UNIVERSIDAD NACIONAL
"SANTIAGO ANTÚNEZ DE MAYOLO"

ESCUELA DE POSTGRADO

"ANÁLISIS DE LAS VULNERABILIDADES MEDIANTE EL USO DE PHISHING PARA MEJORAR LA SEGURIDAD INFORMÁTICA DE LOS EQUIPOS DE CÓMPUTO Y REDES DE LA MUNICIPALIDAD DISTRITAL DE INDEPENDENCIA"

Tesis para optar el grado de Maestro
en Ciencias e Ingeniería
Mención en Auditoria y Seguridad Informática

JOSEPH DARWIN ALVARADO TOLENTINO

Asesor: DR. EDDY JESÚS MONTAÑEZ MUÑOZ

HUARAZ –PERÚ

2017

N° de Registro: T0519

MIEMBROS DEL JURADO

Magister Carlos Antonio Reyes Pareja — Presidente

_____

Magister Alberto Martín Medina Villacorta — Secretario

_____

Doctor Eddy Jesús Montañez Muñoz — Vocal

_____

ASESOR

Doctor Eddy Jesús Montañez Muñoz

AGRADECIMIENTO

- *A mi Alma Mater, Universidad Nacional "Santiago Antúnez de Mayolo" y a la escuela de Postgrado por ser quien me acogió durante los 2 años de mi formación académica y profesional.*
- *A mis padres por su esfuerzo en brindarme la educación que tengo, agradecerles por su cuidado y apoyo, así como su motivación y guía.*
- *Al asesor, Dr. Eddy Jesús Montañez Muñoz, por sus constantes aportes y sus sabios consejos en la consecución de la tesis, también por sus constantes revisiones y oportunas correcciones de esta tesis.*
- *A los docentes de la Escuela Postgrado en especial a los de la mención en auditoria y seguridad informática, a todos y cada uno de ellos, por haberme brindado las herramientas y conocimientos necesarios para llegar hasta aquí, y finalmente a mis compañeros. Gracias por tan buenos momentos y anécdotas.*

A Dios, por darme la oportunidad de vivir y por estar conmigo en cada paso que doy, por fortalecer mi corazón e iluminar mi mente y por darme la salud y la esperanza para terminar este proyecto.

A mis queridos padres, por ser fuente de motivación e inspiración para superarme profesionalmente; por creer y confiar siempre, apoyándome en todas las decisiones que he tomado en la vida y por ser las bases que me ayudaron a llegar hasta aquí.

A mi hermano por su apoyo moral, por cada consejo puntual y oportuno que has sabido darme, por tu apoyo incondicional, por ser mi amigo, mi confidente.

ÍNDICE GENERAL

RESUMEN

El propósito fundamental de la tesis fue el análisis de las vulnerabilidades mediante el uso de phishing para mejorar la seguridad informática de los equipos de cómputo y redes de la Municipalidad Distrital de Independencia.

Investigación exploratorio, descriptivo, no experimental, la población de estudio estuvo comprendida por el personal de la Subgerencia de tecnología de información y Comunicaciones de la Municipalidad y personal Administrativo, Auxiliar de diferentes áreas, con una muestra de 20 personas, el instrumento de recolección de la información fue el cuestionario que fueron aplicadas en la Municipalidad Distrital de Independencia donde se autorizó a 20 usuarios debido a la información y funciones que manejan, se aplicaron en dos sesiones con el objetivo de no saturar de preguntas al usuario de información y de esta manera no sea tedioso debido a sus ocupaciones.Se presenta detalladamente el procesamiento y análisis de los datos utilizando pruebas de concepto para valorar el riesgo. Como discusión final del resultado de las dos categorías de riesgos analizadas, se puede observar que la organización carece de medidas de seguridad adecuadas y que le falta conciencia del tema de la seguridad a nivel organizacional.

Se concluyó que, la MDI puede contar con la mayor tecnología, con los últimos equipos del mercado y el mejor software de seguridad, pero si no se crea una conciencia real y no se educa a todos los empleados en el ámbito de seguridades informáticas no se va a mitigar el riesgo de caer en un ataque de Phishing.

PALABRAS CLAVE: Phishing, Sistemas informáticos, Riesgo, Prevención, Detección, Intercepción, Seguridad.

ABSTRACT

The main purpose of the thesis is the analysis of vulnerabilities through the use of phishing to improve the computer security of the computer equipment and networks of the Municipality of Independencia District.

The research is non-experimental and is considered an exploratory and descriptive study, since it describes what is computer security and the main risks that the lack of it is, and places the object of study in all the problematic manifested.

The processing and analysis of the data are presented in detail using proof of concept to assess the risk. The questions asked in the questionnaire were applied in the Municipality of Independencia District where 20 users were authorized due to the information and functions they handle. The questionnaires were applied in two sessions with the aim of not saturating questions with the information user and thus not be tedious due to their occupations.

As a final discussion of the result of the two categories of risks analyzed, it can be observed that the organization lacks adequate security measures and that it lacks awareness of the issue of security at the organizational level.

It was concluded that MDI can count on the highest technology, the latest equipment on the market and the best security software, but if you do not create a real conscience and do not educate all employees in the field of computer security, Will mitigate the risk of falling into a Phishing attack.

KEYWORDS: Phishing, Computer Systems, Risk, Prevention, Detection, Intercept, Security.

I. INTRODUCCIÓN

Hace algunos años atrás, las actividades bancarias, la comunicación, el correo, etc., eran de carácter físico. Cuando una persona deseaba adquirir algún artículo como por ejemplo, una camisa, un libro, una máquina, etc., debía trasladarse hasta el lugar en donde se encontraba el producto que necesitaba o deseaba comprar. De igual forma al cobrar un cheque, solicitar el saldo de una cuenta o retirar dinero, se requería que la persona se trasladara hasta el banco para gestionar estas transacciones. En conclusión, se puede decir que no podía haber transacción que se realizara si la persona no se encontraba físicamente en el lugar; en este contexto, las técnicas de ataques se puede decir que eran personales, robo y falsificación de cheques, documentos, etc.

Hoy en día debido a la evolución de las tecnologías de la información y su aplicación en los procesos operativos y de negocio de las empresas, se ha viabilizado la creación de aplicaciones de negocio, portales de comercio electrónico, correo electrónico que facilitan la realización de actividades de compra y gestión bancaria. Sin embargo, también gracias a la tecnología, las personas están más expuestas a que puedan ser víctimas de ataques más sofisticados, a través de técnicas de ataques mejor elaboradas, usando lo que actualmente se ha conceptualizado como Ingeniería Social, que no es otra cosa que saber cómo convencer a la gente de que nos entregue información confidencial, tocando su lado sensible, con el único fin de llevar a cabo un ataque mediante el cual se realizará un

fraude, robo o cualquier actividad dolosa en contra de una empresa o persona específica.

Frente a estos hechos, las empresas y las personas deben empezar a enterarse y entender los riegos y las diferentes formas en que pueden ser sorprendidas por gente inescrupulosa que cada vez más, se prepara técnicamente para cometer actos ilícitos.

Con el desarrollo de la presente tesis se pretende sintetizar las bases conceptuales en las que se basa esta forma de estafar y además hacer ciertas recomendaciones que mitiguen los riesgos a los que actualmente las empresas y las personas están expuestas, lo que será realizado por una persona que tiene los conocimientos necesarios para poder realizar políticas de seguridad que minimicen estos riesgos, quién será guiada por un profesional con la experiencia necesaria para completar el proyecto.

Tambien se llegó a identificar la realidad problemática de la Subgerencia de Tecnología de Información y las Comunicaciones de la Municipalidad Distrital de Independencia, los cuales son que no cuenta con una planeación formal, las actividades que se realizan son improvisadas con una producción que varía de mes a mes, esto no le ha permitido realizar una acción efectiva para anticiparse y prepararse a los cambios que podrían afectar los objetivos organizacionales así como establecer las bases para determinar el elemento riesgo y minimizarlo. Por lo que es evidente que el Subgerente no ha identificado el curso concreto de acción que ha de seguirse y los principios que habrán de orientarlo.

La Subgerencia de Tecnología de Información y las Comunicaciones no cuenta con un ambiente adecuado en donde deberían estar ubicados los servidores que alojan toda la información de la Municipalidad Distrital de Independencia, además hay escasez de buenos equipos informáticos.

Según lo observado en toda la infraestructura de la Municipalidad Distrital de Independencia, tanto en cableado, infraestructura y seguridad de la información se tiene deficiencia, por lo cual se plantea el análisis de las vulnerabilidades mediante el uso de phishing para mejorar la seguridad informática de los equipos de cómputo y redes de la Municipalidad Distrital de Independencia.

1.1. Objetivos

1.1.1. Objetivo general

Aplicar técnicas de Phishing para el análisis de las vulnerabilidades a fin de mejorar la seguridad informática de los equipos de cómputo y redes de la Municipalidad Distrital de Independencia.

1.1.2. Objetivos específicos

1. Aplicar técnicas de Phishing para medir la seguridad informática de los equipos de cómputo y redes de la Municipalidad Distrital de Independencia.
2. Concientizar y alertar de los riesgos que conlleva utilizar Internet y las nuevas tecnologías a los trabajadores de la Municipalidad Distrital de Independencia a fin de mejorar la seguridad informática.
3. Realizar un caso práctico de cómo se lleva a cabo un ataque de

Phishing en la Municipalidad Distrital de Independencia, para determinar medidas prácticas de prevención de dichos ataques.

4. Dar una propuesta de seguridad sobre los ataques de Phishing y su prevención a futuro.

1.2. Hipótesis

1.2.1- Hipótesis:

Con el análisis de las vulnerabilidades mediante el uso de Phishing se mejorará la seguridad informática de los equipos de cómputo y redes de la Municipalidad Distrital de Independencia.

1.2.2- Hipótesis nula:

H0: Con el análisis de las vulnerabilidades mediante el uso de Phishing no se mejorará la seguridad informática de los equipos de cómputo y redes de la Municipalidad Distrital de Independencia.

1.3. Variables

1.3.3. Definición de las variables

Variable independiente: Análisis de las vulnerabilidades mediante el uso de Phishing.

Variable dependiente: Seguridad Informática de los Equipos de Cómputo y Redes de la Municipalidad Distrital de Independencia.

1.3.3. Operacionalización de variables

Variable	Definición Conceptual	Dimensiones	Indicadores	Unidad de medida	Escala
Independiente 1. Análisis de las vulnerabilidades mediante el uso de Phishing	Es un término informático que denomina un modelo de abuso informático y que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria).	Medidas de seguridad ante ataques de Phishing.	Porcentaje de Incidencias de ataque de Phishing.	N° de Ataques	Ordinal Porcentaje
Variable	**Definición Conceptual**	**Dimensiones**	**Indicadores**	**Unidad de medida**	**Escala**
Dependiente. 2. Seguridad Informática de los Equipos de Cómputo y Redes de la Municipalidad Distrital de Independencia.	Se entiende por seguridad informática al conjunto de normas, procedimientos y herramientas, que tienen como objetivo garantizar la disponibilidad, integridad, confidencialidad y buen uso de la información que reside en un sistema de información.	Medidas de seguridad en equipos de cómputo y redes.	Nivel de Confiabilidad de la información Nivel de riesgo	N° de incidentes	Ordinal Porcentaje

1.3.4. Matriz de consistencia

<table>
<tr><th colspan="6">ANÁLISIS DE LAS VULNERABILIDADES MEDIANTE EL USO DE PHISHING PARA MEJORAR LA SEGURIDAD INFORMÁTICA DE LOS EQUIPOS DE CÓMPUTO Y REDES DE LA MUNICIPALIDAD DISTRITAL DE INDEPENDENCIA.</th></tr>
<tr><th>PROBLEMAS</th><th>OBJETIVOS</th><th>HIPÓTESIS</th><th>VARIABLES DE ESTUDIO</th><th>INDICADORES</th><th>METODOLOGÍA</th></tr>
<tr><td>GENERAL</td><td>GENERAL</td><td>GENERAL</td><td>INDEPENDIENTE</td><td>INDEPENDIENTE</td><td></td></tr>
<tr><td rowspan="3">¿En qué medida el análisis de las vulnerabilidades mediante el uso de Phishing mejorará la seguridad informática de los equipos de cómputo y redes de la Municipalidad Distrital de Independencia?</td><td>Aplicar técnicas de Phishing para el análisis de las vulnerabilidades a fin de mejorar la seguridad informática de los equipos de cómputo y redes de la Municipalidad Distrital de Independencia.</td><td rowspan="3">Hipótesis H1
Con el análisis de las vulnerabilidades mediante el uso de Phishing se mejorará la seguridad informática de los equipos de cómputo y redes de la Municipalidad Distrital de Independencia.
Hipótesis H0
Con el análisis de las vulnerabilidades mediante el uso de Phishing no se mejorará la seguridad informática de los equipos de cómputo y redes de la Municipalidad Distrital de Independencia.</td><td>Análisis de las vulnerabilidades mediante el uso de Phishing</td><td>Porcentaje de Incidencias de ataque de Phishing.</td><td rowspan="3">Tipo de estudio
Exploratorio, tecnológico.
Diseño de investigación
Descriptivo Simple.
Población y muestra:
20 trabajadores que laboran en la Municipalidad Distrital de Independencia.
Técnica de recolección de datos
Cuestionario estructurado.</td></tr>
<tr><td>ESPECIFICO</td><td>DEPENDIENTE</td><td>DEPENDIENTE</td></tr>
<tr><td>1. Aplicar técnicas de Phishing para medir la seguridad informática de los equipos de cómputo y redes de la Municipalidad Distrital de Independencia.
2. Concienciar y alertar de los riesgos que conlleva utilizar Internet y las nuevas tecnologías a los trabajadores de la Municipalidad Distrital de Independencia a fin de mejorar la seguridad informática.
3. Realizar un caso práctico de cómo se lleva a cabo un ataque de Phishing en la Municipalidad Distrital de Independencia, para determinar medidas prácticas de prevención de dichos ataques.
4. Dar una propuesta de seguridad sobre los ataques de Phishing y su prevención a futuro.</td><td>Seguridad Informática de los Equipos de Cómputo y Redes de la Municipalidad Distrital de Independencia.</td><td>Nivel de Confiabilidad de la información
Nivel de riesgo</td></tr>
</table>

II. MARCO TEÓRICO

2.1. Antecedentes

General

Diversos países se han ocupado de los temas del fraude y las estafas a través de Internet. Uno de ellos es el Convenio de Cibercriminalidad de Budapest pero además otros países han dedicado esfuerzos legislativos para castigar estas acciones.

Algunos países ya han incluido el Phishing como delito en sus legislaciones, mientras que en otros aún están trabajando en ello.

Argentina

En Argentina, el 19 de septiembre de 2011 fue presentado un proyecto para sancionar el Phishing, bajo el Nº de Expediente S-2257/11, Proyecto de Ley para tipificar el Phishing o Captación Ilegítima de Datos en el Senado de la Nación. Mediante este proyecto se busca combatir las diferentes técnicas de obtención ilegítima de información personal.

Estados Unidos

En los Estados Unidos, el senador Patrick Leahy introdujo el Ley Anti-Phishing de 2005 el 1 de marzo de 2005. Esta ley federal de anti-phishing establecía que aquellos criminales que crearan páginas web falsas o enviaran

spam a cuentas de correo electrónico con la intención de estafar a los usuarios podrían recibir una multa de hasta $250,000 USD y penas de cárcel por un término de hasta cinco años.33

Algunos estados tienen leyes que tratan las prácticas fraudulentas o engañosas o el robo de identidad y que también podría aplicarse a los delitos de phishing. Aquí se puede encontrar los estados que actualmente castigan este tipo de delitos.

A Nivel Nacional

Al revisar investigaciones en el ámbito nacional relacionas con ataques de phishing u otra investigación se encontró que según la Tesis de nombre "El estándar de consumidor razonable aplicado en los consumos fraudulentos generados por clonación" para optar el Título de Abogado presentado por PAOLA VICTORIA MEZA ALAYO nos dice:

La mayoría de personas, hoy en día, posee una tarjeta de crédito, normalmente para la compra de bienes y/o contratar servicios. Apuesto que la mayoría de nosotros al haber firmado el contrato de tarjeta de crédito no lo ha leído y es más, no sabe que tiene un deber de custodia de la misma; es decir, no sabe que al momento de hacer uso de la misma, tiene la obligación de vigilarla de manera que no vaya ser víctima de una clonación. Sin embargo, muchos factores, entre ellos la confianza que se tiene al comprar en un establecimiento, hace que nos descuidemos y que días después (cuando nos

llega el estado de cuenta de la tarjeta) nos percatemos que existen consumos que no reconocemos.

En la actualidad, las tarjetas de crédito han servido como un medio eficiente para agilizar las transacciones comerciales; sin embargo, el mismo avance tecnológico que nos trajo ventajas ha traído una serie de riesgos.

Uno de los riesgos que nos conlleva el utilizar las tarjetas de crédito son los consumos fraudulentos, que son aquellos consumos realizados por una tercera persona ajena a las partes intervinientes en el sistema de tarjetas de crédito. Al respecto, si bien existen varias formas de que se realice el consumo fraudulento solo estudiaremos la clonación de las referidas tarjetas. Es por ello, que analizaremos las resoluciones emitidas por INDECOPI sobre la materia, de manera que podamos abordar el estándar de consumidor que se necesita para enfrentar este tipo de operaciones.

A Nivel Local

Al revisar investigaciones en el ámbito local relacionas con ataques de phishing u otras no se ha encontrado ninguna investigación por lo cual esta investigación va a resultar una base para futuras investigaciones.

2.2. Bases teóricas

2.2.1. Phishing

Phishing o suplantación de identidad, Es un término informático que denomina un tipo de abuso informático y que se comete mediante el

uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria). El cibercriminal, conocido como phisher, se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo común un correo electrónico, o algún sistema de mensajería instantánea o incluso utilizando también llamadas telefónicas.[1]

Dado el creciente número de denuncias de incidentes relacionados con el phishing, se requieren métodos adicionales de protección. Se han realizado intentos con leyes que castigan la práctica y campañas para prevenir a los usuarios con la aplicación de medidas técnicas a los programas.

2.2.2. Historia del Phishing

2.2.2.1. Origen del término

El término Phishing proviene de la palabra inglesa "fishing" (pesca), haciendo alusión al intento de hacer que los usuarios "muerdan el anzuelo".[2] A quien lo practica se le llama phisher.[3] También se dice que el término Phishing es la contracción de password harvesting fishing (cosecha y pesca de contraseñas), aunque esto probablemente es un acrónimo

[1] Ed Skoudis. Phone phishing: The role of VoIP in phishing attacks. 13 de junio de 2006
[2]Suplantación o robo de identidad (phishing) - http://www.ri5.com.ar/ayudaphishing.php
[3] Stutz, Michael AOL: A Cracker's Paradise? - 29 de enero de 1998

retroactivo, dado que la escritura 'ph es comúnmente utilizada por hackers para sustituir la f, como raíz de la antigua forma de hacking telefónico conocida como phreaking.[4]

La primera mención del término Phishing data de enero de 1996. Se dio en el grupo de noticias de hackers alt.2600,[5] aunque es posible que el término ya hubiera aparecido anteriormente en la edición impresa del boletín de noticias hacker 2600 Magazine.[6] El término Phishing fue adoptado por quienes intentaban "pescar" cuentas de miembros de AOL.

2.2.2.2. Phishing en AOL

Quienes comenzaron a hacer Phishing en AOL durante los años 1990 solían obtener cuentas para usar los servicios de esa compañía a través de números de tarjetas de crédito válidos, generados utilizando algoritmos para tal efecto. Estas cuentas de acceso a AOL podían durar semanas e incluso meses. En 1995 AOL tomó medidas para prevenir este uso fraudulento de sus servicios, de modo que los

[4] "phishing, n." OED Online, March 2006, Oxford University Press. Oxford English Dictionary Online. - 9 de Agosto de 2006
[5] "Phish, v." OED Online, March 2006, Oxford University Press. Oxford English Dictionary Online. http://dictionary.oed.com/cgi/entry/30004303/ - 9 de Agosto de 2006
[6] Ollmann, Gunter. Phishing Guide: Understanding and Preventing Phishing Attacks. Technical Info. -10 de julio de 2006.

crackers recurrieron al Phishing para obtener cuentas legítimas en AOL.

El Phishing en AOL estaba estrechamente relacionado con la comunidad de warez que intercambiaba software falsificado. Un cracker se hacía pasar como un empleado de AOL y enviaba un mensaje instantáneo a una víctima potencial. Para poder engañar a la víctima de modo que diera información confidencial, [7] el mensaje podía contener textos como "verificando cuenta" o "confirmando información de factura". Una vez el usuario enviaba su contraseña, el atacante podía tener acceso a la cuenta de la víctima y utilizarla para varios propósitos criminales, incluyendo el spam. Tanto el Phishing como el warezing en AOL requerían generalmente el uso de programas escritos por crackers, como el AOLHell.

En 1997 AOL reforzó su política respecto al Phishing y los warez fueron terminantemente expulsados de los servidores de AOL. Durante ese tiempo el Phishing era tan frecuente en AOL que decidieron añadir en su sistema de mensajería instantánea, una línea de texto que indicaba: «no one working at AOL will ask for your password or billing information» («nadie que trabaje en AOL le pedirá a usted su contraseña o

[7] AOL: A Cracker's Paradise? Michael Stutz. Wired News. 29 de enero de 1998.

información de facturación»). Simultáneamente AOL desarrolló un sistema que desactivaba de forma automática una cuenta involucrada en Phishing, normalmente antes de que la víctima pudiera responder. Los phishers se trasladaron de forma temporal al sistema de mensajería instantáneo de AOL (AIM), debido a que no podían ser expulsados del servidor de AIM. El cierre obligado de la escena de warez en AOL causó que muchos phishers dejaran el servicio, y en consecuencia la práctica.[8]

2.2.2.3. Intentos recientes de Phishing

Los intentos más recientes de Phishing han tomado como objetivo a clientes de bancos y servicios de pago en línea. Aunque el ejemplo que se muestra en la primera imagen es enviado por phishers de forma indiscriminada con la esperanza de encontrar a un cliente de dicho banco o servicio, estudios recientes muestran que los phishers en un principio son capaces de establecer con qué banco una posible víctima tiene relación, y de ese modo enviar un correo electrónico, falseado apropiadamente, a la posible víctima.[9] En términos generales, esta variante hacia objetivos específicos en el Phishing se ha denominado spear Phishing (literalmente

[8]History of AOL Warez. 28 de septiembre de 2006.
[9]Phishing for Clues, Indiana University Bloomington, 15 de septiembre de 2005 (en inglés)

pesca con arpón). Los sitios de Internet con fines sociales también se han convertido en objetivos para los phishers, dado que mucha de la información provista en estos sitios puede ser utilizada en el robo de identidad. [10] Algunos experimentos han otorgado una tasa de éxito de un 90% en ataques Phishing en redes sociales.[11] A finales de 2006 un gusano informático se apropió de algunas páginas del sitio web MySpace logrando redireccionar los enlaces de modo que apuntaran a una página web diseñada para robar información de ingreso de los usuarios.[12]

2.2.3. Técnicas de Phishing

La mayoría de los métodos de Phishing utilizan la manipulación en el diseño del correo electrónico para lograr que un enlace parezca una ruta legítima de la organización por la cual se hace pasar el impostor. URLs manipuladas, o el uso de subdominios, son trucos comúnmente usados por phishers; por ejemplo en esta URL: http://www.nombredetubanco.com/ejemplo, en la cual el texto mostrado en la pantalla no corresponde con la dirección real a la cual conduce. Otro ejemplo para disfrazar enlaces es el de utilizar direcciones que contengan el carácter arroba: @, para posteriormente

[10] [http://www.pcworld.com/resource/article/0, aid, 125956, pg, 1, RSS, RSS, 00.asp/ Phishing Scam Takes Aim at MySpace.com. Jeremy Kirk. IDG Network. 2 de junio de 2006 (en inglés)
[11] Tom Jagatic and Nathan Johnson and Markus Jakobsson and Filippo Menczer. Social Phishing. A publicarse en Communications of the ACM. 3 de junio del 2006. (en inglés)
[12] Malicious Website / Malicious Code: MySpace XSS QuickTime Worm. Websense Security Labs. 5 de diciembre de 2006.

preguntar el nombre de usuario y contraseña (contrario a los estándares). [13] Por ejemplo, el enlace: http://www.google.com@members.tripod.com/ puede engañar a un observador casual y hacerlo creer que el enlace va a abrir en la página de www.google.com, cuando realmente el enlace envía al navegador a la página de members.tripod.com (y al intentar entrar con el nombre de usuario de www.google.com, si no existe tal usuario, la página abrirá normalmente). Este método ha sido erradicado desde entonces en los navegadores de Mozilla[14] e Internet Explorer.[15]

Otros intentos de Phishing utilizan comandos en JavaScript para alterar la barra de direcciones. Esto se hace poniendo una imagen de la URL de la entidad legítima sobre la barra de direcciones, o cerrando la barra de direcciones original y abriendo una nueva que contiene la URL ilegítima.

En otro método popular de Phishing, el atacante utiliza contra la víctima el propio código de programa del banco o servicio por el cual se hace pasar. Este tipo de ataque resulta particularmente problemático, ya que dirige al usuario a iniciar sesión en la propia página del banco o servicio, donde la URL y los certificados de

[13] Berners-Lee, Tim. Uniform Resource Locators, IETF Network Working Group, 28 de enero de 2006
[14] Fisher, Darin. Warn when HTTP URL auth information isn't necessary or when it's provided. Bugzilla. 28 de Agosto de 2005
[15] Microsoft. A security update is available that modifies the default behavior of Internet Explorer for handling user information in HTTP and in HTTPS URLs Microsoft Knowledgebase Database. 28 de Agosto de 2005

seguridad parecen correctos. En este método de ataque (conocido como Cross Site Scripting) los usuarios reciben un mensaje diciendo que tienen que "verificar" sus cuentas, seguido por un enlace que parece la página web auténtica; en realidad, el enlace está modificado para realizar este ataque, además es muy difícil de detectar si no se tienen los conocimientos necesarios.

Otro problema con las URL es el relacionado con el manejo de Nombre de dominio internacionalizado (IDN) en los navegadores, puesto que puede ser que direcciones que resulten idénticas a la vista puedan conducir a diferentes sitios (por ejemplo dominio.com se ve similar a dominio.com, aunque en el segundo las letras "o" hayan sido reemplazadas por la correspondiente letra griega ómicron, "o"). Al usar esta técnica es posible dirigir a los usuarios a páginas web con malas intenciones. A pesar de la publicidad que se ha dado acerca de este defecto, conocido como IDN spoofing[16] o ataques homógrafos,[17] ningún ataque conocido de Phishing lo ha utilizado.

2.2.4. Lavado de dinero producto del Phishing

Actualmente empresas ficticias intentan reclutar teletrabajadores por medio de correos electrónicos, chats, irc y otros medios, ofreciéndoles no sólo trabajar desde casa sino también otros jugosos beneficios.

[16] Evgeniy Gabrilovich and Alex Gontmakher. The Homograph Attack. Communications of the ACM 45(2):128. febrero del 2002
[17] Johanson, Eric. The State of Homograph Attacks Rev1.1. 'The Shmoo Group. 11 de Agosto de 2005.

Aquellas personas que aceptan la oferta se convierten automáticamente en víctimas que incurren en un grave delito sin saberlo: el blanqueo de dinero obtenido a través del acto fraudulento de Phishing.

Para que una persona pueda darse de alta con esta clase de «empresas» debe rellenar un formulario en el cual indicará, entre otros datos, su número de cuenta bancaria. Esto tiene la finalidad de ingresar en la cuenta del trabajador-víctima el dinero procedente de estafas bancarias realizadas por el método de Phishing. Una vez contratada, la víctima se convierte automáticamente en lo que se conoce vulgarmente como mulero.

Con cada acto fraudulento de Phishing la víctima recibe el cuantioso ingreso en su cuenta bancaria y la empresa le notifica del hecho. Una vez recibido este ingreso, la víctima se quedará un porcentaje del dinero total, pudiendo rondar el 10%-20%, como comisión de trabajo y el resto lo reenviará a través de sistemas de envío de dinero a cuentas indicadas por la seudo-empresa.

Dado el desconocimiento de la víctima (muchas veces motivado por la necesidad económica) ésta se ve involucrada en un acto de estafa importante, pudiendo ser requerido por la justicia previa denuncia de los bancos. Estas denuncias se suelen resolver con la imposición de devolver todo el dinero sustraído a la víctima, obviando que este únicamente recibió una comisión.

2.2.5. Fases

En la primera fase, la red de estafadores se nutre de usuarios de chat, foros o correos electrónicos, a través de mensajes de ofertas de empleo con una gran rentabilidad o disposición de dinero (Hoax o Scam). En el caso de que caigan en la trampa, los presuntos intermediarios de la estafa, deben rellenar determinados campos, tales como: Datos personales y número de cuenta bancaria.

Se comete el Phishing, ya sea el envío global de millones de correos electrónicos bajo la apariencia de entidades bancarias, solicitando las claves de la cuenta bancaria (Phishing) o con ataques específicos.

El tercer paso consiste en que los estafadores comienzan a retirar sumas importantes de dinero, las cuales son transmitidas a las cuentas de los intermediarios (muleros).

Los intermediarios realizan el traspaso a las cuentas de los estafadores, llevándose éstos las cantidades de dinero y aquéllos —los intermediarios— el porcentaje de la comisión.

2.2.6. Daños causados por el Phishing

Ejemplo de una gráfica que muestra el incremento en los reportes de Phishing desde octubre de 2004 hasta junio de 2005.

Los daños causados por el Phishing oscilan entre la pérdida del acceso al correo electrónico a pérdidas económicas sustanciales. Este tipo de

robo de identidad se está haciendo cada vez más popular por la facilidad con que personas confiadas normalmente revelan información personal a los phishers, incluyendo números de tarjetas de crédito y números de seguridad social. Una vez esta información es adquirida, los phishers pueden usar datos personales para crear cuentas falsas utilizando el nombre de la víctima, gastar el crédito de la víctima, o incluso impedir a las víctimas acceder a sus propias cuentas.

Se estima que entre mayo de 2004 y mayo de 2005, aproximadamente 1,2 millones de usuarios de computadoras en los Estados Unidos tuvieron pérdidas a causa del Phishing, lo que suma a aproximadamente $929 millones de dólares estadounidenses.[18] Los negocios en los Estados Unidos perdieron cerca de 2000 millones de dólares al año mientras sus clientes eran víctimas.[19]

El Reino Unido también sufrió el alto incremento en la práctica del Phishing. En marzo del 2005, la cantidad de dinero reportado que perdió el Reino Unido a causa de esta práctica fue de aproximadamente £12 millones de libras esterlinas.[20]

[18] Kerstein, Paul: "How Can We Stop Phishing and Pharming Scams?" CSO, 19 de Julio de 2005.
[19]Kerstein, Paul (19 de julio de 2005). How Can We Stop Phishing and Pharming Scams? CSO.
[20] Richardson, Tim: "Brits fall prey to phishing", The Register, 3 de mayo de, 2005.

2.2.7. Anti-Phishing

Existen varias técnicas diferentes para combatir el Phishing, incluyendo la legislación y la creación de tecnologías específicas que tienen como objetivo evitarlo.

2.2.7.1. Respuestas organizativas

Una estrategia para combatir el Phishing adoptada por algunas empresas es la de entrenar a los empleados de modo que puedan reconocer posibles ataques. Una nueva táctica de Phishing donde se envían correos electrónicos de tipo Phishing a una compañía determinada, conocido como spear Phishing, ha motivado al entrenamiento de usuarios en varias localidades, incluyendo la Academia Militar de West Point en los Estados Unidos. En un experimento realizado en junio del 2004 con spear Phishing, el 80% de los 500 cadetes de West Point a los que se les envió un correo electrónico falso fueron engañados y procedieron a dar información personal.[21]

Un usuario al que se le contacta mediante un mensaje electrónico y se le hace mención sobre la necesidad de "verificar" una cuenta electrónica puede o bien contactar con

[21] Bank, David: "'Spear Phishing' Tests Educate People About Online Scams", The Wall Street Journal, 17 de Agosto de 2005.

la compañía que supuestamente le envía el mensaje, o puede escribir la dirección web de un sitio web seguro en la barra de direcciones de su navegador para evitar usar el enlace que aparece en el mensaje sospechoso de Phishing. Muchas compañías, incluyendo eBay y PayPal, siempre se dirigen a sus clientes por su nombre de usuario en los correos electrónicos, de manera que si un correo electrónico se dirige al usuario de una manera genérica como («Querido miembro de eBay») es probable que se trate de un intento de Phishing.

2.2.7.2. Respuestas técnicas

Alerta del navegador Firefox antes de acceder a páginas sospechosas de Phishing.

Hay varios programas informáticos anti-Phishing disponibles. La mayoría de estos programas trabajan identificando contenidos Phishing en sitios web y correos electrónicos; algunos software anti-Phishing pueden por ejemplo, integrarse con los navegadores web y clientes de correo electrónico como una barra de herramientas que muestra el dominio real del sitio visitado. Los filtros de spam también ayudan a proteger a los usuarios de los phishers, ya que reducen el número de correos electrónicos relacionados con el Phishing recibidos por el usuario.

Muchas organizaciones han introducido la característica denominada «pregunta secreta», en la que se pregunta información que sólo debe ser conocida por el usuario y la organización. Las páginas de Internet también han añadido herramientas de verificación que permite a los usuarios ver imágenes secretas que los usuarios seleccionan por adelantado; sí estas imágenes no aparecen, entonces el sitio no es legítimo.[22] Estas y otras formas de autentificación mutua continúan siendo susceptibles de ataques, como el sufrido por el banco escandinavo Nordea a finales de 2005.[23]

Muchas compañías ofrecen a bancos y otras entidades que sufren de ataques de Phishing, servicios de monitoreo continuos, analizando y utilizando medios legales para cerrar páginas con contenido Phishing. También han surgido soluciones que utilizan el teléfono móvil[24] (Smartphone) como un segundo canal de verificación y autorización de transacciones bancarias

El [www.apwg.org/ Anti-Phishing Working Group], industria y asociación que aplica la ley contra las prácticas de Phishing, ha sugerido que las técnicas convencionales de Phishing podrían ser obsoletas en un futuro a medida que la

[22] "Security: Bank to Require More Than Passwords," CNN, July 14, 2005.
[23] Phishers target Nordea's one-time password system. Finextra. 12/10/2005.
[24]"Verificación y autorización de transacciones con el Smartphone", SafeSigner.

gente se oriente sobre los métodos de ingeniería social utilizadas por los phishers.[25] Ellos suponen que en un futuro cercano, el pharming y otros usos de malware se van a convertir en herramientas más comunes para el robo de información.

