



**FACULTAD DE CIENCIAS EMPRESARIALES  
ESCUELA ACADÉMICO PROFESIONAL DE  
ADMINISTRACIÓN PÚBLICA**

**TESIS**

**ANÁLISIS DE LAS VULNERABILIDADES EN SEGURIDAD  
INFORMÁTICA DE LOS EQUIPOS DE CÓMPUTO Y  
REDES DE LA MUNICIPALIDAD DISTRITAL DE  
INDEPENDENCIA, MEDIANTE EL USO DE PHISHING**

**2017**

**PARA OPTAR EL TÍTULO PROFESIONAL DE  
LICENCIADO EN ADMINISTRACIÓN PÚBLICA**

**Autor**

**Bach: Alvarado Tolentino Joseph Darwin  
ID ORCID: 0000-0001-8321-8870**

**Asesor**

**CPC. Hernández Terán Saúl  
ID ORCID: 0000-0002-4394-4250**

**Línea de Investigación:  
Gestión Empresarial y Emprendimiento**

**Pimentel-Perú**

**2018**

**ANÁLISIS DE LAS VULNERABILIDADES EN SEGURIDAD INFORMÁTICA DE  
LOS EQUIPOS DE CÓMPUTO Y REDES DE LA MUNICIPALIDAD DISTRITAL  
DE INDEPENDENCIA, MEDIANTE EL USO DE PHISHING 2017**

**Aprobación de la tesis**

---

**Mg. Hernández Terán Saúl**

**Asesor Metodólogo**

---

**Mg. Reyes Reyes Carla Angélica**

**Presidente de Jurado**

---

**Mg. Hernández Terán Saúl**

**Secretario de Jurado**

---

**Mg. Valera Aredo Julio Cesar**

**Vocal de Jurado**

## 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.

Este proyecto recoge los fundamentos de los ataques de ingeniería social en los sistemas informáticos. El objetivo principal es lograr comprender su naturaleza y ser capaces de valorarlos como la amenaza que representan en los trabajadores de la Municipalidad Distrital de Independencia. Por tal de conseguir el objetivo se realizan pruebas de concepto para valorar el riesgo, cambiando a menudo la perspectiva a la del atacante. A raíz de este proyecto, se espera formar una base, para que en un futuro sea posible incrementar la seguridad de dichos equipos informáticos con tecnologías de prevención, detección e intercepción de estos ataques, proponiendo la 'Interacción Humano-Computador Segura' como punto de partida.

Como sabemos hoy en día los atacantes usan maniobras de convencimiento, sea llamadas de teléfono, mensajes de texto, correos electrónicos, redes sociales, con el fin de atraer a las víctimas y lograr su objetivo, que es obtener información valiosa y datos importantes, por lo cual este proyecto va a desmitificar los ataques de ingeniería social, dejando de verla como algo sólo para gente diestra, acercándola al público general para expandir su conocimiento, y del mismo modo ofrecer una nueva visión de todo lo que rodea la seguridad informática, concienciando y alertando de los riesgos que conlleva utilizar Internet y las nuevas tecnologías a los trabajadores de la Municipalidad Distrital de Independencia (Victimas) para que en un futuro no caer en maniobras psicológicas que usan los atacantes.

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 ingeniería social.

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

## **ABSTRACT**

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

This project collects the basics of social engineering attacks on computer systems. The main objective is to understand their nature and be able to value them as the threat they represent in the workers of the District Municipality of Independencia. In order to achieve the objective, concept tests are carried out to assess the risk, often changing the perspective to that of the attacker. As a result of this project, it is expected to form a base, so that in the future it will be possible to increase the security of said computer equipment with technologies of prevention, detection and interception of these attacks, proposing the 'Human-Computer Interaction Segura' as a point of departure.

As we know today, attackers use convincing maneuvers, be it telephone calls, text messages, emails, social networks, in order to attract victims and achieve their objective, which is to obtain valuable information and important data, for which this project will demystify social engineering attacks, not seeing it as something only for right-handed people, bringing it closer to the general public to expand their knowledge, and in the same way offer a new vision of everything that surrounds computer security, raising awareness and warning of the risks involved in using the Internet and new technologies to the workers of the District Municipality of Independencia (Victims) so that in the future they do not fall into psychological maneuvers that the attackers use.

It was concluded that the MDI can count on the best technology, with the latest equipment in the market and the best security software, but if you do not create a real awareness and you do not educate all the employees in the field of IT security, you will not will mitigate the risk of falling into a social engineering attack.

**KEY WORDS:** Social engineering, Phishing, Computer Systems, Risk, Prevention, Detection, Interception, Security.

## ÍNDICE GENERAL

	Página
RESUMEN .....	iii
ABSTRACT .....	iv
CAPÍTULO I: INTRODUCCIÓN.....	9
1.1. Realidad Problemática .....	9
1.2. Trabajos Previos .....	10
1.3. Teorías relacionadas al tema.....	15
1.4. Formulación del Problema.....	23
1.5. Justificación e Importancia de la Investigación .....	23
2.1. Hipótesis .....	25
1.6. Objetivos de la Investigación.....	25
1.7. Definición de la terminología .....	26
CAPÍTULO II: MATERIAL Y MÉTODOS.....	29
2.1. Tipo y diseño de la investigación .....	29
2.2. Localidad e institución donde se desarrollará el proyecto .....	29
2.3. Población y muestra.....	29
2.4. Variables, Operacionalización.....	30
2.5. Matriz de consistencia .....	32
2.6. Técnicas e instrumentos de recolección de datos, validez y confiabilidad.....	33
2.7. Plan de procesamiento y análisis estadístico de la información .....	34
2.8. Aspectos éticos .....	35
2.9. Criterios de rigor científico.....	36
CAPÍTULO III: RESULTADOS .....	38
3.1. Resultados, análisis e interpretación de la investigación .....	39
3.2. Discusión de los resultados de la investigación .....	49
CAPÍTULO IV: CONCLUSIONES Y RECOMENDACIONES.....	52
4.1. Conclusiones.....	52
4.2. Recomendaciones .....	54
REFERENCIAS BIBLIOGRÁFICAS .....	56
ANEXOS.....	61

## ÍNDICE DE ILUSTRACIONES

Ilustración 3.1 - Identificación de peligros en la WAN.....	40
Ilustración 3.2 - Peligros en la Internet .....	40
Ilustración 3.3 - Keyloggers .....	41
Ilustración 3.4 - Mouseloggers .....	41
Ilustración 3.5 - Virus informáticos.....	41
Ilustración 3.6 – Virus w32/netsky-p .....	42
Ilustración 3.7 - Conoce un virus informático.....	42
Ilustración 3.8 - Virus master boot record.....	42
Ilustración 3.9 - Tiene correo electrónico institucional.....	43
Ilustración 3.10 - Frecuencia que revisa el correo electrónico .....	43
Ilustración 3.11 - Tipos de archivos que se reciben por el correo electrónico. ....	44
Ilustración 3.12 - Periodicidad que se reciben los archivos .....	44
Ilustración 3.13 - Trato de la información.....	44
Ilustración 3.14 - Anti-spam.....	45
Ilustración 3.15 - Gusanos informáticos.....	45
Ilustración 3.16 - Puntos potenciales de infección .....	45
Ilustración 3.17 - Características de los troyanos .....	46
Ilustración 3.18 - Alto riesgo con los troyanos.....	46
Ilustración 3.19 - Contramedidas para evitar riesgos con los troyanos .....	46
Ilustración 3.20 - El spyware.....	47
Ilustración 3.21 - Medio de transmisión de spyware y Adware .....	47
Ilustración 3.22 - Rootkits. (Alto riesgo).....	47
Ilustración 3.23 - Backdoors.....	48
Ilustración 3.24 - Escaneo en seguridad informática.....	48
Ilustración 3.25 - Adware .....	48
Ilustración 6.1 - Estado Actual de los sevicios de redes y servidores de la MDI.....	61
Ilustración 6.2 - Estado Actual de los servicios de redes y servidores de la MDI .....	62
Ilustración 6.3 - Estado Actual de la información de la MDI.....	63
Ilustración 6.4 - Estado Actual de los servicios de redes y servidores de la MDI .....	64

## ÍNDICE TABLAS

Tabla 2.1 - Muestra.....	30
Tabla 2.2 - Técnicas de Recolección de datos.....	33
Tabla 2.3 - Criterios éticos de la investigación .....	35
Tabla 2.4 Criterios de rigor científico de la investigación .....	36
Tabla 3.5 - Resultados para la categoría de riesgos en la continuidad del proceso.....	38
Tabla 3.6 - Resultados para la categoría de riesgos en la eficacia del servicio de informática.....	39

# **CAPÍTULO I**

## **INTRODUCCIÓN**



# CAPÍTULO I: INTRODUCCIÓN

## 1.1. Realidad Problemática

Hablar de seguridad informática, tratar temas de análisis de sus vulnerabilidades y los riesgos que conllevan es un tema que afecta a nivel mundial, ya sea a instituciones, empresas u organizaciones de diversos sectores.

Todo este contexto se trata en las formas de ataque o de vulnerar datos usando alguna técnica de penetración de archivos, modificación de los mismos o solo espiar con la finalidad de lograr un fin específico del atacante.

Es por ello que la investigación va abarcar el tema en forma de analizar las vulnerabilidades en seguridad informática en una institución pública.

Viendo la realidad de la institución, se puede verificar que la Municipalidad Distrital de Independencia no cuenta con un plan de actividades, dichas actividades que se realizan son improvisadas con una consecución que varía de mes a mes, esto no le ha ratificado llevar a cabo una actividad efectiva para adelantar y notar a los cambios que podrían afectar los objetivos organizacionales, así como fallar las bases para mitigar el riesgo que eso conlleva.

Otro problema es que en la Municipalidad Distrital de Independencia no se cuenta con un ambiente adecuado en donde debería estar ubicado los servidores y equipos de cómputo que alojan toda la información de la MDI, aparte hay escasez de buenos equipos informáticos.

Otro agobio es que en la Municipalidad Distrital de Independencia no se cuenta con un ambiente correcto en donde se ubiquen los equipos de cómputo y servidores que alojan toda la documentación del Municipio, aparte no se cuenta con buenos equipos informáticos.

Y como sabemos hoy en día los atacantes usan maniobras de convencimiento, sea llamadas de teléfono, mensajes de texto, correos electrónicos, redes sociales, con el fin de atraer a las víctimas y lograr su objetivo, que es obtener información valiosa y datos

importantes, por lo cual este proyecto va a analizar las vulnerabilidades en seguridad informática, al mismo tiempo que va a desmitificar los ataques de ingeniería social, dejando de verla como sospecha exclusivamente para genitro diestro, acercándola al representativo habitual para expandir su entendimiento.

## **1.2. Trabajos Previos**

### **1.2.1. A Nivel Internacional**

(Roxin, 2004), sostiene que, dice que la riqueza y fragmentación de las concepciones modernas en cuanto a los valores que llegó a crear el sujeto, facilitaron que lo costumbrista, lo clerical y lo íntegro perdieran poder organizador en la sociedad.

Afirma, asimismo, que, alce este completado, fue necesaria la manifestación del directo para aceptar esas funciones, y que en conocimiento fue, para evaluar a través de obligaciones y tributo, lo que el mundo consideraba que se podía hacer en forma libre sin impactar lo imparcial, y lo que se debe meter un puro en casualidad se afecte de otras personas sus derechos.

