Universidad de Buenos Aires
Facultad de Ciencias Económicas
Escuela de Estudios de Posgrado

Universidad de Buenos Aires
Facultad de Ciencias Económicas
Escuela de Estudios de Posgrado

CARRERA DE ESPECIALIZACIÓN EN INTELIGENCIA ESTRATÉGICA Y CRIMEN ORGANIZADO

TRABAJO FINAL DE ESPECIALIZACIÓN

Impacto de la Ingeniería Social en Argentina a partir de la Pandemia producida por COVID-19

AUTOR: MIGUEL ANTIN

DOCENTE DEL TALLER: JOSÉ LUIS PIBERNUS

[MARZO 2022]

Resumen

El presente trabajo tiene como propósito analizar las metodologías y los alcances de la ingeniería social en Argentina a partir de los ataques dirigidos a organizaciones estatales en pandemia, producida por el Covid-19.

La investigación deja en evidencia la importancia de los distintos métodos utilizados por los cibercriminales para atacar personas u organizaciones. Ya sea con técnicas basadas en el engaño humano o técnicas basadas en la utilización de tecnología. El advenimiento de la pandemia arrojo un crecimiento exponencial en ciberataques y con ello la propagación de nuevas amenazas.

El estudio y la comprensión de la ingeniería social muestra un complejo abanico de posibilidades y vectores de ataque prevenibles para las personas y sus respectivas organizaciones. Es ahí donde se une el conocimiento sobre ciencia, tecnología, comportamiento humano y mucho más transformando, según los especialistas, a la actividad en un arte.

La ejecución de las metodologías en diferentes ámbitos ya sean físico o en el ciberespacio son material necesario para los analistas de inteligencia que trabajen en mesas conjuntas de cibercrimen. Aplica en las fuerzas de seguridad, fuerza armadas, organismos de derechos humanos e instituciones público/privadas. La reciente y masiva utilización de internet cambió el paradigma de trabajo (teletrabajo) producido por la pandemia. Las TICs junto con su acelerado avance, conllevan la necesidad de concientizar y prevenir sobre el funcionamiento de técnicas maliciosas (IS).

No hay al día de hoy un Firewall contra los ataques a las personas, es por esto que la presente investigación intenta dar a luz sobre las técnicas y los principales casos que se fueron manifestando en algunas organizaciones del Estado Argentino durante los años 2020; 2021.

Palabras clave: *ingeniería social, Argentina, cibercrimen, pandemia-Covid19, Ciberinteligencia.*

Índice General

1. Introducción

La elección del tema de estudio surge a partir de los acelerados procesos de trasformación tecnológicas, TICs (tecnologías de la información y comunicación) producidos por la pandemia (Covid-19).

El cibercrimen generalmente apoyado en la ingeniaría social planifica y ejecuta mediante diversas técnicas, sus ataques maliciosos. Aprovechándose del desconocimiento en general de las personas y la psicología humana. Se sabe que el factor humano es el más débil de la cadena. Las empresas privadas al ser afectadas por esta modalidad en ocasiones contratan servicios de "pentesting en IS" (tests de penetración ética a su organización) para identificar y analizar el nivel de seguridad que tienen sus organizaciones, este método procede de una rama de la seguridad informática, en el que, mediante previo acuerdo, un especialista (pentester), intenta vulnerar o hackear de forma ética la organización. A causa del espionaje industrial las organizaciones deben tomar medidas de contrainteligencia para poder asegurar cotidianamente su información, como activo empresarial. La fuga de información es un riesgo y amenaza constante en el mundo empresarial. En las organizaciones del Estados sucede los mismo, pero en muchos casos, son más vulnerables, las organizaciones gubernamentales se encuentran frente a riesgos y amenazas desconocidas. No están advertidas o capacitadas en ataques de este tipo. Se puede tener como ejemplificador el ataque mediante Ransonware (tipo de malware que tiene la particularidad de cifrar los archivos de una computadora) ejecutado en la Direcciona Nacional de Migraciones en el año 2020. Pidiendo como rescate un alta suma de dinero.

La ingeniería social tiene una connotación maliciosa desde el punto de vista de la seguridad informática, ya que está identificada como una vulnerabilidad que se encuentra en las personas y por lo tanto es difícil de prevenir.

Ahora bien, no toda la ingeniería social es mala, la utilizamos todo el tiempo para intentar persuadir a nuestros hijos, o en intervenciones profesionales para que un paciente adopte un tratamiento o para convencer a nuestros familiares de determinadas ideas o creencias.

1.1 Fundamentación

Como material de inteligencia y contrainteligencia es fundamental conocer las prácticas llevadas adelante por lo cibercriminales. Analizando estratégicamente la ciberseguridad que hoy en día se rige cada vez mas más por el conocimiento y el avance

tecnológico. Es notable que a partir de la información que nos ofrecen las fuentes abiertas "OSINT" es posible averiguar números de teléfonos, emails, direcciones IP, geolocalización, análisis de imágenes, conocer ideología política, preferencias personales, interacciones, lugar de trabajo, etc. No solo de personas, sino también de organizaciones.

Revisar la basura es tan solo una de las más antiguas prácticas para recabar información sensible de una persona u organización. Puede ser utilizada para una investigación judicial como técnica (física) de ingeniaría social que generalmente arroja buenos resultados. La adquisición de información es la primera fase del ciclo de un ataque, donde tanto delincuentes como investigadores se apoyan para perfilar inicialmente a sus objetivos.

El ciberespacio abrió un mundo que, combinándolo con técnicas físicas, remotas y la combinación de ambas puede explotar de manera casi perfecta vulnerabilidades de sus objetivos humanos. Esto se denomina hacking con ingeniería social, son técnicas que van desde lo simple como revisar la basura hasta la propagación de un malware especifico en un dispositivo electrónico. Un ejemplo es la utilización de emails infectados mediante la técnica conocida como "phishing". La misma hace referencia a la palabra fishing en inglés ya que intenta referenciar la palabra "pescar", mediante un engaño a su víctima.

Recientemente la Secretaria General de Interpol público un reporte denominado "Ciberdelincuencia: efectos de la covid-19" (2020)[1]. Donde se detallan las tendencias del cibecrimen mundial por región y las principales amenazas relacionadas con el covid-19. Un estudio realizado con acceso a datos de más de 194 países miembros. Sin dudas el aprovechamiento de la pandemia para los ciberdelincuentes es un hecho mundial transformándose en un objeto de estudio.

Hoy en día vemos a diario en los medios de comunicación, las estafas a empresas, a personas civiles, jóvenes o jubilados. Es importante aclarar; todo ser humano sin importar su formación es altamente vulnerable. Se puede engañar con una llamada telefónica, consiguiendo persuadir a una persona para que se dirija voluntariamente hasta su cajero automático para finalizar otorgándole a los atacantes su nuevo código de token del banco. Previamente esta persona fue perfilada por los atacantes, se obtuvieron datos personales, teléfono, su cuenta bancaria, etc. Acción continua los criminales crean un pretexto verosímil o creíble para sus víctimas. Aprovechando una vez más la distracción, la buena fe y el desconocimiento de las personas.

[1] Secretaria General de Interpol (2020). *Ciberdelincuencia: efectos de la Covid-19*. Lyon, Francia.

En el presente encontramos diferentes ataques de IS, las estafas al IFE, falsificación de DNI digital, robo de identidad, intercepción y clonación de mails, caso FADEA por la cual se depositaron 500$ mil dólares en una cuenta falsa. Además, el robo y posterior fuga de datos de IOSFA y RENAPER.

Lo que se intenta demostrar en la presente investigación es el alcance y el nivel de vulnerabilidad que pueden tener los sistemas de seguridad interior en general, hasta los de Defensa.

Las distintas técnicas utilizadas por el cibercrimen generalmente no son conocidas por la sociedad. La educación, el conocimiento y la prevención serán fundamental en el futuro próximo frente a este problema. Además, entendemos que es una herramienta personal y profesional para los futuros analistas de inteligencia a tener en cuenta. Las actualizaciones de nuevas amenazas en ciberseguridad son necesarias e indispensables para la formación de analistas.

Los funcionamientos de los procesos psíquicos y los sesgos cognitivos tendrán un proceso fundamental para crear más especialistas, pero el conocimiento profesional y de la coyuntura ahorrarán tiempo, generarán pensamiento crítico y una mejor toma de decisiones. Llevando conocimiento a la sociedad y una posible formación continua a los futuros analistas de inteligencia. Ya tenemos ejemplos claros de cómo se pudo manipular a la sociedad americana, mediante datos personales, en una elección en EE. UU (caso de Cambridge Analítica). La ingeniería social no es solamente, o únicamente un phishing, si no que va mucho más allá, donde deberíamos poder preguntarnos si no somos manipulados desde un “afuera”.

La reputación de las personas, los Estados y las organizaciones están obligadas a protegerse y regular medidas activas.

1.2 Problema

¿Cuál es el impacto de la ingeniería social en organizaciones estatales de Argentina a partir de la pandemia producida por el COVID-19?

1.3 Justificación de la investigación

La ingeniería social cuenta con diversas definiciones, pero podemos decir que es la actividad mediante la cual una o más personas influyen sobre otra, para manipularla en contra su voluntad y conseguir así, que realice algún tipo de acción en su contra o de terceros.

Una de las tantas definiciones de la Ingeniera Social, Hadnagy (2011) afirma; es el arte, o mejor aún, la ciencia, de maniobrar hábilmente para lograr que los seres humanos actúen en algún aspecto de sus vidas. (p.36). El concepto en sí mismo es desconocido por la sociedad argentina, si bien es antiguo para los profesionales de la seguridad informática no se conoce ampliamente o los alcances de su significado. La ingeniería social es utilizada desde hace mucho tiempo en la seguridad de la información. El concepto se comenzó a utilizar en Estados Unidos a fines de los años 70. Si bien es nuevo en el país, estas prácticas o técnicas, existen desde los comienzos de la humanidad. Presentes en la mitología como el "Caballo de Troya".

Se ve en las grandes y pequeñas estafas, en grandes robos como lo fue el denominado "Robo del Siglo", al Banco Rio en enero del año 2006, en la provincia de Buenos Aires. Se enfoca en las habilidades de un atacante hostil para influir y manipular a las personas con el fin de obtener acceso físico o acceso a información vital.

Según la organización "Asociación Argentina de Lucha Contra el Cibercrimen" (2020) afirma en sus estadísticas un fuerte crecimiento del cibercrimen en cuarentena[2]. En el estudio, se muestra la creciente oleada de casos en el año 2020, como así también las metodologías y las principales provincias afectadas. Vale aclarar que este tipo de delitos de acuerdo a sus características tiene un nivel muy bajo de denuncia en el país. Ya que muchas veces las personas no son conscientes de lo sucedido, no saben dónde realizar la denuncia, o por vergüenza misma y el engaño sufrido deciden no denunciar.

A partir de los expuesto;

Nos formulamos las siguientes preguntas:

1. ¿Cuáles son las distintas modalidades de ingeniería social en las cuales se apoyan los ciberdelincuentes?
2. ¿Cómo se podrán bajar los riesgos o las vulnerabilidades en el factor humano?