2.2.7.3. Respuestas legislativas y judiciales

El 26 de enero de 2004, la FTC (Federal Trade Commission, la Comisión Federal de Comercio) de Estados Unidos llevó a juicio el primer caso contra un phisher sospechoso. El acusado, un adolescente de California, supuestamente creó y utilizó una página web con un diseño que aparentaba ser la página de América Online para poder robar números de tarjetas de crédito.[26]

Tanto Europa como Brasil siguieron la práctica de los Estados Unidos, rastreando y arrestando a presuntos phishers. A finales de marzo de 2005, un hombre estonio de 24 años fue arrestado utilizando una backdoor, a partir de que las víctimas visitaron su sitio web falso, en el que incluía un keylogger que le permitía monitorear lo que los usuarios tecleaban.[27] Del mismo modo, las autoridades arrestaron al

[25] Kawamoto, Dawn: "Faced with a rise in so-called pharming and crimeware attacks, the Anti-Phishing Working Group will expand its charter to include these emerging threats.", ZDNet India, 4 de Agosto de 2005.
[26] Legon, Jeordan: "'Phishing' scams reel in your identity", CNN, 26 de enero de 2004.
[27] Leyden, John: "Trojan phishing suspect hauled in", The Register, 4 de Abril de 2005.

denominado phisher King pin, Valdir Paulo de Almeida, líder de una de las más grandes redes de Phishing que en dos años había robado entre $18 a $37 millones de dólares estadounidenses.[28] En junio del 2005 las autoridades del Reino Unido arrestaron a dos hombres por la práctica del Phishing, [29] en un caso conectado a la denominada «Operation Firewall» del Servicio Secreto de los Estados Unidos, que buscaba sitios web notorios que practicaban el Phishing.[30]

La compañía Microsoft también se ha unido al esfuerzo de combatir el Phishing. El 31 de marzo del 2005, Microsoft llevó a la Corte del Distrito de Washington 117 pleitos federales. En algunos de ellos se acusó al denominado phisher "John Doe" por utilizar varios métodos para obtener contraseñas e información confidencial. Microsoft espera desenmascarar con estos casos a varios operadores de Phishing de gran envergadura. En marzo del 2005 también se consideró la asociación entre Microsoft y el gobierno de Australia para educar sobre mejoras a la ley que permitirían

[28] Leyden, John: "Brazilian cops net 'phishing kingpin'", The Register, 21 de marzo de 2005.
[29] "UK Phishers Caught, Packed Away," eWEEK, junio 27 de 2005.
[30] Nineteen Individuals Indicted in Internet 'Carding' Conspiracy. 20 de noviembre del 2005

combatir varios crímenes cibernéticos, incluyendo el Phishing.[31]

2.2.8. El Phishing como delito

2.2.8.1. General

Diversos países se han ocupado de los temas del fraude y las estafas a través de Internet. Uno de ellos es el Convenio de Cibercriminalidad de Budapest pero además otros países han dedicado esfuerzos legislativos para castigar estas acciones.

Algunos países ya han incluido el Phishing como delito en sus legislaciones, mientras que en otros aún están trabajando en ello.

2.2.8.2. Phishing en Argentina

En Argentina, el 19 de septiembre de 2011 fue presentado un proyecto para sancionar el Phishing [32], bajo el Nº de Expediente S-2257/11, Proyecto de Ley para tipificar el Phishing o Captación Ilegítima de Datos en el Senado de la Nación. Mediante este proyecto se busca combatir las diferentes técnicas de obtención ilegítima de información personal.

[31] Microsoft Partners with Australian Law Enforcement Agencies to Combat Cyber Crime. 24 de agosto del 2005.
[32]Borghello Cristian, Temperini Marcelo Cruzada por la Identidad Digital Marzo 2012.

2.2.8.3. Phishing en Estados Unidos

En los Estados Unidos, el senador Patrick Leahy introdujo el Ley Anti-Phishing de 2005 el 1 de marzo de 2005. Esta ley federal de anti-Phishing establecía que aquellos criminales que crearan páginas web falsas o enviaran spam a cuentas de correo electrónico con la intención de estafar a los usuarios podrían recibir una multa de hasta $250,000 USD y penas de cárcel por un término de hasta cinco años.[33]

Algunos estados tienen leyes que tratan las prácticas fraudulentas o engañosas o el robo de identidad y que también podría aplicarse a los delitos de Phishing. Aquí se puede encontrar los estados que actualmente castigan este tipo de delitos.

2.2.9. Seguridad informática

2.2.9.1. Definición:

La seguridad informática, es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta (incluyendo la información contenida). Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la

[33]Borghello Cristian, Temperini Marcelo Cruzada por la Identidad Digital Marzo 2012.

información [34] . La seguridad informática comprende software, bases de datos, metadatos, archivos y todo lo que la organización valore (activo) y signifique un riesgo si ésta llega a manos de otras personas. Este tipo de información se conoce como información privilegiada o confidencial.

El concepto de seguridad de la información no debe ser confundido con el de seguridad informática, ya que este último sólo se encarga de la seguridad en el medio informático, pero la información puede encontrarse en diferentes medios o formas, y no solo en medios informáticos.

La seguridad informática es la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información seguro y confiable.

2.2.9.2. Análisis de riesgos:

El activo más importante que se posee es la información y, por lo tanto, deben existir técnicas que la aseguren, más allá de la seguridad física que se establezca sobre los equipos en los cuales se almacena. Estas técnicas las brinda la seguridad

[34] Código de Practica para la administracion de la Seguridad de la Información. IDAM, Instituto Argentino de Normalización (2002) - ISO/IEC 17799:2005

lógica que consiste en la aplicación de barreras y procedimientos que resguardan el acceso a los datos y sólo permiten acceder a ellos a las personas autorizadas para hacerlo.

Existe un viejo dicho en la seguridad informática que dicta: "lo que no está permitido debe estar prohibido" y ésta debe ser la meta perseguida.

Los medios para conseguirlo son:

a) Restringir el acceso (de personas de la organización y de las que no lo son) a los programas y archivos.
b) Asegurar que los operadores puedan trabajar pero que no puedan modificar los programas ni los archivos que no correspondan (sin una supervisión minuciosa).
c) Asegurar que se utilicen los datos, archivos y programas correctos en/y/por el procedimiento elegido.
d) Asegurar que la información transmitida sea la misma que reciba el destinatario al cual se ha enviado y que no le llegue a otro.
e) Asegurar que existan sistemas y pasos de emergencia alternativos de transmisión entre diferentes puntos.
f) Organizar a cada uno de los empleados por jerarquía informática, con claves distintas y permisos bien

establecidos, en todos y cada uno de los sistemas o aplicaciones empleadas.

g) Actualizar constantemente las contraseñas de accesos a los sistemas de cómputo.

2.2.9.3. Elementos de un análisis de riesgo

Cuando se pretende diseñar una técnica para implementar un análisis de riesgo informático se pueden tomar los siguientes puntos como referencia a seguir:

- Planes para reducir los riesgos.

2.2.9.3.1. Análisis de impacto al negocio

El reto es asignar estratégicamente los recursos para cada equipo de seguridad y bienes que intervengan, basándose en el impacto potencial para el negocio, respecto a los diversos incidentes que se deben resolver. Para determinar el establecimiento de prioridades, el sistema de gestión de incidentes necesita saber el valor de los sistemas de información que pueden ser potencialmente afectados por incidentes de seguridad. Esto puede implicar que alguien dentro de la organización asigne un valor monetario a cada equipo y un archivo en la red o asignar un

valor relativo a cada sistema y la información sobre ella. Dentro de los Valores para el sistema se pueden distinguir: Confidencialidad de la información, la Integridad (aplicaciones e información) y finalmente la Disponibilidad del sistema. Cada uno de estos valores es un sistema independiente del negocio, supongamos el siguiente ejemplo, un servidor Web público pueden poseer los requisitos de confidencialidad de baja (ya que toda la información es pública), pero de alta disponibilidad y los requisitos de integridad. En contraste, un sistema de planificación de recursos empresariales (ERP), sistema puede poseer alto puntaje en los tres variables. Los incidentes individuales pueden variar ampliamente en términos de alcance e importancia.

2.2.9.3.2. Puesta en marcha de una política de seguridad

Actualmente las legislaciones nacionales de los Estados, obligan a las empresas, instituciones públicas a implantar una política de seguridad. Ej.: En España la Ley Orgánica de Protección de Datos

o también llamada LOPD y su normativa de desarrollo.

Generalmente se ocupa exclusivamente a asegurar los derechos de acceso a los datos y recursos con las herramientas de control y mecanismos de identificación. Estos mecanismos permiten saber que los operadores tienen sólo los permisos que se les dio.

La seguridad informática debe ser estudiada para que no impida el trabajo de los operadores en lo que les es necesario y que puedan utilizar el sistema informático con toda confianza. Por eso en lo referente a elaborar una política de seguridad, conviene:

- Elaborar reglas y procedimientos para cada servicio de la organización.
- Definir las acciones a emprender y elegir las personas a contactar en caso de detectar una posible intrusión
- Sensibilizar a los operadores con los problemas ligados con la seguridad de los sistemas informáticos.

Los derechos de acceso de los operadores deben ser definidos por los responsables jerárquicos y no por los administradores informáticos, los cuales tienen que conseguir que los recursos y derechos de acceso sean coherentes con la política de seguridad definida. Además, como el administrador suele ser el único en conocer perfectamente el sistema, tiene que derivar a la directiva cualquier problema e información relevante sobre la seguridad, y eventualmente aconsejar estrategias a poner en marcha, así como ser el punto de entrada de la comunicación a los trabajadores sobre problemas y recomendaciones en término de seguridad informática.

2.2.9.3.3. Técnicas para asegurar el sistema

- Codificar la información: Criptología, Criptografía y Criptociencia, contraseñas difíciles de averiguar a partir de datos personales del individuo.
- Vigilancia de red. Zona desmilitarizada
- Tecnologías repelentes o protectoras: cortafuegos, sistema de detección de intrusos - antispyware, antivirus, llaves para

protección de software, etc. Mantener los sistemas de información con las actualizaciones que más impacten en la seguridad.

- Sistema de respaldo remoto. Servicio de backup remoto.

2.2.9.3.4. Respaldo de información

La información constituye el activo más importante de las empresas, pudiendo verse afectada por muchos factores tales como robos, incendios, fallas de disco, virus u otros. Desde el punto de vista de la empresa, uno de los problemas más importantes que debe resolver es la protección permanente de su información crítica.

La medida más eficiente para la protección de los datos es determinar una buena política de copias de seguridad o backups: Este debe incluir copias de seguridad completa (los datos son almacenados en su totalidad la primera vez) y copias de seguridad incrementales (sólo se copian los ficheros creados o modificados desde el último backup). Es vital para las empresas elaborar un plan de backup en función del volumen de

información generada y la cantidad de equipos críticos.

Un buen sistema de respaldo debe contar con ciertas características indispensables:

- **Continuo:** El respaldo de datos debe ser completamente automático y continuo. Debe funcionar de forma transparente, sin intervenir en las tareas que se encuentra realizando el usuario.
- **Seguro:** Muchos software de respaldo incluyen cifrado de datos (128-448 bits), lo cual debe ser hecho localmente en el equipo antes del envío de la información.
- **Remoto:** Los datos deben quedar alojados en dependencias alejadas de la empresa.
- **Mantención de versiones anteriores de los datos:** Se debe contar con un sistema que permita la recuperación de versiones diarias, semanales y mensuales de los datos.

Hoy en día los sistemas de respaldo de información online (Servicio de backup remoto) están ganando terreno en las empresas y organismos gubernamentales. La mayoría de los

sistemas modernos de respaldo de información online cuentan con las máximas medidas de seguridad y disponibilidad de datos. Estos sistemas permiten a las empresas crecer en volumen de información sin tener que estar preocupados de aumentar su dotación física de servidores y sistemas de almacenamiento.

2.2.9.3.5. Consideraciones de software

Tener instalado en la máquina únicamente el software necesario reduce riesgos. Así mismo tener controlado el software asegura la calidad de la procedencia del mismo (el software obtenido de forma ilegal o sin garantías aumenta los riesgos). En todo caso un inventario de software proporciona un método correcto de asegurar la reinstalación en caso de desastre. El software con métodos de instalación rápidos facilita también la reinstalación en caso de contingencia.

Existe un software que es conocido por la cantidad de agujeros de seguridad que introduce. Se pueden buscar alternativas que proporcionen iguales funcionalidades pero permitiendo una seguridad extra.

2.2.9.3.6. Consideraciones de una red

Los puntos de entrada en la red son generalmente el correo, las páginas web y la entrada de ficheros desde discos, o de ordenadores ajenos, como portátiles.[35]

Mantener al máximo el número de recursos de red sólo en modo lectura, impide que ordenadores infectados propaguen virus. En el mismo sentido se pueden reducir los permisos de los usuarios al mínimo.

Se pueden centralizar los datos de forma que detectores de virus en modo batch puedan trabajar durante el tiempo inactivo de las máquinas.

Controlar y monitorizar el acceso a Internet puede detectar, en fases de recuperación, cómo se ha introducido el virus.

[35] Fundamentos de Seguridad de Redes, Eric Maiwald (2004) – McGraw Hill, Segunda Edición

2.2.10. Transmisión de datos

2.2.10.1. Definición:

Transmisión de datos, transmisión digital o comunicaciones digitales[36] es la transferencia física de datos (un flujo digital de bits) por un canal de comunicación punto a punto o punto a multipunto. Ejemplos de estos canales son cables de par trenzado, fibra óptica, los canales de comunicación inalámbrica y medios de almacenamiento. Los datos se representan como una señal electromagnética, una señal de tensión eléctrica, ondas radioeléctricas, microondas o infrarrojos.

2.2.10.2. Formas de transmisión de datos entre dispositivos electrónicos:

a) **Transmisión analógica:** Estas señales se caracterizan por el continuo cambio de amplitud de la señal. En ingeniería de control de procesos la señal oscila entre 4 y 20 mA, y es transmitida en forma puramente analógica. En una señal analógica el contenido de información es muy restringido; tan solo el valor de la corriente y la presencia o no de esta puede ser determinado.

[36] Prácticas de Seguridad en Sistemas Conectados a Internet, Juan Manuel da Costa Palacios (2003) – LibrosEnRed

b) **Transmisión digital:** Estas señales no cambian continuamente, sino que es transmitida en paquetes discretos. No es tampoco inmediatamente interpretada, sino que debe ser primero decodificada por el receptor. El método de transmisión también es otro: como pulsos eléctricos que varían entre dos niveles distintos de voltaje. En lo que respecta a la ingeniería de procesos, no existe limitación en cuanto al contenido de la señal y cualquier información adicional.

2.2.11. Diagnostico

Lo principal de esta sección es diagnosticar desde la perspectiva de los riesgos a que está expuesta la información, las medidas adecuadas para que los usuarios resguarden sus datos y de los riesgos en los que la Municipalidad Distrital de Independencia como entidad ha recibido a través de los peligros que nos envuelven en la actualidad.

2.2.11.1. Diagnostico a la Municipalidad Distrital de Independencia

Para estar en posibilidades de emitir una opinión acerca del estado de una entidad, es necesario efectuar un diagnóstico, que debe hacerse con las herramientas e instrumentos idóneos para cada situación, en este caso la determinación de las condiciones de la organización respecto a la problemática

señalada, como es la carencia de seguridad informática, se efectuó con varias herramientas y en diferentes momentos como son: la aplicación de un FODA, un cuestionario, y el análisis de posibles escenarios peligrosos para la Municipalidad Distrital de Independencia.

Gráfico Nº 2.1 – Diseño de la Matriz FODA

Fuente: http://www.gestiopolis.com/analisis-foda-herramienta-estrategica-de-las-organizaciones/

2.2.11.1.1. FODA

El análisis FODA implica evaluar las fortalezas, debilidades, oportunidades y amenazas de una organización y llegar a conclusiones acerca de la manera de desplegar mejor sus recursos en vista de situación interna, externa, y cómo desarrollar

su futura base de recursos. En un diagnóstico organizacional es indispensable llevar a cabo el su análisis de su situación por medio de la preparación del terreno para ajustar la estrategia, tanto las circunstancias de su ambiente externo como con sus recursos internos y sus capacidades. En el uso de esta investigación se realizó con el fin de obtener mayores datos que permitieron vislumbrar elementos importantes, a continuación se presenta el esquema del mismo.

Tabla Nº 2.1. ANÁLISIS FODA. (Fortalezas, Oportunidades, Debilidades, Amenazas) de la Municipalidad Distrital de Independencia.

Ambiente Interno	**Ambiente Externo**
Fortalezas	**Oportunidades**
• Se tiene interés por el desarrollo de los servicios y soluciones de tecnología de información. • Vanguardia en control administrativo en recursos de comunicaciones.	• Contar con una solución administrativa de calidad. • Software amigable. • Contar con entornos de seguridad informática.
Debilidades	**Amenazas**
• Los ejecutivos y empleados desconocen las medidas de prevención. • No se contempla la seguridad informática como núcleo de la institución. • Desconocen cuáles son los resultados de los controles informáticos. • Poco cuidado al elegir el lugar para guardar passwords.	• Perú se encuentra entre uno de los países en recibir más ataques cibernéticos, por lo tanto el entorno externo es amenazante. • Falta de una protección eficaz. • Los delitos más comunes son el espionaje corporativo. • Las empresas consideran poco probable ser víctimas de la delincuencia informática, y no tienen la seguridad constante. • La ingeniería social tiene un alto número de incidencia.

2.2.11.1.2. Resultados del análisis FODA en la Municipalidad Distrital de Independencia.

La situación que se percibió en la institución al iniciar la investigación y a través del diagnóstico de su situación interna y externa es la siguiente:

FORTALEZAS

Las fortalezas que tiene la Municipalidad Distrital de Independencia son:

- La Municipalidad Distrital de Independencia es una institución pública dedicada a representar al vecindario y promover la adecuada prestación de los servicios públicos a fin de fomentar el bienestar de sus vecinos.
- Independencia es un distrito ordenado y saludable, orientado al turismo nacional e internacional, con circuitos turísticos, promoviendo los recursos naturales y arqueológicos con una educación para la protección; cuenta con una diversidad de zonas urbanas y rurales seguras y dotadas de los servicios básicos y con accesibilidad

vial, impulsando núcleos empresariales de producción, comercio y servicios educativos, transporte automotriz y servicios médicos de la región. Con ciudadanos emprendedores y conscientes de sus deberes y derechos y líderes con visión estratégica.

- Tiene interés por mejorar y permanecer en la punta del avance tecnológico.

OPORTUNIDADES

Las oportunidades que cuenta la Municipalidad Distrital de Independencia son:

- El crecimiento tecnológico puede ser de gran aprovechamiento si se cuenta con el personal idóneo para el uso y Operacionalización de la información.
- El servicio de administración que tiene le ha permitido mantener a la población y desarrollar una trayectoria satisfactoria a sus usuarios.

DEBILIDADES

Por otro lado en su ámbito interno las condiciones prevalecientes que presentan conflicto en la entidad son las siguientes:

- Los ejecutivos y empleados desconocen las medidas de prevención a posibles ataques, por tal motivo, la institución está en plena desventaja ya que se encuentra con una difusión deficiente ante la cultura de seguridad informática.
- Se han hecho intentos por establecer controles en la protección de la información pero no se les ha dado seguimiento por lo que desconocen si esos intentos han resultados positivos.
- No se contempla la seguridad informática como núcleo de la institución.
- La gente que labora en las Municipalidad Distrital de Independencia tiene poco cuidado al elegir el lugar para guardar passwords y tira libretas o apuntes confidenciales en la basura.

AMENAZAS

Respecto a las condiciones externas, que representan severos obstáculos a vencer encontramos que:

- Actualmente nuestro país ocupa el séptimo lugar en toda américa en recibir ataques cibernéticos, según Symantec.
- A un alto porcentaje de ordenadores les falta, al menos, una protección como software antivirus actualizado, protección contra el spyware o programas espía, y una barrera de seguridad o firewall que funcione adecuadamente.
- Entre los delitos más comunes están el secuestro y robo de bases de datos, obtención de códigos personales e información confidencial, fraude financiero, espionaje corporativo e industrial y hurto de números de cuentas bancarias.
- Debido a la falta de conciencia de la seguridad cibernética, muchas empresas

consideran poco probable ser víctimas de la delincuencia informática.

- Aunque hoy en día 98% de las empresas e instituciones del mundo utilizan programas antivirus, durante el 2014 más del 90% tuvo problemas relacionados con el spyware y phishing.
- No existen incentivos fiscales para las empresas con el fin de proteger su información. La ingeniería social tiene un alto número de incidencia en la actualidad.

Con los resultados obtenidos se obtuvo un panorama general del estado actual de la Municipalidad Distrital de Independencia, que sirvió de base para posteriormente aplicar un cuestionario que permitió hacer un diagnóstico más amplio.

2.2.11.2. Instrumento

Se conformó un cuestionario que se fundamentó en la metodología de ISACA [37] , y la Operacionalización

[37] ISACA es el acrónimo de Information Systems Audit and Control Association (Asociación de Auditoría y Control de Sistemas de Información), una asociación internacional que apoya y patrocina el desarrollo de metodologías y certificaciones para la realización de actividades auditoría y control en sistemas de información.

contextuada de la conjetura que guío la investigación, el cual constaba de tres partes a) objetivo, b) datos generales y c) preguntas específicas sobre el tema, su aplicación se llevó a cabo en dos sesiones con el objeto de no confundir y hacerlo tedioso a los colaboradores, tenía un total de 25 preguntas, y el propósito específico era conocer sus hábitos de medidas de protección para la información. El instrumento se dividió en dos categorías de la siguiente manera:

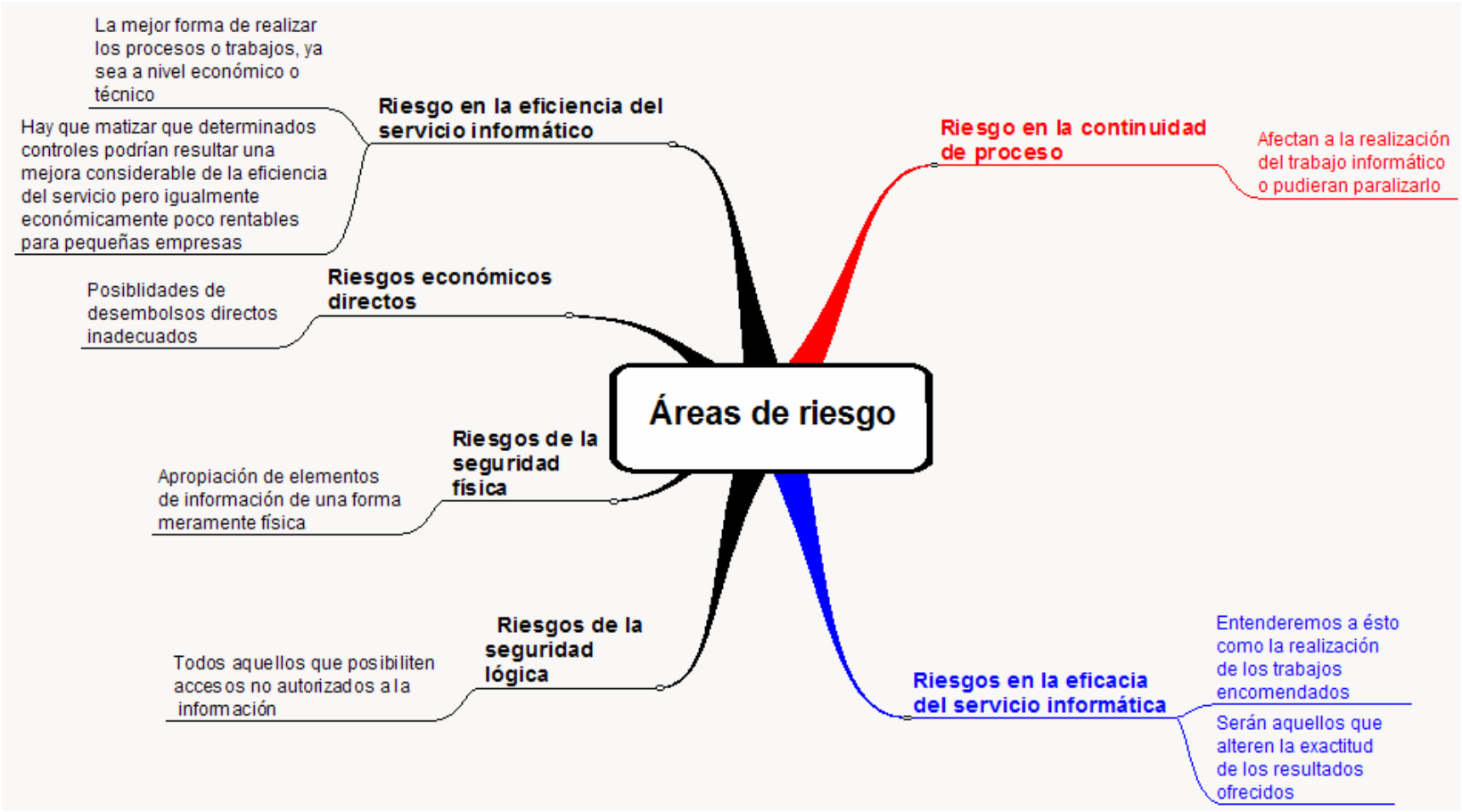
- Riesgos en la continuidad del proceso
- Riesgos en la eficacia del servicio de informática, porque se consideraron los más importantes e imprescindibles:

Para la categoría de riesgos en la continuidad del proceso se elaboraron las preguntas Nº 1 a la 9, dentro de esta categoría se tienen las variables acerca de la identificación de la identificación de peligros en Internet, keyloggers, mouseloggers y virus master boot record por mencionar los más importantes con sus respectivas respuestas y gráficas. Es esencial resaltar que los riesgos que se involucran en la continuidad del proceso pueden paralizar en un grado máximo hasta una empresa lo que ocasionaría mermas inconmensurables, se debe reflexionar que con los datos proporcionados por los colaboradores se obtienen algunas pautas, por lo que la organización confía en su suerte, al no

contar con una propuesta de seguridad en la información y en cualquier momento puede ser blanco de disminuciones que se reflejarán en detrimentos económicos.

Para la categoría de riesgos en la eficacia del servicio de informática, se elaboraron las preguntas Nº 10 a la 25 dentro de esta categoría se establecieron indicadores que se relacionan con la continuidad del proceso como son algunos de ellos los gusanos informáticos, los puntos potenciales de infección y los troyanos.

Mapa Mental Nº 2.1 - Áreas de Riesgo

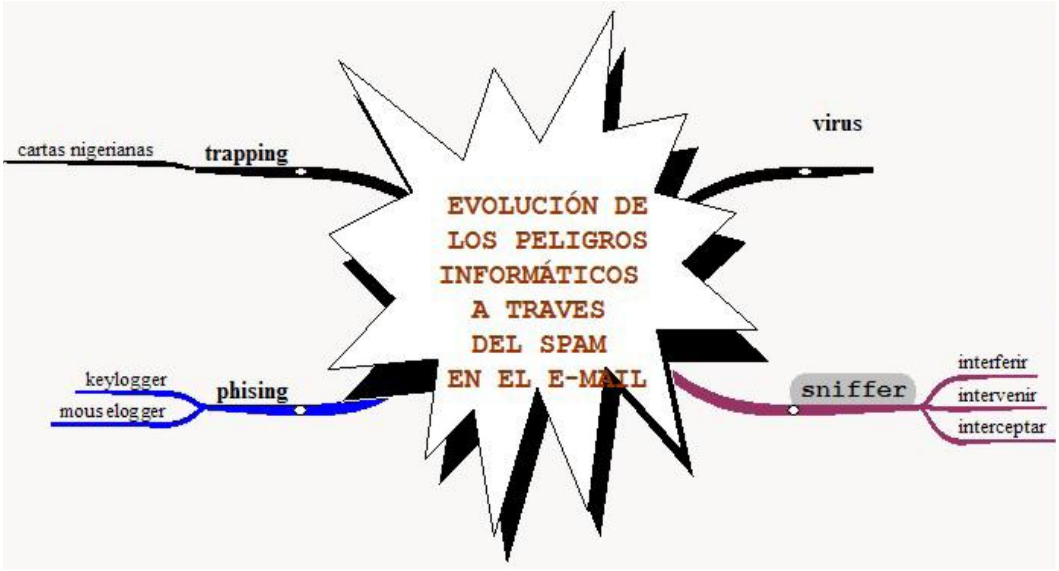


Fuente: www.seguridadinformatica.unlu.edu.ar/files/site/material_taller_gestion_de_riesgo.pdf

2.2.11.3. Evolución de los riegos a que está expuesta la información de la institución a través del spam.

Podrían existir diferentes escenarios de riesgos si no se toman en cuenta las medidas de seguridad que se identifican en el presente trabajo de tesis, algunas de ellas son:

Mapa Mental Nº 2.2 - Evolución de los riesgos informáticos que se deben en la empresa a través del spam por medio del e-mail.



Fuente: http://recursostic.educacion.es/observatorio/web/en/equipamiento-tecnologico/seguridad-y-mantenimiento/263-luis-antonio-garcia-gisbert

2.2.11.4. Riesgos que la empresa ha recibido a través de su correo electrónico

Por no contar con la guía adecuada de identificación de riesgos la institución fue atacada principalmente de spam y en consecuencia la posibilidad de otros riesgos que se

detallaran en el escenario spam, la problemática que tuvo que enfrentar.

2.2.11.5. Escenarios en los que podría situarse la institución y su alto costo financiero.

2.2.11.5.1. Escenario spam

El spam por si solo como tal, no representa ningún peligro pero sí ocasiona un muy alto gasto para la institución, por tener que lidiar con estos correos, pero para las estaciones de trabajo les afecta cuando lleguen a tener un programa oculto como un keylogger, el spam es extremadamente peligroso, así mismo por su naturaleza, es el medio comisivo para los delitos informáticos y es altamente peligroso para los usuarios, ya que ahí se derivan los robos de claves entre otros delitos.

El spam tiene un alto costo, las empresas que no están protegidas de este riesgo llegan a tener altos costos para evitar ser víctimas de delitos. Un ejemplo descriptivo de este gasto es el siguiente:

1. Los filtros de spam que tienen que pagar las empresas por no recibir éste correo basura son muy altos, pero a veces “éstos llega a

ser una arma de doble filo porque los filtros llegan a ser tan efectivos en algunos casos y poderosos que pueden llegar a bloquear a direcciones de las cuales sí desean llegar a recibir mails". Esto es similar a poner un muro de protección sin saber lo que se deja afuera y lo que se deja dentro. El costo es aproximadamente de S/.6,000.00 mensuales a S/.15,000.00.

2. El tiempo de internet que se pierde en toda la parafernalia en los correos en donde se tiene que revisar entre correos que si son útiles y no son útiles, y una vez que se detectó los que sirven para consultarlos o guardarlos y después llegar a borrar los que no sirven que entren en la categoría del spam. Tienen un costo por usuario para 10 analistas que corresponde a 15 minutos aproximadamente cuya erogación de S/.150.00 diarios por 10 analistas.
3. El tiempo de internet que se ocupa según la conexión. El costo es aproximadamente de S/.15.00 diarios.

4. La luz eléctrica que se desperdició por borrar y revisar los correos inútiles. El costo es aproximadamente de S/.15.00 diarios.
5. El tiempo de los empleados de trabajo que le llega a costar a la empresa por distraerse de sus actividades es de aproximadamente entre S/.30.00 y de S/.60.00 diarios.
6. El ancho de banda que se está ocupando para recibir, consultar y borrar los correos basura. El costo es aproximadamente de S/.150.00.

2.2.11.5.2. Escenario sniffer.

Se refiere a cuando cualquier usuario o empresa sea víctima de la instalación de un sniffer en una computadora por medio del spam, la "repercusión inmediata de este peligro es enterarse de toda la información o es un programa de captura de las tramas de red.", las consecuencias de saber el tráfico en la red de una empresa llega a ser peligroso, éste método es tardado y altamente peligroso, si el objetivo principal es capturar claves de usuarios con

cuentas bancarias, si el propósito es conocer todos los archivos e informes de la empresa , ya que de esta manera es posible enterarse con detalle de lo que se gasta en servicios, de archivos para poder conocer la nómina de empleados, archivos personales de los colaboradores, información de todas las actividades que recorren en la red o carpetas compartidas en las que los usuarios compartan información. Suponiendo que se haya instalado un sniffer en la empresa pueden suceder tres alternativas.

Que el usuario que irrumpa el sistema, y así interferir esto es, enterarse de todo lo que se maneje en los archivos de la red, esto puede tener un costo a la empresa de S/.3,000.00 diarios por conocer todas sus actividades.

Que el usuario que irrumpa el sistema pueda intervenir, esto quiere decir que manipule los datos con información irreal y así el resultado estará fuera de la realidad por lo que puede llevar a la empresa a la bancarrota por lo que su costo puede ser el cierre de la empresa.

Que el usuario que irrumpa el sistema pueda interceptar la información, y así poder determinar qué información deja pasar al usuario receptor del archivo, esto puede ser extremadamente peligroso a la empresa por no dejar que fluya la información y el costo por día pudiese ser de S/.30,000.00.

2.2.11.5.3. Escenario phishing

Un escenario en el que podría caer cualquier empresa es ser víctima del phishing, el término phishing "viene de la palabra en inglés fishing haciendo alusión al acto de pescar usuarios mediante señuelos cada vez más sofisticados y de este modo obtener información" financiera y contraseñas, de aquí se derivan:

- **Keylogger:** Es un escenario en el que podría caer cualquier empresa es posible que sea instalado un keylogger en la computadora del administrador financiero, con lo que se lograría utilizar como máquina zombie para uso del usuario que haya mandado el correo electrónico (spam) con el fin de poder capturar claves, así, debido a las funciones y

jerarquía del Gerente, se tienen que llevar a cabo pagos de la empresa vía internet, como por ejemplo, pagos de celulares para los directivos de la misma, entre otros servicios que se pagan, también otras áreas hacen uso de las transferencias electrónicas, ya que la gente que labora en el área de Recursos Humanos, tiene que hacer la transferencia de nómina a los empleados de la empresa y si el keylogger se encuentra en operación, entonces ya existe una intrusión que puede apoderarse de la información que alimente el usuario y la contraseña de la cuenta bancaria de la empresa, por lo que tiene la información más valiosa para poder hacer uso de ésta en su beneficio y así lograr realizar las trasferencias que él desee, a su cuenta, hacer pagos personales, u ordenar productos vía internet, este escenario puede costarle a la empresa de S/.3,000.00 hasta S/.30,000.00 por un día que se haga la transferencia por nómina de la empresa.