Para el autor, esta manera ancestral de regulación del rectilíneo se mantiene válido, con las limitaciones propias de que el origen del directo, no puede residir nunca de acuerdo a los cambios y transformaciones de las sociedades, y siempre han existido de una u otra forma vacíos legales, que las leyes a través de los actos de implementar justicia han solucionado generalmente en manera satisfactoria.

Aunque, los agentes en los últimos años, específicamente desde el proceso de la saber de la tecnología de la explicación y la información, la comunidad tiene cambios tan rápidos y profundos, y han resucitado una cantidad insospechada de ilícitos penales ligados a tecnología y a la instrucción de la explicación y la documentación, que la estudios del recto no alcanza a fastidiar y se generan vacíos legales que impiden la desafío frente a la delincuencia, llamado en estos tiempos como delitos informáticos.

Asimismo, indica que las categorías penales de delitos considerados en las legislaciones peruanas, resultan anacrónicos para el entorno auténtico, ya que cuando se redactó el real fuero penal de 1991, el licurgo franquista no obra en cuenta los delitos informáticos.

Los delitos informáticos tienen su radio de acción ante todo en los atentados versus los derechos del autor, quebrantamiento de la franqueza unipersonal, falsificación de documentos informáticos, entre otros. Si se inspecciona el sistema galera peruano, se puede sentir que el texto punitivo tipifica ciertas conductas capital de ser cometidas mediante nociones informáticos, el turismo sexual infantil (artículo 181-A); la pornografía infantil (artículo 183-A); el trampa intensificado empleado sistema de transferencia electrónica de fondos de la telemática en familiar, (numeral 3 del segundo acápite del artículo 186); el infracción de engaño en la administración de personas jurídicas en la modalidad de uso de capital informáticos (Inciso 8 del artículo 198), e además el infracción de daños (artículo 205), desde la vertiente del embestida versus el hardware (en su índole de acertadamente ajuar), el borde indebido a una colchoneta de datos,( artículo 207-A), el boicot informático (artículo 207-B) y sus agravantes (artículo 207-C).

Al respecto (Tiedermann, 2000), refiere que la labranza del seguido no es permanecer puñado a viejas tipos teóricas que nado sirven destino, por otra parte, es adaptarse y proveerse de nuevos modos de profilaxis y favor de la comunidad. Es por este litigio que el recto galera debe inspeccionarse a sí mismo, y encuadrarse en esta historia que protejan a las personas, mas no ocultarse en acequias legales que no ayudan a nadando.

El mismo (Peña, 2007), manifiesta que la nebulosa del ciberdelito, requiere un observación particular y conocimientos de enjuiciamiento, para poder acatar con la labor de arreglar suficientemente estos delitos con miras hacia una adecuada protección social, dado que el éxito de la sociedad informática es progresiva en nuestro entorno, ya sea en el franja audiencia o sea en el desprovisto (el factoría, la movimiento bancaria, la acción industrial, el negocio de los particulares y empresas, etc.)

(Hugo, 2004), en su investigación menciona que ha llegado el segundo que el recto mazmorra responda a las múltiples exigencias sociales que el mundo moderno reclamo, y de este modo, rompa su sólida franja anquilosada y evolucione conjuntamente con el recurso del estudio científico, para así permitir el vivo resguardo de la tranquilidad y de la comunidad, visto que, a la estimación, se está quedando impedido en esta asignatura de los novísimos delitos informáticos.

(Rubio, 2015) en su tesis Doctoral: “*Un Marco para el Análisis de Riesgos en Ciberseguridad*” tiene como objetivo intercalar un escenario integrado para la observación de inconvenientes en ciberseguridad que facilite la toma de decisiones respecto a la soltura de los sistemas considerados.

Menciona que la mayor preocupación que debe resolverse en el recinto de la sociedad de la información, es la inexistencia de modelos de control y prospección de propina sofisticados, que estén al nivel de las factoras. Para ello, la metodología de deber que llevó a maroma ha constado de una fase de investigación e investigación de los marcos y metodologías existentes en la actualidad, de la misma manera que su implantación y uso en entidades privadas y administraciones públicas. después, analizó los resultados observados, viendo las deficiencias encontradas en dichas implantaciones en casos reales y las sugerencias trasladadas por los propios afectados. Siguiendo a esa etapa hubo una profesión de información y trabajo de recorrido, a fin de delimitar medios soluciones a las carencias actuales, diseñando las propuestas que en su juicio se desarrollan. por último, dichas propuestas se implantaron en casos reales, analizando sus ventajas sobre los anteriores modelos usados.

(Aguirre, 2017) en su tesis de Maestría: “*Ciberseguridad en Infraestructuras Críticas de información*” menciona el importante acrecentamiento del uso de diversas tecnologías de la documentación para los víveres de servicios vitales de una comarca con la escasez de controles de ciberseguridad en las infraestructuras que soportan dichos servicios. en consecuencia, servicios esenciales tales como las telecomunicaciones o la fortaleza, están utilizando masivamente tecnologías de la documentación porque los grandes beneficios que esto acarrea, no obstante, la administración de la ciberseguridad es una debilidad, a la que se presta poca expectación. Se propone en consiguiente, profundizar la exploración de la ciberseguridad, enfocándose en la ficha de servicios críticos y en el cobijo de las infraestructuras de documentación que contribuyen a su preparación.

De esa manera, se plantea como indefinido precisar los mecanismos y controles de compostura más relevantes que los responsables o proveedores de servicios críticos deben implementar en las infraestructuras críticas, para protegerlas de las amenazas que pudieran afectarlas.

### 1.2.2. A Nivel Nacional

Según (Meza, 2012) en su Tesis titulada *“El tipificado de consumidor razonable aprovechado en los consumos fraudulentos generados por clonación”*, nos dice: La generalidad de personas, hoy en día, posee una tarjeta de préstamo, normalmente para el pago de posesiones y/o emplear servicios. guapo que la totalidad de nosotros a la hacienda firmado el contrato de tarjeta de crédito no lo ha sabido y, es más, no sabe que tiene una responsabilidad de control de la misma; en otras palabras, no sabe que, al momento de hacer uso de la misma, tiene la alianza de vigilarla de manera que no vaya ser perjudicado de una clonación. por el contrario, muchas circunstancias, entre ellos la aplomo que se tiene al deteriorar en un filial, 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 singladura, las tarjetas de préstamo han servido como un ámbito eficiente para facilitar las transacciones comerciales; sin embargo, el mismo adelante tecnológico que nos trajo ventajas ha traído un repertorio de plus.

Uno de las molestias que nos conlleva el servirse las tarjetas de empréstito son los consumos fraudulentos, que son aquellos consumos realizados por un tercer sujeto ajena a las partes intervinientes en el sistema de tarjetas de crédito. Al respecto, si perfectamente 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 clase, de forma que podamos apechugar el unificado de consumidor que se necesita para enemistar este segmento de operaciones.

(Sanchez, 2017) en su tesis *“Adopción de Estrategias de Ciberseguridad en la Protección de la Información en la Oficina de Economía del Ejército, San Borja (2017)”* menciona que es inquietante la inoperancia y poco interés por parte del estado en no soltar las partidas presupuestarias, ya que con ellos se podría implementar una estrategia de Ciberseguridad, las autoridades deberían captar que en la actualidad el ciberespacio e Internet juegan un papel muy notable en distintas áreas de la economía, e invertir en ciberseguridad permite mejorar su certeza y seguridad. En sectores como

la banca, las empresas de comunicaciones, la optimización del uso del vigor y las redes de disposición inteligentes puede utilizar la tecnología de la documentación para atesorar bienes en otras áreas. en conclusión, las autoridades de evento no le están dando la portento que se debe al sinopsis de ciberseguridad, lo cual representa un descuido muy pesado puesto que se encuentran comprometidos muchos de los sectores del vivido (oportunidad que se encuentran provistos de infraestructuras críticas) y si se ven vulneradas una de estas, se puede ver muy comprometida la compensación económica y social de nuestro comarca, por ello no se debe dar con cuentagotas esfuerzos al consumir en este tipo de tecnología, que nos permita montar con información definitiva versus las múltiples amenazas que hoy se encuentran en el ciberespacio.

(Zubiate y Vilchez, 2017) en su tesis de Maestría: *“Propuesta de implementación de un modelo de gestión de ciberseguridad para el centro de operaciones de seguridad (SOC) de una empresa de telecomunicaciones”* menciona que cuando se plantea la implementación de un nuevo modelo de Gestión de Ciberseguridad para el área de servicios de seguridad de una empresa Telco, se propone con la artículo de estilizarse los objetivos estratégicos de la organización, definiendo: funciones, procesos, roles, y responsabilidades que aseguren las actividades del modelo con el fin de suscitar un decisión junto a la empresa. La administración de la ciberseguridad tiene recién pocos antigüedad de investigación, no obstante con una cambio exponencial, ya que la pureza de acceso al internet y su claro uso trae muchos ingresos y a la vez molestias los cuales hay que estar preparados, en la fama existe aportes de investigadores donde realizan estudio de modelos de ciberseguridad que se pueden atribuir a la compañía, la cual contempla las áreas de seguridad de Datos, calma de programa, desenvoltura de componentes, seguridad de vinculación, confianza de Sistemas, seguridad de personas, firmeza Organizacional y soltura Social.

Definiendo como imparcial suministrar al área del SOC un marco de ciberseguridad para producir una posibilidad que le permita implantar, negociar, monitorear, corroborar y mejorar los controles de Ciberseguridad, con el fin de ser un SOC de referencia y presentarse a ser competitivo en el mercado.

### **1.3. Teorías relacionadas al tema**

#### **1.3.1. Ingeniería Social**

Según (Kaspersky.com, 2017), la ingeniería social son técnicas que usan los cibercriminales para atacar a los usuarios ingenuos y estos envíen sus datos confidenciales, a la vez pueden infectar sus PCs con malware o hacer que abran enlaces a sitios infectados.

De igual forma, estos expertos en aplicar técnicas de ingeniería social crecen cada vez que avanza la tecnología, y en la actualidad existen muchos usuarios que no son conscientes de la veracidad de sus datos y no saben con realidad cuál es su información verdadera y como llegar a protegerla.

##### **1.3.1.1. La ingeniería social (IS), su funcionamiento y medidas de protección**

La mayoría de los segmentos de ataques llevan alguna clase de IS. Por ejemplo, tenemos, los clásicos e-mails de "phishing" y engaños por la web. Los e-mails de phishing intentan disuadir, persuadir y captar a los usuarios de que su origen es legítimo con la atención de que lograr robar la documentación o datos de la entidad, por imprudente que parezcan, en cambio, los e-mails que contienen archivos adjuntos con algún tipo de virus a menudo aparentan salir de contactos confiables u ofrecen espacio multimedia que parece inofensivo, como fotos o videos "entretenidos" o "sensibles".

Otras veces, los aficionados en usar técnicas de IS usan métodos más simples de IS para perpetrar a una red u ordenador. también, un pirata informático puede alternar la compañía con perspicacia de una gran cantidad de oficinas, explorar a los trabajadores que estén usando sus computadoras portátiles u otro medio de comunicación y advertir que tipo de dispositivos están usando para atacarlos. Con esta táctica los piratas informáticos ganan un gran número de contraseñas y nombres de beneficiarios, todo sin aprieto de nada, ni de dirigir o enviar un e-mail, ni de registrar un ataque que quede documentado.