El cibercrimen y la ingeniería social serán abordados principalmente, como así también sus técnicas, relacionadas con OSINT (inteligencia de fuentes abiertas), contra

[2] Asociación Argentina de Lucha Contra el Cibercrimen. (2020). *Fuerte Crecimiento de Delito Informáticos en Cuarenta.* Recuperado de https://www.cibercrimen.org.ar/2020/07/08/fuerte-crecimiento-de-delitos-informaticos-en-cuarentena/

inteligencia y ciberseguridad. Con el fin de dar cuenta, conocer, prevenir y utilizar la actividad de ingeniaría social como herramienta preventiva y fundamental. Conocer el ciberespacio hoy demanda mayor conocimiento de los ciberdelincuentes. Además, aportar conocimiento para la toma de decisiones en niveles jerárquicos de anticipación estratégica o los riesgos y amenazas que el avance de las tecnologías de la información y comunicación implican.

1.4 Objetivos

La presente investigación se justifica por diversas razones, la primera de ellas es la de analizar e identificar una realidad nueva y poco investigada mediante método científico. La misma intenta ampliar el conocimiento acerca de una compleja modalidad utilizada por el cibercrimen en pandemia. Intentando aportar una mirada posible a estudios que se realicen en el futuro, sumando al conocimiento académico y a los profesionales pertenecientes a la comunidad científica. Indagar sobre sobre una actividad poco explorada como es el caso de la ingeniería social en Argentina. El trabajo se legitima, asimismo, por la significación social que tiene el cibercrimen hoy en el país. La posibilidad de aportar un conocimiento nuevo que ayude a la prevención y concientización del problema. Además, comprender el mecanismo de los procesos convergentes. Siendo este un contexto particular, de emergencia a partir de la pandemia (covid-19), que invita al autor a realizar la investigación. La principal motivación es arribar a conclusiones válidas, sin sesgos, en beneficio de organizaciones públicas y privadas.

A los resultados esperados se sumará el conocimiento adquirido de la Especialización en Inteligencia Estratégica y Crimen Organizado. Por lo tanto, puede ser una fuente de información para los jóvenes que deberán iniciarse en temas de ciberseguridad, seguridad de la información, ingeniería social, OSINT[3](significa *Open Source Intelligence*, lo que al traducirlo nos da: investigación en fuentes abiertas**)**, cibercrimen, contrainteligencia. Saliendo del secretismo y realizar una apertura del conocimiento. Aportar posibles ideas a los futuros programas de prevención en la sociedad civil. En cuanto a la actividad y a su alcance, la importancia y su apropiada aplicación en la democracia actual.

[3] Ciberpaatrulla.com. (2019) *¿Qué es OSINT? Usos y beneficios de aplicar este sistema para recopilar información.* Recuperado de https://ciberpatrulla.com/que-es-osint/

Asimismo, la investigación descriptiva contribuirá a la formación de quien la realice, así como al área del análisis de inteligencia, para colaborar en futuras mejoras con respecto al ciberespacio y el factor humano.

1.4.1 Objetivos

Se definen los siguientes objetivos, generales y específicos, que guiarán el proceso de investigación.

1.4.2 Objetivos general

- Analizar los ataques centrales de ingeniería social en Argentina en organismos estatales a partir de la pandemia producida por covid-19.

1.4.3 Objetivos específicos

- Describir características metodológicas de la ingeniaría social llevada adelante por los ciberdelincuentes.
- Evaluar el nivel de seguridad en el país, a partir de factores intervinientes a nivel personal, grupal y organizacional para la prevención de la ingeniería social.

1.5 Metodología

La metodología del proyecto incluye el tipo de investigación, las técnicas y los procedimientos que serán utilizados para llevar a cabo la indagación.

Inicialmente el estudio será descriptivo, estará basado en fuentes humanas y bibliográficas con el fin de arribar a un nuevo conocimiento sobre la problemática a estudiar.

La investigación se enmarca dentro de un estudio de tipo cualitativo con el fin de recopilar información por parte de especialistas en la temática. Mediante el instrumento de la Entrevista (semidirigida) se podrá resaltar el testimonio de informantes clave o especialistas. Recopilando y analizando la información con el fin de obtener resultados a los objetivos.

La presente investigación realiza un estudio de caso descriptivo y cualitativo. La metodología se basa en un conjunto de técnicas y procedimientos que se aplican para

desarrollar la investigación y arribar a una conclusión posible. El universo de estudio que se seleccionó para esta investigación son las metodologías de Ingeniería Social utilizadas en Argentina durante el año 2020 y 2021 durante la pandemia producida por el COVID-19.

La investigación es de tipo descriptiva ya que caracteriza la realidad de la situación social que se da en un determinado país y recolecta datos para analizarlos y posteriormente evaluando: Impacto y Metodologías de Ingeniería Social en instituciones estatales de Argentina.

El estudio presenta en primer término una investigación de tipo cualitativa, siendo observadas las cualidades del fenómeno, las experiencias de los especialistas y sus significaciones dentro de sus puestos de trabajo.

Los objetivos apuntan a obtener la información suficiente para dar respuesta a la problemática planteada como a los objetivos descriptos.

Los destinatarios del presente trabajo son todas las personas que integren una organización sea público o privada, y necesiten obtener información, investigación de Ciberinteligencia, para dar respuesta o alerta a la problemática de la ingeniería social y su relación con el cibercrimen.

2. Marco teórico

2.1 La ingeniería social (IS)

Para comenzar a abordar el problema de investigación debemos remontarnos a la pregunta: ¿Que es la ingeniaría social? Según el ingeniero social Christopher Hadnagy (2011) es el arte, o mejor aún, la ciencia de maniobrar hábilmente para lograr que los seres humanos actúen en algún aspecto de sus vidas. El autor continúa diciendo; "Esta definición amplía los horizontes de los ingenieros sociales a todas partes. La ingeniería social es utilizada en la vida diaria, por ejemplo, en la forma en la que los niños consiguen que los padres atiendan sus peticiones. Es utilizada por profesores en el modo de interacción con sus estudiantes y por los doctores, abogados, psicólogos para obtener información de sus pacientes o clientes. Es claramente utilizada por las fuerzas de orden público y en las relaciones de pareja. En definitiva, es utilizada en cualquier interacción humana, desde los bebés hasta los políticos". (p.37) Como plantea el autor al ser utilizadas por las fuerzas del orden público el término de ingeniería social se encuentra muy cercano al de inteligencia. Ya que en ambos hay procesos de obtención, explotación y análisis de información. Según Spadaro (2016) La Inteligencia es un proceso sistemático de recolección, evaluación y análisis de información, cuya finalidad es producir conocimiento útil para la toma de decisiones. (p. 30).

Hay dos vectores principales de ataques en las técnicas; pudiendo ser basados en el uso de la tecnología o en el uso del engaño humano, que desarrollaremos en el presente estudio.

Las empresas con grandes sistemas de seguridad, tecnología, dispositivos biométricos pueden ser víctimas, así lo afirma Gómez Vieytes (2014) en su libro, en palabras de Kevin Mitnick, uno de los hackers más famosos de la historia, "usted puede tener la mejor tecnología, firewalls, sistemas de detección de ataques, dispositivos biométricos…Lo único que se necesita es una llamada a un empleado desprevenido y acceden al sistema sin más. Tiene todo en sus manos". (p. 94). Una desatención en la seguridad de la información podría llegar a significar una fuga masiva de información. Y grandes pérdidas de los activos de una organización.

Kevin Mitnik es considerado uno de los hacker más famosos y audaces del mundo. Así lo afirma Grimes (2018), cuando aparece el termino de *hacker informático* todo el mundo piensa en Kevin Mitnick. En los 70, 80, 90 Kevin era el hacker. Mitnick utilizada

una combinación de ingeniería social y búsqueda de sistemas operativos de bajo nivel para llevar a cabo todo tipo de maniobras indignantes, aunque el daño general que causaba es discutible, especialmente si se compara con los ataques *APT Y Ransomware* mundiales de nuestros días. (p.33). A lo largo de su vida criminal Mitnick, enfrentó varios procesos judiciales por sus intrusiones como ingeniero social en EE.UU. Una vez cumplida su condena colaboró con el gobierno de su país para combatir delitos relacionados a la IS y las telecomunicaciones. Hoy en día es un reconocido consultor internacional y continúa escribiendo libros y participando de eventos de ciberseguridad. Él mismo afirma que, la ingeniería social se basa en cuatro principios fundamentales: 1) Todos queremos ayudar 2) El primer movimiento es siempre de confianza hacia el otro 3) No nos gusta decir no 4) A todos nos gustan que nos alaben[4].

Por esto mismo la IS se percibe como un arte en la cual la creatividad ataca hostilmente a lo desconocido. La sorpresa, el velo, el engaño, la actuación, la magia, la psicología, la ciencia y tecnología (entre otras) se complementan en la actividad. Conocer estos fenómenos es puntualmente apuntar a la concientización y la prevención en las personas.

En su libro Guerra Cibernética, Steel (2005) sostiene, si hasta ahora la sociedad imponía que los espacios tierra, mar y aire eran los que definían la existencia de las tres Fuerzas Armadas, cuando esa misma sociedad perciba que los ataques cibernéticos son desarrollados en un espacio distinto que la afectan sensiblemente en su desarrollo y evolución, ésta habrá de poner en movimiento la energía social que de origen a una fuerza cívico militar, cibernéticamente armada. (p.19)

Pero no podemos asegurar que la IS solo se base en engaños al mismo tiempo. En el libro *"Hacking con Ingeniería Social Técnicas para hackear humanos"* Ramos Varón, Barbero Muñoz, Marugán Rodríguez y Gonzalez Durán (2015) afirman, La ingenia social puede definirse como el conjunto de técnicas de tipo social que pueden usar individuos, grupos u organizaciones de cualquier tipo para manipular o persuadir a objetivos humanos con la intención de que realicen acciones, tomen decisiones o revelen información valiosa para el atacante de forma voluntaria. Además, los autores plantean; lo que la ingeniería social no es simplemente una estafa, un timo o un engaño sin más, aunque en muchas ocasiones se utilicen técnicas de ingeniería social por parte de estafadores y delincuentes para llevar a cabo estas acciones y también empleen la mentira o la manipulación. Esto suele ser un error

[4] Hardvard-deusto.com.(2020). *Seis pasos para no caer en el "arte del engaño"*. Recuperado de https://www.harvard-deusto.com/seis-pasos-para-no-caer-en-el-arte-del-engano

muy habitual. De hecho, la ingeniería social no tiene por qué perseguir un objetivo malévolo o recurrir siempre al engaño. Para ilustrar este ejemplo se podrá decir que un psicólogo que trata a un paciente o un policía que interroga a un sospechoso puede, en muchos casos, comportarse como un auténtico ingeniero social sin que el fin del uso de estas técnicas sea malicioso o ilegal. (p, 17).

No hay una sola modalidad ya que dependiendo de la víctima se puede diseñar nuevas formas de ataque o combinarlas. Barbero Muñoz, Marugán Rodríguez y Gonzalez Durán (2015) plantean que la posibilidad de un éxito depende de un "mix" dependiendo de cuestiones como:

- Experiencia del ingeniero social.
- Formación sobre ingeniería social que tiene la víctima.
- Marco económico, cultural, político e historio del escenario.
- Sensibilización del personal en cuestión de seguridad IT.
- Ataque elegido.

