Universidad de Buenos Aires

Facultades de Ciencias Económicas, Cs. Exactas y Naturales e Ingeniería

Carrera de Especialización en Seguridad Informática

Trabajo Final

Título: Las Técnicas de Ingeniería Social y su incidencia en la seguridad de las organizaciones actuales.

Autoría: Lic. Gabriela Victoria Musso

Tutoría del Trabajo Final: Dr. Juan Pedro Hecht

Año de Presentación: 2019

Cohorte: 2017

Declaración Jurada de origen de los contenidos:

“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”. Al pié de la misma el autor debe firmar en forma manuscrita, en todos los ejemplares impresos entregados, aclarando a continuación sus Nombres y Apellidos y el número de documento personal que lo identifica. Los ejemplares electrónicos entregados incluirán la leyenda “FIRMADO” en lugar de la firma hológrafa.

Resumen – Palabras clave
Abstract – Key Words

El presente Trabajo Final de Especialización, se enfoca en una investigación académica, descriptiva y analítica sobre los conocimientos relacionados a los distintos tipos de Técnicas de Ingeniería Social (en adelante TIS), desde un punto de vista técnico y social, de las que pueden ser víctimas los dos activos más importantes de una organización: sus recursos humanos y, en consecuencia, la información que estos generan.

Ante la ineludible necesidad de capacitar a los integrantes de una organización para que puedan identificar fácilmente las técnicas engañosas más utilizadas, se presenta se expondrán las principales formas de prevenir las técnicas más comunes, complementando con los principales ítems en los que se debe capacitar al personal en campañas de concientización.

Se pretende, acorde estas bases, asesorar al área de Gerencia para que tome la responsabilidad de asegurar que los empleados, contratistas y terceras personas, estén al tanto de las amenazas e inquietudes más frecuentes, cumplan son sus responsabilidades y sean idóneos para los roles asignados, en cuanto a la gestión de la seguridad de la información.

En términos generales, entender cómo generar una gestión eficaz y consistente de los incidentes de seguridad de la información de la organización, con el objetivo de evitar la pérdida, el daño o compromiso de los activos, la interrupción de las actividades, la divulgación no autorizada, modificación, borrado o destrucción de datos e información de la misma, a causa de estas técnicas; más allá de la correspondencia con las leyes, requerimientos comerciales, y regulaciones relevantes de seguridad existentes.

Técnicas – Ingeniería Social – Manipulación – Victima/Victimario - Engaño – Información.-

Índice

Introducción.

La seguridad informática y el cibercrimen han cobrado un papel muy importante en las últimas décadas, sobre todo desde la irrupción del teléfono, durante la década del 60, y con las primeras computadoras durante la década del 70. A raíz del avance del uso de Internet y las redes de comunicaciones, resulta necesario poner especial énfasis en las técnicas de ingeniería social que utilizan hoy en día los especialistas para llevar a cabo sus ataques o para realizarlos directamente a través de las personas.

Los métodos expuestos en el presente trabajo, han ido evolucionando en materia tecnológica, así como la manipulación engañosa también se ha ido perfeccionando a través del tiempo. Tal es así que algunas técnicas surgieron debido auge de las nuevas tecnologías y medios de comunicación.

El presente, abarca el desarrollo de las técnicas que utilizan los Ingenieros Sociales, los métodos más utilizados para obtener información, el tipo de información que puede obtenerse y cómo se utiliza, pudiendo ser beneficiosa para el victimario o comprender un acto delictivo, planteado siempre en el contexto de las organizaciones y su personal.

La seguridad de la información es una parte integral de los sistemas de información durante su ciclo de vida, es una necesidad global independiente de la tecnología, por lo que es importante que las empresas estén alertas. La desinformación o el desconocimiento los puede llevar a ser víctimas de atacantes que tengan como objetivo principal vulnerar sistemas informáticos y/o obtener determinada información organizacional a través de diferentes técnicas.

El objetivo principal del presente trabajo, es proporcionar información detallada, generando conciencia y conocimiento sobre los engaños informáticos, describiendo los distintos tipos de ataques perpetrados mediante el uso de las Tecnologías de la Información y de la Comunicación, que pueden recibir los integrantes de diversas organizaciones a la hora de operar, mediante cualquier tipo de dispositivo electrónico, usuario, clave y/o sistemas organizacionales.

Sustancialmente, resulta necesario:

- Ampliar la noción de las personas operarias de dispositivos digitales,

sean o no profesionales de la informática, realizando un análisis integral de las interacciones técnicas y sociales que se presentan comúnmente y los riesgos que representan para las organizaciones, estableciendo una base holística, descriptiva y analítica, para su prevención.

- Describir en forma sinérgica, las principales formas de evitarlas, utilizando como referencia campañas de concientización reales.
- Diseñar material de apoyo para el área de seguridad informática de la organización, con el objetivo de orientar a profesionales de seguridad y/o a personas que ejerzan cargos a nivel gerencial en la toma de decisiones; o a quienes deseen perfeccionar sus conocimientos y/o habilidades en materia de Seguridad de la Información.

1. Técnicas de Ingeniería Social. Definición y apreciaciones.

Según la compañía internacional de seguridad informática Kasperski lab[1], "La ingeniería social es un conjunto de técnicas que usan los cibercriminales para engañar a los usuarios incautos para que les envíen datos confidenciales, infecten sus computadoras con malware o abran enlaces a sitios infectados. Además, los hackers pueden tratar de aprovecharse de la falta de conocimiento de un usuario; debido a la velocidad a la que avanza la tecnología, numerosos consumidores y trabajadores no son conscientes del valor real de los datos personales y no saben con certeza cuál es la mejor manera de proteger esta información" [1]

En base al concepto anterior, se puede señalar que la ingeniería social está sujeta a que, por medio de canales digitales o informáticos, se efectúe manipulación de personas, en forma metódica, mediante la persuasión, la persuasión, con el objetivo de eludir los sistemas de seguridad, y con miras a obtener información de los usuarios. Se podría efectuar mediante una gran cantidad de herramientas informáticas disponibles, como internet, teléfono, correo electrónico, correo tradicional o contacto directo.

Su objetivo principal, es crear una situación creíble, confiable, sin dejar ningún elemento librado al azar. El éxito del ataque depende del comportamiento del receptor, ya que este, involuntariamente puede contribuir a que el engaño efectivamente se produzca. La precaución de los usuarios de sistemas informáticos, resulta indispensable para frenar o evitar la propagación de una campaña de ingeniería social.

A partir de los años 70, se comenzaron a ejecutar estas técnicas, mediante llamados telefónicas, emulando ser entidades que otorgaban un determinado tipo de servicio, (método que no ha dejado de existir en la actualidad). La finalidad de este llamado era recabar información sobre la víctima [2]. Actualmente, con la llegada de Internet a los hogares, los victimarios abarcan un espectro más amplio. Buscan engañar a las personas para que entreguen voluntariamente información propia. La mutación se dio

[1] Kaspersky Lab, es una compañía internacional de seguridad informática con presencia en aproximadamente 200 países del mundo.

no sólo hacia sitios web, sino también se ha trasladado a mensajes de texto, incluyendo cualquier medio de mensajería móvil, a través de mensajería tradicional, redes sociales, hasta juegos en línea. La importancia de este vector de ataque radica en que los dispositivos móviles almacenan gran cantidad de información personal, como contactos, fotos, conversaciones, usuarios y contraseñas de bancos, redes sociales, correos electrónicos, inclusive información sobre geo localización.

Acorde datos brindados por el INDEC[2] [3], en Argentina, en los meses de julio, agosto y septiembre de 2017 crecieron los accesos a internet, respecto al mismo mes del año anterior 12,7% (julio), 7,4% (agosto) y 6,3% (septiembre).

