-1/>

http://www.academia.edu/29197062/ESTRUCTURAS_DE_CANAL_F%C3%8DSICO_Y_L%C3%93GICO

<https://prezi.com/wtrq3rz8wrn9/tecnologias-atm-y-gsm/>

<http://enlaces.lasindias.com/bookmarks.php/caro/criptomonedas>

<https://prezi.com/vgqyefwpsrpy/tipos-de-malware/>

<http://www.dsn.gob.es/es/sistema-seguridad-nacional/comit%C3%A9-especializados/consejo-nacional-seguridad-mar%C3%ADtima>

<http://www.antilavadodedinero.com/antilavadodedinero-entrevistas-articulo.php?id=427&title=pasos-para-evitar-el-uso-de-bitcoin-en-el-lavado-de-dinero>

<https://www.fiuxy.co/programas-gratis/3476338-tor-browser-3-5-3-proteja-su-privacidad-vigilancia-de-la-red-y-analisis-de-trafico-esp.html>

<http://rockaprend.blogspot.com/2013/08/que-es-tor-y-como-te-anonimiza.html>

<https://tlaxcala2011.blogspot.com/2016/12/como-fue-el-hackeo-de-piratas.html#!>

http://www.abc.es/espana/castilla-leon/abci-diez-principales-incidentes-ciberseguridad-2016-201702131420_noticia.html

<http://blog.gonetfpi.com/2017/02/>

<https://www.slideshare.net/cxocommunity/viagragobar-un-asunto-de-seguridad-nacional>

<https://www.fiuxy.co/programas-gratis/3129843-descargar-tor-navega-anonimamente-gratis.html>

<http://elestimulo.com/elinteres/paises-ya-adoptan-normas-para-evitar-el-uso-de-bitcoin-en-lavado-de-dinero/>

<http://www.laprensa.com.ni/2016/12/17/internacionales/2152213-como-fue-el-hackeo-de-piratas-informaticos-de-rusia-durante-las-elecciones-de-estados-unidos>

https://www.unrc.edu.ar/unrc/uti/pdfs/recomendaciones_phishing.pdf
<https://www.facebook.com/Cybernex-818236584918226/>
<http://lizbethlunaadministracion1b.blogspot.com/2011/10/bonet.html>
<https://softwareonfire.wordpress.com/2013/08/04/que-es-tor-y-como-funciona/>
<https://www.slideshare.net/santiagolimonche/informe-de-inteco-sobre-el-bitcoin>
<https://es.slideshare.net/santiagolimonche/informe-de-inteco-sobre-el-bitcoin>
<http://www.youtube.com/watch?v=GHTq3RzQcKw>
<http://tarcoteca.blogspot.com/2016/08/seguridad-para-telefonía-móvil.html>
<http://www.tic.siteal.iipe.unesco.org/políticas/861/programa-nacional-de-infraestructuras-críticas-de-información-y-ciberseguridad>
<http://www.informaticalegal.com.ar/2011/08/02/argentina-crea-programa-nacional-de-infraestructuras-críticas-de-información-y-ciberseguridad/>
http://www.belt.es/noticiasmdb/HOME2_noticias.asp?id=14681
<http://www.dsn.gob.es/es/sistema-seguridad-nacional/comit%C3%A9-especializados/consejo-nacional-ciberseguridad>
<http://www.ituser.es/actualidad/2017/02/cuales-fueron-los-principales-incidentes-de-ciberseguridad-de-2016>
<http://opensources.info/estos-fueron-los-10-principales-incidentes-de-ciberseguridad-en-2016/>
<https://habeasdatacpdp.wordpress.com/tag/proteccion-de-datos-personales/page/9/>
<https://es.m.wikipedia.org/wiki/Botnet>
https://es.wikipedia.org/wiki/Ataque_de_denegaci%C3%B3n_de_servicio
<http://mutualdepetroleros.com/LEY-25326.pdf>
<https://www.slideshare.net/ESETLA/infografa-ransomware>
<http://eleconomista.com.mx/sociedad/2017/08/19/asi-perfila-oea-coordinador-estrategia-nacional-ciberseguridad>
<https://www.g2khosting.com/blog/que-es-blockchain/>
<https://seguridadenlared404blog.wordpress.com/category/amenazas-de-la-seguridad/>
<https://seguridadenlared404blog.wordpress.com/2017/03/08/botnet/>

<http://servicios.infoleg.gob.ar/infolegInternet/anexos/185000-189999/187698/norma.htm>
<https://pablobenblog.wordpress.com/2017/03/08/botnets/>
<http://www.msn.com/es-ar/noticias/otras/el-gobierno-cre%C3%B3-un-comit%C3%A9-para-elaborar-una-estrategia-de-ciberseguridad/ar-AAp8J6P>
<http://www.icic.gob.ar/>
<https://www.taringa.net/posts/info/18861343/Que-es-una-Botnet.html>
<http://www.ticbeat.com/seguridad/que-es-un-botnet-y-como-evitar-caer-en-uno/>
<http://www.enterbyte.com.ar/2016/04/>
<http://www.enterbyte.com.ar/category/seguridad/>
<https://julietatic2d.wordpress.com/2017/03/08/botnet/>
https://es.wikipedia.org/wiki/Ataques_ransomware_WannaCry

ANEXOS

ANEXO I

Decreto 577/2017 – creación del Comité de Ciberseguridad.

ANEXO II

Convenio De Budapest

ANEXO III

Ley 25.783

ANEXO IV

Carrera Licenciatura en Seguridad en Tecnologías de la Información y Comunicaciones

ANEXO V

Ley 25.326 - PROTECCION DE LOS DATOS PERSONALES

ANEXO VI

Ley 25.506 - FIRMA DIGITAL

ANEXO VII

Ley 25.520 - LEY DE INTELIGENCIA NACIONAL.

ANEXO VIII

Ley 26.388 – Modificación del CÓDIGO PENAL a fin de incorporar los “Delitos Informáticos”.

ANEXO IX

Ley 26.904 - Modificación del CÓDIGO PENAL a fin de incorporar el Ciber-acoso o “Grooming”.

ANEXO X

Ley 27.078 – LEY DE ARGENTINA DIGITAL

ANEXO XI

Ley 27.126 - AGENCIA FEDERAL DE INTELIGENCIA. Creación. Ley N° 25.520. Modificación.

ANEXO XII

Decreto 256/2015 - CORTE SUPREMA DE JUSTICIA DE LA NACIÓN. Transfiérase el Departamento de Interceptación y Captación de las Comunicaciones.