Además, los autores plantean que los ingenieros sociales deberán contar con ciertas habilidades y conocimientos que conformar un perfil muy especializado aclarando; "Entre otras cosas, se podrá decir que el ingeniero social contará de forma ideal con:

- Conocimientos altos de los sistemas de información y de telecomunicaciones.
- Grandes habilidades sociales, aprendidas o desarrolladas.
- Capacidad de improvisación, imaginación y adaptación al cambio.
- Conocimiento avanzado sobre psicología y PNL.
- Ser un experto en seguridad de la información.
- Alto nivel de cultura en general, que le permita sostener pretextos sobre la marcha, recurrir a la improvisación, intervenir en cualquier clase de conversación o interactuar con diferentes perfiles dentro de las organizaciones objetivo". (p.24)

2.2 Principales ataques de IS

A continuación, se intentarán clasificar los ataques más comunes de IS, vale aclarar que no están todas las metodologías empleadas ya que son diversas con un alto nivel de renovación, haciendo del cibecrimen un complejo escenario para los analistas. Se detallan a continuación las metodologías más utilizadas a partir de la "Tesis de Maestría" Méndez Carvajal, A. Estudio de Metodologías de Ingeniería Social (2018).

- Phishing: Son mensajes de correo electrónico, SMS, o comunicados por redes sociales en los cuales poden ingresar a través de un link a una página web (falsa). Los criminales copian la totalidad de una página real y la publican en servidores que presentan vulnerabilidades, estos servidores son de personas ajenas a la entidad y al delincuente, donde se solicitan datos y claves personales, para efectos de actualización de información, blindaje de IP, actualización tecnológica, compras no autorizadas, fraudes, entre otros.
- Vishing**:** Es la modalidad en la cual el ingeniero social, a través de una llamada, busca llamar la atención de su víctima para obtener información sensible. Un ejemplo, es cuando llaman a una tarjetahabiente indicándole que está haciendo compras son sus TC y que, para detener la transacción, debe informar el número de su TC, fecha de vencimiento y CVV (código al respaldo de las TC para autorizar compras).
- Sextorsión**:** Es una forma de extorción en la que se busca chantajear a una persona, por medio de una imagen o video de sí misma comprometedor (desnuda), que pudo haber compartido a través de internet o chat. La victima es coaccionada a cancelar sumas de dinero, para no divulgar la información en la web y entorno social o ejecutar acciones que den gratificación sexual al delincuente.
- Baiting: Es una técnica muy efectiva, que utiliza pendrives con software malicioso, los que dejan en lugares de acceso concurrido de la víctima para que los encuentre y los conecte a sus equipos de cómputo.
- Relaciones Engañosas, Pretextos, Manipulación: Generan relaciones personales con el fin de engañar a la víctima, manipularla y conseguir información.
- Googlear: Es simplemente realizar búsquedas en el buscador Google, pero por ejemplo haciéndolo con "Google Dorks" son búsquedas avanzadas con el fin de obtener información sensible que Google halla indexado. Para la IS este tipo de búsqueda puede ser muy útil, encontrando información relevante de su objetivo.
- Suplantación de Identidad: El ingeniero social asumen un rol que represente autoridad o necesidad, por ejemplo: puede hacerse pasar, en una llamada telefónica, por un usuario legítimo y contactarse con el departamento de IT, para que le cambien su contraseña o caso contrario, hacerse pasar por el personal de IT, indicando a un usuario legítimo que requiere de sus credenciales, para solucionar un problema en el

sistema que está causando el mismo usuario y requiere información sensible por teléfono o correo electrónico.

- Grooming: Proviene del verbo "groom" que alude al hecho de asear, acicalar o peinar a un animal. Se trasladó como préstamo lingüístico para reflejar cuando un adulto se contacta de forma sistemática, deliberada y sostenida en el tiempo con un menor a través de cualquier medio electrónico (chat, SMS, redes sociales, etc.) con la intención de establecer una relación y un control emocional sobre el menor. No necesariamente puede derivar en un ataque sexual hacia el menor ya que los objetivos del ataque pueden ser diversos según la intención del adulto (groomer).
- Fake News: Distribución de noticias falsas en distintos medios de comunicación con el fin de desprestigiar, boicotear, distraer y manipular la opinión pública o la imagen de las personas.
- Carding: Inicialmente se basaba en robar tarjetas de crédito que podían ser usadas para realizar compras ilegales hasta que fueron canceladas. No obstante, hoy en día el principal metido usado para robar información de las tarjeras de crédito, datos financieros u otros detalles sensibles, están relacionados con el malware o phishing.
- Trashing (buscar en la basura): los IS pueden encontrar en las sestas de basura todo tipo de información, tanto física, con electrónica, datos financieros, recibos de servicios públicos, post-it con credenciales, en general información sensible de negocio.
- Acceso Físico: Este tipo de ataque se aprovecha de la solidaridad y buena voluntad de las personas. Suele presentarse cuando un empleado (victima) está ingresando a su empresa, la cual posee algún tipo de restricción en su acceso físico y el atacante con un gesto de torpeza porque olvido sus credenciales, solicita ayuda para poder ingresar. (p.11)

2.3 Legislación Argentina

A día de hoy Argentina cuenta con la Ley de delitos informáticos (Ley 26.388) que ah realizados incorporación y modificaciones al Código Penal. Incluye muchos de los delitos que generalmente se emplean utilizando técnicas de ingeniería social. La legislación los contiene con los siguientes nombres y artículos: Grooming Art. 131. Artículo 128: Será reprimido con prisión de seis (6) meses a cuatro (4) años el que produjere, financiare, ofreciere, comerciare, publicare, facilitare, divulgare o distribuyere, por cualquier

medio, toda representación de un menor de dieciocho (18) años dedicado a actividades sexuales explícitas o toda representación de sus partes genitales con fines predominantemente sexuales, al igual que el que organizare espectáculos en vivo de representaciones sexuales explícitas en que participaren dichos menores.

Será reprimido con prisión de cuatro (4) meses a dos (2) años el que tuviere en su poder representaciones de las descriptas en el párrafo anterior con fines inequívocos de distribución o comercialización.

Será reprimido con prisión de un (1) mes a tres (3) años el que facilitare el acceso a espectáculos pornográficos o suministrare material pornográfico a menores de catorce (14) años.

Difusión de Malware Art. 183, Difusión maliciosa de información; En la misma pena incurrirá el que alterare, destruyere o inutilizare datos, documentos, programas o sistemas informáticos; o vendiere, distribuyere, hiciere circular o introdujere en un sistema informático, cualquier programa destinado a causar daños.

Art.155, Violación de datos personales; Será reprimido con prisión de un (1) mes a dos (2) años e inhabilitación especial de un (1) a cuatro (4) años, el funcionario público que revelare hechos, actuaciones, documentos o datos, que por ley deben ser secretos.

Art. 157 bis: Será reprimido con la pena de prisión de un (1) mes a dos (2) años el que:

1. A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales;

2. Ilegítimamente proporcionare o revelare a otra información registrada en un archivo o en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de la ley.

3. Ilegítimamente insertare o hiciere insertar datos en un archivo de datos personales.

Cuando el autor sea funcionario público sufrirá, además, pena de inhabilitación especial de un (1) a cuatro (4) años.

2.4 Pandemia y cibercrimen

Los acelerados procesos de transformación tecnológica demandados por la pandemia (Covid-19), generaron mayor uso de internet y las TICs. Como recurso básico, la conectividad se trasformó en un servicio indispensable para la población. Para muchas personas fue un momento nuevo, de aprendizaje e incertidumbre. No así para el cibercrimen que, rápidamente observó la situación como oportunidad favorable.

A partir de reportes nacionales e internacionales utilizados en el presente estudio: La Asociación Argentina de Lucha Contra el Cibercrimen (AALCC), Interpol y GAFI, reportaron un fuerte aumento en los ataques de ingeniería social, correos electrónicos mediante phishing, Ransonware dominios maliciosos, fake news, sextorsión, robo de identidad, cyberbullying, grooming, entre otros.

2.5 Casos reales (Covid-19)

La organización "Asociación Argentina de Lucha Contra el Cibercrimen" (2020) afirma en sus estadísticas un fuerte crecimiento del cibercrimen en cuarentena[5]. En el estudio, se muestra la creciente oleada de casos en el año 2020, como así también las metodologías y las principales provincias afectadas.

Recientemente la Secretaria General de Interpol público un reporte denominado "Ciberdelincuencia: efectos de la covid-19" (2020)[6]. Donde se detallan las tendencias del cibecrimen mundial por región y las principales amenazas relacionadas con el covid-19. Un estudio realizado con acceso a datos de más de 194 países miembros. Sin dudas el aprovechamiento de la pandemia para los ciberdelincuentes es un hecho mundial transformándose en una nueva ciberamenaza a investigar.

En esta misma línea el informe con fecha de diciembre del 2020 del GAFI en Ciberdelitos advierte; diversas regiones del mundo informan aumento continuo de estafas relacionadas con el ciberespacio.[7].

---

[5] Asociación Argentina de Lucha Contra el Cibercrimen. (2020). *Fuerte Crecimiento de Delito Informáticos en Cuarenta*. Recuperado de https://www.cibercrimen.org.ar/2020/07/08/fuerte-crecimiento-de-delitos-informaticos-en-cuarentena/

[6] Secretaria General de Interpol (2020). *Ciberdelincuencia: efectos de la Covid-19*. Lyon, Francia. Web: www.interpol.int

[7] FATF (2020), *Update*: *COVID-19-related Money Laundering and Terrorist Financing – Risks and Policy Responses*, FATF, Paris, France, www.fatf-gafi.org/publications/methodandtrends/documents/update-covid-19-ML-TF.html

2.6 El anonimato en internet

Parafraseando a R. Layton & P. Watters (2016) el anonimato en internet es un beneficio para los cibercriminales y una desventaja para las investigaciones judiciales. Entendemos a internet como la red más grande del mundo, donde millones de operaciones, comunicación se ejecutan constantemente alrededor del mundo. La ciber vigilancia existe con norma recientemente aprobada en argentina bajo la figura de "ciberpatrullaje", Resolución 144/2020[8].

Layton & Watters (2016) afirman; Internet es, aparentemente, paradójicamente, la fuente más grande del mundo de vigilancia, y también una de las vías más seguras para enviar mensajes anónimos que existe hoy. La explicación de esta paradoja es la forma en que se utiliza. La mayoría de los usuarios de Internet usa diligentemente las aplicaciones y configuraciones predeterminadas, lo que permite casi todas sus comunicaciones para ser rastreadas, grabadas y analizadas en una fecha posterior, como quedó dolorosamente claro en el amplio escándalo de monitoreo involucrando a la NSA. Algo de esto se hace obligatorio a través de la legislación, otros a través de desarrolladores de software que registran esta información para su interna (o, en algunos casos, análisis externo).

