UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS ELECTRÓNICA E INDUSTRIAL

CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES E INFORMÁTICOS

Tema:

"Las Vulnerabilidades Humanas En Relación A La Seguridad Informática Para Evitar La Fuga De Información Confidencial En El Departamento De Recursos Humanos De La Universidad Técnica De Ambato"

Trabajo de Graduación. Modalidad: Seminario De Graduación "Seguridad Informática", presentado previo la obtención del título de Ingeniero en Sistemas Computacionales e Informáticos.

Subnivel de investigación: Seguridad Informática

AUTOR: María Gabriela Cortez Pinto

TUTOR: Ing. Teresa Milena Freire Aillón

Ambato - Ecuador

Marzo-2013

APROBACIÓN DEL TUTOR

En mi calidad de tutor del trabajo de investigación sobre el tema: **"LAS VULNERABILIDADES HUMANAS EN RELACIÓN A LA SEGURIDAD INFORMÁTICA PARA EVITAR LA FUGA DE INFORMACIÓN CONFIDENCIAL EN EL DEPARTAMENTO DE RECURSOS HUMANOS DE LA UNIVERSIDAD TÉCNICA DE AMBATO"**, de la señorita María Gabriela Cortez Pinto, estudiante de la carrera de Ingeniería en Sistemas Informáticos y Computacionales, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, de la Universidad Técnica de Ambato, considero que el informe investigativo reúne los requisitos suficientes para que continúe con los trámites y consiguiente aprobación de conformidad al Art. 16 del Capítulo II del Reglamento de Graduación para obtener el Título Terminal de Tercer Nivel de la Universidad Técnica de Ambato.

Ambato, Marzo 2013

EL TUTOR

Ing. Teresa Milena Freire Aillón

AUTORÍA

El presente trabajo de investigación titulado: **"LAS VULNERABILIDADES HUMANAS EN RELACIÓN A LA SEGURIDAD INFORMÁTICA PARA EVITAR LA FUGA DE INFORMACIÓN CONFIDENCIAL EN EL DEPARTAMENTO DE RECURSOS HUMANOS DE LA UNIVERSIDAD TÉCNICA DE AMBATO".** Es absolutamente original, auténtico y personal, en tal virtud, el contenido, efectos legales y académicos que se desprenden del mismo son de exclusiva responsabilidad del autor.

Ambato, Marzo ,2013

EL AUTOR

María Gabriela Cortez Pinto

CI: 180429066-4

APROBACIÓN DE LA COMISIÓN CALIFICADORA

La Comisión Calificadora del presente trabajo conformada por los señores docentes Ing. Msc. Luis Solís E Ing. Vicente Morales, revisó y aprobó el Informe Final de trabajo de graduación titulado: **"LAS VULNERABILIDADES HUMANAS EN RELACIÓN A LA SEGURIDAD INFORMÁTICA PARA EVITAR LA FUGA DE INFORMACIÓN CONFIDENCIAL EN EL DEPARTAMENTO DE RECURSOS HUMANOS DE LA UNIVERSIDAD TÉCNICA DE AMBATO",** presentado por la señorita María Gabriela Cortez Pinto de acuerdo al Art. 18 del Reglamento de Graduación para obtener el Título Terminal de Tercer Nivel de la Universidad Técnica de Ambato.

Ing. Mg. Edison Homero Álvarez Mayorga
PRESIDENTE DEL TRIBUNAL

Ing. Mg. José Vicente Morales Lozada
DOCENTE CALIFICADOR

Ing. Mg. David Omar Guevara Aulestia
DOCENTE CALIFICADOR

DEDICATORIA

A Dios.
Por la guía y las bendiciones durante el camino recorrido.

A mi madre María y mis hermanos Juan y Caro.
Por el amor y sobre todo por la fortaleza ante las debilidades y la paciencia frente a los momentos difíciles.

A mis tías Nancy y Matilde.
Por ser las madres que comparten una responsabilidad ante los momentos de dolor.

A Luis
Por todo el amor y comprensión.

María Gabriela Cortez Pinto

AGRADECIMIENTO

A la Facultad de Ingeniería en Sistemas, Electrónica e Industrial y en especial a los profesores que imparten sus conocimientos en la Carrera de Sistemas Computacionales e Informáticos; y, conjuntamente a la Universidad Técnica de Ambato por la oportunidad de superación.

A la Ing. Teresa Freire Directora de este proyecto, que con sus conocimientos, ayudó a la culminación de este trabajo de investigación.

A todo el personal del Departamento de Recursos Humanos de la Universidad Técnica de Ambato, a su Director el Dr. Carlos Fuentes e Ing. Mauricio Molina por el apoyo y la confianza para la realización de la presente investigación.

Al Ing. Msc. Franklin Mayorga por la colaboración y apoyo durante la investigación; así como también a cada uno de los catedráticos de los diferentes módulos del seminario de graduación "Seguridad Informática".

A Luis, mi madre, hermanos y demás familiares por el apoyo, comprensión y amor incondicional.

A todos mis amigos que de una u otra manera apoyaron a la realización de este trabajo.

Gracias a todos.

María Gabriela Cortez Pinto

ÍNDICE

ÍNDICE DE GRÁFICAS

ÍNDICE DE TABLAS

RESUMEN EJECUTIVO

Con el avance agigantado de la tecnología y la importancia de la información para cada una de las instituciones, la necesidad de asegurar la información se ha vuelto una necesidad y los escapes de información y vulnerabilidades de los elementos que intervienen en un sistema informático se ven cada vez más afectados por los ataques y amenazas.

La falta de información o el desconocimiento de los elementos que afectan directamente un sistema informático, pueden llevarnos a pasar por alto la importancia y a su vez la vulnerabilidad del factor humano que trabaja directamente con un computador y la información que este factor puede llegar a manejar.

La Ingeniería Social es una de las grandes ciencias de la intrusión que se enfoca netamente en vulnerar a este factor humano; las empresas no engloban dentro de un plan de seguridad informática este factor que posee un alto grado de vulnerabilidad.

Este proyecto de investigación se enfoca en valorar la vulnerabilidad del factor humano dentro del Departamento de Recursos Humanos de la Universidad Técnica de Ambato, para detectar cuáles son las amenazas con más probabilidad para efectuar un ataque y determinar medidas preventivas y definir procesos para disminuir la vulnerabilidad.

INTRODUCCIÓN

El informe final del proyecto nominado "Las vulnerabilidades humanas en relación a la Seguridad Informática para evitar la fuga de información confidencial en el Departamento de Recursos Humanos de la Universidad Técnica de Ambato" presentada a continuación, se la ha divido en capítulos para su mejor comprensión.

En el **Capítulo I** denominado "**El Problema**", identifica el problema a resolver, el árbol del problema, el análisis crítico; además existe una debida justificación, análisis y planteamiento de objetivos.

En el **Capítulo II** denominado "**Marco Teórico**", se establece el marco teórico sobre el cual se va a desarrollar el trabajo investigativo, presenta además los antecedentes investigativos, la fundamentación legal, hipótesis y el señalamiento de las variables de la hipótesis.

En el **Capítulo III** denominado "**Marco Metodológico**", se determina el enfoque de la investigación, las modalidades de investigación, la población y muestra y la Operacionalización de las variables.

En el **Capítulo IV** denominado "**Análisis e Interpretación de los Resultados**", se realiza el análisis e interpretación de los resultados obtenidos de la investigación de campo realizada.

En el **Capítulo V** denominado "**Conclusiones y Recomendaciones**", el investigador presenta las conclusiones obtenidas de la información recolectada y procede a proponer las recomendaciones para cada una de ellas.

En el **Capítulo VI** denominado "**Propuesta**" se presenta el desarrollo de la alternativa de solución al problema.

Finalmente se ubican los anexos, en los cuales encontramos los documentos recolectados en el Departamento de RRHH como Manual de Procedimientos de Seguridad y los cuestionarios de las técnicas de la encuesta.

CAPITULO I

1. EL PROBLEMA

1.1.**Tema**:

Las vulnerabilidades humanas en relación a la Seguridad Informática para evitar la fuga de información confidencial en el Departamento de Recursos Humanos de la Universidad Técnica de Ambato.

1.2.Planteamiento Del Problema

1.2.1. Contextualización

Un ataque informático es realizado por un delincuente computacional aprovechando las fallas o debilidades dentro de los sistemas, hardware y a su vez en las personas que forman parte del ambiente informático y laboral de una institución.

Más allá de los aspectos técnicos que se le pueda dar a la seguridad informática, las estrategias de ataque basadas en el engaño y que están enfocadas a explotar las debilidades del factor humano son las de Ingeniería Social.

Según el artículo de Help Net Security. [1]. Las vulnerabilidades humanas en relación a la Seguridad Informática son muy comunes para la fuga de la información, a nivel mundial, las empresas se encuentran expuestas a los ataques informáticos realizados al factor humano, se ha registrado un 48% de empresas que han sido víctimas de estos ataques. De todas las encuestas realizadas; 850 profesionales de Tecnologías de la Información y de seguridad a nivel mundial que representan al 86% de profesionales encuestados reconocen a la Ingeniería Social como un problema de seguridad creciente.

La vulnerabilidad humana es sin duda alguna el factor más importante para los delincuentes computacionales, que realizan los ataques de Ingeniería Social, debido a la facilidad en las que estos se llevan a cabo, debido a la utilización de técnicas sencillas y que requieren únicamente la habilidad de convencimiento hacia las víctimas.

Este gran problema a nivel mundial causa grandes pérdidas económicas y sin huellas tecnológicas para analizar estas técnicas se vuelven muy difíciles de detectar para los expertos en seguridad informática.

Una gran máquina de almacenamiento de información es sin duda alguna la mente humana, la cual puede almacenar información muy importante y confidencial para una institución, así como esta gran máquina es capaz de almacenar, también posee vulnerabilidades que la hacen propensa a ataques para extraer esta información, debido a que no es una máquina física con periféricos y software como una computadora; las técnicas que brinda la Ingeniería Social permiten realizar ataques hacia las vulnerabilidades de la mente humana, para extraer información sin forzar la tecnología de una institución con mecanismos de ataque muy sencillos pero a la vez eficientes.

En el Ecuador los ataques o delitos informáticos conceptúan a los ataques de Ingeniería Social como un delito informático. Según una encuesta realizada por la empresa Delote Ecuador en el año 2010, identificó que al menos el 32% del personal de una empresa comparte sus contraseñas con dos o más personas, lo cual puede provocar que los ataques hacia los usuarios de un sistema sean cada vez más satisfactorios.

Las vulnerabilidades de los usuarios conllevan a la exposición de la información confidencial de la institución u organización hacia los atacantes; pudiendo ser aprovechada para fraudes o mala utilización de la misma con fines ilícitos.

La aplicación de medidas preventivas y el conocimiento hacia estos temas sobre nuevas técnicas de robo de información deben ser difundidas y tomadas con la seriedad respectiva para evitar pérdidas económicas que afecten fuertemente a las instituciones ecuatorianas.

Gráfica 1.1 Estadísticas 2010 Delote Ecuador

Las empresas a nivel provincial han tomado pocas precauciones hacia el tema de seguridad informática enfocada principalmente en el factor humano. Poniendo en grave riesgo la información y a su vez a la institución en general.

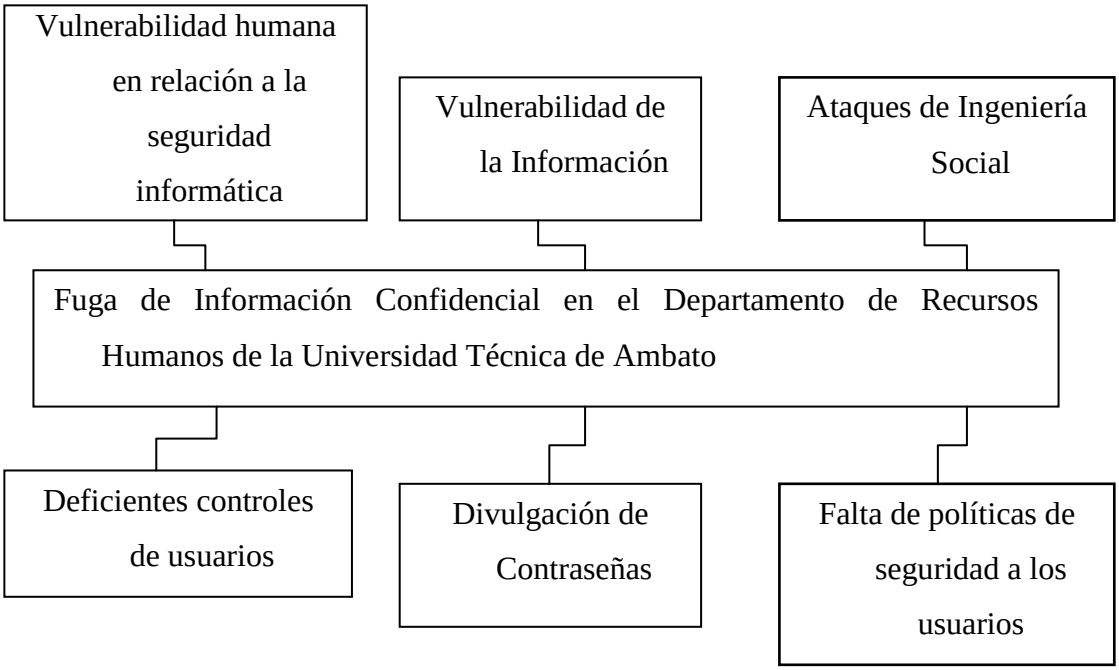
La Universidad Técnica de Ambato posee departamentos vulnerables que manejan información confidencial y valiosa para la misma. El departamento de Recursos Humanos de la institución maneja toda la información relacionada con información privada y profesional de cada uno de los elementos humanos que la conforman.

La fuga de información que puede existir dentro de este departamento puede provocar la desconfianza del personal humano hacia la seguridad de su información y a su vez puede producir que el nivel de prestigio ganado durante años por la solemne institución se pierda.

La exposición de la institución hacia ataques informáticos que pueden afectar la seguridad de la información, deben ser analizados desde el punto de las alteraciones sobre el normal funcionamiento de los procesos que diariamente se realizan, además de las amenazas que significan pérdida en varios aspectos de la institución. Analizar los conocimientos de los usuarios hacia cuán propensos están a ataques y sobre las soluciones inmediatas que se pueden ejecutar para la solución de problemas cuando se vulnera la seguridad informática del departamento de Recursos Humanos de la Universidad Técnica de Ambato se convierte en una necesidad y una brecha de vulnerabilidad muy grande.

La solución a un problema que puede generar pérdidas tanto humanas como económicas para la institución, puede ayudar no solamente a mejorar los métodos de seguridad ya efectuados o implementados para salvaguardar la información de los departamentos, sino también mantener su estabilidad institucional.

Árbol del Problema



Gráfica 1.2. Árbol del Problema

1.2.2. Análisis Crítico

La seguridad de la información dentro de la Universidad Técnica de Ambato debe ser un tema de gran abarque para la institución. Los deficientes controles a los usuarios que están en contacto directo con un computador pueden tener consecuencias graves de fuga de información en el departamento de Recursos Humanos de la institución, poniendo en peligro el prestigio obtenido por la misma durante años y exponiendo la información del personal humano que forma parte de la misma, a su vez causa una gran vulnerabilidad humana en relación a la seguridad informática produciendo una gran amenaza a nivel de factor humano hacia la información.

Los grados de confianza que se crean entre los compañeros de trabajo o colaboradores del departamento, pueden generar grandes lazos de amistad, pero al mismo tiempo, son una gran amenaza cuando se produce la divulgación de las contraseñas y usuarios personales, con lo cual la fuga de información confidencial se puede efectuar y de este modo generar una gran vulnerabilidad de la información poniéndola propensa a robos o ataques maliciosos.

La existencia de políticas para mantener la seguridad de la información, así como también asegurar los equipos informáticos que se utilizan para almacenar la información pueden ser una gran defensa hacia los ataques; pero, al no existir políticas que nos ayuden a salvaguardar la información o la tecnología adecuada dentro del Departamento de Recursos Humanos de la Universidad Técnica de Ambato puede hacer efectivos los ataques de Ingeniería Social y de esta manera vulnerar al factor humano que forma parte del departamento y de este existirá la fuga de información, obstaculizando el pronto análisis y reparación del problema.

1.2.3. Prognosis

El Departamento de Recursos Humanos de la Universidad Técnica de Ambato cuenta con diferentes personas que atienden y tratan directamente con personas tanto propias como ajenas al Departamento y a la institución, con calidez y amabilidad para poder solventar las necesidades de cada uno de los visitantes que acuden diariamente al departamento.

Para lo cual considerar que la exposición de este mismo personal hacia los ataques informáticos directamente enfocados en la vulnerabilidad del factor humano de un sistema de información, es ciertamente una afirmación.

Es importante considerar la gravedad de que exista robo de información que diariamente se maneja y utiliza dentro del departamento de Recursos Humanos de la Universidad Técnica de Ambato.

De este modo la falta de solución a la fuga de información confidencial dentro del Departamento de Recursos Humanos de la Universidad Técnica de Ambato podría llevar a un colapso total de la información de la institución en general, afectando directamente a la funcionalidad de los sistemas informáticos, o a su vez alterando la información; la cual podría no llegar a estabilizarse o a su vez perderse definitivamente, poniendo en riesgo la continuidad de las actividades de la universidad.

1.2.4. Formulación del Problema

¿Cómo incide la vulnerabilidad humana en relación a la Seguridad Informática en la fuga de información confidencial en el Departamento de Recursos Humanos de la Universidad Técnica de Ambato?

1.2.5. Preguntas Directrices

- ¿Cómo analizar las vulnerabilidades humanas en relación a la seguridad informática que evite la fuga de información confidencial en el Departamento de Recursos Humanos de la Universidad Técnica de Ambato?

- ¿Para qué determinar las vulnerabilidades humanas en relación a la seguridad informática que evite la fuga de información confidencial en el Departamento de Recursos Humanos de la Universidad Técnica de Ambato?

- ¿Por qué establecer una guía de seguridad en las vulnerabilidades humanas en relación a la Seguridad Informática para evitar la fuga de información confidencial en el Departamento de Recursos Humanos de la Universidad Técnica de Ambato?

1.2.6. Delimitación

Campo: Seguridad Informática

Área: Técnicas de Ingeniería Social

Aspecto: Fuga de Información Confidencial.

Lugar: Departamento de Recursos Humanos de la Facultad Universidad Técnica de Ambato.

1.3. Justificación

El estudio de las vulnerabilidades humanas es un tema muy poco aplicado en la Seguridad Informática debido al enfoque que esta ha tomado.

Para el investigador le resulta muy interesante desarrollar y concienciar a los profesionales de seguridad, usuarios y clientes de una organización a tomar precauciones sobre las vulnerabilidades ante los comportamientos humanos que ponen en riesgo la seguridad informática de una organización.

Se cuenta con gran cantidad de información que ayudará a resolver de mejor manera las interrogantes que surjan durante el transcurso de la investigación, para de esta manera dar conceptos y conclusiones verídicas al proyecto investigativo.

Dentro del Departamento de Recursos Humanos de la Universidad Técnica de Ambato se realizará un análisis a los usuarios para verificar que tan vulnerable está la información del departamento; este tema ha sido muy poco analizado y aplicado en la Universidad Técnica de Ambato.

Con la investigación se podrá detectar las vulnerabilidades y de esta manera se podrán ejecutar medidas de prevención para lo cual la intervención y participación de los usuarios es requerida dentro del desarrollo investigativo del proyecto.

Es útil a la sociedad debido a que se podrá tomar como inicio para analizar las vulnerabilidades de los usuarios y la información en otras instituciones pudiéndose ser estas: educativas, financiera, gubernamentales y otros. Así como también ayudará a los profesionales a analizar y desarrollar de mejor manera las políticas de seguridad que se aplican dentro de una institución.

El proyecto no requiere de una financiación externa y puede ser plenamente financiada por el investigador, debido a la simplicidad de obtención del material.

Las fuentes de bibliografía se encuentran disposición del investigador, así como también la opinión de expertos en el tema de investigación lo cual facilitará la investigación.

La tecnología necesaria para el desarrollo del proyecto se encuentra disponible para el investigador; además de no requerir equipos especializados ni materiales tecnológicos adicionales a los que el investigador requiera.

Debido a que el proyecto se centra en la utilización de técnicas de vulnerabilidad es factible dar una solución positiva al problema que ayudará a disminuir o a su vez a erradicar el problema que tiene la institución.

1.4. Objetivos

Objetivo General

- Diagnosticar las vulnerabilidades humanas en relación a la Seguridad Informática en la fuga de información confidencial en el Departamento de Recursos Humanos de la Universidad Técnica de Ambato.

Objetivos Específicos

- Establecer las vulnerabilidades humanas en relación a la seguridad informática del Departamento de Recursos Humanos de la Universidad Técnica de Ambato.

- Analizar la fuga de Información Confidencial dentro del Departamento de Recursos Humanos de la Universidad Técnica de Ambato.

- Plantear una propuesta que permita la generación de una guía de procedimientos de Seguridad enfocados al factor humano para disminuir la fuga de información confidencial en el Departamento de Recursos Humanos de la Universidad Técnica de Ambato.

CAPÍTULO II

2. MARCO TEÓRICO

2.1. Antecedentes Investigativos:

- Autor: Gabriela Catherine Torres Andagana, Diego Fernando langa Salcán
- Tema: Estudio e Implementación de una metodología de prevención de intrusos para redes LAN.
- Año: 2010
- Reposa en la Biblioteca de la Escuela de Ingeniería Electrónica y Tecnología en Computación de la Facultad de Informática y Electrónica de la Escuela Superior Politécnica de Chimborazo.
- Caso Práctico: Sistema de Prevención de Intrusos en la Red Corporativa del Municipio de Riobamba.
- Objetivos:
    - General:
        - Estudiar e implementar una metodología de prevención de intrusos en la red corporativa del M.I. Municipio de Riobamba con el fin de proteger la información privada que allí se maneja.

- Específicos:
  - Realizar un estudio de las metodologías de prevención de intrusos existentes.
  - Elegir la metodología más apropiada para ser implementada en el M.I Municipio de Riobamba.
  - Desarrollar un IPS (Sistema de Prevención de Intrusos) para poder tener una política de seguridad aceptable.
  - Implementar el Sistema de Prevención de Intrusos con el Sistema Operativo Linux y la ayuda de diferentes herramientas.
  - Hipótesis: El estudio e implementación de una metodología de Prevención de Intrusos en la red corporativa del M.I Municipio de Riobamba permitirán mejorar los niveles de seguridad de la información privada que la institución maneja.
  - http://dspace.espoch.edu.ec/bitstream/123456789/383/1/38T00192.pdf

Para el investigador tomar esta tesis como antecedentes investigativos ayuda a encaminar su tema por la inclusión de un estudio con referencia a los intrusos y la utilización de políticas de seguridad para la posible solución al problema; lo cual puede tomarse como parte de una solución para la vulnerabilidad humana y evitar la fuga de información confidencial dentro del Departamento de Recursos humanos de la Universidad Técnica de Ambato.