- **Mouselogger:** Es un escenario en el que podría caer cualquier empresa, es muy

parecido a un keylogger, por lo que por suponer este escenario en la computadora de un empleado con funciones de pagos, como de impuestos u otros servicios, podría ser extremadamente peligroso, ya que una vez instalado un mouselogger, la terminal se emplearía como máquina zombie, apoderándose de la información, el intruso que mando el correo electrónico infectado lo cual es muy probable cuando recibimos spam, con el fin de poder capturar claves, por suponer un escenario donde el Gerente Financiero o sus subordinados, donde el área lleva a cabo pagos de la empresa vía internet, como por ejemplo, pagos de celulares para los directivos de la misma, entre otros servicios que se pagan, también otras áreas hacen uso de las transferencias electrónicas, ya que los colaboradores que laboran en el área de recursos humanos tienen que hacer la transferencia de nómina a los empleados de la empresa y si el Mouselogger se encuentra en operación entonces ya existe una intrusión que puede contar el usuario y la

contraseña de la cuenta bancaria de la empresa

2.2.11.5.4. Escenario trapping

Este escenario es de alto peligro, cuando llega el correo de un banco, con el propósito de conocer las preferencias del usuario, por medio del spyware ya que identifica las páginas que navega, de tal modo puede conocer qué dirección de banco teclea, en donde tiene cuenta el usuario, para así hacerse pasar por empleado del banco, mandando un correo de identidad falsa, como por ejemplo de empresa@banamex.com o cualquier otro banco y pedir que actualice su cuenta, login y contraseña por medio de una liga en el correo que abre una página donde simula ser un portal del banco, en esta situación, el usuario tontamente entrega voluntariamente su contraseña. Existen ocasiones en donde para ser atractivo para el usuario les llega un correo en donde les dicen que han obtenido un premio por tener su cuenta bancaria en la empresa, que cuentan con su dinero y que sólo es necesario que actualicen sus datos.

Es importante saber el dato que el jargot del hacker detalló que en Perú “70% de las causas de las vulnerabilidades en las organizaciones, provienen de sus empleados o ex empleados, el restante 30% se originan en Internet”.

2.2.11.5.5. Escenario pharming.

Otro escenario de alto peligro para una empresa es el pharming, ya que tiene por características ser una “nueva amenaza, más sofisticada y peligrosa, que consiste en manipular las direcciones DNS (Domain Name Server) que utiliza el usuario”.

Los servidores DNS son los encargados de conducir a los usuarios a la página que desean ver. Pero a través de esta acción, los ladrones de datos consiguen que las páginas visitadas no se correspondan con las auténticas, sino con otras creadas para recabar datos confidenciales, sobre todo relacionadas con la banca online.

De esta manera al llegar a manipular un DNS por medio del pharming cuando la empresa tenga que hacer una operación en línea para el traspaso de

nóminas de sus colaboradores, obtendrá toda la información y contraseñas para apoderarse de la cantidad que cuente la empresa disponible y así vaciar la cuenta, por todo esto, el costo para la empresa por una pérdida de esta magnitud sería aproximadamente de S/120,000.00.

2.2.11.6. Herramientas más comunes para mitigar los ataques mediante Phishing

Cuando se habla de herramientas de ingeniería social en especial de Phishing, se encuentran algunas herramientas tecnológicas más comunes, las cuales son usadas por expertos en la materia contra los ataques realizados mediante phishing; de igual forma se pueden encontrar algunas herramientas contra los ataques que se llevan a cabo con las técnicas basadas en humanos, estas herramientas son las políticas de seguridad, las cuales dan normatividad del uso y manipulación de la información.

A continuación serán descritas algunas herramientas conocidas para los ataques realizados mediante phishing.

2.2.11.6.1. NETCRAFT

La herramienta Netcraft contiene elementos que pueden indicar indicios de fraude en el sitio web visitado.

Por ejemplo, muestra la popularidad del sitio entre los usuarios (cuanto más visitado, más de fiar), el país donde se aloja el sitio y un índice de riesgo calculado por la propia barra de herramientas.

Se caracteriza por:

- Proteger de los ataques de phishing.
- Vigilar donde se hospeda y proporciona un índice de riesgo de los sitios que han sido visitados.
- Ayudar a defender a la comunidad internauta de fraudes.

La forma de proceder de la herramienta es que cada vez que se informa sobre un mail de phishing se consigue la URL destino a la que se envía la información, y está es bloqueada para la comunidad de miembros. Y dado que en los casos de phishing se envían cantidades masivas

de correo, y es relativamente fácil identificarlos, se descubrirán rápidamente y se producirá el bloqueo de la URL correspondiente.

Para una gran mayoría de gente, un perfil criminal consiste en información que sirve predominantemente para describir las características biográficas de los posibles perpetradores de un crimen. Entonces, los perfiles criminales típicamente contienen información sobre el posible agresor teniendo en cuenta lo siguiente:

- Características demográficas, como edad o género.
- Historia legal, incluyendo cualquier antecedente (por ejemplo historial de ofensas criminales prioritarias).
- Formación vocacional (por ejemplo el trabajo en el que el agresor está inmerso, si hubiera alguno).
- Características familiares (por ejemplo la formación de la familia del agresor).

- Hábitos e intereses sociales (deportes, hobbies u otros intereses que el agresor pueda tener).
- Modo de transportarse (tipo de vehículo, si el agresor tuviera alguno).
- Varias características de la personalidad del individuo (la conducta del agresor, apariencia, etc.).

Adicional a esta información, se debe notar que los perfiles criminales incluyen también frecuentemente información perteneciente a la ubicación aproximada de la residencia del criminal.

Al describir la aplicación de perfiles criminales, se debe enfatizar que contrario a muchas descripciones ficticias, los perfiles criminales por ellos mismos no resuelven ningún crimen. En su lugar, perfilar criminales es bien visto como una fuente que puede ser usada para ayudar en investigaciones criminales cuando los métodos convencionales que se emplean han fallado al identificar al perpetrador.

El porcentaje de uso de esta herramienta, se divide según los países en los que más se utiliza, esto se puede observar en la siguiente tabla:

Tabla Nº 2.2 - Porcentaje de uso de Netcraft

PORCENTAJE	PAÍS
56	Estados Unidos
6	Reino Unido
4	Alemania, Canadá
2	Japón, Holanda, Francia, Suecia, Italia
2	Desconocido
1	Suiza, Australia, Korea, India
12	Resto del mundo

Fuente: https://www.netcraft.com/

Esta herramienta tiene un licenciamiento libre, es decir, se descarga libremente desde Internet y no tiene un costo, simplemente se deben seguir los términos y condiciones de uso para poder usarlo.

El logo mediante el cual puede ser reconocido Netcraft y su barra anti-phishing es el siguiente:

2.2.11.6.2. EARTHLINK

La herramienta Earthlink es una barra de herramientas que califica según sus propios criterios los webs visitados como 'Seguro', 'Sospechoso' o 'Fraudulento'. En este último caso, se bloquea el acceso a dicho web.

Existe un cuarto estado ('Neutral') que no garantiza que sea un sitio seguro, pero no tiene motivos para sospechar de él.

Dentro de las características de esta herramienta se encuentra el bloqueo de ventanas emergentes.

La licencia de esta herramienta es gratuita, por lo que simplemente se la descarga del Internet y se la instala.

El logotipo con el que se puede reconocer a esta herramienta es el siguiente:

2.2.11.6.3. GEOTRUST

La herramienta Geotrust indica la fiabilidad del web visitado mediante un código de colores (rojo - amarillo - verde).

La fiabilidad de un sitio depende de si su validez ha sido o no comprobada por los autores de la barra.

Indicador de Estado

El sitio está verificado y es seguro el uso de información personal y confidencial.

El sitio no está verificado. No tiene por qué ser malo, simplemente no TrustWatch no lo ha verificado.

El sitio visitado es fraudulento.

Dentro de las características de este sitio se encuentran:

- Informar sobre un fraude
- Bloquear ventanas emergentes
- Enseñar el sitio web real que se está visitando

La licencia de este producto tiene un costo de alrededor de 80 euros, la misma que nos garantiza que esta herramienta envía certificados de autenticación del sitio web del que estamos recibiendo la información.

El logotipo con el cual se puede reconocer a esta herramienta es el siguiente:

Existen herramientas o software que sirve para controlar la fuga de información a través de correo electrónico, dispositivos de almacenamiento, impresiones, etc., dentro de estas se puede encontrar algunas.

2.2.11.6.4. WEBSENSE CONTENT PROTECTION SUITE

Combina la concienciación de contenido y contexto apoyando la inteligencia Web a través de la integración con la base de datos de URLs de Websense y la tecnología de clasificación de contenido malicioso ThreatSeeke, así como nuevas capacidades de reconocimiento de información basadas en el contexto que incrementan la precisión de la detección y permiten a las organizaciones crear y hacer cumplir políticas de compartición de información y de usuario específico.

Dentro de las características que se pueden encontrar dentro de esta herramienta se encuentran las siguientes:

- Conocimiento y control del contexto
- Conocimiento mejorado del contenido
- Protección de seguridad avanzada
- Mejoras en administración y despliegue

La licencia de este software o herramienta tiene un costo, como la mayoría de programas cuenta con una versión de prueba.

La imagen con la que se puede reconocer a esta herramienta, es la siguiente:

2.2.11.6.5. SYMANTEC DATA LOSS PREVENTION

Symantec Data Loss Prevention ofrece una solución unificada para detectar, supervisar y proteger la información confidencial sin importar dónde se almacene o cómo se utilice.

Symantec ofrece cobertura completa de los datos confidenciales en sistemas de almacenamiento, endpoints y redes. Al reducir notablemente los riesgos, verá su confianza renovada para demostrar el cumplimiento mientras protege la imagen de la empresa, la propiedad intelectual y los clientes.

Dentro de las funciones principales de esta herramienta podemos encontrar:

- Detección: Localiza la información confidencial
- Supervisión: Comprenda de qué modo se usa la información confidencial
- Protección: Aplicar políticas de seguridad automáticamente
- Administración: Definir políticas universales para toda la empresa

Esta herramienta dispone de una licencia pagada para diversos tipos de empresas, con diferentes tipos de acuerdos y en ciertos casos se pueden encontrar descuentos.

El logotipo con el que se puede distinguir este software es:

2.2.11.6.6. MCAFEE

La empresa McAfee, presenta varias alternativas en cuanto a software y hardware se refiere para controlar la fuga de datos, a continuación se indican los nombres de las mismas:

- McAfee Device Control: Regula el uso de medios portátiles en la red
- McAfee Host Data Loss Prevention: Supervisa y controla la manera en que los empleados transfieren datos de negocio.
- McAfee Network DLP Discover: Identifica y protege los datos delicados.
- McAfee Network DLP Manager: Usa dispositivos a lo largo de la red para controlar la pérdida de datos.
- McAfee Network DLP Monitor: Crea reglas complejas, mediante las cuales controla los datos que son enviados.
- McAfee Network DLP Prevent: Aplica políticas para proteger los datos que están en movimiento.
- McAfee Port Control: Controla el uso de dispositivos portátiles conectados en la red.

Todas estas herramientas, ya sean software o hardware, cuentan con una licencia pagada, la cual depende de la herramienta de la que se trata.

El logotipo con el cual se reconocen estas herramientas es:

2.3. Definición de Términos

Guía de terminología relacionada con la seguridad informática que puede encontrar en el Informe sobre las Amenazas a la Seguridad en Internet de Symantec[38] y en otros materiales relacionados con la seguridad informática. Fuente: https://www.symantec.com/es/mx/theme.jsp?themeid=glosario-de-seguridad

0-day attack: Es un ataque contra una aplicación o sistema que tiene como objetivo la ejecución de código malicioso gracias al conocimiento de vulnerabilidades que, por lo general, son desconocidas para la gente y el fabricante del producto.

Adware: Adware es un software, generalmente no deseado, que facilita el envío de contenido publicitario a un equipo.

Amenaza: Una amenaza informática es toda circunstancia, evento o persona que tiene el potencial de causar daño a un sistema en forma de robo, destrucción, divulgación, modificación de datos o negación de servicio (DoS).

[38] Symantec es una corporación internacional que desarrolla y comercializa software para computadoras, particularmente en el dominio de la seguridad informática, a la par que es el líder del mercado mundial en seguridad de endpoints, seguridad del correo electrónico, prevención contra la pérdida de datos y certificados SS.

Amenazas polimorfas: Son aquellas que tienen la capacidad de mutar y en las cuales cada instancia del malware es ligeramente diferente al anterior a este. Los cambios automatizados en el código realizados a cada instancia no alteran la funcionalidad del malware, sino que prácticamente inutilizan las tecnologías tradicionales de detección antivirus contra estos ataques.

Anchoring (anclaje): Termino de la P.N.L. que posibilita enlazar conceptos a partir de insertar un disparador en la mente, y que al notar un estímulo se dispare, haciendo que se recuerde una sensación, un recuerdo o un estado mental.

Antispam: Es un producto, herramienta, servicio o mejor práctica que detiene el spam o correo no deseado antes de que se convierta en una molestia para los usuarios. El antispam debe ser parte de una estrategia de seguridad multinivel.

Antivirus: Es una categoría de software de seguridad que protege un equipo de virus, normalmente a través de la detección en tiempo real y también mediante análisis del sistema, que pone en cuarentena y elimina los virus. El antivirus debe ser parte de una estrategia de seguridad estándar de múltiples niveles.

Aplicaciones engañosas: Son programas que intentan engañar a los usuarios informáticos para que emprendan nuevas acciones que normalmente están encaminadas a causar la descarga de malware adicional o para que los

usuarios divulguen información personal confidencial. Un ejemplo es el software de seguridad fraudulento, que también se denomina scareware.

Ataques multi-etapas: Un ataque en múltiples etapas es una infección que normalmente implica un ataque inicial, seguido por la instalación de una parte adicional de códigos maliciosos. Un ejemplo es un troyano que descarga e instala adware.

Ataques Web: Un ataque Web es un ataque que se comete contra una aplicación cliente y se origina desde un lugar en la Web, ya sea desde sitios legítimos atacados o sitios maliciosos que han sido creados para atacar intencionalmente a los usuarios de ésta.

Authority (Autoridad): Poder que permite controlar a la gente de la misma organización pero de puestos inferiores.

Blacklisting o Lista Negra: Es el proceso de identificación y bloqueo de programas, correos electrónicos, direcciones o dominios IP conocidos maliciosos o malévolos.

Barnum Statements: Frases genéricas con cabida en cualquier situación.

Bogon: Es un nombre informal que recibe un paquete de Internet que dice ser de un área que no existe.

Bot/Zombie: Ordenador infectado por algún tipo de malware que lo controla remotamente, la cual forma parte de una red de bots (bot net).

Botnet: Conjunto de equipos bajo el control de un bot maestro, a través de un canal de mando y control. Estos equipos normalmente se distribuyen a través de Internet y se utilizan para actividades malintencionadas, como el envío de spam y ataques distribuidos de negación de servicio. Las botnet se crean al infectar las computadoras con malware, lo cual da al atacante acceso a las máquinas. Los propietarios de computadoras infectadas generalmente ignoran que su máquina forma parte de una botnet, a menos que tengan software de seguridad que les informe acerca de la infección.

Caballo de Troya: Son un tipo de código malicioso que parece ser algo que no es. Una distinción muy importante entre troyanos y virus reales es que los troyanos no infectan otros archivos y no se propagan automáticamente. Los caballos de troya tienen códigos maliciosos que cuando se activan causa pérdida, incluso robo de datos. Por lo general, también tienen un componente de puerta trasera, que le permite al atacante descargar amenazas adicionales en un equipo infectado. Normalmente se propagan a través de descargas inadvertidas, archivos adjuntos de correo electrónico o al descargar o ejecutar voluntariamente un archivo de Internet, generalmente después de que un atacante ha utilizado ingeniería social para convencer al usuario de que lo haga.

Canal de control y comando: Es el medio por el cual un atacante se comunica y controla los equipos infectados con malware, lo que conforma un botnet.

Captcha: Imagen distorsionada legible para un humano pero no para una máquina.

Carga destructiva: Es la actividad maliciosa que realiza el malware. Una carga destructiva es independiente de las acciones de instalación y propagación que realiza el malware.

Ciberdelito: Es un delito que se comete usando una computadora, red o hardware. La computadora o dispositivo puede ser el agente, el facilitador o el objeto del delito. El delito puede ocurrir en la computadora o en otros lugares.

Clickjacking: Ataque malicioso dirigido al navegador del usuario que simula estar pulsando sobre algo pero que en realidad pulsa sobre otro sitio.

Cold reading: Técnica para extraer información de alguien sin saber nada de él.

Commitment (Responsabilidad): Forma de ser considerado sujeto de una deuda u obligación.

Consistency (Consistencia): Argumentación de todas las dudas posibles.

Cracker: Persona que hace delitos en Internet.

Crimeware: Software que realiza acciones ilegales no previstas por un usuario que ejecuta el software. Estas acciones buscan producir beneficios económicos al distribuidor del software.

Cross-Site Request Forgery (CSRF): Ataque malicioso que se produce al acceder externamente desde otra web a una web que no válida correctamente la procedencia.

Definiciones de virus: Es un archivo que proporciona información al software antivirus, para identificar los riesgos de seguridad. Los archivos de definición tienen protección contra todos los virus, gusanos, troyanos y otros riesgos de seguridad más recientes. Las definiciones de virus también se denominan firmas antivirus.

Descarga inadvertida: Es una descarga de malware mediante el ataque a una vulnerabilidad de un navegador Web, equipo cliente de correo electrónico o plug-in de navegador sin intervención alguna del usuario. Las descargas inadvertidas pueden ocurrir al visitar un sitio Web, visualizar un mensaje de correo electrónico o pulsar clic en una ventana emergente engañosa.

Domain Name System (DNS): Sistema de nomenclatura jerárquica para ordenadores.

Dumpster Diving: Técnica que consiste en buscar en la basura documentos oficiales de una empresa.

Economía clandestina: En línea es el mercado digital donde se compran y se venden bienes y servicios obtenidos a través de la ciberdelincuencia, con el fin de cometer delitos informáticos. Dos de las plataformas más comunes a disposición de los participantes en la economía clandestina en línea son los canales en servidores IRC y foros Web. Los dos tienen grupos de discusión

que utilizan participantes para comprar y vender bienes y servicios fraudulentos. Los artículos vendidos son datos de tarjetas de crédito, información de cuentas bancarias, cuentas de correo electrónico y toolkits de creación de malware. Los servicios incluyen cajeros que pueden transferir fondos de cuentas robadas en moneda real, phishing y hosting de páginas fraudulentas y anuncios de empleo para cargos como desarrolladores de fraude o socios de phishing.

E-crime o Crimen electrónico: Cualquier tipo de crimen que se produce en Internet.

Encriptación: Es un método de cifrado o codificación de datos para evitar que los usuarios no autorizados lean o manipulen los datos. Sólo los individuos con acceso a una contraseña o clave pueden descifrar y utilizar los datos. A veces, el malware utiliza la encriptación para ocultarse del software de seguridad. Es decir, el malware cifrado revuelve el código del programa para que sea difícil detectarlo.

Exchangeable Image file Format (EXIF): Formato de las imágenes JPG que permite incrustar en su interior información oculta (metadatos).

Exploits o Programas intrusos: Son técnicas que aprovechan las vulnerabilidades del software y que pueden utilizarse para evadir la seguridad o atacar un equipo en la red.File Transfer Protocol (FTP): Protocolo de transferencia de datos en plano basado en el sistema cliente-servidor.

Filtración de datos: Una filtración de datos sucede cuando se compromete un sistema, exponiendo la información a un entorno no confiable. Las filtraciones de datos a menudo son el resultado de ataques maliciosos, que tratan de adquirir información confidencial que puede utilizarse con fines delictivos o con otros fines malintencionados

Firewall: Es una aplicación de seguridad diseñada para bloquear las conexiones en determinados puertos del sistema, independientemente de si el tráfico es benigno o maligno. Un firewall debería formar parte de una estrategia de seguridad estándar de múltiples niveles.

Firma antivirus: Es un archivo que proporciona información al software antivirus para encontrar y reparar los riesgos. Las firmas antivirus proporcionan protección contra todos los virus, gusanos, troyanos y otros riesgos de seguridad más recientes. Las firmas antivirus también se denominan definiciones de virus.

Greylisting o Lista Gris: Es un método de defensa para proteger a los usuarios de correo electrónico contra el spam. Los mensajes de correo electrónico son rechazados temporalmente de un remitente que no es reconocido por el agente de transferencia de correos. Si el correo es legítimo, el servidor de origen tratará de nuevo y se aceptará el correo electrónico. Si el correo es de un remitente de spam, probablemente no se reintentará su envío y por lo tanto, no logrará pasar el agente de transferencia de correos.

Gusanos: Son programas maliciosos que se reproducen de un sistema a otro sin usar un archivo anfitrión, lo que contrasta con los virus, puesto que requieren la propagación de un archivo anfitrión infectado.

Harvesting: Nombre que recibe en seguridad informática el proceso de recoger información de algo o alguien. También recibe el nombre de footprinting.

Hishing (Hardware Phishing): Denominación de ataque de phishing basado en utilizar periféricos para ocultar troyanos u otro tipo de malware debido a la poca sospecha que levanta.

Hoax: Bulo sin fin económico.

Ingeniería social (I.S.): Método utilizado por los atacantes para engañar a los usuarios informáticos, para que realicen una acción que normalmente producirá consecuencias negativas, como la descarga de malware o la divulgación de información personal. Los ataques de phishing con frecuencia aprovechan las tácticas de ingeniería social.

Ingeniería social automatizada (I.S.A.): Término utilizado para referirse a lograr que se efectúe un ataque de I.S. sin depender de una persona.

Internet Protocol (IP): Una dirección IP es una etiqueta numérica que identifica, de manera lógica y jerárquica, a un interfaz de un dispositivo dentro de una red que utilice el protocolo IP, que corresponde al nivel de red del protocolo TCP/IP.

Keystroke Logger o Programa de captura de teclado (Keylogger): Es un tipo de malware diseñado para capturar las pulsaciones, movimientos y clics del teclado y del ratón, generalmente de forma encubierta, para intentar robar información personal, como las cuentas y contraseñas de las tarjetas de crédito.

Liking (Simpatía): Acción o efecto de conectar con otra persona, sufriendo o alegrándose ambas juntas.

Malware: El malware es la descripción general de un programa informático que tiene efectos no deseados o maliciosos. Incluye virus, gusanos, troyanos y puertas traseras. El malware a menudo utiliza herramientas de comunicación populares, como el correo electrónico y la mensajería instantánea, y medios magnéticos extraíbles, como dispositivos USB, para difundirse. También se propaga a través de descargas inadvertidas y ataques a las vulnerabilidades de seguridad en el software. La mayoría del malware peligroso actualmente busca robar información personal que pueda ser utilizada por los atacantes para cometer fechorías.

Man-In-The-Middle: Ataque que consiste en interceptar la comunicación entre dos individuos.

Man-Left-In-The-Middle (MLITM): Ataque a partir de la variable "Referer" del navegador que compromete la seguridad del servidor o de otro atacante.

Mecanismo de propagación: Es el método que utiliza una amenaza para infectar un sistema.

Misdirection (Distracción): Ataque psico-social aprovechándose de las limitaciones perspectivas y de conocimiento de la víctima.

Negación de servicio (DoS): Es un ataque en el que el delincuente intenta deshabilitar los recursos de una computadora o lugar en una red para los usuarios. Un ataque distribuido de negación de servicio (DDoS) es aquel en que el atacante aprovecha una red de computadoras distribuidas, como por ejemplo una botnet, para perpetrar el ataque.

Payload: Encapsulado de datos que permite enviar acciones específicas por el atacante.

Pharming: Método de ataque que tiene como objetivo redirigir el tráfico de un sitio Web a otro sitio falso, generalmente diseñado para imitar el sitio legítimo. El objetivo es que los usuarios permanezcan ignorantes del redireccionamiento e ingresen información personal, como la información bancaria en línea, en el sitio fraudulento. Se puede cometer pharming cambiando el archivo de los equipos anfitriones en la computadora de la víctima o atacando una vulnerabilidad en el software del servidor DNS.

Phisher: Persona que envía phishing.

Phishing: A diferencia de la heurística o los exploradores de huella digital, el software de seguridad de bloqueo de comportamiento se integra al sistema operativo de un equipo anfitrión y supervisa el comportamiento de los programas en tiempo real en busca de acciones maliciosas. El software de bloqueo de comportamiento bloquea acciones potencialmente dañinas, antes

de que tengan oportunidad de afectar el sistema. La protección contra el comportamiento peligroso debe ser parte de una estrategia de seguridad estándar de múltiples niveles.

Phreaker: Persona con avanzados conocimientos en redes telefónicas y su funcionamiento a la cual le gusta ponerlas a prueba.

Pickpocking: Disciplina que se encarga de estudiar como usurpar cualquier objeto de una persona sin que esta lo perciba.

Programación neurolingüística (P.N.L.): parte de la psicología no clínica, que estudia los procesos mentales con el fin de obtener un modelo formal y dinámico de cómo funciona la mente y la percepción humana.

Protección heurística (Heuristics-Based Protection): Forma de tecnología antivirus que detecta las infecciones mediante el escrutinio de la estructura general de un programa, las instrucciones de sus computadoras y otros datos contenidos en el archivo. Una exploración heurística hace una evaluación sobre la probabilidad de que el programa sea malicioso con base en la aparente intención de la lógica. Este plan puede detectar infecciones desconocidas, ya que busca lógica generalmente sospechosa, en lugar de huellas específicas de malware, tales como los métodos tradicionales de antivirus de firmas. La protección heurística debería hacer parte de una estrategia de seguridad estándar de múltiples niveles

Proxy: Es un programa o dispositivo que realiza una acción en representación de otro.

Psico-social: Mezcla de factores psicológicos y sociológicos que influencian sobre algo o alguien.

Rapport (acompasamiento): Termino utilizado cuando dos o más personas se sincronizan porque se sienten comprendidos mutuamente.

Reciprocity (Reciprocidad): Expectativa social que la gente responde acorde a lo recibido.

Redes punto a punto (P2P): Red virtual distribuida de participantes que hacen que una parte de sus recursos informáticos estén a disposición de otros participantes de la red, todo sin necesidad de servidores centralizados. Las redes puntos a punto son utilizadas para compartir música, películas, juegos y otros archivos. Sin embargo, también son un mecanismo muy común para la distribución de virus, bots, spyware, adware, troyanos, rootkits, gusanos y otro tipo de malware.

Rootkit: Componente de malware que utiliza la clandestinidad para mantener una presencia persistente e indetectable en un equipo. Las acciones realizadas por un rootkit, como la instalación y diversas formas de ejecución de códigos, se realizan sin el conocimiento o consentimiento del usuario final. Los rootkits no infectan las máquinas por sí mismos como lo hacen los virus o gusanos, sino que tratan de proporcionar un entorno indetectable para ejecutar códigos maliciosos. Los atacantes normalmente aprovechan las vulnerabilidades en el equipo seleccionado o utilizan técnicas de ingeniería social para instalar manualmente los rootkits. O, en algunos casos, los rootkits

pueden instalarse automáticamente al ejecutarse un virus o gusano o incluso simplemente al navegar en un sitio Web malicioso. Una vez instalados, el atacante puede realizar prácticamente cualquier función en el sistema, incluyendo acceso remoto, intercepción de comunicaciones, así como procesos de ocultamiento, archivos, claves de registro y canales de comunicación.

Scam: Engaño personalizado con fin económico.

Scambaiter: Persona que contesta los scams para engañar al scammer.

Scammer: Persona que envía scams.

Scarcity (Escasez): Factor social que influencia por ser único.

Seguridad basada en la reputación: Es una estrategia de identificación de amenazas que clasifica las aplicaciones con base en ciertos criterios o atributos para determinar si son probablemente malignas o benignas. Estos atributos pueden incluir diversos aspectos como la edad de los archivos, la fuente de descarga de los archivos y la prevalencia de firmas y archivos digitales. Luego, se combinan los atributos para determinar la reputación de seguridad de un archivo. Las calificaciones de reputación son utilizadas después por los usuarios informáticos para determinar mejor lo que es seguro y permitirlo en sus sistemas. La seguridad basada en la reputación debe ser parte de una estrategia de seguridad estándar de múltiples niveles.

Shoulder Surfing: Técnica que consiste en espiar por encima del hombro a la víctima cuando introduce una contraseña o un dato sensible.

Sistema de detección de intrusos: Es un servicio que monitorea y analiza los eventos del sistema para encontrar y proporcionar en tiempo real o casi real advertencias de intentos de acceso a los recursos del sistema de manera no autorizada. Es la detección de ataques o intentos de intrusión, que consiste en revisar registros u otra información disponible en la red. Un sistema de detección de intrusos debe ser parte de una estrategia de seguridad estándar de múltiples niveles.

Sistema de prevención de intrusos: Es un dispositivo (hardware o software) que supervisa las actividades de la red o del sistema en busca de comportamiento no deseado o malicioso y puede reaccionar en tiempo real para bloquear o evitar esas actividades. Un sistema de prevención de intrusos debe ser parte de una estrategia de seguridad estándar de múltiples niveles.

SmiShing (SMS Phishing): Denominación de ataque de phishing basado en enviar un mensaje de texto haciéndose pasar por una entidad oficial.

Social Proof (Aprobación social): Fenómeno psicológico donde se asume que las acciones de otros reflejan el correcto comportamiento de una situación concreta

Software de seguridad fraudulento (rogue): Un programa de software de seguridad rogue es un tipo de aplicación engañosa que finge ser software de seguridad legítimo, como un limpiador de registros o detector antivirus,

aunque realmente proporciona al usuario poca o ninguna protección y, en algunos casos, puede de hecho facilitar la instalación de códigos maliciosos contra los que busca protegerse.

Spam: También conocido como correo basura, el spam es correo electrónico que involucra mensajes casi idénticos enviados a numerosos destinatarios. Un sinónimo común de spam es correo electrónico comercial no solicitado (UCE). El malware se utiliza a menudo para propagar mensajes de spam al infectar un equipo, buscar direcciones de correo electrónico y luego utilizar esa máquina para enviar mensajes de spam. Los mensajes de spam generalmente se utilizan como un método de propagación de los ataques de phishing

Spear Phishing: Denominación de ataque de phishing basado en personalizar en un nivel muy elevado el contenido del mensaje, enviándose en el momento más adecuado.

Spider: Programa que se encarga de hacer peticiones a servidores web y recoge información clave, como sus enlaces, imágenes, etc.

Spoofing: Técnicas de suplantación de identidad generalmente con usos maliciosos o de investigación.

Spyware: Paquete de software que realiza un seguimiento y envía información de identificación personal o información confidencial a otras personas. La información de identificación personal es la información que puede atribuirse a una persona específica, como un nombre completo. La

información confidencial incluye datos que la mayoría de personas no estaría dispuesta a compartir con nadie e incluye datos bancarios, números de cuentas de tarjeta de crédito y contraseñas. Los receptores de esta información pueden ser sistemas o partes remotas con acceso local.

Tabnapping: Ataque malicioso dirigido al navegador del usuario que simula una nueva pestaña pidiendo las credenciales sin que el usuario la haya abierto.

Toolkit: Paquete de software diseñado para ayudar a los hackers a crear y propagar códigos maliciosos. Los toolkits frecuentemente automatizan la creación y propagación de malware al punto que, incluso los principiante delincuentes cibernéticos son capaces de utilizar amenazas complejas. También pueden utilizarse toolkits para lanzar ataques web, enviar spam y crear sitios de phishing y mensajes de correo electrónico.

Troyano: Programa malicioso que obtiene el control sobre un sistema remoto.

Variantes: Son nuevas cepas de malware que piden prestado códigos, en diversos grados, directamente a otros virus conocidos. Normalmente se identifican con una letra o letras, seguido del apellido del malware; por ejemplo, W32.Downadup.A, W32.Downadup.B y así sucesivamente.

Vector de ataque: Es el método que utiliza una amenaza para atacar un sistema.

Virus: Programa malicioso que se propaga por si sólo en la red.

Virus más propagado: Amenaza que se dice está en su apogeo e indica que ya se está extendiendo entre los usuarios informáticos.

Vishing (VoIP Phishing): Denominación de ataque de phishing basado en lanzar ataques a través de la vía telefónica a través de un mensaje que se repite.

Voice Over IP (VoIP): Grupo de recursos que hacen posible que la señal de voz viaje a través de Internet empleando un protocolo IP.

Vulnerabilidad: Es un estado viciado en un sistema informático (o conjunto de sistemas) que afecta las propiedades de confidencialidad, integridad y disponibilidad (CIA) de los sistemas.

Web-Bug: Fichero o imagen inocua que recopila información de quien la visita.

Whisphing (Whale Phishing): Denominación de ataque de phishing basado en usar una técnica concreta sobre una población muy amplia.

III. METODOLOGÍA

3.1. Tipo y diseño de investigación

3.1.1. De acuerdo a la Orientación

La investigación es no experimental porque se realiza sin manipular intencionadamente las variables y sin asignar casualmente a los participantes. En esta investigación no se conforma ningún escenario, sino que se observaron los existentes, ya que para realizar los ataques de Phishing se tiene que vulnerar la seguridad informática tanto de los equipos informáticos y redes de la Municipalidad Distrital de Independencia.

3.1.2. De acuerdo a la técnica de contrastación

La presente investigación se considera un estudio exploratorio y descriptivo, ya que describe lo que es la seguridad informática y los principales riesgos que tiene la carencia de la misma, detalla la situación en un contexto internacional, nacional y local y ubica al objeto de estudio en toda la problemática manifestada, también es documental por la investigación que se hizo en páginas de internet, revistas, journals, tesis, libros, papers, congresos y otros.

3.2. Plan de recolección de la información y/o diseño estadístico

3.2.1. Población

- Personal de la Subgerencia de Tecnología de Información y las Comunicaciones de la Municipalidad Distrital de Independencia.
- Personal Administrativo y Auxiliar de diferentes áreas de la Municipalidad Distrital de Independencia.

3.2.2. Muestra

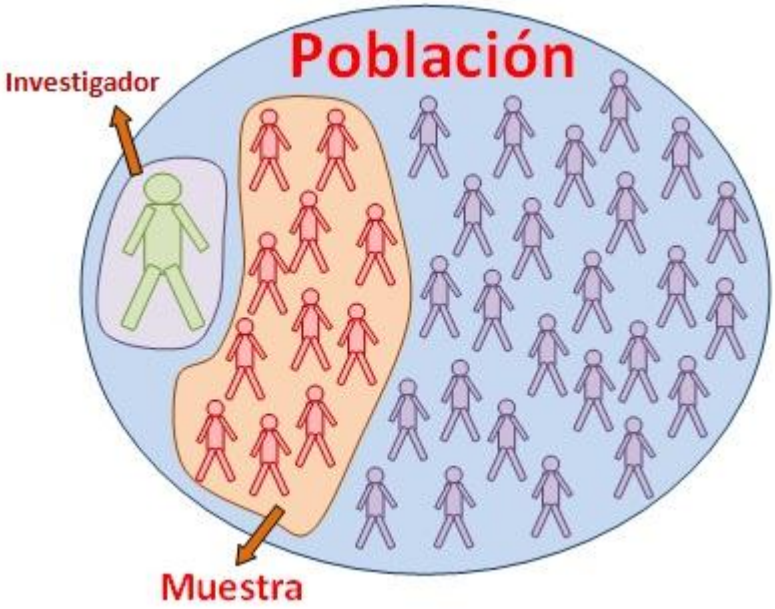
Áreas específicas y funcionales de la Municipalidad Distrital de Independencia, los cuales interactuarán directamente en el desarrollo del proyecto.