Por el contrario, otros usuarios utilizarán programas que tienen como objetivo ocultar la identidad. Estas tecnologías son abundantes, aunque el número que puede de confianza es bastante pequeño. Además, la lista de tecnologías en las que se puede confiar cambios, a medida que surjan exploits o preocupaciones. Quizás la herramienta de anonimizarían más grande actualmente en uso es The Onion Router (TOR). Este sistema, creado por la Marina de los EE. UU. En 2004, permitía el anonimato comunicación mediante el enrutamiento de mensajes a través de una serie de otros usuarios de Tor computadoras, de tal manera que nadie en la red pueda interceptar mensajes, para quién está destinado o de quién se originó (Dingledine, Mathewson, & Syverson, 2004). Tor se basa en conceptos criptográficos avanzados y también en la seguridad en los números. Para, por ejemplo, la presencia de Tor en una computadora puede ser un indicio de irregularidades en nombre del usuario, incluso si no existe ninguna otra evidencia (aunque este hecho por sí sola no podría, y probablemente no debería, conducir a una condena). Para poder no tener esta mancha,

[8] Poder Ejecutivo Nacional (2020). Boletín Oficial de la República Argentina. Recuperado de: https://www.boletinoficial.gob.ar/detalleAviso/primera/230060/20200602

debería ser utilizado por una gran cantidad de personas, incluidos aquellos que "no tienen nada que ocultar" (Solove, 2007). (p, 41)

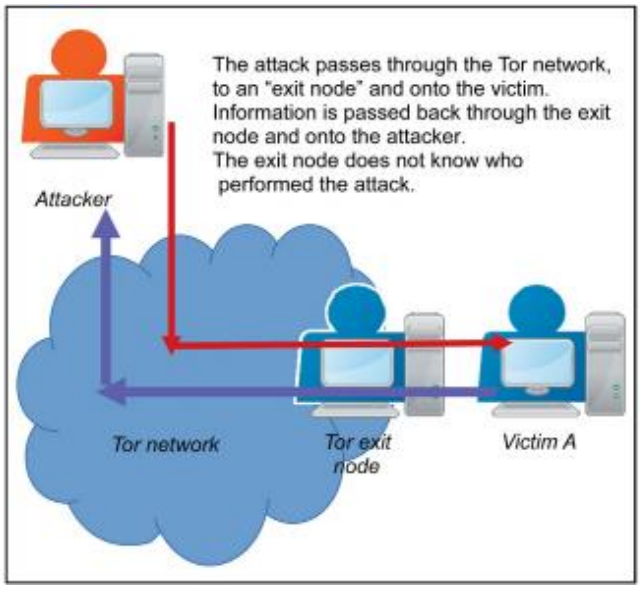

Figura 1 An attack through Tor.

Nota: Adaptado de "*Automating Open Source Intelligence*, Algorithms for OSINT, pág. 44, Edited By Robert Layton Paul A. (2016). Of Elsevier, USA.

2.7 La seguridad de la información

En la comunidad de la seguridad informática, las siglas "CIA" no tienen nada que ver con una cierta agencia de inteligencia estadounidense muy conocida. Estas tres letras significan confidencialidad, integridad y accesibilidad, también conocidas como la *tríada de la CIA*. La tríada de la CIA es tan fundamental para la seguridad de la información que, cada vez que se filtran datos, se ataca un sistema, un usuario muerde un anzuelo de phishing, una cuenta es secuestrada, un sitio web es maliciosamente retirado o se produce una serie de incidentes de seguridad, usted puede estar seguro de que uno o más de estos principios han sido violados. Los profesionales de ciberseguridad evalúan las amenazas y vulnerabilidades basándose en el impacto potencial que tienen en la confidencialidad, integridad y disponibilidad de los activos de una organización. Es decir, sus datos, aplicaciones y sistemas críticos. Basándose en esa evaluación, el equipo de seguridad implementa un conjunto de controles de seguridad para reducir el riesgo en su entorno. (https://searchdatacenter.techtarget.com/es/opinion/Que-es-la-triada-de-la-CIA)

La seguridad de la informática se basa en la conocida “triada” sus siglas son CIA, en español es Confidencialidad, Integridad y Accesibilidad. Son fundamentales para evaluar los distintos ataques informáticos.

2.8 Pen-testing e IS

Las empresas que adoptan buenas medidas de seguridad para proteger su información contratan a consultores especialistas en seguridad informática para que realicen testeos de penetración (pen testing) con técnicas de ingeniería social. Es un intento de hackeo ético para poner a prueba la seguridad de su organización y avaluar que nivel de seguridad les compete. Grimes (2018) afirma, estas pruebas se basan en intentos de hackeos de modo ético y legal. El “atacante” humano puede utilizar su propio ingenio y herramientas nuevas o existentes mientras busca debilidades, basadas ya sea en una maquina o en humanos. Esto incluye bancos, sitios de gobiernos, hospitales y sitios corporativos (p.10).

Se adjunta en (*Anexo 1)* para dar cuenta los requerimientos de la institución. Se basa a una técnica ética para combatir y prevenir la ingeniería social relacionada a la fuga de la información sensible.

En el libro “Social Engineering, Penetration Testing” de Gavin Watson, Andrew Mason y Richard Ackroyd (2014) los autores plantean; Estos procesos, no importa lo fuertes y bien diseñados que sean, solo son tan buenos como las personas quienes las implementan. La formación de concienciación del personal trata de educar a los empleados en comprender los riesgos y ajustar sus comportamientos en consecuencia a través de la capacitación. Los empleados deben estar comprometidos con la necesidad de prácticas laborales seguras en para que cualquier programa de formación de concienciación del personal sea considerado un éxito. Para organizaciones importantes, este trabajo puede ser sustancial y requerirá una gran inversión tanto en aspectos financieros como en aspectos de tiempo para la alta dirección dentro de la organización para su correcta implementación.

Suponiendo que una organización ha realizado un ejercicio para investigar las políticas existentes y procedimientos con miras a crear políticas y procedimientos más seguros. La creación y realización de una evaluación interna de ingeniería social. es una forma de medir la eficacia de las políticas y procedimientos dentro una organización, así como la forma en que el personal implementa y sigue dichos procedimientos. (p. 362)

La seguridad de la organización deberá ser parte de la cultura organizacional para poder ser efectiva, no se comprende como un hecho aplicable a corto plazo. Si no que irá aumentando a medida que las personas junto con las organizaciones adquieran comportamientos en esta dirección. Es por eso que se insiste en que la ciberseguridad deberá ser adoptada en la cultura de las empresa o instituciones del Estado.

3. Diagnóstico

3.1 El phishing como protagonista

Dentro de los principales reportes consultados tanto nacionales como internacionales se referencia al "Phishing" como la técnica más utilizada por lo ciberdelincuentes. Su múltiple utilización puede adaptarse a distintos tipos de ataques. Utilizado para el robo de datos con fraudes, comercialización ilegal de información, extorción, propagación de malware, entre otras.

Según un análisis hecho por la "Asociación Argentina de Lucha Contra Cibercrimen" sobre consulta de delitos informáticos en Argentina entre: el 20 de marzo de 2020 al 1 de julio del 2020[9]. Se describen como principales el ciberbullying, fraude, extorción y phishing.

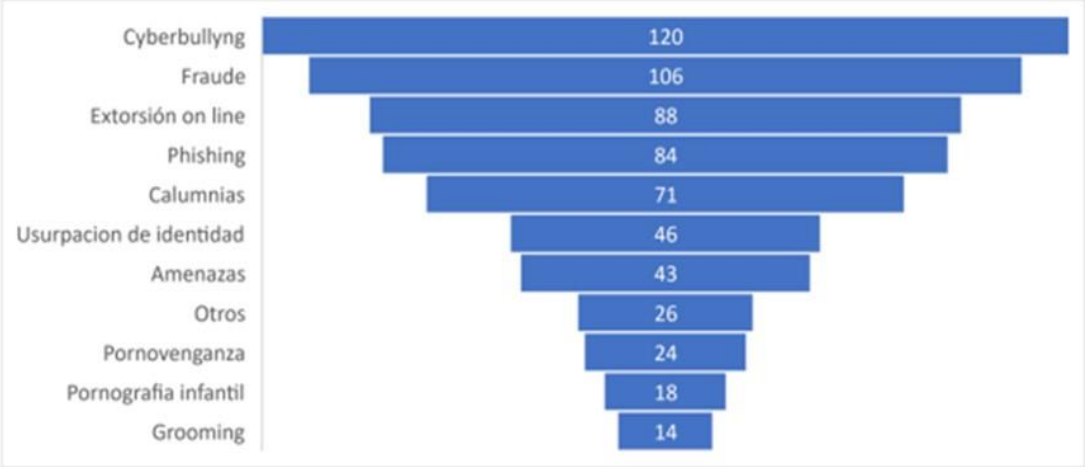

Figura 1 Delitos más consultados. AALCC (2020).

A su vez Interpol en su reporte de "ciberamenazas relacionada con la COVID-19", ubica al Phishing y estafas por encima de otras técnicas. Además, aclara que la proliferación de uso de temáticas relacionadas con la COVID-19 en delitos de phishing y estafas por internet desde el brote de la pandemia. Los ciberdeliencuentes aprovecharon la recesión económica y la ansiedad que padecen las personas para perfeccionar sus técnicas de Ingeniería Social.

Según Hadnagy (2011) la (IS) es el arte, o mejor aún, la ciencia de maniobrar hábilmente para lograr que los seres humanos actúen en algún aspecto de sus vidas. (P, 37).

[9] AALCC.(2020). *Análisis de delitos informáticos en Argentina*. https://www.cibercrimen.org.ar/wp-content/uploads/2020/07/Analisis-de-consultas-de-delitos-inform%C3%A1ticos-covi19-II.pdf

El concepto apunta directamente a algún tipo de manipulación o engaño para conseguir acceso a información crítica.

Figura 2 Principales ciberamenazas identificadas en pandemia Covid-19

Nota: Adaptado de Ciberdelincuencia: efectos de la Covid-19. Interpol (2020)

El GAFI (2020) como fuente de información reportó un número significativo de jurisdicciones de diversas regiones del mundo informan aumento continuo de estafas relacionadas con el ciberespacio, en particular esquemas de phishing por correo electrónico y SMS, estafas de compromiso de correo electrónico empresarial pero también Ransomware"[10].

Recientemente el día 15 de junio del 2021 la empresa Mercado Libre Argentina publicó en sus redes sociales un caso de Phishing contra su marca, propagado a través de la aplicación WhatsApp:

[10] FATF (2020), *Update*: *COVID-19-related Money Laundering and Terrorist Financing – Risks and Policy Responses*,
FATF, Paris, France,
www.fatf-gafi.org/publications/methodandtrends/documents/update-covid-19-ML-TF.html

Figura 3 Tweet de la cuenta oficial de mercado libre. (2021)

3.2 Casos: Argentina 2020/2021

3.2.1 Caso: Ransomware a la Dir. Nac. de Migraciones

El ataque a un organismo del Estado con un Ransomware llamado "Net Walker" que posteriormente filtró información reservada de la Direcciona Nacional de Migraciones (DNM), de la Agencia Nacional de Inteligencia y además pasaportes de ciudadanos argentinos.

El 27 de agosto del 2020 la Dirección Nacional de Migraciones fue atacada. Los ciberdelincuentes reclamaban 76 millones de dólares por los archivos robados en criptomoneda.

El Ransomware no es nuevo como modus operandi para la seguridad informática, lo novedoso es que sea dirigido a una organización gubernamental como lo es la DNM. Se pudo averiguar mediante investigaciones posteriores que el ataque provenía de Rusia. Según el blog de seguridad informática Segu-Info. (4 de Septiembre de 2020) "La Dirección de Migraciones (AR) bajo ataque de Ransomware Net Walker (Actualizado)" [Mensaje de Blog]. Recuperado de https://blog.segu-info.com.ar/2020/08/la-direccion-de-migraciones-ar-contuvo.html?m=0

Marcó un precedente de riesgo a dependencias del Estado, donde la concientización y prevención en ciberseguridad es baja. Net Walker es un producto de software actualizado, que sus afiliados alquilan en la darkweb a cambio de un porcentaje de los fondos conseguidos mediante extorción[11].