Otros ataques requieren una nueva enérgica entre el asaltante y la dañado; en estos casos, el asaltante presiona al beneficiario para que le otorgue inicio a la red con la

disculpa de unas hostilidades cuerdo que es mecánico administrar de inmediato. Los atacantes utilizan en plano metropolitano la enojo, la tropiezo y la pesadumbre para bajarse a los usuarios de que necesitan su ayuda y no pueden negársela. finalmente, es distinguido prestar espera a la ingeniería social como una trayectoria para provocar disputa. Numerosos trabajadores y consumidores no se dan perla de que, con aria una centella de mensaje (como la celebridad, la década de salida o la mando), los piratas informáticos pueden conseguir a múltiples redes haciéndose correr por usuarios legítimos o dependencia del personal de TI. a posteriori de lograrlo, les resulta legible sanar contraseñas y durar principio prácticamente incondicional.

La influencia versus la IS empieza con educarnos; las personas necesitan conocer que no deben hacer click en enlaces sospechosos y siempre deben de chequear sus credenciales que les envían vía e-mail u otro medio digital, además en la compañía u organización se tiene que tener medidas de seguridad, si las condiciones sociales logran su cometido, el resultado es una infección por malware. Para disputar los troyanos, rootkits y otros bots, es interesante con implantar medidas de seguridad al acceso del Internet.

### **1.3.2. Phishing**

Phishing o suplantación de identidad, Es un término informático que denomina un segmento de abuso informático y que se comete mediante el uso de una variedad de técnicas de ingeniería social caracterizado por observar y captar información confidencial de forma fraudulenta (como puede ser una clave o documentación detallada sobre tarjetas de crédito u otra documentación bancaria). El cibercriminal, entendido como phisher, se hace aventajar por un tipo u organismo de entereza en una supuesta comunicación oficial electrónica, por lo habitual un e-mail, o algún sistema de transporte instantánea o además utilizando también llamadas telefónicas.

### **1.3.3. Historia del Phishing**

#### **1.3.3.1. Origen del término**

El vocablo Phishing deriva del acento inglés "fishing" (pesca), haciendo indirecta a la investigación de efectuar que las personas "muerdan el anzuelo".



Quienes practican el Phishing se le ha denotado con el termino phisher. además, se dice que Phishing es la conmovición de “password harvesting fishing” (recoge y pesca de contraseñas), por el contrario, esto probablemente es un acrónimo retroactivo, dado que la escritura 'ph es comúnmente utilizada por hackers para sustituir la f, como raíz de la antigua manera de hacking telefónico aprendida como phreaking.

La primera indicación de la definición Phishing data de enero de 1996. Se dio en el grupo de mensajes de piratas informáticos alt.2600, por el contrario, es potencial que el término ya hubiera redivivo anteriormente en el estampado impresa del boletín de crónicas hacker 2600 Magazine. La definición Phishing fue adoptado por quienes intentaban "pescar" cuentas de miembros de AOL.

### **1.3.3.2. Intentos de Phishing en la actualidad**

Los intentos más recientes de Phishing han tomado como indefinido a compradores de bancos y servicios de pago en tangente. por el contrario, el arquetipo que se signó en la primera imagen es manda por phishers de forma indiscriminada con la perspectiva de hallar a un comprador de dicho banco o servicio, aprendizajes recientes muestran que los phishers en un inicio son capaces de establecer con qué edicto una aparente dañado tiene relación, y de ese modo dirigir un e-mail, falseado apropiadamente, al supuesto lastimado.

En términos generales, este encurtido cerca de objetivos específicos en el Phishing se ha denominado spear Phishing (textualmente pesca con sarcasmo).

Los sitios de Internet con fines sociales incluso se han convertido en objetivos para los phishers, dado que mucha de la documentación provista en estos sitios puede ser utilizada en el impulso de identidad. Algunos experimentos han otorgado un impuesto de éxito de un 90% en ataques Phishing en redes sociales.

Según informes a finales del año 2006 y a inicios del año 2007 un gusano informático se apropió de algunas páginas de la página web MySpace obteniendo re-direccionar los enlaces de estilo que apuntaran a una website diseñada para hurtar documentación de beneficio de los usuarios.

#### 1.3.4. Técnicas de Phishing

La mayoría de los métodos de Phishing utilizan el apaño en el diseño del e-mail para lograr que una asociación parezca una dirección legítima del organismo por la cual se hace exceder el aparente. URLs manipuladas, o el uso de subdominios, son trucos comúnmente usados por phishers; por pauta, en esta URL: <http://www.banco.com/abc>, en la cual el mensaje mostrado en el encabezado de la web no corresponde con la dirección fiel a la cual conduce. Otro dechado para tapar enlaces es el de disfrutar direcciones que contengan el talento arroba: @, para después preguntar el renombre de usuario y contraseña (antónimo a los estándares).

Por prototipo, la conexión: <http://www.google.com@member.dominio.com/> puede falsear a un observador fortuito y hacerlo suponer que la asociación va a abrir en la página de [www.google.com](http://www.google.com), cuando efectivamente la vinculación envía al navegador a la página de [member.dominio.com](http://member.dominio.com) (y al estudiar entrar con el nombre de usuario de [www.google.com](http://www.google.com), si no existe tal usuario, la página abrirá normalmente). Este razonamiento ha sido erradicado desde entonces en los navegadores de Mozilla e Internet Explorer.

Otros intentos de Phishing utilizan comandos en JavaScript para alterar el enrolamiento de direcciones. Esto se hace poniendo una imagen de la URL de la organización legítima sobre el alistamiento de direcciones, o terminando la incorporación de direcciones inicial y abriendo una nueva que contiene la URL ilegítima.

En otro método popular de Phishing, el agresor utiliza contra la dañado la acreditada constitución de programa del mandato o servicio por el cual se hace superar. Este segmento de ofensiva resulta particularmente problemático, visto que dirige al usuario a empezar sesión en la propia página del banco o servicio, donde la URL y los certificados de soltura parecen correctos. En este método de ataque (sabido como Cross Site Scripting) los usuarios reciben un mensaje diciendo que tienen que "comprobar" sus cuentas, seguido por un enlace que parece la landing page auténtica; en ingenuidad, el parentesco está cambiado para llevar a cabo esta ofensiva, también es muy esforzado de detectar si no se tienen los conocimientos necesarios.

### **1.3.5. 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.

### **1.3.6. Seguridad informática**

#### **1.3.6.1. Concepto:**

Hablar de seguridad informática, en el área de la computación apunta en el favor del abastecimiento computacional y todo ello se relaciona con la SI (incluyendo la documentación contenida). Para ello existen una cantidad de protocolos, estándares, métodos, herramientas, reglas y leyes concebidas para reducir y mitigar los posibles riesgos a la seguridad o a la documentación.

La seguridad informática comprende software, bases de datos, metadatos, archivos y todo lo que la empresa valore (esforzado) y signifique un peligro si ésta llega a manos de otras personas. Esta clase de documentación se conoce como documentación privilegiada o confidencial.

La definición de seguridad de la información no es lo mismo que el de seguridad informática, este último solamente se encarga de la seguridad en la atmósfera

informática, sin embargo, la seguridad de la información puede arraigar en diferentes nociones o formas, y no solo en medios informáticos.

#### **1.3.6.2. Análisis de riesgos:**

El activo más destacado 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 lógica que consiste en la tenacidad de barreras y procedimientos que resguardan el filo a los datos y exclusivamente permiten aceptar a ellos a las personas autorizadas para hacerlo.

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

Los fundamentos para conseguirlo son:

- a) Prohibir el acceso (de personas de la organización y de las que no lo son) a los programas y archivos.
- b) Garantizar que los operadores puedan trabajar pero que no puedan modificar los programas ni los archivos que no correspondan (sin una supervisión minuciosa).
- c) Garantizar que se utilicen los datos, archivos y programas correctos en/y/por el procedimiento elegido.
- d) Garantizar que la información transmitida sea la misma que recibe el destinatario al cual se ha enviado y que no le llegue a otro.
- e) Garantizar que existan sistemas y pasos de emergencia alternativos de transmisión entre diferentes puntos.
- f) Instaurar 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.

#### **1.3.6.3. Análisis de riesgo y sus elementos**

Cuando se pretende esbozar una técnica para implementar una exploración de riesgo informático se pueden acoger los siguientes puntos como referencia a seguir:

- Planes para reducir o mitigar los riesgos.

#### **1.3.6.3.1. Análisis de impacto al negocio**

El desafío es achacar estratégicamente los posibles para cada conjunto de desenvoltura y capital que intervengan, basándose en la gracia potencial para el negocio, respecto a los diversos incidentes que se deben ejecutar. Para medir la sucursal de prioridades, el sistema de administración de incidentes necesita entender la valentía de los sistemas de documentación que pueden ser potencialmente afectados por incidentes de serenidad.

Esto puede trasladar que alguno internamente de la compañía asigne una osadía monetaria a cada conjunto y un fichero en la red o asignar una audacia alusiva a cada sistema y la documentación sobre ella. en el interior de la utilidad para el sistema se pueden indagar: Confidencialidad de la documentación, la integridad (aplicaciones e documentación) y por último la Disponibilidad del sistema.

Cada uno de estos valores es un sistema independiente de la importación, ahora supongamos que, en el futuro se trate de normalizar, un caballerizo web afluencia pueden tener los requisitos de confidencialidad de despreciable (ya que toda la documentación es pública), a pesar de de suscripción disponibilidad y los requisitos de respetabilidad. En contradicción, un sistema de planificación de recursos empresariales (ERP), sistema puede favor ínclito puntaje en las tres variables. Los incidentes individuales pueden metamorfosear ampliamente en términos de alcance e prestigio.

#### **1.3.6.3.2. Puesta en marcha de una política de seguridad**

Al presente las legislaciones nacionales de los Estados, obligan a las empresas, instituciones públicas a implantar una política de confianza.

Ejemplo: En España la Ley Orgánica de favor de Datos o llamada LOPD y su normativa.

Estos mecanismos permiten conocer que los operadores tienen solamente los permisos que se les dio.

Por eso en lo relativo a inventar una política de seguridad, conviene:

- Tramar reglas y procedimientos para cada servicio de la compañía.
- Delimitar las acciones a comenzar y escoger las personas a contactar en acontecimiento de detectar una posible intrusión.
- Sensibilizar a los operadores con los problemas ligados con la entereza 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 obtener que los medios y derechos de paso sean coherentes con la política de soltura definida. Incluso, como el gerente suele ser el único en entender acertadamente el sistema, tiene que derivar al cielo cualquier inquietud e información relevante sobre la serenidad, y eventualmente recomendar estrategias a aovar en jornada, de la misma manera que ser el área de filo de la comunicación a los trabajadores sobre problemas y recomendaciones en definición de soltura informática.

#### **1.3.6.3.3. Respaldo de información**

La información compone el activo más importante de las empresas, pudiendo encontrarse afectada por muchas circunstancias tales como robos, incendios, fallas de disco, virus u otros. Desde la perspectiva de la empresa, uno de los problemas más importantes que debe gestionar es la protección constante de su información crítica.

La disposición más valiosa para la protección de los datos es contar una buena política de copias de entereza o backups: Este debe intercalar copias de seguridad total (los datos son almacenados en su conjunto la primera vez) y copias de seguridad incrementales (únicamente se copian los ficheros creados o modificados desde el último backup). Es primordial que las empresas programen los backups en función de la dimensión de información generada y la cantidad de equipos de respaldo de datos.

