UNIVERSIDAD TÉCNICA PARTICULAR DE LOJA

La Universidad Católica de Loja

TITULACIÓN DE INGENIERA EN SISTEMAS INFORMÁTICOS Y COMPUTACIÓN

"Ingeniería social y sus niveles de incidencias en la UTPL"

Trabajo de Fin de Titulación

AUTORA: Espinosa Armijos, Andrea Susana.

DIRECTORA: Pineda Arévalo, Julia Alexandra. Ing.

Loja – Ecuador

2012

CERTIFICACIÓN

Ingeniera
Julia Pineda
DIRECTOR DE TESIS

C E R T I F I C A:

Haber dirigido y supervisado el desarrollo del presente proyecto de tesis previo a la obtención del título de **INGENIERA EN SISTEMAS INFORMÁTICOS Y COMPUTACIÓN**, y una vez que este cumple con todas las exigencias y los requisitos legales establecidos por la Universidad Técnica Particular de Loja, autoriza su presentación para los fines legales pertinentes.

Loja, 17 de octubre de 2012

……

Ing. Julia Pineda
DIRECTOR DE TESIS

CERTIFICACIÓN

Ingeniera
María Paula Espinosa
CO-DIRECTOR DE TESIS

C E R T I F I C A:

Haber dirigido y supervisado el desarrollo del presente proyecto de tesis previo a la obtención del título de INGENIERA EN SISTEMAS INFORMÁTICOS Y COMPUTACIÓN, y una vez que este cumple con todas las exigencias y los requisitos legales establecidos por la Universidad Técnica Particular de Loja, autoriza su presentación para los fines legales pertinentes.

Loja, 17 de octubre de 2012

……
Ing. María Paula Espinosa
CO-DIRECTOR DE TESIS

AUTORIA

Los conceptos, definiciones, análisis, síntesis, conclusiones y recomendaciones son de exclusiva responsabilidad del autor.

Además, es necesario indicar que la información de otros autores empleada en el presente trabajo está debidamente especificada en fuentes de referencia y apartados bibliográficos.

……..

AUTOR

CESIÓN DE DERECHOS

Yo, Andrea Susana Espinosa Armijos, declaro ser autor del presente trabajo y eximo expresamente a la Universidad Técnica Particular de Loja y a sus representantes legales de posibles reclamos o acciones legales.

Adicionalmente declaro conocer y aceptar la disposición del Art. 67, del estatuto Orgánico de la Universidad Técnica Particular de Loja que su parte pertinente textualmente dice: "Forman parte del patrimonio de la Universidad la propiedad intelectual de investigaciones, trabajos científicos o técnicos y tesis de grado que se realicen a través o con el apoyo financiero académico o institucional (operativo) de la Universidad"

……

Andrea Susana Espinosa Armijos

AGRADECIMIENTO

Principalmente a Dios por darme la sabiduría y la salud para la culminación de este trabajo y sobre todo por haber tenido la oportunidad de intercambiar ideas con mis amigos y compañeros.

Gracias a mi familia quienes con su incansable esfuerzo, supieron darme una carrera para mi futuro y apoyarme brindándome todo su amor, por todo esto les agradezco de corazón que estén hoy a mi lado.

A la Ing. Julia Pineda, Directora de Tesis, que con su guía, esfuerzo, dedicación, paciencia y conocimiento contribuyó de manera fundamental a la culminación del presente trabajo de investigación.

A mis amigas, compañeros, profesores y a todas aquellas personas que de una u otra forma, colaboraron o participaron en la realización de este trabajo de investigación.

A la Universidad Técnica Particular de Loja por formarme como persona de bien capaz de enfrentar cualquier reto profesional en el área de la informática y por permitir hacer uso de sus inmediaciones para poder culminar con éxito éste trabajo de investigación.

EL AUTOR

DEDICATORIA

Mi presente trabajo de investigación la dedico con todo mi amor y cariño:

A DIOS, por ser quién me ha dado la vida y sabiduría necesaria para seguir adelante y culminar mi carrera.

A mi Madre Gladys Armijos ya que ella ha sido mi aliciente cada día a través de sus consejos, esfuerzo y apoyo incondicional me han ayudado a cumplir de manera exitosa ésta etapa de mi vida.

A mi Padre Rodrigo Espinosa por quedarse a mi lado y tener la satisfacción de darle un motivo de felicidad y alegría a su vida.

A mis hermanos y sobrinos quienes me brindaron su apoyo incondicional todo el tiempo.

A Juan Pablo por su cariño y amor, por haber compartido cada momento de trabajo y esfuerzo, y que ahora estés conmigo en este día tan importante para mí, sobre todo agradecerte por todo el apoyo para continuar y seguir con mi camino, gracias por estar conmigo y recuerda que eres muy importante para mí.

A mis amigas por estar a mi lado apoyándome siempre y deseándome éxitos en cada momento de mi vida.

EL AUTOR

INDICE DE CONTENIDOS

INDICE DE FIGURAS

INDICE DE TABLAS

RESUMEN

La presente investigación se realizó un estudio sobre la Ingeniería Social y los Niveles de Incidencia en la UTPL, indicando que a pesar de contar con infraestructura tecnológica de seguridad existen una infinidad de métodos y técnicas que permitan a un atacante obtener información confidencial sin necesidad de utilizar tecnología muy sofisticada, una de estas técnicas es la Ingeniería Social. Este tipo de técnica pretende engañar a los usuarios con el fin de obtener información confidencial, a través de la manipulación psicológica y habilidades sociales. La Ingeniería Social puede ser utilizada por personas males intencionados para llegar a obtener información, privilegios, accesos a sistemas y realizar algún tipo acto que perjudique o ponga en riesgo a una organización o sistema.

Por lo antes mencionado, se ha realizado un análisis de las técnicas por medio de encuestas a los miembros de la Universidad para conocer los riesgos que se tienen al ser víctimas de esta y cuáles serían las posibles defensas contra la Ingeniería Social dentro de la UTPL.

En las recomendaciones se han tomado en cuenta aspectos importantes para considerarse en establecimiento de políticas de protección al usuario, capacitaciones al usuario y establecimiento de normativas de seguridad.

OBJETIVOS

OBJETIVO GENERAL

Determinar el nivel de seguridad que tiene la UTPL con respecto a ataques de Ingeniería Social.

OBJETIVOS ESPECIFICOS

I. Conocer sobre los distintos tipos y técnicas de Ingeniería Social y sus riesgos.
II. Conocer que tan vulnerable es la UTPL ante este tipo de ataques.
III. Establecer formas de protección ante la Ingeniería Social y sus difusión a la UTPL
IV. Especificar políticas de seguridad que se deban implementar en la UTPL.
V. Conocer si la Ley del Ecuador nos protege ante este tipo de delitos.

CAPITULO I

1. DEFINICIÓN DE INGENIERIA SOCIAL

En la Ingeniería Social existen varias definiciones que se enfocan a la seguridad informática, pero preexisten contextos diferentes en donde se pretende conocer y comprender como actúa y opera la ingeniería social, por medio de sus técnicas, tretas, artimañas más elaboradas por medio del engaño a la persona y obtener información confidencial, a través de las debilidades propias o de algún sistema que conozca.

El único medio para entender cómo defenderse contra esta clase de ataques es conocer los conceptos básicos que se menciona a continuación:

Wikipédia:

> Ingeniería Social es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos. Un ingeniero social usará comúnmente el teléfono o Internet para engañar a la gente y llevarla a revelar información sensible, o bien a violar las políticas de seguridad típicas. Con este método, los ingenieros sociales aprovechan la tendencia natural de la gente a confiar en su palabra, antes que aprovechar agujeros de seguridad en los sistemas informáticos. Generalmente se está de acuerdo en que "los usuarios son el eslabón débil" en seguridad; éste es el principio por el que se rige la ingeniería social. [1]

Lester:

> Con el término "ingeniería social" se define el conjunto de técnicas psicológicas y habilidades sociales utilizadas de forma consciente y muchas veces premeditada para la obtención de información de terceros. [2]

CAUSAS DE INGENIERIA SOCIAL

Otro aspecto de valoración es conocer las causas que provocan ataques de Ingeniería Social y una serie de problemáticas que se encierran dentro del conocimiento y desconocimiento sobre el tema, para ello mencionaremos alguna de las causas.

- El factor humano que es una parte esencial y primordial de la seguridad. No existe un sistema informático que no dependa de algún dato ingresado por un operador humano. Significa que esta debilidad de seguridad es universal, independiente de plataformas, el software, red, equipo y la edad de la persona que sea afectada.

- Falta de conocimiento y capacitación sobre las distintas técnicas y maneras de ser atacados por medio de la Ingeniería Social.
- Permitir el acceso a alguna parte del sistema, físicamente o electrónicamente, por parte de personas externas o propias de la empresa que no tengan relación con lo que se realice.
- Desconocimiento de políticas y protocolos de la organización por parte de los empleados, para la protección de información sensible.
- Indiferencia del personal para respaldar información y mantenerse alerta a distintos sistemas de seguridad de información.
- Utilización de herramientas que no proporcionen seguridad a la información ni al personal, y con esto permitan el robo, o algún daño al sistema.

Existen muchas causas que permiten que utilicen los atacantes valiéndose de las distintas técnicas de la Ingeniería Social para realizar algún daño o pérdida de información confidencial.

1.1 ANÁLISIS DE LAS TÉCNICAS MÁS UTILIZADAS POR LOS ATACANTES

Para obtener información los atacantes utilizan técnicas que dependen en gran número de la facilidad que se tenga para poder operarlas dentro de la empresa o fuera de ella.

1.1.1 TÉCNICAS PRESENCIALES

1.1.1.1 Observación

La observación es la ruta para buscar la mayoría de escenarios que permitan al ingeniero social obtener información, de un lugar, persona o grupo de personas. Manteniendo una capacidad visual para obtener la mayor cantidad de información en el menor tiempo posible.

Quizá sea un ataque muy simple pero es muy efectivo, observar el entorno y aprovechar los datos que están a la vista cuando el sentido común indica que deberían guardarse en un lugar seguro. Mucha información puede destilarse mediante esta técnica puesto que mediante un análisis sobre el interior, buscar diálogos, seleccionar formas y operaciones que se puedan realizar para obtener información.

Esta técnica se aplica a varios casos en sí que se dan para que se obtenga la información [2]

- Contraseñas puestas en un post-it en la pantalla del ordenador.
- Charlas descuidadas del personal, habladurías con otras personas.
- Oferta ficticia de empleo a empleados de otras empresas, como pretexto para efectuar profundas entrevistas a los mismos.

1.1.1.2 Mirando Por Encima del Hombro

También conocido como surf hombro o mirando por encima del hombro de una persona tratando de obtener su código de acceso, contraseña / PIN[1] mientras lo digita, o tratando de escuchar conversaciones de las cuales puede obtener una mayor cantidad de información en el menor tiempo posible.

Existen algunas variaciones de surf hombro que permiten apropiarse de información de manera ilícita:

- Usando unos binoculares o un telescopio de baja potencia para ver quién digita código PIN.
- Recubrimiento el teclado con una fina capa de material ultravioleta de forma que posteriormente puede ver qué teclas pulsa el usuario.

También hay algunas variaciones auditivas que, permite tratar de apoderarse de una manera más rápida de la información. [15]

- Escuchar a un usuario las pulsaciones en el teclado de su contraseña, permitiendo buscar cuantos caracteres pueda poseer su contraseña.
- Escuchar a un usuario marcar un PIN en un teclado de teléfono y determinar el código PIN desde el sonido de los tonos DTMF[2].

Estas técnicas no solo ocurre a nivel informático sino en seguridad perimetral y de accesos.

1.1.2 TÉCNICAS NO PRESENCIALES

1.1.2.1 Contraseña Perdida

La técnica especializada o empírica del uso de acciones estudiadas o habilidosas que permiten voluntariamente que las personas realicen actos de recuperación de contraseñas, sin importarle las medidas de seguridad que existen.

Para obtener una contraseña se utiliza los propios sistemas de recuperación de contraseñas de casi la mayoría de servicios de la red. [2]

[1] PIN : Número de Identificación Persona
[2] DMTF : Dual Tone Multifrencuency

1.1.2.2 E-MAILS

El e-mails es una herramienta simple y poderosa para la distribución de mensajes a un gran número de personas. Su uso proporciona que los ataques sean posibles gracias a la efectividad que tienen en los usuarios normales los e-mails provenientes de entidades públicas o servicios privados.

El volumen del correo electrónico manejado puede hacer que no se preste la atención necesaria a cada uno de los mensajes que se reciben. Este hecho es muy útil para un atacante informático de ingeniería social.

La mayoría de los usuarios del correo electrónico se sienten bien consigo mismos cuando manejan la correspondencia; se trata del equivalente electrónico de mover el papel de una bandeja de entrada a una de salida. Si el atacante puede realizar una solicitud que no requiera acciones complicadas por parte de la víctima, ésta aceptará hacer algo sin ni siquiera pensar en lo que está haciendo. [16]
En la tabla 1 se muestra objetivo de los ataques, descripción y el costo que determina el riesgo de cada uno de ellos a una organización.

Tabla 1. 1 Ataques en línea por correo electrónico y costos [16]

Objetivos de los ataques	Descripción	Costo
Robo de información de la compañía	El pirata informático se hace pasar por (suplanta a) un usuarios interno para obtener información de la compañía	Información Confidencial Credencial
Robo de Información Financiera	El pirata informático usa la técnica de suplantación de identidad (phishing) (o “spear-phishing”) para solicitar información confidencial de la compañía, como detalles de cuenta	Dinero Información Confidencial Credibilidad
Descarga de malware	El pirata informático engaña a un usuario para que haga clic en un hipervínculo o abra un archivo adjunto y, de esta forma, infecte a la red de la compañía.	Disponibilidad comercial Credibilidad
Descarga de software del pirata Informático	El pirata informático engaña a un usuario para que haga clic en un hipervínculo o abra un archivo adjunto y, de esta forma, descargue un programa suyo que use recursos de la red de la compañía.	Recursos Credibilidad Comercial Dinero

Hay formas comunes de ataque:

- La primera consiste en un código malicioso, como la que utilizan para crear un virus. Este código se oculta generalmente en un archivo adjunto a un correo electrónico. La intención es que un usuario desprevenido abra el archivo y de esta manera infecte la red o su equipo.

- El segundo implica fraude, el bajo nivel de protección y falsas alarmas de virus. Estos han sido diseñados para obstruir los sistemas de correo por un virus de la presentación de informes inexistentes o de la competencia y se pide al destinatario que envíe una copia a todos sus amigos y compañeros de trabajo. Como la historia ha demostrado, esto puede crear un efecto de bola de nieve importante, una vez iniciado.

- La tercera el envió de correo anónimo se lo puede realizar mediante varios remailers[3] que son servidores que reciben mensajes de correo electrónico con instrucciones acerca de donde enviar enseguida el mensaje, y sin revelar el remitente del mensaje [15]. De esta manera se tendrá una buena dosis de anonimato. Se suele usar un remitente falso en lugar de anónimo.

  Un correo siempre deja huella de dónde se envió. Existen empresas que se encargan de enviar los emails al destinatario, pero mostrándose como un remitente a ellos mismos, de forma que el usuario o destinatario nunca conocerá la verdadera persona que lo envió. Por ello el Ingeniero Social utiliza esta técnica para obtener información de manera que el usuario no tenga incertidumbre al momento de recibirlo.

  De acuerdo a estos ataques se genera un alto nivel de desconfianza para recibir o enviar un correo, puesto que puede ser que el mismo terminará siendo víctima de cualquier amenaza.

1.1.2.3 IRC (Internet Relay Chat) U Otros Chats[4]

Por medio de los canales de IRC y Chats se puede llegar a obtener información amplia mediante la ingeniería social. El nivel de seguridad de estos sistemas de comunicación es bajo, ya que existen hackers que intentan engañar a los usuarios de las salas de conversaciones o "Chats" para que descarguen y ejecuten software malicioso: como virus, gusanos, troyanos que pueden dejar desprotegido al computador ante un ataque.

Con el aumento de usuarios de IRC, chats y mensajeros instantáneos los hackers se encuentran en las salas de Chats en Internet, usando herramientas automatizadas, donde envían anuncios en los que proporcionan descargar software para música, antivirus, fotografías, videos, y música, entre otros.

[3] Remailers: Repetidores de correo
[4] Chats: charla o cibercharla

Sin embargo los atacantes utilizan las técnicas de Ingeniería Social en el momento que se realiza esta descarga, donde pueden comprometer al sistema con virus o un *keylogger*[5], [17] que guarda en memoria todo lo que se escribe en el teclado y luego lo envía al intruso, analizando las teclas oprimidas, e ilícitamente el hacker puede deducir fácilmente los *passwords*[6] del usuario.

CERT/CC[7], una de las principales instituciones dedicadas a la seguridad en Internet, emitió que ha recibido informes de ataques de ingeniería social en los usuarios de Internet Relay Chat (IRC)[8] y mensajería instantánea (IM). Los informes de CERT/CC indican que decenas de miles de sistemas recientemente se han comprometido debido al uso indebido de la mensajería instantánea. [19]

En la Tabla 2 los ataques por medio de el envió de correos electrónicos dentro de la organización, y como se filtra un pirata informático para realizar ataques. La distinta funcionalidad y el número de personas que pueden ser objeto de ataque en una organización y el costo que se producirá en cuanto seguridad.

Tabla 1. 2. Ataques por mensajería Instantánea y costos [16]

Objetivos de los ataques	Descripción	Costo
Solicitud de información confidencial de la compañía	Los piratas informáticos usan la suplantación por mensajería instantánea para hacerse pasar por un compañero de trabajo y solicitar información de la compañía	**Información confidencial** Credibilidad comercial
Descarga de malware	El pirata informático engaña a un usuario para que haga clic en un hipervínculo o abra un archivo adjunto y, de esta forma, infecte la red de la compañía.	**Disponibilidad comercial** Credibilidad comercial
Descarga de software del pirata informático	El pirata informático engaña a un usuario para que haga clic en un hipervínculo o abra un archivo adjunto y, de esta forma, descargue un programa suyo, como un motor de correo, que use recursos de la red de la compañía.	**Recursos** **Credibilidad comercial** Dinero

[5] KEYLOGEER: registrador de teclas.
[6] PASSWORD: contraseña o clave.
[7] CERT/CC : Centro de Coordinación de Emergencias Informáticas
[8] IRC Internet Relay Chat.

1.1.2.4 Teléfono

El teléfono es el medio predilecto de los ingenieros sociales, ya que es donde se registra ataques por medio de personificaciones falsas y de persuasión a los usuarios. Las opciones de comunicación la mayoría impersonal, debido a que el usuario objeto del ataque no puede ver al atacante, ya que se valdrán de tretas engañosas, amenazas, confusiones falsas, falsos reportes de problemas, entre otros [19].

El teléfono es un vector de ataque excelente, permite la ocultación del número para mantener un anonimato de manera simple, donde podrán actuar a distancia, incluso desde otro lugar lo que permitirá hacer más difícil la búsqueda y captura del ingeniero social. La voz permite ofrecer mucha información, pero los atacantes buscarán la obtención de la información basándose en el estado de ánimo del interlocutor para de esta manera saber si no es un profesional del medio y por lo tanto obtener un grado de confianza, para que no se produzca denuncia mientras se mantiene contacto telefónico. La mayoría de veces trataran algo puntual o intentaran saltar la barrera en busca de información más profunda.

Los teléfonos móviles, complican un poco a los atacantes, ya que no existe una comunicación directa entre persona y dirección o número telefónico. Pero puede darse llamadas repetitivas desde el mismo número que está intentado establecer comunicación y de esta manera obtener la información.
Se han detectado troyanos que actúan como micrófonos cuando reciben una llamada de cierto número de teléfono reconocido por el software malicioso. Esto permite al atacante llamar a un teléfono infectado, el software malicioso reconoce el número e intercepta la llamada para que no suene y evitar que el afectado se percate, pero a partir de ese momento, el dispositivo actúa como un micrófono y el atacante escucha las conversaciones que se mantienen alrededor del teléfono. Como se muestra en la Figura 1.

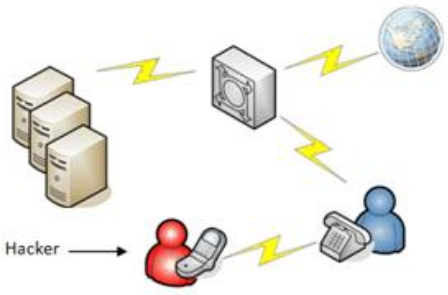


Figura 1. 1. Ataques Telefónicos a Centrales [16]

En la Tabla 3 tenemos las solicitudes de información o acceso telefónico que constituyen una forma de ataque. Si el destinatario sospecha o no decide responder a una solicitud, el pirata informático o atacante sólo tiene que colgar. Sin embargo, hay que tomar en cuenta que dichos ataques son más sofisticados que el hecho de que un pirata informático simplemente llame a una compañía y solicite el

ID y la contraseña de un usuario. Éste normalmente presenta una situación, en la que pide u ofrece ayuda, antes de realmente solicitar la información personal o de la empresa.

Tabla 1. 3. Ataques a Centrales de Conmutación Telefónica y Costos [16]

Objetivos de los ataques	Descripción	Costo
Solicitud de la información de la compañía	El pirata informático se hace pasar por un usuario legítimo para obtener información confidencial.	Información confidencial Credibilidad comercial
Solicitud de información telefónica	El pirata informático se hace pasar por un técnico para obtener acceso a la central PBX con el fin de realizar llamadas externas.	Recursos Dinero
Uso de la central PBX para tener acceso a sistemas informáticos.	El pirata informático entra en los sistemas informáticos, mediante una central PBX, para robar o manipular información, infectar con malware o usar recursos.	

El sistema de voz sobre IP (VoIP)[9], aun no presenta grandes actividades de amenaza, y que existe aun relativamente un bajo número de instalaciones, pero puede generalizarse tanto como el correo electrónico y mensajería instantánea.

1.1.3 TÉCNICAS NO PRESENCIALES NO AGRESIVAS

1.1.3.1 Buscando En La Basura

También conocido como trashing[10], es a menudo un ataque serio efectivo, la obtención de información secreta o privada que se logra por la revisión no autorizada de la basura (material o inmaterial) descartada por una persona, una empresa u otra entidad, con el fin de utilizarla por medios informáticos en actividades delictivas.

[9] VoIP .- Voz sobre Protocolo de Internet
[10] Trashing.- basura.

Entre la basura se puede descubrir todo tipo de material útil:

- Papeles desechados clasificados y sin clasificar
- Directorios telefónicos internos
- Inventarios
- Organigramas.
- Memorandos Internos.
- Manuales de Políticas de la Empresa
- Agendas en Papel de Ejecutivos con Eventos y Vacaciones.
- Manuales de Sistemas.
- Impresiones de Datos Sensibles y Confidenciales.
- "Logins", "Logons" y contraseñas.
- Listados de Programas (código fuente).
- Disquettes y Cintas.
- Papel Membretado y Formatos Varios.
- Hardware Obsoleto

Estas actividades pueden tener como objetivo la realización de espionaje, coerción[11] o simplemente el lucro mediante el uso ilegítimo de códigos de ingreso a sistemas informáticos que se hayan obtenido en el análisis de la basura recolectada. [21]

Los sujetos no permiten caracterizar y plasmar el delito ya que pueden variar, cada atacante se muestra de distinta forma y en distinta ubicación, por lo tanto, mantendrán diferenciaciones en los delitos y de acuerdo al procedimiento penal este se llevara a cabo según su delito.

"Esto puede representar una amenaza importante para usuarios que no destruyen la información crítica o confidencial al eliminarla." [13]. De esta manera resultara más fácil al atacante poder encontrar información potencialmente útil que debería haber sido eliminados en forma segura por ejemplo trituración.

1.1.3.2 Seguimiento De Personas Y Vehículos

Esta técnica permite al atacante observar a la persona y su sistema, con el objetivo de establecer vulnerabilidades y posibles accesos a la empresa, y uno de ellos es conocer a la víctima e investigarla, sin importar los recursos que tiene que utilizar para obtener la información. El trabajo externo del personal, la existencia de muchas sucursales son factores vulnerables para que el atacante empiece a identificar por donde debe iniciar el acercamiento sin causar mayor impacto.

[11] Coerción: amenaza de utilizar la violencia no solo física sino de cualquier otro tipo con el objetivo de condicionar el comportamiento de los individuos.

El propósito del atacante es vulnerar cualquier sitio que le proporcione acercamiento a la víctima, con el fin de llegar a la información que el personal maneje.

1.1.3.3 Vigilancia De Edificios

La seguridad física dentro de la ingeniería social es uno de los controles primordiales a nivel de seguridad del perímetro de un edificio y medio ambiente incluyendo: vigilancia y los dispositivos de detección para el propio edificio, puertas, cerraduras, ventanas y rejas, conducción, la luz del techo, y las trampillas, cámaras internas, detección de intrusos, y sistema de control de acceso.

La seguridad de la información mantendrá controles para su acceso, de manera que si un atacante logra tener éxito y violar la seguridad e ingresar al edificio, estos controles no permitirán que ingrese para extraer la información, sin activar las alertas de seguridad del edificio

1.1.3.4 Ingeniería Social en Situaciones De Crisis

En situaciones de crisis evolucionan los engaños y las puertas a los ataques de ingeniería social, especialmente aquellos en que los usuarios mal intencionados aprovechan el peso de una auditoria o de los reguladores para sacar información.

La posibilidad de que, por el hecho de acreditarse como auditores o inspectores, y con la predisposición de ofrecer máxima ayuda, los usuarios acaben entregando acceso físico y/o lógico a los activos de información de las empresas, sin haber comprobado antes la legitimidad de estos peticionarios.

La crisis expuesta mediante el engaño telefónico y por correo electrónico, es algo que se presenta a menudo y es de conocimiento para una atención oportuna y necesaria, ya que esto puede presentar de distinta manera a las empresas.

1.1.4 MÉTODOS AGRESIVOS

1.1.4.1 Suplantación De Personalidad

La suplantación de identidad adopta muchas formas con la ingeniería social, para engañar a usuarios y convertirlos en víctimas del phising[12] o estafas. En ocasiones, los atacantes se

[12] Phising: estafa por correo electrónico

apoyan en vulnerabilidades tecnológicas para obtener el control de cuentas de correo electrónico o perfiles de mensajería instantánea, aumentan los casos en los que son los propios usuarios quienes crean cuentas ficticias o falsificadas con la intención de actuar bajo el anonimato de un nombre falso, dañar los intereses de terceros o cualquier otro motivo. En cualquier caso, la suplantación de identidad supone hacerse pasar por otra persona física o jurídica.

La suplantación de identidad llegó al mundo de los blogs y las redes sociales arrasando con perfiles de empresas y particulares, y la realidad es que sigue presente, manteniendo un cierto clima de inseguridad en la red.

"Se trata de una práctica muy común, y que acostumbra a llevar aparejada la comisión de distintos delitos, lo que puede llegar a comprometer seriamente a la víctima de la sustracción, especialmente en aquellos casos en los que se utiliza la cuenta suplantando la identidad del verdadero usuario." [24]

1.1.4.2 Chantaje O Extorsión

La ingeniería social se ha visto como una técnica de manipulación y extorsión de las empresas, organizaciones y personas con una finalidad egoísta. Los ingenieros sociales no solo usan tácticas para atacar a las empresas, también pueden llegar a corromper las fronteras de seguridad e intimidad de las personas infectando los equipos de virus y gusanos.

No sólo debe saber usar un buen sistema operativo ni saber infringir contraseñas de alta seguridad, sino también en poseer ciertas características como el ingenio, persuasión, argumentación, razonamiento, sutileza y el carisma, además existen muchas personas que no pueden evitar dejarse seducir por estas cualidades. Él es quien trata a las demás personas como sus marionetas y puede tomar ventajas de su conocimiento para su propia conveniencia; es una persona lista y timadora. Al igual que estafadores y defraudadores en general, los ingenieros sociales aprovechan de la credulidad humana.

La seguridad es, al final, siempre es un problema de personas, pero "la ingeniería social intensifica la necesidad de abordar la debilidad humana como un problema que requiere soluciones". [25]

Maneras de actuar de un ingeniero social mediante un chantaje o extorsión [26]:

- La capacidad de persuadir, coaccionar o manipular a otras personas.
- La credibilidad y la empatía útil para mentir de manera convincente y el establecimiento de la confianza, lograr que la gente a abrirse y revelar información casual, por ejemplo, halagarlos o coqueteando.
- La confianza, la valentía y la agresividad, junto con la experiencia para saber cuándo presionar.

- Ser buenos para escuchar, recordar, relacionar, y el uso de fragmentos de información útil.

1.1.4.3 Presión Psicológica

Con el manejo de la Ingeniería Social se requiere solamente de astucia, manipulación, paciencia y una buena dosis de psicología.

Mediante esta técnica se pretende penetrar en redes y obtener secretos, engañando a los usuarios para comprometer su seguridad. Su éxito radica en apelar a las inclinaciones más profundas de la persona: el miedo, el deseo, la codicia o incluso a la bondad natural."

La naturaleza del comportamiento humano y de nuestras debilidades psicológicas, fácilmente pueden ser explotadas para obtener información mediante el uso de técnicas básicas y avanzadas; esto a un lado, la inteligencia que requieren libremente renunciar a que el conocimiento y alardear en grupos, en forma de presumir una través del uso de la ingeniería social, pero hay que cuestionar la calidad de la información, tal como se atrevería uno cuestionar la inteligencia recogidas a través del uso de la tortura o la presión psicológica.[27]

Hoy en día las empresas se centran en la inteligencia, y emplean los psicólogos y sociólogos de tiempo completo, no sólo en un papel analogía, pero también forma parte del programa de capacitación fundamentales de empresas, cada oficial de inteligencia se examina el potencial para la debilidad y la posible "sugestivo", es decir, se puede manipular el agente, a convertirse o debilitar, a divulgar información confidencial.

1.2 ATACANTE

1.2.1 PERFIL DE UN ATACANTE INFORMÁTICA

Es una persona de apariencia normal con miedos y dudas, es una persona obsesiva por la información es extrovertida e investiga todo lo relacionado con la informática y electrónica le gusta pasar horas y hasta días frente al computador acumulando conocimiento técnicos elevados y saber cómo utilizarlos.

Los estudios han encontrado que suelen ser [28]:

- Sexo masculino
- Edad entre 16 y 35 años

- Solitarios
- Inteligentes
- Competentes técnicamente

Existen en la sociedad distintos tipos de atacantes de forma acertada que nos permitirá identificarlos correctamente y conocerlos. Es posible crear un perfil de cada uno de ellos y conocer sus intenciones.

1.2.2 PERFIL DE UN INGENIERO SOCIAL

Los Ingenieros Sociales son personas que desde una corta edad se ven involucrados en el uso de equipos e Internet, son personas que tratan de conocer y aprender diferentes maneras de obtener beneficios sin verse inmersa su propia identidad.

Características que presenta un Ingeniero Social:

- Por lo general trabaja solo.
- Mantiene un lenguaje corporal bien preparado para mantener conexión con otras personas.
- Es educado, mantiene una postura adecuada, un saludo cordial, habla con seguridad y mira a la persona a los ojos, se adapta a las normas y al protocolo, la etiqueta, no se queja ni critica a nadie y hace sentir bien a los demás.
- También busca estar informado de nuevas tecnologías existentes.
- Un Ingeniero social no necesita apuntarse a los grupos de hackers ni leer ningún manual técnico.

Sin embargo, lo que un Ingeniero Social trata es de manipular los sentimientos y emociones de las personas tales como el miedo, la curiosidad, el sexo, la avaricia, la compasión y el deseo de agradar hacer bien su trabajo, el que contenga estas características se convierten en posible víctima de la Ingeniería Social.

Por lo tanto, un Ingeniero Social no necesariamente sale a buscar sus víctimas, es decir sabe que las personas padecen las mismas debilidades dentro y fuera de Internet, Además no necesariamente el IS necesita conocer sobre tecnología o ser una persona técnico.

1.2.3 DISTINTOS TIPOS DE ATAQUES

Tabla 1. 4. Descripción de Ataques

TIPOS DE ATACANTES	DESCRIPCIÓN
HACKER	• Un Hacker es alguien con conocimientos profundos sobre tecnología. Normalmente él sabe que terreno pisar y como evaluar las distintas circunstancias que se le presenten. • No difunde sus conocimientos, se jacta de ser un individuo soberbio, pero si comparte sus conocimientos con otros especialistas si son interesantes. • El Hacker aprende y trabaja solo, ya que lo único que lo rige es las ansias de buscar conocimiento.
CRACKER	• Tiene la capacidad de romper sistemas y Software y obtener seriales, o cracks con la finalidad de modificar el software o hardware de su estado original, es decir craquear sistemas. Este a diferencia de los hackers busca un beneficio personal que puede ser económico o por realizar algún daño. • El cracker investiga perfectamente ambas caras de la tecnología, sea en la parte física de la electrónica o en la parte de programación.
LAMERS	• Conocidos por su falta de conocimiento y obtención de cualquier tipo de información que encuentre en el Internet, ya que utiliza las herramientas de otros hacker que han creado y de esta manera se benefician de ellas. • El términos de Lamers es usado dentro de salas de chats y foros para describir a los usuarios que se comportan como novatos incompetentes durante más tiempo de lo normal. Aparentemente son inofensivos ya que solo presume de conocimientos o habilidades que realmente no posee.
BUCANEROS	• Un bucanero no interesa conocer ni aprender nada de tecnología especialmente de electrónica e informática. Son comerciantes que manejan negocios el cual no tiene escrúpulos a la hora de explotar un producto a nivel masivo, es un empresario que busca ganar dinero rápido de manera poco legal.
NEWBIE	• Es un novato simplemente. Le interesa navegar en Internet y presenta un verdadero interés por aprender y conocer, es un individuo que no le interesa sociabilizarse mucho, al igual que los Lamers investiga programas existentes y creados por otros hackers que le permitan el manejo y uso de apropiación

	de información siguiendo muy despacito los paso a ejecutar.
WANNABER	• Es un individuo que no aprende nada y se presiona al máximo en busca de resultados, mantiene mucha paciencia y tolerancia a cualquier situación que se le presente, su mayor dedicación es buscar quien le enseñe a ser un hacker.
PHISHERS	• Se los conoce por los ataques de Phishing que permiten la duplicación de una página Web para hacer creer a su visitante que se encuentra en la página original y de esta manera obtendría la información. Con esto se logra ampliar las redes y buscar más ataques propicios a empresas grandes y pequeñas. • Cuando se realizan ataques utilizan métodos rápidos, donde los usuarios finales les dan la facilidad de acceso y trabajar en forma paralela sin producir alteraciones o que los usuarios se den cuenta, ya que esto les generara una pérdida económica.
PIRATAS INFORMÁTICOS	• Es un Hacker, que busca programas para beneficio propio, que permite realizar copias de los distintos programas y venderlos sin contar con derechos de copyright. Son conocidos como estafadores, piratas que comercializan y crean copias ilegales.

1.3 MOTIVACIONES DEL ATACANTE

Las motivaciones del atacantes “Son los componentes claves para comprender a los hackers, pues permiten identificar qué propósito hay detrás de un intento de intrusión” [29].

- Reto: considerado como el elemento inicial de un hacker, puesto que aun no tiene su objetivo definido y por lo tanto juegan con el sistema al que ingresan sin importarles los daños que pueden ocasionar.
- Codicia: Este es su objetivo la mayoría de las veces, el deseo de obtener dinero, bienes, servicios o información que les proporcione mas lucro.
- Propósito mal intencionado: Generalmente el causar daños a una organización es su visión principal, el realizar daños como accesos no autorizados al sistemas, denegación de servicios, cambios o modificaciones a sitios Web, ingreso a correo electrónico, mal uso de contraseña, etc.