Entre septiembre de 2017 –último mes del trimestre mencionado– y el mismo mes de 2016 se observó que los accesos móviles (pospagos) de organizaciones aumentaron 7,6% y representaron 84,0% del total de accesos de organizaciones, mientras que para el mismo período los accesos fijos disminuyeron levemente 0,3% y representaron 16,0% del total.

En este escenario, podemos observar que las organizaciones fueron convergiendo a accesos más flexibles, sin necesidad de una conexión en un lugar físico permanente (oficina, casa, etcétera). Las organizaciones esperan que sus integrantes puedan cumplir con sus compromisos en su casa, oficina u otro espacio, que no sea físicamente el de la empresa, lo que produce, en ocasiones que los miembros de las organizaciones tengan que usar sus propios dispositivos [2]; implicando tener acceso a los datos de la compañía en cualquier lugar y/o punto de conexión con acceso a la red.

Resulta de suma importancia tener en cuenta que el factor que determina la seguridad del hardware y el software es el humano, más allá de todas las soluciones y medidas de seguridad que puedan implementarse en la empresa. Por lo expuesto, puede afirmarse que cualquier política de seguridad empresarial es tan fuerte como lo sea el conocimiento de sus empleados en materia de seguridad informática. De manera que sea por acción u omisión, el usuario es el eslabón más vulnerable de la cadena de seguridad, por lo que el desconocimiento de técnicas básicas para securizar

[2] Instituto Nacional de Estadística y Censos (INDEC).

correctamente la información y el mal uso de las herramientas de protección informática, incrementan las brechas de seguridad.

Las técnicas que usan los cibercriminales para engañar a los usuarios suelen ser multifacéticas. Además, existen variedad de métodos y medios físicos, informáticos y sociales que permiten ejecutar ataques de ingeniería social; algunos no requieren de un gran equipamiento y otros involucran equipamiento de alta tecnología que funcione acorde su fin.

2. Clasificación.

A continuación, se desarrollarán, acorde la bibliografía analizada, las técnicas más importantes, cómo funciona cada una y como prevenir que se propaguen en su campo de acción.

Se pretende, acorde el conocimiento de estas bases, asesorar para que los recursos humanos internos o externos de una organización, estén al tanto de las amenazas e inquietudes existentes, cumplan son sus responsabilidades y sean idóneos para los roles asignados, en cuanto a la gestión de la seguridad de la información.

2.1. Phishing

A los efectos de abordar esta técnica se tendrán en cuenta las siguientes definiciones:

Según Avast[3], "el phishing es un método que los ciberdelincuentes utilizan para engañarle y conseguir que revele información personal, como contraseñas o datos de tarjetas de crédito y de la seguridad social y números de cuentas bancarias. Lo hacen mediante el envío de correos electrónicos fraudulentos o dirigiéndole a un sitio web falso". [4]

Según la empresa de seguridad Pandasecurity[4], "el phishing se refiere al envío de correos electrónicos que tienen la apariencia de proceder de fuentes de confianza (como bancos, compañías de energía etc.) pero que en realidad pretenden manipular al receptor para robar información confidencial. Por eso siempre es recomendable acceder a las páginas web escribiendo la dirección directamente en el navegador". [5]

En base a las definiciones anteriores, expresadas por empresas privadas creadoras de software destinado a la seguridad informática, se puede decir que esta tecnica, consiste en engañar a una persona o varias, mediante

[3] Avast es un software antivirus y suite de seguridad de la firma checa Avast Software, desarrollada a principios de la década de 1990.
[4] Panda Security es una empresa española especializada en la creación de soluciones de seguridad informática.

algún medio informático, caracterizado por tener una apariencia real, y con el fin de que la víctima revele información (personal u organizacional), como contraseñas o datos de tarjetas de crédito y seguro, obra social y números de cuentas bancarias.

Existen diferentes técnicas de phishing. Una característica muy común es donde no existe contacto entre el hacker y el usuario. El atacante se esconde detrás de una página web o intercepta los datos cuando estos circulan por la red. Redirige al usuario vía email a la página web fraudulenta, se hospeda en ella se inserta código malicioso en la página para lograr infectar el ordenador de la víctima o guiarla a otra página web [6]. En otro caso muy similar, el cibercriminal se sirve de distintos métodos tales como: elementos ocultos, anuncios publicitarios o enlaces HTML disfrazados [7]. El cibercriminal puede instar al usuario a visitar la página web mediante diferentes tipos de banners de publicidad de interés para la víctima. Cabe destacar que el interés de la víctima lo pudo haber obtenido a través de diferentes tareas de inteligencia previas.

Otra técnica también muy común consiste en la manipulación de la URL para hacer creer al usuario que, al hacer clic en un enlace que lo conduciría a la página web de una organización legítima, sin embargo, lo redirige a una página web fraudulenta, perteneciente al victimario. En este caso manipular el URL (Uniform Resource Locator) sustituyendo el nombre de dominio completo por una dirección IP, que el usuario final no es capaz de distinguir. Otra forma de llevarlo a cabo, consiste en la utilización de algunas de las codificaciones que muchos navegadores web admiten (“Escape Encoding”; “Unicode Encoding”; “UTF- 8 Encoding” e incluso juntar varias de ellas [6]. Asimismo, otra variable posible reside en el cambio de caracteres por otros similares, generando en la victima la creencia de estar accediendo a un URL verídico. No obstante, al iniciar el proceso de búsqueda de dominio, la interpretación que realice el servidor no será la misma. Para lograr el éxito mediante la utilización de esta variable, el victimario busca parejas de letras y números que se asemejen a simple vista; por ejemplo si se junta una “r” con una “n”, se consigue el efecto visual de una “m” (“cornpany” / ”company”) [6]. El formato normalizado de codificación de URL permite la inserción de un nombre de usuario y su contraseña [6].

Existe una gran cantidad de casos reales de phishing para analizar, que son llevados a cabo a nivel nacional e internacional. No hay límites geográficos, ni de tiempo, aprovechando siempre el uso de las nuevas Tecnologías de la Información y la Comunicación.

La empresa "Eset"[5], sostiene que es posible que se intenten engaños con direcciones como, por ejemplo, "https://www.twiitter.com" para hacerla pasar por la original "twitter.com", o "https://www.rnercadolibre.com" para que parezca "mercadolibre.com".

2.1.2. Como prevenir los ataques de Phishing.

Las formas más efectivas utilizadas como prevención para los ataques de Phishing son:

- Filtros de spam: pueden ser utilizados para la protección de correos no deseados. Generalmente, los filtros evalúan el origen del mensaje, el software utilizado para enviar el mensaje y la apariencia del mensaje para determinar si es correo no deseado. Ocasionalmente, los filtros de spam pueden incluso bloquear correos electrónicos de fuentes legítimas, por lo que no siempre es 100% exacto.
- Configuración del navegador: sólo debe permitir la apertura de sitios web confiables, de manera que ésta debe modificarse para evitar la apertura de sitios web fraudulentos. Los navegadores mantienen una lista de sitios web falsos y cuando el usuario intenta acceder al sitio web, la dirección se bloquea o se muestra un mensaje de alerta.
- Gestión de contraseñas: muchos sitios web requieren el ingreso de información para el inicio de sesión por parte de los usuarios. De manera que, una forma de garantizar la seguridad es mediante la solicitud de cambio de contraseñas al usuario periódicamente como también el uso de diferentes contraseñas para cada cuenta, sin repetir la misma en varias oportunidades o en todas estas.

[5] ESET es una compañía de seguridad informática que desarrolló el "ESET NOD32", un potencial software antivirus.