Un excelente sistema de respaldo debe sumar con ciertas características imprescindibles:

- **Continuo:** El respaldo de datos debe ser totalmente automático y continuo. Debe funcionar de forma clara, sin injerirse en las tareas que se encuentra realizando el usuario.
- **Seguro:** Muchos softwares de respaldo contienen cifrado de datos (128-448 bits), lo cual debe ser hecho localmente en el equipo antes de la remisión de la información.
- **Remoto:** Los datos deben quedar almacenados en dependencias alejadas de la empresa.
- **Mantenimiento de versiones anteriores de los datos:** Se debe contar con un sistema que permita la recuperación de versiones diarias, semanales y mensuales de la información.

#### 1.4. Formulación del Problema

Actualmente en la ciudad de Huaraz y la Municipalidad Distrital de Independencia, hay un serio problema con la seguridad de la información, tanto es el caso que mientras más avanza la tecnología, aparecen nuevas formas de robo de información, ya sea en físico o digital, a la vez que en la Municipalidad Distrital de Independencia hasta ahora no implementan estrategias de seguridad informática en el uso de datos, lo cual si ocurre un robo o pérdida de información perjudicaría en gran parte a la entidad, retrasando los tramites y procesos administrativos que se llevan diariamente.

Siendo así, se plantea la siguiente cuestión:

¿Mediante el uso de la ingeniería social y phishing, se analizará e identificará las vulnerabilidades en seguridad informática de los equipos tecnológicos de la Gerencia de Administración y Finanzas de la Municipalidad Distrital de Independencia?

#### 1.5. Justificación e Importancia de la Investigación

##### 1.5.1. Teórica

Existen pocas investigaciones en el ámbito local sobre los ataques de ingeniería social, el cual una investigación de este tipo sería beneficiosa para la Municipalidad Distrital de Independencia, para las instituciones del distrito de Independencia y las empresas de la ciudad de Huaraz.

### **1.5.2. Tecnológico**

Hoy en día las nuevas tecnologías han evolucionado conforme aparecen las necesidades de las personas, y consecuentemente la importancia de crear, implementar y mejorar las ya existentes, por lo que esta investigación lograra dar una visión de cómo son los ataques de ingeniería social y phishing, como prevenirlos o mitigar los riesgos que conllevan ser afectador por dichos ataques.

### **1.5.3. Operativo**

Mientras más avanza la tecnología, aparecen nuevas formas de robo de información, ya sea en físico o digital, por lo tanto, el presente proyecto buscara proyectar la forma en cómo se realizan estos ataques, su manera de persuadir y realizar el robo, a la vez de como reducirlos o mitigarlos.

### **1.5.4. Metodológico**

En el presente proyecto se utilizará una metodología de reducción de riesgos por ataques de ingeniería social y phishing, a la vez se concientizará a los usuarios a no dejarse persuadir por los atacantes que usan estas técnicas, de esa forma crear una conciencia en los trabajadores de la Municipalidad Distrital de Independencia, a la vez que esta investigación servirá para futuras investigaciones en el ámbito de la seguridad informática y seguridad de la información.

### **1.5.5. Económico**

En el ámbito económico podemos apreciar que, si ocurre un ataque de ingeniería social, se habla de pérdidas económicas y al mismo tiempo de información valiosa, por lo tanto, prevenir de un ataque de ingeniería social nos ayudara a proteger nuestra información y reducir perdidas económicas.

### **1.5.6. Social**

Actualmente los avances de nuevos proyectos tecnológicos optimizan las tareas y crean nuevas aplicaciones, los cuales ayudan a que la humanidad cuente con



herramientas para confrontar las futuras necesidades, ello dará realce a crear nuevos proyectos de investigación.

Además, se dará a conocer a la ciudad de Huaraz mediante esta investigación, de qué manera los ataques de ingeniería social influyen en la seguridad informativa.

## **2.1. Hipótesis**

Mediante el uso de ingeniería social y phishing se va lograr analizar e identificar las vulnerabilidades en seguridad informática de los equipos tecnológicos de la MDI.

## **1.6. Objetivos de la Investigación**

### **1.6.1. Objetivo General:**

Identificar métodos de ingeniería social y phishing para el análisis de las vulnerabilidades a fin de mejorar la seguridad informática de los equipos tecnológicos de la Gerencia de Administración y Finanzas de la Municipalidad Distrital de Independencia.

### **1.6.2. Objetivo Específicos:**

1. Identificar métodos de ingeniería social para medir la seguridad de la información de los equipos de tecnológicos de la Gerencia de Administración y Finanzas de la Municipalidad Distrital de Independencia
2. Desmitificar los ataques de ingeniería social, dejando de verla como algo sólo para expertos, acercándola a la población y a los trabajadores de la Gerencia de Administración y Finanzas de la Municipalidad Distrital de Independencia para transmitir su prudencia.
3. Entregar una nueva visión de todo lo que envuelve a la seguridad informática, con un plan de capacitación sensibilizando y advirtiendo de los riesgos que sobrelleva utilizar el Internet y las tecnologías informáticas al personal de la Gerencia de Administración y Finanzas de la Municipalidad Distrital de Independencia.

## 1.7. Definición de la terminología

- Adware: Programa spyware que simula al usuario pulsando ciertos banners de publicidad.
- Captcha: Imagen distorsionada legible para un humano, pero no para una máquina.
- Cracker: Persona que hace delitos en Internet.
- 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.
- E-crime: Crimen electrónico. Cualquier tipo de crimen que se produce en Internet.
- Exchangeable Image file Format (EXIF): Formato de las imágenes JPG que permite incrustar en su interior información oculta (metadatos).
- Exploit: Programa que se utiliza para obtener privilegios en un sistema local o remoto.
- Hishing (Hardware Phishing): Denominación de ataque de phishing basado en utilizar periféricos para ocultar troyanos o otro tipo de malware debido a la poca sospecha que levanta.
- Ingeniería social (IS): Arte de persuadir a alguien para que haga algo sin su voluntad.
- Ingeniería social automatizada (ISA): Término utilizado para referirse a lograr que se efectúe un ataque de IS sin depender de una persona.
- Keylogger: Programa spyware que captura las teclas introducidas.
- Malware: Conjunto de programas maliciosos para un internauta.
- Man-In-The-Middle: Ataque que consiste en interceptar la comunicación entre dos individuos.
- Payload: Encapsulado de datos que permite enviar acciones específicas por el atacante.
- Pharming: Ataque a través de la suplantación de servidores DNS para robar credenciales.
- Phisher: Persona que envía phishing.
- Phishing: Engaño masivo a través de correos electrónicos.

- **Pickpocking:** Disciplina que se encarga de estudiar como usurpar cualquier objeto de una persona sin que esta lo perciba.
- **Proxy:** Es un programa o dispositivo que realiza una acción en representación de otro.
- **Rootkit:** Troyano que invade la parte más crítica del sistema operativo.
- **Shoulder Surfing:** Técnica que consiste en espiar por encima del hombro a la víctima cuando introduce una contraseña o un dato sensible.
- **SmiShing (SMS Phishing):** Denominación de ataque de phishing basado en enviar un mensaje de texto haciéndose pasar por una entidad oficial.
- **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:** Programa espía que recopila información del usuario para enviarla a una empresa externa. Esta dentro del conjunto de malware.
- **Tabnapping:** Ataque malicioso dirigido al navegador del usuario que simula una nueva pestaña pidiendo las credenciales sin que el usuario la haya abierto.
- **Troyano:** Programa malicioso que obtiene el control sobre un sistema remoto.
- **Virus:** Programa malicioso que se propaga por sí sólo en la red.
- **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.
- **Whisphing (Whale Phishing):** Denominación de ataque de phishing basado en usar una técnica concreta sobre una población muy amplia.

# **CAPÍTULO II**

## **MATERIAL Y MÉTODO**

## **CAPÍTULO II: MATERIAL Y MÉTODOS**

### **2.1. Tipo y diseño de la investigación**

La investigación es Descriptiva Simple, porque los datos adquiridos en la investigación son directamente de la observación porque se va describir hechos reales, en un período y espacio definitivo.

Por lo tanto, al realizar la presente tesis el investigador busca y almacena información relacionada con la SI, GSI, y técnicas de ingeniería social y phishing.

### **2.2. Localidad e institución donde se desarrollará el proyecto**

La tesis se desarrollará en la Municipalidad Distrital de Independencia.

### **2.3. Población y muestra**

#### **2.3.1. Población:**

- Personal de la Subgerencia de TIC.
- Personal de la Gerencia de Administración y Finanzas.
- Personal Administrativo de diferentes áreas de la Municipalidad Distrital de Independencia.

#### **2.3.2. Muestra**

Áreas funcionales de la Municipalidad Distrital de Independencia, los cuales se involucran en el desarrollo de la tesis.

Para la determinar de la muestra, se consideró el método no probabilístico.

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

Tabla 2.1 - Muestra

<b>Areas</b>	<b>Total</b>
Subgerencia de TIC	6
Gerencia de Administración y Finanzas	4
Áreas específicas y funcionales de la Municipalidad Distrital de Independencia	10
<b>Total</b>	<b>20</b>

## **2.4. Variables, Operacionalización.**

### **2.4.1. Variable Independiente**

Análisis de las vulnerabilidades usando técnicas de ingeniería social y phishing

### **2.4.2. Variable Dependiente.**

Seguridad Informática de los Equipos de tecnológicos de la Gerencia de Administración y Finanzas de la MDI.

### 2.4.3. Operacionalización de variables

Variable	Definición Conceptual	Dimensiones	Indicadores	Unidad de medida	Escala
<b>Independiente</b>	Es una expresión informática que menciona un tipo de abuso informático y que se comete mediante el uso de un tipo de ingeniería social determinado por querer obtener información confidencial de forma engañosa (como puede ser una contraseña o información precisa sobre tarjetas de crédito u otra información financiera).	Medidas de seguridad ante ataques de ingeniería social.	✓ Porcentaje de Incidencias de ataque de ingeniería social.	Nº Ataques	Ordinal
1. Análisis de las vulnerabilidades usando técnicas de ingeniería social y phishing					Porcentaje
Variable	Definición Conceptual	Dimensiones	Indicadores	Unidad de medida	Escala
<b>Dependiente.</b>	Se concibe por seguridad informática al conjunto de normas, procedimientos y herramientas, que tienen como objetivo garantizar la disponibilidad, integridad, confidencialidad y el buen uso de la información que ocupa en un sistema de datos.	Medidas de seguridad en equipos de cómputo y redes.	✓ Nivel de Integridad	Muy bueno, Bueno, Regular, Malo, Muy malo	Nominal
2. Seguridad Informática de los Equipos de tecnológicos de la Gerencia de Administración y Finanzas de la Municipalidad Distrital de Independencia			✓ Nivel de Confidencialidad		
			✓ Nivel de disponibilidad		