1.4 FASES DE LA INGENIERÍA SOCIAL

Los atacantes o hacker dentro de la ingeniería social buscan y analizan la manera de intimidar o confundirlo al usuario y de esta manera buscar beneficios más rápidos y seguros, podrían utilizar tretas como: compañeros de trabajo, auditores, administradores, familiares, y de esta manera explotar la información obtenida.

"Los métodos de la ingeniería social están organizados de la siguiente manera" [30]:

- Una fase de acercamiento es el proceso de mantener una buena relación de confianza con el usuario, intentando ganárselo indicando que es compañero nuevo de la empresa, proveedor, cliente, parte de la administración y de esta manera buscar la obtención en la información.

Dentro de esta fase tenemos el reconocimiento y búsqueda de nuestra víctima, en donde analizamos las vulnerabilidades que estén presentes para ser explotadas valiéndonos de herramientas y utilizando las técnicas de Ingeniería Social y de esta manera conseguir obtener la mayor cantidad de información.

- Una fase de alerta, permite conocer o tener una sospecha de algún riesgo que permita perturbar al usuario y proporciones información veraz y eficaz.

A través de esta fase se permite buscar y saber si existen accesos al sistema por parte de atacantes, si presentan distintas configuraciones realizadas al sistema. También establecer factores de riesgo habilidades, destrezas y conocimientos de seguridad informática, donde registren modificaciones realizadas por parte de un atacante.

Además no siempre se realizaran ataques por acceso al sistema sino también usando otros recursos que me permitan obtener información de cualquier manera, para ello se sustenta y se utiliza las técnicas de la Ingeniería Social, que permiten acceder a la información de varias maneras y causar daños.

- Una fase de cubrimiento de huellas permite destruir toda evidencia de actividades ilícitas y lo hace por varias razones como, poder seguir teniendo un acceso al sistema comprometido ya que si borra sus huellas los administradores o las personas encargadas de la seguridad de la red no tendrán rastros claros del atacante y podrá seguir ingresando al sistema en cualquier momento.

CAPITULO II

2. ESTUDIOS DE CASOS DE INGENIERIA SOCIAL

INTRODUCCION

Dentro del estudio de la Ingeniería Social se ha podido identificar y conocer muchos casos sobre ataques utilizando las técnicas como: observación, suplantación, correo electrónico, teléfono y otras más que han permitido revelar información sensible, o bien violar políticas de seguridad. Sin embargo muchos de los ataques registrados son por el descuido y falta de conocimiento del usuario, así como también proporcionar información en distintos medios sin que exista mayor seguridad electrónica.

En Internet se puede encontrar varios ejemplos de personas que han sufrido ataques de cualquier medio utilizando la Ingeniería Social y valiéndose de cualquier herramienta que le permite acceder a la información.

2.1 CASOS REALES

2.1.1 E-MAILS

2.1.1.1 Correos Maliciosos Que Simulan Provenir De CORREOS[13] [32]

Se envía un correo electrónico cuyo texto solo se puede ingresar pulsando un enlace que redirige al usuario hacia otro sitio en este caso un dominio belga del cual se descargará rápidamente un virus. El engaño es rápido y muy tentador para el usuario ya que se envía como un mensaje normal de otro correo, donde le informan que ha recibido un telegrama online y la forma de visualizarlo es pulsando en un enlace con ficheros malicioso.

A continuación en la Figura 3 se presenta un correo malicioso enviado. Los mensajes pueden variar ligeramente pero la mayoría de los que se han detectado en esta oleada tienen el siguiente aspecto:

[13] CORREO: Sociedad Estatal Correos y Telégrafos (Empresa España)

Figura 2. 1. Correo Electrónico Malicioso [32]

2.1.1.2 Campaña De Correo Masivo Con Un Falso Mensaje De DHL[14]

Se ha enviado correos falsos que contienen virus indicando ser un mensaje de la empresa de servicios de correo DHL [33] que buscan engañar al usuario para que este abra y ejecute el archivo. Los atacantes utilizan las técnicas del la Ingeniería Social en este caso mejorando la técnica de suplantación, el mensaje redactado correctamente e incluye un archivo adjunto que a simple vista pareciera ser un documento de texto (.doc), aunque en realidad es un ejecutable (.exe). A continuación en la figura 4 se indica el texto de este correo.

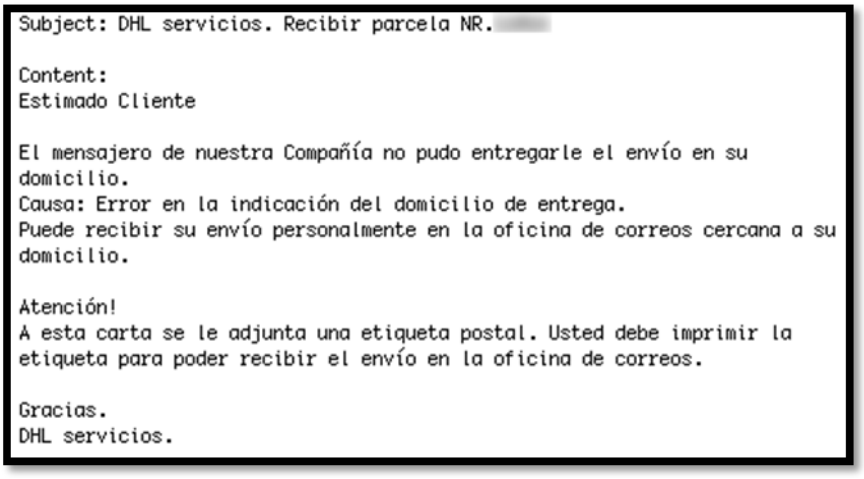


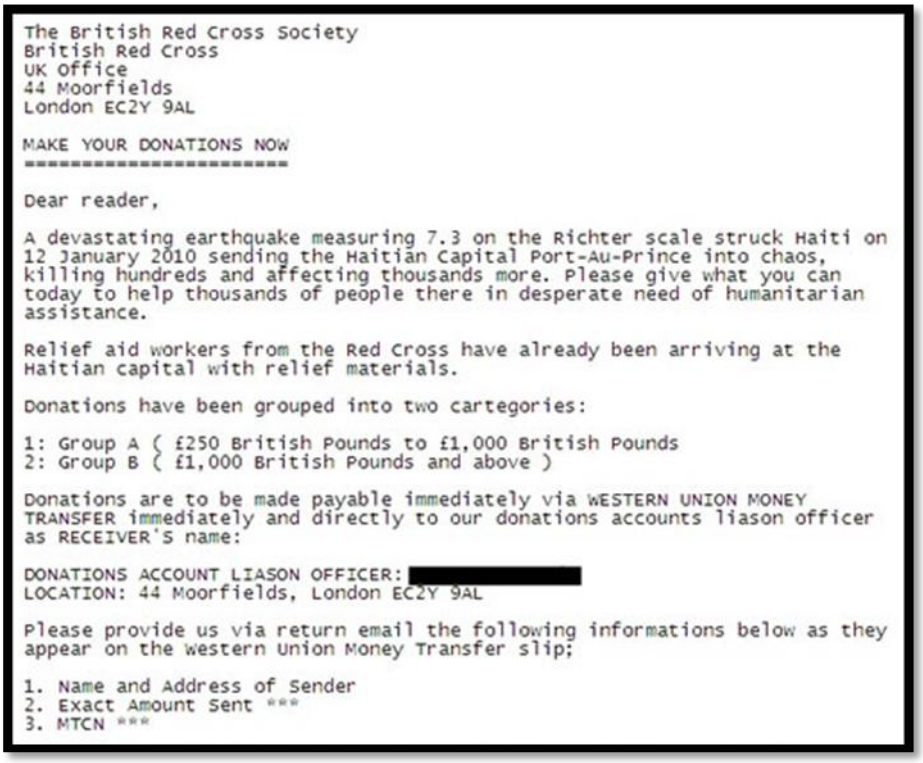
Figura 2. 2. Correo Electrónico Con Falso Mensaje DHL [33]

Este mensaje está conformado por una etiqueta postal falsa, con un número de fichero aleatorio, en realidad es un virus con diferentes características, desde un falso virus hasta un troyano capaz de proporcionar tomar control del computador.

14 DHL.- empresa de Alemania que realiza envíos a todo el mundo.

2.1.1.3 Terremoto De Haití Aprovechado Para Engañar A Los Usuarios[34]

Cuando se produjo el terremoto en Haití el 12 de enero los atacantes ya estaban listos para aprovechar esta oportunidad. Cuando un usuario buscaba información sobre esta noticia y se le presentaban a sitios poco seguros, no confiables, donde podían enlazarse con páginas maliciosas.



The British Red Cross Society
British Red Cross
UK Office
44 Moorfields
London EC2Y 9AL

MAKE YOUR DONATIONS NOW

Dear reader,

A devastating earthquake measuring 7.3 on the Richter scale struck Haiti on 12 January 2010 sending the Haitian Capital Port-Au-Prince into chaos, killing hundreds and affecting thousands more. Please give what you can today to help thousands of people there in desperate need of humanitarian assistance.

Relief aid workers from the Red Cross have already been arriving at the Haitian capital with relief materials.

Donations have been grouped into two cartegories:

1: Group A (£250 British Pounds to £1,000 British Pounds
2: Group B (£1,000 British Pounds and above)

Donations are to be made payable immediately via WESTERN UNION MONEY TRANSFER immediately and directly to our donations accounts liason officer as RECEIVER'S name:

DONATIONS ACCOUNT LIASON OFFICER: [redacted]
LOCATION: 44 Moorfields, London EC2Y 9AL

Please provide us via return email the following informations below as they appear on the Western Union Money Transfer slip;

1. Name and Address of Sender
2. Exact Amount Sent ***
3. MTCN ***

Figura 2. 3. Descarga de un Falso Programa e Infección De Equipo [34]

El envió de correos phishing, buscando engañar a los usuarios para que ayuden con donativos a las víctimas, pero en realidad las páginas del pago son falsa e intentan apoderase de la ingenuidad de las personas.

Con el acceso a estas páginas fraudulentas, intentan al usuarios persuadir de que su equipo está siendo infectado para de esta manera sugerirle descargue la solución de seguridad, de esta manera el usuarios compraría y descargaría el falso programa, sin darse cuenta que el usuario habrá dado una fuerte suma de dinero por algo que no funciona o simplemente infectara su equipo.

2.1.1.4 Microsoft Outlook Web Access (OWA) [35]

Se difunde por correo electrónico un mensaje falso que simula ser una actualización (OWA)[15] de la aplicación de Microsoft para acceder al programa Outlook a través de Internet. Una vez que el usuario realice falsas actualizaciones, esta infectando su equipo.

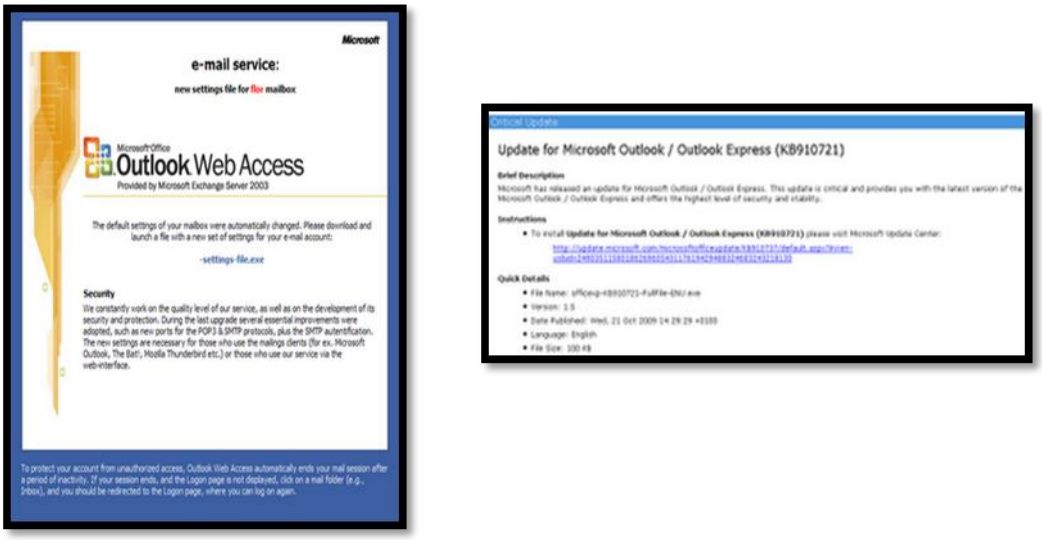


Figura 2. 4. Actualización en la Web Fraudulenta [35]

2.1.1.5 Facebook Aprovechado Para Engañar A Los Usuarios [36]

Los Usuarios de Facebook reciben un correo falso, o una invitación a unirse a un grupo de protesta para criticar un falso rumor en el que se afirma que en Facebook se cobrará por sus servicios a partir de los 6 meses. En la figura 7 se indica el tipo de correo.

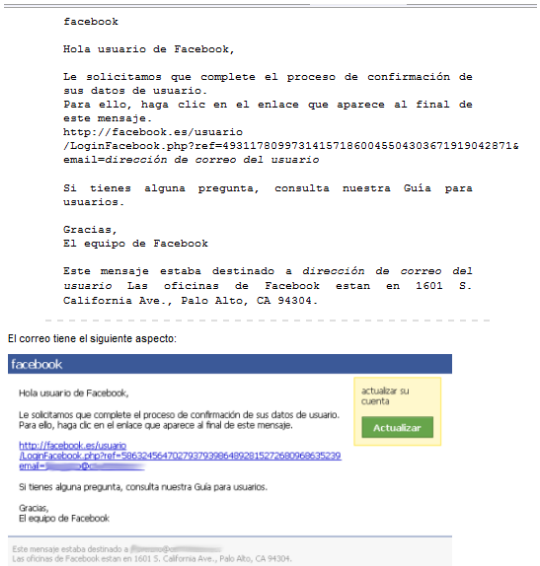


Figura 2. 5. Ataque en Red Social Facebook [36]

[15] Microsoft OWA: Microsoft Outlook Web Access

Mediante este vínculo se solicita al usuario que acceda a una dirección de Internet para confirmar sus datos como forma de engaño, sin darse cuenta el usuario que es una suplantación de la pagina original de Facebook y de esta manera sus datos serán sustraídos.

2.1.1.6 Nueva Oleada De Falsas Ofertas De Empleo [37]

Con el uso masivo del correo electrónico y las falsas ofertas de empleo a través del correo conocido como scam[16], los atacantes de una supuesta empresa buscan una víctima por correo e incluso por teléfono, de esta manera solicitan al usuario una cantidad de dinero por supuestos tramites. Para compensar esto los atacantes envían un cheque falso y para cuando la víctima se ha dado cuenta, el banco le notificara que es un cheque falso o sin fondos. A continuación en la figura 8 formato del correo.

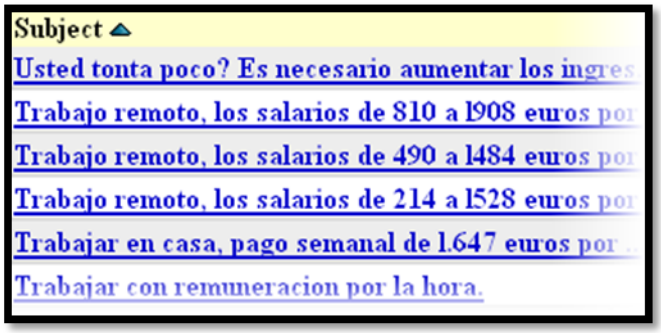


Figura 2. 6. Falsas Ofertas de Empleo [37]

2.1.1.6 Correo Malicioso Tras La Muerte De Michael Jackson [38]

El envío masivo de correos electrónicos con información a la muerte de Michael Jackson el día 25 de junio. El correo combina información verídica con información nueva muy impactante como por ejemplo: “video exclusivo de la CNN”. Directamente con este correo electrónico contiene enlaces a páginas no confiables, y a través de estas, la descarga de archivos con código malicioso. A continuación en la figura 9 el correo electrónico.

[16] SCAM: estafa a través de a un correo electrónico fraudulento

Figura 2. 7. Correo Malicioso Muerte De Michael Jackson [38]

En el uso de la ingeniería social, los atacantes aprovecharon el impacto de la noticia para enviar correos con enlaces que dirigen a páginas maliciosas e incitan la descarga de ficheros que contienen código malicioso.

2.1.1 CHATS

2.1.1.1 Suplantación De Un Programa De Envío De SMS [39]

El atacante utiliza una más de sus artimañas en este caso el engaño a través de correo electrónico no deseado y chats, involucrando al usuario a que descargue un software malicioso. A continuación en la figura 9 se proporcionaba la imagen de una empresa para realizar la descarga.

Figura 2. 8. Suplantación de un programa de envió de SMS

El usuario recibe un correo donde se le ofrece un falso software de envió de mensajes SMS de movistar existente, con el uso gratuito busca que lo descargue de una página web cuyo enlace esta en el correo, pero en realidad se trata de la descarga de un troyano.

Finalmente existen muchos más casos de ataques de Ingeniería Social en internet como técnica de infección principal, dando a conocer como el Ingeniero Social busca conseguir habilidades sociales relacionadas con la comunicación entre las personas, y de esta manera analizar posibles víctimas para propiciar distintos ataques dentro y fuera de la red.

Con la utilización de varias técnicas de Ingeniería Social que han venido desarrollándose y creando nuevas amenazas, en donde los usuarios resultan afectados de manera directa debido al uso inadecuado del Internet.

CAPITULO III

3. ANÁLISIS DE INCIDENTES DE INGENIERIA SOCIAL A USUARIOS DE LA UTPL

INTRODUCCIÓN

Con este trabajo se quiere lograr que una vez finalizado el análisis, se tenga en claro el concepto de Ingeniería Social, su objetivo, quienes lo utilizan, donde lo emplean, quienes son los más vulnerables y sobre todo, de qué manera se puede realizar un ataque y las nuevas amenazas que hoy por hoy pueden resultar de gran ayuda para emplear la Ingeniería social en todo ámbito laboral.

Con la utilización de recursos como la elaboración de Encuestas realizadas a Secretarias de Escuelas, Secretarias del Departamento Financiero, Docentes y Estudiantes, se pudo conocer las distintas debilidades frente a la Ingeniería Social.

Con el desarrollo de encuestas y resultados obtenidos a través de ellos podemos indicar cuáles son las vulnerabilidades con porcentajes más altos, y a quienes se pudo realizar ataques utilizando las técnicas de Ingeniería Social.

Para ello, se presentará un informe detallado de cada una de los ataques que se realizó en algunos de los departamentos de la UTPL, se describirá como se aplicó cada una de las técnicas de Ingeniería Social y sus resultados.

3.1 ANALISIS DE TECNICAS DE INGENIERIA SOCIAL

3.1.1 ENCUESTAS

Las Encuestas realizadas a los usuarios como: Secretarias de Escuelas, Secretarias del Departamento Financiero, Docentes y Estudiantes, tienen como objetivo principal obtener indicadores directos sobre el conocimiento de la Ingeniería Social y posibles vulnerabilidades.

El procedimiento de selección de usuarios de la Universidad para la realización de encuestas, se considero a quienes manejan información crítica de la Universidad.

Para el desarrollo de las encuestas se dividió en dos estratos, uno el de empleados de la Universidad en los que están: Secretarias de Escuelas, Secretarias del Departamento Financiero, Docentes, Personal Administrativo; y Estudiantes, la muestra a las que se aplicó la encuesta fueron:

- 100 Empleados de la UTPL. (Para ver encuestas Anexo 1)
- 150 Estudiantes de la UTPL (Para ver encuestas Anexo 2)

A partir de esto se pudo obtener resultados del conocimiento o desconocimiento del tema de Ingeniería Social y en donde existen mayores casos de vulnerabilidad. . (Para ver resultados Anexo 2)

- **ANÁLISIS DE RESULTADOS:**

Los resultados obtenidos se muestran a través de las distintas preguntas que se hizo en las encuestas, a empleados y estudiantes de la Universidad. De acuerdo a los datos estadísticos obtenidos a continuación se presenta algunas de las preguntas que proporcionaron información notable sobre el desconocimiento de la Ingeniería Social y las distintas herramientas que se usan para la obtención de información.