Para la determinación de la muestra, se consideró el método no probabilístico[39].

En cual consistió en elegir a los sujetos en una muestra no probabilística, dicha muestra fue generalmente seleccionado en función a la accesibilidad o a criterio personal e intencional del investigador.

[39] El muestreo no probabilístico: Es una técnica de muestreo donde las muestras se recogen en un proceso que no brinda a todos los individuos de la población iguales oportunidades de ser seleccionados.

Gráfico Nº 3.1 – Ejemplo de Muestreo No Probabilístico



Fuente: http://www.universoformulas.com/estadistica/inferencia/

El tamaño de la muestra se detalla en la siguiente tabla.

Tabla Nº 3.1. Muestra

Áreas	**Total**
Subgerencia de Tecnología de Información y las Comunicaciones	6
Otras Áreas	14
Total	**20**

3.3. Instrumentos de recolección de la información

3.3.1. Encuesta:

Se desarrolló un cuestionario de preguntas el cual estuvo dirigido a un número de personas especificas poseedoras de dicha información.

3.3.2. Observación Directa:

Se observó el proceder y comportamiento de los funcionarios y trabajadores de la Municipalidad Distrital de Independencia al momento de presentar la información requerida.

3.3.3. La Observación Sistemática:

Se empleará para medir el nivel de aprendizaje en la capacidad de actitud ante el área. Esta técnica consiste no sólo en observar, mirar y escuchar a los educandos en situaciones y actividades de aprendizaje, sino también en preguntas, analizar, probar, reconocer y apreciar el desempeño. A partir de la forma como los educandos hablan, discuten, participan en clase, llevan a cabo experimentos, hacen deporte, cantan, interactúan, etc.

3.4. Plan de procesamiento y análisis estadístico de la información

3.4.1. Plan de Procedimiento

El procedimiento de la información se realizó acudiendo y laborando en los ambientes de la Municipalidad Distrital de Independencia, especialmente en el área de la Subgerencia de Tecnología de Información y las Comunicaciones, con la finalidad de formular las preguntas correspondientes a los funcionarios y trabajadores seleccionados en la muestra.

3.4.2. Interpretación de la información

Para el análisis de los resultados obtenidos en las encuestas se utilizó la herramienta del paquete ofimática Microsoft Office Excel 2016, con la finalidad de procesar los datos e interpretarlos, dichos datos estaban conformados por las respuestas a las preguntas planteadas en el cuestionario (Anexo 5).

Las preguntas realizadas en el cuestionario diagnóstico fueron aplicadas en la Municipalidad Distrital de Independencia donde se autorizó a 20 (usuarios) unidades de trabajo debido a la información y funciones que manejan ser parte de esta tesis. Los cuestionarios se aplicaron en dos sesiones con el objetivo de no saturar de preguntas al usuario de información y de esta manera evitar falsedad en sus respuestas y sea tedioso debido a sus ocupaciones.

Dicho cuestionario se conformó en base al fundamentó de la metodología de ISACA, y la Operacionalización contextuada de la conjetura que guío la investigación, el cual constaba de tres partes a) objetivo, b) datos generales y c) preguntas específicas sobre el tema, su aplicación se llevó a cabo en dos sesiones con el objeto de no confundir y hacerlo tedioso a los colaboradores, tenía un total de 25 preguntas, y el propósito específico era conocer sus hábitos de medidas de protección para la información. El instrumento se dividió en dos categorías de la siguiente manera:

- Riesgos en la continuidad del proceso
- Riesgos en la eficacia del servicio de informática, porque se consideraron los más importantes e imprescindibles:

Para la categoría de riesgos en la continuidad del proceso se elaboraron las preguntas Nº 1 a la 9, dentro de esta categoría se tienen las variables acerca de la identificación de la identificación de peligros en Internet, keyloggers, mouseloggers y virus master boot record por mencionar los más importantes con sus respectivas respuestas y gráficas. Es esencial resaltar que los riesgos que se involucran en la continuidad del proceso pueden paralizar en un grado máximo hasta una empresa lo que ocasionaría mermas inconmensurables, se debe reflexionar que con los datos proporcionados por los colaboradores se obtienen algunas pautas, por lo que la organización confía en su suerte, al no contar con una propuesta de seguridad en la información y en cualquier momento puede ser blanco de disminuciones que se reflejarán en detrimentos económicos.

Para la categoría de riesgos en la eficacia del servicio de informática, se elaboraron las preguntas Nº 10 a la 25 dentro de esta categoría se establecieron indicadores que se relacionan con la continuidad del proceso como son algunos de ellos los gusanos informáticos, los puntos potenciales de infección y los troyanos.

IV. RESULTADOS

Interpretar los resultados de una investigación, es un paso muy importante durante el proceso de ésta, porque con base en lo que arrojan se podrá elaborar una propuesta que permita mejorar la problemática detectada que casi siempre es el propósito u objetivo de una investigación. Para el caso de este objeto de estudio, La Municipalidad Distrital de Independencia y después de la aplicación de los instrumentos explicados en el capítulo correspondiente a Metodología y Diagnóstico se obtuvieron los siguientes resultados:

Cuadro Nº 4.1 – Resultados para la categoría de riesgos en la continuidad del proceso.

Escala / Preguntas	Escala de calificación			
	R1	**R2**	**R3**	**R4**
Pregunta N° 01	23%	77%		
Pregunta N° 02	13%	25%	15%	47%
Pregunta N° 03	13%	87%		
Pregunta N° 04	8%	92%		
Pregunta Nº 05	20%	80%		
Pregunta N° 06	8%	92%		
Pregunta N° 07	33%	67%		
Pregunta N° 08	3%	97%		
Pregunta N° 09	0%	100%		

Cuadro Nº 4.2 – Resultados para la categoría de riesgos en la eficacia del servicio de informática.

Escala / Preguntas	Escala de calificación						
	R1	R2	R3	R4	R5	R6	R7
Pregunta N° 10	5%	95%	0%	0%			
Pregunta N° 11	3%	22%	27%	3%	20%	3%	22%
Pregunta N° 12	15%	23%	52%	10%			
Pregunta N° 13	23%	0%	52%	25%			
Pregunta N° 14	57%	5%	0%	5%	33%		
Pregunta N° 15	47%	8%	30%	15%			
Pregunta N° 16	37%	3%	8%	52%			
Pregunta N° 17	18%	47%	8%	27%	0%		
Pregunta N° 18	34%	15%	13%	28%	10%		
Pregunta N° 19	33%	15%	44%	8%			
Pregunta N° 20	72%	18%	5%	5%			
Pregunta N° 21	29%	28%	23%	20%			
Pregunta N° 22	54%	8%	25%	13%			
Pregunta N° 23	18%	27%	23%	32%			
Pregunta N° 24	5%	20%	52%	23%			
Pregunta N° 25	20%	45%	25%	0%	10%		

4.1. Resultados, análisis e interpretación de la investigación

Como resultado, análisis e interpretación de la aplicación del instrumento aplicado tenemos lo siguiente:

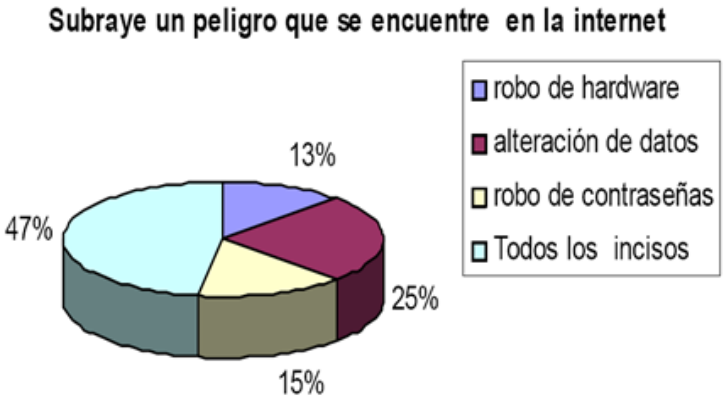
4.1.1. Para la categoría de riesgos en la continuidad del proceso.

Se elaboraron las preguntas Nº 1, 2, 3, 4, 5, 6, 7, 8 y 9, dentro de esta clasificación se establecieron indicadores en la continuidad del proceso que se consideró eran de mayor importancia por el alto riesgo que pueden ocasionar al usuario y en ésta se tienen las siguientes preguntas con sus respectivas respuestas y gráficas.

Gráfico Nº 4.1- Identificación de peligros en la red de área mundial

Como puede observarse más de las ¾ partes de los colaboradores opinaron sí reconocer peligros, pero se verificaría en la siguiente pregunta.

Gráfico Nº 4.2-Peligros en la Internet. (Alto riesgo)

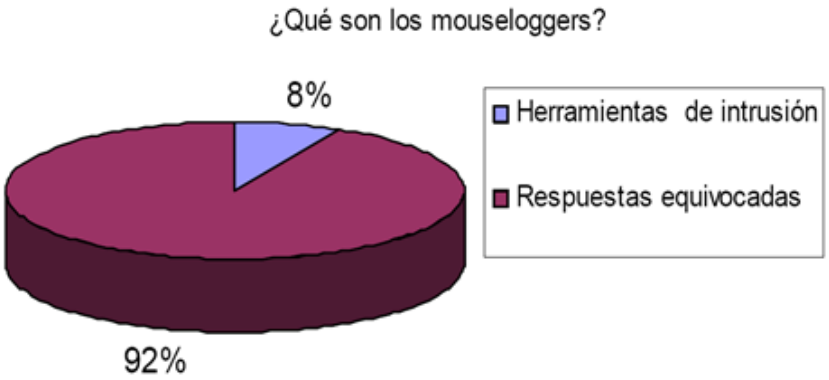


Al analizar la presente gráfica, se puede decir que más de la mitad se equivoca al identificar peligros y el 40% los identifica correctamente.

Gráfico Nº 4.3- Keyloggers. (Alto riesgo)

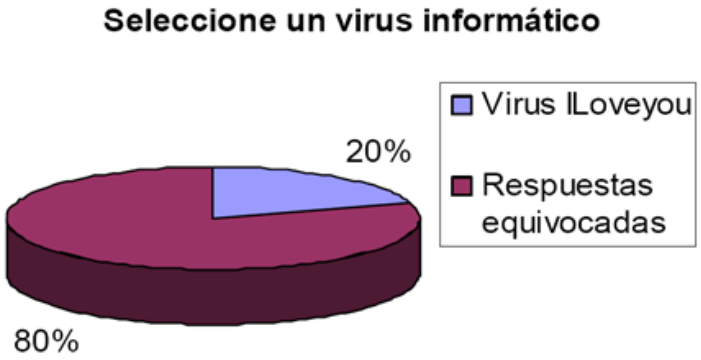
Un porcentaje considerable de los sujetos, se equivocaron al cuestionarlos acerca de los keyloggers y sólo un poco más del 10% respondió afirmativamente.

Gráfico Nº 4.4- Mouseloggers. (Alto riesgo)



Casi el total de los sujetos manifestaron desconocimiento acerca de los mouseloggers porque responden equivocadamente.

Gráfico Nº 4.5- Virus informáticos existentes

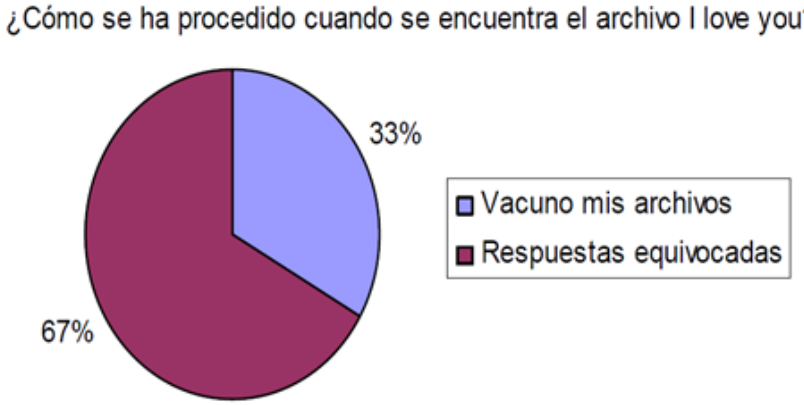


Como puede observarse más de las ¾ partes de los colaboradores no conoce uno de los virus más importantes

Gráfico Nº 4.6 -Archivo w32/netsky-p

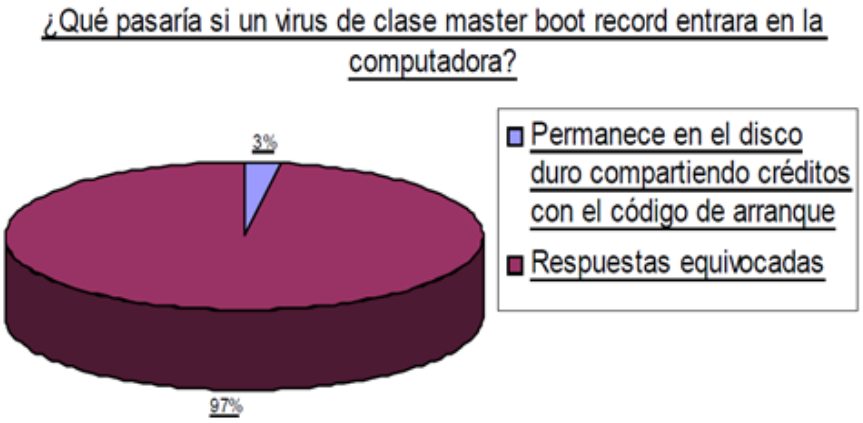
La mayoría de los colaboradores no han empleado un virus, esto quiere decir no haberlo ejecutado, con el propósito de conocer si sus respuestas son certeras.

Gráfico Nº 4.7 - Si conoce un virus informático, cómo se procede con el archivo I love you



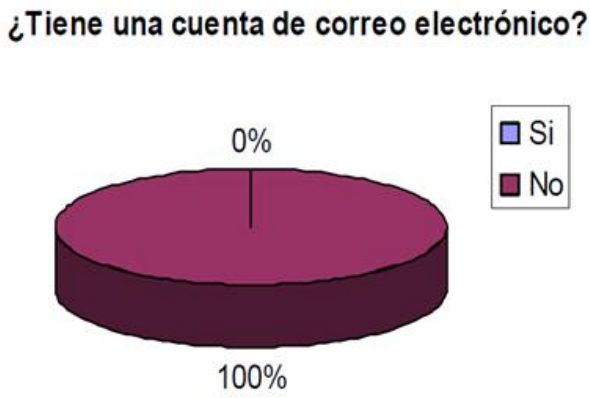
Casi una tercera parte de los colaboradores se equivoca, los demás si conocen una secuencia acorde al peligro.

Gráfico Nº 4.8- Virus de clase master boot record. (Alto riesgo)



Casi el 100% de los colaboradores se equivoca.

Gráfico Nº 4.9 - Cuenta con correo electrónico de la organización

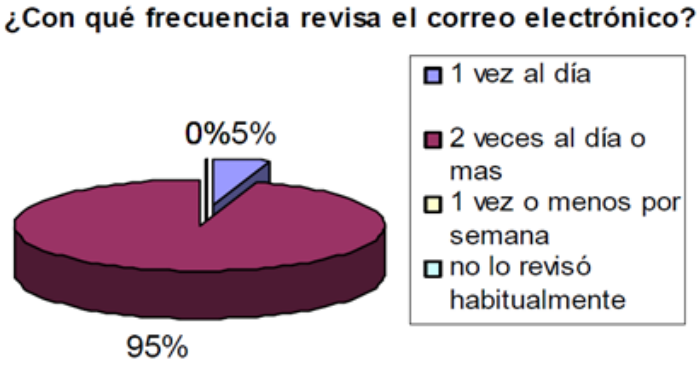


El 100% de los colaboradores estamos expuestos a un riesgo de punto final.

4.1.2. Para la categoría de riesgos en la eficacia del servicio de informática.

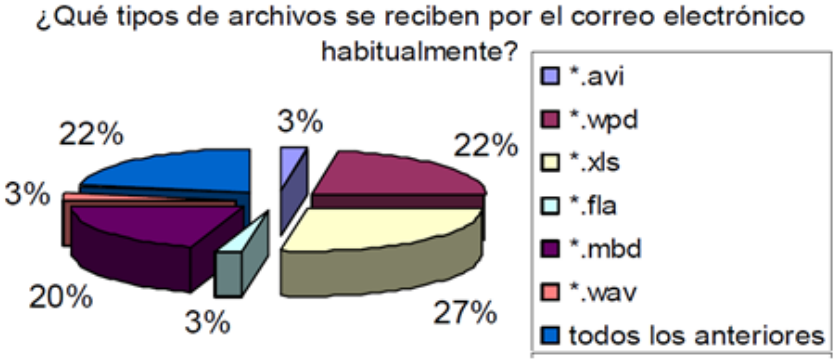
Las preguntas de la Nº 10 a la 25 se elaboraron para valorar el conocimiento del colaborador acerca de amenazas, dentro de esta categoría se establecieron indicadores que se relacionan con la continuidad del proceso porque también se consideró eran de mayor importancia por el alto riesgo que pueden ocasionar al usuario y en esta clasificación se tienen las siguientes preguntas con sus respectivas respuestas y gráficas.

Gráfico Nº 4.10 - Frecuencia con que se revisa el correo electrónico



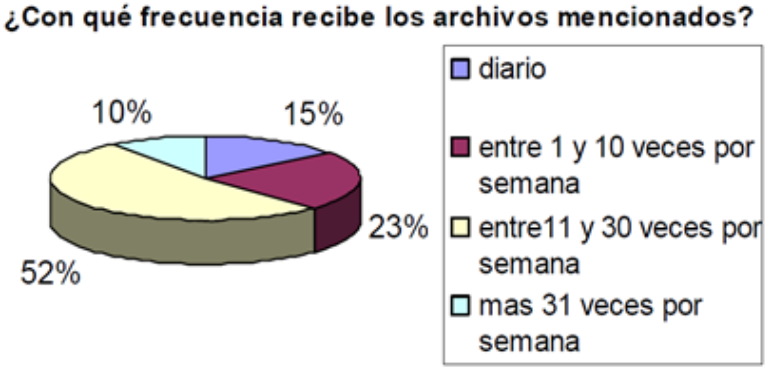
Casi el total de los respondientes revisa su correo continuamente para sus tareas y el 5% sólo lo revisa 1 vez al día.

Gráfico Nº 4.11- Tipos de archivos que habitualmente se reciben por el correo electrónico.



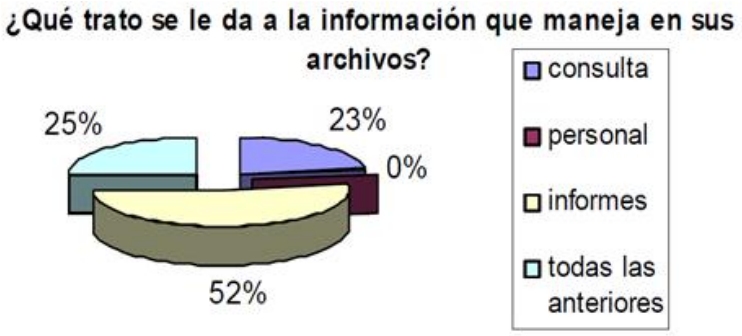
El 100% de los colaboradores realiza sus actividades con medios electrónicos de diversos software que tienen múltiples vulnerabilidades.

Gráfico Nº 4.12 - Frecuencia que se reciben los archivos mencionados



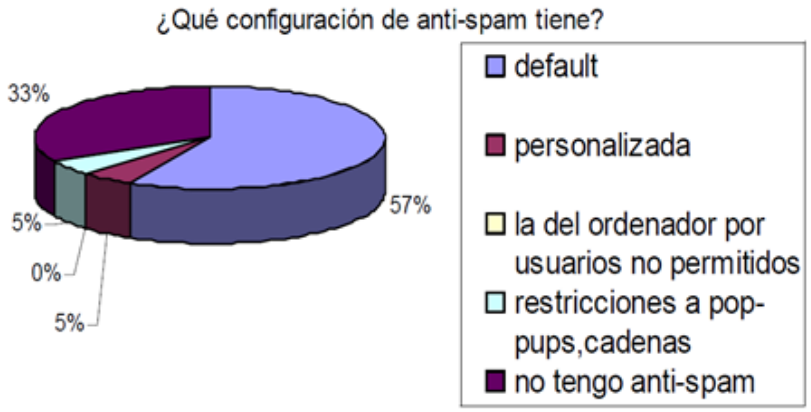
Los empleados reciben archivos con diferentes intervalos de variabilidad pero el más frecuente es el de 11 y 30 veces por semana.

Gráfico Nº 4.13- Enfoque de la información



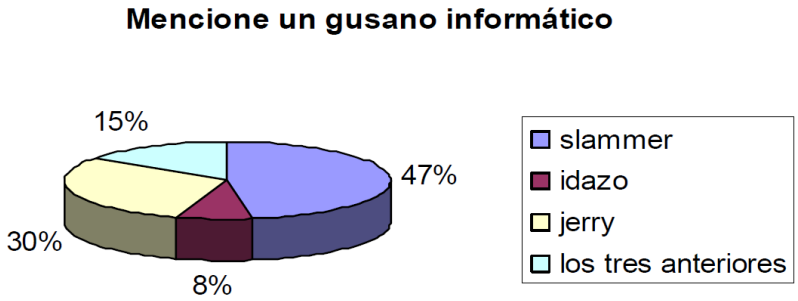
Un poco más de la mitad de los sujetos respondieron que la información de sus archivos es referente a informes.

Gráfico Nº 4.14 - Anti-spam. (Alto riesgo)



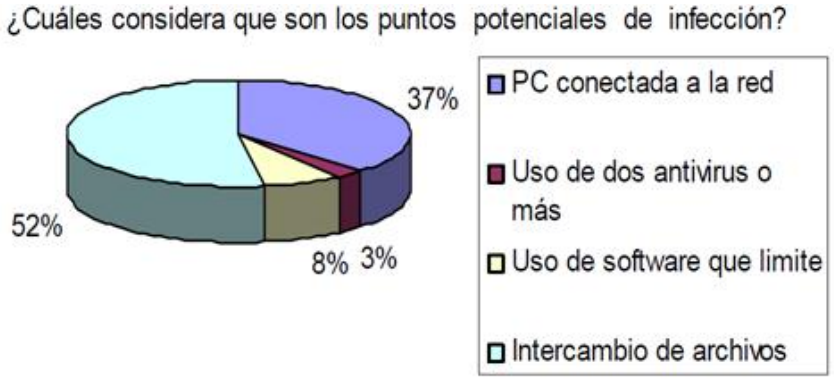
Más de la mitad de los colaboradores utiliza configuración default en el spam, un porcentaje mínimo con restricciones, el 0% personalizada, y un poco más de la cuarta parte respondió no tiene anti-spam.

Gráfico Nº 4.15- Conocimiento de gusanos informáticos. (Alto riesgo)



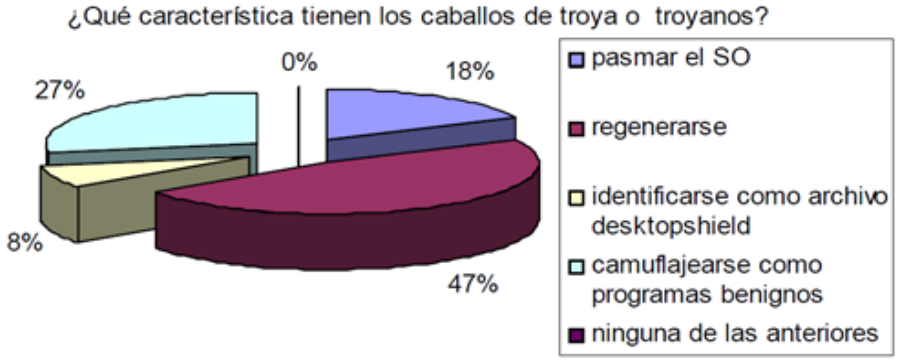
Al cuestionarlos acerca del conocimiento de los gusanos informáticos, menos del 10% de los colaboradores respondió afirmativamente.

Gráfico Nº 4.16 - ¿Conoce puntos potenciales de infección que representen peligro a su información? (Alto riesgo)



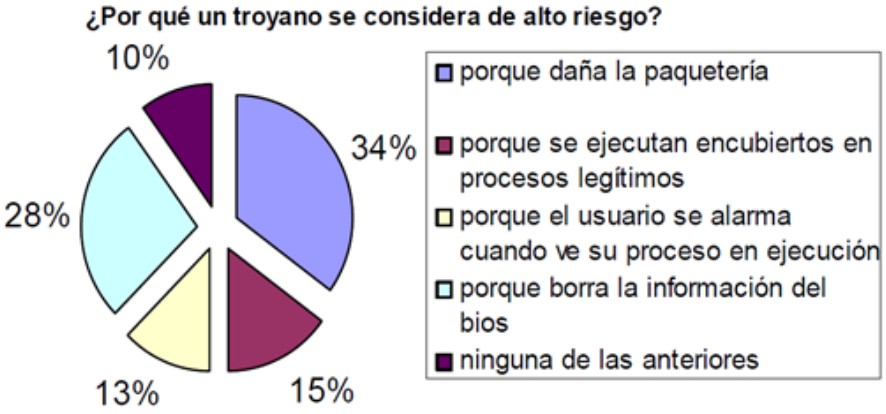
Más de la mitad de los colaboradores no tiene los suficientes cuidados para cuidar sus activos y los pone en riesgo.

Gráfico Nº 4.17- Características de los troyanos. (Alto riesgo)



Al analizar la siguiente gráfica, se observó que ¾ de los sujetos se equivocaron al identificar las características de los troyanos informáticos.

Gráfico Nº 4.18- ¿Por qué son un alto riesgo los troyanos?

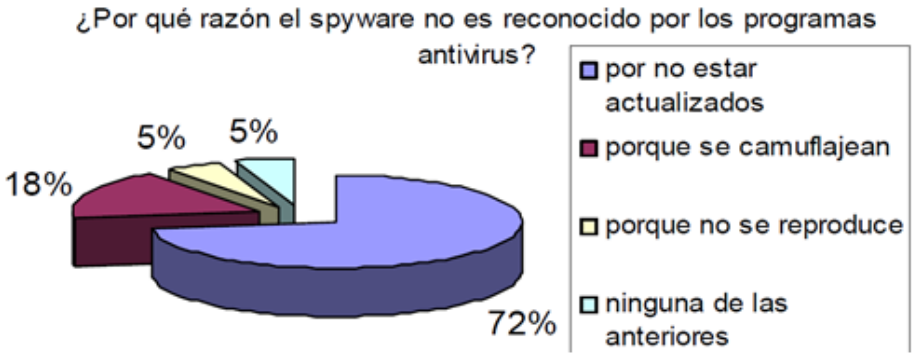


Al cuestionarlos acerca de las causas del riesgo de los troyanos, se pudo observar que el porcentaje de sujetos que se equivocaron es muy cercano al total.

Gráfico Nº 4.19- Contramedidas para troyanos

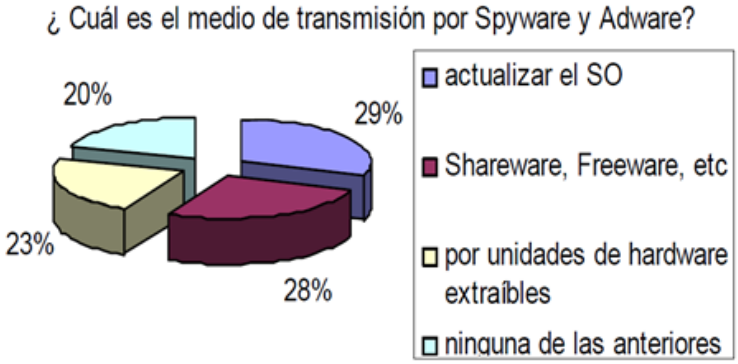
Analizando las respuestas acerca de las contramedidas para los troyanos se puede ver que hay un porcentaje sumamente grande de error en las contestaciones.

Gráfico Nº 4.20- Porque no es reconocido el spyware. (Alto riesgo)



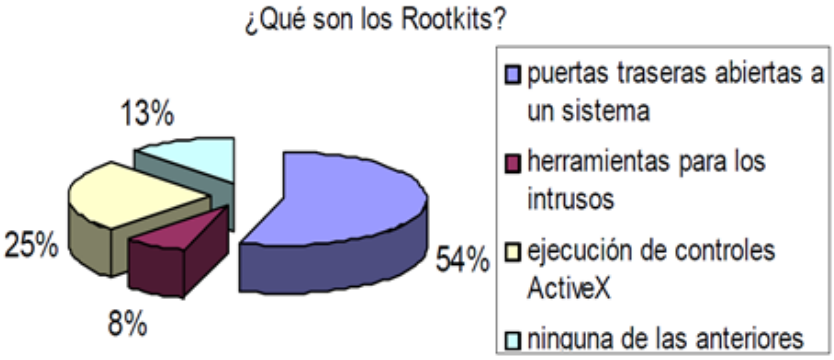
Casi la totalidad, menos 5% de los sujetos que respondieron el cuestionario, ignoran que el spyware no se reproduce como los virus.

Gráfico Nº 4.21- Medio de transmisión de spyware y Adware



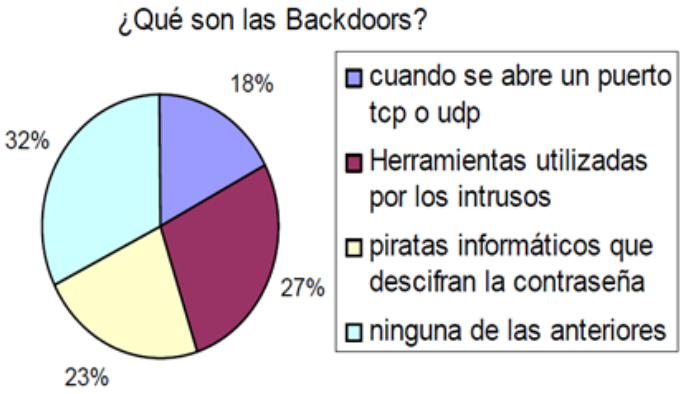
Una cantidad considerable cercana al 75% de colaboradores desconoce el medio de transmisión del spyware y Adware.

Gráfico Nº 4.22 - Rootkits. (Alto riesgo)



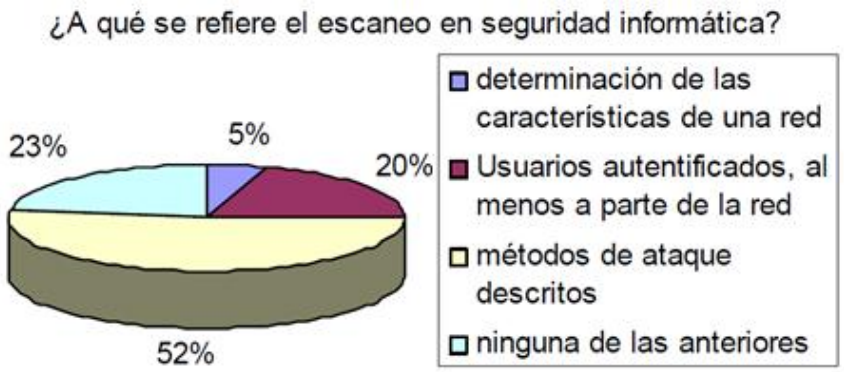
Casi la totalidad de los sujetos desconoce las herramientas de intrusos llamadas rootkits, las cuales son de alto riesgo por que toman el control de la terminal de punto final sin que el usuario se dé cuenta.

Gráfico Nº 4.23- Backdoors. (Alto riesgo)



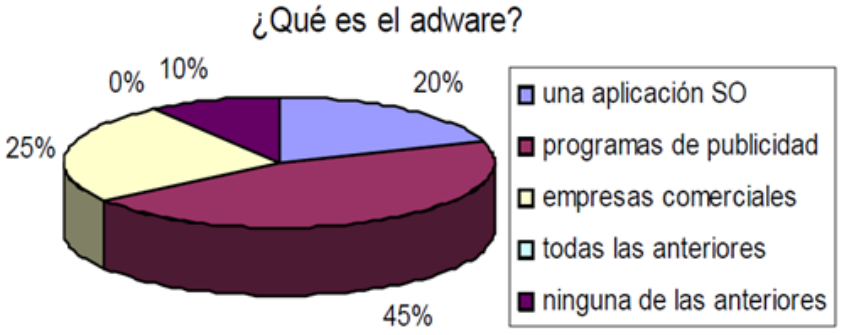
Más de la tercera parte respondió erróneamente al contestar de las amenazas por backdoors, siendo éstas de alto riesgo para cualquier usuario en la empresa.

Gráfico Nº 4.24- Escaneo en seguridad informática. (Alto riesgo)



Una cantidad mínima de 5%, conoce el concepto de determinación de las características de una red con el objetivo de identificar los equipos disponibles y alcanzables desde Internet.

Gráfico Nº 4.25- Adware



Sólo el 10% de los sujetos respondieron saber que se conoce como adware.

4.2. Caso práctico

4.2.1. Inserción de un keylogger para obtener información confidencial

Como parte del tema de estudio, se realizó un ataque de ingeniería social a la Municipalidad Distrital de Independencia, para analizar cuál es la manera de realizar un ataque, los pasos que se siguen, las herramientas que se utilizan, los métodos a través de los cuales se puede atacar; a continuación son descritos los pasos que realizaron y las herramientas que se usaron para alcanzar el objetivo.

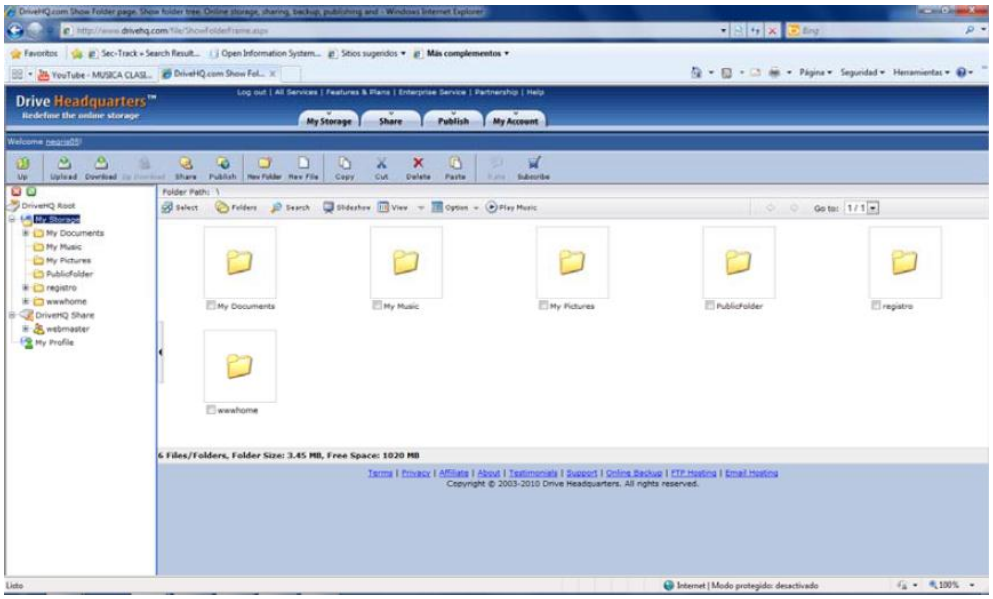
Los pasos que se siguieron para realizar este ataque fueron:

- Buscar un servidor FTP o de correo.
- Buscar un keylogger que cumpla con el objetivo planteado y pueda enviar los logs guardados de alguna manera, en este caso vía FTP o de correo.
- Configurar el keylogger y se crea el instalador.
- Generae un solo archivo, entre el keylogger y una imagen cualquiera para enviárselo a la víctima.
- Cambiar la imagen del archivo para que no sea sospechoso.
- Guardar este archivo en un cd.
- Crear una carta con una excusa convincente hacia la víctima para que use el cd y se ejecute el keylogger.
- Recibir y revisar los logs generados.