## 2.5. Matriz de consistencia

ANÁLISIS DE LAS VULNERABILIDADES EN SEGURIDAD INFORMÁTICA DE LOS EQUIPOS DE CÓMPUTO Y REDES DE LA MUNICIPALIDAD DISTRITAL DE INDEPENDENCIA, MEDIANTE EL USO DE PHISHING 2017					
PROBLEMAS	OBJETIVOS	HIPÓTESIS	VARIABLES DE ESTUDIO	INDICADORES	METODOLOGÍA
<b>GENERAL</b>	<b>GENERAL</b>	<b>GENERAL</b>	<b>INDEPENDIENTE</b>	<b>INDEPENDIENTE</b>	<b>Tipo de estudio</b>
¿Mediante el uso de la ingeniería social y phishing, se analizará e identificará las vulnerabilidades en seguridad informática de los equipos tecnológicos de la Gerencia de Administración y Finanzas de la Municipalidad Distrital de Independencia?	Identificar métodos de ingeniería social y phishing para el análisis de las vulnerabilidades a fin de mejorar la seguridad informática de los equipos tecnológicos de la Gerencia de Administración y Finanzas de la Municipalidad Distrital de Independencia.	<b>Hipótesis H1</b>	Análisis de las vulnerabilidades usando técnicas de ingeniería social y phishing	Porcentaje de Incidencias de ataque de ingeniería social .	Exploratorio, tecnológico.
	<b>ESPECIFICO</b>	Mediante el uso de ingeniería social y phishing se va lograr analizar e identificar las vulnerabilidades en seguridad informática de los equipos tecnológicos de la Gerencia de Administración y Finanzas de la Municipalidad Distrital de Independencia	<b>DEPENDIENTE</b>	<b>DEPENDIENTE</b>	<b>Diseño de investigación</b>
	1. Identificar métodos de ingeniería social para medir la seguridad de la información de los equipos de tecnológicos de la Gerencia de Administración y Finanzas de la Municipalidad Distrital de Independencia		Seguridad Informática de los Equipos de tecnológicos de la Gerencia de Administración y Finanzas de la Municipalidad Distrital de Independencia	Nivel de Integridad	Descriptivo Simple.
	2. Desmitificar los ataques de ingeniería social, dejando de verla como algo sólo para expertos, acercándola a la población y a los trabajadores de la Gerencia de Administración y Finanzas de la Municipalidad Distrital de Independencia para transmitir su prudencia.			Nivel de Confidencialidad	<b>Población y muestra:</b>
	3. Entregar una nueva visión de todo lo que envuelve a la seguridad informática, con un plan de capacitación sensibilizando y advirtiendo de los riesgos que sobrelleva utilizar el Internet y las tecnologías informáticas al personal de la Gerencia de Administración y Finanzas de la Municipalidad Distrital de Independencia.			Nivel de disponibilidad	20 trabajadores que laboran en la Gerencia de Administración y Finanzas de la Municipalidad Distrital de Independencia.
					<b>Técnica de recolección de datos</b>
					Test estructurado.



## 2.6. Técnicas e instrumentos de recolección de datos, validez y confiabilidad

### 2.6.1. Metodología

#### 2.6.1.1. Empíricos - Método de la observación directa

Se considera a aquello que percibe en forma directa la sorpresa de observación. No participa en el acto de la finalidad de análisis.

Describe de forma detallada su acto.

#### 2.6.1.2. Lógicos - Método Hipotético Deductivo

Se plantea la hipótesis a escindir de métodos inductivos. Se llega a inferir en la demostración de la hipótesis a través del método deductivo.

Después, los resultados podrán ser contrastados por métodos empíricos.

### 2.6.2. Técnicas de recolección de datos

Tabla 2.2 - Técnicas de Recolección de datos

Técnica	Uso	Instrumento
<b>Entrevista</b>	Personal de la Subgerencia de TIC, personal de otras áreas de la Gerencia de Administración y Finanzas.	Cuestionario
<b>Revisión documentaria</b>	Archivos de fichas de registro. Documentos de gestión, manuales y políticas de seguridad de la información.	Hoja de cotejo
<b>Encuesta</b>	Personal de la Subgerencia de TIC, personal de otras áreas de la Gerencia de Administración y Finanzas	Ficha de encuesta

### **2.6.3. Instrumentos de recolección de la información**

#### **Encuesta:**

Se desarrolló un test de preguntas el cual estuvo destinado a un número de personas de la Subgerencia de TIC y de otras áreas de la Gerencia de Administración y Finanzas de la Municipalidad Distrital de Independencia.

#### **Observación Directa:**

Se observó el provenir y proceder de los trabajadores de la Municipalidad Distrital de Independencia al momento de presentar la documentación requerida.

### **2.7. Plan de procesamiento y análisis estadístico de la información**

#### **Plan de Procedimiento**

Se realizó concurriendo a las oficinas de la MDI, con el propósito de prescribir el test correspondiente al personal que han sido seleccionado en la presente muestra.

#### **Interpretación de la información**

Al analizar los resultados que se han obtenido en el presente test, se ha utilizado la herramienta de Microsoft su paquete de ofimática el Office Excel 2019, con el propósito de procesar la información e explicarlos, dicha información está conformado por las respuestas a las preguntas del test (Anexo).

Las preguntas del presente test se aplicaron a 20 trabajadores de la MDI.

Dicho test se elaboró siguiendo la metodología de ISACA, con el propósito de conocer las prácticas de medidas de protección para la información de los trabajadores de la MDI.

El instrumento se fraccionó en dos tipos de categorías:

- 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 hicieron las preguntas N° 1 a la 9.

Para la categoría de riesgos en la eficacia del servicio de informática, se hicieron las preguntas N° 10 a la 25.

## 2.8. Aspectos éticos

Tabla 2.3 - Criterios éticos de la investigación

Criterios	Características éticas del criterio
Medio ambiente	El proyecto garantiza el cuidado del medio ambiente ya que no va a involucrar uso de los mismos.
Confidencialidad	Garantiza la reserva de identidades y datos personales del personal de la Municipalidad Distrital de Independencia, así como información confidencial de la institución.
Objetividad	Se utilizara herramientas exclusivamente técnicas y conocimiento científico de la realidad concreta.
Originalidad	Se tendrá cuidado al momento de referenciar las fuentes bibliográficas de donde se ha obtenido la información presentada, para evitar totalmente el plagio intelectual.
Veracidad	Se presentará información de veraz y manteniendo mucho cuidado en la que reviste la confidencialidad.
Derechos laborales	La propuesta de solución que elaboraré procurará guardar amplio respeto a todos los derechos del personal de la Municipalidad Distrital de Independencia en estudio.

## 2.9. Criterios de rigor científico

Mis criterios se fundamentan esencialmente en una base de rigor teórico-científica.

Tabla 2.4 Criterios de rigor científico de la investigación

<b>Criterio</b>	<b>Características científicas</b>	<b>Acciones o estrategias</b>
<b>Confiabilidad</b>	Los cálculos estadísticos para medir el nivel de confiabilidad serán paulatinamente riguroso basado en las formulaciones en bases estadísticas.	a) Aplicación de las técnicas de análisis estadístico.
<b>Credibilidad</b>	La rigurosidad científico con respecto a la credibilidad importa la valoración de los contextos en las que la tesis sea reconocida como creíble, por la búsqueda de argumentos fiables y que sean idóneos de demostración en los resultados de esta tesis.	a) Respeto por los hechos y situaciones generados en el contexto temporal y espacial de la tesis. b) Estimación valorativa de los datos y/o información derivada de los instrumentos Aplicados.
<b>Validación</b>	Para que se reconozca la validación de los instrumentos de recolección de datos y la propuesta de solución que propongo, elevaré este proyecto al Juicio de Expertos.	a) Valoración por el juicio de expertos de los instrumentos de investigación

# **CAPÍTULO III**

## **RESULTADOS**

### CAPÍTULO III: RESULTADOS

Interpretar los resultados de la tesis, es un obra muy notable durante el desarrollo de ésta, debido a con base en lo que arrojan se podrá tramar una propuesta que permita mejorar la problemática detectada que casi siempre es el propósito u objetivo de una tesis.

Se tomó como muestra la subgerencia de tecnologías de la información y áreas específicas y funcionales de la MDI, para que después de la perseverancia de los fundamentos explicados en el Capítulo II: Metodología y Diagnóstico se obtuvieron los siguientes resultados

Tabla 3.5 - Resultados para la categoría de riesgos en la continuidad del proceso.

PREGUNTAS	ESCALA DE CALIFICACIÓN			
	R.1	R.2	R.3	R.4
Pregunta N° 01	23%	77%		
Pregunta N° 02	13%	25%	15%	47%
Pregunta N° 03	13%	87%		
Pregunta N° 04	08%	90%		
Pregunta N° 05	20%	80%		
Pregunta N° 06	08%	92%		
Pregunta N° 07	33%	67%		
Pregunta N° 08	03%	97%		
Pregunta N° 09	00%	100%		

Tabla 3.6 - Resultados para la categoría de riesgos en la eficacia del servicio de informática.

PREGUNTAS	ESCALA DE CALIFICACIÓN						
	R.1	R.2	R.3	R.4	R.5	R.6	R.7
Pregunta N° 10	05%	95%	00%	00%			
Pregunta N° 11	03%	22%	27%	03%	20%	03%	22%
Pregunta N° 12	15%	23%	52%	10%			
Pregunta N° 13	23%	00%	52%	25%			
Pregunta N° 14	57%	05%	00%	05%	33%		
Pregunta N° 15	47%	08%	30%	15%			
Pregunta N° 16	37%	03%	08%	52%			
Pregunta N° 17	18%	47%	08%	27%	00%		
Pregunta N° 18	34%	15%	13%	28%	10%		
Pregunta N° 19	33%	15%	44%	08%			
Pregunta N° 20	72%	18%	05%	05%			
Pregunta N° 21	29%	28%	23%	20%			
Pregunta N° 22	54%	08%	25%	13%			
Pregunta N° 23	18%	27%	23%	32%			
Pregunta N° 24	05%	20%	52%	23%			
Pregunta N° 25	20%	45%	25%	00%	10%		

### 1.1. Resultados, análisis e interpretación de la investigación

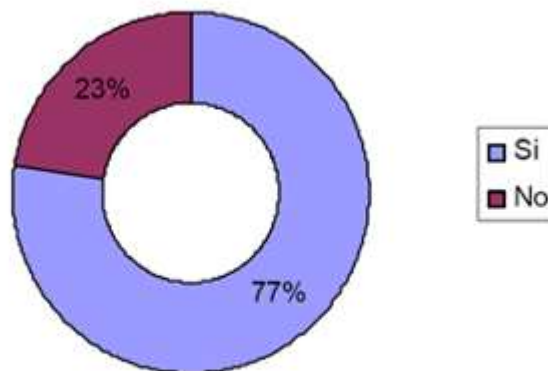
Con la aplicación del instrumento tenemos el siguiente resultado, análisis e interpretación:

### 1.1.1. Para la categoría de riesgos en la continuidad del proceso.

Las preguntas N° 1 al 9, se elaboraron dentro la categoría de riesgos en la continuidad del proceso, de esta clasificación se constituyeron sus respectivos indicadores.

Ilustración 3.1 - Identificación de peligros en la WAN

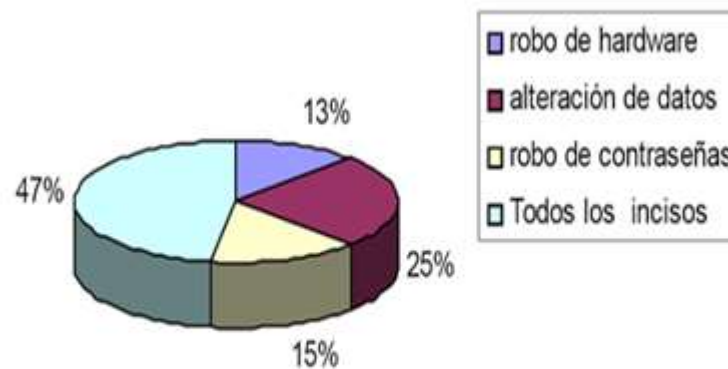
¿Conoce que peligros se encuentran en Internet?