- **RESULTADOS DE ENCUESTAS REALIZADAS A EMPLEADOS**

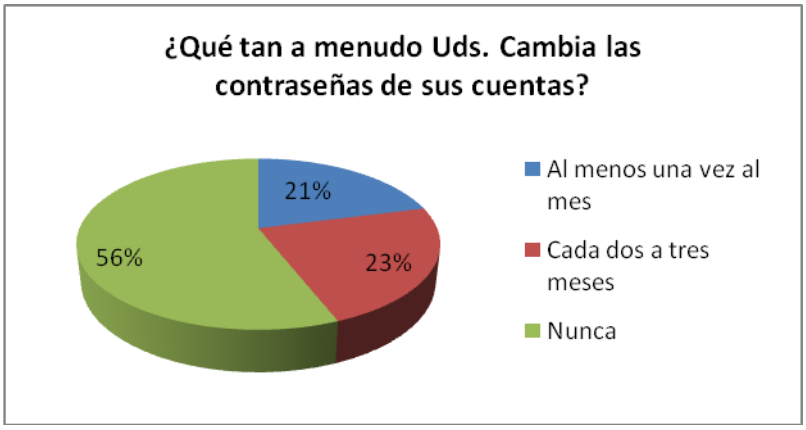


Figura 3. 1. Cambio De Contraseña

Figura 3. 2. Compartición De Clave

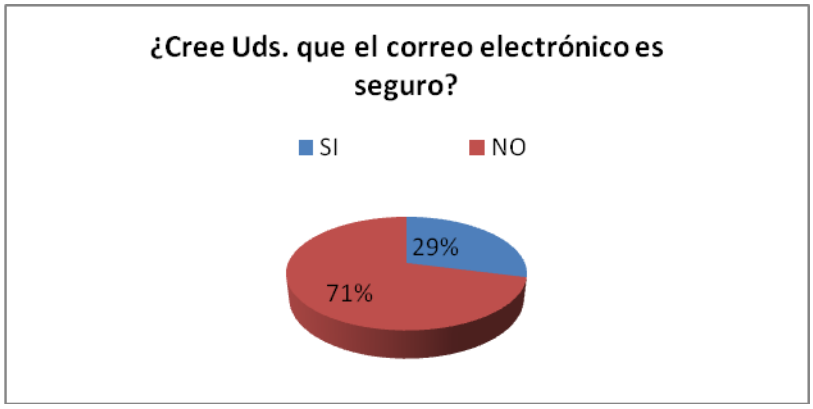


Figura 3. 3. Correo Electrónico

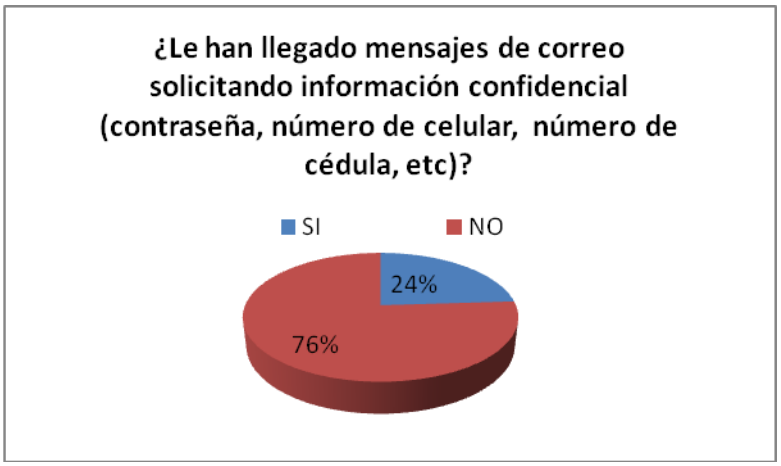


Figura 3. 4. Información confidencial

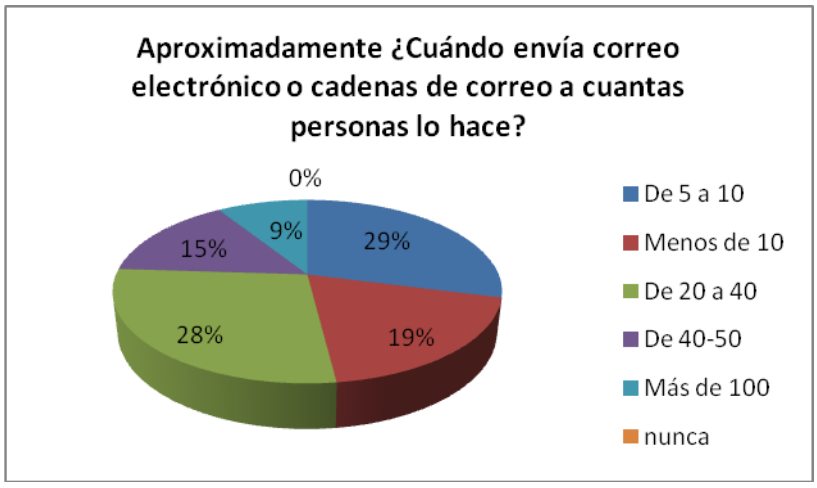


Figura 3. 5. Cadenas de Correo Electrónico

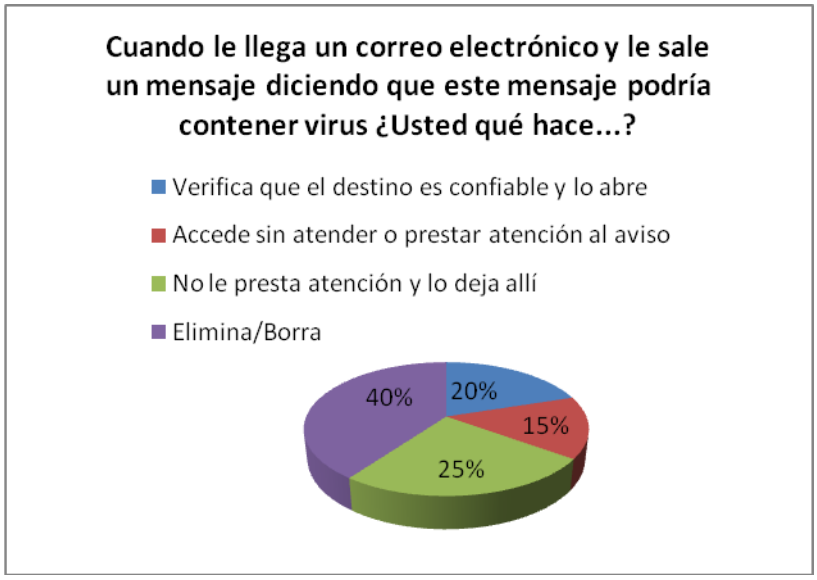


Figura 3. 6. Correo Electrónico y Virus

Figura 3. 7. Descuido de Contraseña

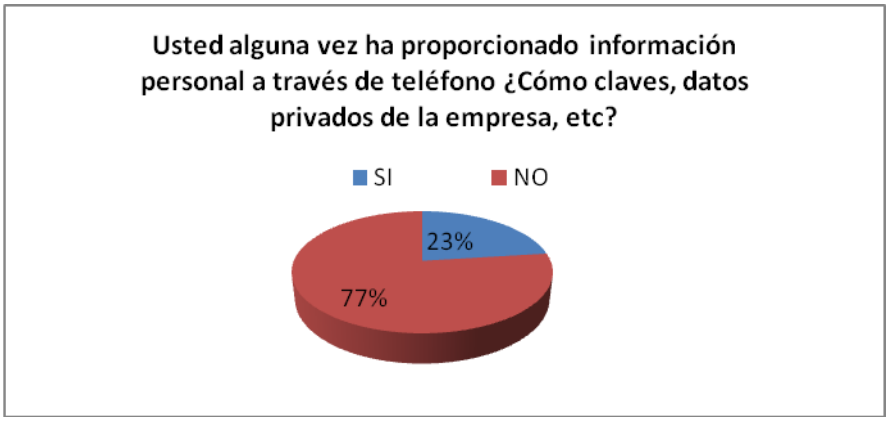


Figura 3. 8. Información Telefónica

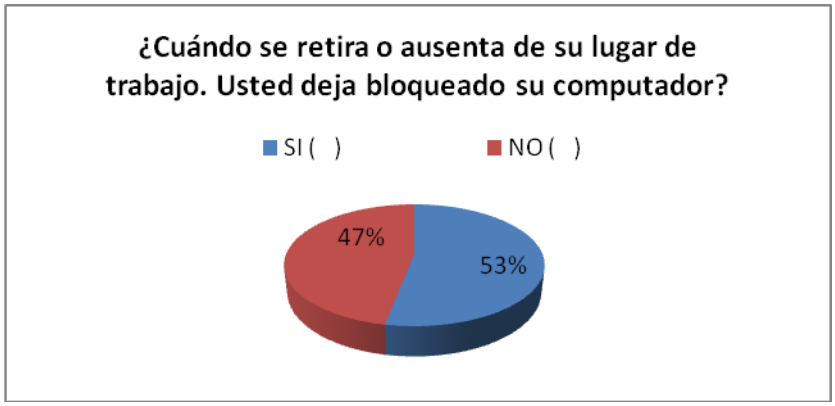


Figura 3. 9. Computador Bloqueado

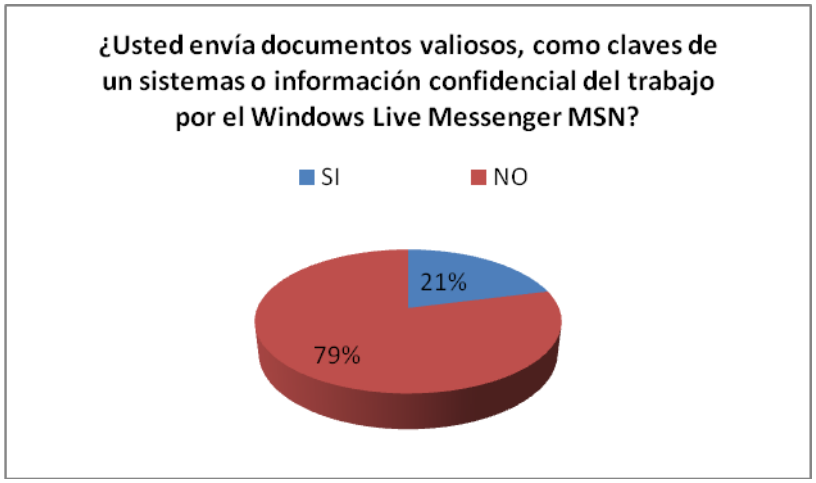


Figura 3. 10. Utilización de Windows Live Messenger MSN

- **RESULTADOS DE ENCUESTAS REALIZADAS A ESTUDIANTES**

Figura 3. 11. Ingeniería Social

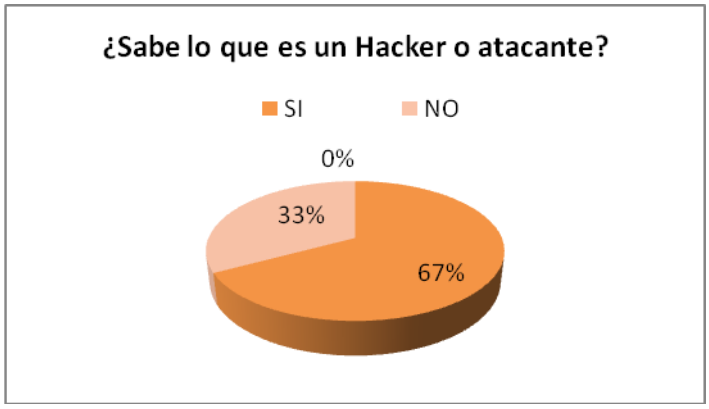


Figura 3. 12. Hacker o Atacante

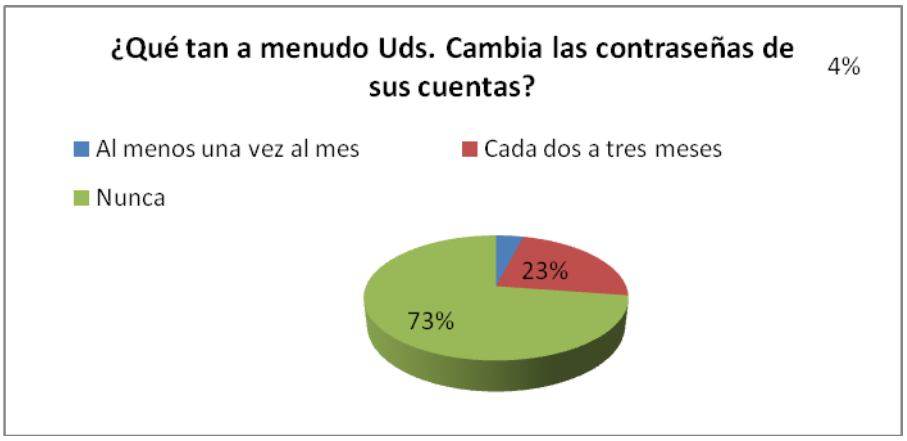


Figura 3. 13. Cambio De Contraseña

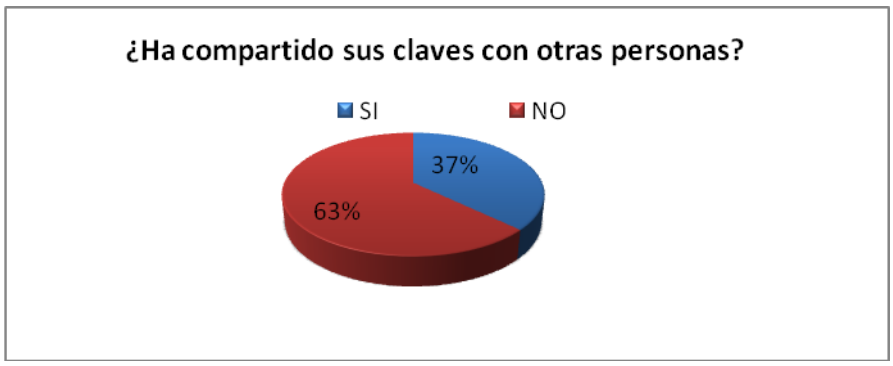


Figura 3. 14. Compartición De Claves

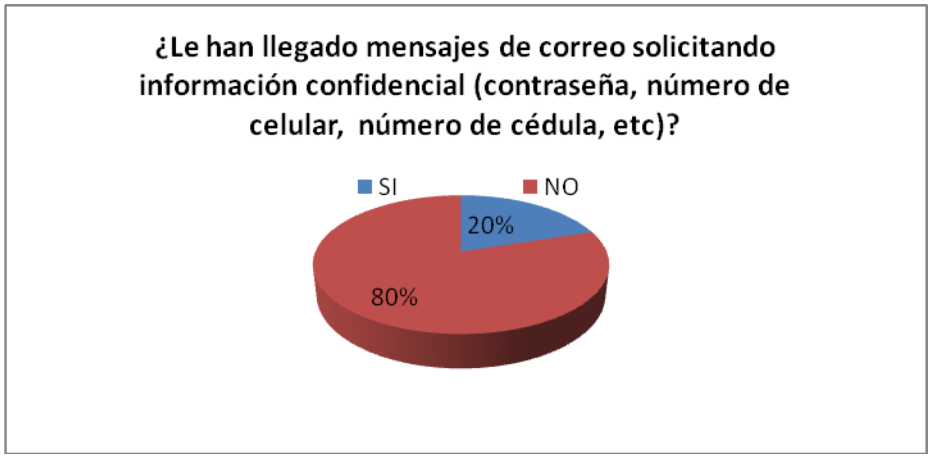


Figura 3. 15. Correo con Solicitud de Información

Figura 3. 16. Mensaje o Alerta de páginas

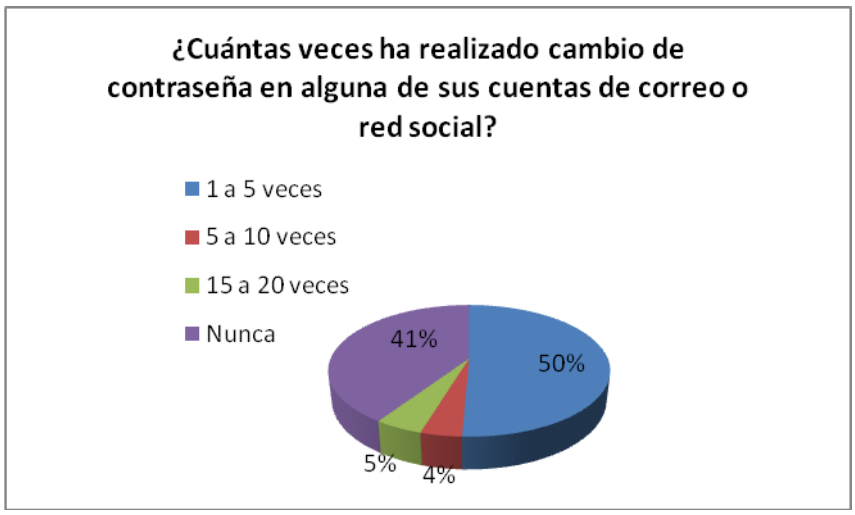


Figura 3. 17. Cambio de contraseña en Correo o Red Social

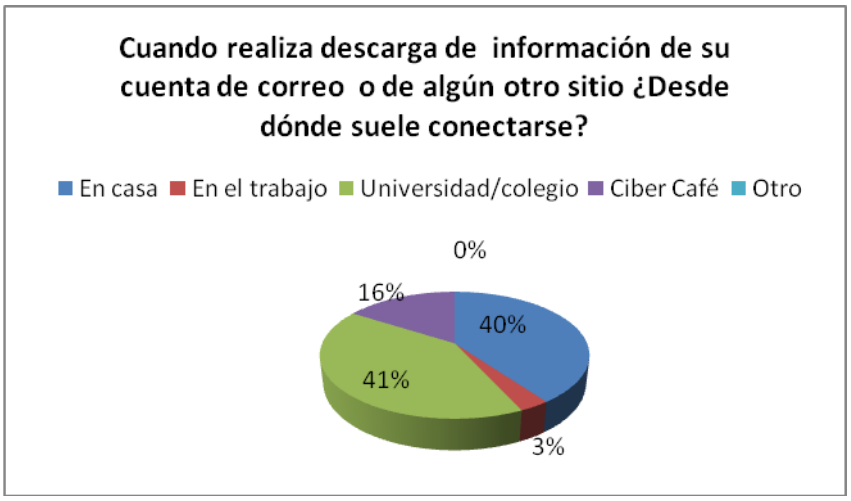


Figura 3. 18. Descarga de Información

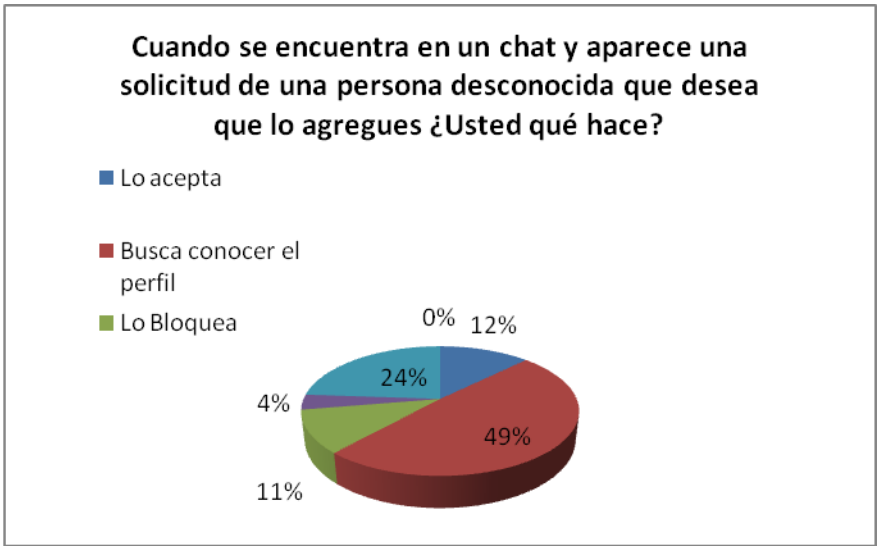


Figura 3. 19. Chat

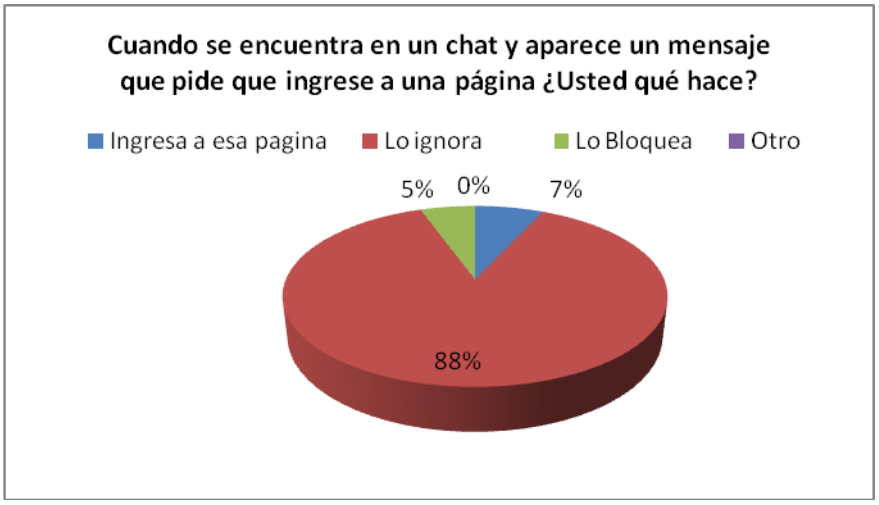


Figura 3. 20. Chat Ingreso a Página

Con el desarrollo de las encuestas realizadas a Empleados y Estudiantes de la UTPL, se pudo introducir a un análisis y observación sobre aspectos contemplados dentro de las encuestas, las mismas que marcaron la problemática para la aplicación de las técnicas escogidas para la Ingeniería Social. Análisis de algunas de las respuestas seleccionadas:

- Los usuarios indican que no cambian contraseñas, y tampoco el nivel de seguridad de las mismas.
- El uso y manejo del correo electrónico es algo cotidiano, demostrando un alto índice de envió de cadenas de correo.
- El acceso e ingreso a páginas que se presentan en sus cuentas de correo son utilizadas.
- Compartir información confidencial mediante el uso de correo electrónico a páginas que solicitan información personal.
- Algunos usuarios envían información confidencial mediante chats.

Los resultados obtenidos muestran que el conocimiento de las expectativas y grado de satisfacción de los usuarios, es una preocupación constante debido a la poca importancia que se les da a varios aspectos generales del manejo de información, y a la mala utilización de las herramientas electrónicas. Con el número de respuestas otorgadas dentro de la encuesta se pudo lograr los indicadores de percepción altos, para establecer los distintos criterios para realizar los distintos ataques de ingeniería social aplicados a la UTPL.

Entre ellos se pudo establecer cuales nos aportarían mejor información detallada:

- Técnica de suplantación y observación
- Técnica de envió de correo electrónico
- Técnica de teléfono
- Técnica robo de contraseña

Estas técnicas contribuirían definitivamente a la realización del estudio y evaluación de los aspectos más importantes recogidos mediante las encuestas, pero sobre todo para la de interpretación de resultados y diseño de políticas.

3.2 TÉCNICAS DE INGENIERÍA SOCIAL APLICADAS A LA UTPL

Se han seleccionado estas técnicas de Ingeniería Social en base a los resultados obtenidos por las encuestas antes realizadas a estudiantes y personal docente de la Universidad, y a estudios realizados posteriormente para investigar qué tipo de técnicas de Ingeniería Social se puede aplicar a continuación se las describe:

- Técnica de suplantación y observación
- Técnica de envió de correo electrónico
- Técnica de teléfono
- Técnica robo de contraseña

Las formas de ataques han sido distintas ya que cada una de ellas involucra manejar el tiempo y el lugar para desarrollar, es decir analizar donde existiría menor riesgo de sospecha, y lugares más vulnerables para poder realizar los ataques.

3.2.1 Técnica De Suplantación Y Observación

La ejecución de estas técnicas consistió en utilizar las distintas habilidades, conocimientos y aptitudes desempeñadas, para identificar posibles víctimas y dar inicio a la extracción de información. Para la realización de estas técnicas dentro de la UTPL básicamente se lo dividió en dos puntos estratégicos: Área de Secretarias y Departamento Financiero.

Para la suplantación se analizó que era más factible suplantar al personal de Soporte Técnico debido a que ellos tienen más acceso a los diferentes sitios de la UTPL y el personal esta consiente que este personal de la UTPL cambia constantemente de gestores y no tiene ningún tipo de identificación.

OBJETIVO:

- Obtener información de la UTPL mediante las técnicas de observación y suplantación.

VICTIMAS:

- 15 Secretarias de Escuelas y 8 Secretarias del Departamento Financiero.

HERRAMIENTA:

- Habilidad y conocimiento sobre las técnicas de observación y suplantación.

DESARROLLO DEL ATAQUE:

Para desarrollar estas técnicas se las ejecutó por separado y se las asocio dependiendo del lugar y la cantidad de personas que se encontraban en un departamento, para ello se realizó de la siguiente manera:

- Esta técnica se la realizaba una vez al día, desde lugares propicios y en silencio y tratando de memorizar la mayor cantidad de información disponible, por motivos de no levantar sospecha alguna.
- Se suplanto la identidad del personal de soporte técnico explicando a la secretaria que se iba a revisar el antivirus.
- Las secretarias proporcionaban disponibilidad total del equipo, mientras ellas hacían otro tipo de actividad o algunas de ellas se retiraban del departamento.
- Existían casos en donde se podía ingresar al usuario administrador del equipo y observar que tipo de información maneja.
- Se pudo recoger datos del equipo como dirección IP y usuario. (Ver anexo 5)
- La técnica de observación se la realizó ingresando de manera particular a las escuelas sin necesidad de preguntar algún tipo de información, asimismo cuando existía demasiadas personas en cada departamento y se podía observar libremente la documentación sensible sobre los escritorios o pantallas de los equipo. (Ver anexo 5)

RESULTADOS:

Al finalizar la ejecución de la técnica se obtuvo los siguientes resultados:

- Un 82% proporcionara información confidencial como:
  - claves del equipo
  - documentos con los que trabajan
  - datos personales (direcciones …)
  - etc., mientras que con
- un 18% no entregan información.

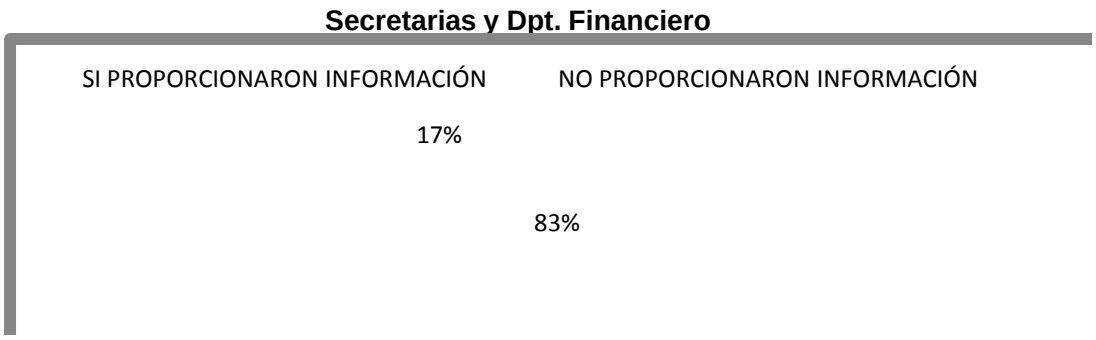


Figura 3. 21. Porcentajes de Técnica de Observación y Suplantación

De esto se puede concluir que:

- Existe el riesgo de fuga de información dentro de la UTPL debido a que un gran porcentaje de secretarias entera información a personal desconocido.
- El personal de soporte técnico es fácilmente suplantable por lo cual se debe tomar controles de seguridad para que no ocurra esto.

3.2.2 Técnica De Envió De Correo Electrónico

El correo electrónico es una forma de acercamiento hacia la víctima que permite introducirse disfrazado de muchas formas, ya sea que la dirección de correo electrónico resulte familiar o el asunto del e-mail de cierta forma "ataque" los sentimientos como la curiosidad, la avaricia, la compasión o el miedo es donde el usuario se vuelve susceptible a abrirlo.

Al haber obtenido mediante la técnica de observación información sobre los usuarios como la dirección de correo, permite de una manera más rápida centrar el objetivo en lanzar ataques por medio de correo electrónico hacia los usuarios de la UTPL, como Área de Secretarias, Departamento Financiero y Estudiantes.

OBJETIVO:

- Determinar cuántas personas contestan correos no solicitados.

VICTIMAS:

- 40 Correos Electrónico dividido: 20 Secretarias de la UTPL y 20 a Estudiantes de la UTPL.

HERRAMIENTAS:

- Para poder desarrollar esta técnica se utilizo herramientas como WhoReadMe[17] y ReadNotify[18] que son servicios de correo electrónico de seguimiento en línea que permitió el envió de mensajes desde su sitio web y recibir mensaje de alerta cuando ha sido recibido y abierto el archivo adjunto.

DESARROLLO DEL ATAQUE:

[17] ***WhoReadMe:*** *es un servicio* gratuito *y online para saber si los* e-mails *que envías son leídos por su destinatario.*
[18] ***ReadNotify:*** *es un servicio web destinado a la gestión y control de los correos enviados, pudiendo borrarlos, saber cuando fueron abiertos o reenviados, o averiguar datos de la máquina en que se abrieron.*

- Para la obtención de correos electrónicos de secretarias y estudiantes se lo consiguió con la utilización de la técnica de observación, la cual permitió obtener correos electrónicos de documentos confidenciales, en donde constaban datos de secretarias y estudiantes.
- Primeramente antes de enviar el correo electrónico se busco de que manera el mensaje puede ser tentativo para el usuario y de esta manera asegurarse que lo abra, el sujeto del mensaje fue de AVISO IMPORTANTE desde un correo creado para poder enviar cualquier tipo de mensaje, el correo es móvile_technology@hotmail.com.ar y su contenido trataba sobre la nueva tecnología móvil, de esta manera sea tentativo al usuario y abra el correo, posteriormente ejecute al archivo adjunto que enlazaría a la página que contiene incrustada una imagen transparente con un identificador dentro del correo electrónico el cual permitiría verificar que ha sido recibido y ejecutado.(Ver anexo 6)
- Una vez recibido una notificación al correo de que ha sido abierto y ejecutado el archivo adjunto, se habilita una ventana en la herramienta ReadNotify en donde envían los datos del equipo donde fue leído el mensaje y ejecutado el archivo. (Ver anexo 6)

RESULTADOS:

- De un total 20 correos enviados a Secretarias de Escuelas y Departamento Financiero, se indica que abrieron y ejecutaron el mensaje un 55%, mientras que un 45% ignoraron el mensaje recibido.

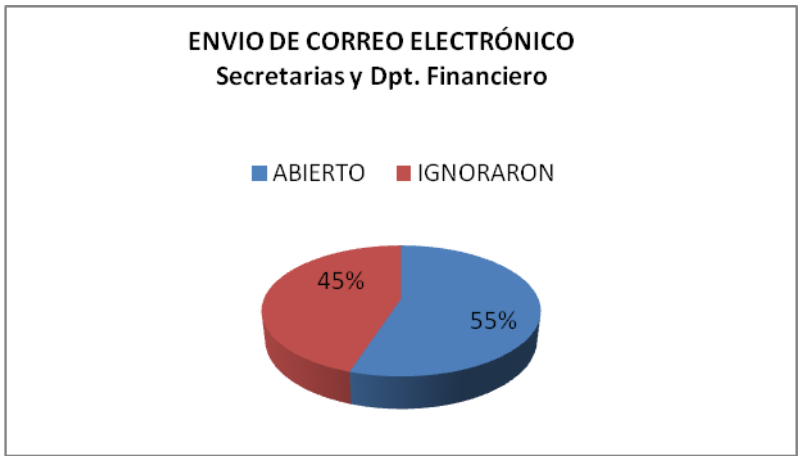


Figura 3. 22. Porcentajes de Técnica de Envío de Correo Electrónico a Secretarias

- Con un total de 20 correos de estudiantes obtenidos, se realizó el envió del correo electrónico con las mismas características que el email enviado a las secretarias. En donde con un 40% abrieron y ejecutaron archivo adjunto, mientras que un 60% ignoraron el email recibido.

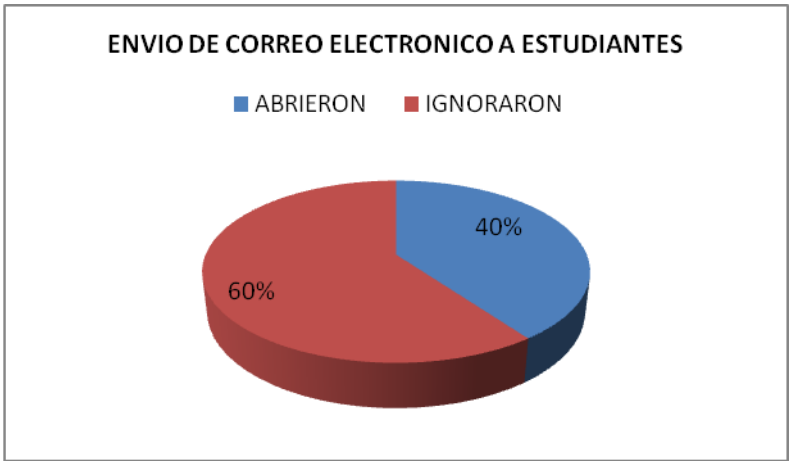


Figura 3. 23. Porcentajes de Técnica de Envío de Correo Electrónico a Estudiantes

Observaciones:

Con el envió de correo electrónico a empleados y estudiantes se pudo observar con un 5% de diferencia quienes abrieron y ejecutaron el correo más fueron los empleados. EL uso de este medio es continuo y por ende se encuentran propenso a recibir cualquier cantidad de correo no deseado, solo por tener un título llamativo.

3.2.3 Técnica De Teléfono

Una de las técnicas más fáciles de usar para los ingenieros sociales es el teléfono, puesto que le permite tener varias ventajas sobre la víctimas, es decir al realizar una llamada se puede ocultar el número y mantener el anonimato, permite actuar a distancia de la victima lo que proporciona hacer difícil su búsqueda y solicitar información suplantando a personas internas de la empresa.

Cuando se realiza la llamada de teléfono es posible que no conteste la persona que estamos buscando o que simplemente no nos brinde información.

OBJETIVO:

- Establecer vínculos de relación con los usuarios mediante la técnica del teléfono, y obtener información confidencial.

VICTIMAS:

- Un total de 20 usuarios, Secretarias y Personal administrativo.

HERRAMIENTA:

- Teléfono.

DESARROLLO DEL ATAQUE:

- Para la realización de este ataque por medio del uso telefónico fue fácil la obtención de los números y extensiones de las Secretarias y personal administrativo, ya que se encuentran subidas en Internet, en la página de la Universidad a disposición de cualquier usuario.
- Una vez obtenido los números telefónicos del personal de la Universidad, se empezó a realizar las distintas llamadas a las Secretarias en horarios en los que me puedan atender, y solicitando de manera cordial, originando conversaciones amenas, en donde la secretaria puedan proporcionar información confidencial de su trabajo.
- Se suplanto a personal de Soporte Técnico, indicando que se necesitaba configurar el antivirus y si la secretaria nos podía ayudar, dándonos algunos datos del equipo como: dirección IP, usuario, clave, nombres y apellidos, área donde trabajan.
- Para ello seguimos un contexto de conversación, estudiando ataques relacionados por medio del teléfono realizado por otras personas y de esta manera poder involucrarnos de mejor manera en la búsqueda de información por este medio. (Ver anexo 7)

RESULTADOS:

- Con la realización de la técnica de teléfono y la obtención de información, se indica que con un 30% SI contestaron y proporcionaron información confidencial sobre su trabajo y divulgación de información de otras personas, mientras que con 40% NO proporcionaron información alguna, y finalmente un 30% no contestaron llamadas.

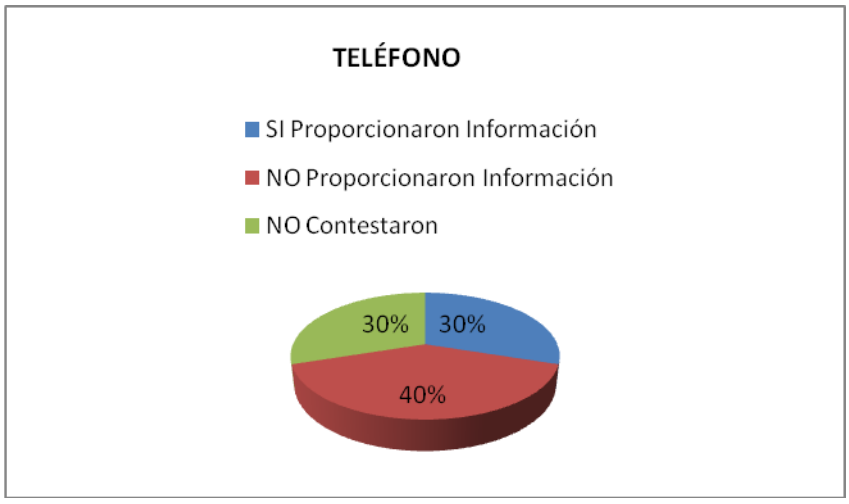


Figura 3. 24. Porcentajes de Técnica Teléfono

Observaciones:

Al realizar este ataque y a pesar de no ser un medio tan explícito se pudo lograr obtener información propia y de uso confidencial de los usuarios, quienes a pesar no ver físicamente a la persona, y no conocerla proporcionan información sin preocuparse de a quien se la entreguen.

3.2.4 Robo de Contraseña

El robo de contraseña es uno de las técnicas que sigue teniendo en auge a los Ingenieros Sociales ya que son los mismos usuarios los que permiten, que se apropien de información sensible. A través del uso de passwords que no mantienen un nivel de seguridad confiable.
Dentro de los correos electrónicos que poseen estudiantes y usuarios de la UTPL, se buscó una herramienta que permita obtener el password o clave de su cuenta de correo.

OBJETIVO:

- Obtener información de la cuentas de correo.

VICTIMAS:

- Estudiantes que no borran sus datos cuando acceden a cuentas en distintas páginas y sitios.

HERRAMIENTA:

- Utilización de servicios botservices[19], para el envió de correos electrónicos.

DESARROLLO DEL ATAQUE:

- Para la obtención de las cuentas de correo de estudiantes, se manejó la técnica de observación en las salas de cómputo de la Universidad, especificando que es allí en donde puede obtener las cuentas de correo electrónico sin ningún tipo de problema.
- Con el servicio de botservices se envía el correo electrónico a los usuario, este email una vez abierto pide ingresar sus datos a una página falsa en este caso de Hotmail (observar Figura 27), que suplanta la verdadera, en donde luego de un corto tiempo le llega al correo del atacante los datos del usuario que ha cometido el error de ingresar sus datos. (Ver anexo 8)

[19] *Blue Ocean Trading Services : proporciona un conjunto de servicios tecnológicos para envió de correos..*

Figura 3. 25. Suplantación de página Hotmail

RESULTADOS:

- De un total de 30 direcciones de correo a las que fueron enviadas las solicitudes y que fueron abiertas e ingresaron sus datos en la página falsa se pudo obtener las claves, en un 67% de éxito y con un 33% no registraron información alguna.

Figura 3. 26. Porcentajes de Robo de contraseñas

Con la realización de esta técnica se lograron obtener varias contraseñas las mismas que se borraron al finalizar la investigación.

Finalmente existen muchos mecanismos para la obtención de información sensible, pero sin duda el usuario es el eslabón más débil en cuanto a seguridad y confidencialidad de la información, ya que en el desarrollo de cada una de las técnicas de Ingeniería Social no existió una preocupación en un alto porcentaje de usuarios en otorgar y facilitar los datos que manejan en la Universidad.

Mediante el uso de encuestas que permitieron conocer el grado de conocimiento y realidad sobre el tema de Ingeniería Social en los usuarios de la Universidad, y por otra parte la aplicación de las

técnicas de Ingeniería Social a las distintas vulnerabilidades que encontramos en las encuesta, obteniendo resultados y realizando un análisis de cada uno de los ataques y de esta manera concluir cada una de ellas.

Cuando se realizo la encuesta el primer paso fue que los usuarios de la Universidad nos proporcionen ciertamente la información auténtica de lo que conocían o desconocían, esto permitiría saber que vulnerabilidades debíamos explotar, al momento de obtener los datos se observaron mas vulnerabilidades de las que habían indicado o señalado en las encuesta.

Por ello se puede decir que no existió un grado de sinceridad en las encuestas por parte de los usuarios de la Universidad, esto debido a la realización y aplicación de determinadas técnicas de Ingeniería Social antes mencionadas.

.

CAPITULO IV

4. LEYES CONTRA DELITOS INFORMATICOS

INTRODUCCIÓN

El presente capítulo pretende conocer de forma general la conceptualización respecto a delitos informáticos, tipos de delitos, código de procedimiento legal en el Ecuador y los lineamientos establecidos sobre estatutos de delitos informáticos dentro de la UTPL, con lo cual se busca tener un claro entendimiento de los criterios y medidas contempladas en la Universidad en caso que exista algún incidente de seguridad en donde se utilice técnicas de Ingeniera Social.

4.1 LEGISLACIÓN EN EL ECUADOR SOBRE TIPOS DE ATAQUES

4.1.1 Delitos Informáticos

Con el desarrollo de tecnologías informáticas se han abierto las puertas a nuevas posibilidades de delincuencia. La gran cantidad de perjuicios ocasionados es a menudo muy superior a la delincuencia tradicional y también son mucho más elevadas las posibilidades de que no llegue a descubrirse o castigarse. Además la necesidad de diferenciar los delitos informáticos del resto y conocer cómo se maneja dentro del marco legal.

Se entiende Delito como: “acción penada por las leyes por realizarse en perjuicio de algo o alguien, o por ser contraria establecida por aquellas”. [40]

Las conductas ilícitas en las que se utiliza la computadora, se denomina “delitos informáticos”, “delitos electrónicos”, “delitos relacionados con la computadora”, “crímenes por computadora”, “delincuencia relacionada con el computador” [41]. No existe una definición universal propia de delito informático sin embargo nos podemos basar en opiniones de varios especialistas para definir.

El delito informático involucra acciones criminales que en primera instancia los países han tratado de poner en figuras típicas, tales como: robo, fraudes, falsificaciones, estafa, sabotaje, entre otros, por ello, es primordial mencionar que el uso indebido de las computadoras es lo que ha creado la necesidad imperante de establecer regulaciones por parte de la legislación.

4.1.2 Delincuencia Informática

Durante el 2011, los incidentes que por su envergadura son dignos de reseña, son:

- Contenido abusivo. Fundamentalmente SPAM y Phishing. El incidente tipo ha sido aquel en el que los usuarios de las instituciones daban sus credenciales en páginas engañosas de Phishing, utilizándose dichas credenciales para el envío masivo de correo basura.
- Contenido malicioso. Alertas de inyección de código, ya sea por vulnerabilidad de aplicación o robo de credenciales. En las últimas semanas de 2011 y principios de 2012 se ha notado una disminución en el número de servidores comprometidos. También se incluyen en esta categoría los informes relativos a troyanos bancarios que han aumentado durante este año.
- Robo de credenciales. Considerable aumento de robo de contraseñas (correo electrónico, banca on-line, ...) mediante técnicas de phishing o usuarios afectados por troyano bancario.[42]

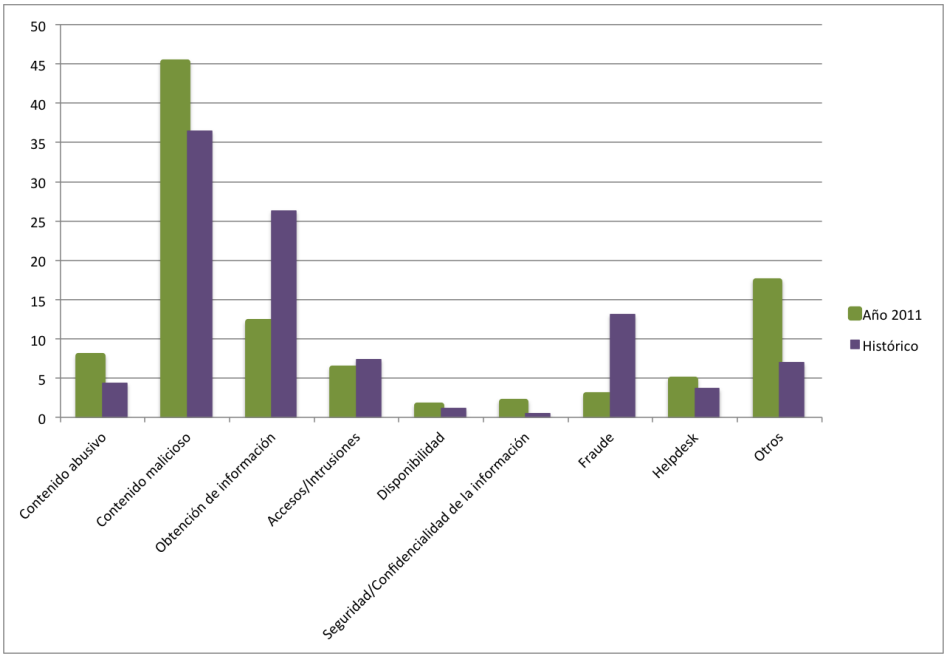


Figura 4. 1. Evolución de Incidentes de Seguridad [42]

DETALLE INCIDENTES:

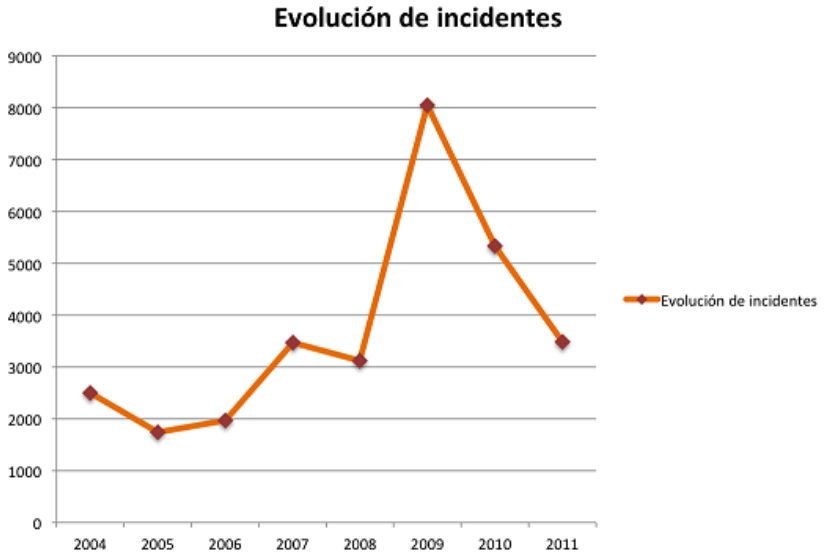


Figura 4. 2. Cifras de evolución de incidentes de seguridad [42]

La tendencia durante el 2011 se ha enmarcado en ataques de infraestructuras criticas, el fraude en todas sus vertientes (phishing, scams, código malicioso, redirecciones etc...) El hacktivismo[20] y el cibercrimen serán términos cada vez más comunes, los ataques dirigidos y especializados, los troyanos que se distribuyen utilizando dispositivos y casos de filtración de información, no sólo como el famoso WikiLeaks sino la distribución de datos confidenciales de usuarios, se repetirán como se han repetido a lo largo del 2011, dándosele cada vez más importancia a la privacidad de los usuarios en el uso de los servicios de Internet. [42]

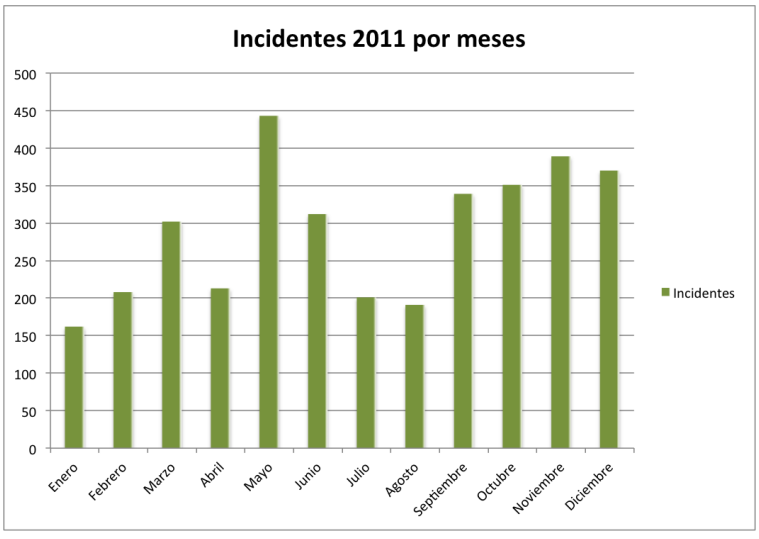


Figura 4. 3. Estadísticas de Vulnerabilidades 2011 [42]

[20] *Hacktivismo: un acrónimo de hacker y activismo.*

4.2 CONDICIONES LEGALES ESTABLECIDAS EN LA LEGISLACION ECUATORIANA

En la legislación del Ecuador se mantienen leyes y decretos que establecen apartados y especificaciones acorde con la importancia de la información y de las tecnologías, ellas son:

4.2.1 Ley Orgánica de Transparencia y Acceso a la Información Pública. [46]

- El principio general de la Ley Orgánica de Transparencia y Acceso a la Información Pública es la publicidad de información. Es decir, que toda aquella información que poseen las entidades públicas personas jurídicas de derecho privado en directa relación con el Estado, las organizaciones de trabajadores y entidades del Estado e Instituciones de Educación Media y Superior que reciban fondos estatales, es pública.

- Aquellas personas que incumplan con la ley serán sancionados con multa equivalente a la remuneración de un mes de sueldo o salario, suspensión de sus funciones por treinta días y destitución del cargo si se persiste en negar la entrega de información. La sanción para las entidades privadas es una multa de cien a quinientos dólares por cada día de incumplimiento.

4.2.2 Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos [46]

- Los contratos que se generen y perfeccionen en Ecuador por medios electrónicos a través del intercambio de mensajes de datos o comprando en sitios web en Internet sean válidos y de efectos civiles, comerciales y jurídicos en general, idénticos a los actuales contratos por escrito.

- Que las firmas electrónicas no son un escaneo de una firma o una foto digital de una firma sino un conjunto de algoritmos que cumplen con ciertos requisitos legales establecidos en la Ley se consideren con igual validez jurídica que las firmas manuscritas.

- Precautelar los derechos de los usuarios que hacen negocios en Internet normando la publicidad en línea, fortaleciendo el derecho a la privacidad de los usuarios y otros temas de protección al consumidor en un medio completamente nuevo en el cual es necesario innovar para estar acordes a la tecnología y a los nuevos modelos de negocios.

4.2.3 Ley de Propiedad Intelectual [46]

- El objetivo de brindar por parte del Estado una adecuada protección de los derechos intelectuales y asumir la defensa de los mismos, como un elemento imprescindible para el desarrollo tecnológico y económico del país.