Todos estos pasos se describen a detalle en las siguientes páginas.

Lo primero que se debe hacer es buscar un servidor FTP o configurar un correo electrónico como dicho medio; actualmente existen varios en la Web, para este caso se utilizó el servidor drivehq.com; en este lugar, se llenan los datos para completar el registro, como se realiza para crear un correo gratuito o una suscripción cualquiera. Una vez creada la cuenta, se puede encontrar varias carpetas, en las que se puede compartir toda clase de información.

Gráfico Nº 4.26 - Servidor FTP



Con el fin de manejar de una manera más fácil y ordenada los logs que se van a generar con el keylogger, se creó una carpeta “registro”, lugar en el cual se guardarán los archivos enviados remotamente.

Después de haber creado la cuenta en el servidor FTP, se descarga un keylogger que pueda administrarse de manera remota, en este caso se utilizó el Ardamax 4.6; una vez descargado se lo instala en la máquina

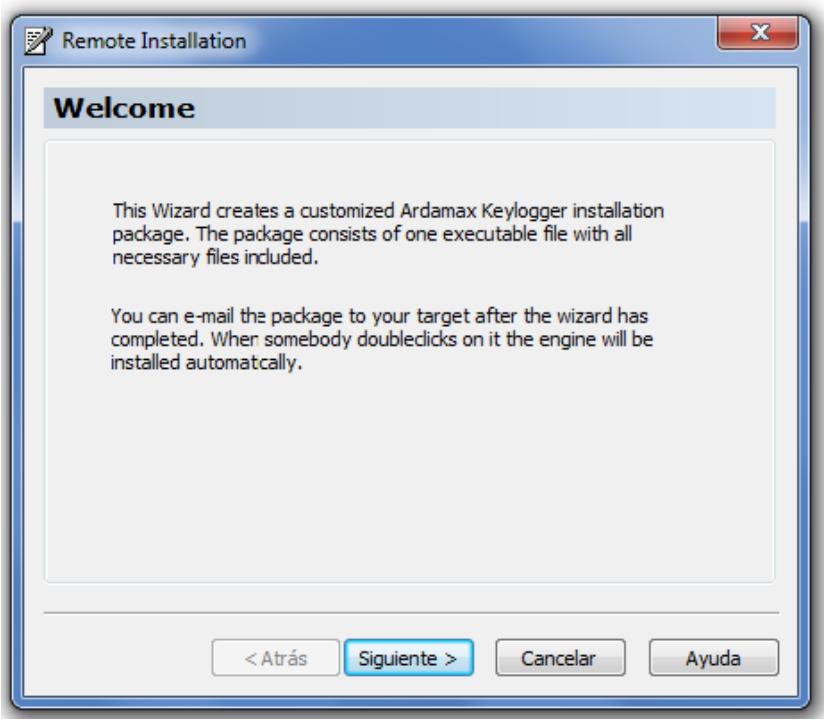
en la que se va a crear el instalador para la víctima; la instalación del mismo se realiza a través de un wizard como cualquier programa.

Una vez instalada o configurada la herramienta, se registra el programa con la clave y el usuario que viene cuando realizamos la descarga; en caso de no realizar este registro no se lo podrá usar de manera remota.

Cuando está registrado el keylogger, se procede a configurar el instalador que actúa de manera remota, se hace de la siguiente manera:

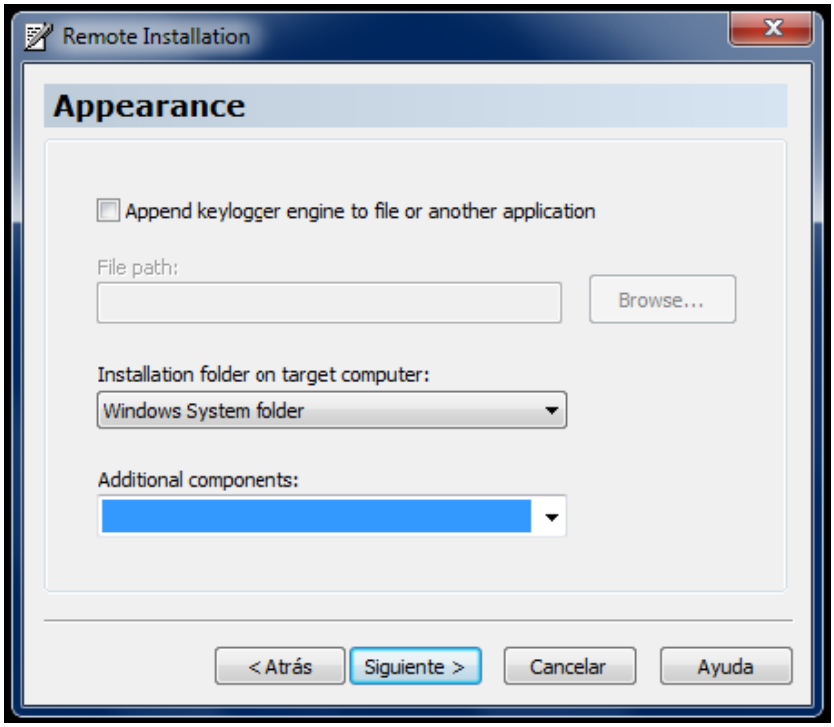
1. Click derecho en el ícono de Ardamax y se escoge la opción de Remote Installation o Instalación Remota, la primera pantalla que aparece es la bienvenida, en la que se explica que este wizard crea un paquete de instalación personalizado; éste da como resultado un archivo ejecutable con todos los archivos necesarios incluidos e indica que este paquete o instalador puede ser enviado por e-mail una vez que se ha completado el wizard y cuando alguien presione doble click sobre este se instalará automáticamente.

Gráfico Nº 4.27 - Inicio de instalación Ardamax



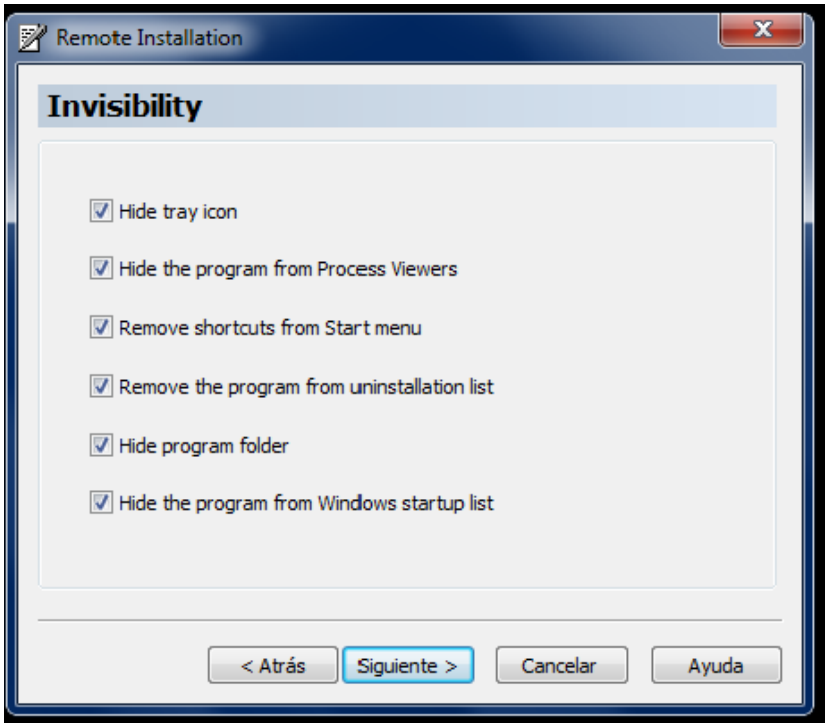
2. La siguiente pantalla muestra en la carpeta en la que se instalará el keylogger y se puede escoger si se desea componentes adicionales, sin embargo, es mejor no escoger ningún componente adicional para que el keylogger tenga mejor efectividad y no sea detectado.

Gráfico Nº 4.28 - Carpeta de instalación de keylogger



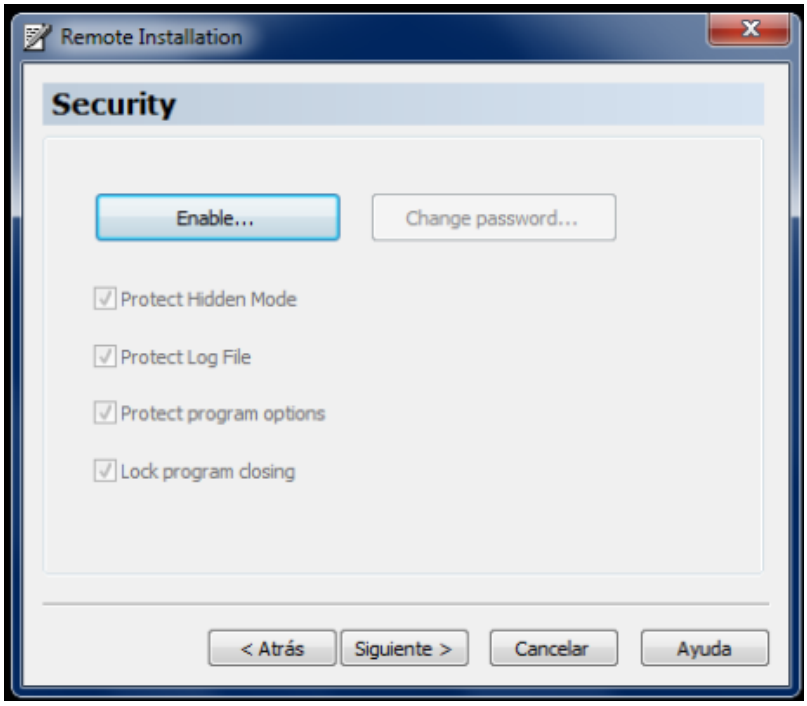
3. En la tercera pantalla se puede escoger las opciones de invisibilidad con las que se desea instalar el keylogger; lo óptimo es poner un check en todas las opciones para que sea completamente invisible e indetectable.

Gráfico Nº 4.29 - Invisibilidad del keylogger



4. En la cuarta pantalla se encuentra la seguridad del keylogger, es decir aquí se puede habilitar una contraseña para abrir los archivos o logs que serán generados por el keylogger, en caso de habilitar la contraseña existen varias opciones de lo que va a ser protegido con la misma.

Gráfico Nº 4.30 - Clave de seguridad del keylogger

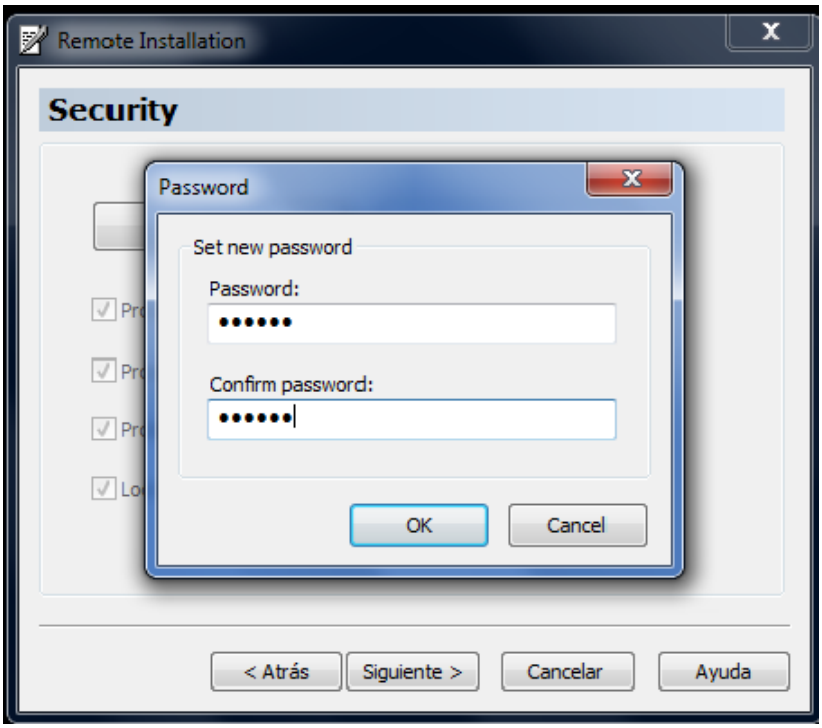


5. En la quinta pantalla se habilita la contraseña para los logs, archivos, vistas, etc.

Gráfico Nº 4.31 - Configuración de contraseña

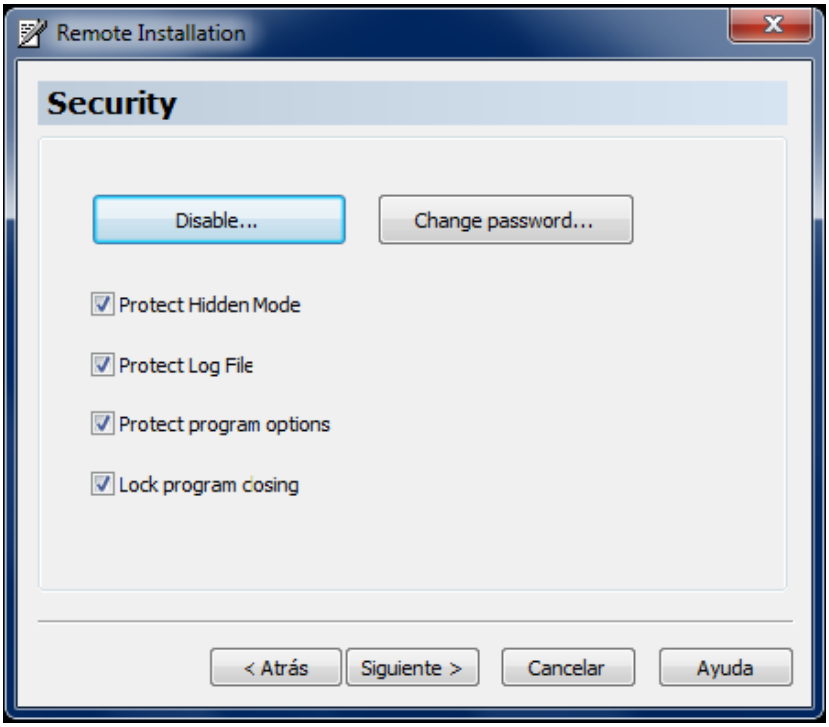
6. Se escribe la contraseña y se la confirma.

Gráfico Nº 4.32 - Confirmación de contraseña



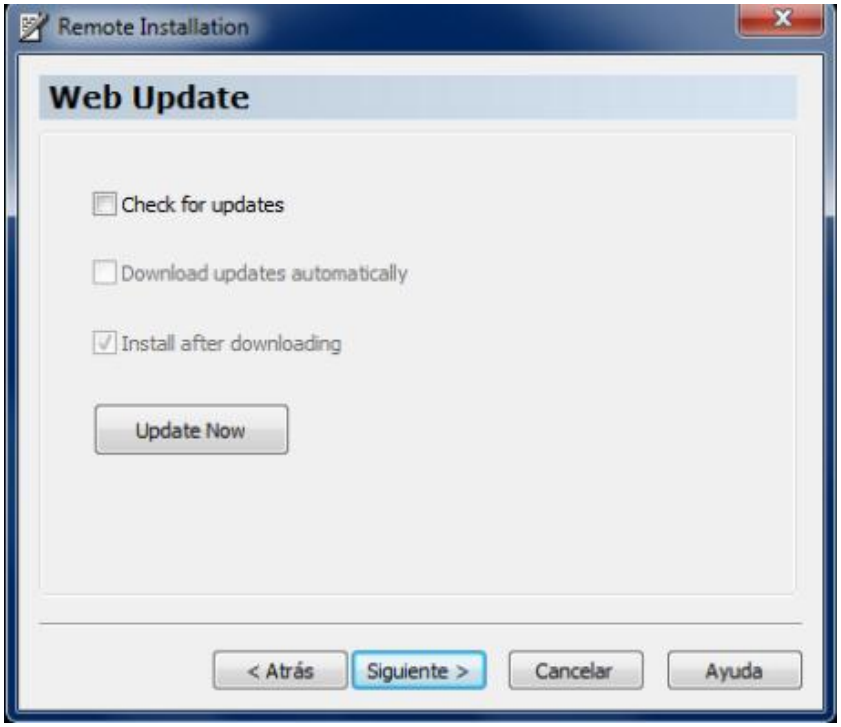
7. Una vez habilitada la contraseña existe la opción de deshabilitarla o cambiarla y seleccionar qué es lo que va a proteger la nueva contraseña.

Gráfico Nº 4.33 - Opciones de seguridad del keylogger



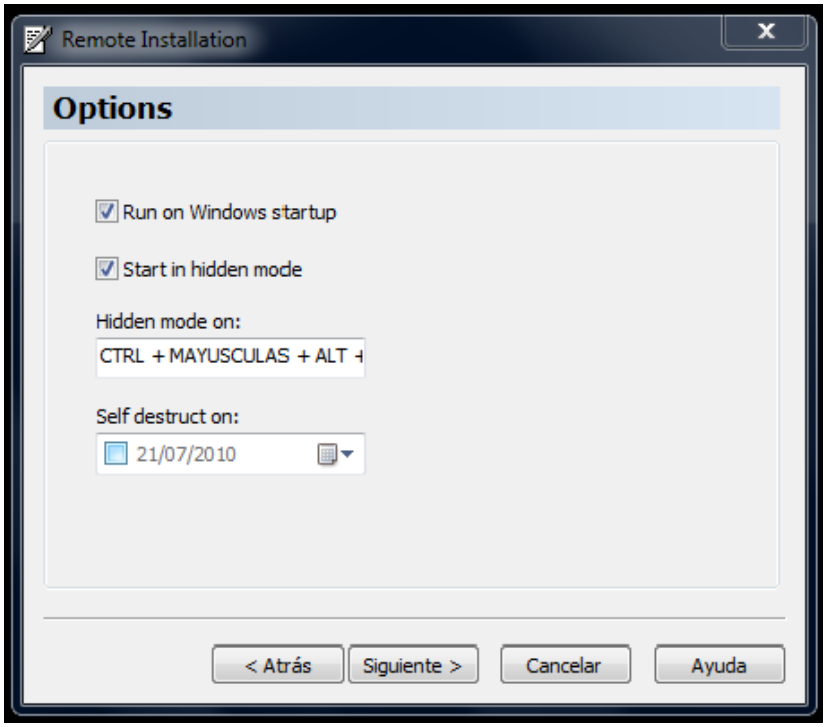
8. En la pantalla de actualizaciones Web, se puede escoger: si se desea que busque actualizaciones, que se actualice automáticamente o que se actualice en ese momento; pero lo recomendable es no seleccionar ninguna de ellas, para que no sea detectado en el momento de realizar dichas actualizaciones.

Gráfico Nº 4.34 - Actualizaciones de keylogger



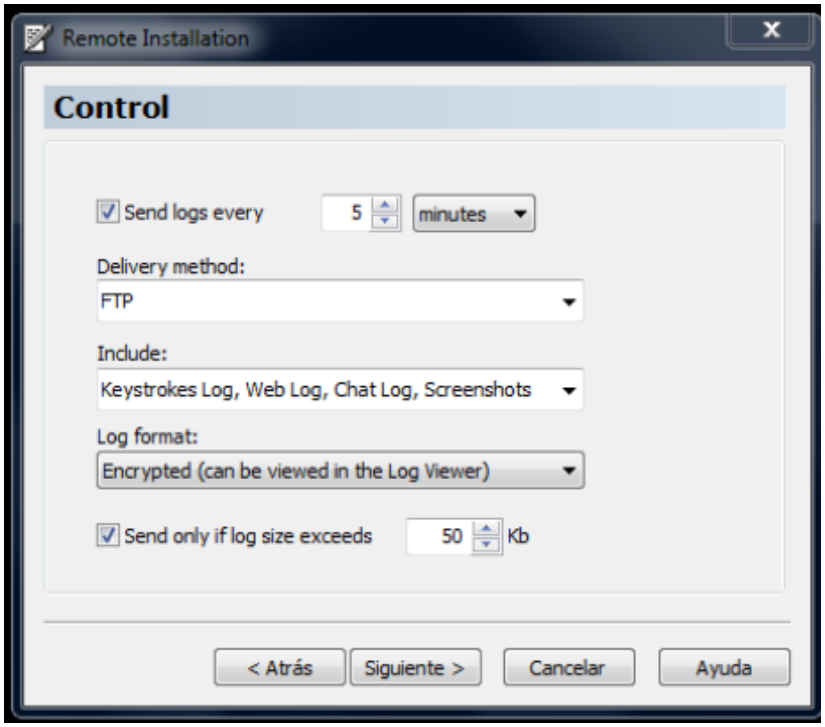
9. En las siguientes opciones se puede seleccionar si se desea que inicie cuando se arranca Windows, que inicie en modo escondido, indica cuáles son las teclas que se deben presionar para poder ingresar al keylogger cuando inicia en modo escondido e indica la opción también de que se autodestruya y en qué fecha. Lo recomendable es que inicie cuando inicia Windows y que lo haga en modo escondido.

Gráfico Nº 4.35 - Opciones de inicio del keylogger



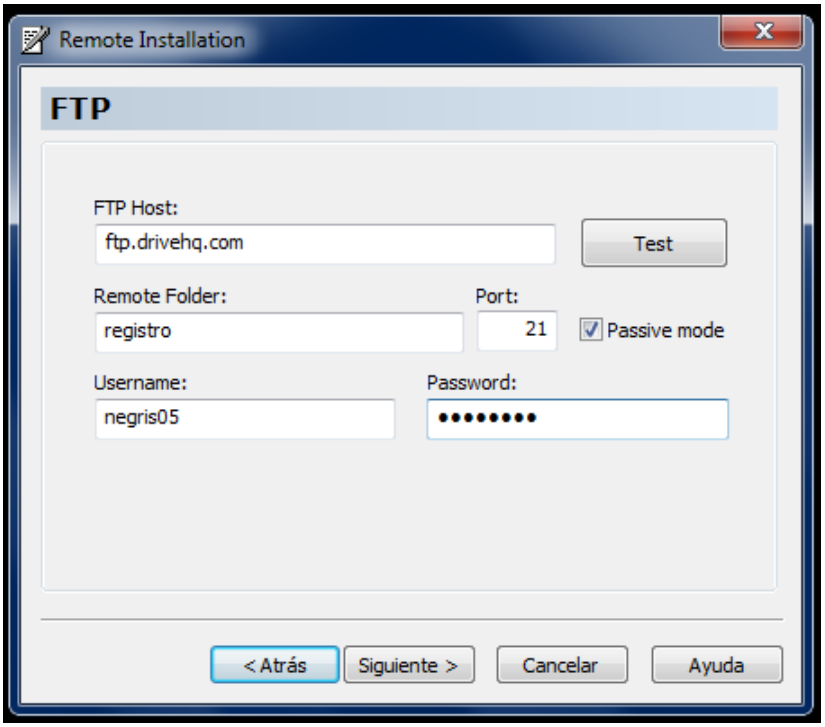
10. En la siguiente pantalla se debe configurar cada cuanto tiempo se desea que sean enviados los logs, el método de entrega, es decir, si se quiere que sea por correo electrónico, vía FTP, etc., o se puede combinar las formas de entrega; en este caso se entregarán en un servidor FTP. Se puede escoger lo que se desea capturar; las pulsaciones, los sitios Web visitados, los chats, las pantallas; se puede escoger el formato del log, puede ser en formato Web o encriptado, de manera que puede ser visualizado únicamente en el visor de logs de Ardamax; y por último se puede escoger el peso mínimo de los logs para que sean enviados.

Gráfico Nº 4.36 - Opciones de envío de logs



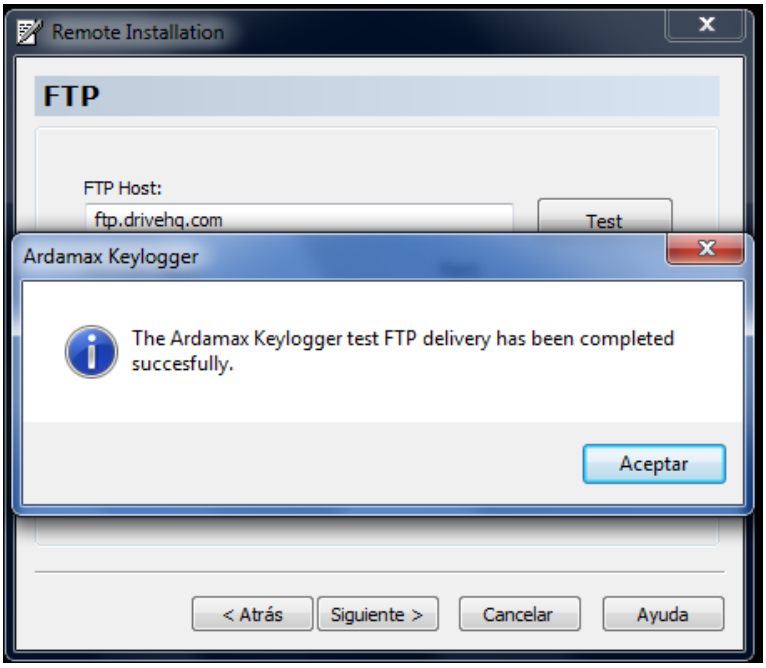
11. Ahora según el caso se debe configurar donde se realizará la entrega de los logs, en este caso es configurado el servidor FTP. Para iniciar se ingresa la dirección del host a donde se enviarán los archivos; se ingresa el nombre de la carpeta donde se los guardará, el puerto mediante el cual se ingresa en el servidor y se pone el nombre y la contraseña del servidor FTP. Para comprobar que se reciban los logs existe la opción de realizar un test o prueba.

Gráfico Nº 4.37 - Datos del servidor FTP



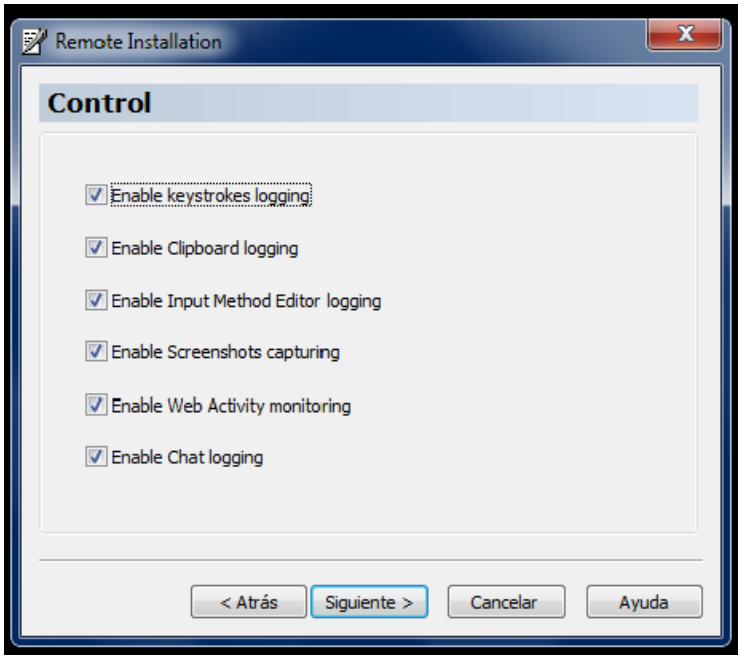
12. Una vez realizado este test, el keylogger despliega una pantalla en la que indica que la entrega de prueba fue exitosa, por lo que los logs llegarán correctamente.

Gráfico Nº 4.38 - Prueba de conexión con el servidor FTP exitosa.



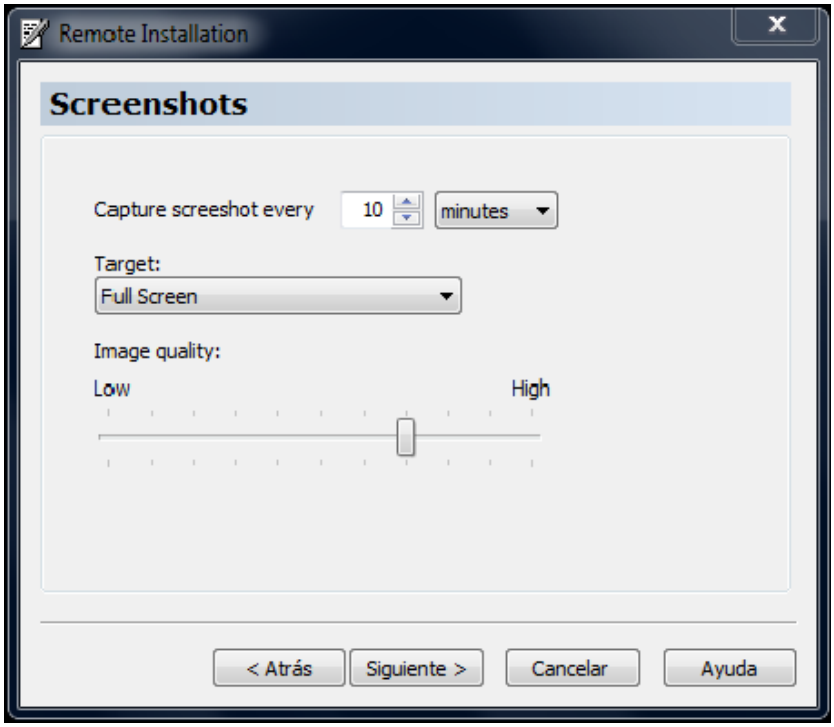
13. Después se puede escoger que es lo que va a estar habilitado para los logs; en este caso se seleccionan todas las opciones para ver qué información podemos obtener.

Gráfico Nº 4.39 - Opciones de lo que capturará el keylogger



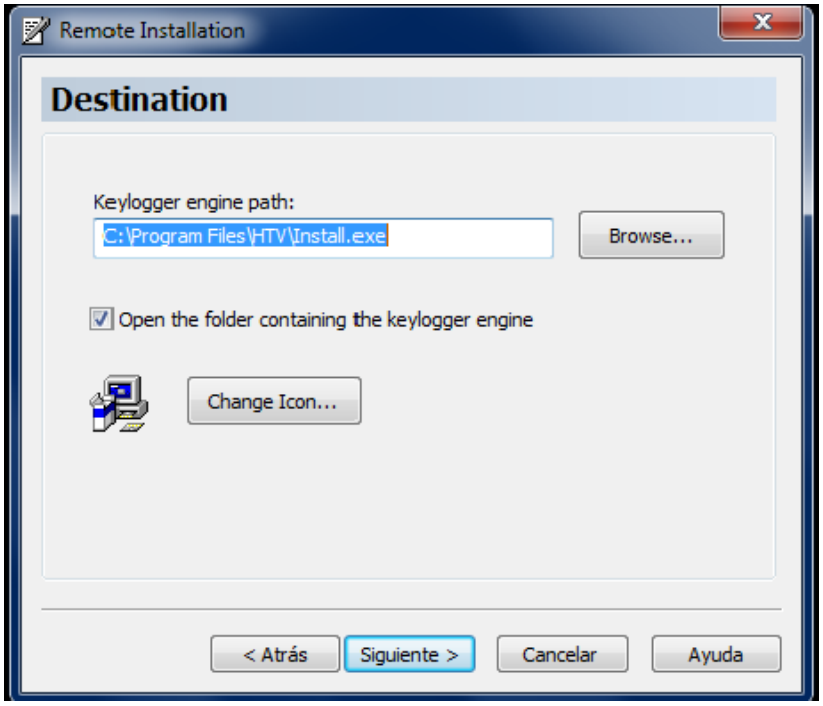
14. Si se desea capturar pantallas, se puede definir el tiempo entre cada captura, se puede definir si se requiere la pantalla completa y la calidad de la imagen.

Gráfico Nº 4.40 - Opciones de captura de pantalla



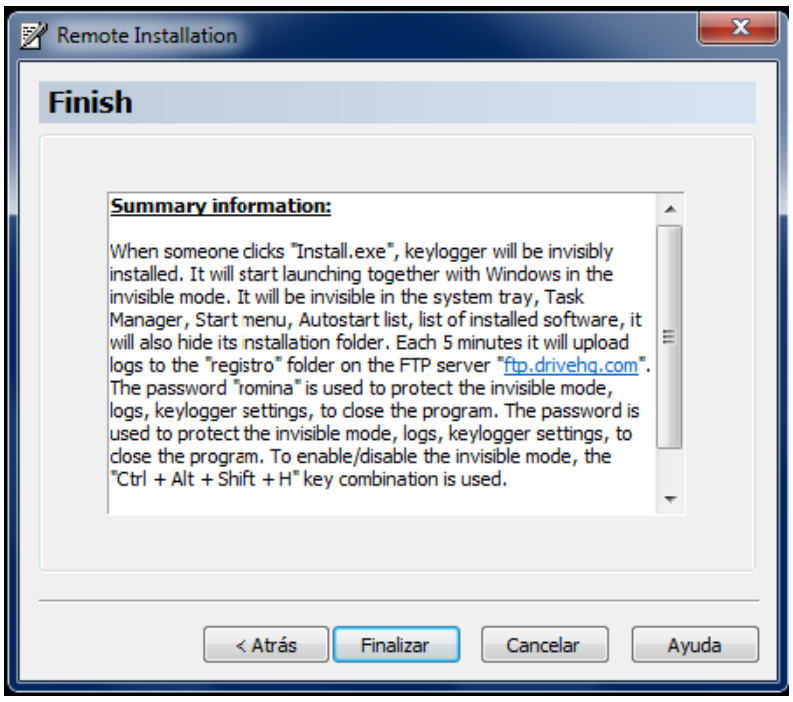
15. Luego de configurar todas las opciones antes mencionadas, se debe indicar dónde se va a crear el archivo de instalación y para evitar sospechas en la víctima podemos cambiar el ícono con el que va a ser creado el instalador.