- Sistema CAPTCHA[6]: procedimientos basados en un test público y automático que distingue a los ordenadores de los humanos, como doble factor de autenticación.
- Sistemas de monitoreo: procedimientos automáticos que realicen búsquedas de componentes defectuosos o lentos, a los efectos de optimizar recursos.
- Verificación de SSL: En presencia de un enlace inserto en un correo electrónico, el usuario debe proceder a verificar su validez mediante la constatación de la existencia de certificado SSL ("Secure Socket Layer", en español "Capa de puertos seguros") válido, mediante el URL, ya que éste debe comenzar con "https". Por otro lado, los sitios legales por lo general no utilizan URL acortada para solicitar datos personales. En éstas no se puede comprobar si el destino es legítimo. En general, los correos electrónicos enviados por un atacante están enmascarados por lo que parecen enviados por un emisor cuyos servicios son utilizados por el destinatario. Por lo tanto resulta necesario realizar cambios en los hábitos de navegación para evitar la técnica de referencia. En caso de requerir algún tipo de verificación, es necesario que la compañía verifique antes de transmitir cualquier información en línea.
- Doble validación de identidad: validar la identidad del contacto con el remitente por otro medio, antes de brindar una respuesta.

2.2 Phishing telefónico (Vishing)

Sobre esta técnica, el Banco Bilbao Vizcaya Argentaria (BBVA)[7] establece que "el término deriva de la unión de dos palabras: 'voice' y 'phishing' y se refiere al tipo de amenaza que combina una llamada telefónica fraudulenta con información previamente obtenida desde internet." [8]

[6] Captcha o CAPTCHA son las siglas de Completely Automated Public Turing test to tell Computers and Humans Apart. Test de Turing público y automático para distinguir a los ordenadores de los humanos.

[7] Banco español con sede social en Bilbao (BBVA), presidido por Carlos Torres Vila. Es una de las mayores entidades financieras del mundo y está presente principalmente en España, México, América del Sur, Estados Unidos y Turquía.

Tal como lo expresa la entidad bancaria privada internacional, este término es una combinación de las palabras “voz” y “phishing” y hace referencia a estafas de phishing que se lleva a cabo mediante tecnología de voz (generalmente por el teléfono de atención al público), intentando engañar a los individuos del otro lado de la línea, para que revelen información crucial de carácter financiero o personal. Algunos atacantes pueden usar cambiadores de voz para ocultar la identidad.

Dentro del plano empresarial, los atacantes pueden hacerse pasar por una figura de autoridad, un técnico, un cliente o un compañero de trabajo para obtener información confidencial, contribuyendo al compromiso directo de una organización al aprovecharse de la disposición de las personas. Un claro ejemplo de personal con mayor nivel de exposición y vulnerabilidad, es el personal de la “mesa de atención al cliente” o “recepción”, ya que su trabajo es brindar asesoramiento de manera amable y educada a las personas que se comuniquen por cualquier medio con la entidad en la que ellos trabajan.

Los victimarios, generalmente, pueden obtener los números de teléfono necesarios del sitio web de una organización, en adición a cualquier correo electrónico que se utilice para el soporte al cliente. Mediante la utilización de los datos obtenidos, intentarán conseguir la mayor cantidad de información posible (incluidos los números de teléfono directos del CEO, los títulos de los empleados, la dirección, el número de obra social, entre otros) por parte del empleado con el que hablan o a partir de un cliente con acceso a datos sueltos, que luego relacionarán entre si o con nuevos datos, que pueden ser obtenidos en las redes sociales u otros sitios y que posteriormente servirán para responder preguntas de seguridad simples. Por otro lado, el victimario puede solicitar un restablecimiento de la contraseña o incluso intentar realizar intentos de modificaciones en la cuenta de un cliente para tener acceso a la misma, realizando el engaño con apoyo de un medio técnico.

2.2.1 Como prevenir los ataques de Vishing.

- No se debe proporcionar información ni personal, ni de la empresa. Se deben pedir detalles sobre la identidad de quien emite la llamada. Si quien llama no puede contestar, se debe asumir que ese representante no es

legítimo.

- Realizar las comunicaciones pertinentes: tal como con las actividades de phishing, hay que notificar a la empresa que supuestamente se ha comunicado, informando que tipo de información le han solicitado. [4]

Asimismo, el sitio denominado “Security Throught Education” [9], expone que desde las empresas se pueden tomar los siguientes recaudos:

- Efectuar ataques simulados, son una forma efectiva de evaluar las vulnerabilidades.
- Los informes extensos proporcionan datos procesables sobre las respuestas de los empleados ante diversos escenarios.
- Identifique qué departamentos o empleados son más susceptibles.
- Sobre la base de los resultados de la evaluación de vishing, desarrolle una evaluación continua y un proceso de capacitación para combatir con éxito los ataques de vishing.

2.3 Dumpster Diving

Según NIVEL4 Labs[8], esta técnica se describe como “Dumpster Diving: sumergirse en el basurero” [10].

Con el objetivo de ampliar este tipo de ataque, podemos decir que esta técnica es perpetrada por un software y se refiere al acto de “husmear” o indagar entre la basura, es decir en los documentos que la víctima elimino o suprimió, o archivos que se ha descartado en computadoras y celulares, datos del historial de navegación o en los archivos que almacenan las cookies, de esta manera se pueden obtener documentos con información personal o financiera de una persona u organización.

La naturaleza de los elementos y/o la información encontrada puede ser de gran variedad, desde registros médicos, hojas de vida, fotos personales y correos electrónicos, estados de cuenta bancarios, detalles de cuentas o información sobre software, registros de soporte técnico y mucho más,

[8] NIVEL4 Labs corresponde al área de Investigación, Innovación y Desarrollo. Es una empresa dedicada a ofrecer servicios y soluciones de seguridad informática para pequeñas y grandes empresas.

incluyendo elementos provenientes de hechos delictivos descartados por presuntos delincuentes o víctimas.

Dicha información puede ser utilizada como material para ejecutar una acción o ataque.

2.3.1 Como prevenir ataques de Dumpster Diving.

A los efectos de mitigar este tipo de ataques, es necesario:

- Eliminar los datos importantes que figuran en los blocks de notas, anotaciones, documentos confidenciales, configuraciones, e-mails, que se guarden en dispositivos de almacenamiento.

En cuanto a los dispositivos móviles corporativos extraviados o dañados:

- Establecer políticas de seguridad en cuanto a qué procedimiento seguir. Los dispositivos, pueden guardar links de acceso, información personal, notas confidenciales, documentos digitales, contraseñas de la empresa, que indique parámetros de infraestructura.
- Utilizar un instrumento para cortar el papel, que ira desechado en la basura, de forma que ningún dato importante sea visible.

2.4 Mensajes Hoax.

Según la precedentemente citada empresa española especializada en la creación de soluciones de seguridad informática Pandasecurity, “el mensaje suele pertenecer a una cadena de correos electrónicos que indica a los receptores que los reenvíen a todas las personas que conozcan. Su finalidad es generar alarma y confusión entre los usuarios”. [11]

Es decir, este tipo de mensajes, que casi siempre son enviados a través de un correo electrónico, incitan al usuario a comprometer los activos de la empresa, buscan causar un impacto en el destinatario, son fácilmente identificables, suelen utilizar un lenguaje que genera sensación de urgencia, amenaza, alarma o miedo, alentando a las víctimas a transmitir la información a otras personas lo antes posible, pueden incluir anuncios falsos, supuestamente provenientes de fuentes verídicas, y trasmiten noticias falsas

que simulan haber sido escritas por medios de comunicación social legítimos. Generalmente, estos tipos de mensajes indican que un supuesto virus provocara daños o hechos muy graves. En adición a las características expuestas anteriormente, otros daños secundarios que pueden llevar a cabo son la pérdida de productividad, pérdida de credibilidad, saturación de redes locales y de mensajes.