2.2. Fundamentación Legal

El presente proyecto se basa en las siguientes leyes registradas en la versión del año 2012 de la Constitución de la República del Ecuador:

SECCIÓN TERCERA

Comunicación e información

Art. 16.-Todas las personas, en forma individual o colectiva, tienen derecho a:

1. Una comunicación libre, intercultural, incluyente, diversa y participativa, en todos los ámbitos de la interacción social, por cualquier medio y forma, en su propia lengua y con sus propios símbolos.
2. El acceso universal a las tecnologías de información y comunicación.

SECCIÓN OCTAVA

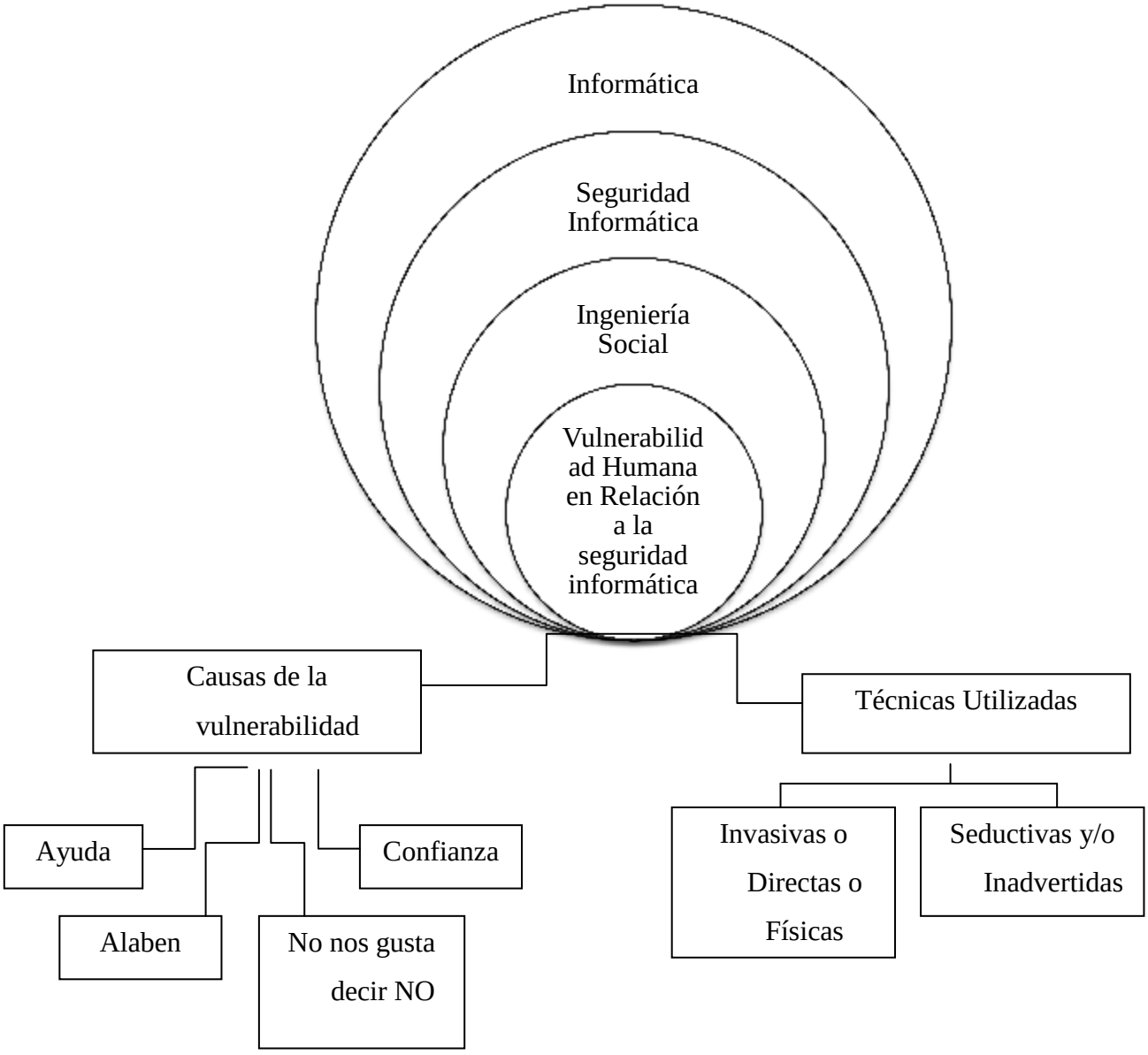
Ciencia, tecnología, innovación y saberes ancestrales

Art. 385.-- El sistema nacional de ciencia, tecnología, innovación y saberes ancestrales, en el marco del respeto al ambiente, la naturaleza, la vida, las culturas la soberanía, tendrá como finalidad:

1. Generar, adaptar y difundir conocimientos científicos y tecnológicos.
2. Recuperar, fortalecer y potenciar los saberes ancestrales.
3. Desarrollar tecnologías e innovaciones que impulsen la producción nacional, eleven la eficiencia y productividad, mejoren la calidad de vida y contribuyan a la realización del buen vivir.

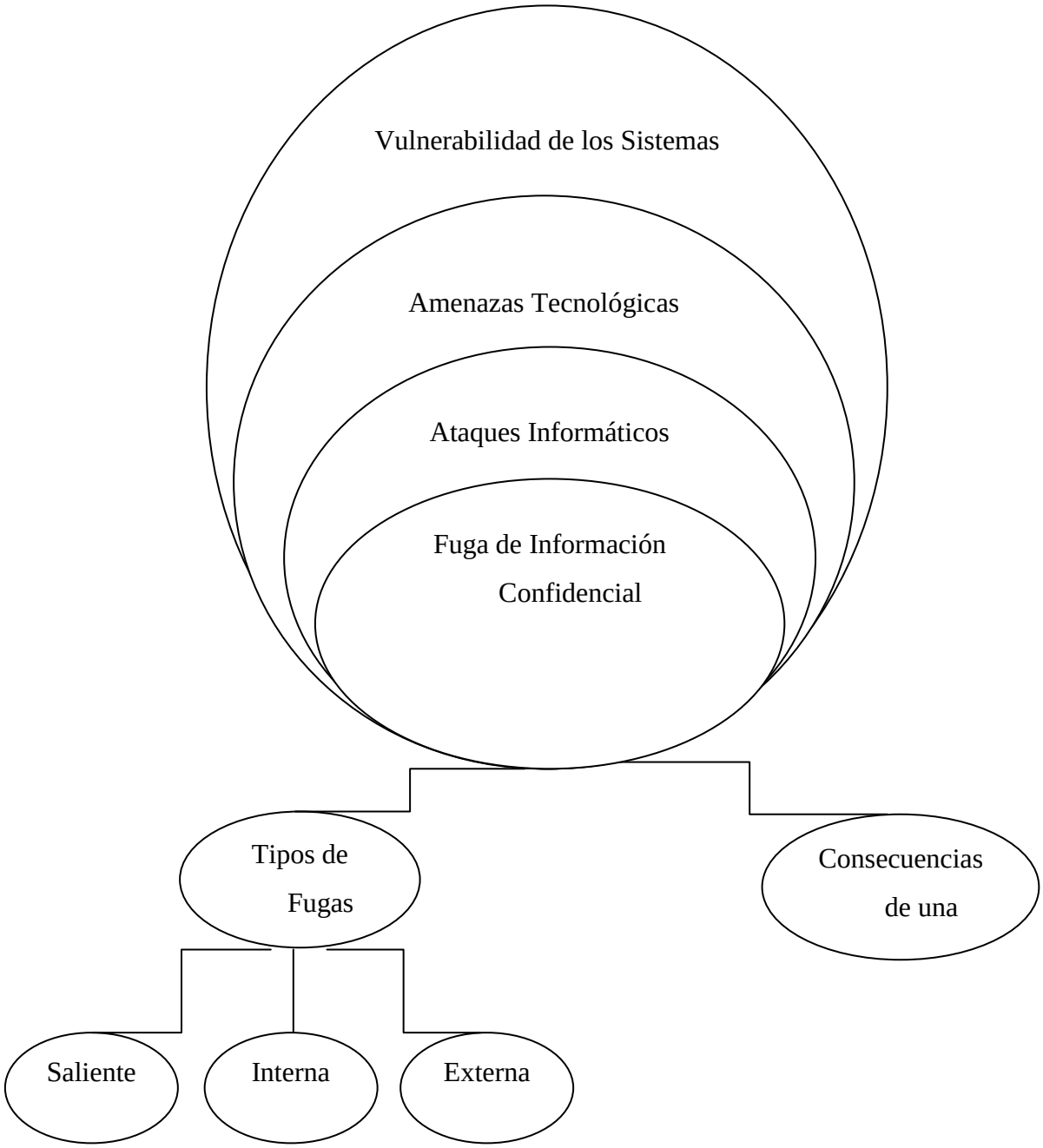
2.3. Categorías Fundamentales

Variable Independiente



Gráfica 2.1. Categorías de la Variable Independiente

Variable Dependiente



Gráfica 2.2. Categorías de la Variable Dependiente

Informática

Según OLMEDO, José Joaquín-Hermoso; MONTERO NAVARRO, Antonio; MARTÍN, Santiago; "et al". La Informática la define como una ciencia que se encarga del estudio y se ocupa del tratamiento automático y legítimo de la información, así como la forma de tratarla. O como la ciencia que se encarga de estudiar los computadores.

La comprensión de la informática como una ciencia que estudia la complejidad de los computadores y a su vez la información que dentro de ella se maneja y trata; es un concepto muy generalizado debido al concepto que engloba conceptos.

Según MARCO GALINDO, María Jesús; MARCO SIMÓ, Josep María; BLÁZQUES PRIETO, Josep; "et al". La informática es el conjunto de conocimientos que actualmente tenemos respecto a un artilugio tecnológico que llamamos ordenador. Y cuando decimos conjunto de conocimientos nos referimos a conceptos como ciencia, tecnología, negocio e implicaciones de todo tipo para el individuo y la sociedad.

Este concepto de informática nos lleva a pensar que es una ciencia sumamente compleja que conlleva acciones y procesos que pueden llegar a afectar a un individuo y a la sociedad. Lo cual desacuerda al concepto dado por OLMEDO en el cual solo enfoca las acciones tecnológicas y deja de tomar en cuenta las acciones de un individuo involucrado en la ciencia.

Según el análisis se podría concluir que la Informática "Es una ciencia destinada al estudio y atención que se le da a la información para tratarla de forma automática, utilizando sistemas computacionales y los componentes electrónicos que para ello se utilizan; mediante los conocimientos de un individuo para el tratamiento automático de la misma."

Seguridad Informática

La Seguridad Informática ayuda al aseguramiento de la información cuando esta es automatizada y almacenada en algún medio informático.

Según AGUILERA, Purificación (Internet; desconocido; 22, 10,2011; 12h2 pm) Es una disciplina que se encarga del diseño de métodos y procedimientos y técnicas para poder conseguir un sistema computacional seguro y confiable.

La apertura de este concepto nos lleva a entender a la seguridad informática como una rama de la Informática que tiene a cargo la seguridad tanto de la información como de los elementos computacionales físicos que se encuentran inmersos en la misma.

Ingeniería Social

Popularizada por Kevin Mitnick la ingeniería social se ha convertido en el arte de la persuasión. La ingeniería social puede aprovecharse de los instintos humanos para realizar un ataque computacional hacia la información de una organización; o a su vez, realizar actos delictivos en contra de la economía de la misma.

Según Wikipedia (Internet; 21, 10, 2011; 27,10 ,2011; 14h05 pm) "La práctica de obtener información confidencial a través de la manipulación de usuarios legítimos. Es una técnica que pueden usar ciertas personas, tales como investigadores privados, criminales, o delincuentes computacionales, para obtener información, acceso o privilegios en sistemas de información que les permitan realizar algún acto que perjudique o exponga la persona u organismo comprometido a riesgos o abusos."

Esta definición a lo mejor no abarca en su totalidad la gran rama de la Ingeniería Social dentro de la Seguridad Informática pero se puede observar que el concepto

de la obtención de información mediante la manipulación de las personas se mantiene, produciendo gran expectativa sobre el sector humano de la sociedad.

Vulnerabilidad Humana en relación a la Seguridad Informática

La vulnerabilidad humana en relación a la Seguridad Informática es la exposición del factor humano hacia los ataques que están directamente enfocados al sector humano de los sistemas informáticos, de esta manera el atacante obtiene datos confidenciales como usuarios y contraseñas para ganar acceso y efectuar un ataque a los sistemas.

La vulnerabilidad humana en relación a la Seguridad Informática es el factor más importante que influye y compone una oportunidad para los atacantes de conseguir sus propósitos y de esta manera quebrantar la seguridad de los sistemas.

Causas de la Vulnerabilidad

Analizar las causas de la vulnerabilidad humana nos lleva a tomar como base los principios de Kevin Mitnick.

- Todos queremos ayudar
- El primer movimiento es siempre de confianza hacia el otro
- Nos gusta que nos alaben
- No nos gusta decir NO

Analizando estos principios las principales causas para la existencia de una vulnerabilidad son generalmente la falta de capacitación al sector humano de las organizaciones sobre los potenciales problemas o ataques a los que están totalmente expuestos.

Técnicas Utilizadas dentro de la Ingeniería Social

Entre las técnicas más utilizadas para vulnerar la seguridad informática usando al factor humano como principal factor de ataque son las Técnicas de Ingeniería Social, las mismas que se utilizan están dirigidas a obtener datos sensibles del personal de una institución.

Según BISCIONE, Carlos A. (Internet; desconocido; 28,10, 2011 10h14 am) Las técnicas y Herramientas de Ingeniería Social se clasifican en dos grupos:

- Invasivas o Directas o Físicas: Dentro de estas encontramos varias subcategorías.
    - Uso del teléfono para personificación falsa y persuasión
    - Acceso al lugar de trabajo para obtener acceso físico o tratar de conseguir información valiosa.
    - Dumpster Diving buscar información en la basura.
    - Uso de Internet-Intranet de la empresa.
    - Técnicas de Fuera de la oficina como: almuerzo de negocios o reuniones de negocios.
- Seductivas y/o Inadvertidas
    - Generar un perfil de autoridad dentro de la empresa.
    - Utilizar carisma, modales amistosos y generar confianza
    - Generar reciprocidad mediante el ofrecimiento de ayuda.
    - Consistencia, el contacto repetido para generar familiaridad.
    - Actuar como un compañero de trabajo que necesita de información.
    - Ingeniería Social Invertida creando una persona de autoridad dentro del ambiente laboral, de esta manera las personas le pedirán información a él. [1]

Vulnerabilidad de los Sistemas

La vulnerabilidad de los sistemas se puede definir como las debilidades, fallas o amenazas que existen dentro de un sistema computacional o de su información y aplicaciones. Las vulnerabilidades se descubren de manera seguida en grandes sistemas, lo cual pone en grave riesgo los mismos.

Según Anónimo (Internet; desconocido; 27, 10, 2011; 15h41 pm) la vulnerabilidad es el grado de exposición de un sistema a los efectos de una amenaza, determinada por el sujeto, comunidad y sujeto de hacer frente a un cambio tecnológico.

La vulnerabilidad de los sistemas está directamente relacionada con la amenaza debido a que no puede existir una amenaza si en una primera instancia no se ha detectado la existencia de una vulnerabilidad; lo sistemas se encuentran expuestos a estas amenazas debido a que las vulnerabilidades son expuestas mucho antes de que exista una solución o se tomen precauciones para controlarlas.

Amenazas Tecnológicas

Según EMM, David (Internet; 24, 03, 2010; 22, 10, 2011; 11h53 am) “El actual panorama de amenazas se presenta muy complejo. Los ciberdelincuentes recurren a una amplia gama de amenazas para capturar equipos y obtener ganancias ilícitas. Entre estas amenazas se incluyen los troyanos de distintos tipos, los gusanos, los virus y los códigos de explotación, estos últimos diseñados para activar programas maliciosos (malware) que aprovechen las vulnerabilidades de los sistemas operativos o de las aplicaciones. Los piratas informáticos también utilizan sofisticadas técnicas para ocultar la actividad de estos programas maliciosos o para evitar en lo posible que las soluciones antivirus encuentren, analicen y detecten los códigos maliciosos”. [2]

Las amenazas tecnológicas afectan directamente a las vulnerabilidades encontradas en los sistemas tecnológicos, ya que estas usan estas para alcanzar sus objetivos. Estas amenazas están directamente ligadas por factores que afectan directamente la seguridad de la información y la infraestructura tecnológica.

Ataques Informáticos

Los ataques informáticos se centran en vulnerar la tecnología como hardware y software para afectar de manera directa su correcto funcionamiento; de esta manera se logra romper las seguridades que en la tecnología se puedan colocar para salvaguardar la información. A este concepto podemos incorporar los ataques directamente relacionados con técnicas para vulnerar el factor humano que es el más propenso hacia ataques con finalidad de substracción de información importante y confidencial.

Fuga de Información Confidencial

La fuga de información confidencial es la divulgación la cual se debe tanto a los ataques tecnológicos y los niveles de seguridad de la información digitalizada que se posea en un entorno sensible a los ataques y robo de información.

Según PACHECO, Federico (Internet; 19, 01, 2011; 28, 10, 2011; 13h12 pm) "La confidencialidad se refiere a la característica que implica que la información sea accedida solamente por los usuarios autorizados. Por su parte, la privacidad habla más bien de una garantía de confianza respecto a la propia información y su uso, diferenciándose de lo público y de lo secreto."

La fuga de la información confidencial es el escape de información priorizada; considerada importante y privada la cual está transformada por estos aspectos en el Activo más importante y sensible a ataques de una organización.

Tipos de Fuga de Información Confidencial

Según CLEARSWIFT (Internet, Desconocido; 04, 01,2012; 14:45 pm) las fugas de información se pueden clasificar en tres categorías:

1. Fuga Saliente: Este tipo de fuga de información es aquella que está en contacto directo con el Internet como el correo electrónico, Web, entre otros.
Este tipo de fuga puede causar varias pérdidas importantes de información como puede ser:

- Pérdida de propiedad intelectual y de otra información confidencial de la empresa, como previsiones financieras, presupuestos, datos sobre la competencia, planes de marketing, etc.
- Pérdida de datos confidenciales de los clientes, como información de crédito personal (PCI) o historiales de compras.
- Pérdida de información de identificación personal (PII), como números de identificación o historias de pacientes.
- Contenido publicado en páginas de la Web 2.0 y de redes sociales.

2. Fuga Interna: Este tipo de fugas se dan generalmente por el incumplimiento de las políticas de seguridad aplicadas dentro de una empresa. El envió de información errada entre departamentos puede traer graves consecuencias tanto políticas, despidos de personal y económico a la empresa.

3. Fuga Entrante: Este tipo de fuga difiere de la saliente y la interna debido a que en esta actúan elementos de software agresivos y maliciosos como son: spyware, pishing y spam. Estos pueden pueden viajar con el correo electrónico o los mensajes instantáneos entrantes o llegar a través de descargas automáticas o de

ejecutables cuando se visitan sitios Web maliciosos. El objetivo del software malicioso es poner en peligro los equipos y provocar fugas de datos.

Consecuencias de la Fuga de Información Confidencial

Las principales consecuencias de la fuga de información pueden ser:

- Pérdida de información considerada como activo de la empresa.
- Irresponsabilidad en el manejo de información.
- No respeto de las políticas y protocolos de seguridad vigentes en la entidad u organización.
- No existencia de medidas preventivas para la contratación y la desvinculación de personal a la organización.
- Eliminación insegura de los datos.
- Comunicación y establecimiento de relaciones laborales para conocimiento de la gente que labora en la organización.

De esta manera las vulnerabilidades y probabilidades de ataques son muy elevados y la aplicación de técnicas para robo de información son de alta probabilidad positiva para generar resultados.

2.4. Hipótesis

La vulnerabilidad humana en relación a la Seguridad Informática influye en la fuga de información confidencial en el Departamento de Recursos Humanos de la Universidad Técnica de Ambato.

Unidades de Observación: Personal del Departamentos de Recursos Humanos de la Universidad Técnica de Ambato.

2.5. Señalamiento de variables

Variable Independiente: Vulnerabilidades Humanas en relación a la Seguridad Informática.

Variable Dependiente: Fuga de Información Confidencial

CAPITULO III

3. MARCO METODOLÓGICO

3.1. Enfoque

El presente trabajo investigativo tomará un enfoque Cuali-Cuantitativo con las siguientes consideraciones:

Siempre estará considerado dentro de su entorno natural, se considera la participación de las personas que intervienen con el problema dentro del problema, considerando su cultura y creencia, se considerará interna porque nos permite analizar de manera interna el problema, se considera interpretativa porque nos permite analizar sus resultados.

Se considera como normativa porque se generará una norma o herramienta a seguir, se considera nomotética porque llevará a un fin concreto, se considera externa porque se determinará la influencia del problema con relación a la sociedad, se considera explicativa porque nos permitirá explicar los resultados a obtener.

3.2. Modalidades Básicas de la Investigación

La presente investigación tiene las siguientes modalidades:

Modalidad Bibliográfica o Documentada: Se ha considerado esta modalidad porque se ha tomado información de Internet, Libros virtuales, Tesis, Artículos publicados en la Web, Libros y otros.

Modalidad Experimental: Se ha considerado la relación de la variable independiente VULNERABILIDAD HUMANA EN RELACIÓN A LA SEGURIDAD INFORMÁTICA su influencia y relación en la variable dependiente FUGA DE INFORMACIÓN CONFIDENCIAL para considerar sus causas y sus efectos.

Modalidad De Campo: Se ha considerado esta modalidad ya que el investigador irá a recoger la información primaria directamente de los involucrados a través de encuestas.

3.3. Tipos de Investigación

Se ha realizado la Investigación Exploratoria, ya que permitió plantear el problema de la investigación ¿Cómo incide la vulnerabilidad humana en relación a la Seguridad Informática en la fuga de información confidencial en el Departamento de Recursos Humanos de la Universidad Técnica de Ambato? como de la misma manera ayudo a plantear la hipótesis La vulnerabilidad humana en relación a la Seguridad Informática influye en la fuga de información

confidencial en el Departamento de Recursos Humanos de la Universidad Técnica de Ambato.