- Dentro de la ley de propiedad intelectual uno de los principales problemas que enfrenta esta rama del derecho moderno, es la piratería y falsificación de las obras del intelecto humano, las cuales traen graves consecuencias económicas y sociales; a más de los perjuicios de los titulares de derechos de propiedad intelectual, pues esta pérdida no solo afecta a los fabricantes de los productos falsificados, sino a la reducción de ingresos tributarios e inclusive la pérdida de empleos, debido a los efectos negativos resultantes de la mano de obra clandestina, de las labores creativas y de investigación, perjudicando la vitalidad cultural y económica de un país. [45]

- La ley incluye en su codificación la protección de bases de datos que se encuentren en forma impresa u otra forma, así como también los programas de ordenador (software) los cuales hoy son considerados como obras literarias.

4.2.4 Ley Especial de Telecomunicaciones [46]

- La Ley Especial de Telecomunicaciones tiene por objeto normar en el territorio nacional la instalación, operación, utilización y desarrollo de toda transmisión, emisión o recepción de signos, señales, imágenes, sonidos e información de cualquier naturaleza por hilo radioelectricidad, medios ópticos y otros sistemas electromagnéticos.

- Declara que es indispensable proveer a los servicios de telecomunicaciones de un marco legal acorde con la importancia, complejidad, magnitud tecnología y especialidad de servicios, así como también asegurar una adecuada regulación y expansión de los sistemas radioeléctricos, y servicios de telecomunicaciones a la comunidad que mejore de forma permanente la prestación de los servicios existentes.

4.2.5 Ley de Control Constitucional (Reglamento Habeas Data) [46]

- La ley de Control Constitucional establece que las personas naturales o jurídicas, nacionales o extranjeras, que desean tener acceso a documentos, bancos de datos e informes que sobre si misma o sus bienes están en poder de entidades públicas, de personas naturales o

jurídicas privadas, así como conocer el uso y finalidad que se les haya dado o se les este por dar, podrán imponer el recurso de Habeas Data para requerir las respuestas y exigir el cumplimiento de las medidas tutelares prescritas en esta ley, por parte de las personas que posean tales datos o informaciones.

4.3 CÓDIGO DE PROCEDIMIENTO PENAL Y CÓDIGO DE PROCEDIMIENTO CIVIL DE ECUADOR

Los delitos informáticos que se tipifican, mediante reformas al Código de Procedimiento Penal, se muestran a continuación en la siguiente tabla:

Tabla 4. 1. Infracciones informáticas [45]

INFRACCIONES INFORMÁTICAS	REPRESIÓN	MULTAS
Delitos contra la información protegida (CPP Art. 202)		
1. Violentando claves o sistemas	6 meses a 1 año	$ 500 a $1.000
2. Seguridad nacional o secretos comerciales e industriales	1 año a 3 años	$1.000 - $1.500
3. Divulgación o utilización fraudulenta	3 a 6 años	$2.000 – $10.000
4. Divulgación o utilización fraudulenta por custodios	6 a 9 años	$2.000 – $10.000
5. Obtención y uso no autorizados	2 meses a 2 años	$1.000 - $2.000
Destrucción maliciosa de documentos (CPP Art. 262)	3 a 6 años	---
Falsificación electrónica (CPP Art. 353)	3 a 6 años	---
Daños informáticos (CPP Art. 415)		
1. Daño dolosante	6 meses a 3 años	$60 - $150
2. Servicio al público o vinculado con la defensa nacional	3 a 5 años	$200 - $600

3. No delito mayor	8 meses a 4 años	$200 - $600
Apropiación ilícita (CPP Art. 553) **1. Uso fraudulento** **2. Uso de medios (claves, tarjetas magnéticas, otros instrumentos)**	6 meses a 5 años 1 a 5 años	$500 - $1.000 $1.000 - $2.000
Estafa (CPP Art. 563)	5 años	$500 - $1.000
Contravenciones de tercera clase (CPP Art. 606)	2 a 4 días	$7 - $14

La persona que violenta claves, sistemas de seguridad para obtener información, lesiona la intimidad y por consiguiente la confidencialidad de la persona jurídica en muchos casos. Es por esta razón, que los Legisladores, deben estar conscientes que la delincuencia informática avanza con pasos agigantados y que las leyes ecuatorianas deben estar acorde con los avances tecnológicos.

Ecuador ha dado considerablemente sus primero pasos en las leyes existentes, donde se contemplan especificaciones de la información y la informática, lo cual significa un avance muy importante ante el desarrollo tecnológico que se ha tenido en los últimos años en el país, pero es evidente que aún falta mucho por legislar, para asegurar que no queden en la impunidad los actos que se comentan relacionados con las tecnologías.

4.4 MANEJO DE POLITICAS SOBRE DELITOS INFORMATICOS EN LA UTPL

En la actualidad la Universidad Técnica Particular de Loja, no cuenta con políticas para delitos informáticos, es decir la Universidad maneja Status propios para la organización de la misma.

Dentro de los Status de la Universidad que se encuentran subidos en la página de la UTPL http://www.utpl.edu.ec/utpl/informaciongeneralleyesyreglamentosvinculadosconlautpl, está la sección de Sanciones la cuales indican que dentro del Titulo VII, se expone:

Art. 66.- El Consejo Superior, de conformidad a lo dispuesto en la Ley de Educación Superior, establecerá las sanciones y los organismos competentes para ejecutarlas, según el grado de la falta, para el personal docente, los estudiantes, y administrativos que, culposa o deliberadamente, atentaren al ejercicio de los deberes y derechos de los miembros de los diversos estamentos de la Universidad,

o impidieren de cualquier modo el desarrollo normal de la educación de los alumnos o la culminación de sus estudios, o actuaren en contra de la visión y misión de la Universidad.
Los procesos se ajustarán a las garantías del debido proceso y derecho a la defensa establecidas en la Constitución Política de la República del Ecuador.

Indicando que esta es la única en donde se expone sobre algún tipo de sanción para los miembros de la UTPL en el caso que cometieran alguna falta, pero no existe una política propiamente que especifique algún delito informático que se acometiera.

En el caso que hubiese algún delito informático por parte de algún miembro de la Universidad existirá una Resolución y se establecería como norma interna de acuerdo al caso presentado.

Existen Políticas de Uso, para Recursos Abiertos OERS y Políticas de uso Blog, además de documentos de Instructivos y Procesos para la transferencia general de proyectos, en donde están presente lineamiento sobre distintas políticas en el manejo y uso de documentos de la Universidad.

Otras políticas que se están desarrollando para los gestores de la Universidad, en donde se expone sobre la responsabilidad, confiabilidad, disponibilidad de la Información que ellos manejan cuando realizan sus servicios dentro de la Universidad.

En otro tema dentro de políticas de la UTPL, están establecidos lineamientos para los contratos del personal en donde se establece la confidencialidad relacionada con la propiedad intelectual e industrial en general, secretos industriales, software de computación, “know how”, recetas formulas, patentes, signos distintivos, planes de mercado, publicidad o producción, relación de vendedores, estudiantes, clientes, finanzas, operaciones, o asuntos de negocios, programas de estudios, campañas publicitarias, lanzamiento de productos, estrategias, presupuestos, salarios del personal de la Universidad, fusiones, adquisiciones y/o cualquier operación o asunto de negocios; motivo por el cual, el Profesional se halla prohibido de hacer uso de dicha información en asuntos que no estén relacionados con el contrato o divulgación a terceras personas, sino cuenta con autorización escrita de la Universidad, así como tampoco revelar el contenido de documentos que llegara a elaborar o los tramites que llegara a realizar en el trabajo aun después de haber concluido el servicio.

En el caso de que cometiera alguna infracción o falta se regirían las leyes establecidas a Nivel de las Leyes del Estado Ecuatoriano.

Finalmente se puede observar que no existe una política específica que proteja a los miembros de la Universidad y la información de la UTPL contra los delitos informáticos.

4.5 INICIATIVA PARA EL MANEJO DE DELITOS INFORMÁTICOS EN ECUADOR

4.5.1 Propuestas De Reforma de Leyes Contra Delitos Informáticos

Un análisis de las leyes del código penal ecuatoriano que se han promulgado están dirigidas a proteger la utilización de la información y procesada mediante el uso de computadoras, la protección de los derechos de los ciudadanos y de los equipos.

Las nuevas generaciones de delincuente que exponen los gobiernos, las empresas y los ciudadanos a ese tipo de peligros, existen nuevos delitos informáticos que presentan una realidad difícil de controlar, y que traspasa las fronteras de los países, por ello mediante la cooperación entre organismos estatales es primordial estudiar los casos que se han incrementado frente a los nuevos delitos informáticos.

Existen leyes en otros países que han abordado nuevos tipos de delitos informáticos que no se especifican dentro del Código Penal Ecuatoriano, en donde se especifica el tipo de delito y las sanciones que se están aplicando.

4.5.2 Propuestas Internas

4.5.2.1 Departamento de Criminalística de la Policía Judicial

En el Reglamento para el Departamento de Criminalística, constituye que: “Bajo la dirección de los fiscales, corresponde a los departamentos de criminalística, acudir al lugar de los hechos para proteger la escena del delito; buscar, fijar, levantar, etiquetas las muestras dando inicio a la cadena de custodia, y analizar todos los indicios, señales o evidencias sobre un presunto hecho delictivo, de conformidad con lo establecido en Código de Procedimiento Penal”.[46]

La Policía Judicial, mantiene Departamentos de Criminalística en las provincias de: Pichincha, Guayas, Manabí, Chimborazo, Azuay, Tungurahua e Imbabura Loja, Cotopaxi y Los Ríos. Los departamentos de criminalística cuentan con las siguientes secciones:

Tabla 4. 2 Secciones del Departamento de Criminalística

Secciones del Departamento de Criminalística			
Inspección ocular técnica	Audio, video y afines	Fotografía pericial	Dibujo y planimetría
Identidad física humana	Registro de Detenidos	Balística	Biología
Identificación de grabados y marcas seriales	Incendios y explosivos	Análisis Informático y Telecomunicaciones	Centro de Acopio y conservación de evidencias
Química analítica	Toxicología Analítica	Física	Documentología

El Departamento de Criminalística, de la Policía Judicial, cuenta con una sección especializada en Análisis Informático y Telecomunicaciones.

Según el Reglamento de la Policía Judicial en el Art. 81, se especifica que, a la Sección de Análisis Informático y Telecomunicaciones le corresponde: [45]

1. Identificar los procesos y autores de fraude, falsificación, invasión y atentado de los sistemas informáticos y de telecomunicaciones.

2. Recopilar y mantener actualizada la información referente a medidas de seguridad informática y en Telecomunicaciones.

3. Mantener la cadena de custodia.

4. Demás funciones que se le asignen, creen y/o dispusiere la autoridad legal tendiente al esclarecimiento de un hecho punible.

4.5.2.1.1 Proyectos Propuestos en Ecuador

1. El Gobierno Nacional del Ecuador, de acuerdo con el proyecto del Plan de Seguridad Ciudadana y Modernización de la Policía (2008-2009) (28), ha presupuestado invertir progresivamente 320 millones de dólares en equipamiento, capacitación, servicios, y remodelación de la Policía.[45]

   Esto se pondrá en marcha, en las ciudades de Quito y Guayaquil se prevé implementar los Centros de Ciencias Forenses, estos estarán equipados con infraestructura y tecnología moderna, permitiendo, una mejora de la investigación del delito.

Conjuntamente se maneja la posibilidad de habilitar en cada provincia del país 15 Unidades de Apoyo Criminalístico, los mismos que contarán con herramientas básicas de investigación, así como también unidades de criminalística móviles que operarían a nivel nacional.

El proyecto también contempla la adquisición de herramientas como ADN Forense, microscopio electrónico que permite confirmar residuos de pólvora, elementos que actualmente no existen en el país, así como también dotar de nuevos terminales y servidores para el Sistema IBIS (Sistema Integrado de Identificación Balística), IAFIS (Sistema Integrado Automático de Identificación de Huellas Dactilares) que se conservan en el Departamento de Criminalística.

2. PROYECTO CERT ECUADOR/CC. Desarrollo del proyecto implementación del CERT Ecuador .- Centro de Respuesta a Incidentes Informáticos debe ser: detectar e identificar la amenaza, bloquearla, monitorizarla, reportar, guardar registros y evidencias de la amenaza responderla, pedir información a los organismos o actores involucrados dentro de la respuesta a la amenaza de ser necesario, hacer uso de la infraestructura disponible y necesaria y comunicar a los demás equipos de apoyo o CSIRT's conectados, para así mitigar las posibles consecuencias que produce un incidente de seguridad informática y promover la recuperación eficaz y efectiva de la información que fue sujeto del incidente, para luego crear un registro almacenado y generar la información respectiva y generar experiencia para compartirla con otros miembros integrados en las redes de confianza. El Centro de Respuesta a Incidentes Informáticos brindará asesoramiento a las entidades públicas para implantar medidas tecnológicas que mitiguen el riesgo de sufrir ataques informáticos mediante el estudio de los aspectos técnicos de ciberdelitos, colaborará también en la resolución de cualquier incidente en coordinación con la Fiscalía General del Estado y proporcionará información sobre vulnerabilidades, alertas y avisos de amenazas a los sistemas de información. [47]

4.5.2.2 Unidad de Delitos Informáticos en el Ministerio Publico

Con el incremento de delitos informáticos el Director Nacional de Informática del Ministerio Publico del Ecuador propone, un Plan Operativo de creación de la Unidad de Delitos Informáticos del Ministerio Público (UDIMP). [45]

La Unidad de Delitos Informáticos del Ministerio Público, tendrá la misión de:

- Investigar, perseguir y prevenir todo lo relacionado con la criminalidad informática en todos sus aspectos y ámbitos tales como: amenazas, injurias, pornografía infantil, fraudes, terrorismo informático y hacking.

Entre los objetivos establecidos para dicha unidad se establecen los siguientes: [46]

1. Investigar y perseguir a nivel pre-procesal y procesal penal toda infracción que utilice a la informática como medio o fin para la comisión de un delito.

2. Capacitar a los miembros de la unidad a nivel técnico para combatir esta clase de infracciones.

3. Contribuir y colaborar con la formación continua de los investigadores.

4. Formar y mantener alianzas con unidades Especiales de investigación a nivel internacional.

5. Desarrollar una política de Seguridad Informática General.

6. Implementar a nivel nacional el Sistema de Información de Delitos Informáticos

7. Promover canales de comunicación y trabajo con las distintas estructuras y organizaciones gubernamentales implicadas con la lucha contra el fenómeno de la delincuencia informática.

La coordinación nacional la estructura estaría compuesta de la siguiente manera:

- ✓ **Coordinación Nacional**: Establecerá las políticas y directrices generales de la investigación de los Delitos Informáticos.

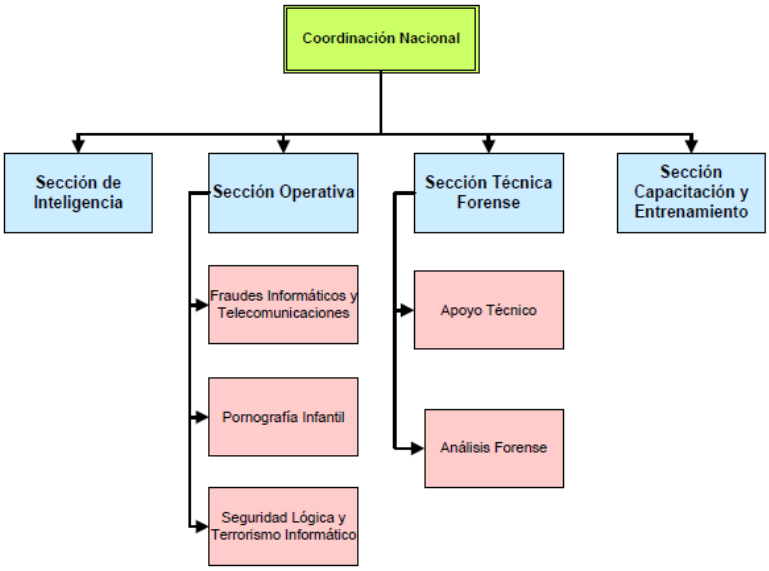
- ✓ **Sección de Inteligencia:** Se encargará de la recolección de las evidencias e indicios relacionados con el cometimiento de los delitos informáticos.

- ✓ **Sección Operativa:** Realizará las investigaciones de lo relacionado con la criminalidad informática.

- ✓ **Sección Técnica y Forense:** Brindará apoyo técnico y realizara el análisis forense de las evidencias.

- ✓ **Sección de Capacitación y Entrenamiento:** Formación del personal de la Unidad, de la acreditación de los Peritos Informáticos a nivel nacional.

Tabla 4. 3 Estructura de Unidad de Delitos Informáticos del Ministerio Público [45]



4.5.2.3 Peritos Profesionales del Ecuador

El colegio de Peritos Profesionales en Ecuador como son: Pichincha, Guayas, Tungurahua, Los Ríos, El Oro, Manabí, mantienen una estructura a nivel de ellos para el manejo de los distintos incidentes ocasionados por la delincuencia informática. [45]

Permitir la creación de un Ley de Defensa del Perito Ecuatoriano, debido a que en Ecuador y provincias mencionadas anteriormente no mantienen una política que establezca lineamientos que permita establecer condiciones para el ejercicio profesional de este nivel.

4.5.3 Medidas Existentes en Otro Países

Los países de Latinoamérica como Chile, Argentina, Colombia, Perú, cuentan con regulación, a nivel legislativo que tipifican los delitos informáticos, mientras que en otros países se ha procedido a la reforma de los Códigos de Procedimiento Penal para la aplicación de las sanciones, ante las infracciones informáticas cometidas.

Otros países Alemania, Austria, Francia, Estados Unidos y España son países que cuentan con un sistema de leyes que abarcan otro tipo de delitos que en las Leyes del Ecuador aun no son considerados.

4.5.3.1 Delitos Informáticos: Aplicación Chile [45]

Chile el primer país sudamericano en sancionar la ley contra delitos informáticos, a continuación la siguiente tabla lista las leyes, decretos y normas que han incorporado:

Tabla 4. 4. Legislación en Chile [45]

AÑO	LEY / DECRETO/ACUERDO	ORDENANZA
1970	Ley 17336 (Inicial)	Ley de Propiedad Intelectual (incluye programas de computadora, a través de la Ley 18957 - 1990)
1993	Ley 19223	Ley de Delitos Informáticos. Figuras penales relativas a la informática
1999	Decreto 81/99	Uso de la Firma Digital y Documentos Electrónicos en la Administración del Estado
1999 2002	Ley 19628 Ley 19812	Protección de la vida privada. Protección de datos de carácter personal.
2002	Ley 19799	Ley de Firma Electrónica. Documentos Electrónicos, Firma Electrónica y Servicios de Certificación de Firma Digital
2003	NCH 2777	Código de práctica para la Gestión de la Seguridad de la Información
2004	Ley 19927	Pornografía Infantil

Se establece delitos informáticos en los que se incluyen los siguientes tipos de actos ilícitos de acuerdo a lo que establecen sus articulados:

- ✓ Sabotaje.
- ✓ Espionaje informático.
- ✓ Destrucción maliciosa de la información.
- ✓ Divulgación de información no autorizada.

Detalle de Artículos de Ley nº 19.223: [46]

Articulo 1. “El maliciosamente destruya o inutilice un sistema de tratamiento de información o sus partes o componentes, o impida o obstaculice o modifique su funcionamiento, sufrirá la pena de presidio menor e su grado medió a máximo.

Si como consecuencia de estas conductas se afectaren los datos contenidos en el sistema, se aplicarán la pena señalada en el inciso anterior, en su gado máximo.”

Articulo 2. “El que con ánimo de apoderarse, usar o conocer indebidamente la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo a medio.”

Articulo 3. “El que maliciosamente altere, dañe, los contenidos y datos contenido en un sistema de tratamiento de información, será castigado con presidio menor en su grado medio.”

Articulo 4. “El que maliciosamente revele o difunda los datos contenidos en un sistema de información sufrirá la pena de presidio menor en su grado medio. Si quien incurriere en estas conductas es el responsable del sistema de información, la pena se aumentará en un grado.”

Esta ley es la pionera en abordar expresamente el tema de los delitos informáticos.

4.5.3.2 Delitos Informáticos: Aplicación Argentina[45]

Argentina es uno de los países que a nivel de legislación ha desarrollado el tema sobre los delitos informáticos. Contempla la Ley 26388 en la que se penalizan los delitos electrónicos y tecnológicos.
La siguiente tabla muestra las leyes y decretos que mantiene Argentina y que contemplan especificaciones de informática e información:

Tabla 4. 5. Legislación en Argentina [45]

AÑO	LEY / DECRETO/ ACUERDO	ORDENANZA
1933	Ley 11723	Régimen Legal de Propiedad Intelectual.
1996	Ley 24766	Ley de Confidencialidad.
1998	Ley 25036	Ley de Propiedad Intelectual (Modificación de la Ley 11723)
2000	Ley 25326	Habeas Data (Modificada en el 2008)
2001	Ley 25506	Firma Digital
2002	Decreto 2628/	Reglamentación de Firma Digital
2004	Ley 25891	Servicio y Comunicaciones Móviles
2005	Ley 26032	Difusión de Información
2008	Ley 26388	Delitos Informáticos.

En el Código Penal Argentino sobre el uso de las tecnologías de la información, en la cual se sanciona:

- ✓ Pornografía infantil.
- ✓ Destrucción maliciosa y accesos no autorizados a la información y sistemas de información.
- ✓ Intercepción e interrupción de las comunicaciones electrónicas y de telecomunicaciones.
- ✓ Divulgación de información no autorizada.

4.5.3.3 Delitos Informáticos: Aplicación Colombia [45]

Colombia establece mecanismos que permitan mantener las siguientes leyes decretos y acuerdos, relacionados con la informática y la información:

Tabla 4. 6. Legislación en Colombia [46]

AÑO	LEY / DECRETO/ ACUERDO	ORDENANZA
1985	Ley 57	Transparencia y Acceso a la Información Gubernamental
1999	Ley 527	Información en forma de mensaje de datos
2000	Decreto 1747	Entidades de Certificación, los Certificados y las Firmas Digitales
2000	Resolución 26930	Estándares para la autorización y funcionamiento de las entidades de certificación y sus auditores.
2001	Ley 679	Explotación, la Pornografía y el Turismo Sexual con Menores de Edad
2003	Decreto 2170	Certificación y Firmas Digitales
2004	Proyecto de Ley 154	Reglamento del Derecho a la Información
2006	Acuerdo PSAA06-3334	Reglamentación de medios electrónicos e informáticos en la justicia.
2009	Ley 1273	Ley de la protección de la información y de los datos

Colombia ha tenido un desarrollo particular con respecto a la investigación de:

- ✓ Delitos de índole informático, factores como el narcotráfico, lavado de dinero, falsificación y terrorismo, ha incentivado que este país implemente unidades de investigación que les colabore en los procesos de indagación de actos ilícitos en los que se utilizan medios tecnológicos o que afectan sistemas de tecnología o de información.[46]

Colombia ha recibido la ayuda de EE.UU para la persecución de criminales informáticos con la utilización de laboratorios del FBI.

4.5.4 Propuestas Generales para la Ley de Delitos Informáticos del Ecuador

Durante del desarrollo y estudio hemos conocido las herramientas y organismos con los que cuenta el Ecuador para la investigación de los delitos de índole tecnológicos, así como las propuestas ofrecidas por otros organismos que permitirían el desarrollo de unidades de investigación de los delitos informáticos, además se han identificado iniciativas que permiten la adecuación y mejora del Departamento de Criminalística de la Policía Judicial del Ecuador.

Luego de analizar la realidad de los delitos informáticos en el Ecuador y exponer mecanismos y herramientas existentes para su análisis, se recomienda considerar por sectores: los siguientes aspectos:

A nivel Gubernamental:

1. Construir y alinear las políticas de lucha en contra de la delincuencia informática, en donde se encuentren enfocadas a la minimización de delitos informáticos.
2. Estudiar los nuevos delitos informáticos y tratar de establecer leyes que permitan controlar el uso de la tecnología a través del manejo de Internet.
3. Impulsar mecanismos de cooperación con otros países con el objetivo de prevenir y sancionar el delito informático.

A nivel Marco Legal:

1. Reformas al Código de Procedimiento Penal del Ecuador sobre penalizaciones a las infracciones informáticas o delitos informáticos.
2. Creación de nuevas normas legales y sanciones para las distintas conductas ilícitas producidas mediante el Internet.
3. Establecer mecanismos de protección penal respecto de la delincuencia informática.
4. Implementación de mecanismos de mayor rigurosidad en los procedimientos de acreditación de peritos informáticos, en la que los profesionales acrediten además de sus conocimientos técnicos, procedimientos de manejo de evidencias, criminalística, e incluso respaldar sus conocimientos con certificaciones.
5. Se debería sancionar con penas mayores a quienes utilicen sus conocimientos para traspasar mecanismos de seguridad de servidores, bases de datos etc.

A nivel de Formación:

1. Desarrollo de programas de capacitación al órgano legal (Fiscales, Jueces, Abogados) sobre los delitos informáticos y la informática legal.
2. Capacitación a los profesionales de tecnología en aspectos básicos de informática legal, forense, criminalística, manejo de evidencias digitales, etc.
3. Desarrollo de programas de especialización que contemplen profesionales en informática forense y/o legal que pueden darse en cooperación con organismos especializados o entre convenios universitarios.
4. Mantener un sistema de información sobre los últimos delitos informáticos descubiertos a las distintas entidades.

A nivel Tecnología:

1. Participación y transferencia de conocimiento con países, con quienes se hayan establecido convenios internacionales, para el manejo de los delitos informáticos.

2. Implementación de laboratorios especializados forenses informáticos para garantizar los resultados de investigaciones.

A nivel Sociedad:

1. Señalar a los usuarios sobre las posibilidades u probabilidad de ocurrencia de delitos informáticos.
2. Concientización del efecto e impacto de los delitos informáticos sobre la sociedad.
3. Difusión por distintos medios de comunicación las medidas de salvaguarda tal su información privada y confidencial de las entidades en donde se trabaja.
4. Concientización en las organizaciones de que las medidas de seguridad más que un gasto son una inversión que proveen mecanismo para evitar este tipo de delitos.
5. Mantener un uso adecuado del Internet y los distintos sitios que nos presentan para garantizar nuestra información.

CAPITULO V

5. MECANISMO DE PROTECCION DE SEGURIDAD PARA EVITAR LA INGENIERIA SOCIAL

En el presente capítulo se describen mecanismos de protección de seguridad para evitar Ingeniería social en la UTPL basándose en medios necesarios e incorporando propuestas de capacitaciones, boletines de seguridad y propuesta de políticas de buen uso, destinadas a formalizar la privacidad de la información de la Universidad y personal, ante posibles acometidas de Ingeniería Social, con la finalidad de brindar un uso seguro a la información que manejan.

De esta manera establecer comportamientos seguros y responsables de los usuarios, además de la información que manejan dentro y fuera de la Universidad, así como información personal del usuario, y finalmente procedimientos para salvaguardar nuestros datos.

5.1 CONCIENTIZACIÓN DE USUARIOS DE LA UTPL

5.1.1 Capacitación

La capacitación es una herramienta fundamental para ofrecer la posibilidad de mejorar la eficiencia del trabajo en cuanto a seguridad, permitiendo a su vez que la misma se adapte a las nuevas circunstancias que se presentan tanto dentro como fuera de la Universidad. Proporciona a los empleados la oportunidad de adquirir mayores aptitudes, conocimientos y habilidades para desempeñarse con éxito.

5.1.2 Boletines

Asegurarse de concientizar y capacitar también a los empleados nuevos y antiguos sobre las nuevas amenazas, los métodos de acceso inseguros a sus equipos y el cumplimiento de políticas y procedimientos de seguridad. Esto se lo puede realizar con la incorporación de Boletines de seguridad, por ello se ha dejado una propuesta de ello. (Ver anexo 9)

5.1.3 Reuniones

Establecer reuniones y lograr que los usuarios asimilen de que manera son susceptibles ante los métodos de engaño de los Ingenieros Sociales y mostrarles con ejemplos reales (cuya repercusión

haya sido muy grande) de manera que logren medir el peligro de brindar cualquier información a un extraño. De esta manera estarán mucho más preparados ante cualquier intento de manipulación.

5.1.4 Participación de Seminarios

Hacer participes a todos los usuarios de la Universidad los seminarios que se dictan en la Universidad sobre temas de seguridad de la información y combinarla con el establecimiento de políticas bien definidas sobre pautas de comportamiento de los usuarios cuando enfrentan cualquier tipo de ataque.

5.1.5 Acuerdos de confidencialidad

5.2 POLÍTICAS DE SEGURIDAD

5.2.1 Política General

OBJETIVO

- Minimizar los riesgos de ataques de Ingeniería Social a usuarios finales de la Universidad.

ALCANCE

Aplicación de política de seguridad de información, dirigida a todos los usuarios que estén vinculados con la Universidad.

RESPONSABLES

Usuarios de la Universidad y terceros, que interactúan de manera usual u ocasional con los servicios que facilita, como acceder a información sensible, son responsables de informarse y mitigar los ataques de Ingeniería Social.

DEFINICIONES

La utilización de recursos de información de la UTPL, dispone de datos importantes, relevantes y que, tiene un valor importante para la institución y por consecuente esta debe ser protegida, debido a las incidencias que se presentan a diario por medio la Ingeniería Social.

Mediante el uso de recursos y formas de protección, se pretende garantizar, minimizar irregularidades en el ámbito de ataques u desinformación que se presenten y de esta manera proporcionar que los usuarios desarrollen sus labores.

A continuación se establece un conjunto de controles para evitar los ataques de Ingeniería Social a través de:

- **Normas:** Definiciones concretas de cada tema de seguridad, basada en aspectos específicos destinados al usuario, que luego se adaptaran a asegurar la información y protegerse la Ingeniería Social.
- **Procedimientos:** Detalle de actividades y tareas que debe realizar los usuarios para cumplir las definiciones de las políticas. .
- **Estándares:**

Conjunto de parámetros específicos de seguridad para la Ingeniería Social.

Por ello es política de la Universidad:

- Asegurar que sea procesada toda la información necesaria y suficiente para la marcha de la Universidad únicamente en los sistemas informáticos y procesos transaccionales. (Integridad)
- En base al acuerdo de confidencialidad para administradores, garantizar que toda la información este protegida del uso no autorizado, revelaciones accidentales, espionaje industrial, violaciones de privacidad y otras similares originadas de terceros no autorizados. (Confidencialidad)
- Garantizar que los sistemas informáticos brinden información segura para ser utilizada en la operatoria de cada uno de los procesos.(Confiabilidad)
- Garantizar que todos los accesos a datos y/o transacciones cumplan con los niveles de autorización correspondientes para su utilización y divulgación (Autorización).
- Garantizar que todos los medios de procesamiento y/o conservación de información cuenten con medidas de protección física que eviten el acceso y/o utilización indebida por personal no autorizado, así como permitan la continuidad de las operaciones. (Protección Física).
- Asegurar el registro e identificación inequívoca de los usuarios en el uso de los sistemas, de tal manera que no puedan negarla en ningún momento. (No repudio)

Estos principios se garantizaran a través del cumplimiento de una o varias de las normas que a continuación se proponen.

5.2.2 Norma 1 | Tratamiento Información Escritorio Limpio

a. Objetivo

Definir y gestionar la manera adecuada el uso de información que se maneja, y la utilización adecuada de documentos confidenciales tomando en cuenta: su forma, medio de comunicación, el riesgo y el tipo, para poderle dar el nivel de seguridad respectivo.

b. Consideraciones Generales

5.2.2.1 Definiciones de Información

- Se deberá considerar como información a todo dato relacionado con los procesos que lleva la Universidad cualquiera sea su forma y medio de comunicación y / o conservación:

    - Información en los sistemas y / o reportes impresos
    - Formularios / comprobantes propios y / o de terceros
    - Cartas / Fax propios y / o terceros
    - Títulos / Certificados de terceros

5.2.2.2 Riesgos de Información

- El usuario que maneja la información deberá identificar los posibles riesgos a los que está expuesta la información que manipula teniendo en cuenta la posibilidad de que personal interno o externo puede:
    - Divulgación no autorizada
    - Modificación de datos
    - Indisponibilidad de información de clave
    - Apropiación de información
    - Proporcionar Información telefónica

5.2.2.3 Clasificación de Información

- El usuario de información deberá analizar su información para proceder a clasificar, basándose principalmente en su valor, uso y los posibles perjuicios que puede ocasionar en caso de pérdida para la Universidad.

5.2.2.3.1 Información Pública

- Debe considerarse de acceso al público, a la información que no presente riesgo significativo a la Universidad.

5.2.2.3.2 Información de Acceso Autorizado

- Toda información tiene un dueño y es la persona quien debe proporcionar permiso para utilización de la misma.
- La información debe conservarse en un lugar que no represente peligro, es decir cualquier tipo de manipulación, y sea un riesgo para la Universidad.
- Para la realización de impresiones de documentos confidenciales se debería utilizar una impresora que proporciones seguridad a la misma.
- Se deberá destruir toda información y sus correspondiente lógicos / físicos cuando se considere en desuso.
- La información no deberá ser enviada a personal extraño ni menos por medio de sistemas externos a la UTPL como mensajería instantánea y canales IRC.

5.2.3 Norma 2 | Seguridad En Telefonía

a. Objetivo

Asegurar la integridad, confidencialidad y disponibilidad de la información en su transmisión y recepción telefónica tanto interna como externa.

b. Consideraciones Generales

- Los usuarios que utilizan el teléfono no deben proporcionar información confidencial por medio de una llamada.
- No se debe detallar actividades que se encuentren desarrollando, por este medio.
- Evitar utilizar el teléfono para proporcionar información personal o privada de la Universidad.

5.2.4 Norma 3 | Seguridad En El Correo Electrónico

a. Objetivo

Definir pautas generales para el manejo del correo electrónico.

b. Consideraciones Generales

- Todos los correos electrónicos disponen de parámetros de seguridad para el envió y recepción de correo electrónico los cuales están presentes mediante alertas para que el usuario este atento.

- El usuario debe verificar si el remitente es confiable cuando recibe un email, puesto que puede ser falsas cadenas, recibir virus, o publicidad no solicitada (spam).
- El usuario deberá eliminar a los usuarios que representen algún tipo de peligro o con quienes no desea tener ningún tipo de contacto (ver procedimiento PRO1NO1 Eliminar Usuarios)
- El usuario no deberá aceptar correos de desconocidos, lo ideal es asegurarse de saber de quién se trata antes de revisar el email o responderle.
- El usuario no deberá enviar cadenas de correo bajo ningún tipo de consideración.
- Verificar con antivirus si los correos no tienen virus.
- No enviar información confidencial por este medio como: Usuario y contraseñas
- Se puede especificar algunas consideraciones para el envió de correos masivos.

5.2.5 Norma 4 | Administración de Contraseñas

a. Objetivo

Gestionar la configuración y el tiempo de duración de contraseñas.

b. Consideraciones Generales

- Los usuarios deberán crear la contraseña tomando en consideraciones las pautas de seguridad (ver estándar técnico ET1NO1: Creación de Contraseñas)
- No usar la misma contraseña en todos los sitios que mantengo una cuenta activa, es factible que no se pueda tener una contraseña para cada cuenta, sin embargo, lo ideal es contar con tres contraseñas: de bajo, medio y alto nivel de seguridad, para ser usada en los diferentes sitios dependiendo de la criticidad de la información y de esta manera no sufrir algún ataque de Ingeniería Social.
- No pegar papeles con la contraseña en la pantalla del computador ni mucho menos documentos visibles con las contraseñas, de modo que cualquier atacante pueda apropiarse.
- Los usuarios deberán cambiar periódicamente la contraseña, existen sitios de banca en línea que mantienen políticas de criticidad de la información, pero también existen sitios que no poseen este tipo de políticas y es posible tener ataques de Ingeniería Social.
- La contraseña es individual por lo cual no debe ser dado a nadie por ningún motivo.
- Tomar a consideración las sesiones como: caducidad de una sección, intentos fallidos y bloqueos de cuentas.