2.4.1 Como prevenir ataques de Hoax.

Para prevenir este tipo de ataques se aconseja:

- Ignorar sus instrucciones y no reenviar este tipo de mensaje, a fin de evitar su expansión.
- Para su identificación: normalmente incluyen en el encabezamiento el nombre de agencias u organizaciones reconocidas.
- No están fechados, para simular su fecha de origen y perdurar circulando en la red.

2.5. Correo no deseado/SPAM.

Según la aplicación de correo electrónico MDaemon Email Server [9], establece que "se denomina Spam o "correo basura" a todo tipo de comunicación no solicitada, realizada por vía electrónica".

De este modo se entiende por Spam cualquier mensaje por correo, no solicitado y que normalmente tiene el fin de ofertar, comercializar o tratar de despertar el interés respecto de un producto, servicio o empresa. Aunque se puede hacer por distintas vías, la más utilizada entre el público en general es mediante el correo electrónico [12].

2.5.1. Como prevenir ataques de Correo No Deseado/SPAM.

- Un buen hábito es tener dos cuentas de correo electrónico. Una organizacional, y una (o dos) personal. La empresarial, debe ser utilizada solo

[9] MDaemon Email Server es una aplicación de servidor de correo electrónico con funciones de groupware para Microsoft Windows, lanzada por primera vez por Alt-N Technologies en 1996.

para cuestiones laborales. Las personales, una puede ser utilizada para contactos de confianza, y la otra para participar en blogs, publicar en la web, suscripciones, entre otras, donde no sea importante recibir spam.

- Leer las políticas de privacidad de los sitios donde se introducen datos personales o dirección de correo.
- Establecer reglas de correo electrónico. Lo ideal es que estas reglas ya estén incluidas dentro del mismo servidor de correo electrónico, regladas por el mismo administrador.

2.6. Aplicaciones Maliciosas.

Según Malwarebytes[10], "las aplicaciones maliciosas pueden ocultarse en aplicaciones aparentemente legítimas, especialmente cuando se descargan a través de sitios web o mensajes y no desde una App Store segura" [13].

Las aplicaciones informáticas[11] que los usuarios descargan en los ordenadores pueden ser dañinas para los sistemas, ya que pueden incluir malware.

Este tipo de aplicación puede producir una infinidad de eventos en nuestro ordenador, como por ejemplo ralentizarlos, llenar las pantallas de publicidades, otorgar errores graves, aumento de la actividad del sistema, perdida del espacio disponible en el disco, gran utilización de recursos del sistema. Es por esta razón que, en caso de otorgar autorización a los empleados para descargar o instalar aplicaciones en los dispositivos otorgados por la organización, lo ideal es otorgar que permisos deben aceptar, indicando a qué tipo de información organizacional pueden brindar y/o acceder, para que sean responsables de sus actos.

2.6.1. Como prevenir ataques a través de Aplicaciones Maliciosas.

[10] Malwarebytes Anti-Malware es un software anti-malware para Microsoft Windows, macOS y Android que detecta y elimina el malware. Fabricado por Malwarebytes Corporation, se lanzó por primera vez en enero de 2006.

[11] Una aplicación informática (también llamada aplicación o app) es simplemente un programa informático creado para llevar a cabo o facilitar una tarea en un dispositivo informático.

- Instalar solamente aplicaciones legítimas, descargaras desde el sitio del proveedor.
- Evitar las “Fake Security Apps”, que son aplicaciones que se muestran como antivirus y que comprometen al sistema operativo con software malicioso.
- Prestar especial atención a los permisos que se les otorga a las aplicaciones nuevas.

2.7. Redes Sociales

Las redes sociales son un medio por el cual se transmite la información, a través de ella se efectúan una infinidad de casos en los que se aplican las TIS.

Si bien la mayoría de las empresas no permiten a los empleados la utilización de redes sociales en su horario laboral, éstas forman parte de la vida cotidiana y que de alguna u otra manera siempre tendrá algún tipo de relación con la organización.

Como se mencionó anteriormente las personas son el eslabón más débil de la cadena de seguridad de una organización. Si la empresa no posee pautas de seguridad claramente establecidas, los empleados pueden realizar actividades que, sin intención pueden dañar la seguridad de la misma, revelando pistas o posibles respuestas a preguntas de seguridad. Este daño se puede dar simplemente por publicar en una red social una fotografía con el uniforme de la empresa, sus credenciales de identificación, zonas internas de edificios privados; o, directamente documentación física y/o virtual y/o datos que los criminales pueden recolectar, por única vez o periódicamente, para ejecutar su plan.

Las redes sociales son medios, a través del cual un ingeniero social puede conseguir una gran multiplicidad de información. Son medios críticos en seguridad y privacidad debido a la gran cantidad de usuarios y al ferviente deseo de publicar información confidencial de parte de éstos [14].

La considerable cantidad de posibles víctimas, las altas probabilidades de éxito en el intento de establecer una relación con alguien, la variada amplitud de edades, el pequeño riesgo de identificación en el caso de que el

ataque sea descubierto y la ausencia de coste hacen a estas redes muy atractivas para los victimarios [14]

La información que se maneja en las redes sociales es información pública. Esto significa que la persona que publica en la red de manera voluntaria ciertos datos, permitiendo el acceso a otros usuarios. Esta información, aunque quiera ser borrada por el usuario, puede ser encontrada por cualquier persona en buscadores como Google usando las palabras adecuadas [14].

El objetivo del victimario, de usar las redes sociales es principalmente conseguir información sobre el usuario, normalmente, para complementar una técnica de Ingeniería Social.

En la mayoría de las redes sociales se puede buscar cuáles son los intereses de la víctima para saber cómo empezar una buena conversación con ella y ganarse su confianza. Probablemente las redes sociales, proporcionen opciones para privatizar o limitar el acceso a los datos a personas ajenas al usuario. En el caso de que el ingeniero social quiera dirigir su ataque a una persona en particular, debe conseguir poder tener acceso a los datos.

Según un estudio realizado por alumnos de las universidades de Atlanta, Boston y el Instituto Eurecom [14], las personas tienen tendencia a confiar en los amigos que han sido contactados por ellos mismos. Por este motivo, uno de los ataques que puede tener más éxito es conseguir engañar a la víctima para que envíe una solicitud de amistad a su atacante utilizando la psicología. Una vez que se establece un contacto, el atacante puede instar a la víctima a visitar páginas web fraudulentas o incluso puede mandarle un correo personalizado con la certeza de que no sospechará de que se trate de un ataque de phishing.

Facebook[12], Twitter[13], LinkedIn y otras plataformas de medios sociales ayudan a las personas a conectarse, pero también a conocer sus gustos y disgustos, familia, niños y pasatiempos. Con esta información, los atacantes

[12] Facebook, Inc. es una compañía estadounidense que ofrece servicios de redes sociales y medios sociales en línea con sede en Menlo Park, California.
[13] Twitter es un servicio de microblogging, con sede en San Francisco, California, EE.UU, con filiales en San Antonio y Boston en Estados Unidos.

pueden crear algún tipo de comunicación, con disparadores emocionales adecuados para con éxito su objetivo. Estas tácticas son puramente psicológicas y funcionan mejor cuando se utilizan sobre una persona específica, para obtener más información sobre la organización para la que trabaja.

Por otro lado, las redes sociales son una tecnología que muchas empresas han adoptado, para desarrollar marketing sin mayores costos, ya que puede alcanzar a un gran número de clientes potenciales. Las compañías publican eventos corporativos, nuevos productos, comunicados de prensa, relaciones con proveedores y actualizaciones que pueden relacionarlos con eventos.