Gráfico Nº 4.41 - Carpeta donde se creará el instalador



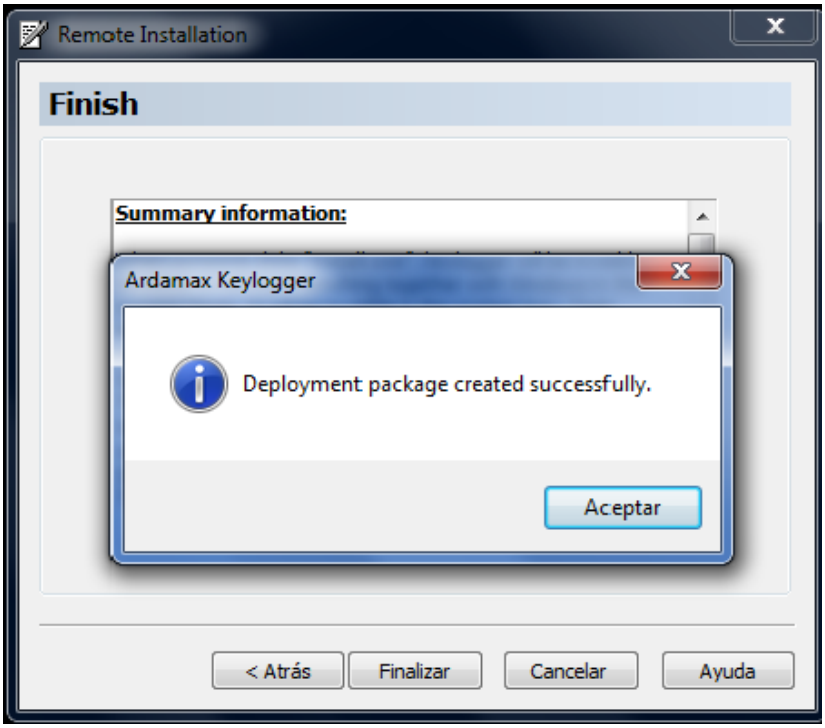
16. Aparece una pantalla de resumen del keylogger, antes de indicar que el instalador fue creado.

Gráfico Nº 4.42 - Resumen del keylogger



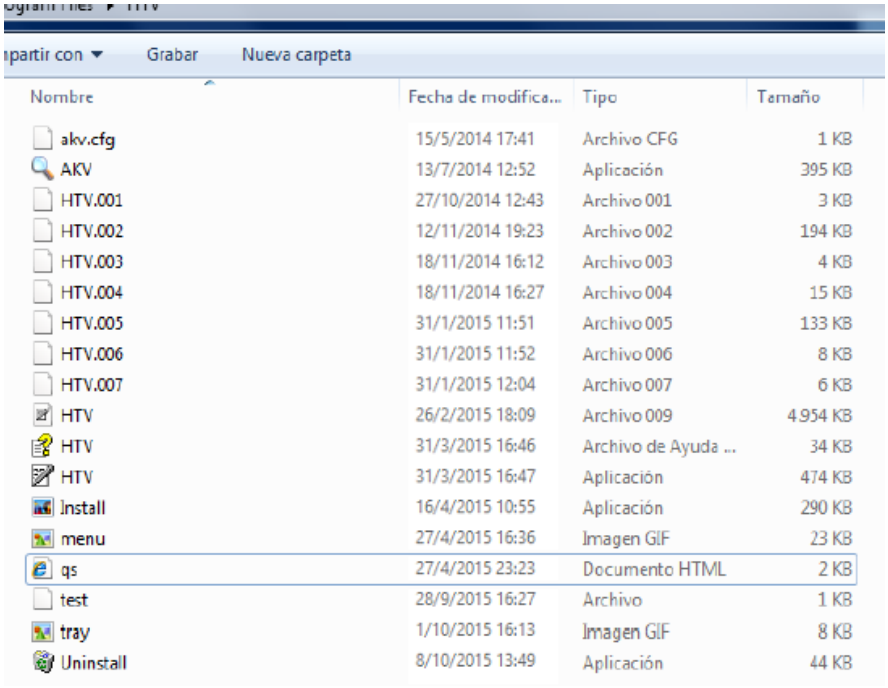
17. Por último, despliega una pantalla con un mensaje indicando que el paquete o instalador fue creado exitosamente.

Gráfico Nº 4.43 - Creación del instalador satisfactoria



18. Aquí se puede observar con el ícono de una imagen el archivo Install, con el cual se generará el ataque.

Gráfico Nº 4.44 - Instalador creado



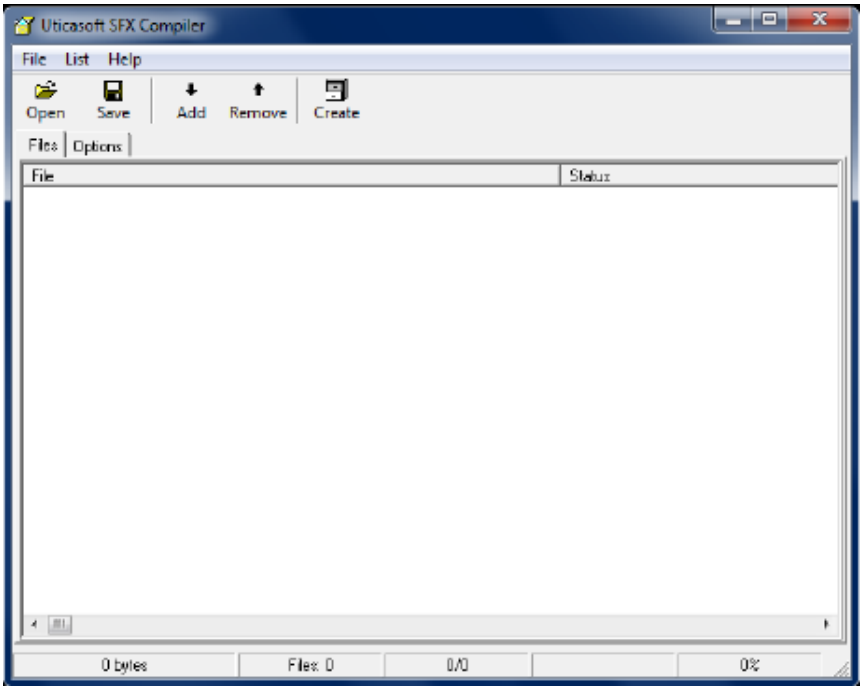
Una vez creado el instalador del keylogger se lo unió a una imagen, de manera que, al momento que la víctima abrió el archivo, puede observar una imagen común y automáticamente se instaló el keylogger en un segundo plano sin levantar sospechas.

Para poder unir el keylogger a la imagen se necesita un programa que lo haga, en este caso se utilizó el programa Uticasoft SFX Compiler[40]; el procedimiento a seguir para crear un solo archivo es el siguiente:

Se abre el programa y despliega esta pantalla, en la que se abren los archivos que se desea unir.

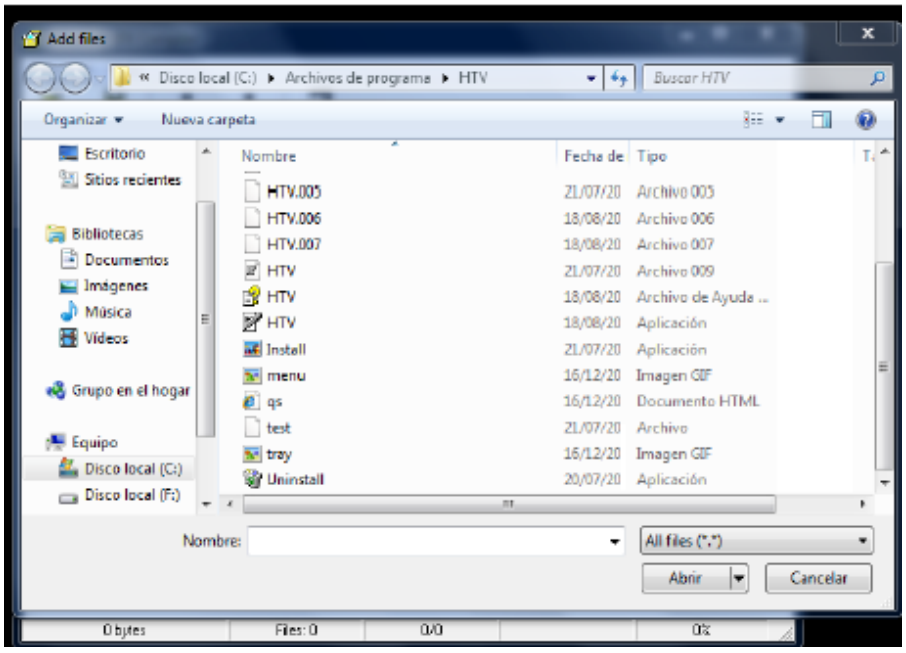
[40] Programa con licencia gratuita, creado por Jobin Rezai.

Gráfico Nº 4.45 - Inicio compilador de archivos



Se añaden los archivos uno por uno, para este caso el instalador.

Gráfico Nº 4.46 - Añadir instalador de keylogger

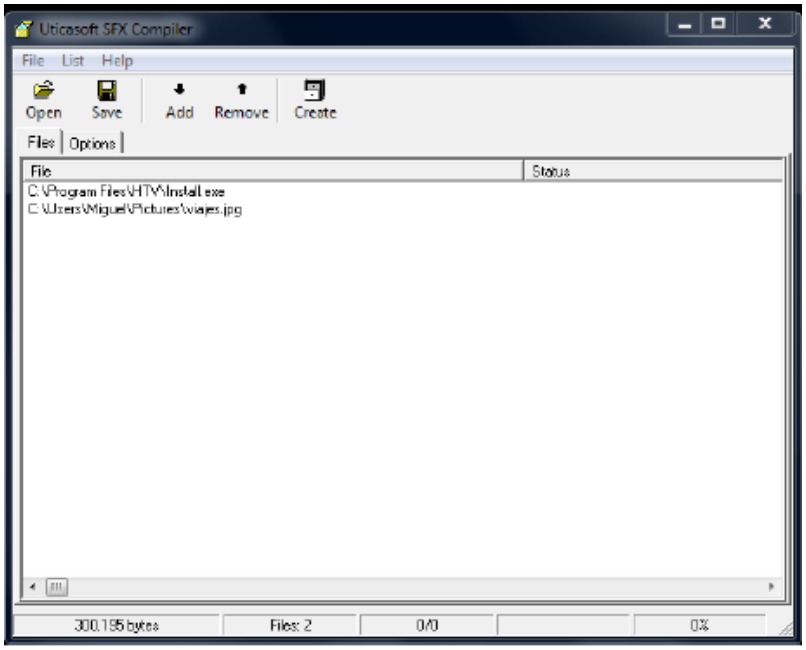


Se añade el siguiente archivo, es decir, la imagen.

Gráfico Nº 4.47 - Añadir imagen

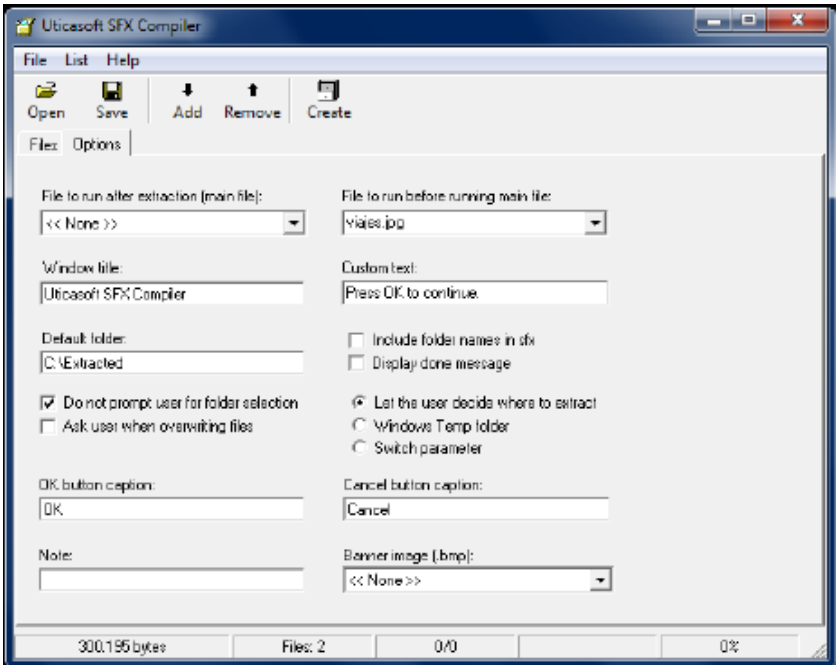
En esta pantalla se puede observar que los archivos fueron abiertos y están listos para ser unidos, pero antes, deben ser configuradas las opciones de orden de ejecución de los archivos.

Gráfico Nº 4.48 - Archivos que serán compilados



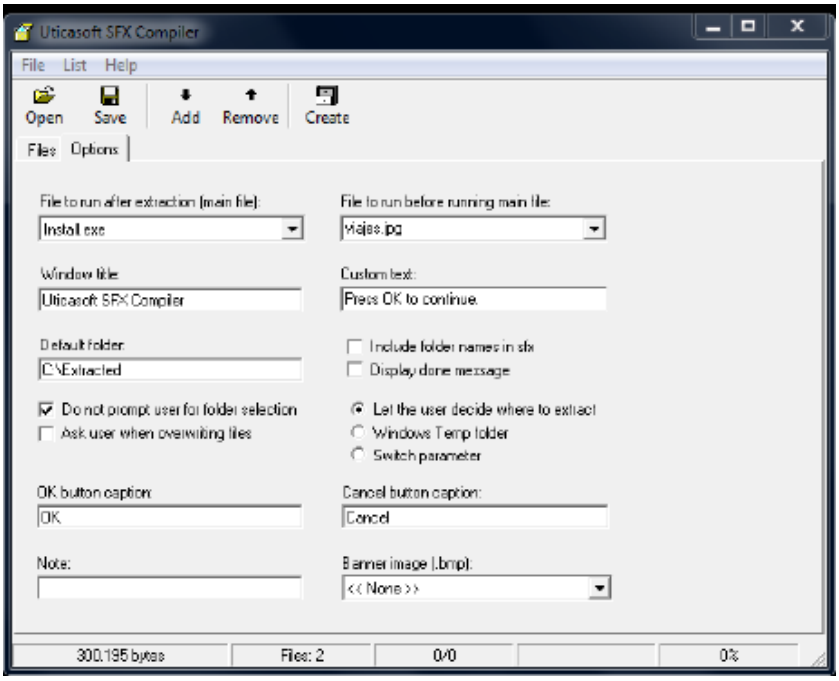
En la pestaña Options se puede escoger que archivo se desea ejecutar primero y cual después de la extracción, existen más opciones, pero en este caso no serán utilizadas.

Gráfico Nº 4.49 - Opciones de ejecución



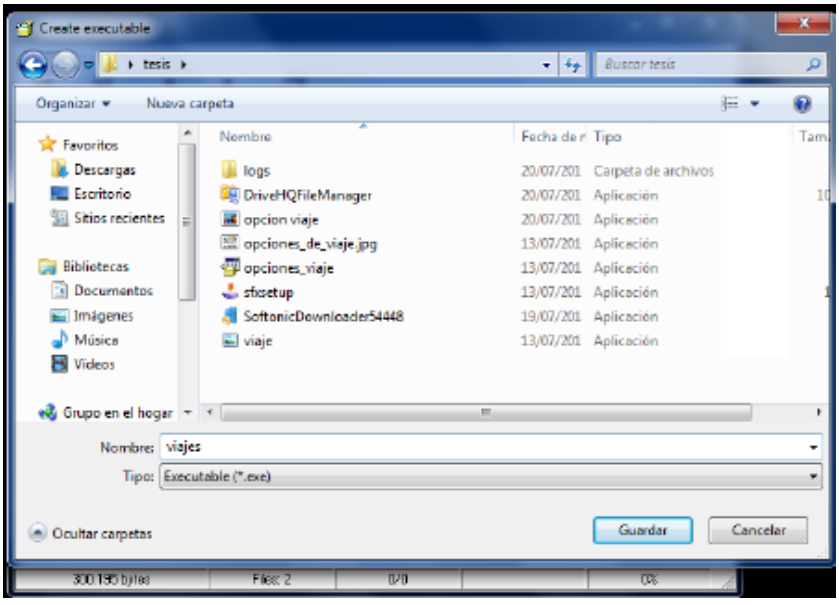
En base a las necesidades de este estudio, primero debe ejecutarse la imagen viajes.jpg y luego de la extracción el archivo Install.exe.

Gráfico Nº 4.50 - Archivo que se ejecuta primero



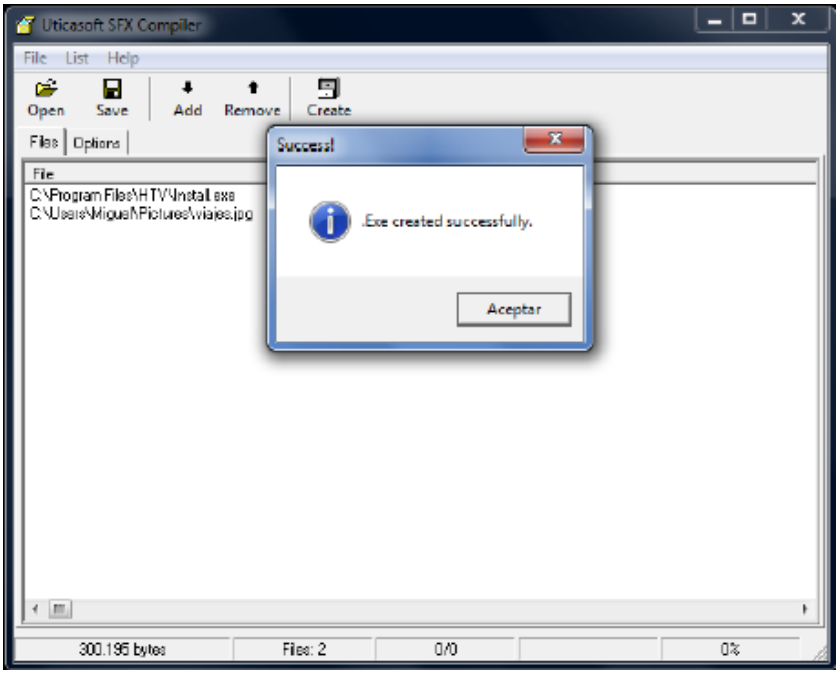
Se debe presionar el botón Create y escoger en donde se desea crear el archivo unido y que el nombre con el que lo vamos a identificar.

Gráfico Nº 4.51 - Carpeta de creación de archivo



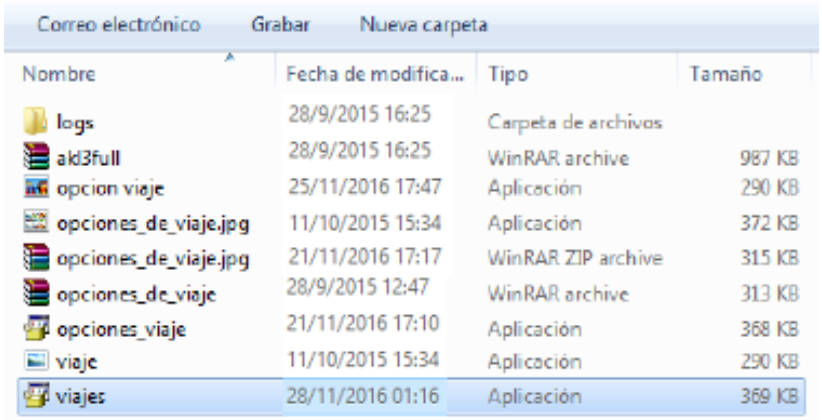
Se lo guarda y se despliega un mensaje en el que indica que el archivo fue creado exitosamente.

Gráfico Nº 4.52 - Creación exitosa



En esta lista de archivos, se puede observar el archivo viajes que fue unificado.

Gráfico Nº 4.53 - Archivo creado

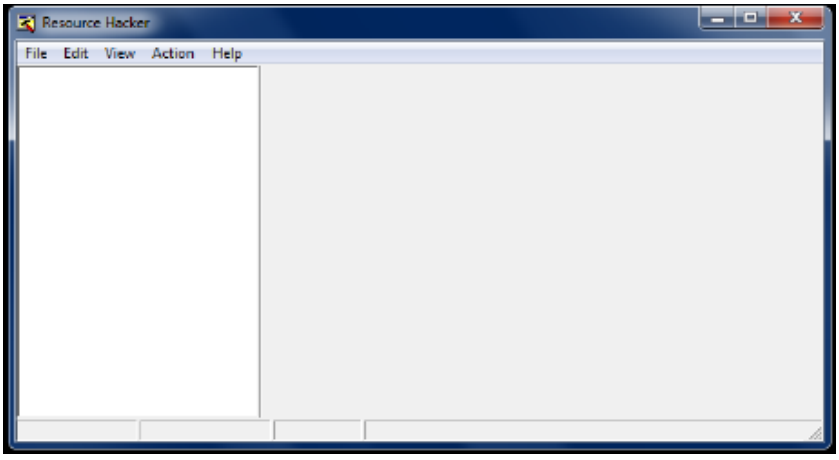


Cuando ya se ha unificado el instalador y la imagen, se obtuvo un solo archivo, el mismo que tiene el ícono de un archivo ejecutable, por lo que es probable que la víctima no se sienta segura de abrirlo. Para evitar este problema existe la opción de cambiar el ícono del archivo, de manera que parezca una imagen normal y no genere dudas en la persona que la va a abrir; para esto será utilizado otro programa; en este caso se usará el Resource Hacker[41].

El procedimiento para cambiar este ícono es el siguiente:

Se ejecuta el programa y aparece una pantalla en la que se abre el archivo del que se cambiará el ícono.

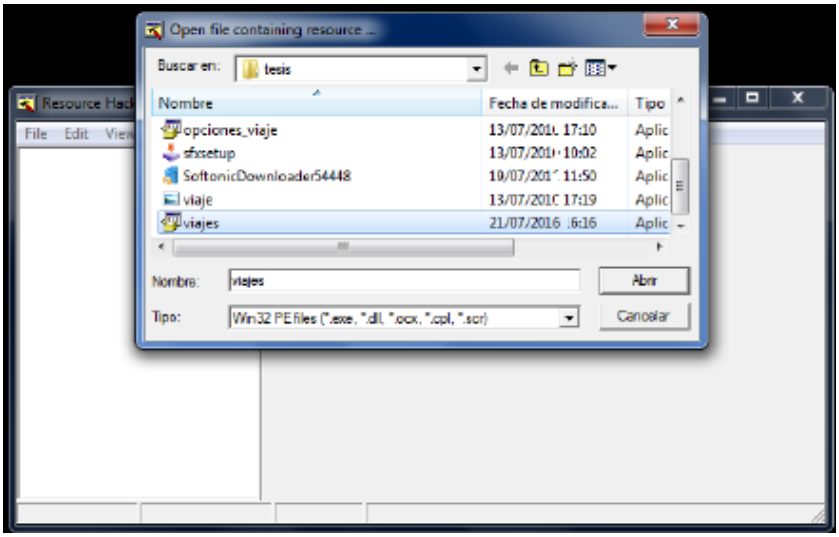
Gráfico Nº 4.54 - Inicio de Resource Hacker



Se abre el archivo viajes.

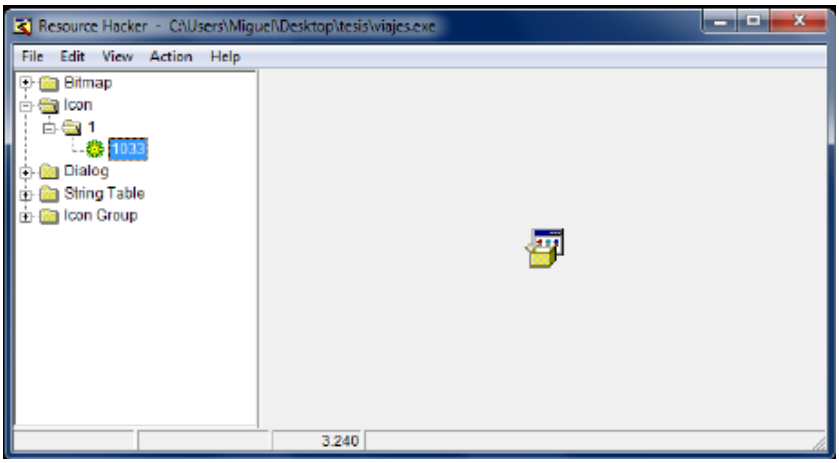
[41] Programa con licencia gratuita, creado por Angus Johnson.

Gráfico Nº 4.55 - Escoger el archivo



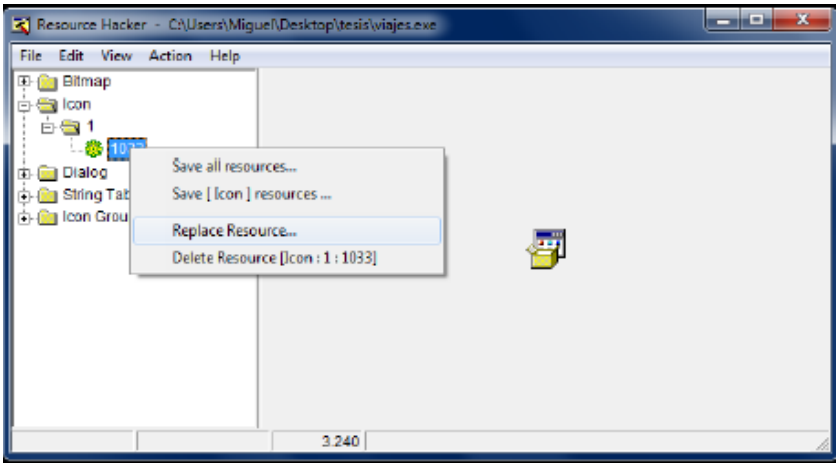
En la pantalla inicial aparecerán varias carpetas, dentro de estas existe una llamada Icon. Dentro de ésta se encuentra otra carpeta, la cual puede tener diversos nombres y dentro de la misma encontramos un archivo; si se le da click aparecerá la imagen del ícono que tiene actualmente el archivo.

Gráfico Nº 4.56 - Icono que se cambiará



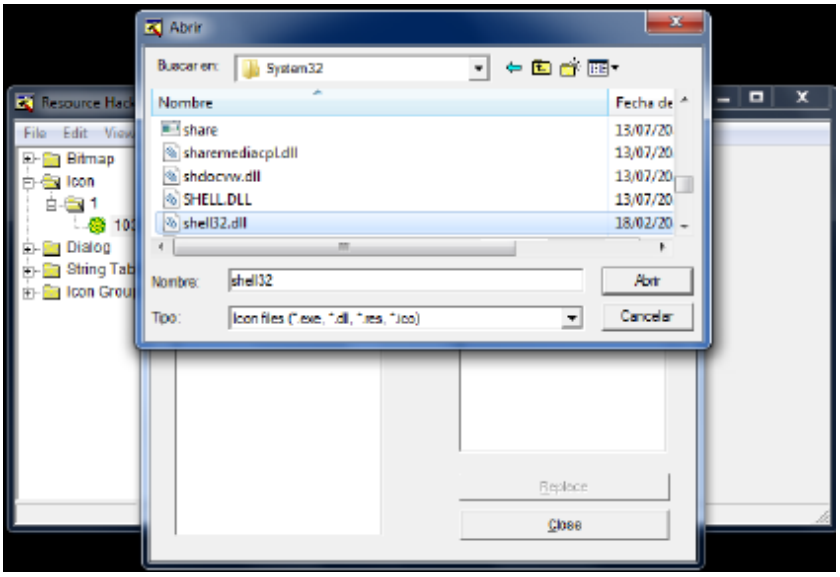
Se debe dar click derecho sobre ese archivo y seguidamente dar click sobre Replace Resource para cambiar la imagen del ícono.

Gráfico Nº 4.57 - Reemplazo de figura



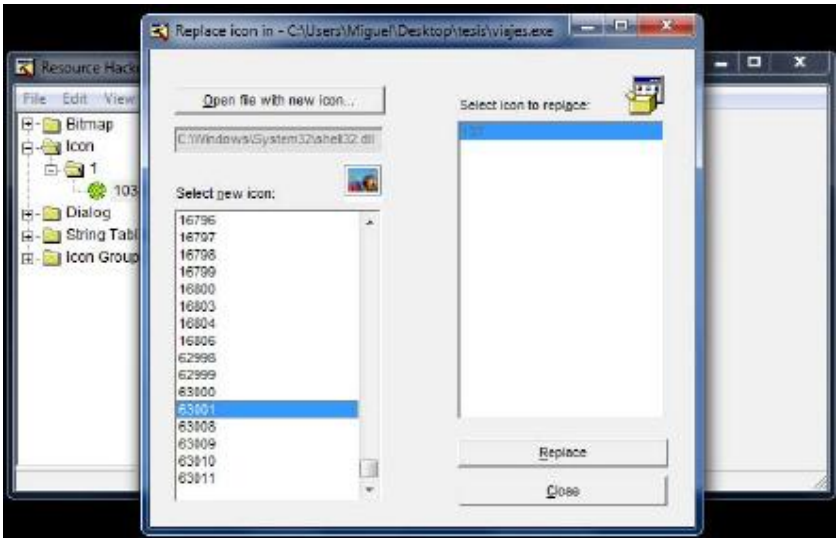
Aparece una pantalla en la que se debe abrir el archivo del cual se va a escoger la imagen que reemplazará la actual.

Gráfico Nº 4.58 - Archivo con íconos nuevos



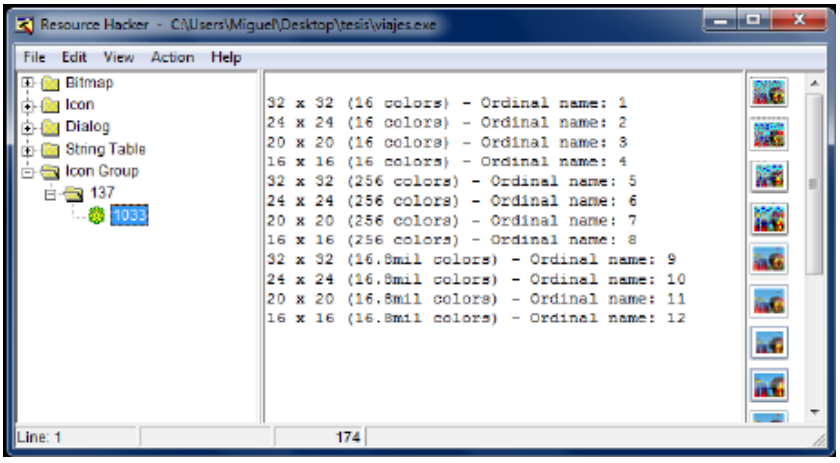
Si se ingresa en el archivo de los íconos de Windows, se puede escoger la imagen de un video, una imagen, etc.

Gráfico Nº 4.59 - Nuevo ícono del archivo



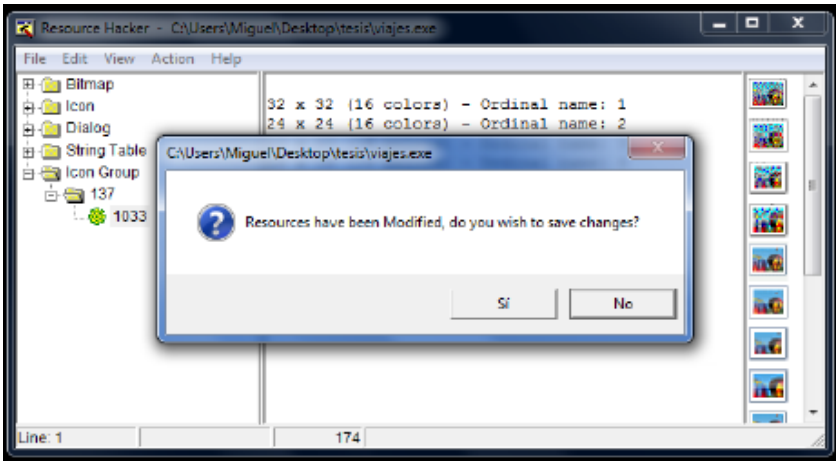
Una vez elegida la nueva imagen, se puede observar que cambia el dibujo anterior y que aparece el que se escogió.

Gráfico Nº 4.60 - Icono reemplazado



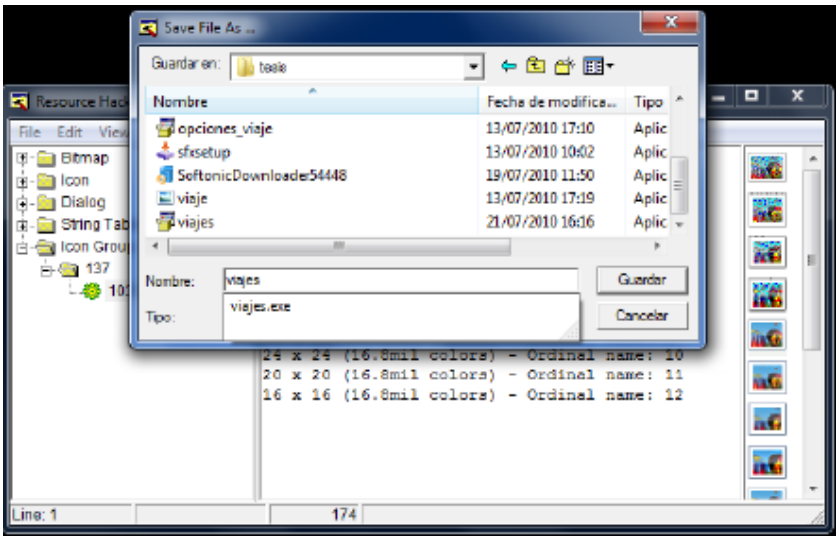
Se despliega una pantalla en la que pregunta si se desean guardar los cambios realizados en el ícono.

Gráfico Nº 4.61 - Guardar los cambios



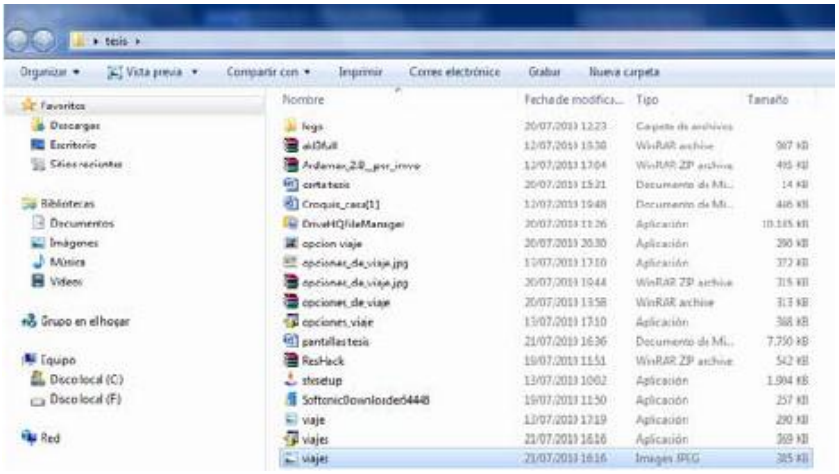
Se indica el lugar en el que se va a guardar el archivo con el nuevo ícono.

Gráfico Nº 4.62 - Carpeta destino



En esta pantalla observamos el archivo unificado ya con el ícono de una imagen normal.