Se ha considerado la Investigación Descriptiva porque permitió analizar el problema en sus partes como delimitar en tiempo y en espacio construyendo el Análisis Crítico, la Contextualización y los Antecedentes Investigativos.

Por otro lado se ha tomado la investigación Correlacional ya que ha permitido medir la compatibilidad de Variable Independiente Vulnerabilidades Humanas en relación a la Seguridad Informática con la Variable Dependiente fuga de información confidencial.

3.4. Población y Muestra

Población

La población está conformada por 7 personas del Departamento de Recursos Humanos del Campus Ingahurco y 4 personas del Departamento de Recursos humanos del Campus Huachi.

Muestra

Debido a que el tamaño de la población es pequeño el investigador trabaja con toda como muestra para la investigación.

3.5. Operacionalización de Variables

Hipótesis:

La vulnerabilidad humana en relación a la Seguridad Informática influye en la fuga de información confidencial en el Departamento de Recursos Humanos de la Universidad Técnica de Ambato.

Variable Independiente: Vulnerabilidades humanas en relación a la Seguridad Informática

Concepto	**Categorías**	**Indicadores**	**Ítems**	**Técnicas e instrumentos**
Es la exposición del factor humano hacia los ataques informáticos para obtener acceso a los sistemas.	Factor Humano	• Conocimiento de seguridad • Manejo de información	¿Qué porcentaje de conocimiento de los protocolos de seguridad poseen?	Encuesta mediante un cuestionario al personal.
	Ataques Informáticos	• Suplantación de Identidad • Nivel de seguridad de contraseñas • Personalización de contraseñas	¿El personal está propenso a la suplantación de identidad? ¿Cuáles son los niveles de seguridad de las contraseñas?	Encuesta a través de un cuestionario aplicada al personal. Encuesta a través de un cuestionario aplicada al personal.
	Acceso	• Facilidad • Frecuencia • Seguridad	¿Qué niveles de facilidad, frecuencia y seguridad del acceso al departamento se usan?	Encuesta a través de un cuestionario aplicado al administrador.
	Sistemas	• Tipos de Sistemas • Estado funcional	¿Qué tipo de sistemas se usa y cuál es su estado funcional?	Encuesta a través de un cuestionario aplicado al administrador.

Tabla 3.1. Operacionalización de la Variable Independiente

Variable Dependiente: Fuga de Información Confidencial

Concepto	**Categorías**	**Indicadores**	**Ítems**	**Técnicas e instrumentos**
Es el escape de información priorizada, considerada importante y privada de una institución.	Información Priorizada	Tipo Cantidad Características Importancia	¿Cuál es la información priorizada? ¿Es considerada como importante?	Encuesta a través de un cuestionario aplicada al personal y administrador.
	Privada	Manejo Respaldo	¿Cómo es manejada y asegurada la información privada?	Encuesta a través de un cuestionario aplicada al administrador.
	Institución	Seguridades de los sistemas Ataques	¿Se han registrado ataques en institución? ¿Existen seguridades en los sistemas?	Encuesta a través de un cuestionario aplicado al administrador.

Tabla 3.2. Operacionalización de la Variable Dependiente

3.6. Recolección y Análisis de la Información

SECUNDARIA	PRIMARIA
• Se recolectó de estudios realizados anteriormente como Tesis de Grado que se han realizado anteriormente. • Se encuentra registrada en documentos y material impreso: libros, revistas especializadas, tesis de grado, etc. • Las fuentes de información son: bibliotecas, archivos, internet.	• Se recolecta directamente a través del contacto directo con el personal del Departamento de Recursos Humanos de la Universidad Técnica de Ambato.

Tabla 3.3. Recolección y Análisis de la Información

Técnicas de Investigación

BIBLIOGRÁFICAS	DE CAMPO
• El análisis de documentos (lectura científica) • El fichaje	• La encuesta

Tabla 3.4. Técnicas de Investigación

Recolección de la Información

PREGUNTAS	EXPLICACIÓN
1. ¿Para Qué?	Recolectar Información primaria para comprobar y contrastar la Hipótesis
2. ¿A Qué Personas o Sujetos?	La información se tomará al personal que actualmente labora en el Departamentos de Recursos Humanos
3. ¿Sobre Qué Aspectos?	Vulnerabilidades Humanas en relación a la Seguridad Informática
4. ¿Quién?	María Gabriela Cortez Pinto
5. ¿Cuándo?	De acuerdo al cronograma establecido
6. ¿Lugar de Recolección de la Información?	Universidad Técnica de Ambato
7. ¿Cuántas veces?	Una sola vez
8. ¿Qué técnicas de recolección?	Encuesta
9. ¿Con Qué?	Cuestionario
10. ¿En Qué Situación?	Situación Normal y Cotidiana

Tabla 3.5. Recolección de la Información.

3.7. Procesamiento y Análisis de la Información

- Revisión y Codificación de la Información
- Categorización y Tabulación de la Información
  - Tabulación Manual

- Análisis de los datos

La presentación de los datos se lo hará a través de los datos, cuadros para analizarlos e interpretarlos.

- Interpretación de los Resultados
  1. Describir los resultados
  2. Estudiar cada uno de los resultados por separado
  3. Redactar una síntesis general de los resultados

CAPITULO IV

4. ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

4.1.Análisis e Interpretación de Resultados

Encuesta aplicada al Personal del Departamento de Recursos Humanos de la UTA

1. ¿Conoce sobre los ataques de Ingeniería Social?

N°	ÍTEMS	FRECUENCIA	%
1	SI	3	27%
2	NO	8	73%
TOTAL		**11**	**100%**

Tabla N° 4.1. Frecuencia Pregunta 1

Fuente: Departamento de Recursos Humanos de la UTA

Autor: Gabriela Cortez

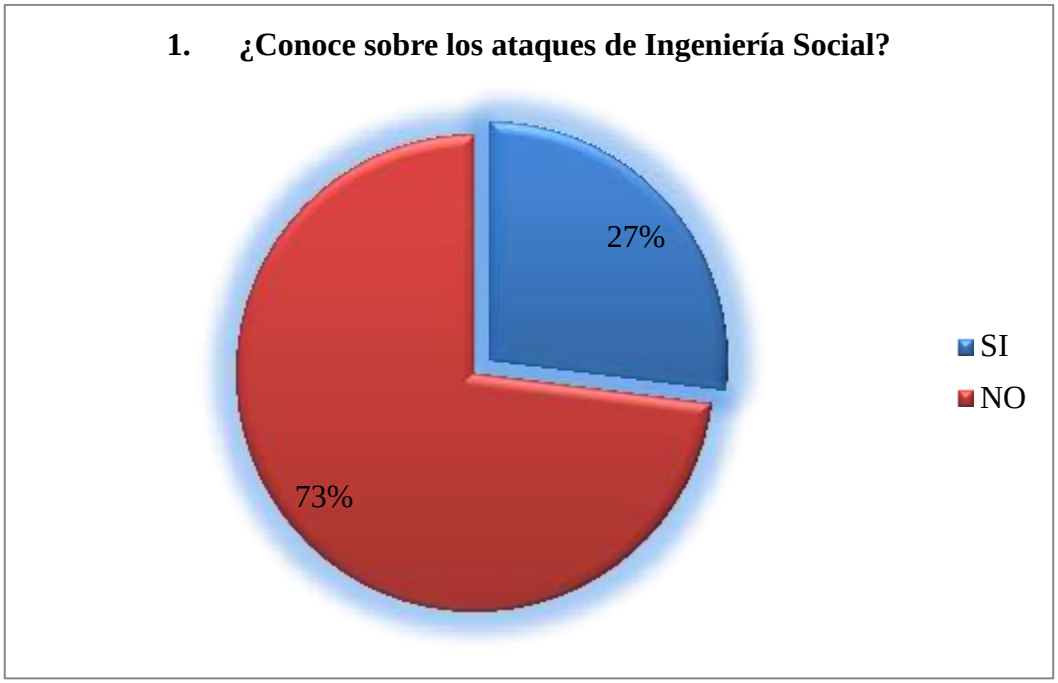


Grafico N° 4.1. Gráfico Pregunta 1

Fuente: Departamento de Recursos Humanos de la UTA

Autor: Gabriela Cortez

Interpretación:

De las personas encuestadas, el 27% conoce sobre los ataques de Ingeniería Social y el 73% de las personas encuestadas no conocen sobre los ataques de la Ingeniería Social.

Análisis:

De los datos obtenidos se puede establecer que una de las causa de la vulnerabilidad humana es el desconocimiento por parte del factor humano.

2. ¿Conoce usted cuáles son los procedimientos de seguridad que debe seguir en caso de que exista un ataque informático o de Ingeniería Social dentro del departamento?

N°	ÍTEMS	FRECUENCIA	%
1	SI	3	27%
2	NO	8	73%
TOTAL		**11**	**100%**

Tabla N° 4.2. Análisis Pregunta 2

Fuente: Departamento de Recursos Humanos de la UTA

Autor: Gabriela Cortez

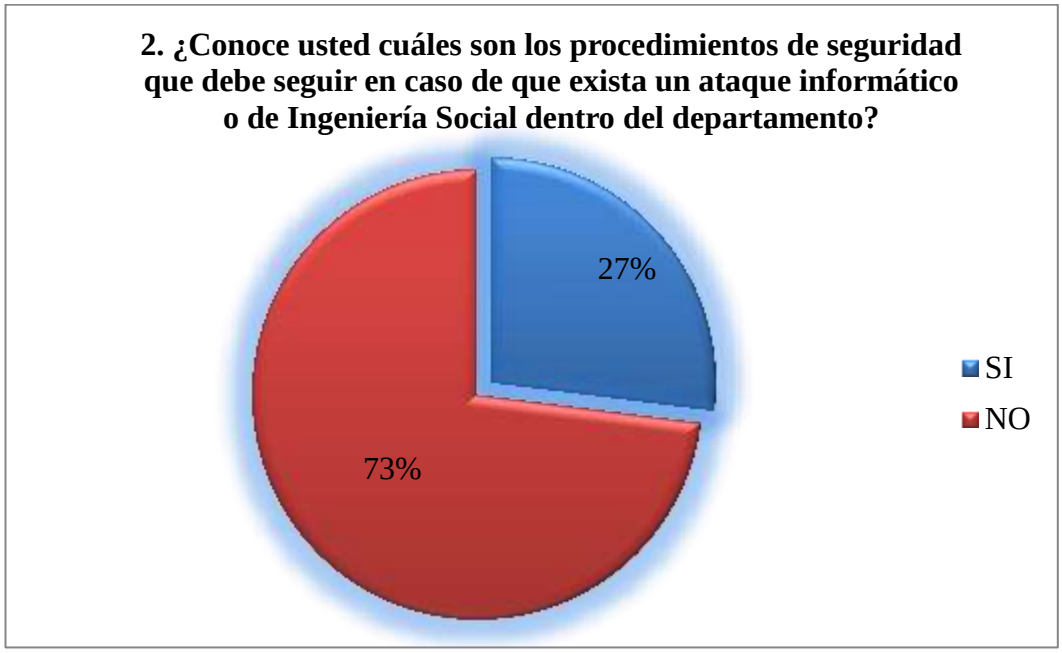


Grafico N° 4.2. Grafico Pregunta N°2

Fuente: Departamento de Recursos Humanos de la UTA

Autor: Gabriela Cortez

Interpretación:

De las personas encuestadas, el 27% conoce sobre los procedimientos que se debe seguir en caso de que exista algún tipo de ataque informático incluyendo los ataques de Ingeniería Social dentro del Departamento de Recursos Humanos de Universidad Técnica de Ambato y el 73% desconoce los procedimientos que se debe seguir en caso de que exista algún tipo de ataque informático incluyendo los ataques de Ingeniería Social dentro del Departamento de Recursos Humanos de Universidad Técnica de Ambato.

Análisis:

De los datos podemos deducir que el departamento de Recursos Humanos de la Universidad Técnica de Ambato posee un alto nivel de vulnerabilidad por la falta de procedimientos de prevención de ataques informáticos.

3. ¿Cree usted que la tecnología y los equipos que existen dentro del departamento son suficientemente seguros y no sufrirán un ataque de Ingeniería Social?

N°	ÍTEMS	FRECUENCIA	%
1	SI	6	55%
2	NO	5	45%
TOTAL		**11**	**100%**

Tabla N° 4.3. Frecuencia Pregunta 3

Fuente: Departamento de Recursos Humanos de la UTA

Autor: Gabriela Cortez

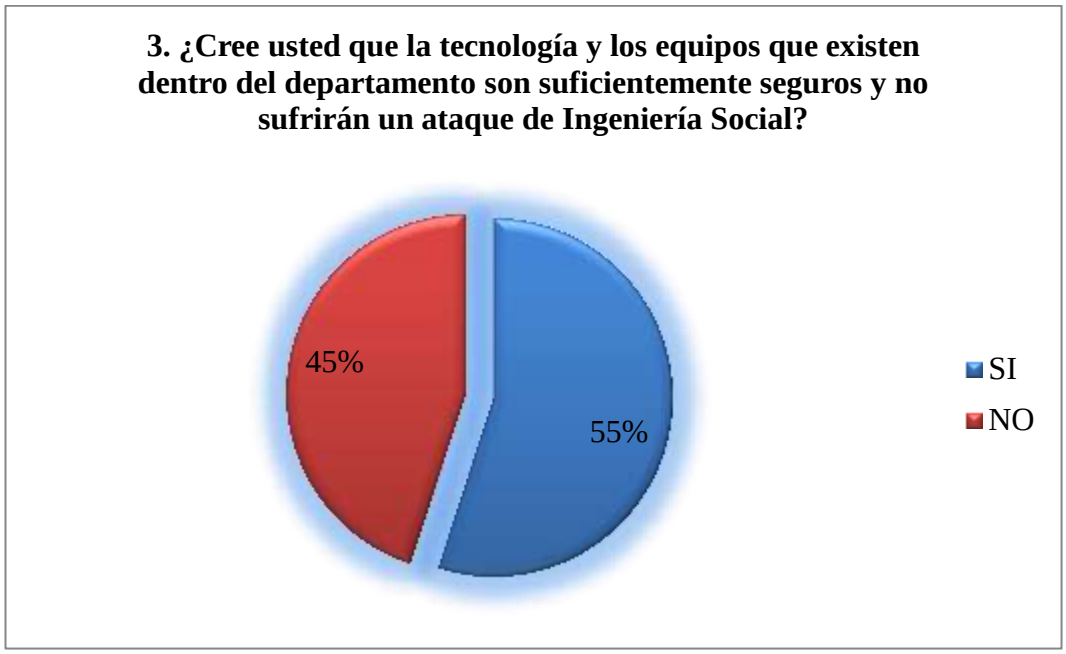


Grafico N° 4.3. Grafico Pregunta N°3

Fuente: Departamento de Recursos Humanos de la UTA

Autor: Gabriela Cortez

Interpretación:

De las personas encuestadas, el 55% cree que la tecnología y los equipos tecnológicos que existen dentro del departamento son suficientemente seguros y no sufrirán un ataque de Ingeniería Social y el 45% de las personas encuestadas cree que la tecnología y los equipos tecnológicos que existen dentro del departamento no son lo suficientemente seguros y sufrirán un ataque de Ingeniería Social dentro del Departamento de Recursos Humanos de Universidad Técnica de Ambato.

Análisis:

El desconocimiento sobre el tipo de ataques que puede sufrir la información del departamento eleva el nivel de vulnerabilidad frente a los mismos.

4. Para el acceso a su computador destinada para sus labores diarias en su lugar de trabajo, utiliza usted:

N°	ÍTEMS	FRECUENCIA	%
1	Contraseña de Seguridad	11	100%
2	No existe ningún tipo de Restricción	0	0%
3	Necesita de un administrador para el acceso	0	0%
	TOTAL	**11**	**100%**

Tabla N° 4.4. Frecuencia Pregunta 4

Fuente: Departamento de Recursos Humanos de la UTA

Autor: Gabriela Cortez

Grafico N° 4.4. Grafico Pregunta N°4

Fuente: Departamento de Recursos Humanos de la UTA

Autor: Gabriela Cortez

Interpretación:

De las personas encuestadas, el 100% de las personas asegura que utiliza una contraseña de seguridad para el acceso al computador destinada para sus labores diarias en su lugar de trabajo.

Análisis:

De los datos obtenidos se puede observar que la vulnerabilidad de los sistemas e información en el departamento es elevada.

5. ¿Cree usted que está propenso a algún tipo de ataque de Ingeniería Social?

N°	ÍTEMS	FRECUENCIA	%
1	SI	8	73%
2	NO	3	27%
TOTAL		**11**	**100%**

Tabla N° 4.5. Frecuencia Pregunta 5

Fuente: Departamento de Recursos Humanos de la UTA

Autor: Gabriela Cortez

Grafico N° 4.5. Grafico Pregunta N°5

Fuente: Departamento de Recursos Humanos de la UTA

Autor: Gabriela Cortez

Interpretación:

De las personas encuestadas, el 73% que corresponde a cuatro personas cree que se encuentra propenso a algún tipo de ataque de Ingeniería Social y 27% de las personas encuestadas que corresponde a dos personas cree que no se encuentra propenso a algún tipo de ataque de Ingeniería Social.

Análisis:

Se determina que el desconocimiento de los tipos de ataques informáticos existentes es muy frecuente y puede afectar directamente a la información del Departamento de Recursos Humanos de la Universidad Técnica de Ambato.

6. ¿Utiliza usted una misma contraseña de seguridad para acceder a todas sus cuentas personales?

N°	ÍTEMS	FRECUENCIA	%
1	SI	0	0%
2	NO	11	100%
TOTAL		**11**	**100%**

Tabla N° 4.6. Frecuencia Pregunta 6

Fuente: Departamento de Recursos Humanos de la UTA

Autor: Gabriela Cortez

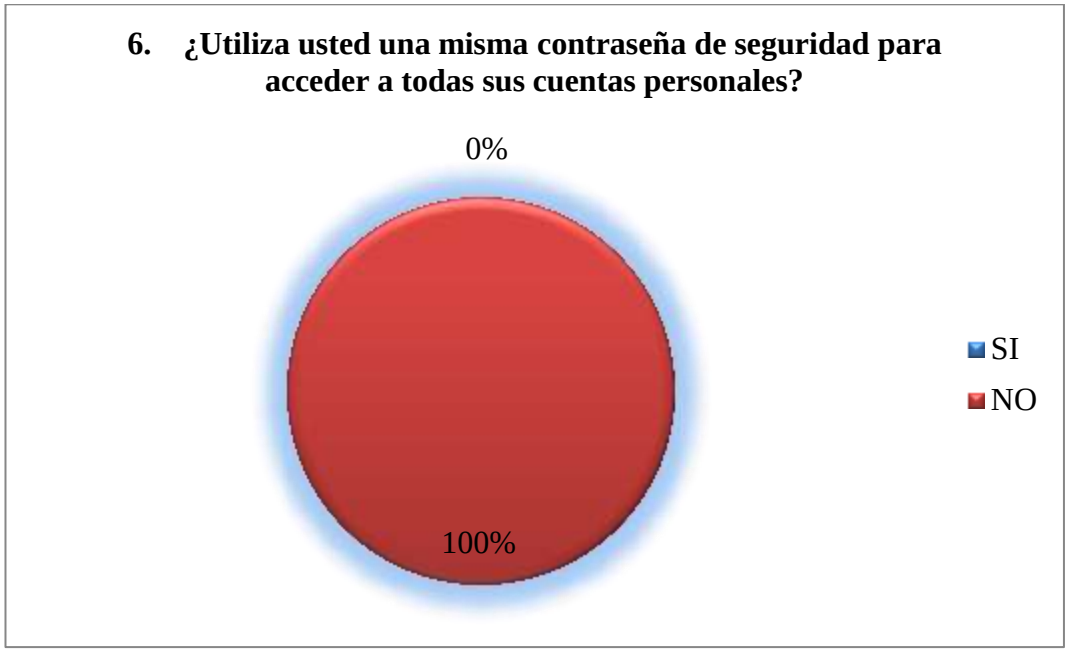


Grafico N° 4.6. Grafico Pregunta N°6

Fuente: Departamento de Recursos Humanos de la UTA

Autor: Gabriela Cortez

Interpretación:

De las personas encuestadas, el 100% de las personas asegura que no utiliza una misma contraseña de seguridad para el acceso a sus cuentas personales.

Análisis:

El personal del departamento de Recursos Humano posee precauciones en cuanto a la utilización de claves.

7. ¿Ha compartido alguna vez su contraseña de seguridad con alguna persona de su confianza?

N°	ÍTEMS	FRECUENCIA	%
1	SI	2	33%
2	NO	4	67%
TOTAL		**11**	**100%**

Tabla N° 4.7. Frecuencia Pregunta 7

Fuente: Departamento de Recursos Humanos de la UTA

Autor: Gabriela Cortez

Grafico N° 4.7. Grafico Pregunta N°7

Fuente: Departamento de Recursos Humanos de la UTA

Autor: Gabriela Cortez

Interpretación:

De las 11 personas encuestadas, el 64% de las personas no ha compartido sus contraseñas de seguridad con alguna persona que posea su confianza; en cambio el 36% de las personas encuestadas si ha compartido su contraseña con alguna persona de su confianza; en este caso con los compañeros de trabajo del Departamento de Recursos Humanos de la Universidad Técnica de Ambato.

Análisis:

La existencia de divulgación de las contraseñas pone en elevado riesgo la información. Lo cual nos lleva a contradecir el concepto de Seguridad Informática que según AGUILERA, Purificación (Internet; desconocido; 22, 10,2011; 12h2 pm) Es una disciplina que se encarga del diseño de métodos y procedimientos y técnicas para poder conseguir un sistema computacional seguro y confiable.

8. ¿Qué parámetros utiliza usted en su contraseña?