Se observa que el 77% de los colaboradores consideraron sí reconocer peligros.

Ilustración 3.2 - Peligros en la Internet

Marque un peligro que conoce que se encuentra en Internet

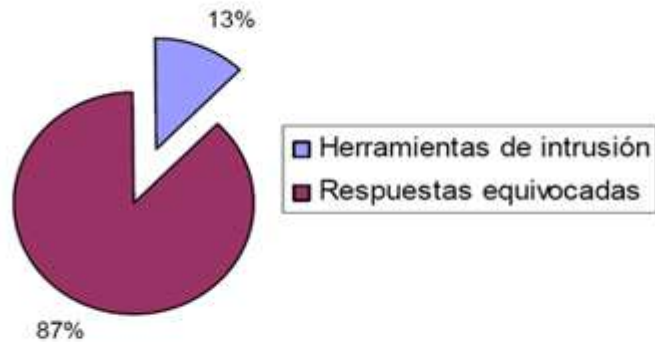


Se analiza que más de la mitad se equivoca al identificar los peligros en la internet y el 47% los identifica correctamente.



Ilustración 3.3 – Los Keyloggers

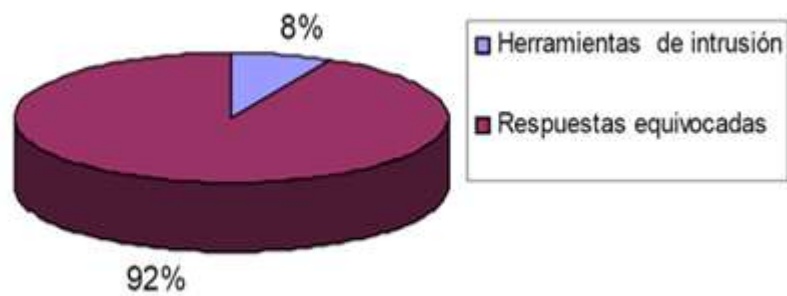
¿Qué son los Keyloggers?



El 87 % se equivocó acerca de los Keyloggers y sólo el 13% respondió afirmativamente.

Ilustración 3.4 – Los Mouseloggers

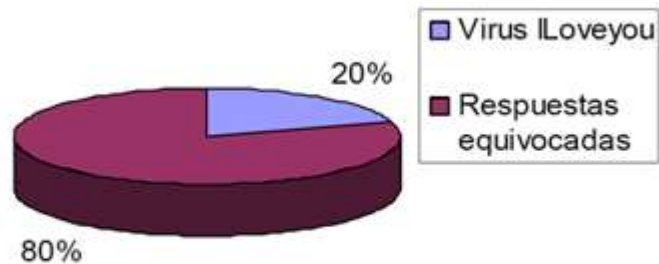
¿Qué son los Mouseloggers?



El 92% respondió equivocadamente acerca de los Mouseloggers.

Ilustración 3.5 - Virus informáticos

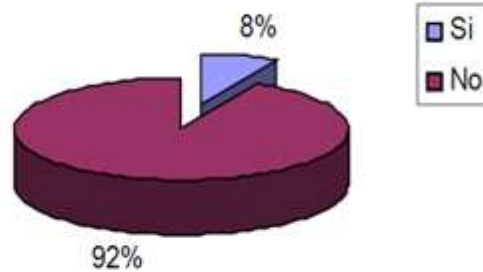
Marque un virus informático



Se observa que el 80% de los colaboradores no conoce uno de los virus más importantes.

Ilustración 3.6 – Virus w32/netsky-p

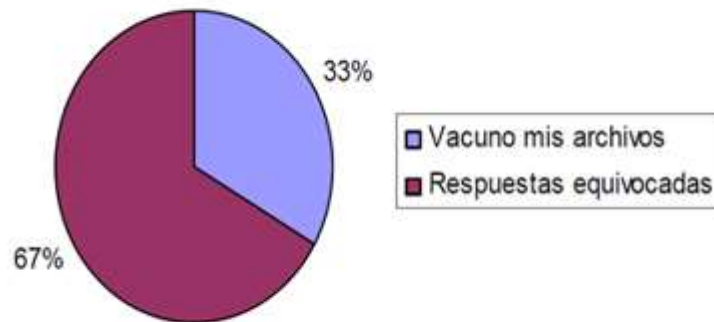
¿Alguna vez has empleado el archivo w32/netsky-p?



El 92% de los trabajadores no han empleado un virus.

Ilustración 3.7 - Conoce un virus informático

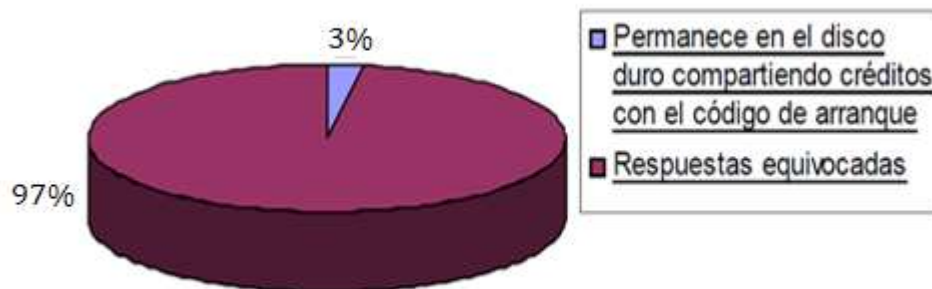
¿Cómo se ha procedido cuando se encuentra el archivo I love you?



El 67% de los trabajadores se equivoca acorde al peligro.

Ilustración 3.8 - Virus master boot record.

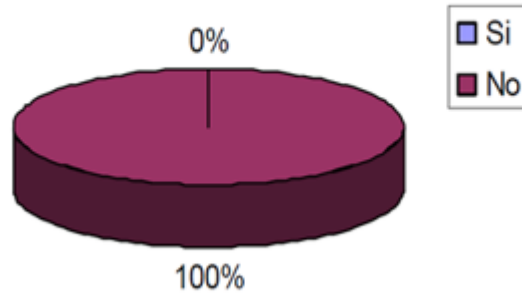
¿Qué pasaría si un virus master boot record entrara en la PC?



El 97% de los colaboradores se equivoca.

Ilustración 3.9 - Tiene correo electrónico institucional

¿Tiene una cuenta de correo electrónico institucional?



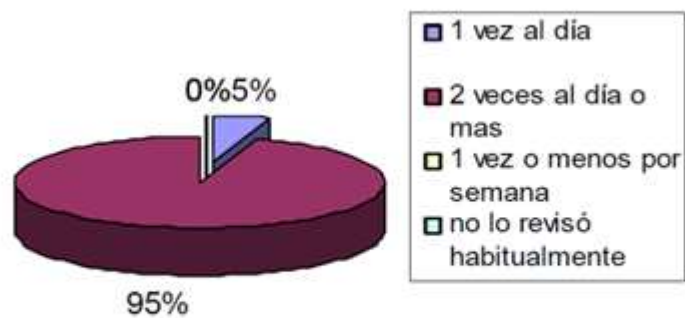
El 100% de los trabajadores están expuestos a una vulnerabilidad.

**1.1.2. Para la categoría de riesgos en la eficacia del servicio de informática.**

Las preguntas N° 10 al 25, se elaboraron dentro la categoría de riesgos en la eficacia del servicio de informática, de esta clasificación se constituyeron sus respectivos indicadores.

Ilustración 3.10 - Frecuencia de revisar el e-mail

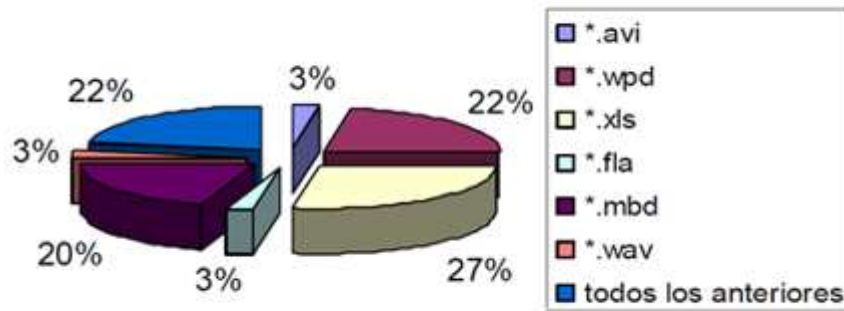
¿Con qué frecuencia revisa el correo electrónico?



El 95% de trabajadores revisa su correo continuamente para sus tareas y el 5% revisa solo 1 vez al día.

Ilustración 3.11 - Archivos que se reciben por el e-mail.

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



El 100% de los trabajadores realiza sus actividades usando medios electrónicos

Ilustración 3.12 - Periodicidad que se recibe algún archivo

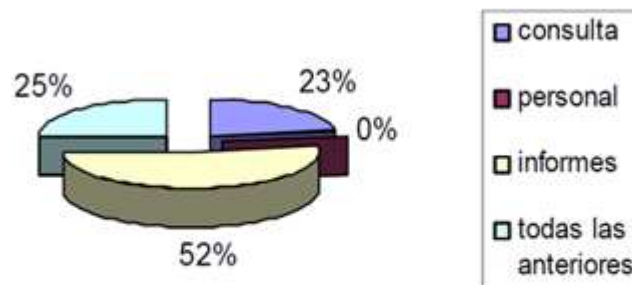
¿Con que frecuencia recibe los archivos mencionados?



Los trabajadores reciben archivos con diferentes intervalos de frecuencia, pero el que más recibe tiene un 52%.

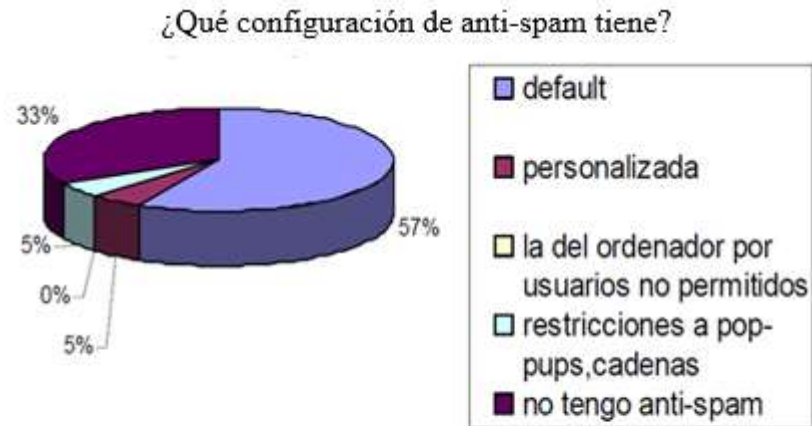
Ilustración 3.13 - Trato de la información

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



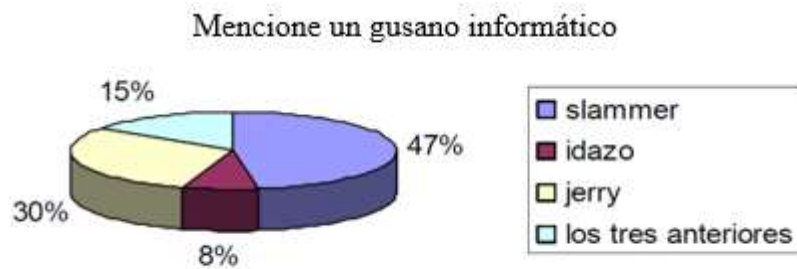
El 52% de trabajadores respondieron que la información de sus archivos es referente a informes.