2.7.1. Como prevenir ataques a través de Redes Sociales.

- Configuraciones de seguridad: resulta ineludible configurar las cuentas de las redes sociales para que no otorguen información privada. Mantener las configuraciones de privacidad y seguridad actualizadas.
- Exposición de datos: establecer pautas generales a nivel organizacional para que los empleados no puedan exponer datos, fotografías, comentarios, referencias, relacionadas a la organización en las redes sociales.
- Verificar parámetros de seguridad: tener en cuenta establecer privacidad en cuanto a la geolocalización en comentarios o fotos, que puedan afectar el ámbito laboral.
- Establecer conciencia de seguridad: ser consciente de la seguridad cuando se trata de información que se hace pública en cualquier plataforma de redes sociales.
- Establecer directrices: la organización deberá estableces directrices claras en el uso de las redes sociales, para la totalidad de los empleados, incluidos los ejecutivos de alto nivel. Deben implementarse políticas claras de seguridad de la compañía para informar posibles mensajes extraños, de origen desconocido o de remitente no seguro, recibidos a través de correo electrónico corporativo.

2.8. Tailgaiting

Johnny Long, en el libro “No tech hacking: a guide to social engineering Dumpster Diving and Shoulder Sourfing”, señala que el concepto de referencia “significa seguir a una persona autorizada a un edificio… método sin tecnología para obtener acceso a un edificio seguro” [15].

En este método, un atacante puede evadir controles de acceso físico como puertas electrónicas e ingresar a una organización sin autorización obteniendo acceso a un edificio seguro, incluso si tiene pases de tarjetas inteligentes o datos biométricos aprovechando la solidaridad o inconsciencia de un empleado. Estas medidas de seguridad, normalmente, pueden evitar que personal no autorizado ingrese a edificios, sistemas o redes.

El “tailgating” funciona principalemten en empresas de tamaño mediano. En estas los atacantes pueden iniciar conversaciones con los empleados y usar esta aparente familiaridad para superar los controles de la recepción. Contrario a esto, en las organizaciones de mayor dimensión, compuestas por gran cantidad de recursos humanos, es poco probable que suceda, ya que todo integrante de la organización está obligado a ingresar mediante el uso de distintos factores de identificación.

En el primer tipo de organización, el atacante, mediante este tipo de técnica, tiene mayor probabilidad de cumplir con su objetivo: obtener acceso físico al sitio, a como dé lugar.

2.8.1. Como prevenir los ataques de Tailgaiting.

- Resguardar las credenciales personales de ingreso, evitando facilitarlas a personas desconocidas.
- Al momento de ingresar a un lugar restringido con algún tipo de control de acceso, no partir el ingreso sin antes identificarse.

2.9. Shoulder Surfing

Según Johnny Long, en el libro “No tech hacking: a guide to social engineering Dumpster Diving and Shoulder Sourfing” ésta técnica “es un ataque clásico sin tecnología. Es un ataque simple. Todo lo que un atacante

hace es mirar por encima del hombro de la víctima para ver lo que él o ella está haciendo.” [15].

La información que obtiene el victimario puede ser la identificación del usuario, datos confidenciales, patrón de desbloqueo, pin o alguna otra contraseña, en una computadora u otro dispositivo vistos en texto plano.

“Shoulder surfing” puede llevarse a cabo en cualquier ámbito físico, incluso cuando la gente utiliza sus computadoras, como cafeterías, aeropuertos, restaurantes, hoteles, o incluso una zona de estar al aire libre, como plazas, parques, zonas céntricas, donde tenga una conexión a internet.

2.9.1. Como prevenir los ataques de Shoulder Sourfing

- Mantener la privacidad: procurar la mayor privacidad posible, siempre que introduzcamos en algún medio algún tipo de información, no solo de carácter confidencial.
- Observar alrededor: nadie a nuestro alrededor debe estar prestando atención a lo que hacemos, a nuestras claves, accesos o movimientos que realizamos con tarjetas de acceso, de crédito, o documentación.
- Teclados con resguardo: en caso de ser posible, utilizar los teclados con resguardo para que no puedan ser visualizados los códigos, limitado a un ángulo de la visual del victimario.

2.10. Pretexting

El hacker utiliza un escenario inventado asumiendo una identidad o un rol para incitar a la víctima a proporcionar información confidencial o para provocar que el usuario haga algo que no haría en una situación normal. Para un mayor éxito en el ataque, el cibercriminal debe convertirse en la entidad creada, imitando como habla, como camina, como se sienta, como se viste o su lenguaje corporal. La historia debe ser creíble y simple; un escenario que haga sentir a la víctima cómoda y relajada [6].

Se puede definir como la práctica de presentarse como otra persona para obtener información privada, creando una identidad completamente

nueva o haciéndose pasar por una persona. También se puede utilizar para hacerse pasar por personas en ciertos trabajos. La etapa esencial de esta técnica se basa en la realización de una buena investigación previa, para elaborar un buen pretexto, por lo que se tienden a usar dialectos o expresiones familiares en el ámbito de afectación.

Este ataque de tipo social, se da generalmente con un operador humano, y un canal telefónico. Frecuentemente esta técnica es muy utilizada por las autoridades (juzgados, fiscalías, fuerzas federales y provinciales), y periodistas, además de personas que trabajan en call centers, para empresas privadas.

2.10.1. Como prevenir ataques de Pretexting.

- Mantener un perfil criterioso: en principio se debe tener la astucia de no brindar datos privados, y de solicitar en todos los casos datos específicos, que no se encuentren publicados en la web.
- Doble factor de autenticación: implementar el uso de sistemas, mediante medidas de seguridad extra.

2.11. Baiting

Esta técnica incluye un medio digital en soporte físico, que se inserta en algún medio infectado con Malware, es similar a los ataques de phishing. Permite alcanzar a muchas personas en el mismo ataque, los recursos son muchos más caros y el riesgo al que se expone el victimario es mayor. Esto se puede explicar con un ejemplo muy sencillo: un ingeniero que finge regalar un dispositivo electrónico (por ejemplo, un pendrive) con la excusa de ser una manera de promocionar una empresa. El número de víctimas puede ser muy grande pero el coste de un pendrive siempre es mayor que el coste de un email y el ingeniero expone su identidad al estar repartiendo el dispositivo infectado en vez de estar detrás de un ordenador [6]. Los atacantes pueden usar música o descargas gratis de películas, si ofrecen sus credenciales a una determinada página.

2.11.1. Como prevenir ataques de Baiting.

- Dispositivos desconocidos: en caso de insertar dispositivos desconocidos en una computadora personal, o en una computadora ajena un dispositivo propio, escanear los mismos con un antivirus.
- Descarga de archivos: descargar archivos únicamente desde páginas desconocidas y confiables.

3. Perfiles y motivaciones.

El conjunto de las técnicas descriptas anteriormente, reflejan algunas de las características intrínsecas al ser humano. Por un lado, el victimario se encuentra generalmente envuelto en actitudes negativas como la maldad, la mala intencionalidad, la codicia y, por otro lado, la víctima en este caso integrantes de organizaciones, que se caracterizan por tener la obligación de brindar un correcto asesoramiento ante la prestación de un servicio, presentan características y/o emociones como el miedo, la bondad, la paciencia, entre otras. Existe, además otra caracterización de un determinado tipo de empleado, que en principio poseen las características de las víctimas, pero que puede tronarse victimario, por encontrarse envuelto en actitudes de resentimiento o insatisfacción por su puesto o cargo, lo que deriva en un posible problema, este tipo de personalidad no se aborda en el presente trabajo, ya que considero requiere un estudio psicológico y criminológico especifico determinado.