N°	ÍTEMS	FRECUENCIA	%
1	Números	9	39%
2	Letras Minúsculas	9	39%
3	Letras Mayúsculas	4	17%
4	Símbolos o caracteres especiales	1	4%
TOTAL FRECUENCIA		**23**	**100%**

Tabla N° 4.8. Frecuencia Pregunta 8

Fuente: Departamento de Recursos Humanos de la UTA

Autor: Gabriela Cortez

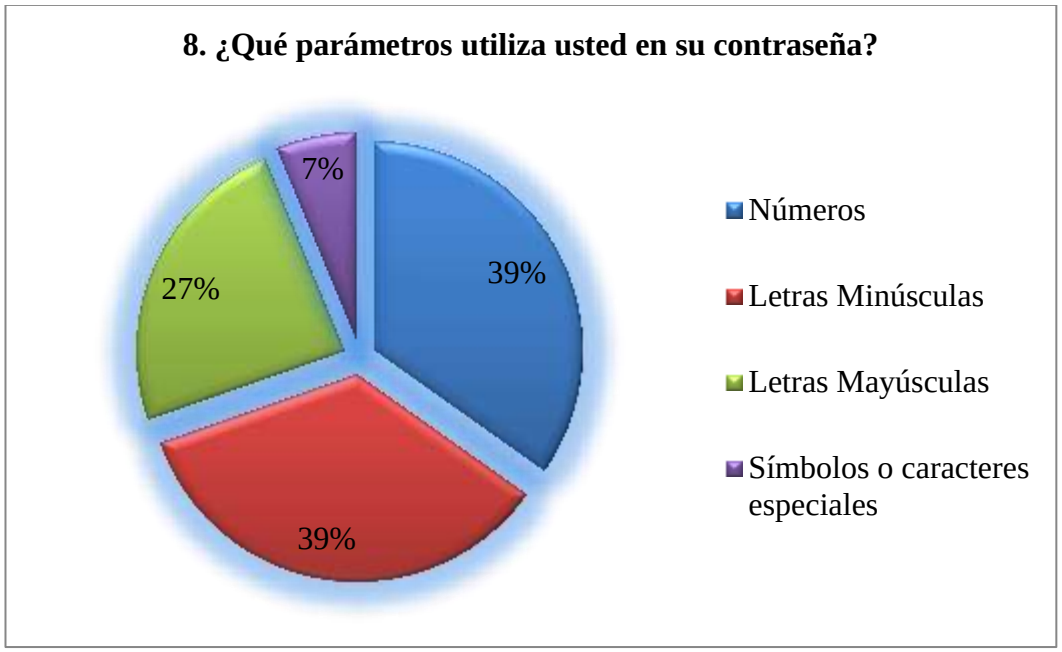


Grafico N° 4.8. Grafico Pregunta N°8

Fuente: Departamento de Recursos Humanos de la UTA

Autor: Gabriela Cortez

Interpretación:

De las personas encuestadas, el 39% de las frecuencias obtenidas se utilizan parámetros de claves numéricos y parámetros alfabéticos minúsculos en su contraseña de seguridad, el 27% de las frecuencias detalla que también se utiliza Letras Mayúsculas como parámetro en su contraseña de seguridad y solamente el 7% de la frecuencia adopta como parámetro de contraseña los símbolos o caracteres especiales dentro de su contraseña de seguridad.

Análisis:

Se puede concluir que la combinación de parámetros o a su vez la utilización de un solo tipo de parámetros para claves de seguridad expone de manera considerable los niveles de vulnerabilidad; a su vez la combinación de todos los parámetros descritos pueden aumentar los niveles de seguridad de las contraseñas.

9. En su clave de seguridad utiliza:

N°	ÍTEMS	FRECUENCIA	%
1	Nombres	5	26%
2	Apellidos	6	32%
3	Fechas Importantes	2	11%
4	Placa del Auto	0	0%
5	Número de Cédula	5	26%
6	No contesta	1	5%
TOTAL FRECUENCIA		**19**	**100%**

Tabla N° 4.9. Frecuencia Pregunta 9

Fuente: Departamento de Recursos Humanos de la UTA

Autor: Gabriela Cortez

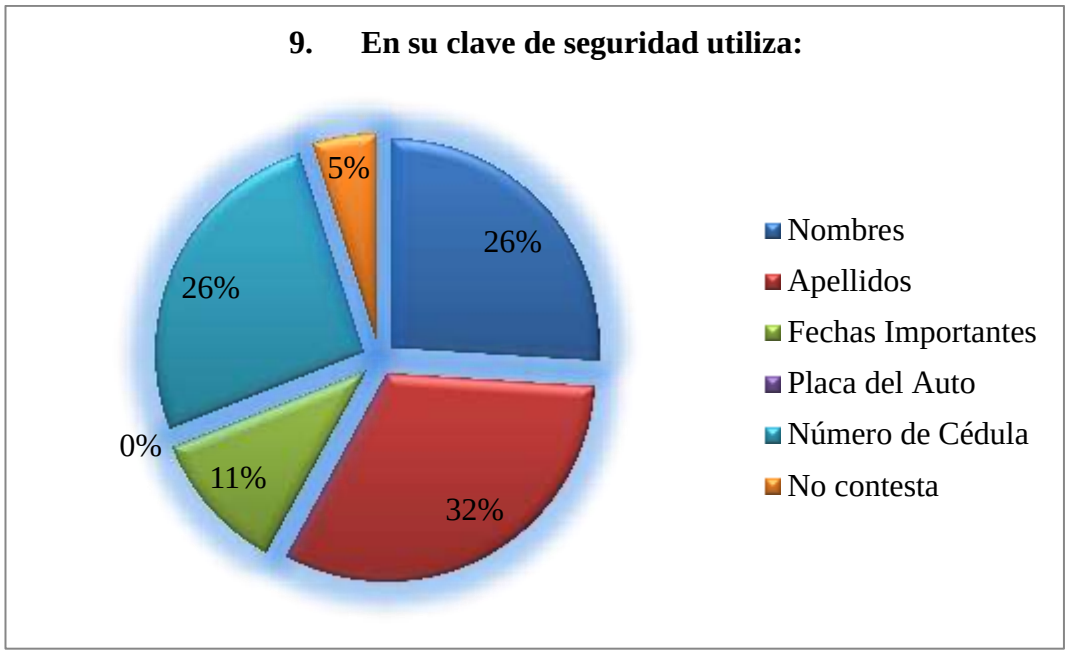


Grafico N° 4.9. Grafico Pregunta N°9

Fuente: Departamento de Recursos Humanos de la UTA

Autor: Gabriela Cortez

Interpretación:

De las personas encuestadas, se obtuvieron las siguientes frecuencias de los parámetros personales utilizados en las contraseñas de seguridad de los colaboradores del departamento de Recursos Humanos de la UTA, el 26% utiliza sus nombres para crear su contraseña de seguridad,; el 32% utiliza sus apellidos para la creación de su contraseña de seguridad, el 11% utiliza fechas importantes para ellas en la creación de sus contraseñas de seguridad, el 0% lo que quiere decir que ninguna persona utiliza la placa de sus auto como un parámetro a usar en su contraseña de seguridad; el 26% utiliza su número de cédula para la creación de una contraseña de seguridad y el 5% de las personas no contesta esta pregunta porque asegura no utilizar ninguno de estos parámetros parta la creación de su contraseña de seguridad.

Análisis:

Se puede determinar que el personal del Departamento de Recursos Humanos de la Universidad Técnica de Ambato utiliza datos personales para proteger su información tanto privada como la información del departamento poniendo en riesgo la seguridad de la información y del departamento.

10. ¿Alguna vez ha sido víctima de robo informático?

N°	ÍTEMS	FRECUENCIA	%
1	SI	1	9%
2	NO	10	91%
TOTAL		**11**	**100%**

Tabla N° 4.10. Frecuencia Pregunta 10

Fuente: Departamento de Recursos Humanos de la UTA

Autor: Gabriela Cortez

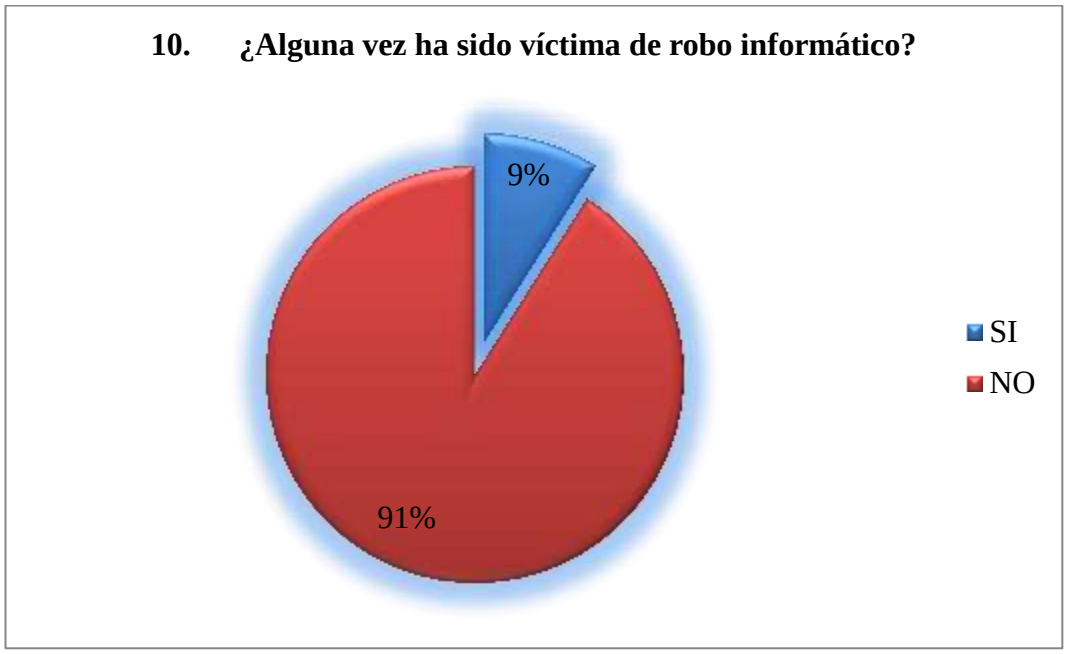


Grafico N° 4.10. Grafico Pregunta N°10

Fuente: Departamento de Recursos Humanos de la UTA

Autor: Gabriela Cortez

Interpretación:

De las personas encuestadas, el 9% del Departamento de Recursos Humanos de la UTA afirma haber sido víctima de robo informático y el 91% afirma no haber sido víctima de robo informático.

Análisis:

Lo cual demuestra que la vulnerabilidad humana dentro del departamento de Recursos Humanos de la UTA existe.

11. ¿Se utiliza algún tipo de seguridad física para los visitantes cuando ingresan al departamento o las instalaciones?

N°	ÍTEMS	FRECUENCIA	%
1	SI	0	0%
2	NO	11	100%
TOTAL		**11**	**100%**

Tabla N° 4.11. Frecuencia Pregunta 11

Fuente: Departamento de Recursos Humanos de la UTA

Autor: Gabriela Cortez

Grafico N° 4.11. Grafico Pregunta N°11

Fuente: Departamento de Recursos Humanos de la UTA

Autor: Gabriela Cortez

Interpretación:

De las personas encuestadas, el 100% del personal del departamento de de Recursos Humanos de la UTA afirma que no existe ningún tipo de seguridad física para los visitantes.

Análisis:

Los datos obtenidos afirman la existencia de una vulnerabilidad hacia los ataques de Ingeniería Social o cualquier tipo de ataque informático que requieran el acceso físico hacia un equipo.

12. ¿Con qué frecuencia se recibe a las personas dentro del Departamento?

N°	ÍTEMS	FRECUENCIA	%
1	Muy Frecuente	7	64%
2	Frecuente	3	27%
3	Poco Frecuente	1	9%
	TOTAL	**11**	**100%**

Tabla N° 4.12. Frecuencia Pregunta 12

Fuente: Departamento de Recursos Humanos de la UTA

Autor: Gabriela Cortez

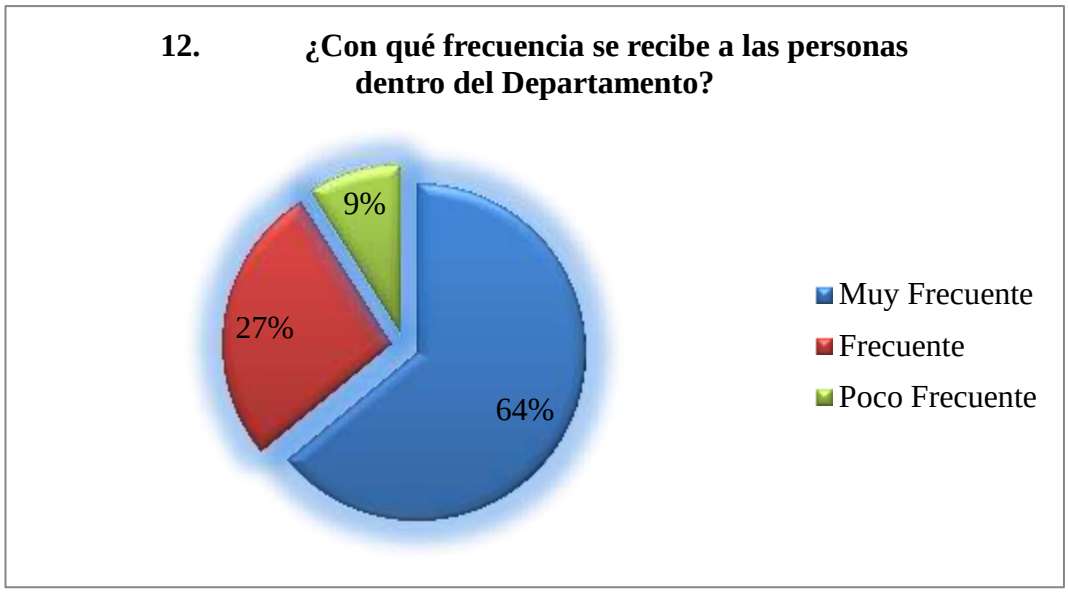


Grafico N° 4.12. Grafico Pregunta N°12

Fuente: Departamento de Recursos Humanos de la UTA

Autor: Gabriela Cortez

Interpretación:

De las personas encuestadas, el 64% afirma que se recibe a las personas de manera Muy frecuente dentro del departamento, el 27% afirma que solamente se reciben a las personas de manera Frecuente y el 9% dice recibir a los visitantes de manera Poco frecuente dentro del Departamento de Recursos Humanos de la Universidad Técnica de Ambato.

Análisis:

Debido a la afluencia de gente es necesario establecer procesos para controlar esta afluencia.

13. ¿Según su criterio como clasificaría usted la importancia de la información que maneja?

N°	ÍTEMS	FRECUENCIA	%
1	Muy Importante	8	73%
2	Importante	2	18%
3	Medianamente Importante	1	9%
4	Poco Importante	0	0%
TOTAL		**11**	**100%**

Tabla N° 4.13. Frecuencia Pregunta 13

Fuente: Departamento de Recursos Humanos de la UTA

Autor: Gabriela Cortez

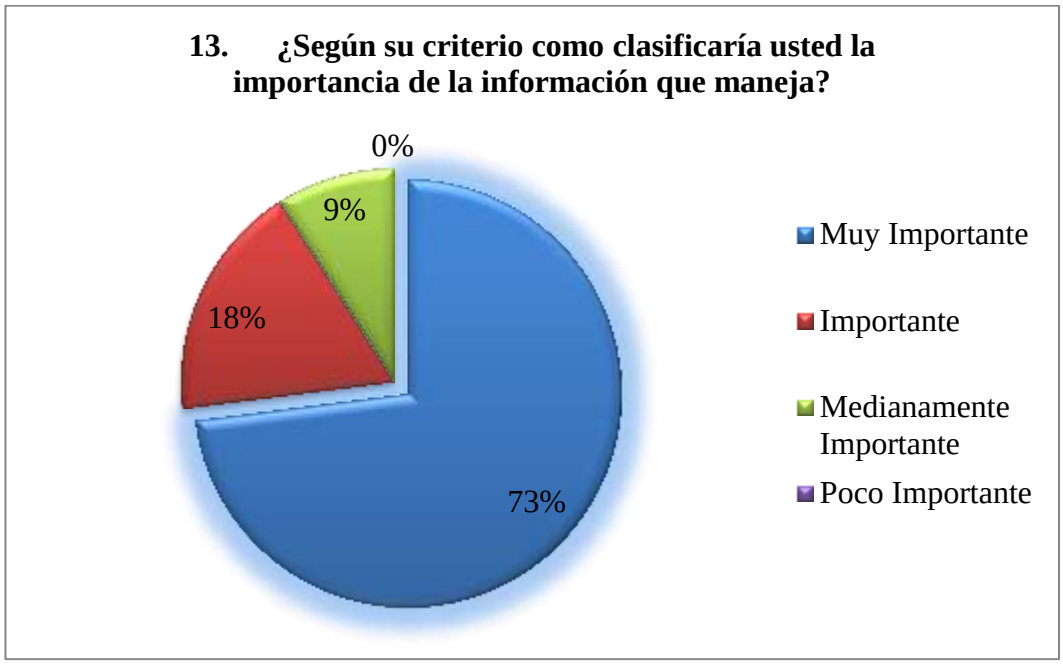


Grafico N° 4.13. Grafico Pregunta N°13

Fuente: Departamento de Recursos Humanos de la UTA

Autor: Gabriela Cortez

Interpretación:

De las personas encuestadas, el 73% considera que su información es Muy importante para el departamento; el 18% considera que su información es Importante; mientras que el 9% Medianamente Importante y el 0% consideran que la información que maneja es Poco Importante.

Análisis:

Los datos obtenidos revelan la importancia de la información manejada dentro del departamento.

ENCUESTA APLICADA AL ADMINISTRADOR DEL SISTEMA DEL DEPARTAMENTO DE RRHH DE LA UTA

1. ¿Qué tipo de sistemas se utiliza dentro del departamento de RRHH?

N°	ÍTEMS	FRECUENCIA	%
1	Contable	0	0%
2	Transaccional	1	50%
3	Apoyo a las Decisiones	0	0%
4	Control de Personal	0	0%
5	Información	1	50%
TOTAL FRECUENCIA		**2**	**100%**

Tabla 4.14. Frecuencia Pregunta 1 Administrador

Fuente: Departamento de Recursos Humanos de la UTA

Autor: Gabriela Cortez

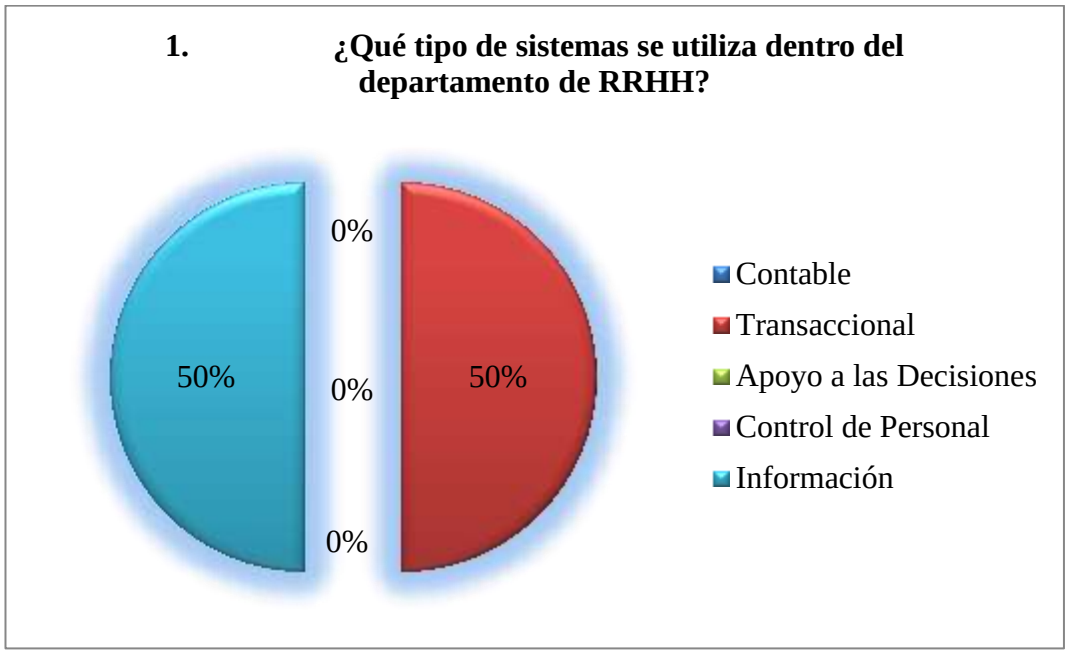


Gráfico 4.14. Gráfico Pregunta 1 Administrador

Fuente: Departamento de Recursos Humanos de la UTA

Autor: Gabriela Cortez

Interpretación:

Se obtiene que dentro del departamento se realizan movimientos de dinero y de información dentro del sistema.

Análisis:

Los datos obtenidos revelan la importancia de la información manejada dentro del departamento, así como la seguridad que debe ser aplicada dentro de cada una de las transacciones y movimientos de información.

2. **¿Cómo se encuentra actualmente el sistema?**

N°	ÍTEMS	FRECUENCIA	%
1	Funcional	0	0%
2	Necesita Actualizaciones	1	100%
3	Poco Funcional	0	0%
TOTAL FRECUENCIA		**1**	**100%**

Tabla 4.15. Frecuencia Pregunta 2 Administrador

Fuente: Departamento de Recursos Humanos de la UTA

Autor: Gabriela Cortez

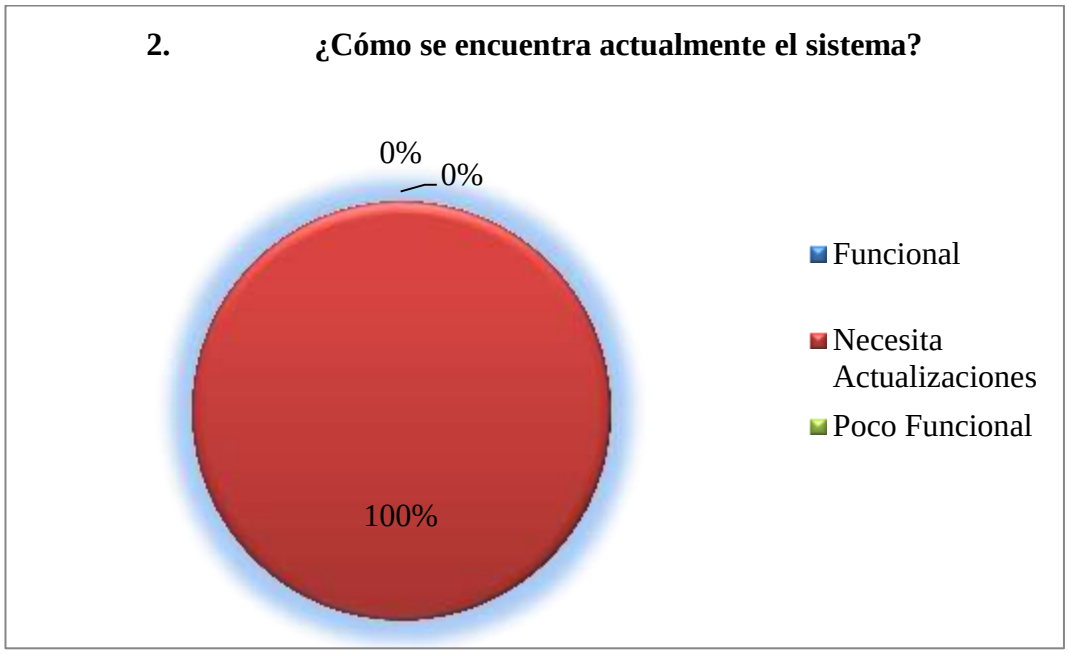


Tabla 4.15. Gráfico Pregunta 2 Administrador

Fuente: Departamento de Recursos Humanos de la UTA

Autor: Gabriela Cortez

Interpretación:

Una vez encuestado el administrador se conoce que el sistema necesito actualizaciones anuales.