5.2.6 Norma 5 | Respuestas A Incidentes Y Anomalías De Seguridad

a. Objetivo

Establecer las medidas a tomar luego de un incidente de seguridad.

b. Consideraciones Generales

- Los miembros de la Universidad, serán capacitados en cuestiones de seguridad de la información, según sea el área operativa y en función de las actividades que se desarrollan. Este tipo de capacitación está encargado el CSIRT-UTPL.
- Las solicitudes de asistencia, efectuados por usuarios o áreas de proceso, con incidentes de seguridad, deberán ser atendidos.
- Elaboración de un boletín donde se explica situaciones contraproducentes a la seguridad y dar respuesta a incidentes. (ver procedimiento PRO2NO2: Boletín de Seguridad Y Anexo 9).

5.2.7 Norma 6 | Capacitación de Seguridad

a. Objetivo

Capacitar a los usuarios de la Universidad, en temas de seguridad.

b. Consideraciones Generales

- El área de seguridad y CSIRT-UTPL tienen la responsabilidad de concientizar a los empleados y estudiantes de la UTPL en temas de seguridad
- El CSIRT-UTPL deberá enviar un boletín de seguridad a los miembros de la UTPL, cada mes para temas de seguridad.
- Los empleados y estudiantes de la UTPL pueden manifiesten sobre temas de seguridad de concientización que ayuden a mejorar la seguridad de la Universidad.

5.2.8 Norma 7 | Manejo y Uso CSIRT-UTPL

a. Objetivo

Dar a conocer a los usuarios de la Universidad, el uso de CSIRT-UTPL como respuesta a incidentes de seguridad.

b. Consideraciones Generales

- Los incidentes de seguridad que sufran los usuarios de la UTPL deberá ser notificada por medio de una llamada a la extensión del CSIRT-UTPL o por un correo electrónico a csirtutpl@utpl.edu.ec
- El CSIRT-UTPL deberá dar notificaciones de respuesta a los incidentes de seguridad investigando a todos los involucrados.
- CSIRT-UTPL deberá enviar un reporte oficial a la víctima y los involucrados.

5.2.9 Norma 8 | Acceso Autorizado De Personal Interno / Externo

a. Objetivo

Establecer conductas de seguridad con los usuarios para el manejo de la información o de equipos.

b. Consideraciones Generales

- Permitir acceder a departamentos toda aquella persona, que tenga contacto directo como empleado o estudiante y utilice los servicios de la Universidad.

- Identificar previamente al usuario consultando de que departamento ha sido enviado, si tiene permisos explícitos a los que este accederá, junto a la información personal del usuario que está manejando.

- Indicar que los alumnos, son usuarios limitados, estos tendrán acceso únicamente a los servicios de Internet y recursos compartidos de la red institucional, cualquier cambio sobre los servicios a los que estos tengan acceso, será motivo de revisión y modificación de esta política, adecuándose a las nuevas especificaciones.

- Mantener un respaldo en documento de la persona que llega al departamento, e identificarla a través de sus datos personales o número de cédula.

- Los usuarios cuando mantengan un acceso al equipo o red por parte de terceros es estrictamente restrictivo y permisible únicamente mediante firma impresa y documentación de aceptación de confidencialidad hacia la institución y comprometido con el uso exclusivo del servicio para el que le fue provisto el acceso.

5.3 ESTÁNDAR TÉCNICO

5.3.1 ET1NO1 | Creación de Contraseñas

TITULO	Estándar Técnico : Creación de Contraseñas
VERSION	1.0
AUTOR	Andrea S. Espinosa A.
ESTADO	Propuesta

- La longitud permisible de la contraseña debe tener una longitud mínima de 8 (ocho) caracteres.

- La contraseña debe tener una combinación alfanumérica, incluida en estos caracteres especiales.
- No se debe utilizar letras adyacentes del teclado como *asdfgh*, o numero consecutivos como *123456.*

- La contraseña no debe estar conformada por el nombre del usuario o cualquier otra información como: número cédula, nombres o apellidos, etc.

- Las contraseñas no deben poder deducirse de la información personal, información de otras personas o de información relacionada con gustos, preferencias, aficiones, ni nada que se pueda llegar a obtener o interpretar con su información o la de otros, incluso si esta información no está en línea.

5.4 PROCEDIMIENTOS

5.4.1 PRO1NO1 | Bloqueo de Usuario

TITULO	Procedimiento : Bloqueo de Usuario
VERSION	1.0
AUTOR	Andrea S. Espinosa A.
ESTADO	Propuesta

a. Hotmail

Paso 1: vez que ha ingresado en la cuenta de Hotmail, se debe acceder a “Iniciar sesión” y buscar el correo de la persona que deseo eliminar.

Paso 2: Una vez que has encontrado al usuario que deseas eliminar, se debe “Señalar el correo” que se encuentra en la parte central de la pantalla y eliminar sin abrirlo al correo. La Figura 5.1.

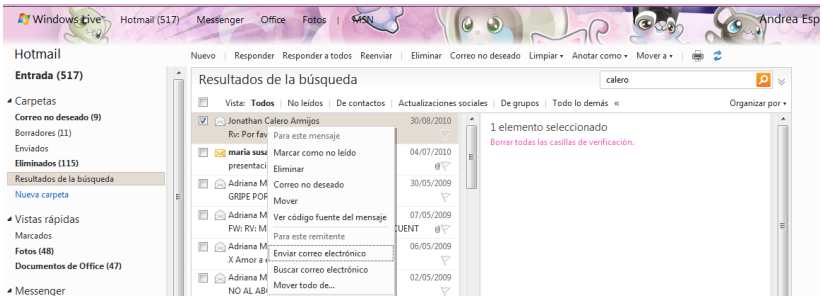


Figura 5. 1. Eliminación de correo

Paso 3: Luego se busca en “contactos” al usuario y se procede a “Eliminarlo “de la lista.

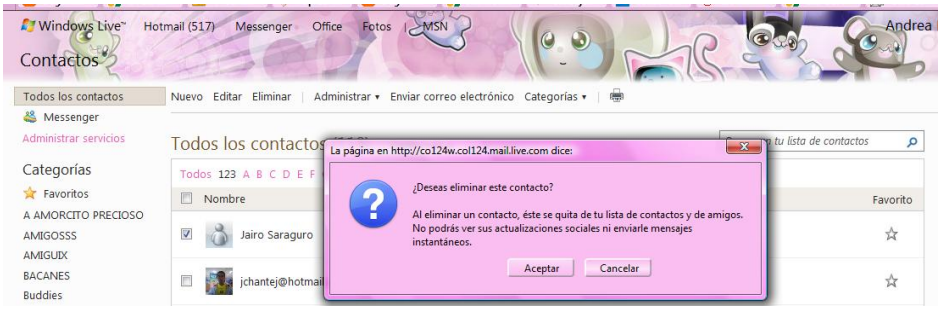


Figura 5. 2. Eliminar contacto

Paso 4: Luego hacer clic en “Aceptar” y se elimina el usuario.

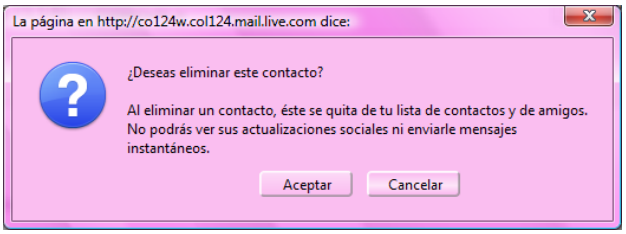


Figura 5. 3. Aceptar para eliminar contacto

5.5 PROCEDIMIENTOS

5.5.1 PRO2NO2 | Respuestas A Incidentes Y Anomalías De Seguridad

TITULO	Procedimiento : Respuestas A Incidentes Y Anomalías De Seguridad
VERSION	1.0
AUTOR	Andrea S. Espinosa A.
ESTADO	Aprobado

Presentación del Boletín

- Diseño del boletín de seguridad que nos permita mantener en contacto con los miembros de la UTPL. (ver en Anexo 9)

Con la utilización de mecanismos de protección de seguridad para evitar posibles ataques de Ingeniería Social, y buscar la manera de concienciar a los usuarios la importancia de proteger sus activos tecnológicos y la información que ellos manipulan, ya que esto es parte de la seguridad de la información. Basar programas de seguridad de la información en el cumplimiento de normativas ya que es condicionante decisivo de la financiación y la concienciación sobre la seguridad. Sin embargo, los fundamentos de un programa de seguridad no pueden llegar únicamente de la mano de iniciativas relacionadas con el cumplimiento de normativas o de la última herramienta tecnológica que promete protección contra los ataques, se debe trabajar de la mano con los usuarios que manejan la misma.

Aquí se ha puesto a consideración algunas de las normativas que pueden utilizarse para el manejo de la información por parte de los usuarios.

CONCLUSIONES

- Mediante encuestas realizadas a los miembros de la UTPL se pudo verificar que un 70% de los miembros de la Universidad no tienen conocimiento en cuanto a la existencia de la Ingeniería Social.
- Se pueden obtener información sensible (usuarios y contraseñas), ya que se el personal de la UTPL proporciona información fácilmente por distintos medios de la Universidad y **es susceptible a engaños**.
- Mediante la ejecución de las técnicas de ingeniería social se pudo evidenciar que el XX% entregar información sensible fácilmente, el XX% del personal no deja bloqueando su computado.
- Facilidad de acceso a los distintos departamentos por parte de usuarios tanto internos como externos, esto permite que se pueda dar robo de información, robo de claves, alteración de documentos.
- No hay lineamientos de seguridad que permitan a los usuarios proteger de la información y sus equipos de ataques como la ingeniería social. El teléfono es un medio muy poderoso para obtener información confidencial como: calificaciones de estudiantes, direcciones domiciliarias, direcciones de correo electrónico, nombres y apellidos de compañeros de trabajo.
- En el momento que se realizó las técnicas de ingeniería social se pudo evidenciar que el personal de Soporte Técnico no mantienen un sistema de identificación por lo que implica un fallo de seguridad; y cualquier persona podría suplantar a la identidad de este personal.
- En el Ecuador no un entidad o organización que pueda proporcionar información de delitos informáticos en ecuador por lo cual no se puede observar cual es el nivel de incidentes de seguridad en el ecuador.. No existen un porcentaje cuantitativo de ataques de Ingeniería Social en el Ecuador, existe solamente de algunos países de Sudamérica, en donde se lo toma en forma general junto con otros países.
- Existen leyes que no se especifican bien en los delitos informáticos o crímenes que se cometen, existen leyes en otros países que se las puede adaptar a la realidad de delitos que se han presentado en el Ecuador.

RECOMENDACIONES

- Incentivar mecanismos de cooperación con todos los miembros de la UTPL con el fin de disminuir ataques progresivos a los usuarios como: robo de información y claves, ataques por correo electrónico, suplantación de personas.
- Evitar publicar datos pasivos del personal y direcciones de correo electrónico de los miembros de la UTPL.
- Capacitar al usuario para el manejo y uso de claves, correo electrónico, teléfono dentro de la universidad y fuera de ella.
- Verificar previamente la veracidad de la fuente que solicite cualquier información sobre la red, equipo, información de la Universidad etc., su localización y las personas que se encuentran al frente de la misma.
- Establecer normas de seguridad en cuanto a gestores para el manejo y uso de información y de equipos.
- Controlar los accesos físicos a los distintos lugares de la Universidad que maneje información importante.
- **Establecer políticas que protejan al usuario y la información sensible que maneja de la Universidad.**
- Se debe establecer normativas de seguridad tanto a nivel del personal como de los sistemas para minimizar el impacto que puede tener un ataque de ingeniería social.

BIBLIOGRAFÍA

[1] Wikipedia Enciclopedia Libre, Ingeniería social (seguridad informática), [En línea http://es.wikipedia.org/wiki/Ingenier%C3%ADa_social_(seguridad_inform%C3%A1tica)], Citado el: 23 de Noviembre de 2009.

[2] Ingeniería Social, Teacher Lester,http://www.scribd.com/doc/7215979/Texto-Ingenieria-Social, 18 de octubre de 2008 Citado el: 24 de Noviembre de 2009.

[3] Ingeniería Social en el Siglo XXI, 8 Noviembre 2009, disponible; http://ingenieriasocialsigloxxi.wordpress.com/category/3-como-se-hace-ing-social/ , 8 de Noviembre de 2009, Citado el: 25 de Noviembre de 2009.

[4] Ingeniería social, Adrian Ramírez http://hackstory.net/index.php/Ingenier%C3%ADa_social_es#T.C3.A9cnicas_de_Ingenier.C3.ADa_Social, 21 de abril de 2009, Citado el: 30 de Noviembre de 2009

[5] Blog de tecnología, conversaciones en línea, http://blogs.laprensagrafica.com/litoibarra/?p=298, 01 de Septiembre de 2009, Citado el: 1 de Diciembre de 2009

[6] Revistas Ciencias La Ingeniería Social, acercándonos a los molestos Spam, Phishing y Hoax, Arteaga García Alían, http://www.revistaciencias.com/publicaciones/EkEkVFVEyZorqSOkTo.php, 3 de Junio de 2008, Citado el: 2 de Diciembre de 2009

[7] Introducción a la Ingeniería Social, Publicado el 22 de Mayo, 2007, http://valenzine.com/blog/2007/introduccion-a-la-ingenieria-social/ , Citado el: 3 de Diciembre de 2009

[8] [HACK] CURSO INGENIERIA SOCIAL 4-1Fri Octubre 4 18:56:09 CEST 2002, CAPITULO IV Técnicas de Ingeniería Social, http://mailman.jcea.es/pipermail/hacking/2002-October/001188.html, Citado el: 3 de Diciembre de 2009

[9] SEGURIDAD INFORMÁTICA, AMENAZAS, http://seguinfo.wordpress.com/category/amenazas/, 12 de diciembre de 2009, Citado el: 6 de Diciembre de 2009

[9] Ranking de ESET de abril: Crecen los niveles de detección de ataques, 01 de Mayo de 2008 disponible en: http://www.zma.com.ar/novedades/noticias.php?id=37, Citado el: 15 de Diciembre de 2009

[10] Instituto Nacional de Tecnologías de la Comunicación, Resumen Ejecutivo De La Segunda Oleada Del Estudio Sobre Seguridad De La Información Y E-Confianza En Los Hogares Españoles http://www.inteco.es/Seguridad/Observatorio Citado el: 18 de Diciembre de 2009

[12] Francisco José Oteo Fernández, Javier López Redondo, ISO/IEC 13335. Disponible en:http://www.eset.com.pa/threat-center/articles/informe_malware_america_latina.pdf Citado el: 26 de Diciembre de 2009

[13] SANS Institute Info Sec Reading Room, Social Engineering, Documento: A Means To Violate A Computer System, Malcolm Allen (updated June 2006) Citado el: 30 de Diciembre de 2009

[14] TopBits.com disponible en: http://www.byteguide.com/es/shoulder-surfing.html Citado el: 26 de Diciembre de 2009

[15] Enviar mail anónimo, Seguridad, en Blog e Internet, marzo 2006 disponible en: http://www.einicio.com/paginas/enviar-email-anonimo.html Citado el: 1 de Enero de 20010

[16] Microsoft TechNet, Cómo proteger la información confidencial de las amenazas de la ingeniería social, publicado marzo de 2006 disponible en: http://technet.microsoft.com/es-es/library/cc875841.aspx Citado el: 1 de Enero de 2010

[17] Seguridad en proyectos de gobierno electrónico, Diplomado de gobierno electrónico, disponible en: http://www.cca.org.mx/funcionarios/cursos/ge/contenidos/modulo6/material/06.pdf Citado el: Citado el: 3 de Enero de 2009

[18] CERT Coordination Center (CERT/CC), Social Engineering**,** disponible en: http://www.cert.org/incident_notes/IN-2002-03.html

[19] Sum Microsystems, Carlos A. Biscione Technical Account Manager North of Latin America Sun Microsystems, Documento: Ingeniería Social Para No Creyentes.

[20] Social engineering- Security Portal Lost letter technique, Disponible en: http://www.social-engineering.eu/techniques/lost_letter/

[21] Informática Jurídica, Posibles Sujetos De Los Delitos Informáticos. Disponibles en: http://www.informatica-juridica.com/trabajos/posibles_sujetos.asp

[22] Edpacsthe Edp Audit, Control, And Security Newsletter, Social Engineering Techniques, Risks, And Controls, APRIL–MAY 2008, Disponible en: http://www.informaworld.com/smpp/ftinterface~content=a792909009~fulltext=713240930

[23] Inteco- Cert, Blog de la Seguridad de la Información, La crisis económica y la ingeniería social,http://www.inteco.es/blog/Seguridad/Observatorio/BlogSeguridad/Articulo_y_comentarios?postAction=getDetail&blogID=1000077536&articleID=1000162977 Citado el: 05 de enero 2010

[24] Pablo F Burgueño, Cómo actuar en caso de suplantación de identidad en blogs y redes sociales, Pablo F Burgueño, junio 2009, disponible en:

http://www.pabloburgueno.com/2009/06/como-actuar-en-caso-de-suplantacion-de-identidad-en-blogs-o-redes-sociales/

[25] Re-Floating the Titanic: Dealing with Social Engineering Attacks, David Harley Imperial Cancer Research Fund, London, Disponible en: http://cluestick.info/hoax/harley_eicar98.htm, Citado el: 15 de Febrero de 2009

[26] Social Engineering Techniques, Risks, and Controls, Gary Hinson, April 2008, http://www.informaworld.com/smpp/section?content=a792909009&fulltext=71324092 8

[27] Social Engineering, Alex Bomberg, International Intelligence Limited, Disponible en: http://www.hg.org/article.asp?id=5778 Citado el: 18 de Febrero de 2009

[28] El Sendero del Hacker http://www.scribd.com/doc/9700132/El-Sendero-Del-Hacker . 01 de Abril de 2009. Citado el: 29 de 02 de 2010

[29] Seguridad Informática, http://nuestro.net78.net/clases_jjaa/Seg_Inf/ACI%20%96%20425%20Clase_05b%20Herramientas%20y%20M%E9todos%20de%20Hacking.ppt 2006 Citado el: 1 de 03 de 2010

[30] KioskeaNet http://es.kioskea.net/contents/attaques/ingenierie-sociale.php3 16 de octubre de 2008, Citado el: 3 de 03 de 2010

[31] Utilización de *hacking* ético para diagnosticar, analizar y mejorar la Seguridad Informática en la intranet de vía celular comunicaciones y representaciones http://bieec.epn.edu.ec:8180/dspace/bitstream/123456789/765/8/T10527CAP1.pdf V Gaibor - 2007 Citado el: 15 de 03 de 20010

[32] Inteco Centro de Respuestas A incidentes de Seguridad http://cert.inteco.es/securityAdvice/Actualidad/Avisos_seguridad_no_tecnicos/Correos_maliciosos_simulan_provenir_CORREOS_201005 12 de mayo 2010. Citado el: 12 de 05 de 2010

[33] Detalle de aviso de seguridad para usuarios no técnico, Inteco Centro de Respuestas A incidentes de Seguridad http://cert.inteco.es/securityAdvice/Actualidad/Avisos_seguridad_no_tecnicos/Spam_falso_men saje_de_DHL_20100419, 19 de abril de 2010. Citado el: 19 de abril de 2010

[34] Inteco Centro de Respuestas A incidentes de Seguridad, Detalle de aviso de seguridad para usuarios no técnico, http://cert.inteco.es/securityAdvice/Actualidad/Avisos_seguridad_no_tecnicos/Terremoto_Haiti_infectar_usuario_20100119 19 de enero 2010. Citado el: 23 de 01 de 2010

[35] Noticias Sobre La Seguridad de la Información, http://blog.segu-info.com.ar/2009/10/estafa-usuarios-de-owa-un-nuevo-vector.html, 21 de Octubre de 2009, Citado el: 10 de abril de 2010

[36] Inteco Centro de Respuestas A incidentes de Seguridad, Detalle de aviso de seguridad para usuario no técnico, http://cert.inteco.es/securityAdvice/Actualidad/Avisos_seguridad_no_tecnicos/Facebook_aprovechado_para_enganar_usuarios_2010013, 13 de enero 2010, Citado el: 15 de enero de 2010.

[37] Inteco Centro de Respuestas A incidentes de Seguridad, Detalle de aviso de seguridad para usuario no técnico, http://cert.inteco.es/securityAdvice/Actualidad/Avisos_seguridad_no_tecnicos/Nueva_oleada_de_falsas_ofertas_de_empleo_02122009, 21 de diciembre de 2009, Citado el: 18 de Enero de 2010

[38] Inteco Centro de Respuestas A incidentes de Seguridad, Detalle de aviso de seguridad para usuarios no técnico http://cert.inteco.es/securityAdvice/Actualidad/Avisos_seguridad_no_tecnicos/Correo_malicioso_tras_la_muerte_Michael_Jackson, 30 de junio de 2006, Citado el: 25 de febrero de 2010

[39] Inteco Centro de Respuestas A incidentes de Seguridad, Detalle de aviso de seguridad para usuarios no técnicos, http://cert.inteco.es/securityAdvice/Actualidad/Avisos_seguridad_no_tecnicos/Malware_SMS_Gratis, 05 de marzo de 2009, Citado el: 27 de febrero de 2010

[40] María de la Luz Lima, Delitos Electrónicos Pág. 100, Ediciones Porrua - México 1984. Citado el: 25 de abril de 2010

[41] Convenio de Cyber-delincuencia del Consejo de Europa Estados miembros del Consejo de Europa y otros Estados – Budapest 2001 http://www.coe.int, 11 Febrero de 2009, Citado el: 25 de abril de 2010

[42] REDIRIS, Incidentes de seguridad que afectan a la Red Académica y de Investigación Española,RedIRIS, para el año 2011, http://www.rediris.es/cert/doc/informes/2011/node3.html,2012-01-27, Citado el: 10 de Octubre de 2012.

[43] Pedro Miguel Lollet R, Auditoria Forense, Publicado por ACGAF, http://auditoriaforense.net/ Citado el: 25 de abril de 2010

[44] RODRÍGUEZ, Gonzalo, ALONSO, Jaime.“Derecho Penal e Internet”. Editorial la Ley. 2.002 pp.266, http://www.proasetel.com/paginas/articulos/acceso_no_autorizado.htm, 2006, Citado el: 25 de abril de 2010

[45] Facultad de Ingeniería en Electricidad y Computación Maestría en Sistemas de Información Gerencial, Laura Ureta, “RETOS A SUPERAR EN LA ADMINISTRACIÓN DE JUSTICIA ANTE LOS DELITOS INFORMÁTICOS EN EL ECUADOR", Citado el: 11 de octubre de 2010.

[46] Delitos Informáticos, Universidad Técnica Particular de Loja, Citado en: 15 de octubre 2010

[47] Proyecto Cert Ecuador/CC, Desarrollo de Proyecto de Implementación del CERT Ecuador , https://sites.google.com/site/certecuadorcc/home, Citado el: 09 de Octubre de 2012

,

ANEXOS

ANEXO 1- ENCUESTAS PARA DOCENTES Y PERSONAL ADMINISTRATIVO

Edad…….

Sexo Masculino ( ) Femenino ( )

¿Sabe lo que es Ingeniería Social?

SI ( ) NO ( )

¿Sabe lo que es un Hacker o Atacante?

SI ( ) NO ( )

¿Qué tipo de correo más utiliza?

Hotmail ( )
Gmail ( )
Yahoo ( )
Mail UTPL ( )
Outlook Express ( )
Otro……..

Con que Frecuencia utiliza el correo electrónico

Cada día ( )
Varias veces por semana ( )
Al menos una vez a la semana ( )
Casi nunca ( )
Otro……

¿Qué tan a menudo Uds. Cambia las contraseñas de sus cuentas?

Al menos una vez al mes ( )
Cada dos a tres meses ( )
Nunca ( )

¿Ha compartido sus claves con otras personas?

SI ( ) NO ( )

¿Cree Uds. que el correo electrónico es seguro?

SI ( ) NO ( )

¿Le han llegado mensajes a su correo solicitando información confidencial (usuarios, contraseñas, número de celular, número de cédula, etc)?

SI ( ) NO ( )

Aproximadamente ¿Cuándo envía correo electrónico o cadenas de correo a cuantas personas lo hace?

De 5 a 10 ( )
De 10 a 25 ( )
De 25 a 35 ( )
Más 50 ( )
Más de 100 ( )

Cuando le llega un correo electrónico y le sale un mensaje diciendo que este mensaje podría contener virus ¿Usted qué hace...?

Verifica que el destino es confiable y lo abre ( )
Accede sin atender o prestar atención al aviso ( )
No le presta atención y lo deja allí ( )
Elimina/Borra ( )

¿Ha descuidado su contraseña dejándola en algún lugar visible?

SI ( ) NO ( )

Usted alguna vez ha proporcionado información personal a través de teléfono ¿Cómo claves, datos privados de la empresa, etc.?

SI ( ) NO ( )

¿Cuándo se retira o ausenta de su lugar de trabajo. Usted deja bloqueado su computador?

SI ( ) NO ( )

Cuándo recibe cartas o fax. ¿Usted averigua si realmente le ha enviado el remitente?

SI ( ) NO ( )

¿Alguna vez ha sufrido algún ataque agresivo como chantaje o extorsión para robarle claves o información confidencial?

SI ( ) NO ( )

Cuan a menudo utiliza el Windows Live Messenger MSN?

A diario ( )
Varias veces a la semana ( )
Una vez a la semana ( )
Nunca ( )

¿Usted envía documentos valiosos, como claves de un sistemas o información confidencial del trabajo por el Windows Live Messenger MSN?

SI ( ) NO ( )

Cuando realiza descarga de información confidencial de su cuenta de correo o de algún otro sitio ¿Desde dónde suele conectarse?

En casa ( )
En el trabajo ( )
Universidad ( )
Ciber Café ( )
Otro……

ANEXO 2- ENCUESTAS PARA ESTUDIANTES

Edad…….

Sexo Masculino ( ) Femenino ( )

¿Sabe lo que es Ingeniería Social?

SI ( ) NO ( )

¿Sabe lo que es un Hacker o atacante?

SI ( ) NO ( )

¿Qué tipo de correo más utiliza?

Hotmail ( )
Gmail ( )
Yahoo ( )
Mail UTPL ( )
Otro…….

Con que Frecuencia utiliza el correo electrónico

Cada día ( )
Varias veces por semana ( )
Al menos una vez a la semana ( )
Casi nunca ( )
Otro……

¿Qué tan a menudo Uds. Cambia las contraseñas de sus cuentas?

Al menos una vez al mes ( )
Cada dos a tres meses ( )
Nunca ( )

¿Ha compartido sus claves con otras personas?

SI ( ) NO ( )

¿Le han llegado mensajes de correo solicitando información confidencial (contraseña, número de celular, número de cédula, etc)?

SI ( ) NO ( )

Cuándo le sale un mensaje, alerta o algo llamativo en su pantalla mientras navega. ¿Usted rápidamente se enlaza a la página?

SI ( ) NO ( )

Aproximadamente ¿Cuándo envía correo electrónico o cadenas de correo a cuantas personas lo hace?

Menos de 10 ( )
De 20 a 40 ( )
De 40-50 ( )
Más de 100 ( )

¿Cuántas veces ha realizado cambio de contraseña en alguna de sus cuentas de correo o red social?

1 a 5 veces ( )
5 a 10 veces ( )
15 a 20 veces ( )
Nunca ( )

¿Alguna vez ha sufrido algún ataque agresivo como chantaje o extorsión para robarle claves o información confidencial?

SI ( ) NO ( )

Cuando realiza descarga de información de su cuenta de correo o de algún otro sitio ¿Desde dónde suele conectarse?

En casa ( )
En el trabajo ( )
Universidad/colegio ( )
Ciber Café ( )
Otro……

¿Ha ingresado alguna sala de chat?

SI ( ) NO ( )

Cuando se encuentra en un chat y aparece una solicitud de una persona desconocida que desea que lo agregues ¿Usted qué hace?

Lo acepta ( )
Busca conocer el perfil ( )
Lo Bloquea ( )
Lo Denuncia ( )
O Elimina ( )
Otro……

Cuando se encuentra en un chat y aparece un mensaje que pide que ingrese a una página ¿Usted qué hace?

Ingresa a esa pagina ( )

Lo ignora ( )

Lo Bloquea ( )

Otro……

Alguna vez ha descargado virus desde:

Navegador ( )

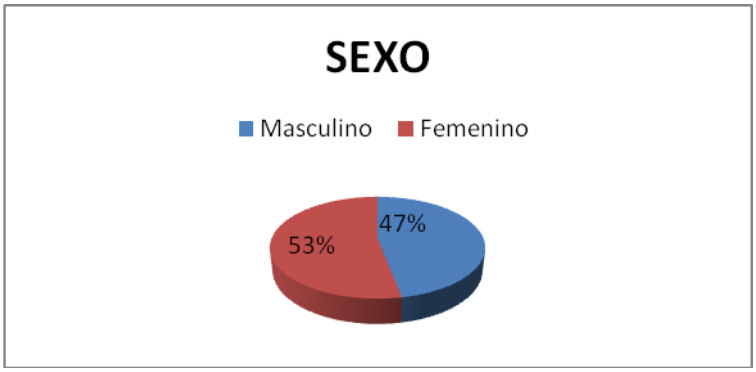
Correo Electrónico ( )

Dispositivos de almacenamiento (CD, USB) ( ) Otros……

ANEXO 3- ANALISIS DE LA ENCUESTAS DE DOCENTES Y PERSONAL ADMINISTRATIVO

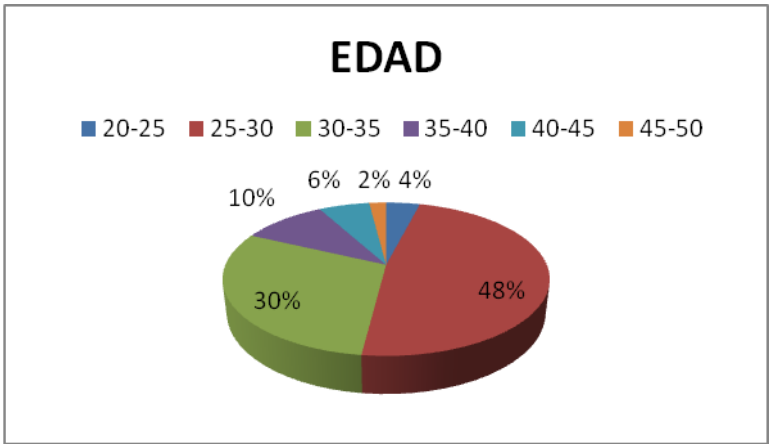
El estudio tiene por objeto indagar en el conocimiento de los docentes y personal administrativo de la UTPL manifiestan sobre el tema de la Ingeniería Social. Está basado en las respuestas de 100 encuestas, divididas entre hombres y mujeres y edad de la siguiente manera:

SEXO: Masculino 47 y Femenino 53



Anexo 3 - Figura 1. SEXO Masculino Femenino

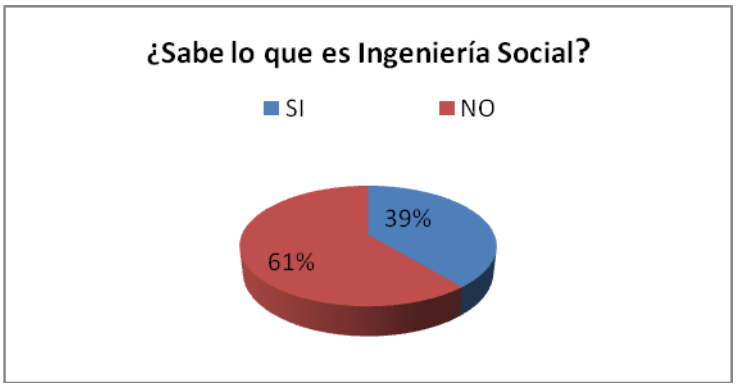
Edad: 25 a 45 años



Anexo 3 - Figura 2. Edad

A continuación, se presenta un resumen de las principales conclusiones del estudio, que son desarrollados de acuerdo al conocimiento obtenido durante la realización de las encuestas.

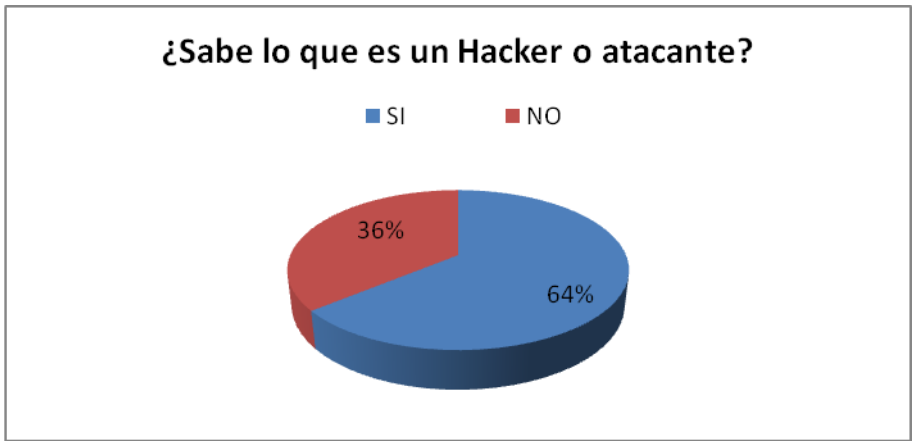
- En la primera pregunta:



Anexo 3 - Figura 3. Ingeniería Social

De las personas encuestadas se ha obtenido que un 61 % NO sabe o desconoce lo que es Ingeniería Social, y un 39 % responde SI sabe lo que Ingeniería Social.

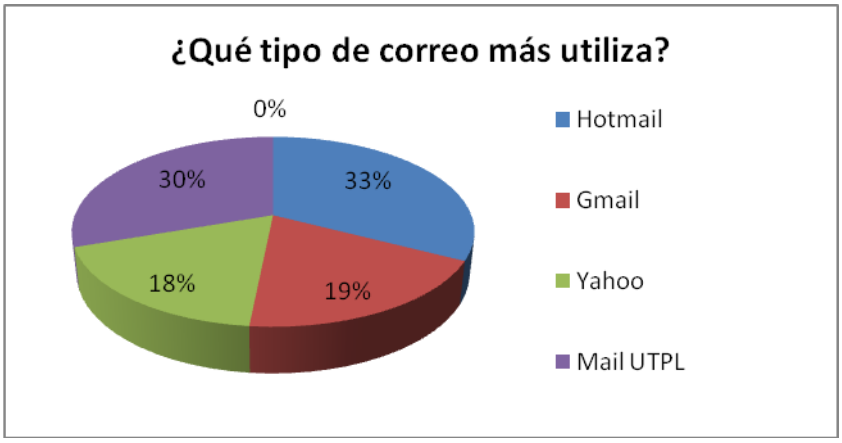
- En la segunda pregunta:



Anexo 3 - Figura 4. Hacker o Atacante

En la segunda pregunta tenemos que un NO tiene un 64% alto y un SI 36 %, un porcentaje bajo de si sabe lo que es un Hacker o atacante. Existe una diferencia considerable entre ambas contestaciones con respecto a la pregunta.