Los perfiles que se describen a continuación, son complejos y diversos. Por esta razón, no se pretende desarrollarlos en su totalidad, ya que abarcan diferentes ámbitos disciplinarios específicos, como la psicología, la sociología, entre otros; sino que se busca informar sobre algunas de las metodologías más frecuentes con las que se presenta.

3.1. Perfil del victimario.

Para cumplir sus objetivos, los ingenieros sociales, deben conocer el perfil y las características de la víctima. Esto le facilita el trabajo, ya que es esencial para la elaboración de los objetivos. Al efecto de no dejar rastros, deben planificar la técnica y tener precaución en su trabajo. Para ello deberán saber cómo y dónde buscar la información. Para esto, es necesario que tengan conocimientos de tecnología, tecnologías de la información y la comunicación, aplicaciones y bases de datos.

Asimismo, para alcanzar el logro de sus objetivos, resulta conveniente que el victimario pueda infundir confianza, ser imperturbables, pacientes y tolerantes ante las diferentes situaciones, sin perder la calma, asumiendo la

actitud adecuada ante cada situación. Además, debe contar con capacidad de expresión, improvisación, persuasión, resolución de imprevistos y autocontrol.

3.2. Perfil de la víctima.

Este perfil suele estar compuesto por actitud de servicio y proactividad, es decir que su comportamiento tiende a ser anticipatorio y entusiasta ante diversas situaciones, que colabore y/o brinde soluciones ante distintos acontecimientos de la organización, lo que lo llevará a obtener un reconocimiento por su ayuda y trabajo. Además, los empleados que tienen mayor experiencia en su área de trabajo, tienden a caer en este perfil, ya que tienen mayor dominio del área y son más propensos a brindar información comprometedora. No obstante, algunas personas que no poseen conocimiento relacionado a su área y/o de carácter tecnológico, son blancos fáciles, ya que pueden filtrar información de importancia sin darse cuenta, debido a la falta de capacitación o a la falta de criterio organizacional.

4. Ataques de ingeniería social en las organizaciones públicas y privadas.

A los efectos de llevar a cabo un efectivo análisis del presente punto, es importante destacar la diferencia entre las organizaciones públicas y privadas. Para ello, se procederá a citar definiciones de diferentes autores, a fin de realizar una breve aproximación al tema:

4.1. Empresas Públicas.

“Instrumento de intervención del poder público en la economía, mediante la producción de bienes y servicios, en cualquier sector de actividad, organizado en forma de empresa, que en principio se financia con las contraprestaciones recibidas de sus clientes en forma de precios y en la que la participación del Estado en su propiedad le otorga el control de la misma” [16].

4.2. Empresas privadas.

“Son aquellas organizaciones que pertenecen a inversionistas privados, por lo general estas organizaciones son conformadas por un conjunto de socios, aunque existen casos donde la propiedad total de la empresa es de un solo inversionista. Estas empresas por lo general suelen ser la el pilar fundamental de la economía de una país y trabajan en paralelo a las empresas estatales (públicas)” [17].

4.3. Factores en común.

Ambos tipos de instituciones tienen en común una gran variedad de factores:

- El principal promotor de su funcionamiento es el elemento humano. Todas las empresas están conformadas por personas que trabajan en ella o que intervienen como usuarios externos.
- Otro ente fundamental para su funcionamiento son los bienes materiales, la información y los datos con los que llevan a cabo sus actividades diarias.
- Tienen aspiraciones en común, realizaciones si se logran estas

aspiraciones y sentido de pertenencia.

- Poseen producción, transformación, y probablemente algún tipo de prestación de servicios. Capacidad técnica y financiera.

En base a ello, se puede decir que ambos tipos están compuestos por elementos tangibles e intangibles, cuya finalidad puede ser la satisfacción de necesidades y/o deseos, otorgar un servicio, u obtener un beneficio económico. Sin embargo, las funciones que realizan las diferentes entidades públicas y privadas, son heterogéneas y poseen un variado índice de implementación de las nuevas tecnologías en función de la actividad a la que se dediquen. De este modo, mientras la mayoría de ellas dispone de una página web corporativa, otras hacen uso intensivo del comercio electrónico.

El informe denominado “Human Factor 2019” [18], elaborado por la empresa líder en ciberseguridad “Proofpoint[14]”, en el cual se han analizado datos de la base de clientes de la compañía durante 18 meses, además de las tendencias de ciberataques, revela las tácticas con las que los cibercriminales se dirigen a personas que forman parte de las empresas, antes que atacar a sus sistemas e infraestructuras de Tecnologías de la Información. De este surge que las acciones más comunes que realizan son instalar malware, realizar transacciones fraudulentas o robar datos, entre otras.

Kevin Epstein, vicepresidente de Threat Operations para Proofpoint, señala que "actualmente, los cibercriminales se están dedicando a atacar de manera agresiva a los usuarios, ya que resulta mucho más fácil y rentable enviar correos electrónicos fraudulentos, robar credenciales y subir archivos maliciosos a aplicaciones en la nube que crear un exploit caro, lento y con una mayor probabilidad de error". Además, expone que "más del 99% de los ciberataques depende de la interacción humana, lo que convierte a los usuarios individuales en la última línea de defensa de una organización. Para reducir significativamente este riesgo, las empresas necesitan un enfoque holístico en ciberseguridad, centrado en las personas, que contemple una formación eficaz de los empleados en esta materia, así como sistemas de defensa por capas que les den visibilidad de cuáles son sus usuarios más

[14] Eric Hahn, ex CTO de Netscape, fundó la compañía en 2002. Presta servicio a más de 4,000 empresas en todo el mundo. La compañía se hizo pública en abril de 2012.

atacados", dejando vislumbrar los siguientes puntos de interés para el presente trabajo:

- Más del 99% de las amenazas registradas en el estudio, se han activado mediante la acción de una persona.
- Los señuelos relacionados con Microsoft[15], son los más usados. "Alrededor de 1 de cada 4 correos electrónicos de phishing enviados en 2018 estaba asociado a productos de Microsoft. En 2019 ha habido un cambio en cuanto a almacenamiento en la nube en términos de eficacia, con DocuSign[16] y el phishing en servicios cloud de Microsoft. La mayoría de estos cebos de phishing tenía como objetivo el robo de credenciales."
- Los victimarios están perfeccionando sus técnicas y herramientas, con el objetivo de obtener un beneficio económico o robo de datos.
- En el tiempo que duro el análisis, los principales ataques han sido a través de troyanos bancarios, robo de información, administración remota y otros diseñados para permanecer en los dispositivos y hurtar continuamente datos de utilidad.
- Los cibercriminales atacan a personas comúnmente atacadas o VAP ("Very Attacked People"), cuyos perfiles pueden encontrarse a través de páginas web, web corporativas, redes sociales o publicaciones.
- Los victimarios, imitan la rutina de los trabajadores de la organización, en cuanto al envío de mails.
- Las áreas de educación, finanzas y publicidad han sido las industrias con más alto promedio de ataques.
- El kit de phishing Chalbhai[17], fue el tercero más popular en el primer semestre del año 2019, siendo su objetivo conseguir credenciales de los principales bancos y compañías de comunicaciones globales, entre otras organizaciones, utilizando correo electrónico.

[15] Windows es el nombre de una familia de distribuciones de software para PC, teléfonos inteligentes, servidores y sistemas desarrollados y vendidos por Microsoft y disponibles para múltiples arquitecturas.
[16] Compañía estadounidense con sede en San Francisco, California, que ayuda a las organizaciones a conectarse y automatizar la forma en que preparan, firman, actúan y gestionan acuerdos.
[17] Nueva generación de phishing a la venta en la Darknet.