Análisis:

Analizado los datos del sistema se puede verificar que el sistema posee fallas de seguridad hasta por un año los cual eleva el grado de vulnerabilidad del sistema en relación a la seguridad.

3. ¿Qué tipo de información se maneja en el departamento de RRHH de la UTA?

N°	ÍTEMS	FRECUENCIA	%
1	Información de los Docentes	1	25%
2	Financiera	1	25%
3	De estudiantes	0	0%
4	De proyectos	0	0%
5	Presupuestos	1	25%
6	Otro	1	25%
TOTAL FRECUENCIA		**4**	**100%**

Tabla 4.16. Frecuencia Pregunta 3 Administrador

Fuente: Departamento de Recursos Humanos de la UTA

Autor: Gabriela Cortez

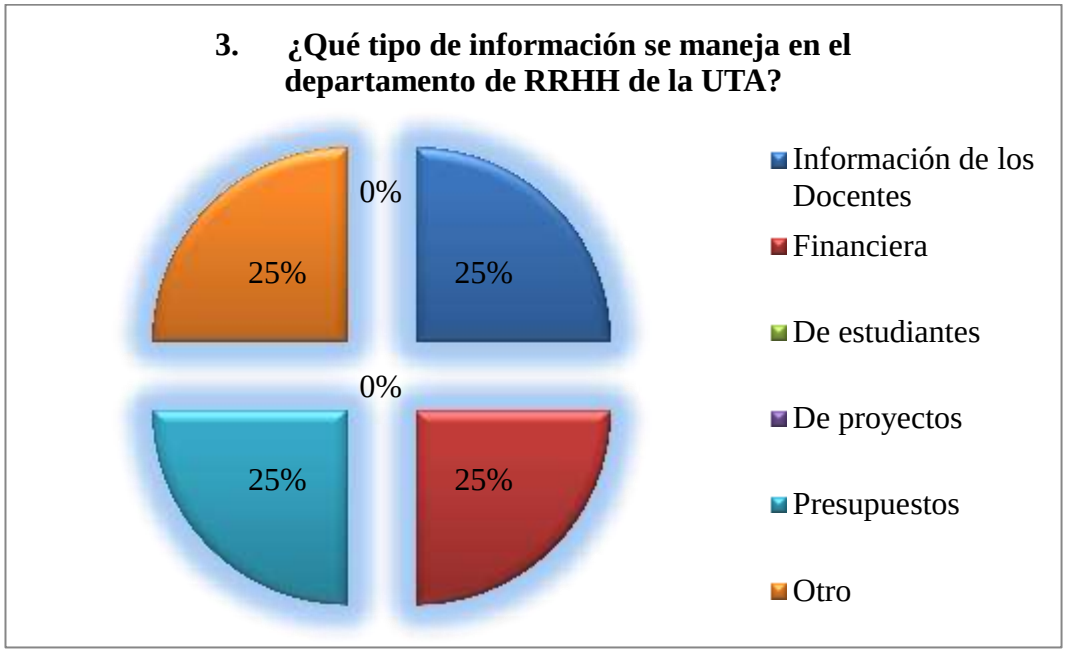


Tabla 4.16. Gráfico Pregunta 3 Administrador

Fuente: Departamento de Recursos Humanos de la UTA

Autor: Gabriela Cortez

Interpretación:

Una vez encuestado el administrador se conoce que el sistema utilizado dentro del departamento de Recursos Humanos de la UTA maneja información en relación a Docentes de la Universidad, Financiera, de presupuesto y además manejan otro tipo de información la cual es especificada como Estadística.

Análisis:

Analizado los datos obtenidos se puede retomar que la información del departamento es considerada como confidencial y requiere de la seguridad necesaria para salvaguardarla.

4. ¿La información del Departamento es considerada importante?

N°	ÍTEMS	FRECUENCIA	%
1	SI	1	100%
2	NO	0	0%
TOTAL FRECUENCIA		**1**	**100%**

Tabla 4.17. Frecuencia Pregunta 4 Administrador

Fuente: Departamento de Recursos Humanos de la UTA

Autor: Gabriela Cortez

Tabla 4.17. Gráfico Pregunta 4 Administrador

Fuente: Departamento de Recursos Humanos de la UTA

Autor: Gabriela Cortez

Interpretación:

De los resultados de la encuesta se encuentra que el 100% de la información generada por el departamento de recursos Humanos de la Universidad Técnica de Ambato es considerada como importante.

Análisis:

De los resultados obtenidos se puede determinar que la información es de alto contenido confidencial.

5. ¿La información es guardada de manera física?

N°	ÍTEMS	FRECUENCIA	%
1	SI	1	100%
2	NO	0	0%
TOTAL FRECUENCIA		**1**	**100%**

Tabla 4.18. Frecuencia Pregunta 5 Administrador

Fuente: Departamento de Recursos Humanos de la UTA

Autor: Gabriela Cortez

Tabla 4.18. Gráfico Pregunta 4 Administrador

Fuente: Departamento de Recursos Humanos de la UTA

Autor: Gabriela Cortez

Interpretación:

Una vez encuestado el administrador se conoce que la información generada por el departamento de Recursos Humanos de la UTA es almacenada de manera física.

Análisis:

Analizado los datos obtenidos se puede observar que la seguridad de los datos se los mantiene almacenados de manera física en caso de existir algún tipo de ataque informático.

6. ¿Se realizan respaldos de la información?

N°	ÍTEMS	FRECUENCIA	%
1	SI	1	100%
2	NO	0	0%
TOTAL FRECUENCIA		**1**	**100%**

Tabla 4.19. Frecuencia Pregunta 6 Administrador

Fuente: Departamento de Recursos Humanos de la UTA

Autor: Gabriela Cortez

Tabla 4.19. Gráfico Pregunta 6 Administrador

Fuente: Departamento de Recursos Humanos de la UTA

Autor: Gabriela Cortez

Interpretación:

Obtenidos los resultados se conoce que la información es respaldada.

Análisis:

De los resultados obtenidos se puede analizar que esta información es respaldada según los resultados obtenidos de la pregunta N° 5 de la encuesta aplicada al Administrador se puede deducir que la información que es respaldad es almacenada de manera física.

7. ¿Con que frecuencia se realizan los respaldos?

N°	ÍTEMS	FRECUENCIA	%
1	Diariamente	0	0%
2	Semanalmente	0	0%
3	Mensualmente	1	33,33%
4	Semestralmente	1	33,33%
5	Anualmente	1	33,33%
TOTAL FRECUENCIA		**3**	**100%**

Tabla 4.20. Frecuencia Pregunta 7 Administrador

Fuente: Departamento de Recursos Humanos de la UTA

Autor: Gabriela Cortez

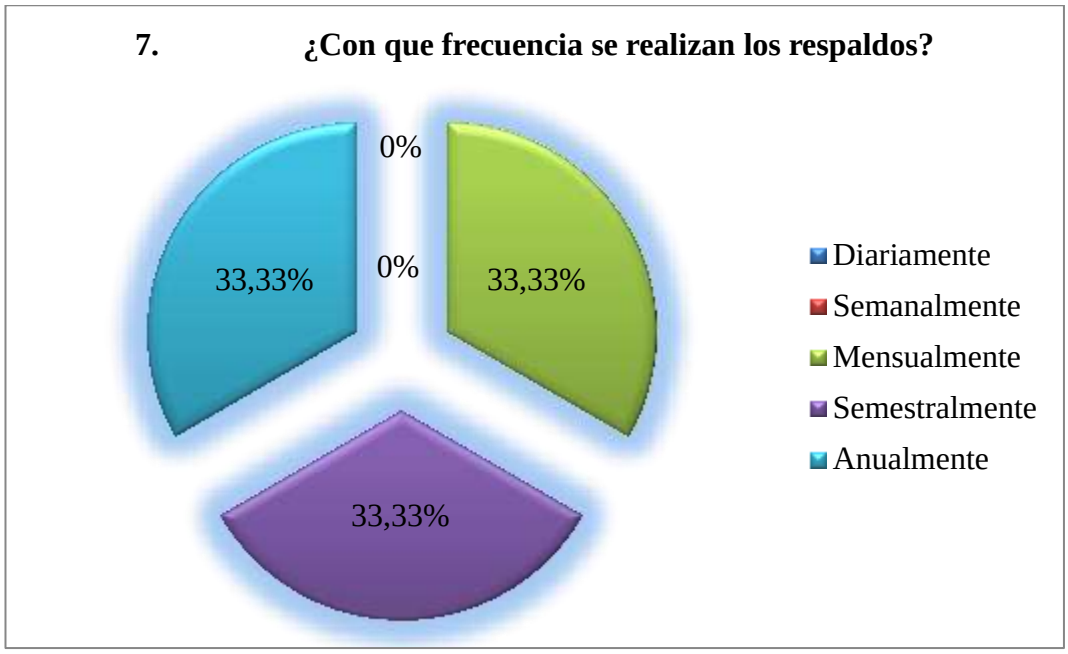


Tabla 4.20. Gráfico Pregunta 7 Administrador

Fuente: Departamento de Recursos Humanos de la UTA

Autor: Gabriela Cortez

Interpretación:

Según los datos obtenidos de la encuesta se obtiene que se realizan respaldos mensualmente, semestralmente y anualmente.

Análisis:

De los resultados obtenidos se puede analizar que los períodos de respaldo de la información no liberan a la misma de un ataque informático.

8. ¿Se han registrado ataques informáticos dentro del departamento?

N°	ÍTEMS	FRECUENCIA	%
1	SI	0	0%
2	NO	1	100%
TOTAL FRECUENCIA		**1**	**100%**

Tabla 4.21. Frecuencia Pregunta 8 Administrador

Fuente: Departamento de Recursos Humanos de la UTA

Autor: Gabriela Cortez

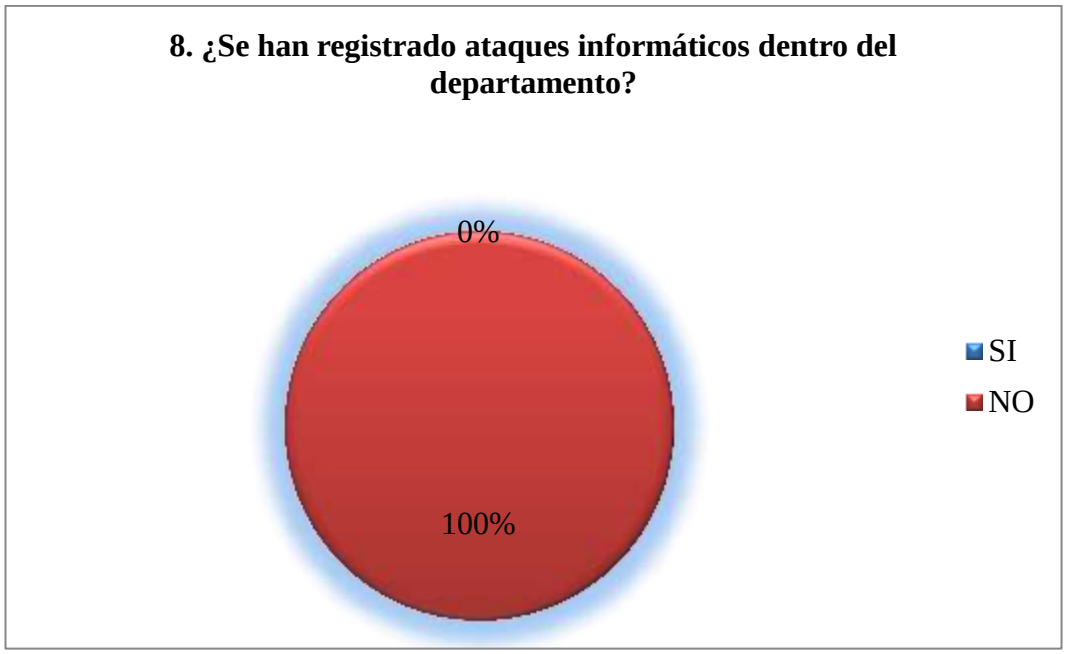


Tabla 4.21. Gráfico Pregunta 8 Administrador

Fuente: Departamento de Recursos Humanos de la UTA

Autor: Gabriela Cortez

Interpretación:

Según los datos obtenidos no se han registrado ataques informáticos dentro de departamento.

Análisis:

De los resultados obtenidos se puede analizar que si bien no hay ataques registrados a la información del departamento de recursos humanos, no linera a la misma o elimina las vulnerabilidades de ataques a la misma.

9. ¿Existen seguridades aplicadas dentro del departamento?

N°	ÍTEMS	FRECUENCIA	%
1	SI	0	0%
2	NO	1	100%
TOTAL FRECUENCIA		**1**	**100%**

Tabla 4.22. Frecuencia Pregunta 9 Administrador

Fuente: Departamento de Recursos Humanos de la UTA

Autor: Gabriela Cortez

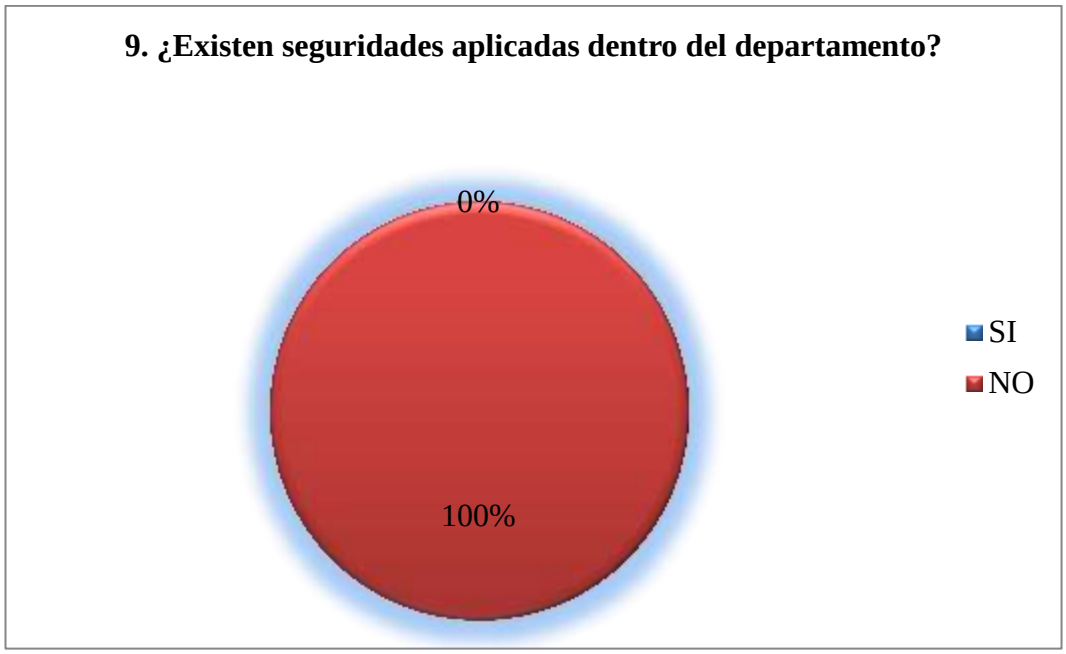


Tabla 4.22. Gráfico Pregunta 9 Administrador

Fuente: Departamento de Recursos Humanos de la UTA

Autor: Gabriela Cortez

Interpretación:

De la encuesta aplicada se obtiene que; no existen seguridades aplicadas dentro del departamento de recursos Humanos de la Universidad Técnica de Ambato.

Análisis:

Los datos arrojan que la seguridad informática no es aplicada directamente en el sistema de información del departamento, del mismo modo no se posee conocimiento de las vulnerabilidades humanas que son un gran nivel de amenaza hacia un ataque de Ingeniería Social.

4.2.INTERPRETACIÓN

De la investigación realizada se puede tomar las preguntas 1, 2 y 7 de la Encuesta aplicada al personal las cuales toman como principales características para la interpretación de la hipótesis; estas son, los ataques de Ingeniería Social, el conocimiento sobre los procedimientos a seguir en caso de ser víctimas de un ataque y sobre la divulgación de contraseñas entre compañeros.

Además se toma también la pregunta 9 de la Encuesta aplicada al Administrador del Sistema de Recursos Humanos en la cual se hace referencia a la seguridad informática existente dentro del Departamento de Recursos Humanos de la Universidad Técnica de Ambato cuyos resultados nos ayudan a defender la hipótesis de que las vulnerabilidades humanas en relación a la Seguridad Informática influyen en la fuga de información confidencial. Por lo cual podemos deducir que la hipótesis es afirmativa y se la acepta.

CAPITULO V

5. CONCLUSIONES Y RECOMENDACIONES

5.1.Conclusiones

- Existen pocas medidas de control para la afluencia de gente dentro del Departamento de Recursos Humanos lo que incrementa los niveles de vulnerabilidad al no existir procedimientos de control establecidos.
- El personal del departamento no está capacitado en cuanto a los ataques informáticos que pueden darse dentro del Departamento de Recursos Humanos de la Universidad Técnica de Ambato de los cuales podrían llegar a ser víctimas.
- Las contraseñas de seguridad dentro del departamento se comparten causando un riesgo elevado en el manejo de información crítica dentro del departamento pudiendo esta ser robada o plagiada.
- Tanto el departamento como su personal desconocen de los procesos de seguridad a seguir en caso de ataques informáticos.
- El departamento no cuenta con un documento guía con los procedimientos y medidas de prevención en contra de los ataques informáticos.

5.2. Recomendaciones

- Se recomienda implementar un sistema de control para el acceso de personas externas a la institución como: empresarios, estudiantes o público en general de la Universidad Técnica de Ambato.
- Se recomienda realizar un plan de capacitación en materia de Seguridad Informática poniendo énfasis en Ataques Informáticos enfocados en vulnerar al Factor Humano.
- Se recomienda aplicar normativas para la creación, utilización y divulgación de las contraseñas de seguridad utilizadas dentro del Departamento de Recursos Humanos de la Universidad Técnica de Ambato.
- Establecer los procesos de seguridad a seguir en caso de existir un ataque informático dentro del Departamento de Recursos Humanos de la Universidad Técnica de Ambato a través de la publicación y difusión de la documentación correcta.
- Crear un manual con normas, políticas y contramedidas enfocadas en la Seguridad Informática referente a las vulnerabilidades humanas principalmente en los ataques informáticos de Ingeniería Social.

CAPITULO VI

6. PROPUESTA

6.1. DATOS INFORMATIVOS

- **Título**

Manual de Políticas, Procedimientos y Contramedidas de Seguridad Informática referentes a las Vulnerabilidades Humanas.

- **Institución**

Departamento de Recursos Humanos de la Universidad Técnica de Ambato

- **Beneficiarios**

Personal del Departamento de Recursos Humanos de la Universidad Técnica de Ambato

- **Ubicación**

Avenida Chile y Colombia

- **Tiempo Estimado para la Ejecución**

1. Fecha Estimada de Inicio: Enero 2012
2. Fecha de Finalización: Noviembre 2012

- **Equipos Técnico Responsable**

1. Investigador: María Gabriela Cortez Pinto
2. Director RRHH: Dr. Carlos Fuentes
3. Director RRHH: Ing. Mauricio Molina

6.2.Antecedentes de la Propuesta

De la investigación realizada previamente se desprende que las vulnerabilidades humanas en relación a la Seguridad Informática representa una amenaza muy grande para la información del departamento de Recursos Humanos de la Universidad Técnica de Ambato, por el desconocimiento de estas vulnerabilidades, las cuales representan un tipo de ataque informático.

Adicionalmente la poca preocupación hacia la importancia de la confidencialidad de la información conlleva un alto riesgo a la estabilidad de la información del departamento. Debido al gran avance de la tecnología sus métodos de seguridad de la información son incompletos; además de no poseer muy claros los procesos de seguridad para mantener fiable la información y la integridad del entorno.

El Departamento de Recursos Humanos de la UTA dispone de grandes cantidades de información que implican directamente a todo el personal docente y administrativo de la institución.

Para salvaguardar la información del Departamento de Recursos Humanos de la Universidad Técnica de Ambato, se observó la necesidad de proporcionar al factor humano de este departamento una guía que les ayude a identificar y minimizar la vulnerabilidad del factor humano; de este modo se puede evitar ataques informáticos que vulneren la información mediante la utilización de técnicas aplicadas de dentro de la Ingeniería Social.

6.3.JUSTIFICACIÓN

El desarrollo de la siguiente propuesta se lo ha realizado debido al interés y a la vez la preocupación del personal del Departamento de Recursos Humanos de la Universidad Técnica de Ambato para mejorar sus conocimientos sobre cuáles son los riesgos, las normas, las políticas necesarias, las medidas preventivas y los procedimientos a seguir para mantener la seguridad de la información evitando su fuga y minimizar las vulnerabilidades humanas existentes dentro del departamento de la UTA.

Un manual de políticas, procedimientos y contramedidas para la Seguridad Informática es un elemento necesario para establecer medidas de control y preventivas contra los Ataques Informáticos referentes a las vulnerabilidades humanas del Departamento de Recursos Humanos; así como también establecer los procesos a seguir para poder llevar a cabo los controles necesarios para la prevención.

Además la propuesta ayudará en varios aspectos al personal del departamento como:

- **Identificación de los ataques informáticos referentes a la vulnerabilidad Humana:** Es un punto de interés debido a que se trata de dar a conocer los tipos de amenazas en los diversos elementos vulnerables con la interacción con las personas, medios electrónicos o interacción física.

- **Conocimiento de Información Pública y Confidencial:** Establecer medios de identificación de la información que puede considerarse pública y la que debe considerarse confidencial.

- **Capacitación de Medidas de Seguridad:** Asegurar que las medidas de prevención sean conocidas por el personal del departamento de Recursos Humanos de la Universidad Técnica de Ambato.