[11] Krebs on Secutiry. (2021). *Arresto, incautaciones vinculas a NetWalker Ransomware*. https://krebsonsecurity.com/2021/01/arrest-seizures-tied-to-netwalker-ransomware/

En una investigación técnica extrajudicial realizada por Ing. Pedro Albiol (2020) deja expuesto el funcionamiento del malware "NetWalker" con pruebas de las metodologías utilizadas, como por ejemplo **"As a service"** significa que los desarrolladores no participan directamente. Solo brindan el soporte y plataforma para que otras personas (*partners*/afiliates) hagan utilización del mismo a cambio de un porcentaje (%) de las ganancias obtenidas. Los *partners* son los que realizan la infección como *insiders*, explotando una vulnerabilidad web o a través de técnicas de ingeniería social, spear phishing adjuntando un código malicioso (VBS o Powershell), etc.

Se estima que en tan solo 4 meses (entre marzo y julio) recaudaron aproximadamente 25 millones de dólares, transformándolo en el malware de mayor beneficio de la historia (Mcafee, 2020) (p.3).

Creemos de gran importancia apoyar desde la actividad académica y organizaciones del Estado este tipo de investigaciones ya que arrojan hipótesis posibles para la comprensión del funcionamiento de en este caso el Ransomware.

Albiol (2020) concluye: El ataque fue combinado y se produjo en 2 etapas.

Primero tuvo que vulnerar el sistema de la víctima con técnicas de hacking (phishing, vulnerabilidades web, intrusiones en la red, reconocimiento, movimientos laterales, elevación de privilegios, entre otros). Descargó la información, la comprimió y la subió a DropMeFiles. Finalmente, lanzó el malware en la retirada para exigir el rescate mediante ciber extorsión. (p.32)

Además, el autor se manifiesta sobre el futuro de las investigaciones donde los especialistas en laboratorio, deben utilizar el malware en cuestión para su análisis;

Albiol (2020) El análisis del malware no solo ayuda a resolver el cibercrimen, sino que también brinda importante información a los profesionales de seguridad a la hora de desarrollar mecanismos efectivos de defensa y de mitigación de riesgos. Es por ello que es importante estar atentos a los proyectos de ley que pretenden penalizar la tenencia de malware, ya que criminaliza nuestro trabajo de investigación y nuestra labor profesional diaria a la hora de proteger las infraestructuras críticas del país y a los ciudadanos. (p.34)

3.2.2 Caso: BEC a FAdeA

En el año 2021 otro ataque se concretó seguido con estafa a la Fábrica Argentina de Aviones (FAdeA), en la producción del avión Pampa IA-63 (aeronave de combate).

Con la modalidad BEC (Business Email Compromised) se robaron 480 mil dólares. Según el blog de seguridad informática Segu-Info. (7 de abril de 2021) "Roban U$S 480 mil a fábrica de aviones FAdeA mediante estafas BEC" [Mensaje Blog]. Recuperado de https://blog.segu-info.com.ar/2021/04/roban-us-480-mil-fabrica-de-aviones.html

La táctica de BEC en términos generales funciona cuando ciberdelincuentes se apropian de las cuentas de correo electrónico ajenas y dialogan con sus clientes como si fueran parte de la empresa. Así, logran desviar fondos a cuentas bancarias que ellos controlan.

Es un riesgo alto por tratarse de intrusiones persistentes en el sistema. El atacante espera el momento idóneo para atacar. Dando cuenta que algunos tipos de malware pueden infiltrarse en los sistemas y permanecer realizando espionaje.

En el caso argentino se reportó un "bug" (error) de la empresa Microsoft en un programa de mensajería[12]. También se podría tratar de un "ataque del día cero", son ataques a vulnerabilidades recientemente parcheadas (arregladas) en sistemas operativos. Los usuarios deben actualizar y reparar con parches. Se los llama de día 0 porque son nuevas vulnerabilidades de los sistemas, sin protección alguna hasta que se logre actualizar.

La intrusión en el caso FAdeA, dejó vulneradas las negociaciones del Ministerio de Defensa argentino en la fabricación de un avión de combate.

Cabe aclarar que a partir de la decisión administrativa N° 641/21 se aprobaron los "REQUISITOS MINIMOS DE SEGURIDAD DE LA INFORMACIÓN PARA LOS ORGANISMOS DEL SECTOR PÚBLICO NACIONAL", que son aplicables a todas las entidades jurisdicciones comprendidas en el inc. a) del art. 8° de la ley 24.156.

A partir de los casos mencionados el director nacional de ciberseguridad aprobó un modelo referencial de políticas de seguridad de la información. En el anexo se detalla: Objeto, Alcance, Principios Básicos, Revisión y Actualización, Lineamientos Específicos. Recuperado de https://www.boletinoficial.gob.ar/detalleAviso/primera/257620/20220216

[12] Revista Defensa. (2021). *Ciberataques de hacker estafa a la argentina FADEA cerca del medio millón de dólares*. https://www.defensa.com/cyberseguridad/ciberataque-hackers-estafa-argentina-fadea-cerca-medio-millon

La publicación de estas políticas públicas da una iniciativa y directivas claras a las organizaciones del Estado. Las mismas deberán tomar en cuentas ciertos protocolo, frente a incidentes relacionados a las TICs y el ciberespacio. Sin dudas una nueva política que se empieza a generar frente a las nuevas amenazas producidas en pandemia.

Figura 4 Campaña #BECareful: INTERPOL insta a los ciudadanos a tener cuidado con las estafas BEC**.** Interpol [13]

3.2.3 Caso: Filtración del RENAPER y IOSFA

En el mes de octubre se dio a conocer filtraciones en un foro de hacking "Raidorums.com" donde se expuso los datos del presidente de la nación, los mismos contenían DNI, fecha de nacimiento, domicilio particular, además el n° de trámite del DNI muy utilizado en pandemia por RENAPER para realizar trámites administrativos.

La filtración mostró pruebas con información y datos personales de funcionarios del gobierno y se empezó a sospechar de la posible obtención de toda la base de datos del registro nacional de las personas. A su vez el Renaper emitió un comunicado oficial sobre la filtración de datos personales de sus bases de datos, afirmando que; "El sábado 9 de octubre el Renaper tomó conocimiento de que un usuario de Twitter identificado con el nombre de @aniballeaks -cuenta que fue denunciada y que actualmente se encuentra suspendida- había

[13] Interpol (2020). Estafas a empresas por e-mail mediante suplantación de identidad (BEC, Business Email Compromise). https://www.interpol.int/es/Delitos/Delincuencia-financiera/Estafas-a-empresas-por-e-mail-mediante-suplantacion-de-identidad-BEC-Business-Email-Compromise

publicado en dicha red social las imágenes de 44 individuos, entre los cuales se encontraban funcionarios y personajes públicos de conocimiento en general”[14].

Figura 5 Usuario en foro de hacking ofreciendo base de datos del Renaper, Argentina[15].

Los datos filtrados en la red social twitter provocaron una alerta sobre la posibilidad de que sea una de las filtraciones más grande ya que se trata de los datos de los 45 millones de argentino y argentinas. Si bien a día de hoy a una investigación en curso y las comunicaciones de las instituciones oficiales no fueron claras. Apreciaron en los medios de comunicación notas al supuesto ciberdelincuente que habría realizado la filtración ofrecida en radioforums.com posteriormente. Esta acción también podría tratarse de ingeniería social ya que se presente como un adolescente mal llamado “hacker” que solo lo hacía por dinero y para divertirse. La inverosimilitud de los hechos con los comunicados solo hace pensar en los desprevenido y el nivel de desconocimiento que hay en el Estado en ciberseguridad. La protección de datos personas es un derecho que a partir de la pandemia quedó en repetidas ocasiones vulnerado como fue el caso de NetWalker (Ransomware) en Migraciones.

Además, en el mismo foro, un mes antes del caso Renaper, se había ofrecido la base de datos de IOSFA (Instituto de obra social de las Fuerzas Armadas y de Seguridad). La obra social mediante comunicado oficial el día 29/09/21 planteo: “se trata de una base de datos obsoleta e incompleta, ya que muchos de sus registros correspondían a afiliados dados de baja, muchos fallecidos y con datos faltantes. Se informa además que ya se inició la denuncia ante la Justicia Federal y la Policía Federal y la Subsecretaria de Ciberdefensa”[16] pero así mismo planteo en el comunicado “chequear” en la página web oficial y las campañas

[14] Argentina.gob.ar (2021) *El Renaper detectó el uso indebido de una clave otorgada a un organismo público y formalizó una denuncia penal*. Recuperado de https://www.argentina.gob.ar/noticias/el-renaper-detecto-el-uso-indebido-de-una-clave-otorgada-un-organismo-publico-y-formalizo

[15] Raidforums.com. (2021) Recuperado de https://raidforums.com/Forum-Databases?page=2

[16] Iosfa.gob.ar (2021). Recuperado de https://iosfa.gob.ar/novedades/132/informacion-sobre-base-de-datos-de-afiliados

actuales para no caer en posibles correos electrónicos malicioso o phishing a partir de la filtración de datos de los usuarios. Es decir, que la institución se vio vulnerada y afectada en la seguridad de la información de sus afiliados.

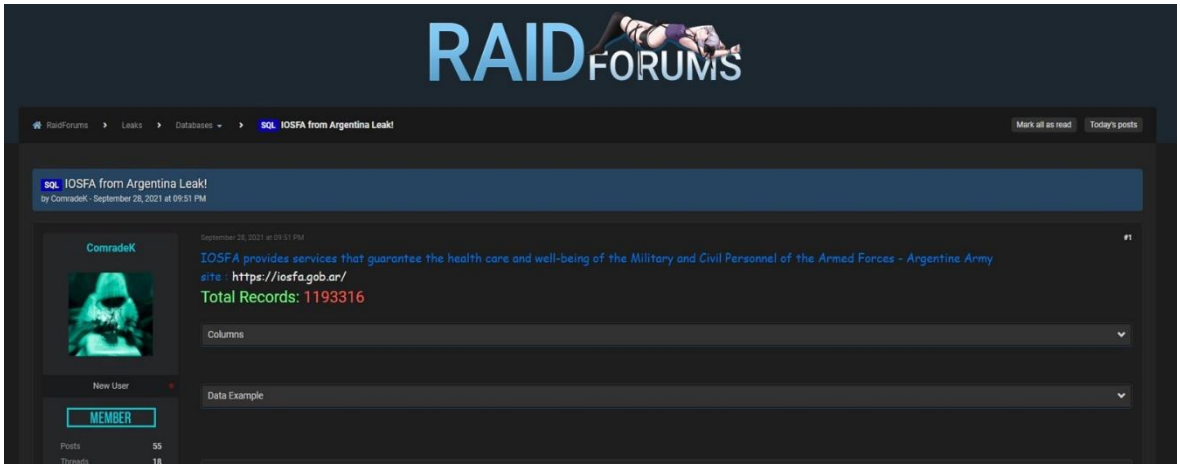

Figura 6 Usuario en un foro de hacking ofrece base de datos de IOSFA[17]

3.2.4 Caso: Ransomware en el Senado de la Nación Argentina

De manera continua a los casos anteriormente citados, a comienzo del año 2022, el día 12 de enero a las 4am horas, un Ransomware dirigido, atacó el sistema informático del Honorable Senado de la Nación Argentina.