Para mitigar estos riesgos, las empresas suelen optar por subcontratar servicios como el soporte informático, el alojamiento en la nube, o cualquier otro servicio de carácter tecnológico a proveedores de servicios externos especializados. En estos casos, es necesario tomar precauciones y vigilar la relación con los proveedores exigiendo además un buen nivel de servicio, garantías sobre la protección de la información confidencial de los clientes y protección de las comunicaciones entre empresa y proveedor.

La ingeniería social, está íntimamente relacionada al “arte del engaño” y la persuasión, y/o manipulación psicológica de personas, que las lleva a realizar actividades que acorde los parámetros de seguridad de las organizaciones, no deberían hacer; y, además, se encuentra directamente conectada al éxito de técnicas utilizadas para llevar a cabo ataques virtuales, que buscan explotar el eslabón más débil de la estructura de seguridad, es decir el factor humano.

La defensa más apropiada en estos casos es la concientización y la formación de los empleados en las técnicas de ingeniería social que utilizan los ciberdelincuentes para engañar a sus víctimas, y poder distinguir los mensajes maliciosos de los que no lo son.

Para establecer esquemas de seguridad, existen una serie de normas estandarizadas sobre Sistemas de Gestión de Seguridad de la Información, denominadas ISO/IEC 27000. Estas, proveen estándares y guías sobre buenas prácticas en sistemas de gestión de seguridad de la información, generalmente aceptadas. En tanto el listado de normas recomendadas para su implementación en torno al tema de referencia, se encuentran numeradas y detalladas en el Anexo I.

5. Capacitación y campañas de concientización.

El propósito de las campañas de concientización, es influir y capacitar a determinado grupo de personas sobre diferentes aspectos relacionados a las Técnicas de Ingeniería Social existentes.

Para realizar una correcta campaña de concientización, es necesario tener en cuenta dos puntos sumamente importantes como base: por un lado, su planificación, y por otro lado la utilización eficaz de los instrumentos de transmisión de los mensajes que se quieren hacer llegar a los destinatarios.

En relación a la planificación, en primer lugar, hay que determinar la temática a trabajar, es decir elaborar un diagnóstico, de acuerdo a la necesidad observada. Luego, identificar a quienes va a estar dirigida, acotar el número de participantes de acuerdo a áreas de interés, ya que no todos los factores cuentan con la misma responsabilidad y/o permisos y adecuar las características al área abordada. Paso seguido, corresponde la determinación de objetivos a partir de las necesidades detectadas.

La segunda instancia consiste la definición de los medios, es decir a través de que métodos y elementos se van a transmitir los mensajes, la definición de las las estrategias, estableciendo de que forma el mensaje impactara racional y emocionalmente en el receptor, con el objetivo de crear conciencia y cambios de conductas y actitudes. Finalmente, la organización debe implementara la campala y, luego de un tiempo prudencial, especificado previamente en los objetivos de la misma, realizar una instancia de evaluación.

La gerencia, a través del área de Seguridad de la Información, debe ejecutar medidas, buscando generar hábitos o determinados comportamientos, influyendo en el pensamiento y accionar del personal al que está dirigida, sin caer en el error de que éstos, confundan una campaña con mera información.

Para que haya una correcta comunicación, se necesita de un feedback, es decir una respuesta, a la totalidad de los usuarios de una organización. El éxito de la misma no estará en la popularidad de la campaña, sino en cómo originó un cambio de comportamiento tras su implementación, acorde los objetivos propuestos.

Lo expuesto, permite vislumbrar que, disponer de normas y estándares de seguridad, incluyendo campañas de concientización dentro de estos últimos,

va a permitir una gestión efectiva de la seguridad de la información en las organizaciones, identificar los riesgos a los que está expuesta por parte del recurso humano integrante de todas las áreas, y establecer las medidas adecuadas para su tratamiento.

5.1. Temáticas relevantes para la capacitación del personal.

Las temáticas sugeridas para que las organizaciones puedan desarrollar campañas que atañen a evitar las TIS, son las siguientes:

- Considerar la prohibición de compartir fotos con el uniforme de trabajo, lugar e identificación personal, fotos indicando el logo de la empresa, dirección, en las redes sociales.
- Utilizar siempre para cuestiones laborales el mail que brinda la institución, y cuanto a cuestiones personales, usar el email personal.
- Mantener el resguardo de la información confidencial sobre el ámbito interno del trabajo.
- Poner especial cuidado en la protección de los dispositivos móviles de la flota empresarias, que se otorgue a los empleados, ya que este posee valiosa información de la organización.
- Siempre cerrar sesión en las cuentas corporativas. No permitir que el sistema o el navegador recuerden la contraseña, tanto en equipos fijos como móviles.
- Capacitar respecto de la utilización de contraseñas seguras. Establecer parámetros de seguridad.
- Establecer políticas de seguridad y uso adecuado, para reducir la amenaza de Ingeniería social.
- Realizar entrenamientos de conciencia de seguridad [19]. Cada persona en la organización debe recibir oportunamente capacitación básica sobre seguridad.
- Efectuar verificaciones de fondo [19], no solo en equipamiento y personal propio de la empresa, sino también de proveedores y otros trabajadores contratados antes de que se conviertan en integrantes de la organización.
- Establecer mecanismos de acceso adecuado para asegurarse que el

ingreso solo de las personas autorizadas a las secciones restringidas de la organización.

- Referente a la fuga de datos es necesario implementar una monitorización constante de toda la información sobre la organización que se encuentra disponible en Internet, lo que dificultará la recolección pasiva de información del atacante mediante varias herramientas. [19]
- Es importante realizar simulacros de ataques de ingeniería social [19]. Se deben realizar actividades acorde un plan de simulacros previamente establecido, involucrando a la totalidad de los empleados de la organización, en el cual se imite un suceso de apariencia real, con los objetivos de tomar las medidas e indicaciones necesarias en caso de que ocurra verdaderamente.
- Establecer una política de clasificación de datos [19]. Debe haber una clasificación adecuada de los datos en función de sus niveles de criticidad y el personal que puede tener acceso. La clasificación de datos asigna un nivel de sensibilidad a la información de la empresa.
- Implementar en cada nivel de clasificación de datos, el establecimiento reglas para ver, editar y compartir la información [19]. En esta implementación se busca que loe empleados obtengan un mecanismo de seguridad sobre la información de acceso público y la que, sin autorización, no se puede divulgar.

6. Conclusiones

Lo expuesto en el presente Trabajo Final de Especialización permite arribar a las siguientes conclusiones:

En cuanto a las técnicas de ingeniería social, se muestran las más comunes, perpetradas mediante el uso de las tecnologías, a través de las habilidades de los Ingenieros Sociales, para engañar a integrantes de distintas organizaciones a la hora de operar dispositivos electrónicos. Por ello, se han reunido las técnicas más comunes y se ha simplificado en que consiste cada una, para influenciar el pensamiento y las acciones e los individuos.

En relación a sus efectos, se indica cómo se pueden moderar o mitigar, a los efectos de agilizar el proceso de implementación de las mejores prácticas en Seguridad de la Información.

Se incluyeron las metodologías más frecuentes con las que se presentan las víctimas, y los victimarios de las presentes técnicas, qué es lo que buscan y que utilizan para obtenerlo.

En cuanto a las organizaciones públicas y privadas, se han descripto las similitudes y diferencias entre el ámbito público y privado, detectando que el factor humano es el más vulnerable. Por ello, surge como una parte obligatoria e imprescindible, la importancia de capacitar al personal, y la necesidad de una profunda y robusta estrategia de seguridad en el área de Informática de la organización, sin importar la dimensión de la entidad.