Con la creación del manual se consigue un documento de guía contra los ataques informáticos referentes a la vulnerabilidad humana, informando sobre los controles, procesos a seguir para varios eventos de amenaza y medidas preventivas. Debido a que estos ataques son muy difíciles de detectar lo más recomendable es utilizar un documento guía, en el cual se establezca los lineamientos y pautas necesarios para minimizar la vulnerabilidad humana y evitar de este modo la fuga de información.

6.4. OBJETIVOS

6.4.1. Objetivos General

Generar un Manual de Políticas, Procedimientos y Contramedidas de Seguridad Informática enfocado hacia los ataques informáticos que vulneran al Factor Humano; con políticas, procedimientos y medidas de prevención que permitan disminuir la fuga de información confidencial del departamento de Recursos Humanos de la Universidad Técnica de Ambato.

6.4.2. Objetivos Específicos

- Identificar la existencia de las amenazas dentro del Departamento de Recursos Humanos de la Universidad Técnica de Ambato.
- Identificar las principales vulnerabilidades.
- Analizar los riesgos e impacto de las amenazas.
- Establecer las políticas, procedimientos y medidas preventivas

6.5. ANÁLISIS DE FACTIBILIDAD

Dentro del ámbito de la política es viable realizar el proyecto ya que se debe asegurar la información de las instituciones públicas y mucho más de la información del departamento de Recursos Humanos debido a que la universidad es calificada como una universidad Clase "A" y debe contar con los manuales adecuados de seguridad y prevención.

Dentro del ámbito Socio-cultural el proyecto es viable debido a que ayudará al personal del departamento de Recursos Humanos de la Universidad Técnica de Ambato a capacitarse sobre los ataques informáticos.

En el ámbito tecnológico el proyecto es viable debido a que el investigador dispone de la tecnología necesaria para realizar el proyecto, así como las herramientas informáticas necesarias para poder brindar una solución correctiva y medidas de prevención adecuadas.

Dentro del ámbito organizacional es viable porque ayudará al departamento a implementar seguridades respecto a la información; salvaguardando la integridad de los datos tanto del departamento de Recursos Humanos como de la Universidad Técnica de Ambato en general.

El proyecto es viable en cuanto a equidad de género debido a que el manual permitirá que tanto el personal masculino como femenino se capacite y ponga en funcionamiento las medidas de seguridad dentro del departamento de Recursos Humanos de la Universidad Técnica de Ambato.

Dentro del ámbito ambiental el proyecto es viable debido a que no dañará al medio ambiente conservando la naturaleza y la biodiversidad del estado ecuatoriano.

Dentro del ámbito Económico-Financiero es viable porque el departamento cuenta con los medios económicos y financieros necesarios para la realización del proyecto.

Dentro del ámbito legal es viable debido a que el estado ecuatoriano garantiza que la información de las instituciones públicas ecuatorianas posea las seguridades necesarias para salvaguardar la integridad de la institución misma y la confidencialidad de los actos que dentro de ella se producen.

6.6. FUNDAMENTACIÓN TEÓRICA

Dentro del proceso de generación de un documento que contenga los controles necesarios y más óptimos de los procesos hay que considerar lo siguiente:

6.6.1. Manual

Un manual es según Anónimo (Internet; desconocido; 04/02/2012; 9:57 am) "Instrumento administrativo que contiene en forma explícita, ordenada y sistemática información sobre objetivos, políticas, atribuciones, organización y procedimientos de los órganos de una institución; así como las instrucciones o acuerdos que se consideren necesarios para la ejecución del trabajo asignado al personal, teniendo como marco de referencia los objetivos de la institución".

Mediante este concepto podemos afirmar que un manual es la herramienta necesaria con la cuentan las empresas para poder ejecutar sus labores, y ejecutar las políticas, para complementar sus funciones y satisfacer los requerimientos que la institución requiere de una unidad de la institución.

6.6.2. Manual De Políticas

Según Anónimo (Internet, Desconocido; 09/03/2012; 11:01 am) un manual de políticas es un "Documento que incluye las intenciones o acciones generales de la administración que es probable que se presenten en determinadas circunstancias. Las políticas son la actitud de la administración superior".

Según MARTÍNEZ, Cristina (Internet, 26/11/2006; 09/03/2012; 11:14 am) Un manual de políticas que posee todas las acciones generales que pueden presentarse en determinadas circunstancias.

Determinando que un manual de políticas posee las guías necesarias para la toma de acciones generales en caso de que exista una acción determinada ayudará a identificar cada uno de los responsables en los procesos de las acciones.

6.6.3. Importancia del Manual de Políticas

Según MARTÍNEZ, Cristina (Internet, 26/11/2006; 12:13 am) "Su importancia radica en que representa un recurso técnico para ayudar a la orientación del personal y también ayuda a declarar políticas y procedimientos, o proporcionar soluciones rápidas a los malos entendimientos y a mostrar cómo puede contribuir el empleado al logro de los objetivos del organismo. También ayuda a los administradores a no repetir la información o instrucciones".

6.6.4. Tipos de Manuales de Políticas

Según MARTÍNEZ, Cristina (Internet, 26/11/2006; 12:13 am) los manuales de políticas se dividen en:

1. Manuales Generales de Políticas:

Abarcan todo el organismo social, incluye como elemento primario todas aquellas disposiciones generales como tipo fijo, las cuales en forma unilateral las establece cada área a efectos de sus propias responsabilidades y autoridad funcional.

2. Manuales específicos de Políticas:

Se ocupan de una función operacional, un departamento o sección en particular.

Debido al enfoque del manual y que este está netamente enfocado al Departamento de Recursos Humanos de la Universidad Técnica de Ambato se lo identificará como un manual específico de políticas.

6.6.5. Manual De Políticas y Procedimientos

Según LOUMAR (Internet, 2008; 09/03/2012; 2:29 pm) Un manual de políticas y procedimientos es un documento enfocado a dar a conocer, a todo el personal, las políticas de la empresa, así como las instrucciones a detalle, de los pasos a seguir en la ejecución de un trabajo, para canalizar la estrategia administrativa hacia las metas de la empresa, utilizando como apoyo los diagramas de flujo y formatos para la aclaración de información.

Según ÁLVAREZ, Martín (Internet, 2006; 09/03/2012; 2:34 pm) "Un manual de políticas y procedimientos es un manual que documenta la tecnología que se utiliza dentro de un área, departamento, dirección, gerencia u organización.

La elaboración de manuales de políticas y procedimientos implica en primer lugar definir las funciones y responsabilidades de cada una de las áreas que conforman la organización".

6.6.6. Contenido Típico de los Manuales de Políticas y Procedimientos

Según ÁLVAREZ, Martín (Internet, 2006; 09/03/2012; 2:43 pm) Un manual de políticas y procedimientos estándar posee los siguientes elementos:

Portada
Índice

I. Hoja de Autorización del Área
II. Política de Calidad (cuando sea aplicable)
III. Objetivos del Manual
IV. Bitácora de Revisiones y Modificaciones a políticas y procedimientos
V. Políticas
VI. Procedimientos
VII. Formatos
VIII. Anexos

Cada área autorizada debe poseer un manual de políticas y procedimientos.

6.6.7. Procesos

Según el concepto de WIKIPEDIA, un proceso puede entenderse como una secuencia de acciones a ejecutarse con un conjunto de recursos.

En concordancia con este concepto podemos asegurar que un proceso en un conjunto de actividades y complementadas con elementos tanto internos como externos los cuales se encuentran organizados o a la vez en coordinación para que se ejecuten bajo ciertos parámetros o sucesos para poder alcanzar un fin determinado y previamente establecido.

6.6.8. Tipos de Procesos

Según DÍAZ MONTENEGRO QUESNEL, Silvia los procesos se identifican en los siguientes:

6.6.8.1.Procesos Sincrónicos

Definición

Se trata de aquellos procesos que establecen un diálogo síncrono con su contrapartida, sea éste un servidor, un Web Service externo o cualquier otra transacción, externa o interna.

Ventajas

Este tipo de procesos conocen al instante el resultado de las acciones que se lleven a cabo, optimizando la posibilidad de la contrapartida de contestar o llevar a cabo una acción.

6.6.8.2.Procesos Colaborativos

Definición

Se trata de aquellos procesos en los cuales existe la participación de un tercero que tiene que llevar a cabo una tarea en nuestro proceso. Esta tarea se reflejará en una aportación de información o el lanzamiento de otro proceso dentro o fuera del ámbito de nuestro sistema.

En mucha medida, la identificación de un proceso colaborativo dependerá del tiempo de respuesta del intercambio de información. Es decir, si se trata de un proceso que utiliza capacidades externas mediante mecanismos on-line, como un web service por ejemplo, se puede obviar el hecho de que realmente parte del proceso ocurra fuera, porque al no añadir ninguna dificultad de gestión, el error o retraso es más una característica técnica que otra cosa. El proceso colaborativo es aquel en que la responsabilidad sobre errores y retrasos es más bien funcional y donde el tiempo de intercambio es perceptible.

Es de señalar también que los procesos colaborativos dan en realidad lugar a dos etapas:

- Una etapa previa al envío de la información, donde se encuentran los expedientes pendientes de tratamiento
- Una etapa pendiente de respuesta, donde se encuentran los expedientes enviados pendientes de recibir la respuesta del tratamiento. Metodología de definición de procesos.

6.6.8.3.Procesos en tiempo-real

Definición

Se trata de los procesos que ejecutan tareas para cada uno de los expedientes de forma individual. Entran en esta categoría, al menos, todas las transacciones hechas para seres humanos, aunque puedan disparar después acciones masivas.

Ventajas

En este tipo de procesos, se conoce en tiempo real el resultado de las acciones que se lleven a cabo, acortando el tiempo de toma de decisiones.

6.6.8.4.Procesos por lotes

Definición

Se trata de los procesos que ejecutan unas tareas de forma masiva. Esto quiere decir que seleccionarán todos los expedientes para los cuales hay que hacer una determinada tarea y la harán en bloque para todos ellos.

Ventajas

Este tipo de procesos permite utilizar los recursos físicos de computación de forma intensa, sin necesidad de atender a otros procesos más allá del bloqueo de los recursos que se estén tratando en cada momento.

6.6.9. Diagramas de Procesos

Según WIKIPEDIA, "El **diagrama de flujo** o **diagrama de actividades** es la representación gráfica del algoritmo o proceso. Se utiliza en disciplinas como programación, economía, procesos industriales y psicología cognitiva."

Según CALDERÓN UMAÑA, Silvia y ORTEGA VINDAS Jorge "Los diagramas de flujo también conocidos como flujogramas son una representación gráfica mediante la cual se representan las distintas operaciones de que se compone un procedimiento o parte de él, estableciendo su secuencia cronológica. Clasificándolos mediante símbolos según la naturaleza de cada cual".

Según los conceptos se puede concluir entonces que los diagramas de procesos o también conocidos como **Diagramas de Flujo o Flujogramas** son una herramienta técnica para la descripción de los procesos, en la cual se establece el orden o secuencia de las actividades según la naturaleza de acción de cada una de ellas.

6.6.10. Encabezado del Diagrama de Flujo

Según CALDERÓN UMAÑA, Silvia y ORTEGA VINDAS, Jorge se deben seguir las siguientes recomendaciones para establecer el encabezado de los diagramas de flujo:

- Nombre de la institución.
- Título, o sea diagrama de flujo.
- Denominación del proceso o procedimiento.
- Denominación del sector responsable del procedimiento.
- Fecha de elaboración.
- Nombre del analista que realizó el trabajo.
- Nombres y abreviaturas de los documentos utilizados en el proceso o
- procedimiento y de los responsables.
- Simbología utilizada y su significado

Para la elaboración de los diagramas de flujo se incluirán en cada uno de los diagramas los siguientes puntos:

- Nombre de la Universidad
- Nombre de la Facultad
- Nombre del Departamento
- Sello de la Universidad y la Facultad
- Título del Diagrama de Flujo
- Denominación del Proceso
- Denominación del Responsable
- Fecha de elaboración
- Nombre del Investigador

6.6.11. Estructura del diagrama de flujo

Según CALDERÓN UMAÑA, Silvia y ORTEGA VINDAS, Jorge se deben seguir las siguientes recomendaciones para la estructura de los diagramas de flujo:

- Debe de indicarse claramente dónde inicia y dónde termina el diagrama.
- Las líneas deben ser verticales u horizontales, nunca diagonales.
- No cruzar las líneas de flujo empleando los conectores adecuados sin hacer uso excesivo de ellos.
- No fraccionar el diagrama con el uso excesivo de conectores.
- Solo debe llegar una sola línea de flujo a un símbolo. Pero pueden llegar muchas líneas de flujo a otras líneas.
- Las líneas de flujo deben de entrar a un símbolo por la parte superior y/o izquierda y salir de él por la parte inferior y/o derecha.
- En el caso de que el diagrama sobrepase una página, enumerar y emplear los conectores correspondientes.
- Todo texto escrito dentro de un símbolo debe ser legible, preciso, evitando el uso de muchas palabras.
- Todos los símbolos tienen una línea de entrada y una de salida, a excepción del símbolo inicial y final.
- Solo los símbolos de decisión pueden y deben tener más de una línea de flujo de salida.
- Cada casilla de actividad debe indicar un responsable de ejecución de dicha actividad.
- Cada flecha representa el flujo de una información.

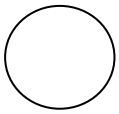
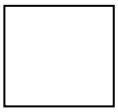
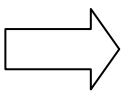
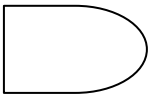
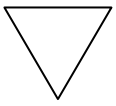
6.6.12. Símbolos usados en los diagramas de flujo

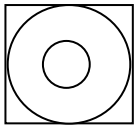
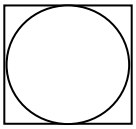
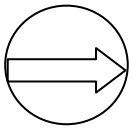
Según ÁLVAREZ, Martín (Internet, 2006; 09/03/2012; 2:34 pm) Se poseen varios estándares de diagramación los cuales están diseñados por las instituciones:

La American Society of Mechanical Engineers (ASME)

Ha desarrollado los símbolos de la Tabla N° 6.1 los cuales, a pesar de que son aceptados en áreas de producción se emplean con poca frecuencia en trabajo de diagramación administrativa, sin embargo su uso administrativo contribuye de acuerdo al manejo e interpretación que se dé en la diagramación.

Tabla N° 6.1. Símbolos de la Norma American Society of Mechanical Engineers (ASME)

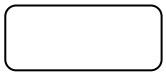
SIMPLES	
SÍMBOLO	**REPRESENTACIÓN**
	**Proceso**.-Indica las principales fases del proceso, método o procedimiento
	**Inspección**.- Indica que se verifica la cantidad y/o calidad de algo.
	**Transporte O Desplazamiento**.- Indica el movimiento de los empleados, material y equipo de un lugar a otro.
	**Deposito Provisional O Espera**.- Indica demora en el desarrollo de los hechos.
	**Almacenamiento Permanente**.- Indica el depósito de algún documento dentro de un archivo o de un objeto cualquiera en un almacén.

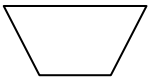
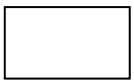
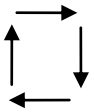
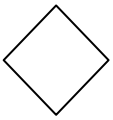
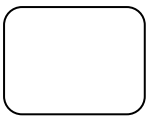
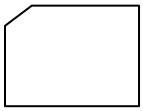
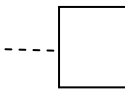
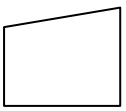
COMBINADOS	
	**Origen De Una Forma O Documento**.- Indica el hecho de elaborar una forma o producir un informe
	**Decisión O Autorización De Un Documento**.- Representa el acto de tomar una decisión o bien el momento de efectuar una autorización.
	**Entrevista**.- Indica el desarrollo de una entrevista entre dos o más personas.
	**Destrucción De Documento**.- Indica el hecho de destruir un documento o parte de él, o bien la existencia de un archivo muerto.

La American National Standard Institute (ANSI)

Ha preparado una simbología para presentar los flujos de información del procesamiento electrónico de datos Tabla N° 6.2, de la cual se emplean algunos símbolos para diagramas de flujo administrativos Tabla N° 6.3.

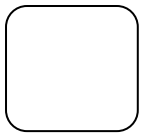
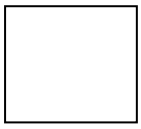
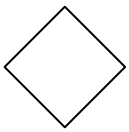
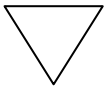
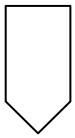
Tabla 6.2. Símbolos de la American National Standard Institute (ANSI)

SÍMBOLO	REPRESENTACIÓN	SÍMBOLO	REPRESENTACIÓN
	**Terminal**.- Indica el inicio o la terminación del flujo. Puede ser acción o lugar, además se usa para indicar una unidad administrativa.		**Conector**.- Representa una conexión de una parte del diagrama de flujo con otra parte lejana del mismo.

	**Disparador**.- Indica el inicio de un procedimiento, contenido de este o el nombre de una unidad administrativa donde se da inicio.		**Conector De Pagina**.- Representa una conexión o enlace con otra hoja diferente, en la que continua el diagrama de flujo.
	**Operación**.- Representa la realización de una operación o actividad relativa a un procedimiento.		**Dirección del Flujo o Líneas de Unión**.- Conecta los símbolos señalando el orden en que se deben realizar las distintas operaciones.
	**Decisión o Alternativa**.- Indica un punto dentro del flujo en que son posibles varios caminos.	* 	**Operación con Teclado.-** Representa una acción en que se utilizan una perforadora o verificadora de tarjeta.
	**Documento**.- Representa cualquier documento que entre, se utilice, se genere o salga del procedimiento	* 	**Tarjeta Perforada**.- Representa cualquier tipo de tarjeta perforada que se utilice en el procedimiento.
	**Nota Aclaratoria**.- No forma parte del diagrama de flujo sino más bien es un elemento que se adiciona a una operación o actividad para dar una explicación de ella.	* 	**Cinta Magnética**.- Representa cualquier tipo de cinta magnética que se utilice en el Procedimiento.
	**Línea De Comunicación**.- Representa la transmisión de información de un lugar a otro mediante líneas telefónicas, de radio, etc.	* 	**Teclado en línea**.- Representa el uso de un dispositivo en línea para proporcionar información a una computadora electrónica u obtenerla de ella.

Nota: los símbolos * son utilizados en combinación con el resto.

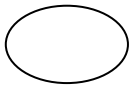
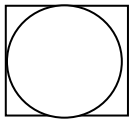
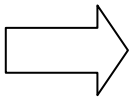
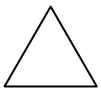
Tabla 6.3. Símbolos de la Norma ANSI para elaborar diagramas de flujo (diagramación administrativa)

SÍMBOLO	REPRESENTACIÓN
	**Inicio o Término**.- indica el principio o el fin del flujo. Puede ser acción o lugar, además, se usa para indicar una oportunidad administrativa o persona quien recibe o proporciona información.
	**Actividad**.- describe las funciones que desempeña las personas involucradas en el procedimiento.
	**Documento**.- representa cualquier documento que entre, se utilice, se genere o salga del procedimiento.
	**Decisión o alternativa**.- indica un punto dentro del flujo en donde se debe tomar una decisión entre dos o más opciones.
	**Archivo**.- indica que se guarde un documento en forma temporal o permanente.
	**Conector de página**.- representa una conexión o enlace con otra hoja diferente, en la que continua el diagrama de flujo.
	**Conector**.- representa una conexión o enlace de una parte del diagrama de flujo con otra parte del mismo.

La Organización Internacional de Estandarización (ISO)

Ha elaborado una simbología para apoyar la garantía de calidad a consumidores y clientes de acuerdo con las normas ISO-9000:2000 Tabla 6.4.

Tabla 6.4. Símbolos de la norma ISO-9000 para elaborar diagramas de flujo.

SÍMBOLO	REPRESENTACIÓN
	**Operación.-** fases del proceso, método o procedimiento
	**Inspección y medición.-** representa el hecho de verificar o supervisar la naturaleza, calidad y cantidad de los insumos y productos
	**Operación e Inspección.-** indica la verificación o supervisión durante las fases del proceso, método o procedimiento de sus componentes
	**Transportación.-** indica el movimiento de personas, material o equipo.
	**Demora.-** Indica retraso en el desarrollo del proceso, método, o procedimiento.
	**Entrada de Bienes.-** Productos o material que ingresa al proceso
	**Almacenamiento.-** Depósito y/o resguardo de información o productos.

6.7. METODOLOGÍA

Lo que se busca con una guía de metodología es prolijidad, control y corrección en cada etapa de desarrollo de un manual con debida identificación de los riesgos tecnológicos, lo que permitirá de forma sistemática poder obtener un producto correcto con los procedimientos y políticas adecuadas para asegurar la información confidencial; así como también, describir en forma escrita y acertada los procesos de seguridad que se deben realizar antes, durante y después de efectuarse un ataque informático.

Para ello es necesario identificar los procesos, procedimientos y políticas que los planes de seguridad ayudarán a efectuar.

El proceso de este manual lleva consigo la responsabilidad operativa y física de la información que se maneja dentro del departamento. Y los procesos para poder llevar a cabo estas acciones de seguridad para proteger la integridad de las acciones y la información; manteniendo la confidencial y disponibilidad de la misma solo para los usuarios autorizados a ella.

La metodología a usar para la generación del manual y la valoración de las vulnerabilidades, será la estructura básica de la metodología de Magerit y Pilar para la valoración de los riesgos y el impacto de una amenaza al factor humano de las tecnologías de la información de una empresa.

6.7.1. Etapas y Pasos de la metodología de MAGERIT

El siguiente resumen esta tomado de los libros digitales de AMUTIO GÓMEZ, Miguel Ángel de los Tomos I, II y III de Magerit v.3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información en versiones pdf:

El esquema completo de Etapas, Actividades y Tareas del Submodelo de Procesos de MAGERIT es el siguiente:

Etapa 1. Planificación del Análisis y Gestión de Riesgos

- Actividad 1.1. Oportunidad de Realización
- Actividad 1.2. Definición de Dominio y Objetivos
- Actividad 1.3. Planificación del Proyecto
- Actividad 1.4. Lanzamiento del Proyecto

Etapa 2. Análisis de Riesgos

- Actividad 2.1. Recogida de Información
- Actividad 2.2. Identificación y Agrupación de Activos
- Actividad 2.3. Identificación y Evaluación de Amenazas
- Actividad 2.4. Identificación y Estimación de Vulnerabilidades
- Actividad 2.5. Identificación y Valoración de Impactos
- Actividad 2.6. Evaluación del Riesgo

Etapa 3. Gestión del Riesgo

Actividad 3.1. Interpretación del Riesgo

Actividad 3.2. Identificación y Estimación de Funciones de salvaguarda

Actividad 3.3. Selección de Funciones de Salvaguarda

Actividad 3.4. Cumplimiento de Objetivos

Etapa 4. Selección de Salvaguardas

Actividad 4.1. Identificación de mecanismos de salvaguarda

Actividad 4.2. Selección de mecanismos de salvaguarda

Actividad 4.3. Especificación de los mecanismos a implantar

Actividad 4.4. Planificación de la Implantación

Actividad 4.5. Integración de resultados

Paso I: Identificación de Activos

Activos

Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos. [UNE 71504:2008]

Valoración cualitativa

Las escalas cualitativas permiten avanzar con rapidez, posicionando el valor de cada activo en un orden relativo respecto de los demás. Es frecuente plantear estas escalas como órdenes de magnitud‖ y, en consecuencia, derivar estimaciones del orden de magnitud del riesgo.