Se intuye que el malware fue oportuno, con conocimiento de los movimientos internos ya que la cámara alta se encontraba en cese de actividades parlamentarias. Además, se habían dado movimientos del personal, el 10 de diciembre del 2021 por el recambio de los legisladores (senadores), produciendo movimientos internos en la institución. Con cambio de autoridades, nuevas designaciones y rotación (entrada y salida) de varios empleados legislativos. Simplemente se identifica este momento como “oportuno” para un

[17] Raidforum.com. (2021) Recuperado de https://raidforums.com/Thread-SQL-IOSFA-from-Argentina-Leak

ataque de tales características como un Ransomware, ya que, al finalizar el presente estudio el caso del senado está siendo investigado por la justicia argentina.

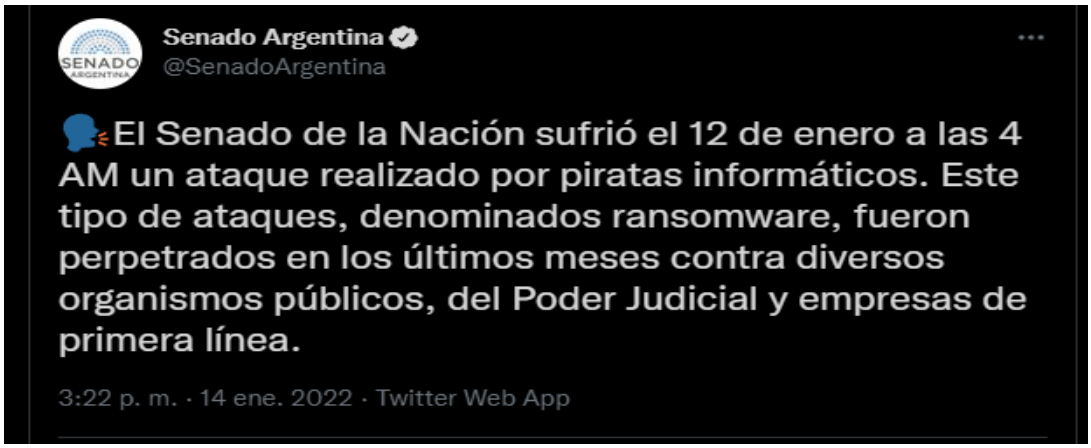

Figura 7 Cuenta oficial de twitter del Senado Argentina informando el incidente[18]

Este último caso junto con otro tipo de estafas a personalidades conocidas puso en la agenda política y mediática nuevamente el tema de la ciberseguridad. En los medios de comunicación más allá de oportunismo, se ve el desconocimiento y la confusión al hablar del ciberespacio, como puede ser la ciberdefensa y la ciberseguridad. Además de seguir hablando de “hackers” en vez de cibercriminales o ciberdelincuentes. Creemos que junto con las nuevas amenazas se tendrá que tomar a la seguridad como cultura organizacional. E irá aumentando con el paso del tiempo, es necesario aclarar que estos cambios de cultura organizacional llevan tiempo y se generan a largo plazo. Los casos de Ransomware son un problema mundial, del presente, que según los números aumentaron y argentina es víctima de esa variable, como así también lo es Estados Unidos.

Desde la dirección nacional de ciberseguridad apoyaron al senado de la nación con el fin de analizar el incidente con su grupo de CERT (Equipo de Respuestas ante Emergencias Informáticas). Son las primeras respuestas del país frente a este tipo de nuevas amenazas surgidas por la pandemia, promover buenas prácticas, capacitaciones y brindar

[18] Twitter.com (2022) cuenta oficial del Senado Argentina. https://twitter.com/SenadoArgentina/status/1482055593980571652?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1482055593980571652%7Ctwgr%5E%7Ctwcon%5Es1_&ref_url=https%3A%2F%2Fwww.diariopopular.com.ar%2Ftecnologia%2Fransomware-el-senado-las-claves-del-ciberataque-n612206

información confiable a la población es un rol clave para mitigar el efecto producido por un Ransomware u otros incidentes.

4. Propuesta de intervención

En base al problema diagnosticado más arriba sobre el phishing como protagonista, damos cuenta como resulta ser la principal técnica utilizada por los ciberdelincuentes. Esta técnica se adapta a distintos tipos de ataques, como puede ser, el robo de datos con fraudes, comercialización ilegal de información, extorción, propagación de malware, entre otras. Ofrecemos como propuesta, más prevención y concientización sobre el Phishing, que es, como se utiliza, quienes lo usan, con que fines, con el fin de que las personas logren detectar posibles robos de datos o extorsiones. Las campañas de prevención mediante distintos medios de difusión son una buena herramienta para tal fin. Los objetivos de esta propuesta tienen como objeto analizar los ataques centrales de ingeniería social en Argentina dentro del contexto de pandemia por covid-19. De esta manera, se logrará describir características metodológicas de la ingeniaría social llevada adelante por ciberdelincuentes dentro del país. Asimismo, evaluar el nivel de seguridad con el que cuenta el país, con el fin de proteger los datos personales y adaptarse a lo que viene con el progreso tecnológico, teniendo en cuenta el avance tecnológico como variante a tener en cuenta en dichas áreas.

Por otro lado, resulta imprescindible que estas campañas de seguridad puedan ser implementadas con conocimientos dados por profesionales de ciberseguridad, quienes son los que cuentan con los conocimientos idóneos para dicho fin. Y dichas campañas de ciberseguridad puedan ser brindadas tanto en un ámbito público como privado, de esta manera, la concientización llegara a más grupos sociales.

a. Estrategias de implementación

Una posibilidad de investigación es empezar a armar mesas y subgrupos de trabajo que siguen a las principales líneas de investigación vinculadas a temáticas relacionadas al cibercrimen e ingeniaría social como, por ejemplo: grooming; análisis de malware; phishing, estafas y engaños; hacking ético; Ransomware; herramientas de OSINT (Open Source Intelligence), indispensables en la etapa de recopilación de información.

Luego las investigaciones podrán ser de forma segura y siguiendo el método científico, siendo conscientes de que, en muchos casos, debemos analizar conductas del crimen organizado en internet, con las precauciones que esto implica. Buscamos identificar

el impacto de la ingeniería social utilizada con fines ilícitos, comprender el modo operatorio de los ciberdelincuentes y los factores que justifican su eficacia. También poner en evidencia el valor de nuestros datos. Luego, trataremos de observar otras variables posibles, para aprender a utilizar la ingeniería social en el área de seguridad. No hay una sola forma de ver la ingeniería social y es por este tema que al igual que el trabajo del análisis de inteligencia son necesario equipos interdisciplinarios con algún conocimiento de ciberseguridad. Un nivel de ciberseguridad adecuado requiere combinar tecnología con factor humano idóneo, por eso nos concentramos en dos ejes: capacitación y concientización.

b. Capacitación y Concientización

Las capacitaciones con fines preventivos son efectivas para advertir a las personas sobre el real poder de alcance de la IS. Por esta razón se insiste en concientizar y capacitar ya que son altos los números de personas que estuvieron ante un intento o ataque concretado. Por ejemplo, los casos de phishing enviados por email.

Ahora bien, identificamos para el público objetivo dos fases:

- Primeras Fases
    - Comunidad educativa:
    - Personal docente;
    - Personal no docente;
    - Estudiantes;
    - Graduados;
    - Investigadores

- Siguientes fases:
    - Personal del sector privado y público que requiera capacitación o concientización

c. Recomendación de Legislación

A partir del estudio realizado sería bueno, contar con campañas nacionales de prevención en cibercrimen e Ingeniería Social. Poner el tema en una agenda para desde el poder ejecutivo tener herramientas para mitigar efectos. Generando tanto en las

organizaciones del Estado como en las privadas la necesidad de la “cultura en ciberseguridad” y la correspondiente concientización sobre la exposición de las personas. A partir de nuestro estudio recomendamos ejes para posible legislación en el ámbito nacional. Que cuenta con un programa nacional de concientización. El mismo tendrá como objetivo prevenir, sensibilizar y generar conciencia en la población sobre la problemática del cibercrimen y la IS, a través del uso de las TICs. La educación y el conocimiento de esta nueva forma de delitos en la sociedad, apuntan a protegerse a sí mismos a terceros y posibilita la mitigación de los efectos causados.

- Creación del Programa Nacional de Prevención y Concientización del Cibercrimen y la Ingeniería Social como Actividad Engañosa;

Con los siguientes fines y objetivos:

- Generar conciencia sobre el uso de técnicas y herramientas tanto como el Phishing, Vishing, Ransomware o ingeniería social (maliciosa) utilizada en el territorio nacional.
- Garantizar la autoprotección de la privacidad como así también la violación física y de datos virtuales.
- Capacitar a la comunidad en general y a los tres poderes del Estado, Poder Ejecutivo, Poder Legislativo y Poder Judicial Nacional.
- Diseñar y desarrollar campañas de difusión de comunicación a los fines de cumplir con los objetivos del presente Programa.
- Brindar información acerca del funcionamiento del cibercrimen y como denunciar este tipo de delitos en la justicia.
- Generar estadísticas nacionales sobre ataques concretados.
- Informar a los usuarios sobre las buenas prácticas de seguridad.
- Diseñar las capacitaciones necesarias por áreas a fines, desde la informática, bases de datos personales, cuentas bancarias, atención al público, seguridad interior, ciberdefensa, etc. Cada poder del Estado o institución podrá evaluar sus requerimientos principales.
- Crear un órgano de consulta con las universidades nacionales y comunidades científicas que tengan conocimientos sobre la temática.

Además, recomendamos la creación de una página web del Estado argentino con información referida al cibercrimen y ataques de ingeniería social que se hayan concretado, con el fin de obtener estadísticas, destinado a la población en general y a la comunidad educativa, con el fin de que obtengan material de información, chat o foros sobre experiencias de las víctimas, acción de prevención e información confiable en general.

Actualmente la Direcciona Nacional de Ciberseguridad público en el Boletín Oficial un documento llamado “Modelo Referencial de Políticas de Seguridad de la Información” se trata de lineamiento que deberá seguir los organismos públicos para implementar obligatoriamente la seguridad de sus activos informáticos. Estas políticas junto con la concientización van en una nueva línea de una cultura organizacional para la seguridad de la información en el ámbito estatal. Por otro lado, se identifica que no hay una política clara que apunte a reducir los casos de ingeniería social.

5. Conclusiones

A modo de cierre, retomaremos el interrogante inicial del presente estudio, nuestro interrogante inicial fue: ¿Cuál es el impacto de la ingeniería social en organizaciones estatales de Argentina a partir de la pandemia producida por el COVID-19?