Gráfico Nº 4.63 - Archivo con nuevo ícono



Una vez que se realizó todo el proceso antes mencionado y se tiene el instalador listo para que el usuario o víctima lo abra, se debe encontrar un método para que este archivo llegue a manos de la persona en cuestión sin sospechar de que se trata; en este caso la víctima es el asistente de planillas de la Municipalidad Distrital de Independencia.

La persona que lleva a cabo el ataque, tiene relación con la víctima; motivo por el cual, sabe que la víctima tiene dicho cargo. Al tener esta información, se grabó el archivo con el instalador del keylogger en un cd y se redactó una carta; en la que se indicaba que la víctima es ganador de un sorteo y el premio era un viaje y se le pedía que abra el archivo del cd para que escogiera el destino al cual deseaba viajar.

Es habitual que, estas promociones o premios atraigan mucho a la gente, que en la ciudad de Huaraz todavía es muy ingenua y no toma las precauciones adecuadas antes de dejarse llevar por este tipo de

engaños; de manera que, efectivamente esta persona abrió el archivo y se instaló el keylogger en su máquina.

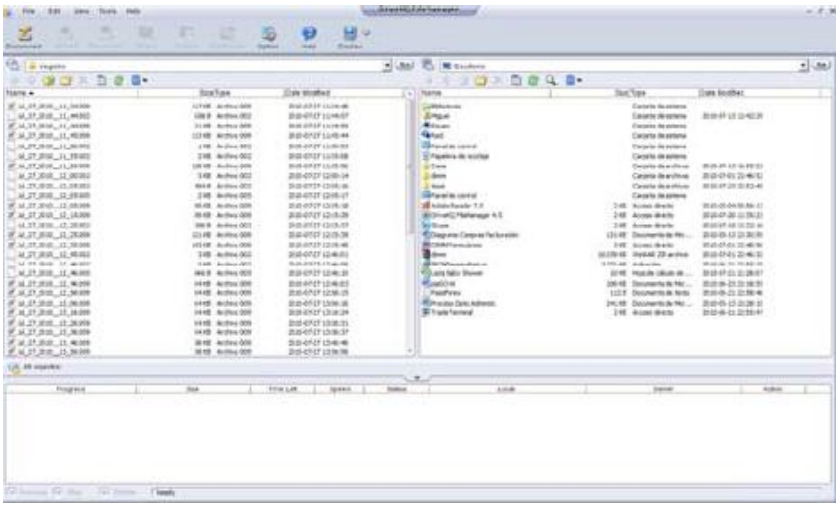
Una vez instalado el programa, se pudo obtener información, que en caso de ser de la competencia sería muy útil.

Para poder usar los logs generados por el keylogger, se debe seguir el siguiente procedimiento:

En el servidor FTP se guardan los logs, los mismos que pueden descargar uno por uno o mediante el instalador de un administrador de archivos del mismo sitio, se pueden descargar todos o los que se deseen.

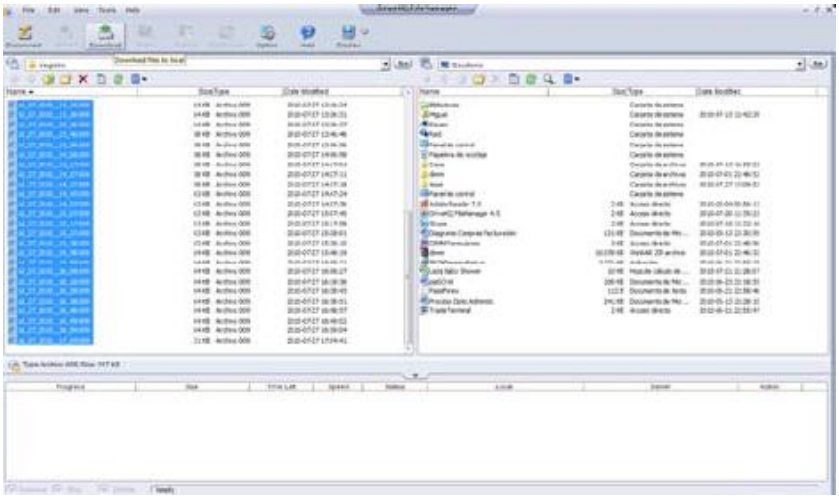
En la siguiente imagen, se puede observar que el administrador de archivos está conectado y que se debe indicar en que carpeta se desea guardar los archivos que se descargarán del servidor.

Gráfico Nº 4.64 - Administrador de archivos FTP



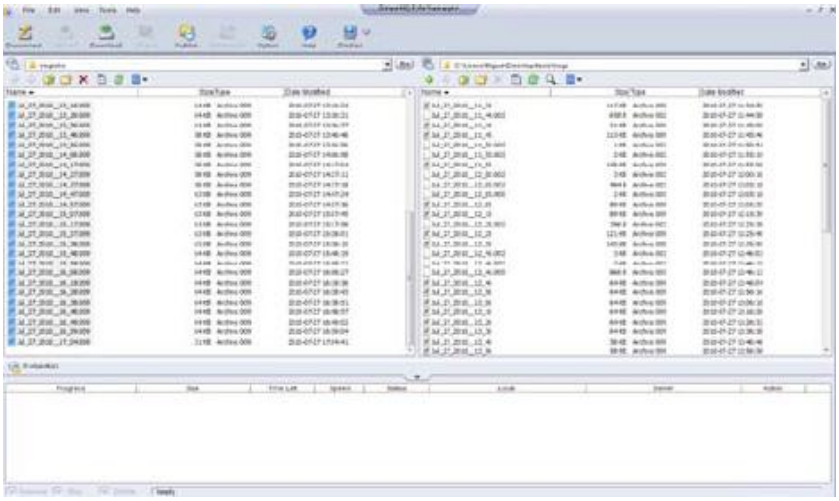
Una vez escogida la carpeta en la que se guardarán los archivos, se seleccionan los archivos que se van a descargar y se presiona el botón de descarga o download.

Gráfico Nº 4.65 - Descarga de archivos



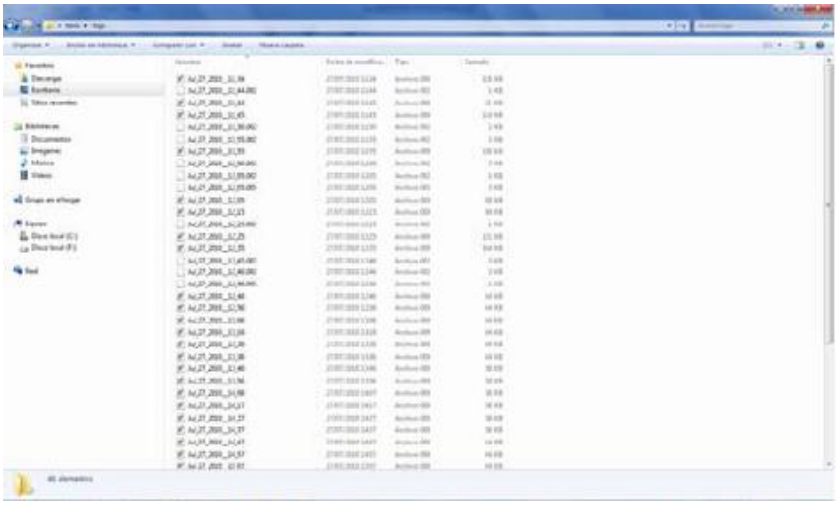
Cuando se han descargado los archivos, se observa que efectivamente los logs se encuentran en el lugar que fue seleccionado.

Gráfico Nº 4.66 - Archivos descargados



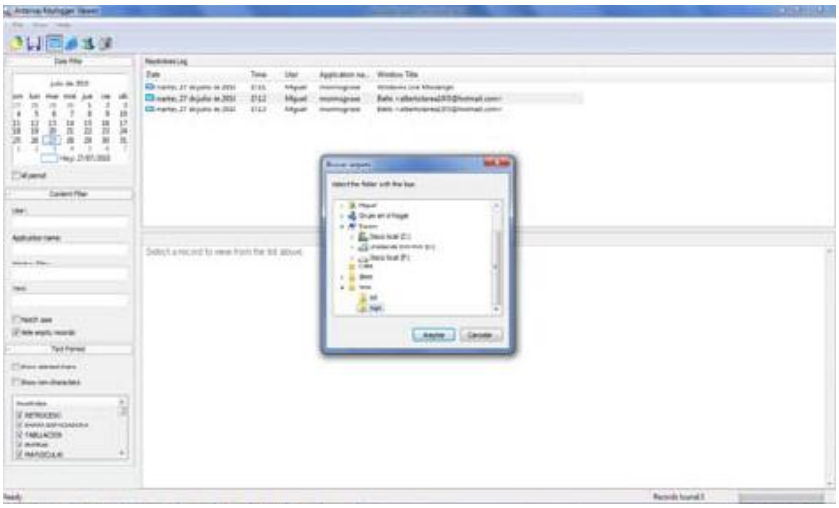
Si se abre la carpeta en la que se guardaron estos registros, se puede constatar que ahí están los archivos descargados.

Gráfico Nº 4.67 - Logs del keylogger



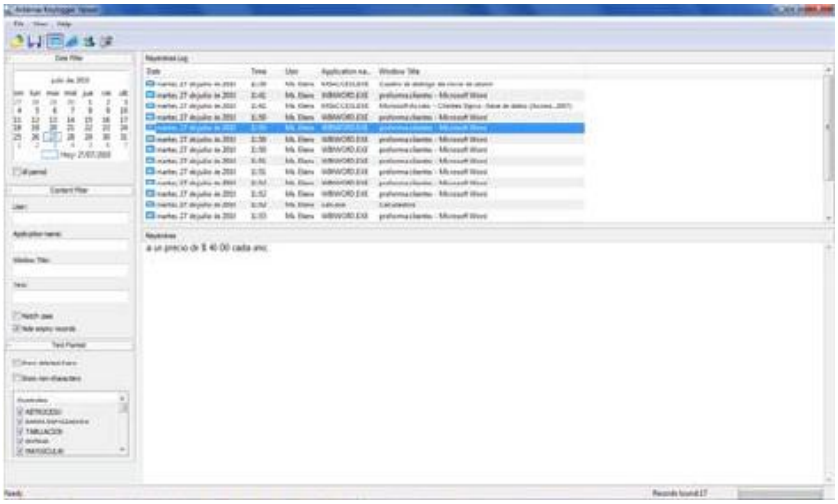
Para poder visualizar estos archivos, se debe abrir el visualizador de logs o keylogger viewer; una vez abierto, se deben abrir los archivos descargados, por lo que ingresamos en la ubicación en la que se guardaron los logs y se los abre.

Gráfico Nº 4.68 - Abrir logs en visor de logs



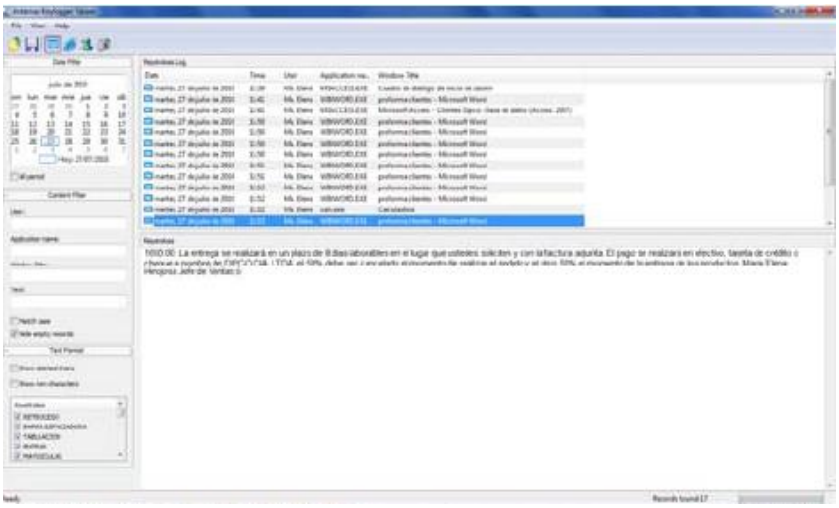
Cuando se abrieron estos archivos, se observa una lista en la que constan los archivos con la fecha de creación, la hora, el usuario del que se generaron los logs, la aplicación de la que se tomaron las capturas y el título de la ventana en la que se estaba trabajando.

Gráfico Nº 4.69 - Lista de logs



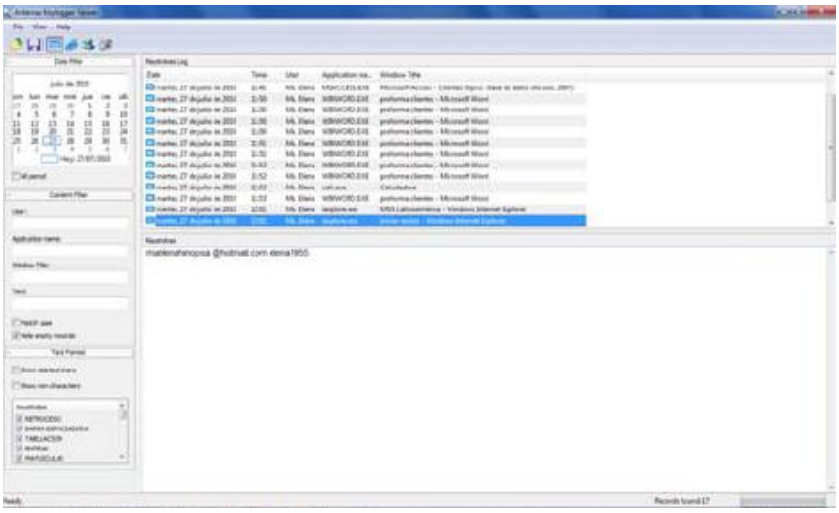
A continuación, se puede observar que, si se da un click en cualquiera de los archivos, en la parte inferior de la lista aparecen los datos que fueron capturados en ese archivo.

Gráfico Nº 4.70 - Contenido de un log



En este caso, por ejemplo, observamos que se capturó el usuario y la contraseña de un correo electrónico gratuito.

Gráfico Nº 4.71 - Datos capturados



En las pantallas anteriores, se puede observar que existen valores, nombres de productos, etc.

De esta manera se puede demostrar que se puede obtener información muy valiosa a través de un ataque de ingeniería social, que todas las

herramientas necesarias están al alcance de nuestras manos, son gratuitas y simplemente se necesita estudiarlas y aprender como funcionan para sacarles el mayor provecho posible.

4.3. Propuesta de seguridad

Se propone una solución para minimizar los riesgos detallándonos los alcances y limitaciones.

4.3.1. Propuesta de seguridad en la información. Caso "Municipalidad Distrital de Independencia"

Una vez efectuada la revisión del Estado del Arte, realizado el diagnóstico de la institución, y después de haber estudiado los resultados del mismo nos abocamos a elaborar la propuesta con base en lo que éstos arrojaron.

Convencidos de la importancia que tiene la seguridad de la información en cualquier organización y tomando en cuenta las opiniones de Symantec, respecto a que la información fluye mediante diversos medios y canales que la tecnología de la información ha sido diseñada considerando sólo la escalabilidad, más que la seguridad, y que un sin número de los mismos tienen una gestión de contraseña no segura, son vulnerables a la falsificación de cuentas y potencialmente de fácil acceso a ataques de servicio, reflexionando sobre el impacto que causan los virus MBR, encriptado, oculto en archivos, diversos troyanos, gusanos, diversas amenazas como backdoors, spyware,

sniffers, código malicioso, backdoors, keyloggers, rootkits por corporativos dedicados a la protección de la información como Sophos, Panda Security, firmas como E&Y, PWC, CYBSEC, Websense UNISYS y centros de investigación a la detección de vulnerabilidades como el CERT e ISACA como se señaló en el capítulo 4, las pérdidas que éstos pueden ocasionar ya sea en aspectos contables, de tiempo, o de privacidad, y pensando en la destrucción que éstos originan y su trascendencia en el factor financiero de la empresa afectada, se ha elaborado la siguiente propuesta, con el propósito de subsanar las carencias que tienen los usuarios para resguardar su información.

Su fundamentación tecnológica está basada en las publicaciones de seguridad, información virtual, noticias de seguridad, boletines de multimedia por Sophos, empresa líder mundial en soluciones de control y seguridad informática para empresas, educación y gobiernos, otra fuerte fundamentación es el Estudio de Percepción Seguridad en Informática por JFS empresa que apoya en la identificación de soluciones tecnológicas e informáticas.

Su fundamentación teórica se basa en la Metodología de Evaluación de Riesgos recomendada por ISACA, que también soportó el cuestionario.

Para su estructuración y entendimiento de la propuesta se conformó por cuatro secciones que son:

- Objetivo
- Alcances y limitaciones de la propuesta
- Formato y estructura de la propuesta
- Recomendaciones básicas de seguridad.

Todos estos que se desglosan a continuación:

4.3.1.1. Objetivo de la propuesta.

Minimizar las vulnerabilidades implícitas en el manejo de la información en los usuarios de computación de punto final.

4.3.1.2. Alcances y limitaciones de la propuesta.

- Está orientada a administradores de sistemas. También puede servir como herramienta para auditores en informática en el análisis de riesgos (apoyándose en los aspectos teóricos señalados en el apartado de identificación de riesgos), así como soporte para el establecimiento de políticas de seguridad y controles preventivos considerando los que son propuestos en el presente capítulo.
- Los controles propuestos son en su mayoría de tipo preventivo.
- Los procedimientos descritos en el desarrollo de la propuesta, atañen al sistema operativo más común en los

usuarios antes mencionados, que es Windows en sus diferentes versiones.

- Esta propuesta se limita a proteger de vulnerabilidades conocidas hasta la fecha en aplicaciones de Internet, así como protocolos y servicios de red, mediante la evaluación de soluciones de software y políticas de seguridad dando recomendaciones s de acuerdo al análisis de riesgos, con el objeto de minimizar los riesgos.
- No se contempla una sola solución integral de seguridad; seguridad perimetral, ni seguridad en la línea de defensa como pueden ser soluciones firewalls empresariales, paquetes integrales de seguridad, detectores de intrusos (IDS's) a nivel organizacional, honeynets, entre otros, puesto que está diseñada para computadoras de punto final, sin embargo, sus elementos pueden conformar la parte complementaria de otro tipo de soluciones existentes en el mercado, o viceversa. No se ofrece ninguna garantía de seguridad de las computadoras de punto final como receta de cocina, pues en el panorama actual no existe propuesta, metodología o solución integral alguna que logre garantizarlo, por lo que únicamente se garantiza la minimizar los riesgos en un

95% basado en la premisa del CERT (anexo 3) contemplada en el análisis de riesgos.

- Esta propuesta es para la protección lógica de la información tomando en cuenta sus propiedades de confidencialidad, integridad y disponibilidad en computadoras de punto final. No se contempla la seguridad física del equipo de cómputo, robo físico del mismo, destrucción y desastres naturales. Es meramente preventiva, detectiva y correctiva. Los controles son planteados tomando en cuenta la evaluación de riesgos desde los puntos de vista de vista: riesgos de la información en la organización desde las aplicaciones de punto final.

4.3.1.3. Formato y estructura de la propuesta

La propuesta está estructurada en un formato de recomendaciones básicas de seguridad, que ayuda a proteger la información del ordenador conectado a la Internet de forma rápida y atacando a las principales vulnerabilidades que embisten la seguridad, así mismo se irán haciendo proposiciones con mayor profundidad, para cada uno de los principales riesgos analizados anteriormente, es decir, se parte de lo básico a lo específico.

La operación la puede llevar a cabo un usuario con conocimientos amplios de computación, el tiempo necesario para implementar la propuesta es el que le tomaría instalar una nueva aplicación en su ordenador, las vulnerabilidades que cubre, son aquellas que perjudican la información del ordenador en un formato general de protección, que, de ser aplicado y seguido continuamente, minimiza el impacto de sufrir algún por la falta de medidas de seguridad.

4.3.1.4. Recomendaciones básicas de seguridad.

A continuación, se mencionan 10 puntos básicos para la protección de una computadora de punto final:

1. **Uso de programas de protección o "antivirus" y su actualización.**

   Asegúrese de que tiene por lo menos un programa Antivirus en su computadora, dos es lo más recomendable. El Antivirus está diseñado para proteger la computadora contra virus conocidos, así que no hay de qué preocuparse. Pero ya que nuevos virus emergen diariamente, los programas antivirus requieren de actualizaciones periódicas continuas. De igual manera, se requiere que se actualice cada año la versión del antivirus, ya que puede cambiar de forma importante la

maquinaria de búsqueda (por ejemplo algunos utilizan técnicas heurísticas que necesitan actualizar la forma en que realizan sus búsquedas). Por lo tanto, asegúrese de actualizar su antivirus regularmente.

2. **No abrir correo electrónico de fuentes desconocidas.**

Una regla muy simple de seguridad es que si no se conoce a una persona que está enviando un correo electrónico, hay que tener cuidado al abrirlo, lo mismo, cualquier archivo adjunto a él. Si se recibe un correo sospechoso, se recomienda borrar el mensaje completo, incluyendo los archivos adjuntos. Incluso si se conoce a la persona que lo está enviando, se debe ejercitar la precaución y actuar con desconfianza, y más aún si tiene ligas a lugares raros o no usuales de los que maneja con esa persona o entidad, debido a que accidentalmente le pueden haber enviado un virus, tal es el caso del virus "te amo", el cual se esparció a millones de personas en el 2000.

3. **Use contraseñas difíciles de adivinar.**

Las contraseñas mantienen lejos a los intrusos, sólo si son difíciles de adivinar, no comparta su contraseña, y no use la misma clave en más de un lugar. Si alguien

adivina su contraseña, no es deseable que tenga posibilidades de usarla en otros lugares, por ejemplo en su cuenta bancaria. Las reglas de oro en la selección de contraseñas son: una contraseña debe tener un mínimo de ocho caracteres, y sea tan incomprensible como sea posible, utilizando mayúsculas, minúsculas, y caracteres especiales entre otros. Es necesario cambiar las contraseñas regularmente, al menos cada 90 días. No le confié su contraseña a nadie.

4. **Proteger la computadora de intrusos de la Internet, usando firewalls personales.**

   Equipe la computadora con un firewall personal. Éstos crean un muro de protección entre su computadora y el mundo exterior. Vienen de dos formas, cortafuegos, tipo software, que corren en su computadora personal y los de tipo hardware que protegen un número de más de dos computadoras al mismo tiempo. Trabajan filtrando datos peligrosos y no autorizados que provienen de la Internet, mientras que permite el tráfico confiable que llega a su computadora. Se pueden encontrar firewalls o cortafuegos en la red, ya sean de uso gratuito como el ZoneAlarm y el Tiny Firewall que vienen con tutoriales sencillos, que emergen después de una instalación

simple, otros buenos y comerciales son los que produce Symantec y Network Associates, por ejemplo: Norton Personal Firewall. El seguir estas prácticas seguras, ayuda a no permitir a los intrusos que entren en su computadora.

5. **No comparta el acceso a su computadora con extraños, aprenda acerca del riesgo de compartir recursos.**

   El sistema operativo de su computadora puede consentir que computadoras en una red, incluyendo la Internet, acceda a su disco duro con el fin de compartir recursos. Esta opción puede permitir a los intrusos infectar su equipo con troyanos o ver sus archivos. Por tanto, a menos que sea realmente necesario que comparta archivos, deshabilite esta opción. Vea los archivos de ayuda, del modo en que su sistema operativo comparte archivos y no permita que los extraños entren en su computadora.

6. **Desconéctese de la Internet cuando no lo esté utilizando.**

   Recuerde que el camino digital tiene una comunicación en los dos lados. Usted envía y recibe información por

medio de él. Desconéctese de la Internet si no la está utilizando, no dé oportunidad que alguien se cuelgue a su máquina. Si no tiene antivirus, ni Firewall, alguien puede infectar su computadora y entrar a ella.

7. **Respalde los datos e información de su computadora.**

   Expertos en computación saben que hay dos tipos de gente: aquellos que han perdido información y los que van a sufrirla. Respalde pequeñas cantidades de información importante para usted en memorias USB y CD. La mayoría de la gente debe hacer respaldos semanales de su información importante. Además asegúrese de tener discos de rescate a la mano de su sistema por si ocurre algún evento.

8. **Baje regularmente actualizaciones de seguridad, o parches de seguridad**

   La mayoría de las empresas proporcionan actualizaciones de sus programas regularmente. Algunas veces, se detectan errores de programación que pueden afectar la seguridad de su computadora y permitir que intrusos la penetren. Cuando son descubiertos, las compañías y los distribuidores los ponen al alcance en sus sitios Web. Se debe estar seguro de que se tienen las

últimas actualizaciones e instalarlas. Cheque regularmente dichas actualizaciones o permita que el actualizador automático lo haga, ya que muchas compañías lo incluyen como una opción más.

9. **Verifique su seguridad en una base de seguridad regular o probada y normalizada. Esto puede ser por periodos de tiempos regulares y reevalué la seguridad de su computadora periódicamente**.

   Los programas y sistemas operativos incluyen varias utilerías que facilitan el trabajo, pero lo pueden dejar vulnerable a intrusos y virus. Se debe evaluar la seguridad en la computadora al menos dos veces al año. Los exploradores de la Internet vienen en su menú de preferencias con un apartado de seguridad, póngalo el que se adecue a sus necesidades, de preferencia ponga uno arriba de lo que requiere como mínimo.

10. **Asegúrese que sus empleados sepan que hacer si su computadora resulta afectada o ya ha sido violada en su seguridad.**

    Asegúrese que todo aquel que use el equipo tenga una formación de seguridad informática y sepa que hacer si

está infectado, que sepa actualizar sus antivirus, bajar parches y como crear una contraseña difícil de adivinar.

V. DISCUSIÓN

5.1. Para la categoría de riesgos en la continuidad del proceso.

Por los resultados de la categoría de riesgos en la continuidad del proceso del capítulo anterior, se puede confirmar que los riesgos que amenaza en la continuidad del proceso pueden paralizar las actividades, es importante reflexionar que con los datos proporcionados por los colaboradores es posible observar que la organización confía en su suerte al no contar con una propuesta de seguridad en la información y en cualquier momento puede ser blanco de ataques internos o externos y sus consecuencias serían incalculables si llegase a parar la continuidad de operaciones a debido a la falta o alteración del activo más importante que viene a ser la información.

5.2. Para la categoría de riesgos en la eficacia del servicio de informática.

Por los resultados de la categoría en la eficacia del servicio de informática del capítulo anterior, se puede confirmar que los riesgos que amenaza en la eficacia del servicio de informática también pueden paralizar las actividades, se consideró ya que eran de mayor importancia por el alto riesgo que pueden ocasionar al usuario y a la Municipalidad Distrital de Independencia.

Como discusión final del resultado de las dos categorías de riesgos analizadas, se puede observar que la organización carece de medidas de seguridad adecuadas y que le falta conciencia del tema de la seguridad a nivel organizacional, aunque ya

ha sufrido percances sumamente difíciles y costosos, también que los usuarios no tienen cultura informática respecto a este tema, ya que las respuestas nos revelan el desconocimiento de las amenazas actuales para su información, por esto no es sorprendente que en la Municipalidad Distrital de Independencia que laboré se desconocen las amenazas informáticas por los usuarios de la misma, haciendo referencia a la encuesta nos deja ver la dificultad para mostrar a la Alta Dirección el valor estratégico que implican los esquemas de seguridad teniendo elementos como los anteriormente mostrados y conociendo que en la actualidad tenemos mayor dependencia tecnológica de las organizaciones a todos sus procesos debemos proteger la información.

VI. CONCLUSIONES

Una vez concluido la presente tesis tanto en la parte teórica como en la parte práctica, se pueden sacar las conclusiones correspondientes en base a lo investigado.

1. Existe una gran cantidad de información en cuanto a ingeniería social y Phishing se trata, tanto en el internet como en libros; se han podido analizar los conceptos, las técnicas de ataque, la estructura de un ataque, cual es el comportamiento de un atacante(Ingeniero Social), en donde se puede conseguir información general y confidencial de la víctima, cómo se puede mitigar el riesgo dentro de una empresa frente a estos ataques; pero a pesar de toda esta información, las personas en la ciudad de Huaraz y especialmente los trabajadores de la Municipalidad Distrital de Independencia no tienen una conciencia real de lo que implica un ataque de este tipo, no saben cuál es el valor real de la información y peor aún, no están conscientes de que todas las personas pueden ser consideradas un blanco de ataque para un ingeniero social.
2. Una vez conocidos todos estos conceptos se concluyó que, la Municipalidad Distrital de Independencia puede contar con la mayor tecnología, con los últimos equipos del mercado y el mejor software de seguridad, pero si no se crea una conciencia real y no se educa a todos los empleados en el ámbito de seguridades informáticas no se va a mitigar el riesgo de caer en un ataque de Phishing o de ingeniería social; esto es bastante complicado de manejar,

debido a que en muchas empresas una sola persona tiene acceso a toda la información sin importar la clasificación que tenga y si no existe la educación adecuada sobre cómo manejar esta información se corre un gran riesgo.

3. Dentro de los conceptos de Phishing, se pueden encontrar las diferentes técnicas que son utilizadas por los ingenieros sociales el momento de realizar un ataque, las mismas que son bastante fáciles de usar y generalmente se aprovechan de la ingenuidad o falta de conocimiento de las personas, quienes sin darse cuenta entregan cualquier tipo de información a personal desconocido y no piensan si quiera que esta información puede causar pérdidas desastrosas dentro de la organización o a una persona específica.
4. Con el caso práctico que se realizó se pudo concluir que, la gran mayoría del personal que labora dentro de la Municipalidad Distrital de Independencia no tiene la educación adecuada en cuanto a seguridades informáticas se trata, no conocen cuales son los riesgos de recibir información como: promociones, premios y propaganda, y no confirmar si esa información es auténtica y no contiene ningún tipo de malware. Se comprobó que con una carta falsa y una "inocente imagen" se puede robar o tener acceso a información confidencial sin que la víctima tenga la menor sospecha de lo que está pasando.
5. Después de revisar los resultados obtenidos mediante el caso práctico se puedo concluir que, mediante un programa no muy complicado como es el keylogger, se puede obtener cualquier tipo de información, en este caso se obtuvieron direcciones y contraseñas de correo electrónico, datos del personal que labora en la entidad, como es su sueldo, sus bonificaciones y otros, también las otras actividades que realiza dicho personal que no son de índole

de su trabajo por el cual se le remunera; todo el software que se utilizó está al alcance de cualquier persona, es cuestión simplemente de estudiar la herramienta y sacarle todo el provecho posible.

6. Cuando se analizó la parte teórica y la parte práctica del presente trabajo de investigación se pudo concluir que, la falta de políticas de seguridad con lo que a Phishing respecta son muy pocas y no se encuentran bien definidas o no abarcan todo lo relevante con respecto a las partes más sensibles de la organización.
7. Dentro de las políticas de seguridad, tampoco se encuentra un plan de capacitación para todos los trabajadores de la Municipalidad Distrital de Independencia, para concientizarles sobre la importancia de mantener una buena seguridad informática y de lo importante que es resguardar la información de cada uno de ellos y de la institución como tal; no se concientiza al personal en lo que a este tema se refiere, cuando es un tema tan importante que puede traer consecuencias muy graves.
8. Durante el proyecto, se han desarrollado distintas pruebas de concepto. El principal ha sido para hacer la encuesta que recogía los conceptos clave de seguridad informática del personal que labora en la Municipalidad Distrital de Independencia.

Aunque se han explicado muchos temas, hay otros que no se han podido dar, o simplemente han sido tratados de manera superficial. Es por eso que este proyecto puede servir como base para otros nuevos proyectos, mucho más específicos, pero ya teniendo una pequeña idea de lo que actualmente está ya funcionando por el mundo. Algunos conceptos, se quedarán obsoletos al ser

publicado el trabajo, o incluso mientras se ha estado haciendo, pero al tratar todo como ideas, estas perdurarán, como ha sido el caso del virus `I love you´, pudiendo evolucionar y adaptarse a los nuevos mercados. Lo importante a partir de ahora es saber coger un nuevo caso de ingeniería social e identificar todos aquellos elementos que logran que se materialice, no memorizar los casos que hubo, porque nunca se repetirán.

En definitiva, la ingeniería social es un ejercicio de innovación, mezclando un proceso con factores humanos, y si se mira un poco más allá de la seguridad informática y los sistemas de seguridad, se puede extrapolar dichas características a todo aquello que nos rodea, pudiendo analizar y decidir nuestras acciones con un poco más de información.

VII. RECOMENDACIONES

1. Se debe crear un plan de capacitación y concientización para todos los empleados, sin importar el cargo que desempeña o el área en la que trabaja, sobre todos los conceptos de Phishing e ingeniería social, cuáles son las técnicas que usan los ingenieros sociales y qué pasos siguen para poder realizar los ataques. Se debe dar a conocer cuáles son los riesgos que se corre al no saber cuidar la información y al entregarle datos personales e información confidencial a cualquier persona.
2. Se debe clasificar la información y se debe mantener un control sobre qué personas tienen acceso a esa información dentro de la compañía, para evitar que una sola persona tenga acceso a toda la información y sea un blanco fácil para un ataque de Phishing o de ingeniería social; dentro de esto también se debe educar al personal sobre el manejo de información confidencial y en caso de ser víctima de un ataque presentar una alerta inmediata al área de seguridad sobre la información que fue entregada.
3. Dar a conocer al personal todas las técnicas que se usan dentro del Phishing y cómo se usan, así como también la manera de reconocer cuando un ingeniero social está poniendo en práctica una de ellas con el personal y cómo evitar caer en las manos del hacker, qué se puede hacer para mitigar el riesgo de ser una víctima del Phishing.
4. Concientizar al personal dentro de las empresas sobre lo peligroso que es abrir un link, un archivo adjunto, un archivo desconocido simplemente porque

reciben algo que les parece novedoso o interesante; educarles sobre la importancia de siempre verificar si ese archivo o página no es peligroso, si no contiene virus o malware y si es enviado por la persona que dice haberlo enviado. Enseñarles que sus datos son muy importantes y que pueden ser capturados mediante phishing por ejemplo si entran en una página web falsa o que pueden instalar cualquier cosa en su equipo sin darse cuenta cuando abren cualquier archivo sin verificar lo que contiene.

5. Dentro del internet se puede encontrar un sin número de programas que pueden ser muy inocentes pero otros pueden causar daños catastróficos dentro de una empresa, de una computadora personal o pueden robar cualquier tipo de información como en el caso práctico de esta tesis; por lo que, se deben mantener siempre activas las alertas automáticas sobre cualquier tipo de software que sea instalado en la computadora, debe realizarse de forma periódica una revisión de los programas que se tienen instalados en el pc o la portátil de cada trabajador, se debe mantener actualizado el antivirus y correr el antivirus al menos una vez al día para evitar que cualquiera de estos programas maliciosos sea instalado en la organización.
6. Se deben crear políticas de seguridad que abarquen todo lo concerniente al Phishing y a vez a la ingeniería social, éstas deben ser claras y pueden basarse en cada una de las técnicas usadas por estos atacantes; las políticas deben ser apoyadas por la parte tecnológica ya que hay casos en que las personas olvidan hacer ciertas cosas, como bloquear la máquina, y en este caso se lo podría realizar automáticamente después de un tiempo de inactividad. Así mismo, las políticas deben ser conocidas por todo el personal, deben ser

medidas para ver su efectividad y se debe controlar periódicamente que todo el personal de la organización las cumpla.