En forma tácita se puede observar la importancia de que todos los sistemas funcionen correctamente, y que las nuevas tecnologías deben ser una estrategia de inversión para los diferentes tipos de organizaciones, siendo la mejor defensa dentro del esquema de seguridad formar en una robusta cultura de seguridad informática al equipo y a uno mismo, no solo a nivel organizacional, sino también personal, donde cada uno de los integrantes debe considerar la seguridad de la empresa a la que pertenece como una parte integral de sus responsabilidades individuales.

Las limitaciones observadas en el desarrollo del presente trabajo, están relacionadas a la diversidad de información que se encuentra afines a las técnicas expuestas. Por lo que, a futuro, en continuidad del presente

trabajo se podría llegar a establecer una normalización sobre el tema, para facilitar el acceso a la información completa, concisa y oportuna.

7. ANEXO I

Para establecer esquemas de seguridad, existen una serie de normas estandarizadas sobre Sistemas de Gestión de Seguridad de la Información, denominadas ISO/IEC 27000. Estas, proveen estándares y guías sobre buenas prácticas en sistemas de gestión de seguridad de la información, generalmente aceptadas. En tanto el listado de normas recomendadas para su implementación en torno al tema de referencia, se encuentran las siguientes [20]:

- ISO/IEC 27000:2009. Proporciona una vista general del marco normativo y un vocabulario utilizado por las normas de la serie.
- ISO/IEC 27001:2005. Especificaciones para la creación de un Sistema de Gestión de la Seguridad de la Información (en adelante SGSI) (2005).
- ISO/IEC 27002:2005. Código de buenas prácticas para la gestión de la seguridad de la información. Describe el conjunto de objetivos de control y controles a utilizar en la construcción de un SGSI. Publicada en 2005 y renombrada en 2007.
- ISO/IEC 27003:2010. Directrices para la implementación de un SGSI. Es el soporte de la norma ISO/IEC 27001.
- ISO/IEC 27004:2009. Describe los criterios de medición y gestión para lograr la mejora continua y la eficacia de los SGSI.
- ISO/IEC 27005:2008. Proporciona criterios generales para la realización de análisis y gestión de riesgos en materia de seguridad (2008).
- ISO/IEC 27006:2007. Es una guía para el proceso de acreditación de las entidades de certificación de los SGSI.
- SO/IEC 27007. Será una guía para auditar SGSI.
- ISO/IEC 27013. Guía de implementación integrada de ISO/IEC 27001 (gestión de seguridad de la información) y de ISO/IEC 20000-1 (gestión de servicios TI).
- ISO/IEC 27034. Guía de seguridad en aplicaciones informáticas.
- ISO/IEC 27035. Guía de gestión de incidentes de seguridad de la información.

8. Bibliografía

[1] Kaspersky, «Ingeniria Social: definición.,» Kaspersky, [En línea]. Available: https://latam.kaspersky.com/resource-center/definitions/what-is-social-engineering.. [Último acceso: 22 09 2019].

[2] ESET, «Welivesecurity. Las técnicas de Ingeniería Social evolucionaron, ¡presta atención!,» Welivesecurity. Available: https://www.welivesecurity.com/la-es/2014/05/21/tecnicas-ingenieria-social-evolucionaron-presta-atencion/. [Último acceso: 20 03 2018].

[3] A. a. i. C. T. d. 2. I. N. d. E. y. C. (INDEC), «Accesos a internet Cuarto Trimestre de 2017. Instituto Nacional de Estadistica y Censos (INDEC),» Accesos a internet Cuarto Trimestre de 2017. Instituto Nacional de Estadistica y Censos (INDEC). Available: www.indec.gob.ar/uploads/informesdeprensa/internet_03_18.pdf. [Último acceso: 20 03 2018].

[4] Avast, «Phishing,» [En línea]. Available: https://www.avast.com/es-es/c-phishing. [Último acceso: 22 09 2019].

[5] Pandasecurity, «Vishing,» Available: https://www.pandasecurity.com/es/security-info/phishing/. [Último acceso: 22 09 2019].

[6] C. S. Vanrell, Estudio de las Técnicas de la Ingeniería Social usadas en ataques de Ciberseguridad y Análisis Sociológico, Madrid, España: Universidad Politécnica de Madrid, 2015.

[7] Research Gate, Ingeniería social: phishing últimas y futuras técnicas, 2015.

[8] S. 2. Banco Bilbao Vizcaya Argentaria, «'Phishing', 'vishing', 'smishing', ¿qué son y cómo protegerse de estas amenazas?» Available: https://www.bbva.com/es/phishing-vishing-smishing-que-son-y-como-protegerse-de-estas-amenazas/ . [Último acceso: 22 09 2019].

[9] Security Through Education, «Don’t Overlook the Human Element in Security Training and Awareness,» Security Through Education, 12 2019. Available: https://www.social-engineer.org/general-blog/dont-overlook-the-human-element-in-security-training-and-awareness/. [Último acceso: 22 09 2019].

[10] N. Labs, «Nuestra información personal y el Dumpster Diving: Un tesoro en la basura». Available: https://blog.nivel4.com/noticias/nuestra-informacion-personal-y-el-dumpster-diving-un-tesoro-en-la-basura/.

[11] Pandasecurity, «Hoax» Available: https://www.pandasecurity.com/es/security-info/hoax/. [Último acceso: 22 09 2019].

[12] Mdaemon, «Mdaemon» Available: https://www.mdaemon.es/lucha-contra-el-spam-desde-mdaemon/. [Último acceso: 2019 09 19].

[13] Malwarebytes Corporation, 2006. Available: https://es.malwarebytes.com/malware/. [Último acceso: 22 09 2019].

[14] D. M. B. D. B. E. K. a. C. P. Irani, «"Reverse Social Engineering Attacks in Online Social Networks"». Available: http://www.syssec-project.eu/m/page-media/3/irani-dimva11.pdf. [Último acceso: 22 09 2019].

[15] J. Long, «“No tech hacking: a guide to social engineering Dumpster Diving and Shoulder Sourfing”,» 2008. Available: https://doc.lagout.org/Others/No%20Tech%20Hacking%20A%20Guide%20to%20Social%20Engineering%20Dumpster%20Diving%20%26%20Shoulder%20Surfing.pdf. [Último acceso: 22 09 2019].

[16] L. Á. H. Recio y J. M. Herrera Maldonado, «Mecanismos de Intervención del Sector Publico. La empresa pública.» Available: http://personal.us.es/lhierro/Luis_Angel_Hierro/Materiales_docentes_files/LA%20EMPRESA%20PUBLICA.pdf. [Último acceso: 20 10 2019].

[17] Conceptodefinicion., «Definición de Empresa Privada.,» 30 07 2019. Available: Recuperado de: https://conceptodefinicion.de/empresa-privada/.. [Último acceso: 25 10 2019].

[18] Proofpoint Essentials, «The Human Factor 2019 Report» Available: https://www.proofpoint.com/us/resources/threat-reports/human-factor. [Último acceso: 25 10 2019].

[19] C. blog, «Anatomía del ataque de ingeniería social y cómo prevenirlo» Available: https://ciberseguridad.blog/anatomia-del-ataque-de-ingenieria-social-y-como-prevenirlo/.. [Último acceso: 22 09 2019].

[20] iso27000.es, «El portal de ISO 27001 en Español». Available: http://www.iso27000.es/. [Último acceso: 22 09 2019].

[21] Security Through Education, «Identity Thieves – Phishing and Pilfering Your PII» Available: https://www.social-engineer.org/general-blog/identity-thieves-phishing-and-pilfering-your-pii/. [Último acceso: 22 09 2019].

[22] Security Through Education, «Pretexting» Available: https://www.social-engineer.org/framework/influencing-others/pretexting/. [Último acceso: 22 09 2019].