La limitación de las valoraciones cualitativas es que no permiten comparar valores más allá de su orden relativo. No se pueden sumar valores.

Paso II: Amenazas

Consiste en determinar las amenazas que pueden afectar a cada activo. Las amenazas son "cosas que ocurren". Y, de todo lo que puede ocurrir, interesa lo que puede pasarle a nuestros activos y causar un daño.

Amenaza
Causa potencial de un incidente que puede causar daños a un sistema de información o a una organización. [UNE 71504:2008]

Valoración de las amenazas

Cuando un activo es víctima de una amenaza, no se ve afectado en todas sus dimensiones, ni en la misma cuantía.

Una vez determinado que una amenaza puede perjudicar a un activo, hay que valorar su influencia en el valor del activo, en dos sentidos:

- **Degradación:** cuán perjudicado resultaría el [valor del] activo
- **Probabilidad:** cuán probable o improbable es que se materialice la amenaza

MA	Muy alta	Casi seguro	Fácil
A	Alta	Muy alto	Medio
M	Media	Posible	Difícil
B	Baja	Poco probable	Muy difícil
MB	Muy baja	Muy raro	Extremadamente difícil

Tabla 6.5. Clasificación de las amenazas

Paso III: Determinación del impacto potencial

Se denomina impacto a la medida del daño sobre el activo derivado de la materialización de una amenaza. Conociendo el valor de los activos (en varias dimensiones) y la degradación que causan las amenazas, es directo derivar el impacto que estas tendrían sobre el sistema.

Paso IV: Riesgo Potencial

Se denomina riesgo a la medida del daño probable sobre un sistema. Conociendo el impacto de las amenazas sobre los activos, es directo derivar el riesgo sin más que tener en cuenta la probabilidad de ocurrencia.

El riesgo crece con el impacto y con la probabilidad, pudiendo distinguirse una serie de zonas a tener en cuenta en el tratamiento del riesgo:

- Zona 1 – riesgos muy probables y de muy alto impacto.
- Zona 2 – cubre un amplio rango desde situaciones improbables y de impacto medio, hasta situaciones muy probables pero de impacto bajo o muy bajo.
- Zona 3 – riesgos improbables y de bajo impacto.
- Zona 4 – riesgos improbables pero de muy alto impacto.

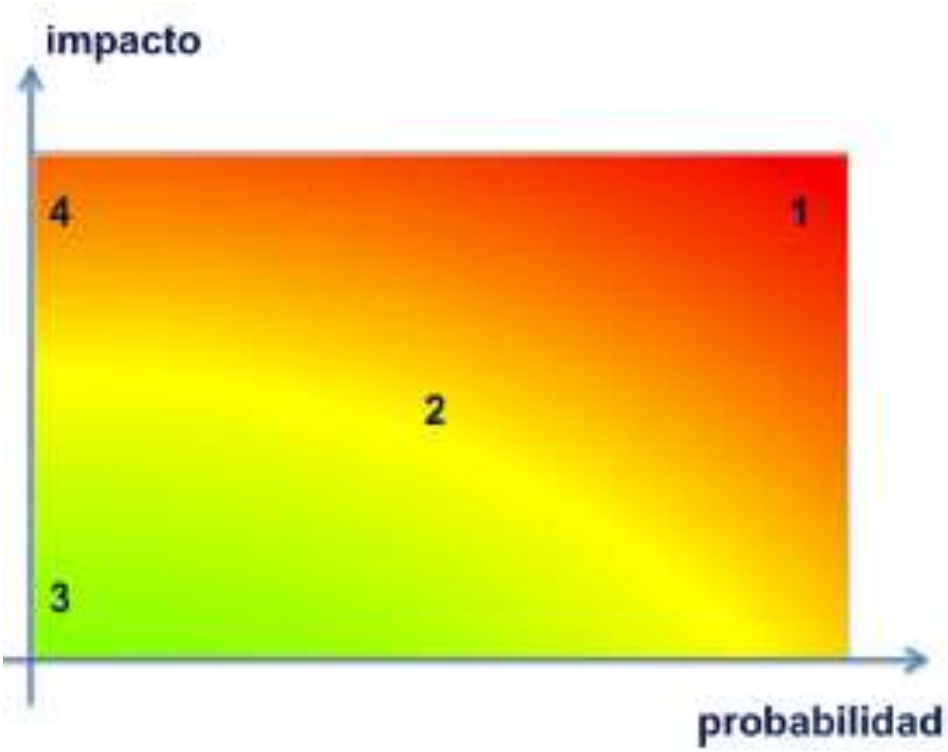


Gráfico6.1. El riesgo en función del impacto y la probabilidad

Para la aplicación de la metodología la medición del riesgo se la realizará por un rango de 1 a 4 y seguido por el color del fonograma de colores para no romper el esquema de colores.

Paso V: Salvaguardas

Se definen las salvaguardas o contra medidas como aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo. Hay amenazas que se conjuran simplemente organizándose adecuadamente, otras requieres elementos técnicos (programas o equipos), otras seguridades físicas y, por último, está la política de personal.

Debido a que la metodología abarca un estudio más profundizado del análisis de los riesgos de una empresa no se tomará en cuenta los temas a profundizar, únicamente se aplicarán estas 5 fases o pasos detallados en la metodología de Magerit.

6.7.1.1. Determinación de las fases de la metodología

Basándonos en la metodología de MAGERIT sus etapas y pasos; se establecen las siguientes fases a seguir para el desarrollo de la propuesta del presente proyecto de investigación:

FASE I – GENERALIDADES

- Introducción
- Alcance
- Objetivos
- Misión
- Visión
- Valores

FASE II – PLANIFICACIÓN DEL ANÁLISIS Y GESTIÓN DE RIESGOS

- Justificación del Proyecto

FASE III -ACTIVOS

- Determinación de Activos

FASE IV- AMENAZAS

- Identificación de las Amenazas

FASE V- VULNERABILIDADES

- Identificación de Vulnerabilidades
- Análisis de las Vulnerabilidades

FASE VI- IMPACTO Y RIESGO

- Análisis de Impacto y Riesgo

FASE VII- SALVAGUARDAS

- Identificación de Salvaguardas
- Generación de Salvaguardas

6.7.2. DESARROLLO DE LAS FASES DE LA METODOLOGÍA

FASE I – GENERALIDADES

6.7.2.1.Introducción

El presente manual posee instrumentos que ayudaran a informar al personal de una organización o área específica sobre las políticas, procedimientos y salvaguardas necesarios, a los cuales se encuentran sujetos y aplicarlos frente a los posibles escenarios existentes.

Las políticas, procedimientos y contramedidas de Seguridad Informática tienen por objeto establecer medidas técnicas, organizacionales y de prevención de la información, así como de las personas que interactúan haciendo uso de los servicios informáticos que provee el Departamento de Recursos Humanos de la Universidad Técnica de Ambato; y, ayudando a la capacitación del personal proporcionando información y contribuyendo con la función informática del Departamento.

Las políticas, están orientadas a establecer mecanismos de control de la confidencialidad de la información y a la vez a minimizar las vulnerabilidades humanas dentro de una dependencia.

El mecanismo adecuado para su difusión y publicación, son los manuales de seguridad, los cuales deben describir los objetivos, políticas, estructura organizacional, procesos, estrategias y contramedidas.

6.7.2.2.Alcance

El manual tendrá como principales componentes las políticas, procedimientos y contramedidas necesarios aplicables a las actividades que se desarrollarán dentro del Departamento de Recursos Humanos de la Universidad Técnica de Ambato para evitar y controlar un ataque enfocado al factor humano.

6.7.2.3.Objetivos

General:

- Establecer una normativa de Seguridad Informática orientada a minimizar los riesgos provocados por vulnerabilidades humanas dentro del Departamento de Recursos Humanos de la Universidad Técnica de Ambato.

Específicos:

- Proporcionar de información necesaria para poder generar una estrategia de seguridad Informática.
- Establecer las medidas para control que abarquen y se enfoquen netamente el mantener la seguridad de la información dentro del Departamento de Recursos humanos de la Universidad Técnica de Ambato

6.7.2.4. Misión del Departamento de RRHH de la Universidad Técnica de Ambato

Aplicar el Sistema Integrado de Desarrollo del Talento Humano motivando a los servidores universitarios para el mejoramiento continuo en la calidad de los productos y servicios que se ofrecen; satisfaciendo las expectativas y demandas de los usuarios internos y externos, en función a alcanzar los objetivos estratégicos institucionales.

6.7.2.5. Visión del Departamento de RRHH de la Universidad Técnica de Ambato

Lograr la Aplicación de un Sistema Integrado de Desarrollo del Talento Humano que propenda el crecimiento profesional, técnico y personal de las y los servidores universitarios para alcanzar un nivel de gestión institucional que se refleje en realizaciones trascendentes acordes al compromiso universitario frente a la colectividad.

FASE II -PLANIFICACIÓN DEL ANÁLISIS Y GESTIÓN DE RIESGOS

6.7.2.6.Justificación del Proyecto

La oportunidad de realización del proyecto se hace verdadera gracias a la necesidad de proveer la información para prevenir los ataques informáticos referentes a la vulnerabilidad humana en el Departamento de Recursos Humanos de la Universidad Técnica de Ambato y al apoyo del personal del mismo.

Se justifica el levantamiento de la información necesaria y la identificación de la evidencia necesaria para el detalle de la partida del proyecto tomando como base la información obtenida y descrita en el presente proyecto de investigación titulado **"Las Vulnerabilidades Humanas en relación a la Seguridad Informática para evitar la fuga de información confidencial en el Departamento de Recursos Humanos de la Universidad Técnica de Ambato"** en los Capítulos 1, 2, 3 y 4.

FASE III –ACTIVOS

6.7.2.7.Identificación de Activos

Para el proyecto de información se tomará únicamente los activos desprendidos de la Variable Dependiente Fuga de Información Confidencial, de la cual se toma la información como principal y único activo a proteger dentro de las salvaguardas correspondientes.

ACTIVO = INFORMACIÓN

FASE IV –AMENAZAS

6.7.2.8.Identificación de las Amenazas

Para la identificación de las amenazas se tomará como punto de partida las técnicas de la Ingeniería Social detalladas en el Marco Teórico del presente proyecto de Investigación clasificadas por el autor BISCIONE, Carlos.

El análisis de las amenazas se las realizará por medio de categorías de los dos tipos de técnicas detalladas. Para ello el investigador clasificará los tipos de ataques en Categorías.

La valoración de las amenazas se la realizará de forma cualitativa mediante la siguiente tabla:

MA	Muy alta
A	Alta
M	Media
B	Baja
MB	Muy baja

INVASIVAS O DIRECTAS O FÍSICAS

IDENTIFICACIÓN DE AMENAZAS EN LAS CATEGORÍAS DE LAS TÉCNICAS DE INGENIERÍA SOCIAL *Departamento de Recursos Humanos de la UTA.*					
No	**CATEGORÍA**	**ESCENARIOS**			
1	**EL TELÉFONO**	Llamadas de Negocios	Llamadas de Soporte	Divulgación De Información Personal	Divulgación de Información Institucional
VALORACIÓN DE LA AMENAZA		**MA**			
2	**EL SITIO DE TRABAJO**	Acceso físico no autorizado	Mirar sobre el hombro	Búsqueda en la Basura	Robar, fotografiar o copiar documentos
VALORACIÓN DE LA AMENAZA		**MA**			
3	**LA BASURA**	Destrucción de Documentos			
VALORACIÓN DE LA AMENAZA		**A**			
4	**LA INTRANET**	Repetición de Passwords		Divulgación de Contraseñas	
VALORACIÓN DE LA AMENAZA		**MA**			

Tabla 6.6. Identificación de Amenazas Técnicas Directas o Físicas

SEDUCTIVAS Y/O INADVERTIDAS

IDENTIFICACIÓN DE AMENAZASEN LAS CATEGORÍAS DE LAS TÉCNICAS DE INGENIERÍA SOCIAL *Departamento de Recursos Humanos de la UTA.*							
No	**CATEGORÍA**	**ESCENARIOS**					
1	**COMPORTAMIENTO HUMANO**	Autoridad	Carisma	Reciprocidad	Consistencia	Validación Social	Ingeniería Social Inversa
VALORACIÓN DE LA AMENAZA		**MA**					

Tabla 6.7. Identificación de Amenazas Seductivas y/o Inadvertidas

FASE V –VULNERABILIDADES

6.7.2.9.Identificación de Vulnerabilidades

La identificación de las vulnerabilidades se tomará de las categorías detalladas en el análisis de las amenazas, estas vulnerabilidades son:

- El Teléfono
- El Sitio de Trabajo
- La Basura
- La intranet
- Comportamiento Humano

6.7.2.10. Análisis de Vulnerabilidades

Para el análisis de las vulnerabilidades existentes dentro del Departamento de Recursos Humanos se tomará en cuenta los tipos de técnicas que se enfocan en la vulnerabilidad del factor humano, se usará como base para la determinación de las mismas la categorización realizada por el investigador.

La determinación de las vulnerabilidades se la realizará bajo una calificación de 1 y 0; en la cual, el 1 significa la existencia de la vulnerabilidad y 0 la inexistencia de la vulnerabilidad.

Para determinar la existencia de la vulnerabilidad se la comparará con las amenazas y los escenarios descritos en la FASE II de la Metodología de la Propuesta.

6.7.2.10.1. Con relación a la Investigación

En relación a la Investigación detallada en el Capítulo 4 del presente proyecto de investigación, se obtiene las siguientes vulnerabilidades:

TÉCNICA	VULNERABILIDAD EXISTENTE	N° PREGUNTA	APLICADA	EXISTENCIA
INVASIVAS O DIRECTAS O FÍSICAS				
EL TELÉFONO				
	Personificación Falsa y Persuasión	5	Personal	1
	Robo de Contraseñas o Claves de Acceso	7	Personal	1
EL SITIO DE TRABAJO				
	Acceso Físico No Autorizado	7 9	Personal Administrador	1
	Shoulder Surfing	X	X	0
	Robar, Fotografiar o copiar documentos	2	Personal	1
	Acceso a servidores	X	X	0
LA BASURA				
	Desecho de documentación sin previa destrucción	X	X	0
LA INTRANET				
	Repetición de Passwords	X	X	0
SEDUCTIVAS Y/O INADVERTIDAS				
	Carisma	8	Personal	1
	Reciprocidad	Todas	Personal Admin.	1
	Consistencia	X	X	0
	Ingeniería Social Inversa	X	X	0
VULNERABILIDADES ENCONTRADAS	**6**			

Tabla 6.8Determinación de Vulnerabilidades

Como se describe en la Tabla 6.8. Se hace visible mediante la investigación la existencia de 6 vulnerabilidades; debido a que mediante esta no se puede evidenciar completamente la existencia de algunas vulnerabilidades se realiza la aplicación de las técnicas para poder confirmar su existencia, tomando en cuenta el criterio del investigador y las posibilidades dentro del Departamento de Recursos Humanos de la Universidad Técnica de Ambato.

6.7.2.10.2. Cuadro de Evidencias de las vulnerabilidades y amenazas

Para poder verificar la existencia de algunas vulnerabilidades fue necesaria la aplicación de algunas de estas.
Por la delicadeza de la información obtenida en la información se realizará la identificación de los datos obtenidos de la siguiente manera:

X: Investigador
Y: Víctima
R: Información Delicada Personal
XXX: Información Confidencial

<u>TÉCNICA</u>: INVASIVAS O DIRECTAS O FÍSICAS

a) El Teléfono

Personificación Falsa y Persuasión

Para la obtención de información de esta técnica se realiza una llamada telefónica al Departamento de Recursos Humanos de la Universidad Técnica de Ambato de la cual se obtiene la información:

Duración de la llamada: 12 min - 34segundos

Desarrollo de la Técnica:

X: Muy Buenos días, Mi nombre es Anabela Santamaría (nombre ficticio), soy ejecutiva de Ventas del Banco XYZ; ¿con quién tengo el gusto?
Y: (La llamada es contestada por una persona del sexo femenino) Muy Buenos días soy **R**
X: Un gusto saludarla **R** estamos ofreciéndole un grupo de consumo con una tarjeta de crédito de la institución XYZ, podríamos conocer cuál es su situación actual con la tarjeta de crédito?
Y: Claro, en este yo ya posea una tarjeta de crédito
X: OK, entonces a usted le convendría adquirir nuestro nuevo grupo de consumo que posee algunas características como descuentos y acumulación de puntos, los cuales pueden ser canjeados por viajes al Caribe; además, este paquete es exclusivo únicamente para un grupo selecto de nuestros clientes, si usted desea podemos revisarle en nuestro sistema su posición actual para poder hacerse acreedora del grupo de consumo totalmente gratis. ¿Desea que le revisemos si usted pertenece a nuestro grupo selecto de clientes?
Y: ¿Cuáles serían los beneficios si en este caso yo constara en la lista?
X: Si en este caso usted pertenece a nuestro grupo selecto de clientes y desea adquirir el servicio, este sería totalmente gratuito y sería activado inmediatamente para poder acceder a descuentos de algunos almacenes afiliados los cuales serían enviados a su domicilio, para que usted conozca los lugares en los cuales posee ventajas por pertenecer y adquirir nuestro nuevo servicio.

Y: Me gustaría que me verifiquen por favor.

X: Con mucho gusto **R**, podría usted facilitarme sus datos personales y su número de tarjeta para confirmarla.

Y: (La persona proporciona) Nombres R, Apellidos R y finalmente su número de tarjeta XXX.

X: Lamento informarle **R** que no se encuentra en nuestra lista de nuestro mejores clientes pero si desea adquirir el servicio del grupo de consumo podemos activarlo, pero el mismo poseerá un costo inicial de $50 y mensualmente tendrá un costo de mantenimiento de $20; ¿desea adquirirlo?

Y: No muchas, gracias.

X: Mil gracias por su tiempo, que tenga un excelente día. Hasta luego.

Y: Hasta Luego.

b) Robo de Contraseñas:

Para obtener una contraseña se realiza la utilización de otras dos técnicas de Ingeniería Social el Carisma y Consistencia. Para la utilización de estas técnicas se utilizan los siguientes elementos:

Memoria Externa de Almacenamiento

Para la aplicación de esta técnica se requirió de 3 días de aplicación de las otras dos técnicas Carisma y Consistencia, para que las personas se acostumbren a la presencia del Investigador para establecer confianza y proceder con la aplicación de la técnica del robo de contraseña.

Desarrollo de la Técnica:

Se espera que **Y** se ausente de su lugar de trabajo, para lo cual se presenta una reunión de la cual requiere su presencia, para lo cual se genera una necesidad de exploración de un documento en un antivirus, para esto se solicita que se facilite la contraseña en la máquina y se puede visualizar perfectamente la misma **XXX** y se obtiene la contraseña de acceso a la máquina de **Y**, posteriormente **Y** se ausenta de su lugar de trabajo y **X** puede hacer uso de la máquina sin supervisión.

c) El Sitio de Trabajo

Acceso físico No Autorizado

Para la aplicación de esta técnica el investigador utiliza el Área de Acceso Restringido que existe dentro del Departamento de Recursos Humanos de la Universidad Técnica de Ambato, para lo cual se requiere previa autorización del Director de Recursos Humanos de la Universidad Técnica de Ambato.

Desarrollo de la Técnica:

Para la aplicación de esta técnica se ingresa a la Universidad Técnica de Ambato y seguidamente se ingresa al Área de Acceso Restringido sin obtener previa autorización del Director. Una vez dentro de la habitación se obtiene la siguiente conversación:

Y: Para poder ingresar a este cuarto se requiere de una autorización.
X: Ya se solicitó, la autorización para poder ingresar a esta área.
Y: ¿Bueno entonces dígame en que le puedo ayudar?.

Como se puede verificar no existe la verificación de la misma y cualquier persona puede ingresar al cuarto de Área Restringida.

Robar, Fotografiar o copiar documentos

Para la aplicación de esta técnica se procedió con la fotografía de documentos con la cámara del celular.

Desarrollo de la Técnica:

Se procede a fotografiar documentos, los cuales son identificados como contrato de un docente de la Universidad Técnica de Ambato:

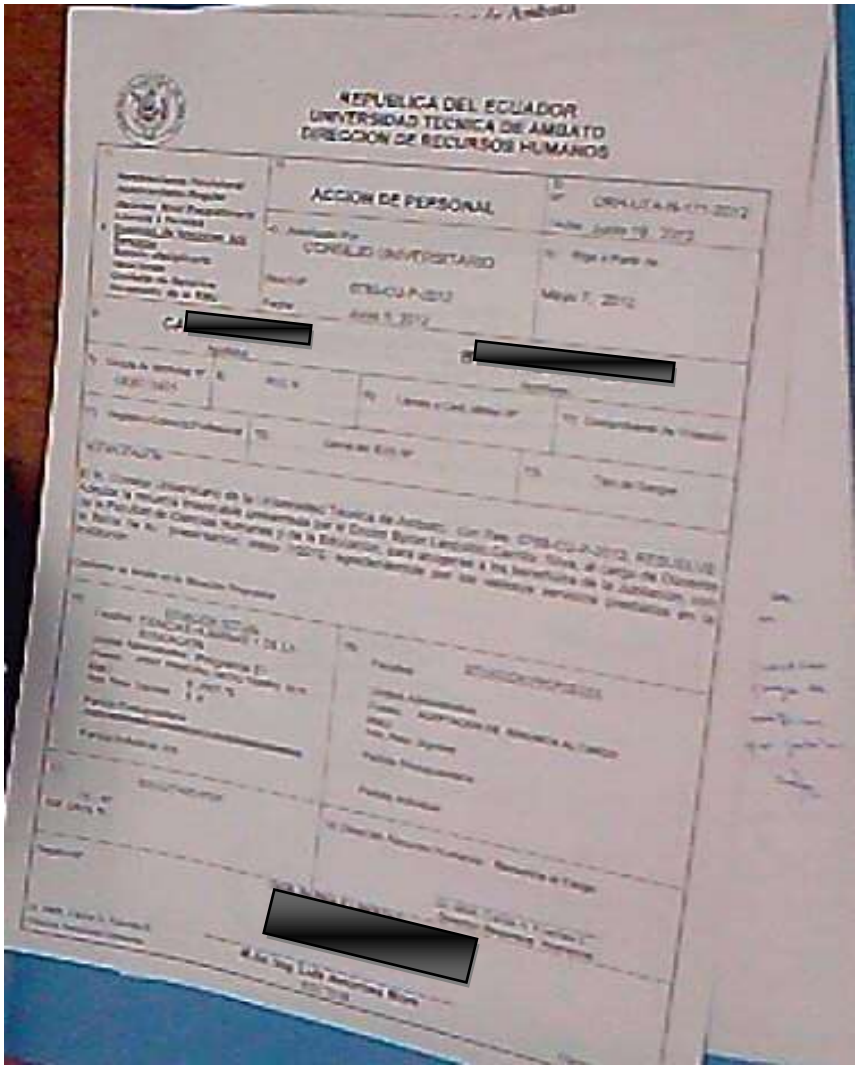


Gráfico 6.2. Evidencia Contrato de Personal

Gráfico 6.3. Evidencia Archivo de Documentos

Gráfico 6.4. Evidencia de Documentos importantes a la vista

Por seguridad se protegen nombres visibles en los documentos de evidencia.