La presente investigación tuvo como objetivo, analizar e identificar una realidad nueva y poco investigada mediante método científico. La misma intentó ampliar el conocimiento acerca de una compleja modalidad utilizada por el cibercrimen en pandemia. Intentando aportar una mirada posible a estudios que se realicen en el futuro, sumando al conocimiento académico y a los profesionales pertenecientes a la comunidad científica. Nos propusimos indagar sobre sobre una actividad poco explorada como es el caso de la ingeniería social en Argentina. El trabajo se legitimó, asimismo, por la significación social que tiene el cibercrimen hoy en el país. La posibilidad de aportar un conocimiento nuevo que ayude a la prevención y concientización del problema. Además, comprender el mecanismo de los procesos convergentes. Siendo este un contexto particular, de emergencia a partir de la pandemia (covid-19), que invitó al autor a realizar la investigación.

Según el análisis mencionado, hecho por la "Asociación Argentina de Lucha Contra Cibercrimen" sobre consulta de delitos informáticos en Argentina entre: el 20 de marzo de 2020 al 1 de julio del 2020. Se describen como principales el ciberbullying, fraude, extorción y phishing. El Phishing como principal técnica utilizada por los ciberdelincuentes para dichos fines, la falta de concientización peligra los datos privados de las personas, los casos mencionados ayudan a dar cuenta de dichos delitos. El presente estudio nos ayudó a darnos cuenta como las personas de forma particular no resultan ser las únicas propensas a sufrir la ciberdelincuencia, sino también, grandes corporaciones, como el caso de Mercado Libre o la base de datos de Renaper.

El contexto de pandemia ha peligrado los ataques de Ingeniería Social, estos ataques fueron posibilitados por los acelerados procesos de transformación tecnológica demandados, se generaron mayor uso de internet, con la nueva modalidad del "teletrabajo" que arrojo a las personas a trabajar de sus casas con redes públicas y o privadas. Las TICs tuvieron un papel fundamental. Como recurso básico, la conectividad se trasformó en un servicio indispensable para la población. Para muchas personas fue un momento nuevo, de

aprendizaje e incertidumbre. No así para el cibercrimen que, rápidamente observó la situación como oportunidad favorable.

Retomando a R. Layton & P. Watters (2016) el anonimato en internet es un beneficio para los cibercriminales y una desventaja para las investigaciones judiciales, dada la imposibilidad de poder arribar a los delincuentes reales de dichas extorciones. Entendemos a internet como la red más grande del mundo, donde millones de operaciones, comunicación se ejecutan constantemente alrededor del mundo. La ciber vigilancia existe con norma recientemente aprobada en argentina bajo la figura de "ciberpatrullaje", Resolución 144/2020. Por lo cual, resulta imprescindible seguir una línea de concientización a nivel provincial como nacional sobre esta resolución.

Las políticas adoptadas mediante decisión administrativa por la Dirección Nacional de Ciberseguridad (Disposición 1/2022) advirtiendo y generando protocolos de seguridad para resguardad los activos informáticos del Estado son una iniciativa frente a esta nueva amenaza. Muchas políticas que se empezaban a implementar tuvieron que adelantarse, los sucesivos casos de ataques obligaron a tomar directivas claras en las organizaciones del Estado. Algunas de las políticas de seguridad a implementar son:

- Un organismo o área responsable de la seguridad de la información que coordinará y velará por el cumplimiento de la política.
- Seguridad de la información de los recursos humanos. Es decir, capacitar y concientizar a los empleados y funcionarios.
- Gestión de activos dentro del organismo. Esto incluye hardware, software, dispositivos de comunicación, dispositivos de apoyo, así como de la propia información y los datos.
- Autenticación, autorización y control de acceso. Este punto está vinculado con la gestión de privilegios para administrar adecuadamente el acceso a la información para que se tenga acceso a lo necesario para desempeñar las funciones.
- Uso de herramientas criptográficas para proteger la información que manipula el organismo, sobre todo cuando se transmite hacia y desde afuera.
- Implementación de medidas de seguridad y monitoreo con relación al acceso físico a la información.
- Seguridad operativa

- Seguridad de las comunicaciones. La política debe establecer las medidas necesarias para proteger la información que se comparte a través de sus redes informáticas para minimizar los riesgos.
- Adquisición de sistemas, desarrollo y mantenimiento de sistemas de información.
- Relación con proveedores
- Gestión de incidentes de seguridad. Lo cual habla de la importancia de establecer medidas para prevenir, detectar, gestionar y resolver un incidente de seguridad que afecte a la información.
- Aspectos de seguridad para la continuidad de la gestión. Esto significa realizar análisis de impacto, establecer formas de recuperación para garantizar la continuidad, sobre todo en el caso de información o servicios críticos.
- Cumplimiento

Llevará tiempo generar que las mismas sean parte de la cultura de las organizaciones, concientizando a sus trabajadores y generando nuevas prácticas de seguridad. Pero es una buena iniciativa.

La ingeniería social tiene un alcance inimaginable no se reduce a una estafa de phishing como ya lo planteamos. Puede darse con fines de espionaje político, campañas de desinformación para perjudicar personas o instituciones. Las fakes news del futuro son las nuevas Deep fakes, que seguramente necesitaremos contar mayor análisis para poder discernirlas ya que serán copias exactas de imágenes y voces de personas mediante inteligencia artificial. El posible peligro que se manifiesta hoy, es que muchas personas tomarán o validarán como cierto algo que no lo es.

Los gobiernos democráticos, hoy se encuentran ante el desafío de desmentir fake news y los analistas de información chequear y usar herramientas para analizar una imagen o video, antes de dar como cierta una información. Las redes sociales viralizan o exponen campañas donde una fuga como la del RENAPER expone los datos personales del presidente de la nación.

El abordaje es amplio, pero debe empezar por lo primero y es advertir a las personas de la velocidad con la que se comparte la información, además del avance tecnológico y las distintas metodologías del cibercrimen junto con la ingeniería social.

Los analistas ya no solo deberán manejar información si no estar actualizados de cuáles son las nuevas metodologías del ciberespacio. Con que herramientas de geolocalización contamos, cómo para dar por cierto una imagen o encontrar una persona

perdida, entre otras cosas. Hoy las investigaciones de OSINT apuntan a esto. Habilidades para una investigación civil más activa y conscientes de las medidas activas que se emplean en el nuevo mundo globalizado por internet y las tecnologías de la comunicación.

El nuevo mundo genera inmediatez para legislar, educar, prevenir y concientizar sobre el poder de las nuevas tecnologías. No debemos retroceder ante ellas, o generar tecnofobia, pero si trabajar para estar a la altura de las circunstancias que nos demande la sociedad.

Los engaños, extorción, robos y estafas por estas metodologías ya son parte de nuestra cotidianeidad. Todas y todos somos vulnerables, nadie puede decir estar cien por ciento seguro al día de hoy.

Además del factor humano se tendrá que tener en cuenta la responsabilidad de las empresas que fabrican nuevas tecnologías, diseñadores de software o programadores para contar con dispositivos seguros que sumados a la concientización del factor humano ayuden al progreso del factor tecnológico. Siendo los dispositivos más seguros en la nueva era digital, ya que muchas veces sus “bugs” errores dejan las puertas abiertas para la explotación de vulnerabilidades. De esta manera se podrá ir reduciendo los riesgos y posteriores consecuencias, como las citadas en esta investigación.

6. Referencias bibliográficas

Libros y Artículos de Revistas científicas

- Albiol, P. (2020). *"Netwalker afectación a migraciones Argentina".* Argentina, SeguInfo: Investigaciones.

- Arias, F. (2006). *El Proyecto de investigación: Introducción a la metodología científica* (5a ed.). Caracas: Episteme.

- Grimes, R. (2018). *Hackear al Hacker. Aprende de los expertos que derrotaron a los hackers*. España. Marcombo.

- Gómez Vieites, A.(2014). *Enciclopedia de Seguridad Informática*. 2°Ed. Madrid: RA-MA.Editorial.

- Hadnagy, C. (2011). *Ingeniera Social. El arte del hackin personal*. Madrid. Ediciones ANAYA MULTIMEDIA.

- Layton, R and Watters, P. (2016). *"Automating Open Source Intelligence Algorithms for OSINT".* USA, Elsevier Inc.

- Ramos Varón, A., Barbero Muñoz, C, A., Murgán Rodriguez, D., Gonzalez Durán, I., (2015). *Hacking con ingeniería Social. Técnicas para hackear humanos*. Madrid: RA-MA Editorial.

- Spadaro, J. R. (2016). *Inteligencia aplicada, crimen trasnacional y derecho público.* Buenos Aires: Autores de Argentina.

- Stel, E. (2005). *Guerra Cibernetica.* Buenos Aires: Círculo Militar.

- Watson, G., Mason., A, Ackroyd., R. (2014) *Social Engineering Penetration Testing Executing Social Engineering Pen Tests, Assessments and Defense.* USA: Syngress is an imprint of Elsevier

Referencias de Tesis

- Méndez Carvajal, A. (2018). Estudio de Metodologías de Ingeniería Social (Tesis de Maestría) Universitat Oberta de Catalunya, España.

Citas de páginas web

- Asociacion Argentina de Lucha Contra el Cibercrimen (2020). *Fuerte Crecimiento de Delitos Informáticos en Cuarentena.* Buenos Aires. Recuperado de https://www.cibercrimen.org.ar/2020/07/08/fuerte-crecimiento-de-delitos-informaticos-en-cuarentena/

- Boletín Oficial de la República Argentina (2020). Ministerio de Seguridad. Resolución 114/2020. Recuperado de https://www.boletinoficial.gob.ar/detalleAviso/primera/230060/20200602

- Boletín Oficial de la República Argentina (2022). Dirección Nacional de Ciberseguridad. Disposición DI-2022-1-APN-DNCIB#JGM. Recuperado de https://www.boletinoficial.gob.ar/detalleAviso/primera/257620/20220216

- *El Renaper detectó el uso indebido de una clave otorgada a un organismo público y formalizó una denuncia penal. (2021).* Recuperado de https://www.argentina.gob.ar/noticias/el-renaper-detecto-el-uso-indebido-de-una-clave-otorgada-un-organismo-publico-y-formalizo

- *Información sobre base de datos de afiliados (2021).* Recuperado de https://iosfa.gob.ar/novedades/132/informacion-sobre-base-de-datos-de-afiliados

- ¿Qué es la triada de la CIA? (2019). Recuperado de https://www.computerweekly.com/es/opinion/Que-es-la-triada-de-la-CIA

- *¿Qué es OSINT? Usos y beneficios de aplicar este sistema para recopilar información. (2019).* Recuperado de https://ciberpatrulla.com/que-es-osint/

- Secretaria General de Interpol (2020*). Ciberdelincuencia: efectos de la covid-19.* Lyon, France. Recuperado de https://www.interpol.int/es/Noticias-y-acontecimientos/Noticias/2020/Un-informe-de-INTERPOL-muestra-un-aumento-alarmante-de-los-ciberataques-durante-la-epidemia-de-COVID-19

- *Seis pasos para no caer en el "arte del engaño"*. (2020). Recuperado de https://www.harvard-deusto.com/seis-pasos-para-no-caer-en-el-arte-del-engano

- *Venta de datos personales en foro, RENAPER Y IOSFA (2021).* Recuperado de https://raidforums.com/Forum-Databases?page=2 https://raidforums.com/Thread-SQL-IOSFA-from-Argentina-Leak

- Cuenta oficial del Senado Argentina. (2022). Recuperado de https://twitter.com/SenadoArgentina/status/1482055593980571652?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1482055593980571652%7Ctwgr%5E%7Ctwcon%5Es1_&ref_url=https%3A%2F%2Fwww.diariopopular.com.ar%2Ftecnologia%2Fransomware-el-senado-las-claves-del-ciberataque-n612206