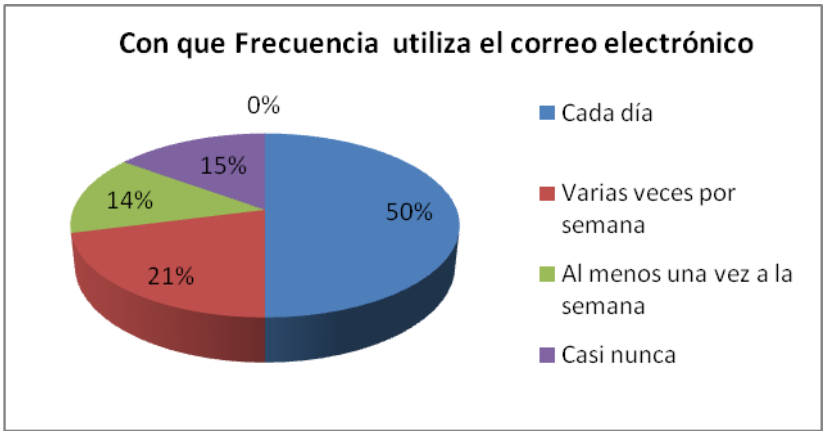
- En la tercera pregunta:



Anexo 3 - Figura 5. Correo Mas Utilizado

En esta pregunta realizada dentro de la encuesta he obtenido respuestas muy variadas y con casi iguales elecciones. Tenemos que 33% utiliza Hotmail, 30% utiliza Mail UTPL, 19% utiliza Gmail, y finalmente un 18% utiliza Yahoo. De acuerdo a estas respuestas tenemos distintas elecciones en la utilización de correo electrónico.

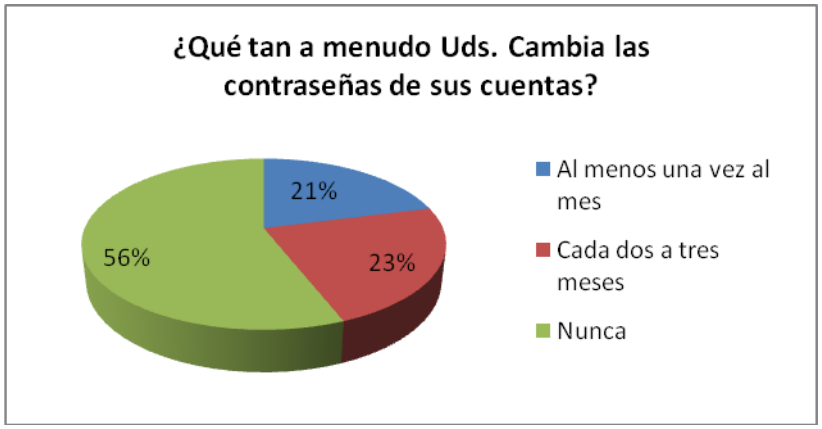
- En la cuarta pregunta:



Anexo 3 - Figura 6. Correo Electrónico Utiliza

Esta pregunta es en relación a la tercera pregunta realizada, aquí lo que se obtiene es la frecuencia con la que utiliza estos correos, tenemos que un 50% lo utiliza cada día, un 21% utiliza varias veces por semana, un 15% utiliza casi nunca y finalmente un 14 % lo utiliza al menos una vez a la semana.

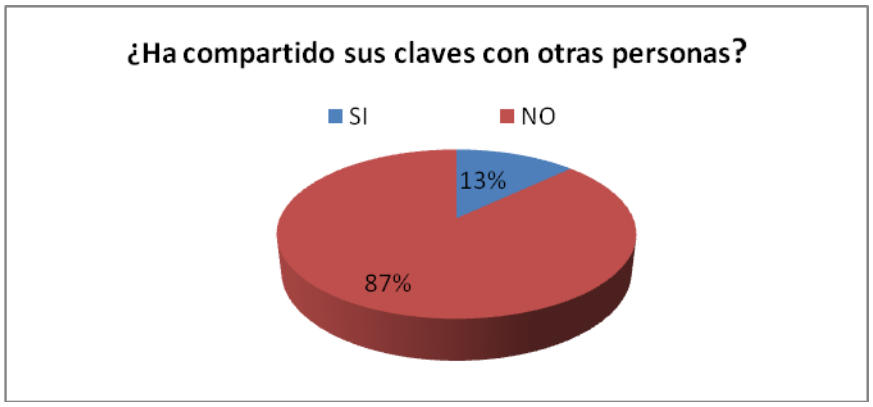
- En la quinta pregunta:



Anexo 3 - Figura 7. Hacker o Atacante

Que tan a menudo cambian las contraseñas respondieron con un 56% que Nunca, y con 23% cada dos a tres mese y un 21 % en último lugar al menos una vez al mes. De esta manera se que no existe un hábito de cambio de contraseña y falta de concientización del valor de cambiar una contraseña y es un punto débil en la seguridad de la información.

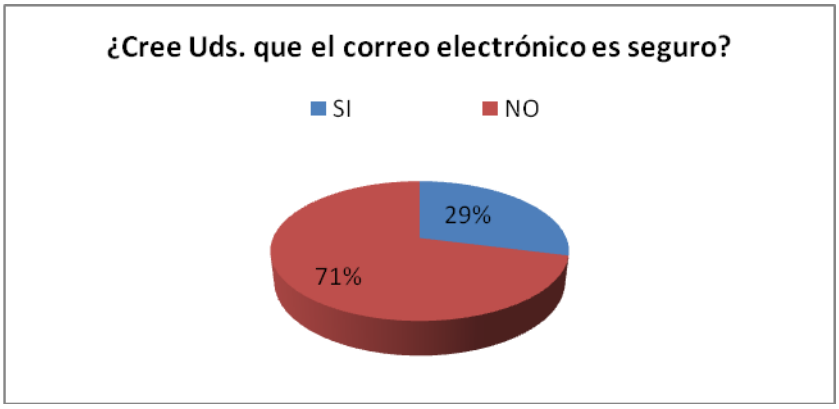
- En la sexta pregunta:



Anexo 3 - Figura 8. Compartición de claves

En esta pregunta sus repuesta ha sido concreta sobre si ha compartido sus claves y por ello tenemos que un NO tiene un porcentaje alto de 87%, y que un bajo tiene 13% con un SI. De esta manera se puede decir que no comparten las claves con otras personas sin descuidar el bajo porcentaje obtenido por un Sí.

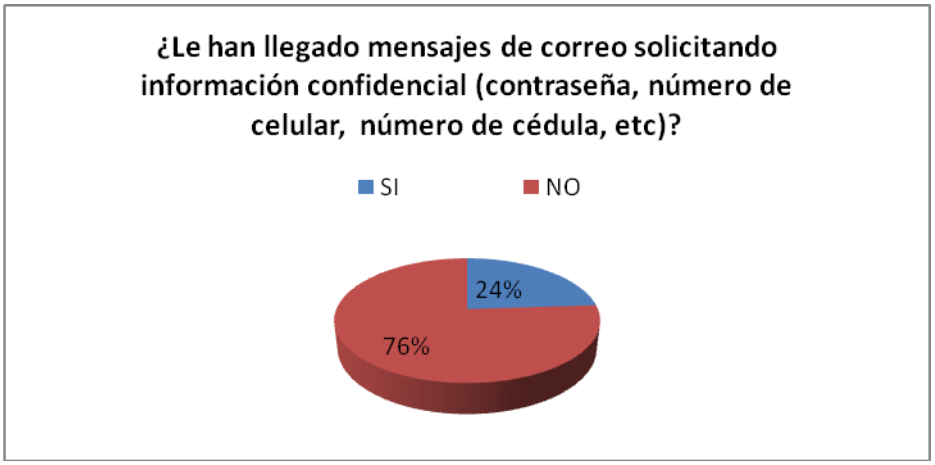
- En la séptima pregunta:



Anexo 3 - Figura 9. Correo electrónico seguro

Si observamos la figura podemos definir que existe 71% de un NO que manifiestan que el correo electrónico es seguro, y por otra parte un 29% indican lo creen, de esta manera podemos indicar que hay existe un porcentaje bajo, sin desconocer que por medio de esta pregunta se tiene indicios que se debe conocer y averiguar mas sobre un correo electrónico y la seguridad que nos proporciona.

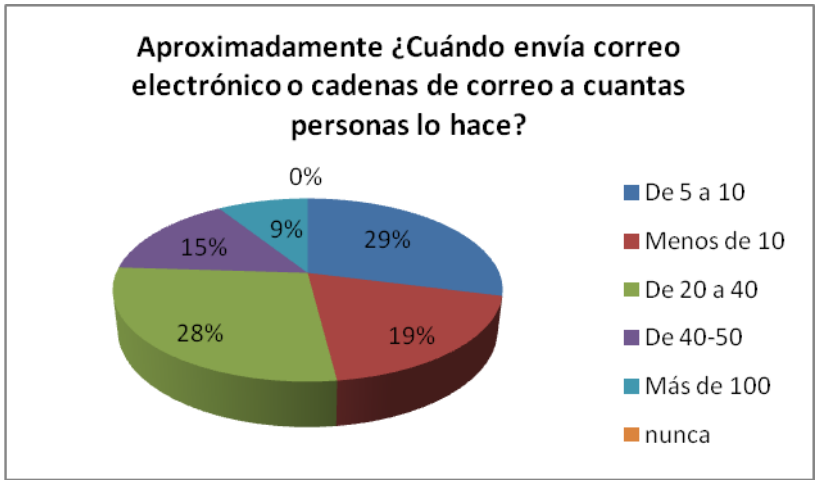
- En la octava pregunta:



Anexo 3 - Figura 10. Mensajes información confidencial

En la pregunta de obtuvo un porcentaje elevado como es de 76% con un NO, mientras que un 24% con un SI, han recibido algún tipo de mensaje de correo solicitando información confidencial.

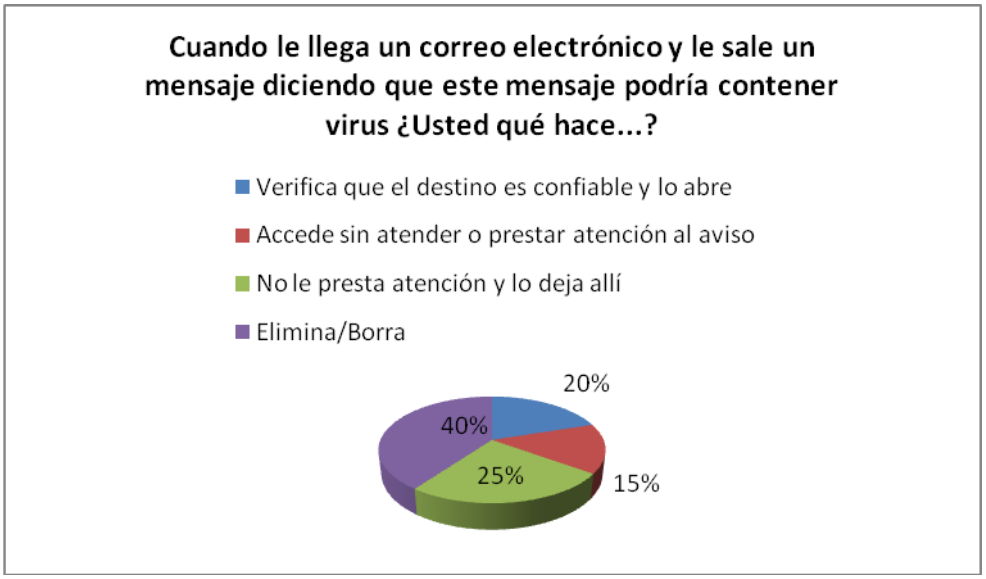
- En la novena pregunta:



Anexo 3 - Figura 11. Cadenas de Correo Electrónico

Con esto nos podemos dar cuenta que no se tiene la conciencia de la implicaciones de seguridad al enviar cadenas SPAM. Así en un alto porcentaje como es 29% que envía de 5 a 10 personas, un 28% envía de 20 a 40 persona, un 19% envía a menos de 10 personas, un 15% envía de 40 a 50 personas y finalmente un 9% envía correos electrónicos a mas de 100 personas.

- En la décima pregunta:



Anexo 3 - Figura 12. Mensaje con virus

Con esta pregunta sobre cuando le llega un correo electrónico y le sale un mensaje diciendo que este mensaje podría contener virus, he obtenido un porcentaje alto de un 40% lo elimina, un 25% no le presta atención y lo deja allí, un 20% verifica que el destino es confiable y lo abre, y finalmente 15% donde acceden si atender o prestar atención al aviso, de esta manera el usuario

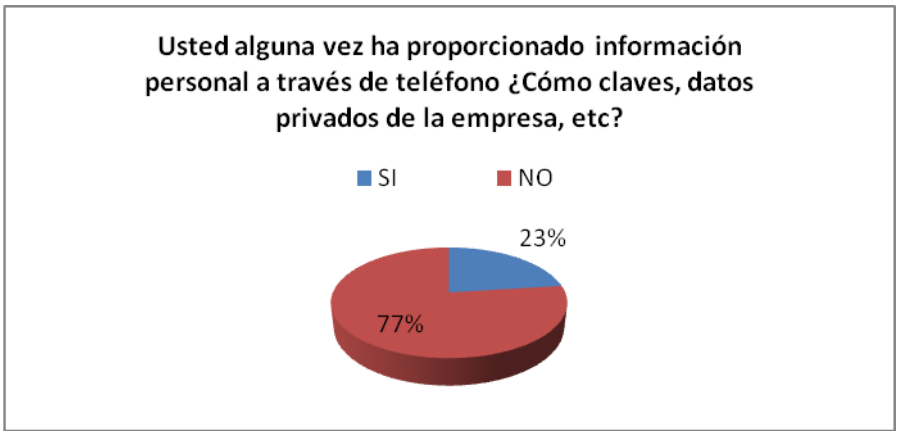
no se preocupa por la seguridad que tenga en su correo sino el acceso al mismo sin importar o tomar en cuenta los incidentes dentro del mensaje.

- En la décima primera pregunta:

Anexo 3 - Figura 13. Contraseña en lugar visible

Con respecto si ha descuidado la contraseña en algún lugar visible se obtiene que un NO mantiene un porcentaje de 82% alto, mientras que 18% con un SI, indicando que descuidan su contraseña, y no existe una seguridad alguna sobre las mismas.

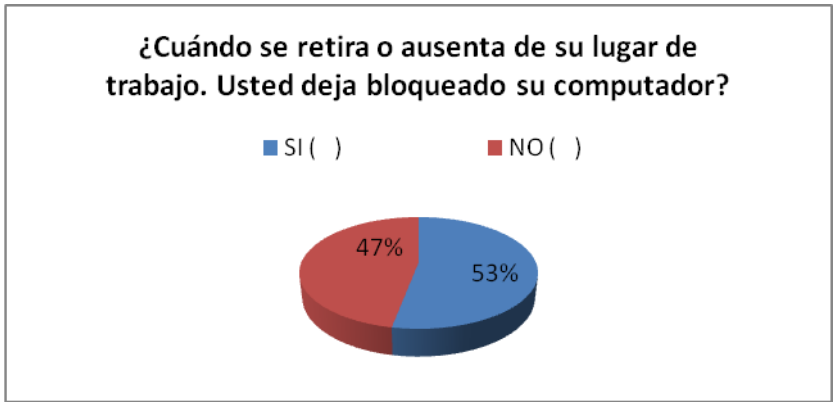
- En la décima segunda pregunta:



Anexo 3 - Figura 14. Información Telefónica

En la siguiente pregunta indica si alguna vez se ha proporcionado información a través del teléfono, con un 77% NO, ha proporcionado este tipo de información, en cambio con un bajo 23% SI han proporcionado, de esta manera se comete este tipo de errores pero con bajo porcentaje. Un porcentaje considerable de personas han entregado información confidencial por medios no seguros.

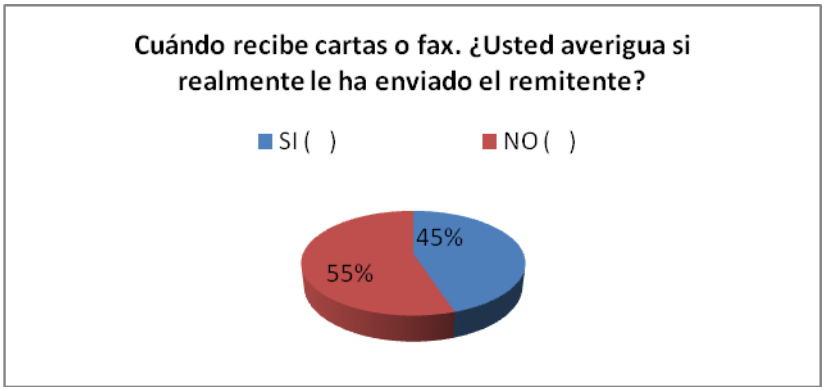
- En la décima tercera pregunta:



Anexo 3 - Figura 15. Bloqueo de Computador

Los porcentajes de la respuesta con respecto a la pregunta son casi equitativos ya que existe un 53% en respuesta SI, y con un NO en cambio un 47%, por lo tanto existe casi equivalente en la respuesta. EL usuario no toma a consideración los múltiples riesgos que corre al dejar su computador con información confidencial a disposición de otros usuarios.

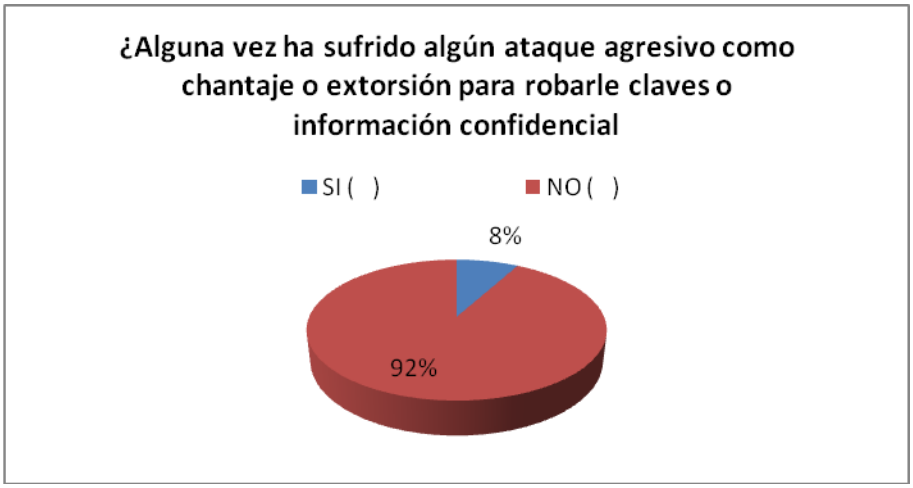
- En la décima cuarta pregunta:



Anexo 3 - Figura 16. Cartas o Fax

Para la pregunta Cuando recibe cartas o fax. Averigua si realmente le ha enviado el remitente, se obtiene un NO con un 55%, indica realmente no averigua, y con un 45% un SI, averigua si ha sido realmente quien le ha enviado el remitente. Existe en los usuarios un conformismo en cuanto a la información que reciben sea de quien fuese, no se preocupan por la seguridad que eso involucra en su trabajo.

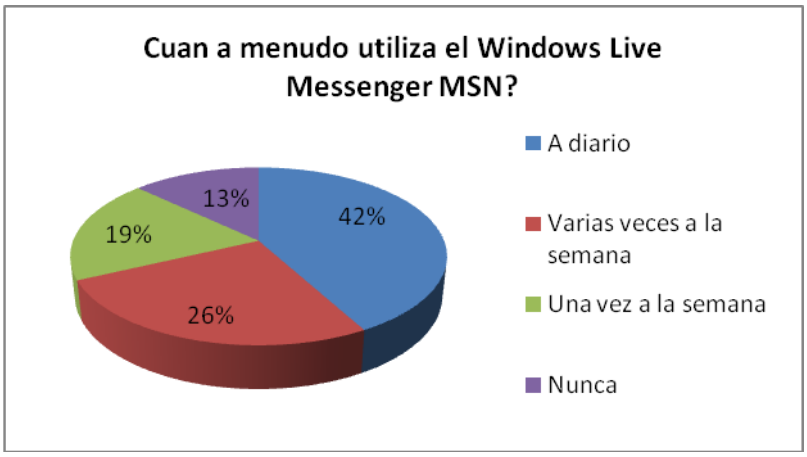
- En la décima quinta pregunta:



Anexo 3 - Figura 17. Ataques de Robo

En la pregunta realizada en la que si alguna vez ha sufrido algún ataque agresivo como chantaje o extorsión para robarle claves o información confidencial, se obtuvo que un 92% contesto NO, y con un 8% contesto que SI, indicando que de alguna manera han existido este tipo de ataques y que probablemente no le dieron la importancia que requería esa problemática.

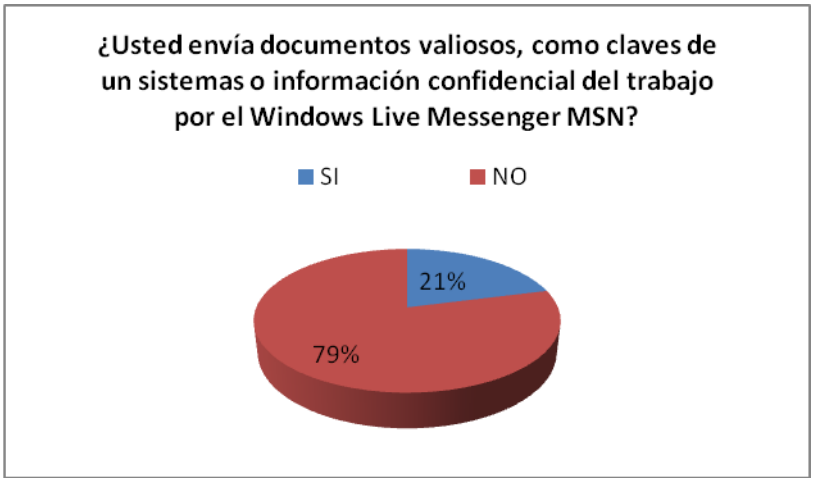
- En la décima sexta pregunta:



Anexo 3 - Figura 18. Utiliza Windows Messenger MSN

Esta pregunta relacionada con otras realizadas antes, nos proporciona cuan a menudo utilizan el Messenger MSN, se obtuvo que con un 42% lo utiliza a diario, un 26% lo utiliza varias veces a la semana, un 19% lo utiliza una vez a la semana, y con porcentaje no tan bajo de 13% nunca lo utilizan.

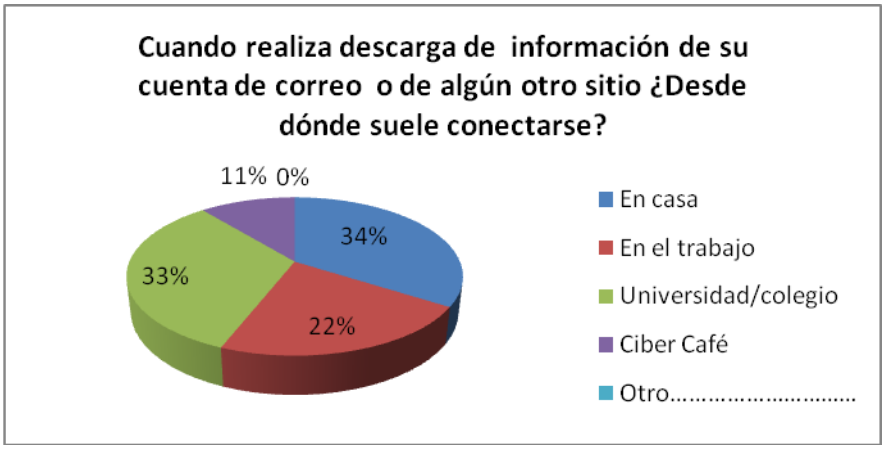
- En la décima séptima pregunta:



Anexo 3 - Figura 19. Envió de documentos por Windows Messenger MSN

Asociada a la pregunta anterior, se interrogaba sobre si se envían documentos valiosos, como claves de un sistema o información confidencial del trabajo por el Windows Live Messenger, donde se manifiesta que con un porcentaje alto de 79% respondió que NO y un bajo pero no insignificante 21% contesto que SI al envió de información confidencial. Igualmente es un porcentaje considerable, ya que puede haber fuga de información por este medio.

- En la décima octava pregunta:



Anexo 3 - Figura 20. Descarga de Información

En la última pregunta de la encuesta realizada donde obtuvimos que con 34% descargan información desde la casa, con 33% lo hacen en la Universidad/ colegio, con un 22% en el trabajo, y finalmente con un 11% desde Ciber Café.

ANEXO 4 - ANALISIS DE LA ENCUESTAS DE ESTUDIANTES

El estudio tiene por objeto indagar en el conocimiento de los estudiantes de la UTPL manifiestan sobre el tema de la Ingeniería Social. Está basado en las respuestas de 150 encuestas, divididas entre hombres y mujeres y la edad de la siguiente manera:

Sexo: Masculino 78 y Femenino 68

Edad: 15 a 40 años

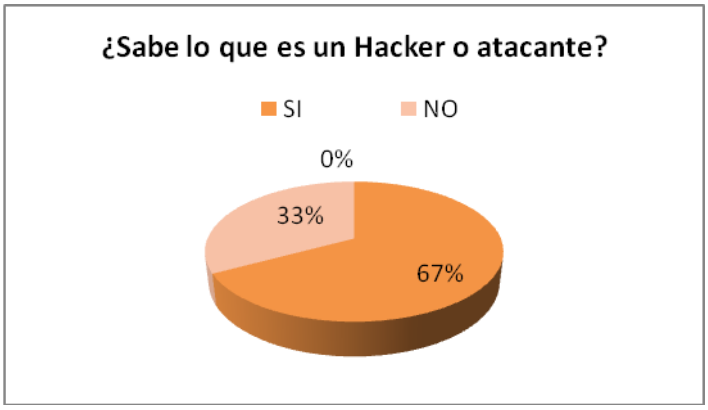
A continuación, se presenta un resumen de las principales conclusiones del estudio, que son desarrollados de acuerdo al conocimiento obtenido durante la realización de las encuestas.

- EN LA PRIMERA PREGUNTA:

Anexo 4 - Figura 1. Ingeniería Social

Se tiene un porcentaje elevado de un 76% que desconocen lo que es Ingeniería Social, y un porcentaje bajo de 24% que conoce lo que es Ingeniería Social. Esto de acuerdo a la pregunta sobre su conocimiento de Ingeniería social.

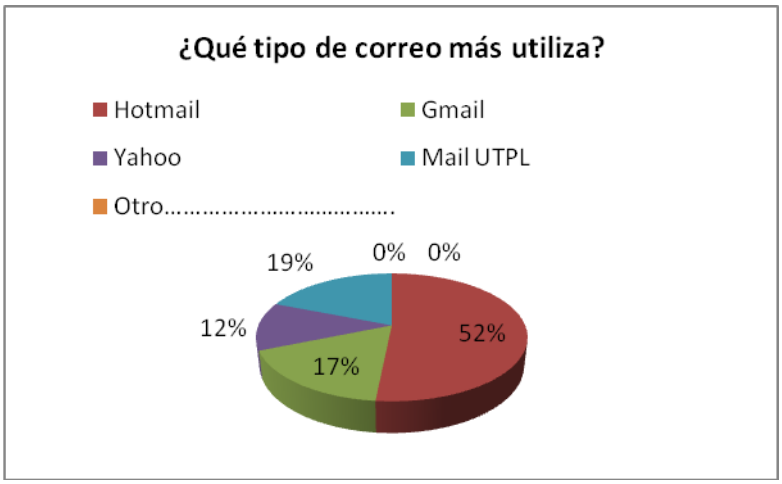
- EN LA SEGUNDA PREGUNTA:



Anexo 4 - Figura 2. Hacker o Atacante

De acuerdo a la pregunta sobre saber lo que es un hacker o atacante, se ha obtenido que un porcentaje bajo de 33% represente el conocimiento sobre el mismo, pero existen un porcentaje alto de estudiantes que desconocen lo que es un Hacker o atacante.

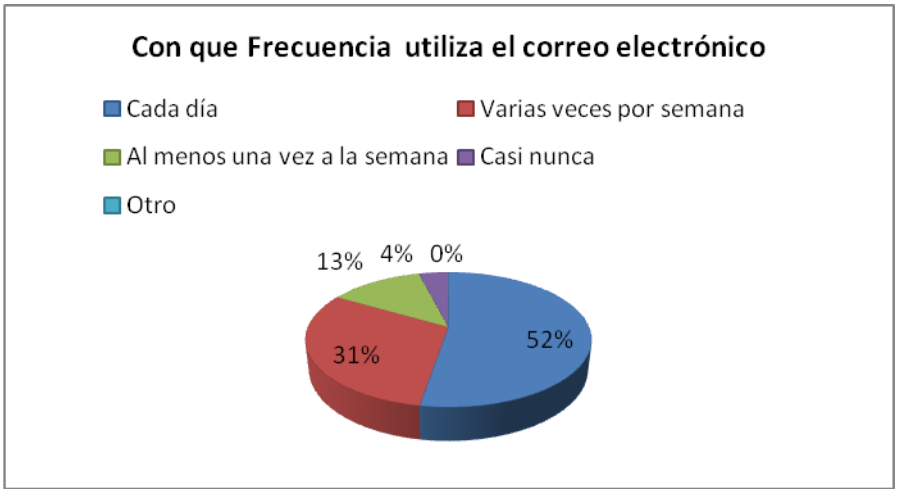
- EN LA TERCERA PREGUNTA:



Anexo 4 - Figura 3. Correo más utilizado

En el siguiente cuadro nos indica que el tipo de correo más utilizado es Hotmail con un 52%, luego con un porcentaje bajo, le sigue Yahoo con un 12%. Además existe la utilización de otras cuentas de correo electrónico como podemos observar, Gmail con un 17% y Mail UTPL con un 19%.

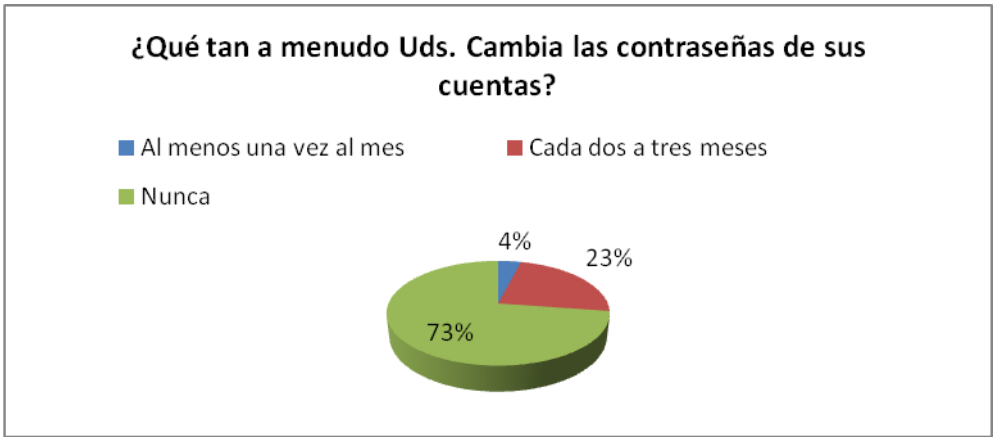
- EN LA CUARTA PREGUNTA:



Anexo 4 - Figura 4. Uso del Correo Electrónico

El uso de del correo electrónico se ve representado en la figura, donde presenta un porcentaje alto de 52% al uso cada diario del correo electrónico, así mismo un 31% al uso de varias veces por semana, pero un se observa que un 4% representa a casi nunca uso de correo electrónico.

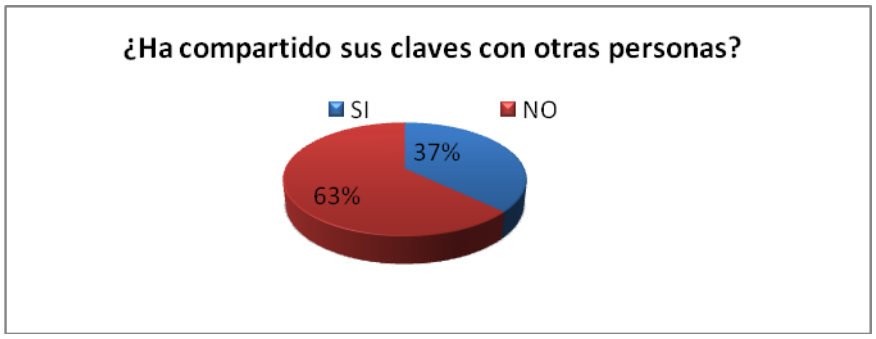
- EN LA QUINTA PREGUNTA:



Anexo 4 - Figura 5. Cambio de contraseñas

De los estudiantes encuestados tenemos que un 73% no cambia las contraseñas de sus cuentas y un 23 % la cambia cada tres meses, así mismo tenemos un bajo nivel sobre 4% que al menos una vez al mes cambian. Esto es un problema muy grave debido a que no toman las consideraciones necesarias al momento de establecer una contraseña ni el uso de la misma.

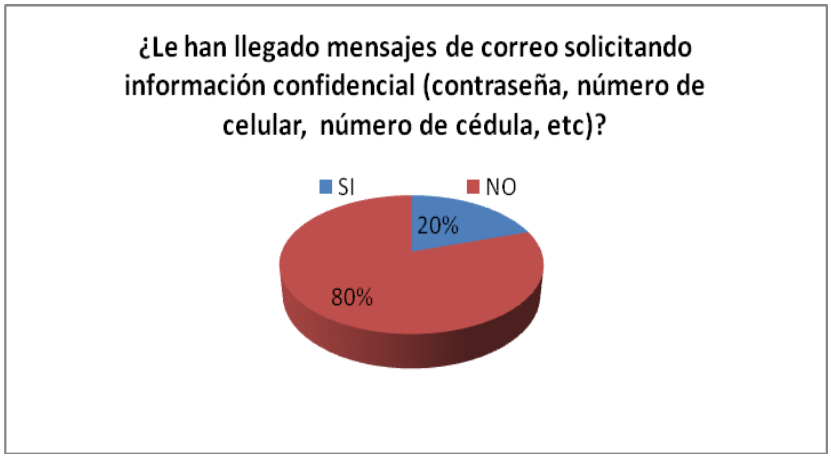
- EN LA SEXTA PREGUNTA:



Anexo 4 - Figura 6. Compartición de claves

En el siguiente cuadro presenta que un porcentaje alto de 63% de estudiante no comparten sus calves con otras personas, mientras que un 37% comparte sus claves con otros. Sin embargo es un porcentaje elevado tomando en cuenta que comparten sus contraseñas con otras personas sin tomar en cuenta los incidentes que pueden involucrarse.

- EN LA SÉPTIMA PREGUNTA:



Anexo 4 - Figura 7. Correo Información Confidencial

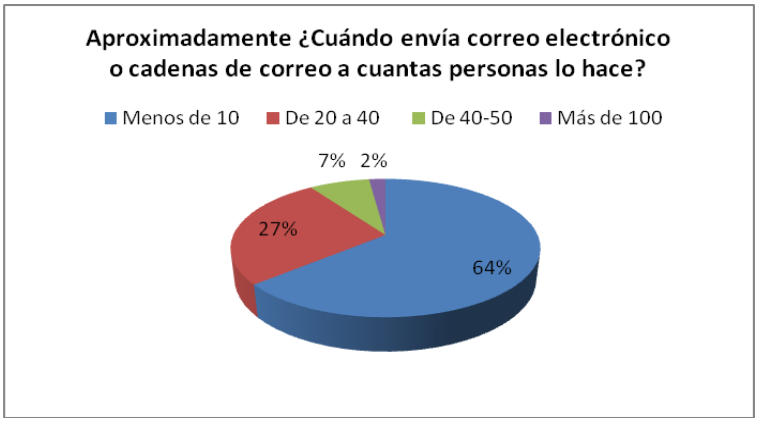
La figura nos indica qué de un total de 100 estudiantes, los mensajes de correo solicitando información confidencial, el SI tiene un porcentaje alto de 80% y de un NO corresponde a un 20%.

- EN LA OCTAVA PREGUNTA:

Anexo 4 - Figura 8. Alerta o Mensaje

En la siguiente pregunta la figura nos presenta 95% de los estudiantes que no se enlazan cuando aparece un mensaje mientras navega, pero existen un mínimo de 5% que si lo hace.