Ilustración 3.14 – Configuración de Anti-spam.



El 52% de los trabajadores utiliza configuración default en el spam, y el 33% respondió no tiene anti-spam.

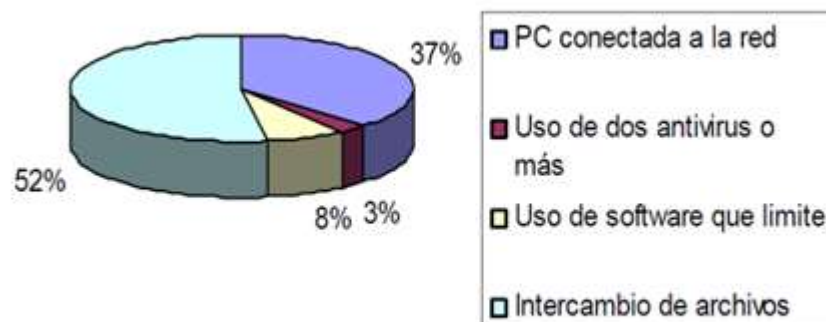
Ilustración 3.15 – Un tipo de Gusano informático.



El 8% de los trabajadores respondió afirmativamente.

Ilustración 3.16 - Puntos potenciales de infección

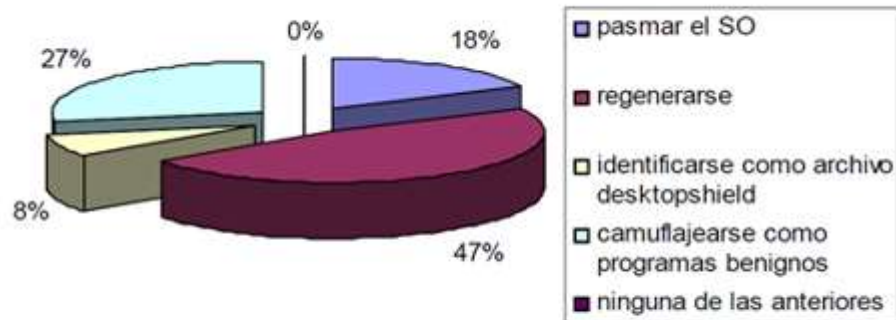
¿Cuáles considera que son los puntos potenciales de infección?



El 52% de los trabajadores no tiene los suficientes cuidados para cuidar sus activos.

Ilustración 3.17 - Características de los Troyanos

¿Qué características tienen los Caballos de Troya o Troyanos?



Se pudo observar que  $\frac{3}{4}$  de los trabajadores se equivocaron al identificar las características de los troyanos informáticos.

Ilustración 3.18 - Alto riesgo con los Troyanos

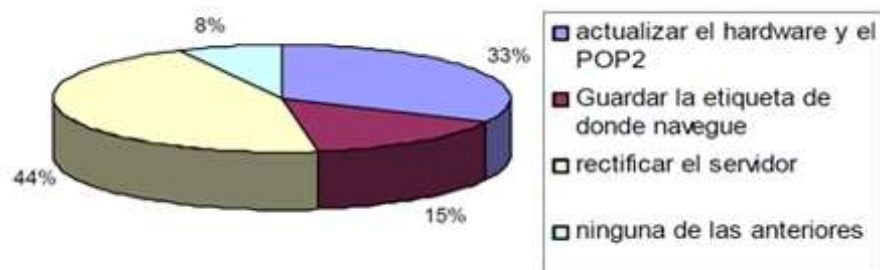
¿Por qué un Troyano se considera de alto riesgo?



Se observó que el porcentaje de trabajadores que se equivocaron es muy cercano al total.

Ilustración 3.19 - Contramedidas para evitar riesgos con los troyanos

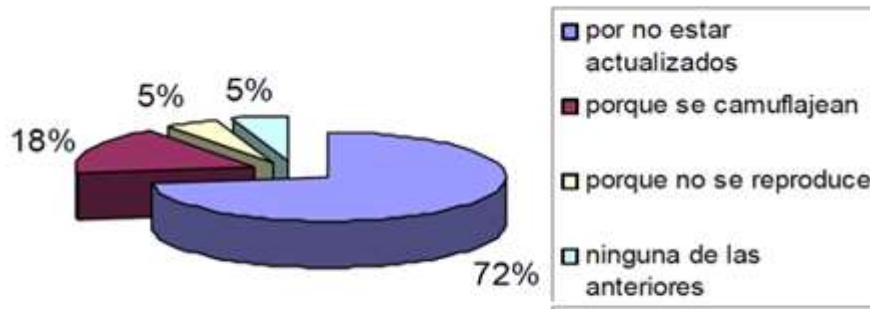
¿Cuáles serían las contramedidas para evitar riesgos por Troyanos?



Se observa que hay un porcentaje grande de error en las respuestas.

Ilustración 3.20 - El Spyware.

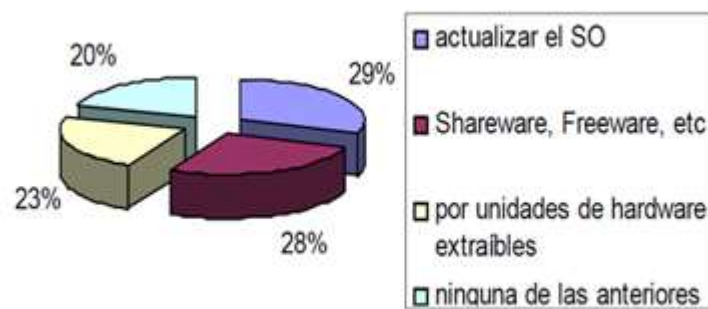
¿Por qué razón el spyware no es reconocido por los programas antivirus?



El 5% de los trabajadores respondieron, que ignoran al spyware no se reproduce como los virus.

Ilustración 3.21 – Formas de transmisión de los Spyware y Adware

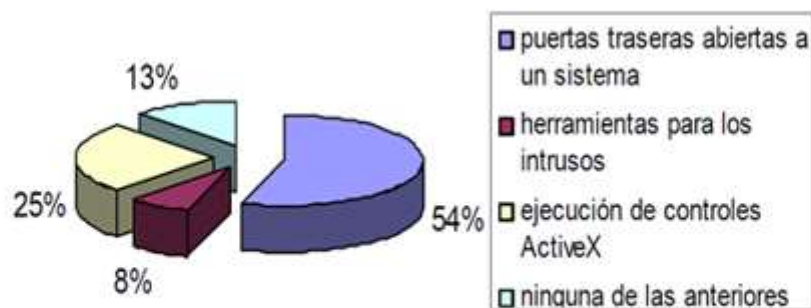
¿Cuál es el medio de transmisión por Spyware y Adware



Casi el 75% de trabajadores desconoce el medio de transmisión del spyware y Adware.

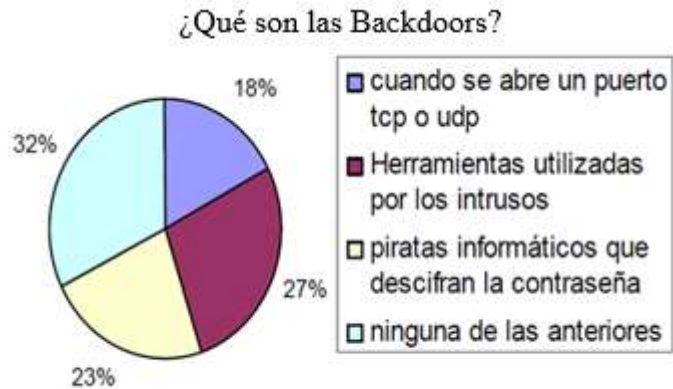
Ilustración 3.22 – Los Rootkits

¿Qué son los Rootkits?



Casi la totalidad de los trabajadores desconoce las herramientas de intrusos llamadas Rootkits.

Ilustración 3.23 - Backdoors



El 77% respondió erróneamente al contestar de las amenazas por las Backdoors.

Ilustración 3.24 - Escaneo en seguridad informática



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

Ilustración 3.25 - Adware



Sólo el 10% de los trabajadores respondió saber que se conoce como Adware.



## **1.2. Discusión de los resultados de la investigación**

### **1.2.1. Para la primera categoría que pertenece a los riesgos en la continuidad del proceso.**

Analizando los resultados del tipo de riesgos que amenazan en la continuidad del proceso, se llega a confirmar que dichos riesgos pueden entorpecer algunas actividades, es por ello sustancial que con la información proporcionada por los trabajadores, es aparente notar que la MDI cede en su acaso al no tener una propuesta de SI y en un santiamén puede sufrir ataques en SI tanto externos como internos y las secuelas serían considerables, si en algún momento llegara a parar la continuidad del proceso en sus operaciones, debido a la mala manipulación de la información o cambio de dicho activo importante.

### **1.2.2. Para la segunda categoría que pertenece a los riesgos en la eficacia del servicio de informática.**

Según los resultados de los riesgos en la eficacia del servicio de informática, se reafirma que dichos riesgos amenazan a la operatividad del mismo, además que acorralan a las actividades, por lo cual se considera a los de mayor prestigio por el mayor peligro que portean al trabajador y a la MDI.

Concluido el análisis y discusión de los resultados de las variedades de riesgos vistas, se percata que la MDI no cuenta con políticas de seguridad informática y dicha carencia se ve a nivel institucional, y todo ello si no se toma en cuenta va a llevar a la institución a sufrir percances difíciles como costosos.

Asimismo que los trabajadores de la MDI no cuentan con conocimiento informático respecto al tema tratado, dado que sus respuestas nos dan a conocer el desconocimiento sobre las amenazas que puede estar involucrada su información, haciendo referencia

al test nos deja ver el desasosiego para demostrar a la gerencia general, el valor principal que implica tener políticas de seguridad, ya que actualmente con el avance de la tecnología las empresas e instituciones deben de proteger y cuidar su información.

**CAPÍTULO IV**

**CONCLUSIONES Y**

**RECOMENDACIONES**

## **CAPÍTULO IV: CONCLUSIONES Y RECOMENDACIONES**

### **4.1. Conclusiones**

Una vez terminado la presente tesis de acuerdo al proceso de investigación se presentan las siguientes conclusiones:

- 1.** Al Identificar las técnicas de ingeniería social para analizar de las vulnerabilidades a fin de mejorar la SI de los equipos tecnológicos de la Municipalidad Distrital de Independencia, se llegó a la conclusión que si no se toma conciencia y no se previene los riesgos en salvaguardar la información como activo más importante, la institución perdería datos importantes y se divulgaría su información confidencial a fin de generar confusión a todo el personal involucrado.
- 2.** Teniendo el conocimiento de todo lo que conlleva la SI, se concluye que la MDI puede disponer de la más grande tecnología, tener equipos últimos, hasta contar con el mejor programa de SI, pero si todo esto no lleva a tener una consciencia en los peligros y vulnerabilidades que se da al hacer uso del Internet, o de confiar en personas, es posible de caer en un ataque de ingeniería social o phishing, para lo cual mitigar dicho riesgo y manejar su peligro va a ser más difícil.
- 3.** Analizado la teórica y la práctica de la tesis, se ha podido indagar y concluir que, si la institución no tiene políticas de SI con lo cual puede mitigar ataques de ingeniería social, la información como activo más importante va a sufrir vulneraciones más susceptibles.
- 4.** Al no tener claras las políticas de SI, también no se está incluyendo a una estrategia de capacitación para todo el personal de la MDI, para darles a conocer según las pruebas de concepto lo que es tener buena SI y lo fundamental que es

salvaguardar la información como activo importante de todos ellos y de la organización como tal, una vez que es un asunto tan fundamental que puede traer secuelas bastante graves más adelante si no se cuida.