7. Dentro de éstas políticas de seguridad debe constar una en la que se indique que cada cierto tiempo se debe realizar un plan de capacitación y concientización para todos los usuarios de la información y de los sistemas de información, de manera que siempre estén alertas sobre los ataques que se traten de realizar y cada uno de ellos pueda tomar medidas al respecto o sepan exactamente que procedimiento deben seguir ante uno de estos ataques.

VIII. REFERENCIAS BIBLIOGRÁFICAS

ALVARADO TOLENTINO, J. D. (2014). *Diseño de una infraestructura de telecomunicaciones con estándares de data center y redes, para garantizar la seguridad de la información y la transmisión de datos de los servidores de la Municipalidad Distrital de Independencia, 2014.* HUARAZ: UNASAM.

BANK, D. (2005). *"'Spear Phishing' Tests Educate People About Online Scams".* The Wall Street Journal.

BERNERS-LEE, T. (2006). *Uniform Resource Locators.* IETF Network Working Group.

BLOOMINGTON, I. U. (15 de septiembre de 2005). *Phishing for Clues.*

BOCIJ, P. (2006). *The Dark Side of the Internet: Protecting Yourself and Your Family from Online Criminals.* Hardcover.

BORGHELLO, C. (Marzo 2012). *Temperini Marcelo Cruzada por la Identidad Digital.*

CLARK, B. (2014). *Rtfm: Red Team Field Manual.* USA.

CNN. (2005). *"Security: Bank to Require More Than Passwords".* CNN.

DA COSTA PALACIOS, J. M. (2003). *Prácticas de Seguridad en Sistemas*

Conectados a Internet. Libros En Red.

DON MURDOCH GSE. (2014). *Blue Team Handbook: Incident Response Edition: A condensed field guide for the Cyber Security Incident Responder.* USA.

ENGEBRETSON, P. (2013). *The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy.* USA.

ERICKSON , J. (2008). *Hacking: The Art of Exploitation.* USA.

EWEEK. (2004). *"UK Phishers Caught, Packed Away".* eWEEK.

FINEXTRA. (2005). *Phishers target Nordea's one-time password system.* Finextra.

FISHER, D. (2005). *Warn when HTTP URL auth information isn't necessary or when it's provided.* Bugzilla.

GABRILOVICH, E., & GONTMAKHER, A. (Febrero del 2002). *The Homograph Attack.* Communications of the ACM.

GARCÍA RAMBLA, J. L. (2012). *Ataques en redes de datos IPv4 e IPv6 2ª edición revisada y ampliada.* Mexico: 0xWORD.

GARRIDO CABALLERO, J. (2011). *Análisis Forense Digital en Entornos Windows. 3ª Edición revisada, remaquetada y ampliada.* Mexico: 0xWORD.

GONZÁLEZ PÉREZ , P. (2014). *Ethical Hacking: Teoría y práctica para la realización de un pentesting.* Mexico: 0xWORD.

GUPTA , M., & SHARMAN, R. (2009). *Social and Human Elements of Information Security: Emerging Trends and Countermeasures.* New York: State University of New York, Buffalo - USA.

IDAM. (2002). *Código de Practica para la administracion de la Seguridad de la Información.* Argentina: Instituto Argentino de Normalizacion - ISO/IEC 17799:2005.

JAGATIC, T., JOHNSON, N., JAKOBSSO, M., & MENCZER, F. (3 de junio del 2006). *Social Phishing.* Communications of the ACM.

JOHANSON, E. (2005). *The State of Homograph Attacks Rev1.1.* The Shmoo Group.

KAWAMOTO, D. (2005). *"Faced with a rise in so-called pharming and crimeware attacks, the Anti-Phishing Working Group will expand its charter to include these emerging threats.".* India: ZDNet.

KERSTEIN, P. (2005). *"How Can We Stop Phishing and Pharming Scams?".* CSO.

KERSTEIN, P. (2005). *How Can We Stop Phishing and Pharming Scams?* CSO.

KIM , P. (2015). *The Hacker Playbook 2: Practical Guide To Penetration Testing.* USA.

KIRK, J., & IDG NETWORK. (02 de Junio de 2006). *Phishing Scam Takes Aim at MySpace.com.* Recuperado el 05 de Mayo de 2015, de

http://www.pcworld.com/resource/article/0,aid,125956,pg,1,RSS,RSS,00.asp/

LEGON, J. (2004). *"'Phishing' scams reel in your identity".* CNN.

LEYDEN, J. (21 de marzo de 2005). *"Brazilian cops net 'phishing kingpin'".* The Register.

LEYDEN, J. (4 de Abril de 2005). *"Trojan phishing suspect hauled in".* The Register.

MAIWALD, E. (2004). *Fundamentos de Seguridad de Redes.* McGraw Hill, Segunda Edición.

MICROSOFT. (2005-2014). *A security update is available that modifies the default behavior of Internet Explorer for handling user information in HTTP and in HTTPS URLs Microsoft Knowledgebase Database.* Microsoft.

Microsoft Partners with Australian Law Enforcement Agencies to Combat Cyber Crime. (24 de Agosto de 2005).

MITNICK, K., & SIMON, W. (2005). *The Art of Intrusion: The Real Stories Behind the Exploits of Hackers, Intruders and Deceivers.* USA.

MITNICK, K., & SIMON, W. (2012). *Ghost In The Wires: My Adventures as the World's Most Wanted Hacker*. USA.

MITNICK, K., SIMON, W., & WOZNIAK, S. (2003). *The Art of Deception: Controlling the Human Element of Security*. USA.

Nineteen Individuals Indicted in Internet 'Carding' Conspiracy. (20 de Noviembre de 2005).

OXFORD UNIVERSITY PRESS. (Marzo de 2006). *"Phish, v." OED Online.* Recuperado el 12 de Mayo de 2015, de Oxford English Dictionary Online: http://dictionary.oed.com/cgi/entry/30004303/

OXFORD UNIVERSITY PRESS. (Marzo de 2006). *"Phishing, n." OED Online.* Recuperado el 12 de Mayo de 2015, de Oxford English Dictionary Online.

PICOLET, J. (2016). *Hash Crack: Password Cracking Manual.* USA.

RANDO, E. (2013). *Hacking con buscadores: Google, Bing & Shodan + Robtex 3ª Edición.* Mexico: 0xWORD.

RANDO, E., ALONSO, C., & GONZÁLEZ, P. (2014). *Hacking de Aplicaciones Web: SQL Injection. 3ª Edición.* Mexico: 0xWORD.

SAFESIGNER. (2006). *"Verificación y autorización de transacciones con el Smartphone".* SafeSigner.

SKOUDIS, E. (2006). *Phone phishing: The role of VoIP in phishing attacks.*

TAN, K. (5 de diciembre de 2010). *Phishing and Spamming via IM (SPIM).* Internet Storm Center.

WEBSENSE SECURITY LABS. (5 de diciembre de 2006). *Malicious Website / Malicious Code: MySpace XSS QuickTime Worm.*

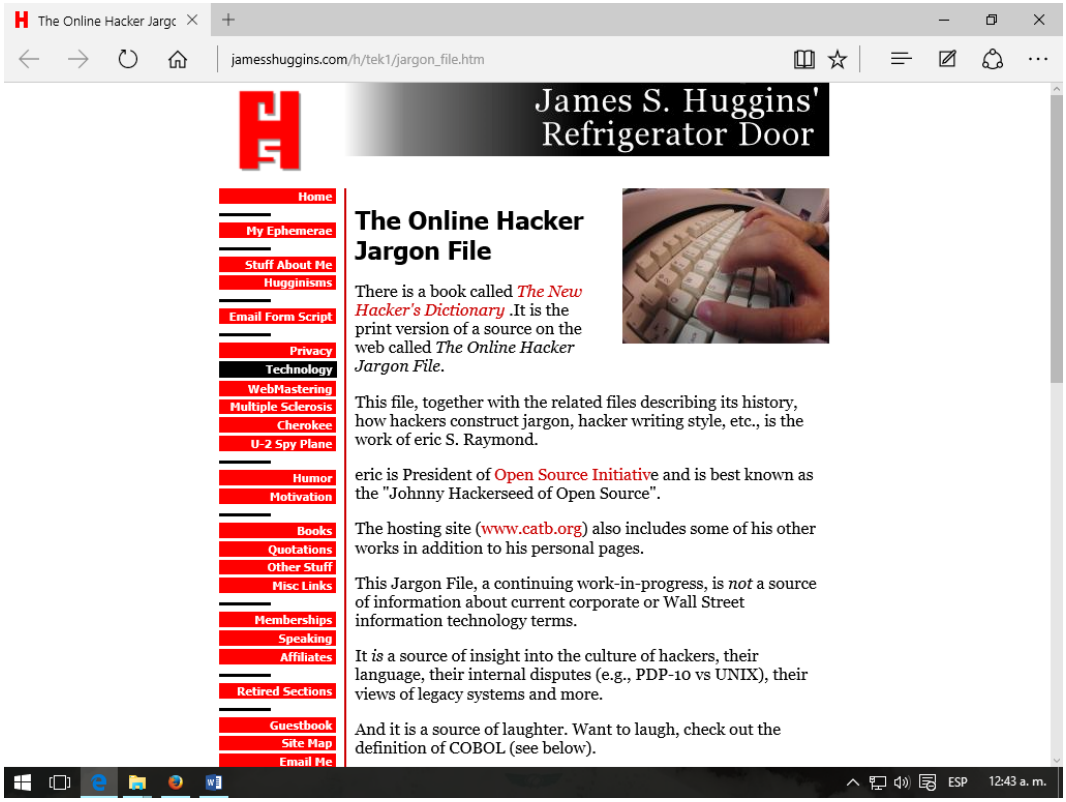
WHITE, A., & CLARK, B. (2016). *Blue Team Field Manual (BTFM) (RTFM).* USA.

ANEXOS

ANEXO Nº 01

Jargon - The definitive compendium of hacker slang.

(El compendio definitivo del argot del hacker.)Este documento es una colección de términos “jerga” de la informática, utilizada por varias sub-culturas hackers en el campo de la computación. Está conformada por conocimientos y material técnico de la informática “underground”. No es un diccionario técnico; lo que se quiere mostrar es el lenguaje que los hackers utilizan para su diversión, comunicación social y debate técnico.



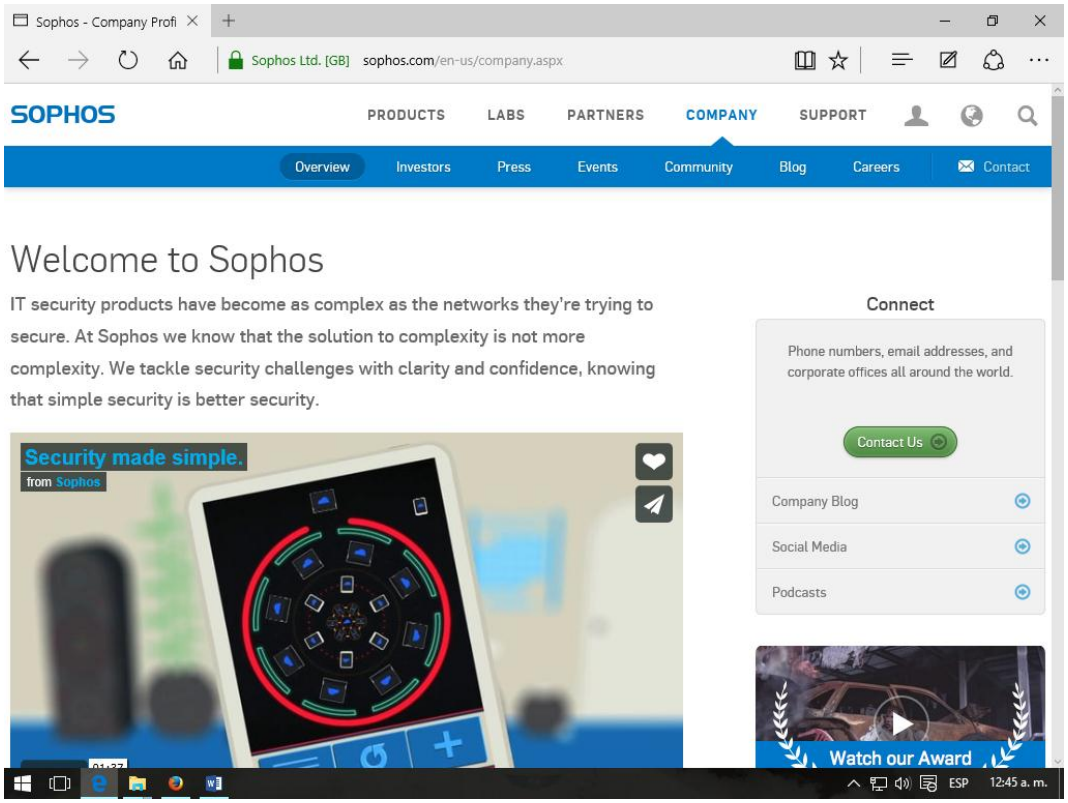
Consulta en línea de Jargon:

http://www.jamesshuggins.com/h/tek1/jargon_file.htm (14/08/2016)

ANEXO Nº 02

SOPHOS

Sophos es un líder mundial en soluciones de control y seguridad informática para empresas, educación y gobiernos, en su portal posee dilatada experiencia en la lucha contra virus, programas espía y spam, tiene soluciones que permite responder rápidamente ante amenazas emergentes, por complejos que resulten, sus análisis y publicaciones de amenazas, información sobre el comportamiento de las amenazas y sistemas operativos que ataca nos otorgaron parámetros importantes para definir el panorama de protección.

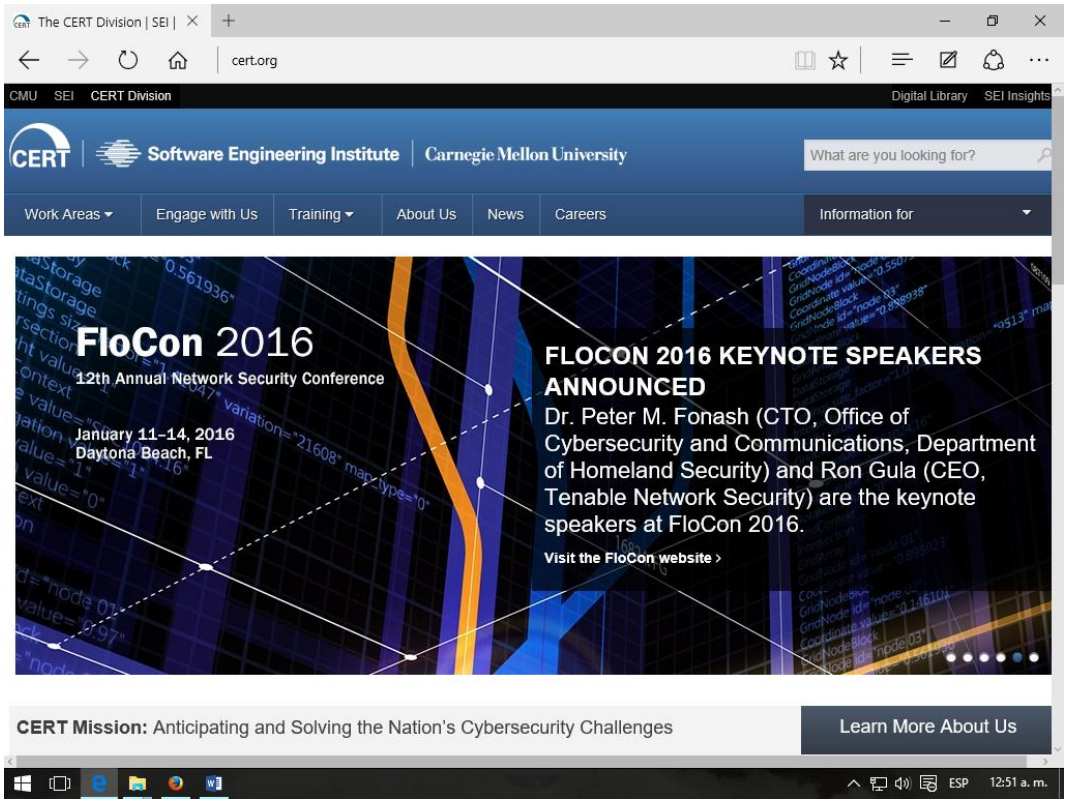


Consulta en línea. www.sophos.com (17/08/2016)

ANEXO Nº 03

CERT (computer emergency readiness times)

Establecido en 1988 el CERT ® Centro de Coordinación es un centro experto en seguridad de internet y vulnerabilidades de software comerciales, un centro federal fundado para la investigación y el desarrollo operado por la universidad de Carnegie Mellon, otorga parámetros impactantes acerca de las debilidades de seguridad en todas las plataformas y paquetería disponible para empresas, siendo un Centro muy reconocido por su labor hacia todo lo referente con software y su seguridad.

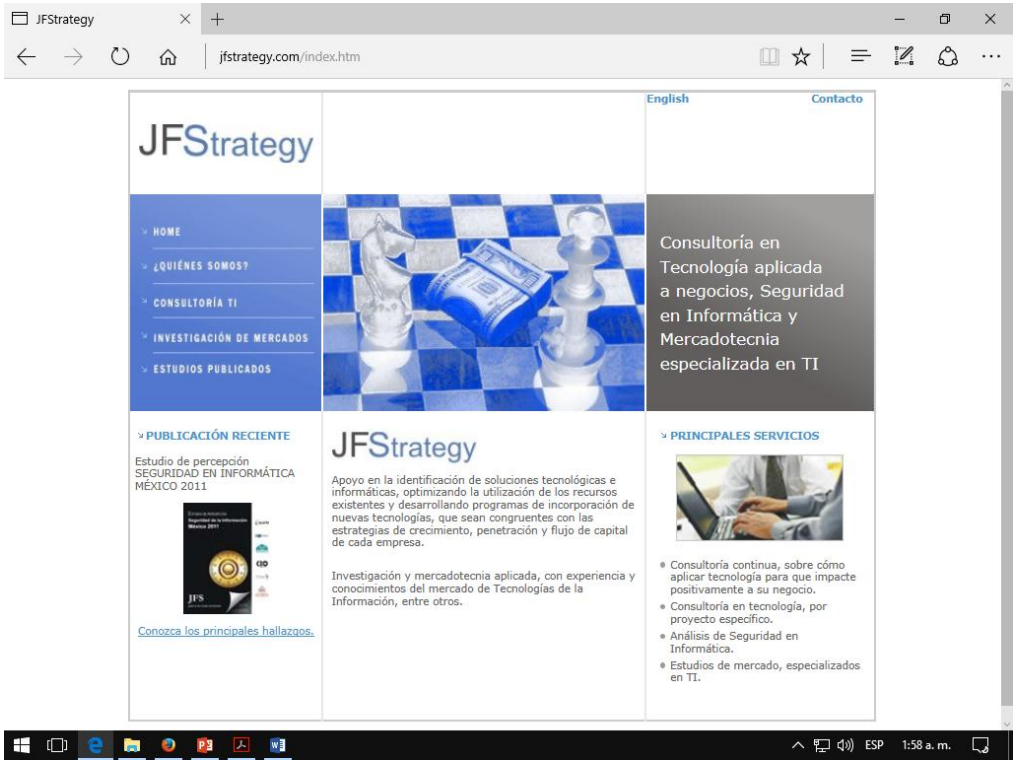


Consulta en línea. http://www.cert.org/ (20/08/2016)

ANEXO Nº 04

Joint Future Systems

Joint Future Systems, S.C. es una empresa con el objetivo de una respuesta a las necesidades de diversas organizaciones por identificar las soluciones tecnológicas e informáticas que mejor se adecuen a sus esquemas estratégicos, operativos y de flujo de capital. Posee un equipo de colaboradores que se ha ido configurando con la experiencia de asesores permanentemente actualizados en materia de tecnología, capaces de entender el entorno y características de cada negocio y recomendar las soluciones tecnológicas más adecuadas, de manera objetiva como la publicación reciente cerca de un "Estudio de percepción de SEGURIDAD EN INFORMÁTICA, MEXICO 2011" disponible en su portal con información.



Consulta en línea. http://www.jfstrategy.com/ (20/08/2016)

ANEXO Nº 05

Cuestionario

UNIVERSIDAD NACIONAL "SANTIAGO ANTÚNEZ DE MAYOLO"
ESCUELA DE POSTGRADO

Cuestionario para usuarios de la red de área local de la Municipalidad Distrital de Independencia que permitirá explorar aspectos de seguridad informática.

El presente cuestionario coadyuvara a la realización de una tesis de maestría en ciencias e ingeniería con mención en auditoria y seguridad informática y tiene por objeto analizar de las vulnerabilidades mediante el uso de phishing para mejorar la seguridad informática de los equipos de cómputo y redes de la Municipalidad Distrital de Independencia.

La información que usted proporcione tendrá un carácter confidencial y anónimo.

Agradecemos de antemano su participación.

PUESTO: _____

PROFESIÓN: _____

EDAD: _____ **SEXO: _____**

INSTRUCCIONES

En las siguientes preguntas responda el inciso que crea correcto.

PREGUNTAS

1. ¿Sabe de los peligros que se encuentran en el Internet?

a) No

b) Si

2. Subraye un peligro que se encuentre en el Internet

a) Robo de hardware
b) Alteración de datos
c) Robo de contraseñas
d) Ambos incisos

3. ¿Qué son los Keyloggers?

a) Protocolos no seguros de red
b) Mensajes basura que generan tráfico en la red
c) Herramientas de intrusión que se instala en una máquina víctima para registrar todo el texto capturado y se obtiene claves de acceso
d) Ninguna de las anteriores

4. ¿Qué son los Mouseloggers?

a) Herramientas de configuración de los mouses
b) Mensajes basura que generan tráfico en la red
c) Software complementario del Mouse
d) Herramientas de intrusión para registrar todo los clicks de un usuario

5. Seleccione por favor un virus informático existente

a) w32/netsky-p
b) I love you
c) I hurt you
d) You know me
e) Los 4 anteriores

6. ¿Alguna vez se ha empleado el archivo w32/netsky-p?

a) No
b) Si

Si conoce un virus informático como lo menciono en la pregunta 5 responda por favor

7. ¿Cómo se ha procedido cuando se encuentra con el archivo I love you?

a) Remito mis datos por Internet
b) Vacuno mis archivos
c) Compro el software complementario

8. ¿Qué pasaría si un virus de clase master boot record entrara en la computadora?

a) Se crearía otro archivo con el código del virus y extensión .com.
b) Se incrustan en el archivo ejecutable de un programa y para disimular el incremento del tamaño del archivo
c) Permanece en el disco duro compartiendo créditos con el código de arranque
d) Los tres anteriores

9. ¿Tiene una cuenta de correo electrónico de la organización?

a) No
b) Si

10. ¿Con qué frecuencia se revisa el correo electrónico?

a) 1 vez al día
b) 2 veces al día o más
c) 1 vez o menos por semana
d) No lo revisó habitualmente

11. ¿Qué tipos de archivos se reciben por el correo electrónico habitualmente?

a) *.avi
b) *.wpd
c) *.xls
d) *.fla

e) *.mbd
f) *.wav
g) Todos los anteriores

12. ¿Con qué frecuencia se reciben los archivos mencionados?

a) Diario
b) Entre 1 y 10 veces por semana
c) Entre 11 y 30 veces por semana
d) Mas 31 veces por semana

13. ¿Qué trato se le da a la información que maneja en sus archivos recibidos?

a) Consulta
b) Personal
c) Informes
d) Todas las anteriores

14. ¿Qué configuración de anti-spam tiene?

a) Automática
b) Personalizada
c) La del ordenador por usuarios no permitidos
d) Restricciones a poppups, cadenas
e) No tengo anti-spam

15. Mencione un gusano informático

a) slammer
b) idazo
c) Jerry
d) los tres anteriores

16. ¿Cuáles considera que son los puntos potenciales de infección?

a) PC conectada a la red

b) Uso de dos antivirus o más
c) Uso de software que limite el acceso libre al ordenador por usuarios no permitidos
d) Ninguna de las anteriores

17. ¿Qué característica tienen los caballos de troya o troyanos?

a) Pasmar el SO
b) Regenerarse
c) Identificarse como archivo desktopshield que bloquea la máquina
d) Camuflajearse como programas benignos
e) Ninguna de las anteriores

18. ¿Por qué un troyano se considera de alto riesgo?

a) Porque daña la paquetería
b) Porque se ejecutan encubiertos en procesos legítimos
c) Porque el usuario se alarma cuando ve su proceso en ejecución
d) Porque borra la información del bios
e) Ninguna de las anteriores

19. ¿Cuáles serían las contramedidas para evitar riesgos por troyanos?

a) Actualizar el hardware y el POP2
b) Guardar la etiqueta de donde navegue y utilizar certificados digitales
c) Rectificar el servidor de la URL
d) Ninguna de las anteriores

20. ¿Por qué razón el spyware no es reconocido por los programas antivirus?

a) Por no estar actualizados
b) Porque se camuflajean como programas benignos
c) Porque no se reproduce, no infecta archivos, ni causa daños a nivel hardware
d) Ninguna de las anteriores

21. ¿Cuál es el medio de transmisión por Spyware y Adware?

a) Actualizar el SO
b) Shareware, Freeware, Navegadores web vulnerables con soporte ActiveX
c) Por unidades de hardware extraíbles
d) Ninguna de las anteriores

22. ¿Qué son los Rootkits?

a) Puertas traseras abiertas a un sistema
b) Herramientas para los intrusos que utilizan para obtener acceso como administrador
c) Instalación y ejecución de controles ActiveX
d) Ninguna de las anteriores

23. ¿Qué son las Backdoors?

a) Cuando se abre un puerto tcp o udp sin que lo sepa la víctima mediante el cual va a ser posible el acceso no autorizado
b) Herramientas utilizadas por los intrusos para hacerse pasar por otros equipos en la red.
c) Piratas informáticos han descifrado la contraseña
d) Ninguna de las anteriores

24. ¿A qué se refiere el escaneo en seguridad informática?

a) Determinación de las características de una red con el objetivo de identificar los equipos disponibles y alcanzables desde Internet
b) Usuarios autentificados, al menos a parte de la red, como por ejemplo empleados internos
c) Métodos de ataque descritos
d) Ninguna de las anteriores

25. ¿Qué es el adware?

a) Una aplicación SO
b) Programas de publicidad no deseada
c) Empresas comerciales invitan a utilizar sus programas
d) Todas las anteriores
e) Ninguna de las anteriores

ANEXO Nº 06

LIBRO DE CÓDIGOS.

Las preguntas realizadas en el cuestionario diagnóstico fueron aplicadas en la Municipalidad Distrital de Independencia donde se autorizó a 20 (usuarios) unidades de trabajo debido a la información y funciones que manejan ser parte de esta investigación. Los cuestionarios se aplicaron en dos sesiones con el objetivo de no saturar de preguntas al usuario de información y de esta manera evitar falsedad en sus respuestas y sea tedioso debido a sus ocupaciones.

1. Esta pregunta se hizo con el propósito de detectar que tan consiente es el usuario del peligro de acceder a internet en una red de área local, pues existen documentos que es necesario compartir así como otros recursos de hardware y software.
2. Si la pregunta anterior fue afirmativa el encuestado debía mencionar un peligro de los que se menciona en el internet.
3. Se incorporó esta pregunta porque los keyloggers son un peligro importante que se adquiere por el internet debido a que capturan todos los impulsos del teclado y después los envían por el internet, evitar estos riegos nos proporcionarían seguridad y evitar la fuga de información que nos evitaría pérdidas económicas.
4. Con esta pregunta corroboramos si el respondiente sabe del funcionamiento de mouseloggers para evitar perdidas de información.

5. Uno de los peligros en la red son los virus y si de verdad los conoce debe de identificar el nombre de alguno de los que han atacado principalmente a las PC y han salido en noticieros televisivos por su alto impacto
6. Se refiere a investigar si el colaborador empleado un virus, y así saber si habla con el conocimiento o nos responde por no quedar como ignorante del tema.
7. Se pregunta si conoce cómo proceder cuando detecta el antivirus, archivo (I love you) de los mas importantes, debido al daño que causo y difusión en noticieros por daños económicos que dejo al dejar estaciones de trabajo fuera de funcionamiento.
8. Se pregunta si conoce los virus clase master boot, porque tienen el record más dañino y es casi imposible borrarlos porque permanece en el disco duro compartiendo créditos con el código de arranque y así ocasionar pérdidas graves económicas.
9. Se pregunta al usuario si tiene una cuenta de correo electrónico para valorar cómo pueden entrar archivos ocultos nocivos a la pc haciéndose pasar por archivos de texto, hojas de cálculo, presentaciones, de no contar con correo solo navega por la web, en donde representa un peligro entrar a diferentes paginas de contraer por este medio virus.
10. Es importante tener un parámetro para conocer las entradas a la red y revisar su correo, de esta manera entre más numero de ocasiones revisa su correo y descarga archivos, hay una probabilidad mayor de recibir infecciones, entonces es necesario herramientas de seguridad para no afectar a las estaciones de trabajo que no tengan privilegios con acceso internet pero sí dentro de las LAN

11. Quisimos conocer el perfil del usuario al recibir correos electrónicos, porque las extenciones de office nos pueden reflejar un uso de correos laboral mientras que las extenciones *.wav, *.avi, *.fla entre otras, son de archivos personales animaciones y música, consideradas de entretenimiento con mayor porcentaje a ser infectadas las terminales
12. Es necesario conocer con qué frecuencia reciben los archivos mencionados para saber en que lapsos de tiempo puede llegar una infección a las estaciones de trabajo.
13. El usuario nos responde el tipo de uso que le da a su información, y así sabremos qué perfil de usuario es y las probabilidades que tiene de contraer virus por la red
14. Deseamos saber si tiene configurado su anti-spam porque de esta manera su correo electrónico tiene un margen de mayor seguridad al recibir sus correos en su estación de trabajo.
15. El propósito fue averiguar si conoce acerca de los gusanos informáticos y que tipo de conocimientos relacionados con seguridad informática tiene el usuario
16. Se quería investigar si el usuario conocía cuáles son los puntos potenciales de infección, para saber si cuida que su equipo no sea infectado, tratando de usar el internet sólo para su uso laboral y en qué porcentaje sus entradas a revisar correo son para su actividad laboral.
17. Se deseaba saber si el respondiente tenia conocimientos de los comportamientos de los virus que se esconden como otros archivos para después causar daños como los caballo de Troya (para borrarlos y detectarlos

porque son difíciles de conocer si una pc tiene un caballo de troya, virus que se camuflajean como programas benignos)

18. Su objetivo fue saber si comprendían el impacto de un virus troyano y el alcance de éste para su información., y para su pc si llega a infectarse.
19. Se incluyó con el propósito de valorar si su conocimiento informático le permite conocer cuáles son las contramedidas para evitar ser víctima de un virus troyano y de esta manera evitar costos altos por infecciones.
20. Esta pregunta se incorporó para saber si su conocimiento sobre seguridad informática le permite conocer que la mayoría de los antivirus no detectan spyware por el comportamiento de los mismos y tener repercusiones diferentes que un virus.
21. El objetivo era darnos cuenta si conocen el medio de transmisión del Spyware (programas para y Adware (ya que tiene una manera de contraerse diferente a los virus y no llegan por correo electrónico).
22. Tuvo como propósito valorar si conocen las herramientas que usan los intrusos y que utilizan para obtener acceso como administrador para así atacar a estaciones de trabajo llamados rootkits
23. Se incorporó porque se quería saber si conoce herramientas backdoors (herramientas para identificar puertos alcanzables de tcp o udp sin que lo sepa la víctima mediante el cual va a ser posible el acceso no autorizado) para determinar equipos disponibles y alcanzables desde Internet que usan los hackers para entrar a diferentes estaciones de trabajo.

24. Se incorporó para estar en posibilidades de valorar si los usuarios saben que se pueden determinar las características de una red donde identificar los equipos disponibles y alcanzables desde el internet
25. Su propósito fue conocer si el usuario puede evitar el adware para evitar que se sature la memoria virtual y se desperdicie tiempo en publicidad molesta.

ANEXO Nº 07

Ampliaciones y trabajos futuros

Uno de los objetivos del trabajo era introducir el tema, pero se sigue requiriendo de mucho más estudio, tanto en expansión como en profundidad. Se aportan un listado de ideas extraídas de entre los elementos mencionados durante el trabajo, relacionadas con las nuevas tecnologías:

- **Dispositivos móviles:** La nueva generación de teléfonos móviles no deja de ser pequeños ordenadores de bolsillo. Estos se catalogan en unos pocos grandes sistemas operativos (webOS, iOS, Android,…), los cuales han sido diseñados y comercializados a gran velocidad. Utilizar técnicas de intrusión tecnológicas a veces puede ser bastante difícil, pero engañar al usuario a través de pantallas y factores psico-sociales es relativamente sencillo. Se puede hacer un estudio específico de este tema cogiendo todos los sistemas operativos y creando una tabla comparativa con maneras de burlar, no su seguridad, sino su usabilidad, atacando directamente al usuario.
- **Minería de datos:** Al realizar este proyecto se hizo un pequeño ejemplo de encuesta donde se han visto que los datos objetivos y los subjetivos eran diferentes. Las personas no se guían por lo que se debería hacer, sino por lo que creen que deben hacer. A partir de esto, se pueden realizar otras pruebas mucho más complejas, estableciendo una metodología de cómo llevarlo a cabo correctamente. Sería interesante conseguir que tal metodología necesitara un número mínimo de muestras, pero diera una orientación del resultado bastante exacta, por tal de hacer un ataque lo más sigiloso posible.

- **Interacción Humano-Computador Segura:** Enfocándolo como un posible remedio de protección contra la ingeniería social y muchos otros ataques. Se resume en hacer bien las cosas, pero ello conlleva un esfuerzo y una complejidad muy grande, teniendo que valorar por un lado que entiende el usuario y por otro que se está ejecutando por la capa de debajo. No es tan diferente a lo que supone llevar a cabo un ataque de ingeniería social, pero en este caso, se ayudaría a la sociedad de otra manera. Dentro de esto, se puede enfocar en varios casos concretos y hacer patrones de ingeniería de software exclusivos.
- **Factores humanos en la red:** Igual que se ha comentado de los móviles, también hay muchos otros protocolos a ser examinados, como, por ejemplo, la web. Se pueden estudiar cuales son los prejuicios más importantes que existen y como llegan a manipular la conducta de la persona. Si un candado impide que el usuario pulse un botón, o contrariamente le da más ganas. Esto crearía una base de conocimientos que ayudaría a tomar mejores decisiones en otros proyectos externos. Además, se puede plantear el crear una herramienta automática que estudie, detecte y extraiga conclusiones de estos factores humanos.