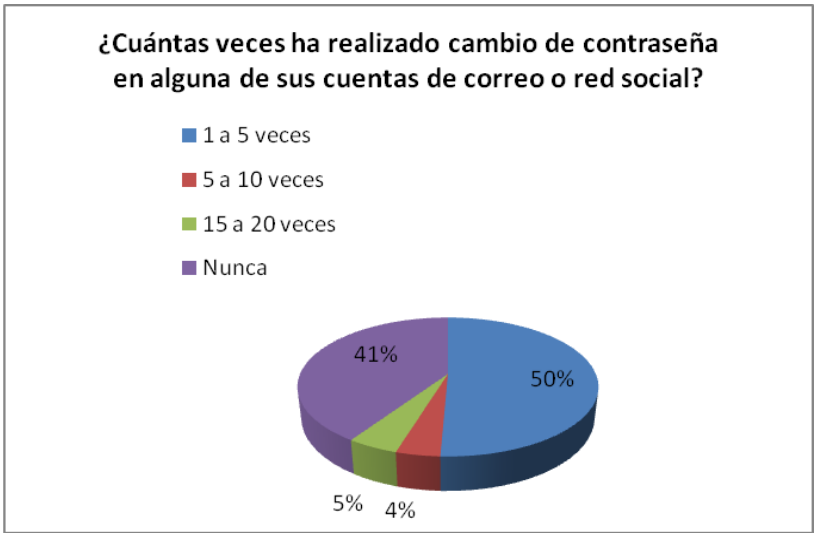
- EN LA NOVENA PREGUNTA:



Anexo 4 - Figura 9. Cadenas de Correo

Cuando se envía un correo electrónico o cadenas, la respuesta de los estudiantes es que ellos envían con un porcentaje alto de 64% que representa menos de 10 personas, y un porcentaje bajo de 2% a quienes envían a más de 100 personas.

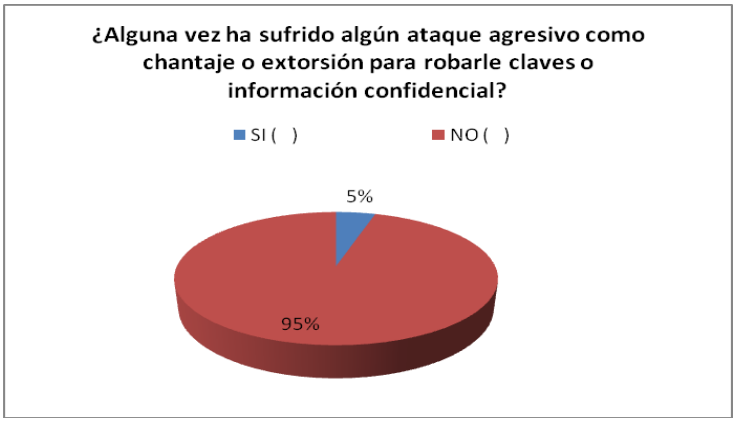
- EN LA DÉCIMA PREGUNTA:



Anexo 4 - Figura 10. Cambio de contraseña

El cambio de contraseñas según el siguiente cuadro lo realiza con un mayor porcentaje 50% de 15 a 20 veces y con un porcentaje bajo de 4% que equivale de 5 a 10 veces que ha r4ealizado el cambio de contraseñas de las cuentas. Esto es un problema muy grave para la seguridad de la información, señalando que el cambio de contraseña se lo debe hacer para evitar futuros incidentes en su seguridad.

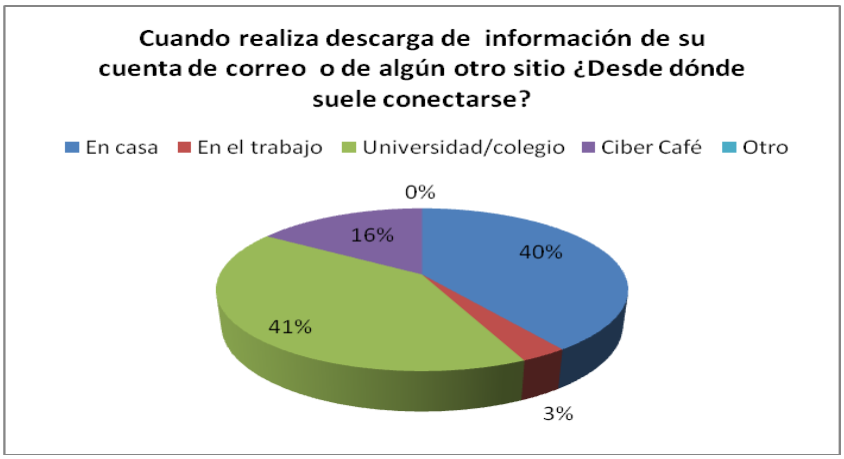
- EN LA DÉCIMA PRIMERA PREGUNTA:



Anexo 4 - Figura 11. Ataques y Robo de clave

Con la siguiente pregunta obtenemos como resultado que un alto porcentaje de 95% no ha sufrido algún tipo de ataque agresivo para obtener información confidencial, mientras que si registra un 5% bajo pero que si ha sufrido este tipo de ataque.

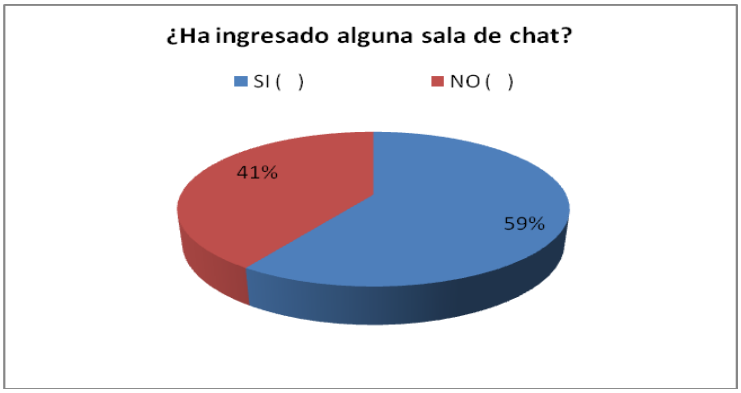
- EN LA DÉCIMA SEGUNDA PREGUNTA:



Anexo 4 - Figura 12. Descarga de Información

Para la descarga de información se obtiene como datos que un porcentaje alto de 41% realiza este método desde la Universidad/colegio, y que un bajo porcentaje de 16% realiza lo realiza desde un Ciber café, tomando en consideración que también lo realizan con 3% desde la casa.

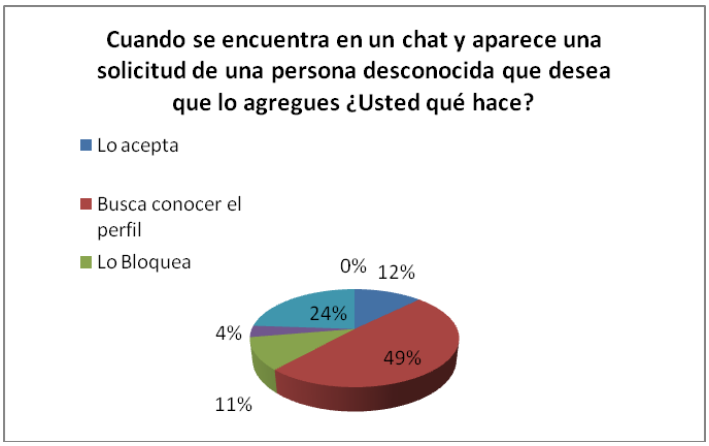
- EN LA DÉCIMA TERCERA PREGUNTA:



Anexo 4 - Figura 13. Sala de Chat

Se observa en la figura que los resultados de acuerdo a la pregunta de ingresar a una sala de chat, t4enemos que un porcentaje de 59% indica que SI ingresan a una sala de chat, pero que un 41% no tan bajo pero no ingresan a la sala de chat. Personas potenciales para un ataque de ingeniería social.

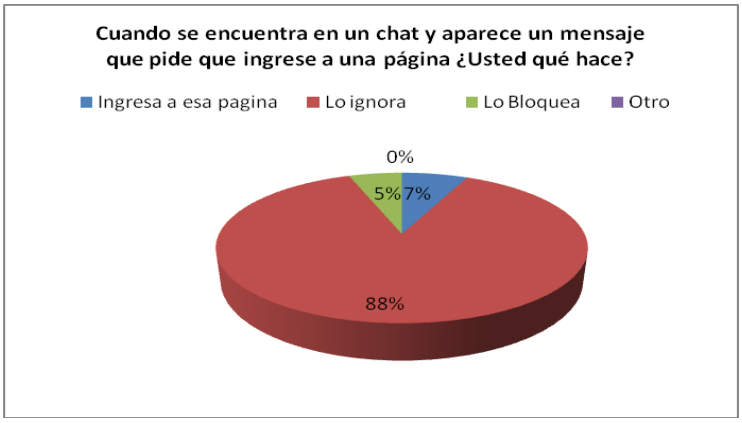
- EN LA DÉCIMA CUARTA PREGUNTA:



Anexo 4 - Figura 14. Chat Persona desconocida

El siguiente cuadro de porcentajes nos indica que valor existe cuando aparece alguna solicitud mientras se está en un chat, se ha obtenido que con un porcentaje alto un 49 % busca conocer el perfil, pero con un porcentaje bajo de 4% lo denuncia. Existen valores de un 12 % quienes lo aceptan, un 11% lo bloquean y un 24% lo acepta.

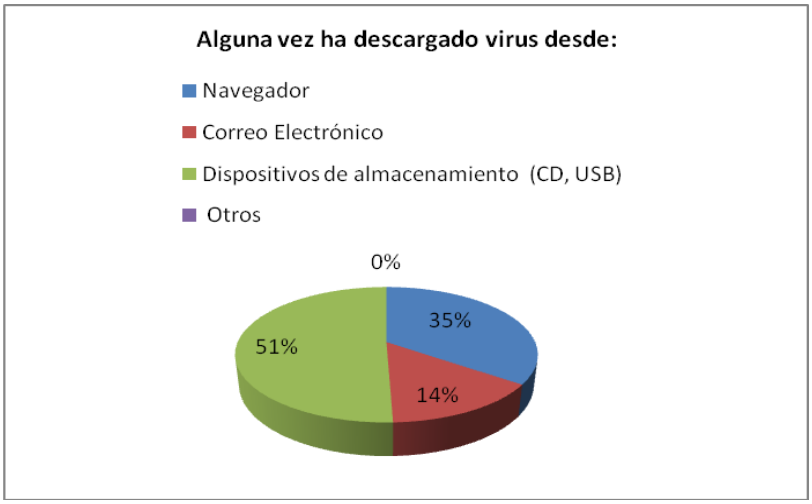
- EN LA DÉCIMA QUINTA PREGUNTA:



Anexo 4 - Figura 15. Chat Ingreso Página

Cuando estamos en un chat y aparece un mensaje que pide que ingresemos a la página Tenemos que con un porcentaje alto de 88% lo ignoran, y con un mínimo porcentaje de 5% lo bloquean, así mismo con un 7% a diferencia ingresan a la página.

- EN LA DÉCIMA SEXTA PREGUNTA:



Anexo 4 - Figura 16. Descarga de Virus

En la última pregunta de la encuesta respecto si ha descargado virus he obtenido que con un porcentaje elevado de 51% desde dispositivos de almacenamiento (USB, CD), pero un 14 % por medio del correo electrónico, y con un 35% por medio del navegador.

ANEXO 5 - TÉCNICA DE SUPLANTACIÓN Y OBSERVACIÓN

Dentro de las técnicas de la Ingeniería Social está las técnicas de suplantación y observación las cuales he utilizado para explotar las distintas vulnerabilidades, que se presentaron de acuerdo al análisis realizado mediante encuestas.

La ejecución de estas técnicas consistió en utilizar las distintas habilidades, conocimientos y aptitudes desempeñadas, para identificar posibles víctimas y dar inicio a la extracción de información. Para la realización de estas técnicas dentro de la UTPL básicamente lo divide en dos puntos estratégicos: Área de Secretarias, Soporte Técnica y Departamento Financiero que son los que poseen un alto porcentaje en proporcionar información sensible a personas internas como externas de acuerdo a las encuestas realizadas.

De forma específica asocie ambas técnicas, con la técnica de suplantación me base en utilizar el acceso a distintos sitios y equipos que tiene el personal de Soporte Técnico, es decir suplante a uno de ellos, y tener acceso a información sin levantar cualquier sospecha. Así mismo la técnica de observación se la realizó en silencio y memorizando información que estaba al alcance.

A continuación se presenta un análisis de la información obtenida mediante el uso de estas dos técnicas de la Ingeniería Social a las Áreas de Secretarias, Área de Soporte Técnico y Departamento Financiero.

ÁREA DE SECRETARIAS

INFORME

ESCUELA: Bioquímica y Farmacia

SECRETARIA: Lic. Luz María Ochoa

Descripción:

En la escuela disponen de un computador individual en donde accedimos a un Usuario **LuzMaria,** de la misma manera permitió adquirir la dirección IP del equipo **172.16.XX.XX.**

- Se proporcionó información mediante un diálogo, en donde se preguntó para que utilizaba su computador y qué tipo de información registraba.
- El tipo de Información que maneja es el sistema académico, el mismo que estuvo abierto mientras que se utilizaba el computador y se observó calificaciones de estudiantes, por ejemplo: González Lapo Gabriela Alejandra, Torres García Karina Noemí, Cuenca Erazo Andrés Vicente.
- En el escritorio se observo documentación confidencial de actas y oficios de estudiantes dirigidos al Dr. Roberto Beltrán solicitando terceras matriculas, en donde se indicaba nombres y apellidos con su cédula de identidad.
- Además se pudo observar cartas dirigidas al director de la escuela Malangón Avilés Omar Germán, PH D. con su correo XXXXX@utpl.edu.ec, dirección UTPL extensión 2205.

Observación:

- Al finalizar pudimos darnos cuenta que no solicitó ninguna identificación, tampoco realizó una llamada para cerciorarse de si pertenecía al grupo de soporte técnico y si habían enviado algún estudiante al realizar algún trabajo.
- Al salir no deja su computador bloqueado, solo indica a las demás personas que va a salir.

ESCUELA: Ingeniería Química E Industrias Agropecuarias

SECRETARIA: Lic. Odalia Armijos

Descripción:

- La secretaria dispone de computador individual para ambas escuelas, además supo proporcionar información personalmente, como el Usuario **cabilogica** y su contraseña**,** de la misma manera la dirección IP del equipo **172.16.0.00.**
- El tipo de Información que maneja es el sistema académico, el mismo que estuvo abierto, además de digitalizar la clave del sistema de matriculación mientras estaban los estudiantes presentes.
- En el escritorio se observo documentación confidencial como calificaciones de estudiantes, en donde se indicaba nombres y apellidos con su cédula de identidad. Por ejemplo Moncayo Cuenca Luis Ángel, Orellana Vera Edgar Fabián, Ortega Torres Gina Cecilia, Pineda Vélez Jenny Gabriela, Quezada Pardo Ana del Cisne, Quisatagsi Campoverde Gladys Margarita, Rivera Moreno Jenny Maritza etc.
- Además se pudo observar el envió de correo electrónico desde su mail xxxx@utpl.edu.ec, hacia estudiantes de la carrera, indicando autorización de matrícula.

Observación:

- Al finalizar pudimos darnos cuenta que no solicitó ninguna identificación, tampoco realizo una llamada para cerciorarse de si pertenecía al grupo de soporte técnico y si habían enviado algún estudiante al realizar algún trabajo.
- Entrego información mientras el sistema estaba abierto y estudiantes estaban presentes.

ESCUELA: Ciencias Biológicas y Ambientales

SECRETARIA: Lic. Magyener Salazar

Descripción:

- Dispone de un computador individual la secretaria de esta escuela, en donde se pudo acceder un Usuario **GestionAmbiental** y proporcionar su clave para ingresar**,** de la misma manera permitió adquirir la dirección IP del equipo **172.16.XX.XX.**
- Proporciono información que maneja como es el sistema académico, el mismo que estuvo abierto mientras que se utilizaba el computador.
- El computador quedo abierto un documento en donde se realizaba un oficio dirigido al director de la carrera José Ramiro Morocho Cueva y el correo xxxxx@utpl.edu.ec.

- En el escritorio una carta dirigida a la secretaria Salazar López Magyener Araceli de una empresa de electrodomésticos.
- Además se pudo observar documentos personales de la secretaria como una cartilla del Banco de Loja, y su cédula con el número 11030000-0, los mismos que estaban a lado del computador.

Observación:

- Al finalizar pudimos darnos cuenta que no solicitó ninguna identificación, tampoco realizo una llamada para cerciorarse de si pertenecía al grupo de soporte técnico y si habían enviado algún estudiante al realizar algún trabajo.
- Al salir no deja su computador bloqueado, solo indica a las demás personas que va a salir y regresaba en 15 minutos.
- Realizó una papeleta en donde se especificaba su nombre y cédula de identidad ya mencionados, así como el monto de 150 dólares.

ESCUELA: Hotelería y Turismo

SECRETARIA: Lic. Mónica Chamba

Descripción:

- La secretaria dispone de un computador individual, en donde se tuvo acceso a la dirección IP del equipo **172.16.0.00.**
- Proporcionó información mediante conversación vía telefónica sobre calificaciones obtenidas por estudiante que le indicaba su número de cédula #**1100000000.**
- Documentos indicando lista de estudiantes para ingresar notas al sistema.
- Permitió uso de la computadora a otra persona. Ejemplo. Becario, estudiante.

Observación:

- Al finalizar pudimos darnos cuenta que no solicitó ninguna identificación, tampoco realizó una llamada para cerciorarse de si pertenecía al grupo de soporte técnico y si habían enviado algún estudiante al realizar algún trabajo.
- Al salir no dejo su computador bloqueado, y lo ocupó otra persona.

ESCUELA: Comunicación Social

SECRETARIA: Lic. Marlene Paredes

Descripción:

- Dispone de un computador individual, en donde accedimos a un Usuario **Marlene Paredes** y su clave **XXXXX** de la misma manera permitió adquirir la dirección IP del equipo **172.16.0.00..**
- La secretaria maneja el sistema académico, el mismo que estuvo abierto mientras que se utilizaba el computador, además existían documentos abierto de horarios de docentes Ej. Lic. Germania Salinas, Claudia Zumba, María Punin.

- En el escritorio se observo documentación confidencial sobre solicitudes de matrícula de estudiantes Ej. Israel Rodríguez, Katherine Castillo.
- Además se pudo observar cartas dirigidas al director de la escuela Suing Ruiz Abel Romeo, Mgs, con su correo xxxxx@utpl.edu.ec dirección UTPL extensión 2221.

Observación:

- Al finalizar pudimos darnos cuenta que no solicitó ninguna identificación, tampoco realizo una llamada para cerciorarse de si pertenecía al grupo de soporte técnico y si habían enviado algún estudiante al realizar algún trabajo.
- Dejo becaria de reemplazo con su clave la misma que la dejo en un papel adherida a su computador.

ESCUELA: Lengua y Literatura

SECRETARIA: Lic. Rosa Margarita Loján

Descripción:

- Dispone de un computador individual por parte de la secretaria de esta escuela, se pudo acceder al equipo y al Usuario **Rosa,** de la misma manera permitió adquirir la dirección IP del equipo **172.16.0.00.**
- Se obtuvo información mediante un diálogo, en donde se preguntó para que utilizaba su computador y qué tipo de información registraba.
- El tipo de Información que maneja es el sistema académico.
- En el escritorio se observo documentación confidencial como un documento que especificaba nombre, apellidos y número de teléfono convencional, Ej. Diana Hualpa 072542134.
- Además se pudo observar informes de transferencias del Banco de Pichincha. Ej. Pauta Mercedes Roció.

Observación:

- Al finalizar pudimos darnos cuenta que no solicitó ninguna identificación, tampoco realizo una llamada para cerciorarse de si pertenecía al grupo de soporte técnico y si habían enviado algún estudiante al realizar algún trabajo.
- La secretaria presta el computador a otras personas.

ESCUELA: Arquitectura y Arte y Diseño

SECRETARIA: Lic. Luz María Ochoa

Descripción:

- Disponibilidad del computador individual por parte de la secretaria de esta escuela, en donde accedimos a un Usuario **LuzMaria,** de la misma manera permitió adquirir la dirección IP del equipo **172.16.0.00.**
- Se entablo conversación con la secretaria y nos indico la información en la que ella trabaja y lo que realiza.

- El tipo de Información que maneja es el sistema académico, el mismo que estuvo abierto mientras que se utilizaba el computador y se observo calificaciones de estudiantes, por ejemplo: González Lapo Gabriela Alejandra, Torres García Karina Noemí, Cuenca Erazo Andrés Vicente.
- En el escritorio se observo documentación confidencial de actas y oficios de estudiantes dirigidos al Dr. Roberto Beltrán solicitando terceras matriculas, en donde se indicaba nombres y apellidos con su cedula de identidad.
- Además se pudo observar cartas dirigidas al director de la escuela Malangón Avilés Omar Germán, PH D. con su correo xxxxx@utpl.edu.ec, dirección UTPL extensión 2205.

Observación:

- Al finalizar pudimos darnos cuenta que no solicitó ninguna identificación, tampoco realizo una llamada para cerciorarse de si pertenecía al grupo de soporte técnico y si habían enviado algún estudiante al realizar algún trabajo.
- Al salir no deja su computador bloqueado, solo indica a las demás personas que va a salir.

ESCUELA: Ciencias de la Computación y Electrónica y Telecomunicaciones

SECRETARIA: Lic. Lady Sanmartín

Descripción:

- La secretaria no se encontraba en su oficina además que su computador estaba sin bloquear y el sistema académico se encontraba abierto.
- Dispone de un computador individual para ambas carreras.
- En el escritorio se pudo observar documentación oficios de estudiantes dirigidos al Ing. Nelson Piedra director de la carrera de Ciencias de la Computación y a la Ing. Susana Arias directora de la carrera electrónica y Telecomunicaciones.

Observación:

- Al finalizar pudimos darnos cuenta que nadie presto atención a quienes estábamos observando en la oficina de la secretaria.
- La secretaria no dejó su computado bloqueada ni salido del sistema académico

LIDERES

SECRETARIA: Lic. MARTHA HERNANDEZ

Descripción:

- La secretaria dispone de un equipo individual, en donde tuvimos acceso a un Usuario **Martha,** de la misma manera permitió adquirir la dirección IP del equipo **172.16.0.00.**
- Proporciono información mediante un diálogo, así también pidió ayuda en algunas herramientas del computador.

- El tipo de Información que maneja es el sistema académico, el mismo que estuvo abierto ya que se encontraba emitiendo informes académicos a estudiantes que estaban presentes.
- En el escritorio se observo documentación como el Distributivo Académico.
- Además se pudo observar que la secretaria digito su clave del sistema académico y varias personas observaron como digitó su clave.

Observación:

- Al finalizar pudimos darnos cuenta que no solicitó ninguna identificación, tampoco realizo una llamada para cerciorarse de si pertenecía al grupo de soporte técnico y si habían enviado algún estudiante al realizar algún trabajo.
- No deja bloqueado su computador, solo apaga el monitor.
- No se percata que personas ajenas observan como digita su clave.

DEPARTAMENTO ADMINISTRATIVO FINANCIERO – INFRAESTRUCTURA Y SERVICIOS

SECRETARIA: Lic. Tania Gálvez

Descripción:

- Disponibilidad del computador individual por parte de la secretaria, en donde se accedió a un Usuario **Administrador** de la misma manera permitió adquirir la dirección IP del equipo **172.16.0.00.**
- Se observo información de empresas en donde se especificaba facturas de carros indicando la compañía que había emitido la factura **Automotriz Brazil**.
- Además se pudo observar el sistema Financiero que maneja la UTPL abierto, mientras realizaba la búsqueda de información.

Observación:

- Al finalizar pudimos darnos cuenta que no solicitó ninguna identificación, tampoco realizo una llamada para cerciorarse de si pertenecía al grupo de soporte técnico y si habían enviado algún estudiante al realizar algún trabajo.

SECRETARIA: Lic. Silvia Chicaiza

Descripción:

- Disponibilidad del computador individual por parte de la secretaria, en donde se accedió a un Usuario **Administrador** de la misma manera permitió adquirir la dirección IP del equipo **172.16.0.00.**
- Se observo carpetas indicando que tenían facturas y actas, las mismas que no estaban archivadas mientras la secretaria no se encontraba.
- También se pudo observar que se encontraban otros documentos como el MEMORANDUM UTPL al libre acceso.

Observación:

- Al finalizar pudimos darnos cuenta que no solicitó ninguna identificación, tampoco realizo una llamada para cerciorarse de si pertenecía al grupo de soporte técnico y si habían enviado algún estudiante al realizar algún trabajo.
- La secretaria no se encontraba en la oficina, pero el equipo estaba encendido y permitieron el acceso de otras secretarias.

AREA DE GRADUACIONES SOCIO HUMANISTICA

DIRECTORA: María Elvira Aguirre

SECRETARIA: Luisa Cosíos

Descripción:

- Dispone de un computador individual donde trabaja la secretaria, en donde accedimos a un Usuario **Administrador,** de la misma manera permitió adquirir la dirección IP del equipo **172.16.0.00.**
- Indico información que ella maneja mediante un diálogo.
- El tipo de Información que se maneja son los Estudios de Área de Graduaciones, Programa de Investigación Socio Humanística, Psicología, ingles, Notas, Informe de Biblioteca.
- En el escritorio se observó documentación confidencial de actas y oficios dirigidos a Directora María Elvira Aguirre.

Observación:

- Al finalizar pudimos darnos cuenta que no solicitó ninguna identificación, tampoco realizo una llamada para cerciorarse de si pertenecía al grupo de soporte técnico y si habían enviado algún estudiante al realizar algún trabajo.
- Al salir no deja su computador bloqueado.
- El usuario de administrador no pose contraseña.

AREA DE GRADUACIONES SOCIO HUMANISTICA

Dra. Sandra Patricia Díaz Agila

Descripción:

- Dispone de un computador individual, en donde accedimos a un Usuario **sandra,** de la misma manera permitió adquirir la dirección IP del equipo **172.16.0.00.**
- Además nos dio a conocer por ella mismo en lo que trabaja y que documentación mantiene en el equipo.
- El tipo de Información que se maneja son de los Centros Abiertos UTPL, lista de correos y números telefónicos, Ej. Ibarra #000000.

Observación:

- Al finalizar pudimos darnos cuenta que no solicitó ninguna identificación, tampoco realizo una llamada para cerciorarse de si pertenecía al grupo de soporte técnico y si habían enviado algún estudiante al realizar algún trabajo.

- Al salir no deja su computador bloqueado.
- El usuario administrador del equipo de la secretaria no posee contraseña.

COORDINADORA DE ESCUELA

SECRETARIA: Greys Tamaño

Dra. Sandra Patricia Díaz Agila

Descripción:

- Dispone de un computador individual, en donde accedimos a varios Usuario **profesor y docente,** de la misma manera permitió adquirir la dirección IP del equipo **172.16.0.00.**
- Indico la información que ella trabaja en el equipo.
- El tipo de Información que se maneja son de los Proyectos Investigativos de Escuelas.
- Trabaja en un sistema Fox y su clave **XXXX**, la cual se obtuvo debajo del teclado del equipo.

Observación:

- Al finalizar pudimos darnos cuenta que no solicitó ninguna identificación, tampoco realizo una llamada para cerciorarse de si pertenecía al grupo de soporte técnico y si habían enviado algún estudiante al realizar algún trabajo.
- Al salir no deja su computador bloqueado.
- Claves al alcance de cualquier persona

DEPARTAMENTO FINANCIERO

INFORME

SECRETARIA: Lic. Jesenia Romero

Descripción:

- La secretaria trabaja en un solo equipo individual, en donde se pudo acceder a su Usuario, y también permitió adquirir una dirección IP del equipo **172.16.0.00.**
- Se proporciono información mediante un diálogo con el Usuario, en donde nos comento que no poseía contraseña en su computador solo poseía cuenta de administrador.

Observación:

- Al finalizar pudimos darnos cuenta que no solicitó ninguna identificación, tampoco realizo una llamada para cerciorarse de si pertenecía al grupo de soporte técnico y si habían enviado algún estudiante al realizar algún trabajo.
- La cuenta de administrador del equipo no poseía contraseña

INFORME

SECRETARIA: Lic. Saide Loyola

Descripción:

- La secretaria dispone de un computador individual, al cual nos permitió acceder a su computador y dirección IP del equipo **172.16.0.00.**
- En su equipo trabaja en un sistema **ICDE**, el cual estuvo abierto mientras se obtenía los datos mencionados anteriormente, además existían papelitos adheridos a la pantalla del computador con los siguientes datos. Ej. **awrel, 893527, factura C10 00834.**
- En su escritorio existía documentación de pagos realizados, comprobantes de pago **Banco de Loja.**

Observación:

- Al finalizar pudimos darnos cuenta que no solicitó ninguna identificación, tampoco realizo una llamada para cerciorarse de si pertenecía al grupo de soporte técnico y si habían enviado algún estudiante al realizar algún trabajo.

INFORME

SECRETARIA: Lic. Yaneth Tandazo

Descripción:

- La secretaria dispone de un equipo individual, donde pudimos acceder y obtener la dirección IP del equipo **172.16.0.00.**
- En su equipo trabaja en el sistema **BAAN** con usuario **jtandazo**, en donde se estaba registrando pagos de facturas realizadas.
- Existía en su escritorio documentación como oficios de pagos destinados de distintas empresas. Ej. **TELEECUADOR.LTDA**

Observación:

- Al finalizar pudimos darnos cuenta que no solicitó ninguna identificación, tampoco realizo una llamada para cerciorarse de si pertenecía al grupo de soporte técnico y si habían enviado algún estudiante al realizar algún trabajo.
- Deja el sistema BAAN abierto con su usuario ingresado.

INFORME

SECRETARIA: Lic. Flora Carrión

Descripción:

- La secretaria dispone de un equipo individual, donde pudimos acceder y obtener la dirección IP del equipo **172.16.0.00.**
- En su equipo trabaja en el sistema BAAN con usuario **fsimalui**, en donde se estaba registrando pagos de facturas realizadas.
- Existía en su escritorio documentación como comprobantes de egresos.

Observación:

- Al finalizar pudimos darnos cuenta que no solicitó ninguna identificación, tampoco realizo una llamada para cerciorarse de si pertenecía al grupo de soporte técnico y si habían enviado algún estudiante al realizar algún trabajo.
- Deja el sistema BAAN abierto con su usuario.

INFORME

SECRETARIA: Lic. Lucila Matute

Descripción:

- La secretaria dispone de un equipo individual, donde pudimos acceder no se pudo obtener IP por cuanto no poseía conexión a Internet.
- En su equipo no mantiene contraseña, para la cuenta de administrador.
- En su escritorio tenia documentación que estaba ingresando en su computador como Facturas y oficios, Facturas de compras. Ej. **juanmartet factura 043023 con sello de entregado, Tetrix.**

Observación:

- Al finalizar pudimos darnos cuenta que no solicitó ninguna identificación, tampoco realizo una llamada para cerciorarse de si pertenecía al grupo de soporte técnico y si habían enviado algún estudiante al realizar algún trabajo.
- La cuenta de Administrador de su equipo no tienen contraseña.

INFORME

SECRETARIA: Lic. Isabel Fajardo

Descripción:

- La secretaria dispone de un equipo individual, donde pudimos acceder a la dirección IP del equipo **172.16.0.00.**
- En su equipo trabaja en el sistema BAAN con usuario **isabelF**, en donde se estaba registrando pagos.
- En su escritorio tenia documentación de pagos que se estaba ingresando al computador**.**
- Mantenía una lista de distintos pagos que habían realizado la UTPL a distintas entidades.

Observación:

- Al finalizar pudimos darnos cuenta que no solicitó ninguna identificación, tampoco realizo una llamada para cerciorarse de si pertenecía al grupo de soporte técnico y si habían enviado algún estudiante al realizar algún trabajo.
- No dejo cerrando el sistema ni bloqueando el computador y salió al Banco de Loja.
- Dejó abierto el sistema BAAN.

INFORME

SECRETARIA: Lic. Nancy Pizarro

Descripción:

- La secretaria dispone de un equipo individual, donde pudimos acceder a la dirección IP del equipo **172.16.0.00,** mantiene un usuario **administrador.**
- Maneja el sistema BAAN al cual se estaba ingresando y registrando facturas de empresas como Tlecade, McGrawill, Internew.

Observación:

- Al finalizar pudimos darnos cuenta que no solicitó ninguna identificación, tampoco realizo una llamada para cerciorarse de si pertenecía al grupo de soporte técnico y si habían enviado algún estudiante al realizar algún trabajo.
- No dejo cerrando el sistema ni bloqueando el computador y salió al Banco de Loja.
- Debo abierto el BAAN.

SECRETARIA: Lic. Betty Castillo

Descripción:

- La secretaria dispone de dos equipos, en donde la secretaria ocupaba uno y la becaria otro, se pudo acceder a ambos equipos y a la dirección IP de ambos el primer equipo **172.16.0.00.** y el segundo **172.16.0.00.**, también un usuario **tmedina.**
- En el equipo se estaba registrando proveedores y facturas, con valores como IVA. Ej. Cueva Germán factura 2311.

Observación:

- Al finalizar pudimos darnos cuenta que no solicitó ninguna identificación, tampoco realizo una llamada para cerciorarse de si pertenecía al grupo de soporte técnico y si habían enviado algún estudiante al realizar algún trabajo.
- La becaria tiene acceso al sistema de matriculación y BAAN, revelando que la secretaria le provee de la clave.

ANEXO 6 - TÉCNICA DE ENVIO DE CORREO ELECTRÓNICO

El correo electrónico es una forma de acercamiento hacia la víctima que permite introducirse disfrazado de muchas formas, ya sea que la dirección de correo electrónico resulte familiar o el asunto del e-mail de cierta forma "ataque" los sentimientos como la curiosidad, la avaricia, la compasión o el miedo es donde el usuario se vuelve susceptible a abrirlo.

Al haber obtenido mediante la técnica de observación información sobre los usuarios como la dirección de correo, permite de una manera más rápida centrar el objetivo en lanzar ataques por medio de correo electrónico hacia los usuarios de la UTPL, como Área de Secretarias, Departamento Financiero y Estudiantes.

Cuando se envió el correo electrónico se busco que sea tentativo al usuario para que lo pueda abrir y ejecutar de esta manera se enlazaría a la página que contiene incrustada una imagen transparente con un identificador dentro del correo electrónico el cual permitiría verificar que ha sido recibido y ejecutado.

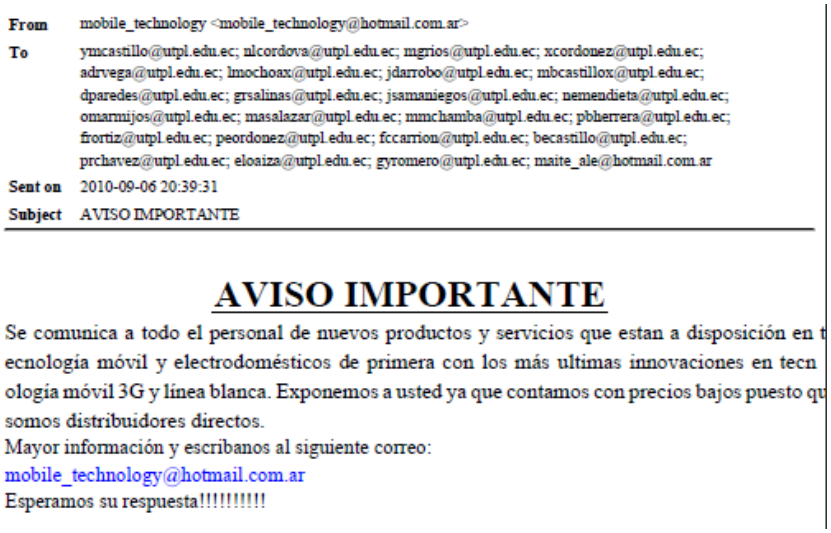
Para poder desarrollar esta técnica utilizamos herramientas como WhoReadMe y ReadNotify que son servicios de correo electrónico de seguimiento en línea que permitió el envió de mensajes desde su sitio web y recibir mensaje de alerta cuando ha sido recibido, ejecutado o borrado.