Sin embargo, en la presente tesis hemos tocado temas puntuales a lo que conlleva un ataque de ingeniería social o phishing, como cuidarnos de ellos y si pasara como mitigarlos. Es por todo que esta tesis va a ser de suma utilidad y como punto de inicio para futuros trabajos más específicos o de mayor utilidad.

## 4.2. Recomendaciones

1. Se debería adoptar el modelo de plan de capacitación planteado en el anexo o generar una estrategia de capacitación y concientización para todos los empleados, sin que importe el cargo que lleva a cabo o el sector en la que labora, sobre todos los conceptos de phishing, cuáles son las técnicas que utilizan los ingenieros sociales y qué pasos siguen para lograr hacer los ataques. Se debería difundir cuáles son los peligros que se corre al no saber proteger la información y al entregarle datos particulares e información confidencial a cualquiera.
2. Se debería clasificar los datos y se debería conservar un control sobre qué personal poseen ingreso a dicha información en la compañía, para evadir que una sola persona tenga ingreso a toda la información y sea un blanco simple para un ataque de phishing; en esto además se debería educar al personal sobre el funcionamiento de información confidencial y en caso de ser víctima de un ataque exponer una alerta instantánea al área especializado en seguridad informática para verificar la información que ha sido entregada.
3. Concientizar al personal de la Gerencia de Administración y Finanzas de la MDI sobre lo malo que es abrir un link, un documento adjunto, un documento desconocido sencillamente pues reciben algo que les parece novedoso o interesante; educarles sobre el valor de continuamente revisar si aquel documento o página no es malo, si no tiene virus o malware y si es enviado por el individuo que dice haberlo enviado. Enseñarles que sus datos resultan muy relevantes y que tienen la posibilidad de ser capturados por medio del uso de la ingeniería social (phishing) ejemplificando si acceden en una página web falsa o que tienen la

posibilidad de instalar cualquier aplicativo en su equipo sin percibir una vez que abren cualquier documento sin revisar lo cual tiene.

4. Difundir a los trabajadores cada una de las técnicas que se aplican dentro del phishing y cómo se aplican, así como además la forma de reconocer una vez que un ingeniero social está poniendo en práctica una de ellas con el personal y cómo evadir caer en las manos del hacker, qué se puede hacer para mitigar el peligro de ser una víctima del Phishing.
5. Se tienen que generar políticas de seguridad de la información que abarquen todo lo concerniente a al phishing, éstas tienen que ser claras y tienen la posibilidad de fundamentarse en todas las técnicas utilizadas por dichos atacantes; las políticas tienen que ser apoyadas por la parte tecnológica debido a que hay casos en que los individuos olvidan hacer ciertas cosas, como bloquear la máquina, y en esta situación se lo podría hacer automáticamente luego de un periodo de inacción. En éstas políticas de seguridad de la información debería constar una en la que se indique que cada cierto tiempo se debería hacer una estrategia de capacitación y concientización para todo el personal que accede a la información y a los sistemas de información, de forma que constantemente se encuentren alertas sobre los ataques que se traten de hacer y todos ellos logre tomar medidas al respecto o sepan exactamente que método tienen que continuar frente a uno de dichos ataques.

## 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.



- ENGBRETSON, 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.

WEBSSENSE 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

Ilustración 6.1 - Estado Actual de los servicios de redes y servidores de la MDI



Ilustración 6.2 - Estado Actual de los servicios de redes y servidores de la MDI



Ilustración 6.3 - Estado Actual de la información de la MDI



Ilustración 6.4 - Estado Actual de los servicios de redes y servidores de la MDI





# CARTA DE AUTORIZACIÓN PARA REALIZAR LA INVESTIGACIÓN DE PARTE DE LA MUNICIPALIDAD DISTRITAL DE INDEPENDENCIA

## Municipalidad Distrital de Independencia SUBGERENCIA DE RECURSOS HUMANOS

*"Año de la Diversificación productiva y del fortalecimiento de la educación"*

Independencia, martes 14 de abril de 2015


Señor  
CPC. Saúl Hernández Terán  
UNIVERSIDAD SEÑOR DE SIPÁN  
Escuela Profesional de Administración Pública  
Lambayeque - Pimentel - Perú

Apreciado,

Yo CPC. Iris Haydee Villegas Huamán, identificada con DNI 31678345, en mi calidad de Subgerente de Recursos Humanos de la Municipalidad Distrital de Independencia, autorizo a su asesorado Alvarado Tolentino Joseph Darwin, estudiante de la Escuela Profesional de Administración Pública, de la Universidad Señor de Sipán, a utilizar información confidencial de la Municipalidad Distrital de Independencia para su tesis denominado ANÁLISIS DE LAS VULNERABILIDADES EN SEGURIDAD INFORMÁTICA DE LOS EQUIPOS DE CÓMPUTO Y REDES DE LA MUNICIPALIDAD DISTRITAL DE INDEPENDENCIA, MEDIANTE EL USO DE PHISHING 2014.

Como condiciones contractuales, el estudiante se obliga a (1) no divulgar ni usar para fines personales la información (documentos, expedientes, escritos, artículos, contratos, estados de cuenta y demás materiales) que, con objeto de la relación de trabajo, le fue suministrada; (2) no proporcionar a terceras personas, verbalmente o por escrito, directa o indirectamente, información alguna de las actividades y/o procesos de cualquier clase que fuesen observadas en la Municipalidad Distrital de Independencia durante la duración de su investigación y (3) no utilizar completa o parcialmente ninguno de los productos (documentos, metodología, procesos y demás) relacionados con el proyecto. El estudiante asume que toda información y el resultado del proyecto serán de uso exclusivamente académico.

Atentamente,

MUNICIPALIDAD DISTRITAL DE INDEPENDENCIA  
GERENCIA DE ADMINISTRACIÓN Y FINANZA  
  
*Iris Villegas*  
C.P.C. Ir. Villegas Huamán  
SUB GERENTE DE RECURSOS HUMANOS

## Cuestionario



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

El presente cuestionario coadyuvara a la realización de una tesis de la Escuela Profesional de Administración Pública y tiene por objeto analizar de las vulnerabilidades en seguridad informática de los equipos de cómputo y redes de la Gerencia de Administración y Finanzas de la Municipalidad Distrital de Independencia mediante el uso de ingeniería social.

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 popups, 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) Pasmarse 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 camuflajan 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 autenticados, 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

# **PROPUESTA DE UN PROGRAMA DE CAPACITACIÓN PARA GERENCIA DE ADMINISTRACIÓN Y FINANZAS DE LA MUNICIPALIDAD DISTRITAL DE INDEPENDENCIA Y SOLUCIONES PARA EL MANEJO Y SEGURIDAD DE SUS DOCUMENTOS**

## **PRESENTACIÓN**

La presente propuesta tiene como finalidad proporcionar los lineamientos necesarios para la implementación de un programa de capacitación, como una herramienta para apoyar a la organización en el logro de sus objetivos y metas, manteniendo a los colaboradores actualizados, comprometidos y motivados. Es necesario que la gerencia reconozca la importancia de contar con colaboradores capacitados en los roles que desempeñan, considerando que la capacitación es una inversión para reducir o eliminar la diferencia entre el desempeño actual y el deseado para contribuir al logro de los objetivos de la organización. Asimismo, con la implementación del programa se pretende minimizar las quejas presentadas por los clientes y aumentar la satisfacción en el servicio.

## **OBJETIVOS DE LA PROPUESTA**

**Objetivo General** Mejorar la actitud y aptitud de los colaboradores, con la ejecución del programa de capacitación, estableciendo el seguimiento requerido para su cumplimiento y mejora continua, con el objetivo de reducir las quejas de los clientes y alcanzar los objetivos que se tienen establecidos.

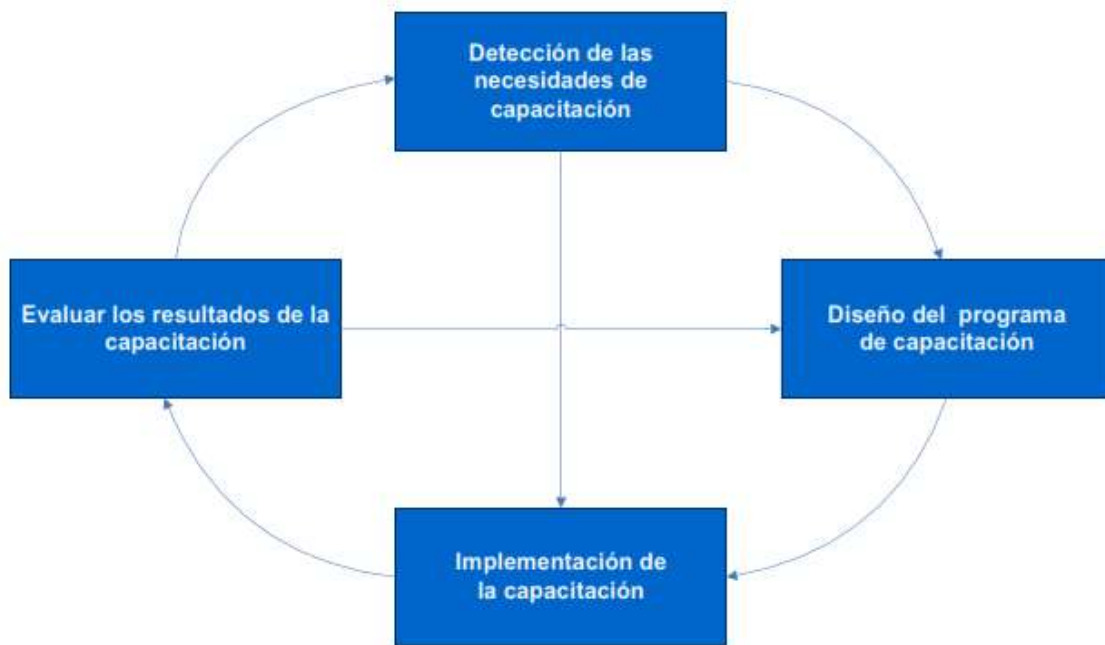
### **Objetivo Específicos**

- ✚ Lograr la participación del personal en la identificación de las necesidades reales de capacitación.
- ✚ Mejorar la actitud de los colaboradores con respecto a sus responsabilidades.
- ✚ Mejorar la aptitud de los colaboradores por medio del conocimiento amplio de las prácticas que se realizan a diario, también concientizarlos acerca de la importancia del trabajo que realizan, haciendo Énfasis en las necesidades que se detectaron en la situación actual.
- ✚ Proponer el plan de capacitación que incluya la totalidad de los colaboradores de la organización.



A continuación, se presentan las fases necesarias para la implementación y seguimiento del programa, las cuales permitirán corregir el proceso cuando sea necesario, adaptándolo a las necesidades de la organización y los colaboradores:

Ilustración 6.5 - Ciclo de capacitación



Fuente: Administración de recursos Humanos, Idalberto Chiavenato Pág. 389