7. Anexos

7.1 Instrumento entrevista semi-dirigida

1. ¿Qué es para usted la Ingeniería Social?
2. ¿Cuál fue el impacto de la IS en la pandemia?
3. Según su criterio, ¿cómo es el desempeño de la legislación argentina en materia de cibercrimen? Puede explicarlo, por favor.
4. ¿Según su punto de vista, hay incentivo a desarrollar una carrera profesional para mitigar nuevas ciberamenazas?
5. ¿Cómo considera usted a las políticas publico/privadas frente a la IS? Fundamente su respuesta.
6. ¿Conoce normas o procesos que hayan provocado un avance en cibeseguridad? Si es así, ¿en qué y por qué?
7. ¿Considera Usted que hay interés en tener y mantener un equipo interdisciplinario para pensar el ciberespacio? Fundamentar
8. ¿Alguna vez sufrió ataques de IS?
9. ¿Cuál es a su criterio la mayor motivación de un ciberdelincuente?
10. ¿Reconoce un buen trabajo de concientización y prevención por parte del Estado?
11. ¿A qué se deben las reiteradas filtraciones como vimos en el caso del Renaper?
12. ¿Tuvo situaciones indeseadas producidas por la pandemia en cuanto al ciberespacio? Explique por favor qué consecuencias tuvo.
13. ¿Cómo ve a futuro, en unos 10 años a la IS?
14. Según su punto de vista, a que se deben las ultimas y continuas fugas de información y posterior publicación en foros web (Renaper)
15. ¿Cómo cree usted que se podría resguardar a las personas frente a la IS y el avance tecnológico?

Entrevista sobre Ingeniería Social. Elaboración propia. Antin (2021), Buenos Aires.

ENTREVISTA ANÓNIMA A ESPECIALISTAS EN IS

Nombre: Jorge

Edad: 44

Cargo/Trabajo: Colaborador de la Justicia, Analista de Cibeseguridad, Docente, Consultor Privado.

¿Qué es para usted la Ingeniería Social?

Es el conjunto de técnicas que se utilizan para obtener información mediante manipulación o arbitrando métodos de análisis para entender el comportamiento de la víctima y poder utilizarlo en su contra.

¿Cuál fue el impacto de la IS en la pandemia?

La pandemia hizo evidente la eficacia de la aplicación de técnicas de ingeniería social, no solo porque los casos se incrementaron, sino que también a la disponibilidad de las personas frente a los dispositivos conectados aumento.

Según su criterio, ¿cómo es el desempeño de la legislación argentina en materia de cibercrimen? Puede explicarlo, por favor.

Argentina viene avanzando respecto a las normativas y en comparación con el mundo, si bien se focaliza en delitos relacionados a menores, se está trabajando en la concientización de adoptar medidas reglamentarias para mermar la cantidad de delitos vinculados al ciberespacio.

¿Según su punto de vista, hay incentivo a desarrollar una carrera profesional para mitigar nuevas ciberamenazas?

Creo que hay poco incentivo en el desarrollo de carreras profesionales, el principal seria el económico y la realidad es que están muy mal pago.

¿Cómo considera usted a las políticas publico/privadas frente a la IS? Fundamente su respuesta.

Muy malas, se tiene conciencia de la metodología, pero las políticas de implementación con muy pobres debido a la falta de conocimiento sobre el funcionamiento de la ingeniería social, y el alcance mas que nada.

¿Conoce normas o procesos que hayan provocado un avance en cibeseguridad? Si es así, ¿en qué?

Hay avances respecto a la concienciación sobre el impacto negativo de los ataques, pero, por ejemplo, la aplicación de las normas ISO 27001 son optativas, por lo que estamos algunos pasos atrasados a otros países que ya implementan las normativas como un todo en gestión de riesgo. Argentina viene desarrollando mas núcleos educativos respecto a la temática pero poca normativa.

¿Considera Usted que hay interés en tener y mantener un equipo interdisciplinario para pensar el ciberespacio? Fundamentar

Seguro que hay interés, pero los bajos presupuestos hacen que una sola persona deba ocupar varios puestos. El problema no esta en el trabajo en equipo, sino en que cuesta hacer entender que la ciberseguridad no es un nicho técnico únicamente. Es mas un licenciado en sistemas, poco sabe de seguridad informática.

¿Alguna vez sufrió ataques de IS?

Si, técnicas de clonado de tarjeta de débito.

¿Cuál es a su criterio, la mayor motivación de un ciberdelincuentes?

El poco control.

¿Reconoce un buen trabajo de concientización y prevención por parte del Estado?

NO malísimo.

¿A qué se deben las reiteradas filtraciones como vimos en el caso del Renaper?

A posibles campañas de desprestigio al estado y espionaje político.

¿Tuvo situaciones indeseadas producidas por la pandemia en cuanto al ciberespacio? Explique por favor.

NO

¿Cómo ve a futuro, en unos 10 años a la IS?

En crecimiento.

Según su punto de vista, a que se deben las ultimas y continuas fugas de información y posterior publicación en foros web

A lo que respondí en la pregunta 11

¿Cómo cree usted que se podría resguardar a las personas frente a la IS y el avance tecnológico?

Son dos cosas totalmente diferentes, el avance tecnológico diría que nada que ver tiene con el avance de la IS, se puede hacer esto sin necesidad de tecnología.

Universidad de Buenos Aires
Facultad de Ciencias Económicas
Escuela de Estudios de Posgrado

Solicitud de evaluación de TRABAJO FINAL DE ESPECIALIZACIÓN (TFE)	Código de la Especialización
Nombre y apellido del alumno Miguel Antin	Tipo y N° de documento de identidad 33315642
Año de ingreso a la Especialización – Ciclo 2020	Fecha de aprobación del TFE en el Taller Agosto 2021

Título del Trabajo Final

Impacto de la Ingeniería Social en Argentina a partir de la Pandemia producida por COVID-19

Solicitud del docente a cargo del Taller

Comunico a la Dirección de la Especialización que el Trabajo Final bajo mi tutoría se encuentra satisfactoriamente concluido. Por lo tanto, solicito se proceda a su evaluación y calificación final.

Firma del docente ……

Aclaración……

Lugar y fecha……

Datos de contacto del Tutor	
Correo electrónico	Teléfonos

Se adjunta a este formulario:

- Trabajo Final de Especialización impreso (indicar cantidad de copias presentadas)
- CD con archivo del Trabajo Final en formato digital (versión Word y PDF)
- Certificado analítico

Fecha	Firma del alumno

Form. TFE v1

PRESENTAR EN LA RECEPCIÓN DE LA ESCUELA DE ESTUDIOS DE POSGRADO

Universidad de Buenos Aires
Facultad de Ciencias Económicas
Escuela de Estudios de Posgrado

INFORME DE EVALUACIÓN DEL TRABAJO FINAL INTEGRADOR DE LA ESPECIALIZACIÓN EN INTELIGENCIA ESTRATÉGICA Y CRIMEN ORGANIZADO – (097 - FCE – UBA)

Alumno: Lic. Miguel ANTIN (cohorte 2020)

Título TFI: ***Impacto de la Ingeniería Social en Argentina a partir de la Pandemia producida por COVID-19***

Evaluador: Natalio Francisco CIMA

Criterios:

1. Conocimiento del tema:

El alumno demuestra un amplio conocimiento del tema tratado, que se demuestran en el desarrollo del marco teórico.

En el mismo aborda los ejes centrales de la cuestión planteada, como ser: La ingeniería social (IS); Principales ataques de IS; Legislación Argentina; Pandemia y cibercrimen; Casos reales (Covid-19); El anonimato en internet; La seguridad de la información Pen-testing e IS.

En estos aspectos abordados, el alumno describe las actividades de actores criminales, que utilizando herramientas de ingeniería social en el ciberespacio, se puede ocasionar daño a organizaciones gubernamentales o no gubernamentales.

Dejando así en relieve, una vulnerabilidad que se vio aumentada a partir del aislamiento obligatorio por la pandemia COVID-19.

2. Actualización del Diagnóstico:

A través del método de recolección de información de entrevista semidirigida (cuestionario), logró obtener de especialista en la materia, una descripción de las principales falencias y vulnerabilidades.

Así también, al someter los casos puntuales de ataques, al tamiz del marco teórico, logra abordar de forma clara y sobre todo resalta el nivel de vulnerabilidad frente a delitos de cibercrimen, a través de la ingeniería social.

3. Pertinencia y coherencia de la propuesta de intervención:

La propuesta descriptiva, es muy pertinente, pues aborda una problemática no considerada en su plenitud previo al aislamiento obligatorio por la Pandemia, si no después de ello.

Es así, como obtiene la coherencia necesaria, pues pone de manifiesto la falta de previsión para estos tipos de delitos.

5. Análisis del TFI

El trabajo refleja un análisis de un escenario que demostró la fragilidad de una sociedad, que todavía no afianzo su manejo de la tecnología, o al menos parte de ella.

La actividad de inteligencia, o más preciso de contrainteligencia, es la encargada de analizar posibles vulnerabilidades y proponer los cambios para que ellas no sucedan.

Por lo cual, como futuro especialista en análisis de inteligencia estratégica y crimen organizado, logró a partir del presente, un análisis pertinente.

5. **Propuesta de calificación numérica**: nueve (9) – Distinguido.

INTERVENCIÓN DEL PROFESOR DE TALLER DE TRABAJO FINAL INTEGRADOR, Mg JOSE LUIS PIBERNUS.

- El TFI evaluado, reúne los procedimientos de metodología de investigación exigidos para el nivel académico de la carrera.
- Cumple con la Guía de la FCE establecida para TFE y con el Reglamento de Posgrado de la UBA.
- Se advierte una excelente integración de contenidos de distintas áreas del posgrado, que le dan un excelente anclaje disciplinar, todo ello frente al complejo problema del lavado de activo como principal actividad del crimen organizado.
- La propuesta de intervención es totalmente coherente con el diagnóstico presentado.
- Propuesta de Calificación: DISTINGUIDO, NUEVE (9).

INFORME FINAL DE EVALUACIÓN DEL DIRECTOR DE LA ESPECIALIZACIÓN EN INTELIGENCIA ESTRATEGICA Y CRIMEN ORGANIZADO:
Adhiero a los informes precedentes y a sus estimaciones.

Juicio concreto: El Licenciado Antin ha realizado un aporte valioso para la comprensión técnica de temas no sencillos para el lector no familiarizado con estos tópicos y en ello radica lo mejor de este trabajo. Supo conciliar conocimiento adecuado con descripción sencilla y accesible. Esa condición del presente TIF lo emplaza como de interés a la capacitación de los especialistas en esta carrera. Por ello, le sugiero que luego de algunos ajustes de sintaxis (en especial cuando caracteriza algunos aspectos de la ingeniería social, donde no conviene dar por sentado la inmediata comprensión del lector de todos los enunciados) publique su TIF ya sea como un manual introductorio o bien avance a mayores contenidos. Destaco el esfuerzo excelente de esta presentación.
Calificación: DISTINGUIDO (NUEVE) 9. -

Dr. José Ricardo Spadaro
Dir Esp en Icia Est y Crim Org
(097) – ENAP-FCE-UBA