A continuación se presenta un informe de los ataques realizados a direcciones de correo electrónico hacia los usuarios de la UTPL.

INFORME

Primeramente con la creación de cuentas de correo electrónico en las distintas herramientas como WhoReadMe y ReadNotify, en donde empezamos formular un mensaje llamativo que lo puedan abrir y ejecutar los distintos usuarios.

A continuación se presenta la imagen del mensaje enviado a los distintos usuarios:



From mobile_technology <mobile_technology@hotmail.com.ar>

To ymcastillo@utpl.edu.ec; nlcordova@utpl.edu.ec; mgrios@utpl.edu.ec; xcordonez@utpl.edu.ec; adrvega@utpl.edu.ec; lmochoax@utpl.edu.ec; jdarrobo@utpl.edu.ec; mbcastillox@utpl.edu.ec; dparedes@utpl.edu.ec; grsalinas@utpl.edu.ec; jsamaniegos@utpl.edu.ec; nemendieta@utpl.edu.ec; omarmijos@utpl.edu.ec; masalazar@utpl.edu.ec; mmchamba@utpl.edu.ec; pbherrera@utpl.edu.ec; frortiz@utpl.edu.ec; peordonez@utpl.edu.ec; fccarrion@utpl.edu.ec; becastillo@utpl.edu.ec; prchavez@utpl.edu.ec; eloaiza@utpl.edu.ec; gyromero@utpl.edu.ec; maite_ale@hotmail.com.ar

Sent on 2010-09-06 20:39:31

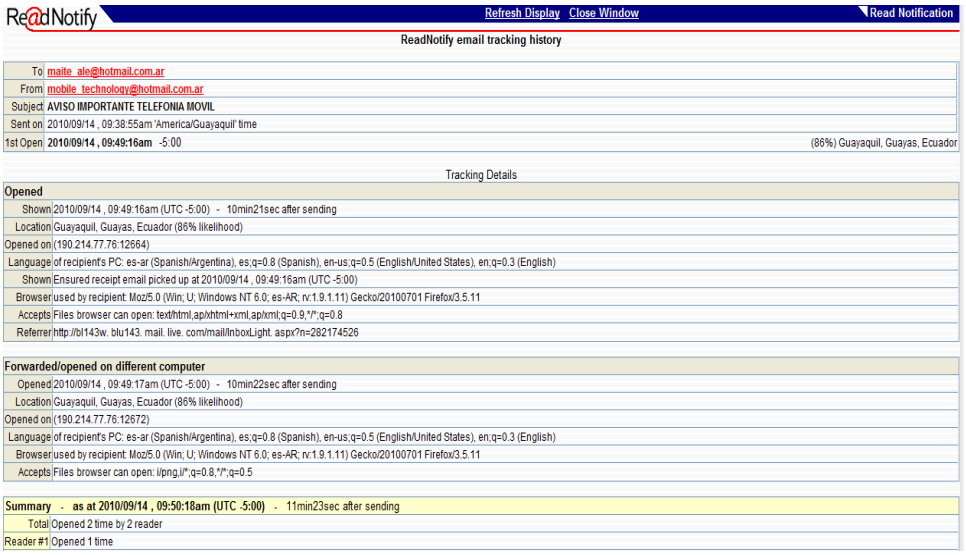
Subject AVISO IMPORTANTE

AVISO IMPORTANTE

Se comunica a todo el personal de nuevos productos y servicios que estan a disposición en t
ecnología móvil y electrodomésticos de primera con los más ultimas innovaciones en tecn
ología móvil 3G y línea blanca. Exponemos a usted ya que contamos con precios bajos puesto qu
somos distribuidores directos.
Mayor información y escribanos al siguiente correo:
mobile_technology@hotmail.com.ar
Esperamos su respuesta!!!!!!!!!!

Anexo 6 - Figura 1. Mensaje Importante

Cuando el mensaje es recibido y abierto, inmediatamente se recibe una notificación con los datos de la persona que abierto el email. Aquí se indica la hora a la cual fue abierto, la dirección IP del equipo.



Re@dNotify — Refresh Display Close Window — Read Notification

ReadNotify email tracking history

To	maite_ale@hotmail.com.ar
From	mobile_technology@hotmail.com.ar
Subject	AVISO IMPORTANTE TELEFONIA MOVIL
Sent on	2010/09/14 , 09:38:55am 'America/Guayaquil' time
1st Open	**2010/09/14 , 09:49:16am** -5:00 (86%) Guayaquil, Guayas, Ecuador

Tracking Details

Opened	
Shown	2010/09/14 , 09:49:16am (UTC -5:00) - 10min21sec after sending
Location	Guayaquil, Guayas, Ecuador (86% likelihood)
Opened on	(190.214.77.76:12664)
Language	of recipient's PC: es-ar (Spanish/Argentina), es;q=0.8 (Spanish), en-us;q=0.5 (English/United States), en;q=0.3 (English)
Shown	Ensured receipt email picked up at 2010/09/14 , 09:49:16am (UTC -5:00)
Browser	used by recipient: Mozi5.0 (Win; U; Windows NT 6.0; es-AR; rv:1.9.1.11) Gecko/20100701 Firefox/3.5.11
Accepts	Files browser can open: text/html,ap/xhtml+xml,ap/xml;q=0.9,*/*;q=0.8
Referrer	http://bl143w. blu143. mail. live. com/mail/InboxLight. aspx?n=282174526

Forwarded/opened on different computer	
Opened	2010/09/14 , 09:49:17am (UTC -5:00) - 10min22sec after sending
Location	Guayaquil, Guayas, Ecuador (86% likelihood)
Opened on	(190.214.77.76:12672)
Language	of recipient's PC: es-ar (Spanish/Argentina), es;q=0.8 (Spanish), en-us;q=0.5 (English/United States), en;q=0.3 (English)
Browser	used by recipient: Mozi5.0 (Win; U; Windows NT 6.0; es-AR; rv:1.9.1.11) Gecko/20100701 Firefox/3.5.11
Accepts	Files browser can open: i/png,i/*;q=0.8,*/*;q=0.5

Summary - **as at 2010/09/14 , 09:50:18am (UTC -5:00)** - 11min23sec after sending	
Total	Opened 2 time by 2 reader
Reader #1	Opened 1 time

Anexo 6 - Figura 2. Mensaje Recibido Re@d Notify

ANEXO 7 - TÉCNICA DE TELÉFONO

INTRODUCCIÓN

Una de las técnicas más fáciles de usar para los ingenieros sociales es el teléfono, puesto que le permite tener varias ventajas sobre la víctimas, es decir al realizar una llamada se puede ocultar el número y mantener el anonimato, permite actuar a distancia de la víctima lo que proporciona hacer difícil su búsqueda y solicitar información suplantando a personas internas de la empresa.
Cuando se realiza la llamada de teléfono es posible que no conteste la persona que estamos buscando o que simplemente no nos brinde información.

Al efectuar esta técnica a los usuarios de la UTPL como Área de Secretarias y Departamento Financiero se profundizo en utilizar medios que proporcionen un mayor acceso a ella como: ser muy educados, hablar siempre claro de forma fluida y ganarse confianza de la víctima.
De esta manera los distintos usuarios de la UTPL dieron información confidencial y valiosa para nuestro informe.

INFORME

Al realizar esta técnica de teléfono dentro de las instalaciones de la UTPL, primeramente indicamos ser técnicos de soporte y deseábamos instalar actualizaciones del antivirus, para ello realizamos dos pasos importantes:

- Se realizo una primera llamada en la que recabaríamos todos los datos como nombres de personas o datos técnicos de la máquina.
- En la segunda llamada que se realizo se descubrió que la misma persona nos revelo mucha más información que en la primera llamada, ya que indicaba los movimientos que había dado últimamente en su equipo, debido a que presentaba problemas técnicos.

DETALLE DE LLAMADA

- Hola Buenos días, con quien hablo?
- …..Soy……. De……
- .- Bien soy de técnico del grupo Soporte Técnico , quería hablar
- Con……..
- .- Soy yo mismo, usted dirá.

  Mi llamada tiene que ver con las actualizaciones de antivirus de las máquinas y queremos que usted mismo nos ayude desde su equipo a realizar modificaciones para ello yo le iré indicando por teléfono los pasos de manera rápida y sencilla.
- - Si bueno,

- Haber primeramente ayúdeme abriendo el icono del antivirus, pero antes de eso dígame el IP de su equipo para poder enviarle las actualizaciones de la fecha.
- .- Espere un momento…..haber es……
- Ahora si ya estoy enviándole solo son minutos, mientras ayúdeme con los datos que necesito…… solo usted trabaja en el equipo…….. qué tipo de información maneja…….. quien no mas está en la oficina……
- Bueno ha terminado disculpe la molestia y gracias por todo cualquier pregunta llame a soporte técnico.
- .- OK Gracias.

Anexo 7 - Tabla 1. Checklist Telefónico

INFORME	ESCUELAS	DEPARTAMENTOS O CITTES
NOMBRE	√	√
APELLIDO	√	√
DIRECCIÓN		
TELÈFONO	√	√
USUARIO	----------	----------
CORREO ELECTRÓNICO	√	√
MANEJO DE INFORMACIÓN	Sistema académico Oficios y actas Certificados. Registro de notas.	Oficios Proyectos Investigaciones Contabilidad

ANEXO 8 - TÉCNICA ROBO DE CONTRASEÑA

INTRODUCCION

Para actuar un Ingeniero social busca obtener información a distancia, pero existen muchos medios que permiten utilizar nuevos métodos como la utilización de correos electrónicos y el robo de contraseñas.

Cuando se tiene una cuenta de correo electrónico no es bueno utilizar en las contraseñas palabras que tengan significado, fechas que se relacionen con nosotros, números de ID, nombres de familiares, etc. Ya que no brindan seguridad y permiten que se las pueda obtener de forma ilícita.

Dentro de los correos electrónicos que poseen estudiantes y usuarios de la UTPL, se busco una herramienta que me permita obtener el password o clave de su cuenta de correo además de información de los usuarios. Para obtener una contraseña, y antes incluso que las de aplicaciones basadas en el uso de diccionarios y la fuerza bruta, están los propios sistemas de recuperación de contraseñas de casi todos los servicios de la red.

En nuestro análisis y búsqueda de password o claves nos basamos en utilizar un servicio de internet que me proporciones obtener la información sin levantar sospecha, esta es una página que se envía al correo y aparece como formulario de la verdadera página del correo en este caso de Hotmail, pero solo es una aplicación donde lo que hace es enviar los datos a una cuenta de correo posteriormente.

A continuación se detalla el tipo de correo que se envía:

INFORME

Primeramente se envía el correo electrónico de este servicio **botservices@hotmail.com**, especificando el motivo y los siguientes asunto **correoahackear@hotmail.com**, mensaje lost: password y enseguida se envía a su correo a donde quiere que le llegue la información **Rcpt_pwd:tucorreo@hotmail.com**: tu contraseña.

Esta cuenta es creada solo para el envío de los correos, y como el usuario no enfatiza en saber de dónde proviene, sino contestan inmediatamente.

---------- INICIO DEL MAIL ----------

PRIMERO TIENES QUE TENER UNA CUENTA EN HOTMAIL PARA COMPONER EL SIGUIENTE MAIL.

LO TIENE QUE MANDAR A: **correoahackear@hotmail.com**

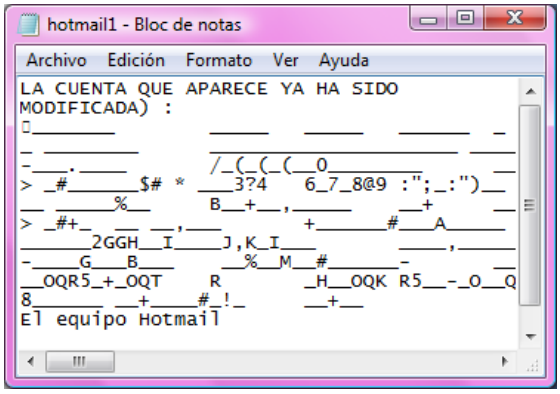
EN EL TEMA DEL MAIL TIENES QUE PONER: FORGOT PASSWORD LUEGO

TIENES QUE ESCRIBIR EL SIGUIENTE CÓDIGO:(en el lugar para escribir el mensaje)

HTPOST/ <aqui pones tu e-mail>DIF%99USER_LIST<aquí pones tu clave>
TO.LOP<aqui pones el nombre de la víctima> //%89"%90,//*mail///lostpassword///
Y FINALMENTE PON ENVIAR... ... Y LISTO EN UNAS HORAS RECIBIRÁS LA CLAVE.

Lo que se indica a continuación son correos de estudiantes que se pudo obtener el correo electrónico y su password:

Y RECIBIRÁS UN ARCHIVO COMO LA FIGURA 1.



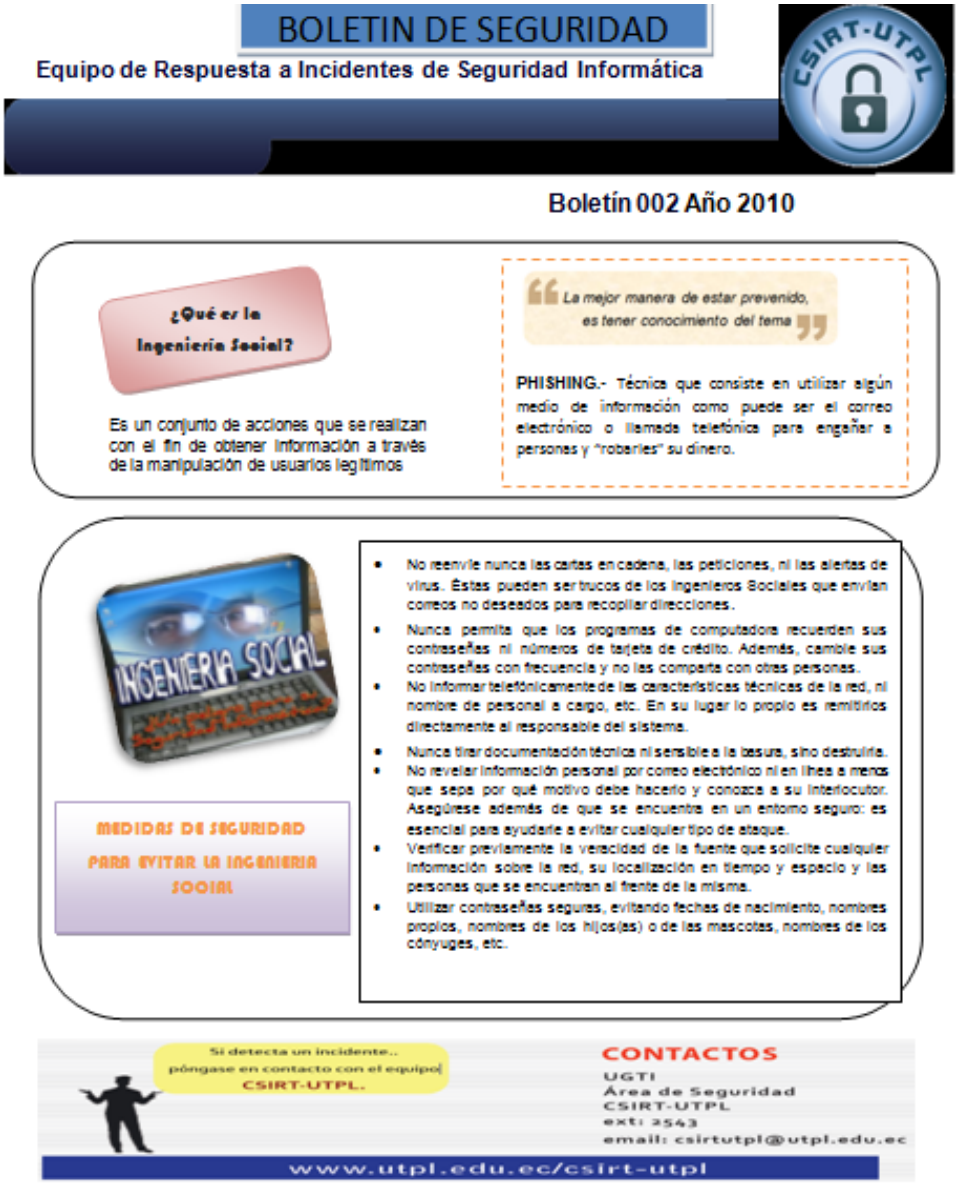
Anexo 8 - Figura 1. Mensaje Hotmail 1

1. **Estudiante:** xxxxx@hotmail.com password: XXXX
2. **Estudiante**: xxxxx @hotmail.com password: XXXX
3. **Estudiante:** xxxxx @hotmail.com password: XXXX
4. **Estudiante:** xxxxx @hotmail.com password: XXXX
5. **Administrativo:** xxxxx @hotmail.com password: XXXX
6. **Administrativo:** xxxxx @hotmail.com password: XXXX
7. **Administrativo:** xxxxx @hotmail.com password: XXXX
8. **Estudiante:** xxxxx @hotmail.com password: XXXX
9. **Estudiante:** xxxxx @hotmail.com password: XXXX
10. **Estudiante:** xxxxx @hotmail.com password XXXX
11. **Estudiante:** xxxxx @hotmail.com password: XXXX
12. **Estudiante:** xxxxx @hotmail.com password: XXXX
13. **Estudiante:** xxxxx @hotmail.com password: XXXX
14. **Estudiante:** xxxxx @hotmail.com password: XXXX
15. **Estudiante:** xxxxx @htomail.com password: XXXX
16. **Estudiante:** xxxxx @hotmail.com password: XXXX
17. **Estudiante:** xxxxx @hotmail.com password: XXXX
18. **Estudiante:** xxxxx @hotmail.com password: XXXX
19. **Estudiante:** xxxxx @hotmail.com password: XXXX
20. **Estudiante:** xxxxx @hotmail.com password: XXXX

Observaciones:

Este correo se envió a 50 administrativos y 50 estudiantes de los cuales respondieron y contestaron al correo 17 estudiantes y 3 administrativos. En muchos de los correos enviados se tomo en cuenta el lugar en donde posiblemente podían ser recibidos sin importarles de que se trataba el correo, y justamente de los administrativos solo se tuvo respuesta baja pero hay que tomar en consideración que fueron lugares propicios para poder realizar este ataque.

ANEXO 9 – BOLETIN DE SEGURIDAD



Anexo 9 - Figura 1. Boletín Informativo

ANEXO 10 – PAPER

INGENIERIA SOCIAL Y SUS NIVELES DE INCIDENCIAS EN LA UTPL

Ing. Julia Pineda
japineda@utpl.edu.ec
Ing. María Paula Espinosa
mpespinosa@utpl.edu.ec
Srta. Andrea Espinosa
asespinosa@utpl.edu.ec

RESUMEN: *A pesar de tener toda una infraestructura tecnológica de seguridad en una organización, se está expuesto a una infinidad de métodos y técnicas que permitan a un atacante obtener información confidencial sin necesidad de utilizar tecnología muy sofisticada, una de estas técnicas es la Ingeniería Social. Este tipo de técnica pretende engañar a los usuarios con el fin de obtener información confidencial, a través de la manipulación psicológica y habilidades sociales. La Ingeniería Social puede ser utilizada por personas males intencionados para llegar a obtener información, privilegios, accesos a sistemas y realizar algún tipo acto que perjudique o ponga en riesgo a una organización o sistema.*

Por lo antes mencionado, se ha realizado un análisis de las técnicas por medio de encuestas a los miembros de la Universidad para conocer los riesgos que se tienen al ser víctimas de esta y cuáles serían las posibles defensas contra la Ingeniería Social dentro de la UTPL.

PALABRAS CLAVES: Ingeniería Social, Hacker, Técnicas, Leyes.

ABSTRACT: Despite having an entire technological infrastructure of an organization's security, is exposed to a myriad of methods and techniques that allow an attacker to obtain confidential information without using very sophisticated technology, one of these techniques is Social Engineering. The technology is intended to deceive users in order to obtain confidential information, through psychological manipulation and social skills. Social engineering can be used by evil-intentioned people to get information, privileges, access to systems and perform some act which harms or endangers an organization or system.

As mentioned above, there has been an analysis of survey techniques by members of the University to understand the risks that need to be victims of this and what the possible defenses against social engineering in the UTPL

INTRODUCCIÓN

La "Ingeniería Social" aplicado al tema de la seguridad informática, es utilizada para describir una serie de procedimientos específicos que permitan ser involucradas con la manipulación de personas u objetos, que servirían para obtener información vital sobre el sistema a atacar.

Aprovechar debilidades psicológicas que son muy complejas de aprender y muy fáciles de realizar. Los ataques mediante técnicas de "Ingeniería Social" mantienen un alto grado de eficacia. En muchos de los casos, la misma está dada por falta de conocimiento o por el tiempo y la poca importancia que se le da a la seguridad.

El presente proyecto pretende realizar un estudio de la Ingeniería social y sus niveles de incidencia mediante datos estadísticos realizados, y de esta manera conocer cuáles son las técnicas que permiten vulnerar los sistemas y analizar las medidas para reducir las probabilidades de éxito. Conocer de qué manera el atacante trabaja con las nuevas amenazas y estas pueden resultar de gran ayuda para emplear Ingeniería Social.

La principal característica de la investigación es realizar un estudio de las vulnerabilidades dentro de la Universidad Técnica Particular de Loja, las políticas de seguridad propuestas y formas de protección hacia el centro universitario y finalmente dar conclusiones y recomendaciones de lo investigado.

1. Definición Ingeniería Social

Wikipedia:

Ingeniería Social es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos. Un ingeniero social usará comúnmente el teléfono o Internet para engañar a la gente y llevarla a revelar información sensible, o bien a violar las políticas de seguridad típicas. Con este método, los ingenieros sociales aprovechan la tendencia natural de la gente a confiar en su palabra, antes que aprovechar agujeros de seguridad en los sistemas informáticos. Generalmente se está de acuerdo en que "los usuarios son el eslabón débil" en seguridad; éste es el principio por el que se rige la ingeniería social. [1]

Lester:

Con el término "ingeniería social" se define el conjunto de técnicas psicológicas y habilidades sociales utilizadas de forma consciente y muchas veces premeditada para la obtención de información de terceros. [2]

2. ANÁLISIS

2.1. TÉCNICAS DE INGENIERIA SOCIAL

Existen tres técnicas de Ingeniería Social que permiten al atacante obtener información de cualquier manera y desde cualquier sitio.

Técnicas Pasivas:

- Observación
- Surf hombro

Técnicas No Presenciales:

- Recuperar la contraseña
- Ingeniería Social y Mail
- IRC u otros chats
- Teléfono o Carta y fax

Técnicas Presenciales No Agresivas:

- Buscando en la basura
- Seguimiento de personas y vehículos
- Vigilancia de Edificios
- Ingeniería social en situaciones de crisis

Métodos Agresivos:

- Suplantación de personalidad
- Chantaje o extorsión
- Presión psicológica

2.1.1. BÚSQUEDAD DE LA INFORMACION DENTRO DE LA UTPL

Para la búsqueda de información se consideró los sitios más vulnerables y quienes manejan información importante para la Universidad, además con la utilización de algunas herramientas como:

- Para la obtención de información se realizaron encuestas a empleados y estudiantes de la Universidad, las preguntas estuvieron enfocadas al tema de Ingeniería Social en general, y de esta manera saber las distintas vulnerabilidades a las que se encuentran expuestos los miembros de la UTPL.
- A través del uso de las técnicas de Ingeniería Social como: suplantación, observación, envió de mails, ataques

por teléfono, robo de contraseña; se pudo acceder a los distintos lugares de la Universidad más vulnerables para la obtención de la información que proporcionan los empleados de la Universidad.

2.1.3 TÉCNICAS DE INGENIERIA SOCIAL APLICADAS EN LA UTPL

Se han seleccionado estas técnicas de Ingeniería Social en base a los resultados obtenidos por las encuestas antes realizadas a estudiantes y personal docente de la Universidad, y a estudios realizados posteriormente para investigar qué tipo de técnicas de Ingeniería Social se puede aplicar a continuación se las describe:

- Técnica de suplantación y observación
- Técnica de envió de correo electrónico
- Técnica de teléfono
- Técnica robo de contraseña

Las formas de ataques han sido distintas ya que cada una de ellas involucra manejar el tiempo y el lugar para desarrollar, es decir analizar donde existiría menor riesgo de sospecha, y lugares más vulnerables para poder realizar los ataques.

3. MECANISMOS DE PROTECCION DE SEGURIDAD PARA EVITAR LA INGENIERIA SOCIAL

Existen mecanismos que nos pueden ayudar a disminuir ataques de ingeniería social
Concientización

1. Capacitación
- La capacitación es una herramienta fundamental para ofrecer la posibilidad de mejorar la eficiencia del trabajo en cuanto a seguridad, permitiendo a su vez que la misma se adapte a las nuevas circunstancias que se presentan tanto dentro como fuera de la Universidad. Proporciona a los empleados la oportunidad de adquirir mayores aptitudes, conocimientos y habilidades para desempeñarse con éxito.

2. Boletines
- Asegurarse de concientizar y capacitar también a los empleados nuevos y antiguos sobre las nuevas amenazas, los métodos de acceso inseguros a sus equipos y el cumplimiento de políticas y procedimientos de seguridad. Esto se lo puede realizar con la incorporación de Boletines de seguridad, por ello se ha dejado una propuesta de ello.

3. Reuniones
- Establecer reuniones y lograr que los usuarios asimilen de que manera son susceptibles ante los métodos de engaño de los Ingenieros Sociales y mostrarles con ejemplos reales (cuya repercusión haya sido muy grande) de manera que logren medir el peligro de brindar cualquier información a un extraño. De esta manera estarán mucho más preparados ante cualquier intento de manipulación.

4. Participación de Seminarios
- Hacer participes a todos los usuarios de la Universidad los seminarios que se dictan en la Universidad sobre temas de seguridad de la información y combinarla con el establecimiento de políticas bien definidas sobre pautas de comportamiento de los usuarios cuando enfrentan cualquier tipo de ataque.

4. LEYES CONTRA DELITOS INFORMATICOS EN LA UTPL

Dentro la Universidad no existen aun políticas contra los delitos informáticos, la UTPL maneja Status propios de la organización.
En el caso que hubiese algún delito informático por parte de algún miembro de la Universidad existirá una Resolución y se establecería como norma interna de acuerdo al caso presentado.
Cuando se cometiera alguna infracción o falta se regirían las leyes establecidas a Nivel de las Leyes del Estado Ecuatoriano [3].

4.1 PROPUESTAS PARA REFORMAR LA LEYES DEL ECUADOR

Durante del desarrollo y estudio hemos conocido las herramientas y organismos con los que cuenta el Ecuador para la investigación de los delitos de índole tecnológicos, así como las propuestas ofrecidas por otros organismos que permitirían el desarrollo de unidades de investigación de los delitos informáticos, además se han identificado iniciativas que permiten la adecuación y mejora del Departamento de Criminalística de la Policía Judicial del Ecuador.
Luego de analizar la realidad de los delitos informáticos en el Ecuador y exponer mecanismos y herramientas existentes para su análisis, se recomienda considerar algunos proyectos:

- Creación de un Plan de Unidad de delitos Informáticos en el Ministerio Publico.
- Colegios de Delitos Informáticos en el Ecuador y sus provincias.
- Apoyarse en las leyes de otros países para reformar las leyes del ecuador, en el ámbito de delitos informáticos.

5. RESULTADO

Como resultado del presente trabajo se obtuvo que en el tema de Ingeniería Social existan aspectos relevantes y distintas maneras de aplicar medidas:

- Desconocimiento sobre el tema de Ingeniería Social, y sus técnicas de ataque.
- El factor humano es el principal exponente clave y el más débil en cuanto a la seguridad de la información.
- Los usuarios divulgan información como claves e información sensible de la UTPL.
- Los usuarios casi abren casi ciegamente cualquier archivo adjunto recibido, concretando de esta forma el ataque.
- No existen leyes bien definidas sobre los delitos informáticos que se han incrementado últimamente.

6. CONCLUSIONES

- ✓ Mediante encuestas realizadas a los miembros de la UTPL se pudo verificar que un 70% de los miembros de la Universidad no tienen conocimiento en cuanto a la existencia de la Ingeniería Social.
- ✓ Se pueden realizar robo de información fácilmente, ya que se proporciona información sensible por distin0tos medios de la Universidad.
- ✓ Facilidad de acceso a los distintos departamentos por parte de usuarios tanto internos como externos.
- ✓ No hay lineamientos de seguridad que deben seguir los usuarios de la Universidad, para protección de la información y sus equipos de ataques: por

correo electrónico, teléfono, observación y suplantación.

- ✓ El personal de Gestión de Servicio no mantienen un sistema de identificación por lo que implica un fallo de seguridad; y que cualquier persona podría suplantar a la identidad de este personal.
- ✓ No existen un porcentaje de incidentes de Ingeniería Social en el Ecuador, constan solamente de algunos países de Sudamérica, en donde se lo toma en forma general junto con otros países.
- ✓ Existen delitos informáticos que no se especifican bien en el código penal Ecuatoriano.
- ✓ Se pueden apoyar en las leyes que se manejan sobre delitos informáticos en otros países, y que se las puede adaptar a la realidad de delitos que se han presentado en el Ecuador.

7. REFERENCIAS

[1] Wikipedia Enciclopedia Libre, Ingeniería social (seguridad informática), [En línea http://es.wikipedia.org/wiki/Ingenier%C3%ADa_social_(seguridad_inform%C3%A1tica), Citado el: 23 de Noviembre de 2009].

[2] Ingeniería Social, Teacher Lester, [http://www.scribd.com/doc/7215979/Texto-Ingenieria- Social, 18 de octubre de 2008 Citado el: 24 de Noviembre de 2009].

[3] Delitos Informáticos, Universidad Técnica Particular de Loja, Citado en: 15 de octubre 2010

GLOSARIO

1 **ANTIVIRUS.-**Programas diseñados para la detección y posible eliminación de virus informáticos.

2 **ATAQUE.-** Acción en la que alguien rompe las reglas de seguridad y preservación de la intimidad de un sistema informático.

3 **CODIGO.-**Término genérico para nombrar las instrucciones de un programa, Tenemos código fuente, legible a simple vista, que son las instrucciones escritas por el programador en un lenguaje de programación. Y código máquina ejecutable, que son las instrucciones convertidas de código fuente a instrucciones que el ordenador o computadora puede comprender.

4 **CONTRASEÑA.-**Forma de autentificación que utiliza información secreta para controlar el acceso hacia algún recurso.

5 **DELITO.-**Crimen genérico o crimen electrónico, que agobia con operaciones ilícitas realizadas por medio de Internet o que tienen como objetivo destruir y dañar ordenadores.

6 **.DOC:** Extensión de un archivo que identifica a un documento de texto. Es interpretada por cualquier procesador de textos.

7 **E-MAIL O CASILLA DE CORREO.-**Dirección de correo electrónico que utiliza una persona o empresa que le permite recibir, enviar y almacenar correos.

8 **EXPLOITS.-** Software que aprovecha alguna debilidad de un sistema operativo. Los Exploits no necesariamente son maliciosos.

8.2 .

9 **FIREWALL O CORTAFUEGO.-**Software de seguridad que impide el acceso de personas no autorizadas a una red interna desde el exterior (como puede ser Internet).

10 **HACKER.-**Experto de programación, sistemas, redes en general, Internet, computadoras y no tiene intenciones malas a diferencia de lo que se escucha comúnmente. Le gusta acceder a lugares prohibidos por diversión, alimento de ego y demostrar que para el, los sistemas más costosos son vulnerables.

11 **HOAX.-** Mensaje de correo electrónico con contenido falso que se distribuye mediante cadenas. Su principal objetivo es obtener direcciones de correo electrónico. También busca molestar a gente y saturar la red y los servidores

12 **INFORMACIÓN.-** Elemento fundamental que manejan los ordenadores en forma de datos binarios.

13 **INGENIERÍA SOCIAL.-** Técnicas y métodos utilizados para engañar a las personas y conseguir información valiéndose de su ignorancia e inocencia.

14 **INGENIERO SOCIAL.-** Persona con alta capacidad de convicción y facilidad para engañar a otras personas y lograr que le digan información confidencial que necesita. Este utilizara como herramientas un teléfono, una charla por chat o en el mejor de los casos lo hará personalmente.

15 **INTERNET.-** Conjunto de redes interconectadas que permiten la comunicación entre millones de usuarios de todo el mundo. Para el acceso a ella los usuarios necesitan tener un prestador de servicios que le provea un nombre de usuario y contraseña.

16 **KEYLOGGER.-** Programa malicioso que registra cada vez que se pulsa una tecla en el teclado y se almacenan en un archivo de texto.

17 **LINK O HIPERVÍNCULO.-** Vínculo que sirve para ir de una sección a otra, o de una página a otra, cuando se navega por Internet o al usar planillas de cálculo o archivos de texto.

18 **MALWARE O MALICIOUS SOFTWARE.-** Programa diseñado para hacer algún daño a un sistema. Puede presentarse en forma de virus, gusanos, caballos de Troya, etc.

19 **PASSWORD O CONTRASEÑA.-** En español palabra clave. Código personal y privado que fue asignado previamente a un usuario determinado. Para comenzar cualquier operación esta clave es requerida.

20 **PHISHING:** Técnica que consiste en utilizar algún medio de información como puede ser el correo electrónico o llamada telefónica para engañar a personas y "robarles" su dinero. Al parecer estos mensajes proceden de un negocio digno de confianza (un banco o compañía de crédito) que solicita "verificación" de los datos por un supuesto problema.

21 **REMAILERS.-**Es un servidor que se encarga de recibir mail, el mismo que borra su encabezado en el cual tiene información del emisor, y los dirigen al destinatario.

22 **SMS.-** (Short Message Service) Servicio de mensajería para celulares.

23 **SPAM.-** Mensaje de correo masivo con contenido publicitario no solicitado.

24 **SPAM SMS,-** Spam que se difunde por dispositivos celulares mediante la tecnología SMS (mensajes de texto cortos).

25 **SPYWARE.-** Software espía que se encarga de recopilar información de usuarios para luego enviarla al servidor de la empresa que le interesa conocer dicha información. Utilizado para conocer gustos de los usuarios para luego hacerles ofertas a medida.

26 **TRASHING.-**Consiste en rastrear en las papeleras en busca de información, contraseñas o directorios.

27 **TROYANO.-** Programa dañino, utilizado normalmente como herramienta para espiar, que suele presentarse disfrazado o incluido dentro de otro programa. Cuando este programa es ejecutado el troyano realiza la acción prevista.

28 **ULTRAVIOLETA.-** Es conocida como luz negra y sirve para el oscurecimiento de las sales que son expulsadas por los seres humanos mediante el sudor.

29 **USUARIO.-**Un usuario es un conjunto de permisos dispositivos o recursos a los cuales se tiene acceso. Un usuario puede ser tanto una persona como una máquina, un programa etc.

30 **VIRUS.-**Programa maligno que infecta un sistema o unidad física de almacenamiento y tiene la capacidad de auto-replicarse. Este necesita un portador o archivo donde incluirse para poder replicarse.

31 **VISHING.-** Evolución de phishing o también conocido como phishing telefónico, pero en esta caso se hace utilizando voz sobre IP (VoIP), telefonía móvil y telefonía terrestre.

32 **VOIP.-** (Voice over Internet Protocol) Tecnología que permite realizar llamadas telefónicas a un muy bajo costo ya que envía la voz en forma de datos a direcciones en Internet en vez de hacerlo a un teléfono fijo).