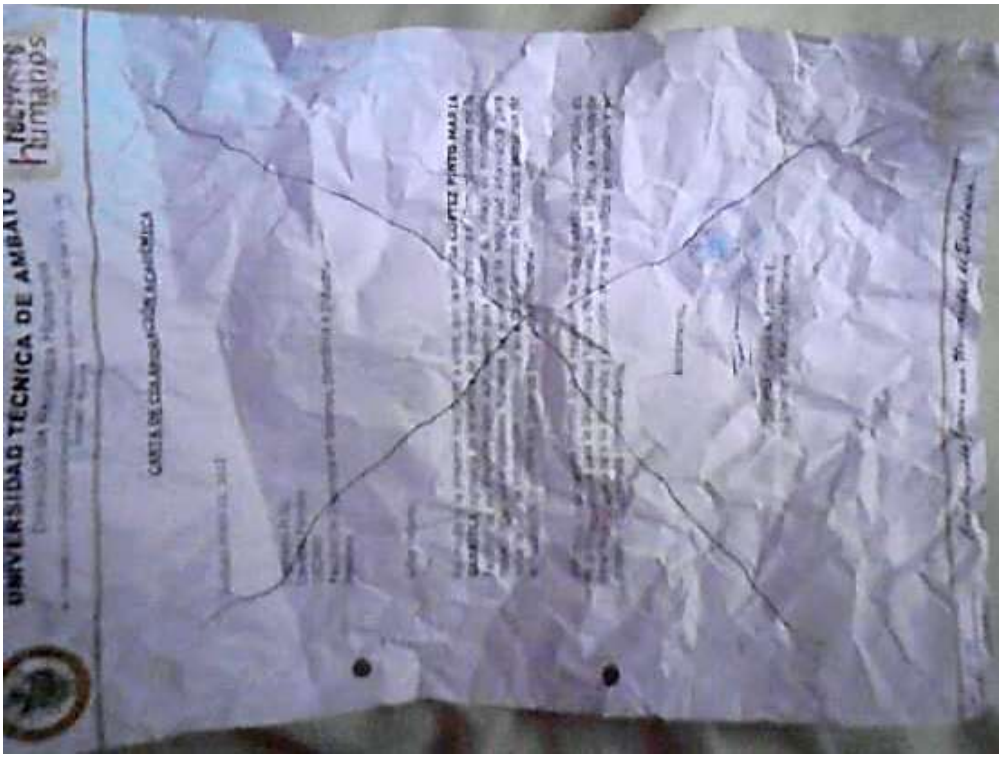
d) La Basura

Desecho de Documentación sin previa destrucción

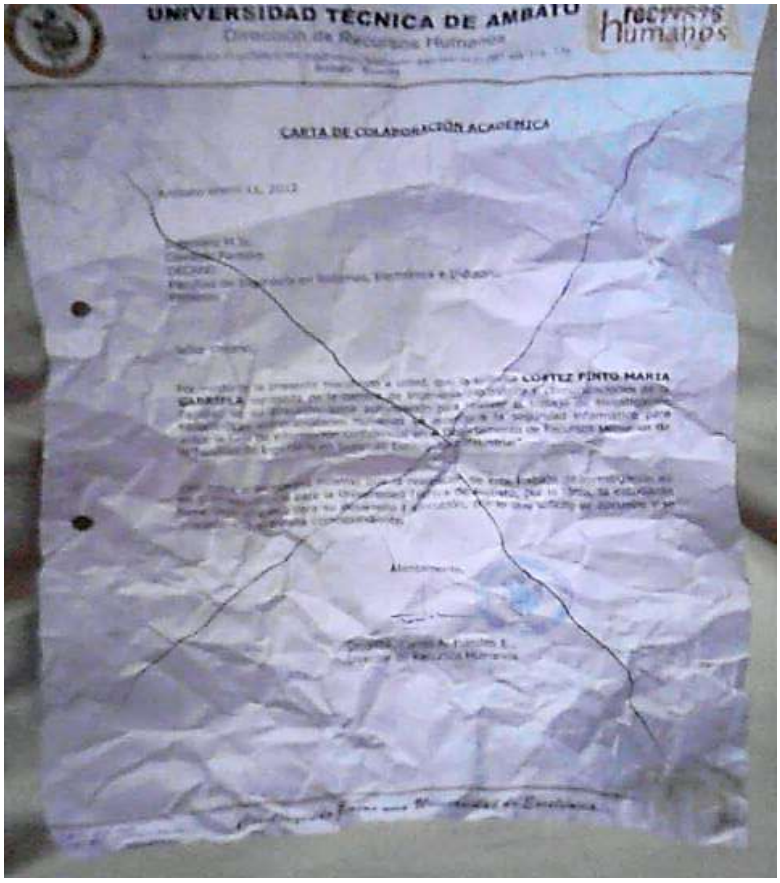
Para la aplicación de esta técnica se sustrae una hoja de una certificación de empleo que posee errores en el nombre de la persona y se la deposita en el recipiente de desechos.
Se fotografía el documento para constancia.

Desarrollo de la Técnica:

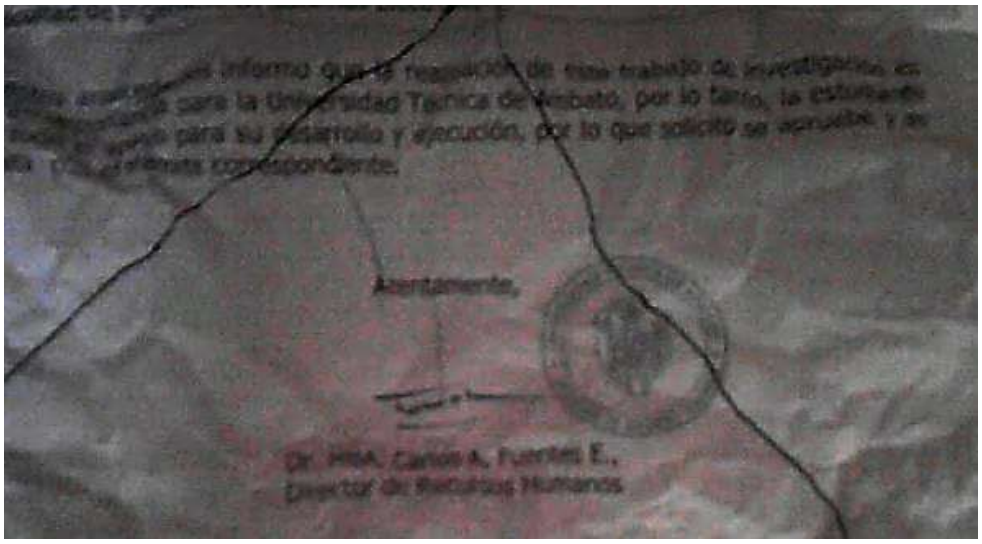
Se arroja una moneda de un centavo al basurero por error y se solicita que por favor se de acceso al recipiente de la basura para poder recogerla. De esta manera se obtiene el documento de evidencia.



Gráfica 6.5. Documento recolectado de Basura 1



Gráfica 6.6. Documento recolectado de Basura 1



Gráfica 6.7. Documento recolectado de Basura 1

e) La Intranet

Para obtener evidencia de la existencia de vulnerabilidad no es necesario aplicar ninguna técnica debido a que en la encuesta aplicada al Personal del Departamento de Recursos Humanos de la Universidad Técnica de Ambato se obtiene en la pregunta N° 7 ¿Ha compartido alguna vez su contraseña con alguna persona de confianza?; se obtuvo un resultado con una respuesta afirmativa del 36% que compartió alguna vez su contraseña lo cual afirma la existencia de esta vulnerabilidad.

SEDUCTIVAS Y/O INADVERTIDAS

a) Carisma, Reciprocidad, Consistencia, Validación Social

La aplicación de estas técnicas se las realizó en acompañamiento de algunas otras técnicas para verificar su existencia.

Carisma: Se aplica un ambiente de respeto y generosidad hacia el personal para poder obtener la información.

Reciprocidad: Se recompensa con ayuda a la persona que ayuda con la información, de varias maneras.

Consistencia: Se realiza la investigación durante varias semanas hasta poder obtener familiaridad con la presencia del investigador en el sitio, para poder obtener acceso a la información.

Validación Social: No se puede aplicar este tipo de técnica seductiva debido a que requiere familiarizarse con temas y problemas personales de una persona en particular para poder utilizarla como señuelo.

b) Ingeniería Social Inversa.

La existencia de esta técnica se determina por la obtención de la información sin requerirla.

Se detalla la información personal obtenida de un colaborador del Departamento de Recursos Humanos de la Universidad Técnica de Ambato, sin haber establecido ninguna pregunta hacia el mismo.

- Nombres y Apellidos
- Ideología Política
- Ubicación exacta de la oficina donde se realiza el manejo del Presupuesto de la Universidad Técnica de Ambato.

Cuadro de Resumen de las evidencias encontradas:

TÉCNICA	VULNERABILIDAD	EVIDENCIA	EXISTENCIA
INVASIVAS O DIRECTAS O FÍSICAS			
EL TELÉFONO			
	Personificación Falsa y Persuasión	Llamada Telefónica	1
	Robo de Contraseñas o Claves de Acceso	Debido a la delicadeza de la información esta técnica se la utilizó solamente con una persona	1
EL SITIO DE TRABAJO			
	Acceso Físico No Autorizado	Se pudo ingresar a realizar una encuesta dentro de este cuarto y sentarse junto a las personas que atienden dentro del mismo.	1
	Robar, Fotografiar o copiar documentos	Se realizó la fotografía de varios documentos del departamento. Además se pudo hacer uso de una de las máquinas del departamento sin ningún tipo de supervisión alguna.	1
	Acceso a servidores	No Aplica debido a que	0

		lo servidores no se encuentran en el departamento	
LA BASURA			
	Desecho de documentación sin previa destrucción	Se obtiene un documento del recipiente de desechos.	1
LA INTRANET			
	Repetición de Passwords	Los usuarios del departamento comparten sus contraseñas entre ellos.	1
SEDUCTIVAS Y/O INADVERTIDAS			
	Carisma	Se utilizaron estas técnicas para ganare la confianza del personal y de esta manera poder obtener información de suma importancia.	1
	Reciprocidad		1
	Consistencia	Se visita el departamento varias veces para poder generar familiaridad.	1
	Ingeniería Social Inversa	Se obtiene información sin requerirla	1
VULNERABILIDADES SATISFACTORIAS			**10**

Tabla 6.9. Cuadro de Evidencias de Aplicación de Técnicas

En relación y haciendo una comparación entre los dos cuadros de vulnerabilidades, el investigador genera un cuadro de vulnerabilidades final que resuma la existencia de todas las vulnerabilidades identificadas y realizar la justificación necesaria para cada una de estas:

TÉCNICA	VULNERABILIDAD	EXISTENCIA O INEXISTENCIA
INVASIVAS O DIRECTAS O FÍSICAS		
EL TELÉFONO		
	Personificación Falsa y Persuasión	1
	Robo de Contraseñas o Claves de Acceso	1
EL SITIO DE TRABAJO		
	Acceso Físico No Autorizado	1
	Mirar sobre el hombro	1
	Robar, Fotografiar o copiar documentos	1
	Acceso a servidores	0
LA BASURA		
	Desecho de documentación sin previa destrucción	1
LA INTRANET		
	Repetición de Passwords	1
SEDUCTIVAS Y/O INADVERTIDAS		
	Autoridad	0
	Carisma	1
	Reciprocidad	1
	Consistencia	1
	Validación Social	0
	Ingeniería Social Inversa	1
VULNERABILIDADES ENCONTRADAS		**11**

Tabla 6.10. Análisis de Vulnerabilidades

Detalladas las vulnerabilidades existentes dentro del Departamento se procede a realizar la justificación de cada vulnerabilidad con la investigación y el cuadro de evidencias de cada una de las vulnerabilidades.

JUSTIFICACIONES:

INVASIVAS O DIRECTAS O FÍSICAS

El Teléfono

Personificación Falsa y Persuasión: Se determina la existencia de esta para ello se utiliza esta técnica para obtener información personal de un colaborador del departamento.

EXISTENCIA DE VULNERABILIDAD = 1

Robo de Contraseñas o Claves de Acceso: Se obtiene este tipo de información aplicando varias técnicas Seductivas y/o Inadvertidas, lo cual realiza termina en un acto inconsciente de revelación de información confidencial de un colaborador exponiendo abiertamente al sistema y la información tanto del departamento como de la institución.

EXISTENCIA DE VULNERABILIDAD = 1

El Sitio De Trabajo

Acceso Físico No Autorizado: Para verificar la existencia de esta vulnerabilidad se aplica la técnica, obteniendo como resultado el acceso sin corroboración.

EXISTENCIA DE VULNERABILIDAD = 1

Shoulder Surfing: La aplicación de esta técnica no fue necesaria debido a que esta técnica trata de obtener información confidencial solamente mirando lo que la víctima digita en su computador y de esta manera obtener información confidencial como Claves de Acceso, Contraseñas y hasta números de cuenta institucionales como privadas.

La vulnerabilidad hacia este tipo de técnica es muy elevada debido a que no se lleva un control adecuado de las visitas y el fácil acceso obtenido tanto a las claves de acceso como a las máquinas y datos personales de los colaboradores.

Para el investigador tomar como una vulnerabilidad existente este tipo de técnica le ayuda a realizar controles para salvaguardar la información.

EXISTENCIA DE VULNERABILIDAD = 1

Robar, Fotografiar o copiar documentos: Para el investigador afirmar la existencia de esta técnica se fundamenta en la evidencia fotográfica de la misma.

EXISTENCIA DE VULNERABILIDAD = 1

Acceso a cuarto de servidores: La aplicación de esta técnica no es posible debido a que dentro del departamento no se encuentra un cuarto de servidores.

EXISTENCIA DE VULNERABILIDAD = 0

La Basura

Desecho de documentación sin previa destrucción: para justificar la existencia de esta vulnerabilidad el investigador se basa en la evidencia colectada y evidenciada mediante fotografías.

EXISTENCIA DE VULNERABILIDAD = 1

La Intranet

Repetición de Passwords: Para realizar la justificación de la existencia de la vulnerabilidad el investigador se basa en la vulnerabilidad identificada en la encuesta aplicada al personal del departamento la cual arrojo una respuesta afirmativa del 36% en divulgación de contraseñas de acceso a los sistemas del departamento.

EXISTENCIA DE VULNERABILIDAD = 1

SEDUCTIVAS Y/O INADVERTIDAS

Autoridad: El investigador analiza la posibilidad de la existencia de esta técnica pero la aplicación de la misma fue complicada debido a que el número de colaboradores es mínimo lo que fortalece los lazos de confianza entre los mismos y elimina cualquier vulnerabilidad entre la aplicación de esta técnica. Además de identificar que el departamento es aquel que realiza la contratación del personal.

EXISTENCIA DE VULNERABILIDAD = 0

Carisma, Reciprocidad, Consistencia: La existencia de las vulnerabilidades que abarcan estas técnicas están explícitamente acompañadas de las técnicas anteriormente descritas y justificadas para lo cual se determina como verdadera la existencia de estas vulnerabilidades.

EXISTENCIA DE VULNERABILIDAD = 1

Validación Social: Debido a que el número de personas que trabajan en el departamento de Recursos Humanos de la Universidad Técnica es pequeño la utilización de esta técnica se dificulta debido a la complejidad del análisis psicológico que se debe realiza a la(s) víctima(s), para lo cual se rechaza la aplicación de esta vulnerabilidad por la complejidad de la misma, y por las consecuencias de la misma al aplicarla.

El investigador se ve en la obligación de rechazar esta técnica por la falta de evidencia para poder realizar la afirmación de la existencia de la misma, a pesar de que con el conocimiento de las técnicas psicológicas a aplicarse no se posee el

conocimiento necesario de la Psicología necesaria para ejecutar este tipo de pruebas.

EXISTENCIA DE VULNERABILIDAD =0

Ingeniería Social Inversa: La existencia de esta vulnerabilidad se justifica mediante la evidencia recolectada en la Tabla 6. 7. Cuadro de Evidencias de las Vulnerabilidades la cual se justifica con la información obtenida sin que esta sea requerida.

EXISTENCIA DE VULNERABILIDAD =1

Para el investigador la obtención de los datos requirió de tiempo de investigación tanto del flujo de la información como de cada una de las personas que conforman el departamento de Recursos Humanos de la Universidad Técnica de Ambato.

FASE VI- IMPACTO Y RIESGO

6.7.2.11. Análisis de Impacto y Riesgo

El análisis sobre el impacto y el riego se lo determina mediante las siguientes tablas:

Análisis del Riesgo:

MA	Muy alto
A	Alto
M	Medio
B	Bajo
MB	Muy bajo

Tabla 6.11. Valoración del Riesgo

Análisis del Impacto:

ZONA 1	1		Muy Probables y de muy alto impacto
ZONA 2	2		Improbables y de impacto medio hasta Muy probables pero de impacto bajo o muy bajo.
ZONA 3	3		Riesgos improbables y de bajo impacto
ZONA 4	4		Riesgos improbables pero de muy alto impacto

Tabla 6.12. Valoración del Impacto

Análisis del Riesgo y Valoración del Impacto

INVASIVAS O DIRECTAS O FÍSICAS				
AMENAZA	**VULNERABILIDAD**	**RIESGO**	**IMPACTO**	
EL TELÉFONO				
	Personificación Falsa y Persuasión	**MA**	**1**	
	Robo de Contraseñas o Claves de Acceso	**MA**	**1**	
EL SITIO DE TRABAJO				
	Acceso Físico No Autorizado	**A**	**1**	
	Shoulder Surfing	**M**	**4**	
	Robar, Fotografiar o copiar documentos	**MA**	**1**	
LA BASURA				
	Desecho de documentación sin previa destrucción	**A**	**1**	
LA INTRANET				
	Repetición de Passwords	**M**	**3**	
	Divulgación de Contraseñas	**A**	**1**	
SEDUCTIVAS Y/O INADVERTIDAS				
COMPORTAMIENTO HUMANO	Autoridad	**MB**	**4**	
	Carisma	**MA**	**1**	
	Reciprocidad	**MA**	**1**	
	Consistencia	**MA**	**1**	
	Validación Social	**MB**	**4**	
	Ingeniería Social Inversa	**A**	**4**	

Tabla 6.13. Determinación del Riesgo e Impacto de las Vulnerabilidades

FASE VII - SALVAGUARDAS

6.7.2.12. Identificación de Salvaguardas

Para poder aplicar los controles y salvaguardas necesarias para minimizar las vulnerabilidades encontradas se identifican necesarios los siguientes tipos de salvaguardas:

- Políticas: Para controlar de manera permanente y establecer un punto de control.
- Procedimientos: Para poder conocer las actividades y la secuencia de las mismas para establecer los controles.
- Contramedidas: Para poder establecer puntos de advertencia para prevención de los ataques.

6.7.2.13. Generación de Salvaguardas

POLÍTICAS:

Generales

- Todo el personal es responsable de mantener la confidencialidad de la información del Departamento de Recursos Humanos de la Universidad Técnica de Ambato.

Teléfono

- Solicitar en cada llamada Nombres e Identidades a las que pertenece la persona que requiere de la ayuda del departamento.
- Es responsabilidad del usuario corroborar los datos suministrados por la persona.
- Es responsabilidad de cada usuario evitar realizar o sostener llamadas de larga duración, que sean sospechosas y que no provean de la información necesaria.
- Negarse a entregar información confidencial como passwords u información personal confidencial.

Sitio de Trabajo

- Controlar el acceso físico de las personas al departamento y hacia áreas de Acceso No Autorizado o Restringido.
- Mantener seguros documentos e información importante dentro y fuera del departamento.
- No Digitar contraseñas o claves de acceso cuando alguien está mirando.
- Restringir el uso de fotocopiadoras, escáneres, cámaras digitales y cámaras de celulares para los documentos más importantes.
- Evitar el acceso no autorizado a servidores y máquinas del departamento sin supervisión.
- Clasificar la información confidencial y salvaguardarla apropiadamente.

La Basura

- Mantener la basura asegurada y monitoreada.
- Destruir datos sensibles expuestos en papel.
- Destruir medios magnéticos y rayar los CD's, DVD's y cualquier otro medio de almacenamiento.
- Eliminar información de discos duros de máquinas no utilizadas.

La Intranet

- Realizar la asignación de passwords seguros con un mínimo de 8 caracteres, una combinación de letras mayúsculas, minúsculas, caracteres especiales y números.
- No utilizar parámetros personales para la generación de passwords que se vayan a utilizar en máquinas utilizadas para la realización de sus actividades laborales, como por ejemplo: nombres, apellidos, números de cedula, etc.
- Evitar dar información sobre cambios o módulos que posea el sistema sobre el cual se trabaja.

Comportamiento Humano

- Los empleados del Departamento deben evitar en lo posible el proveer a personas externas a la institución de información personal o institucional.
- Verificar siempre la identidad de cualquier persona antes de presentar cualquier tipo de información, en cualquiera de los casos de contacto.

PROCEDIMIENTOS

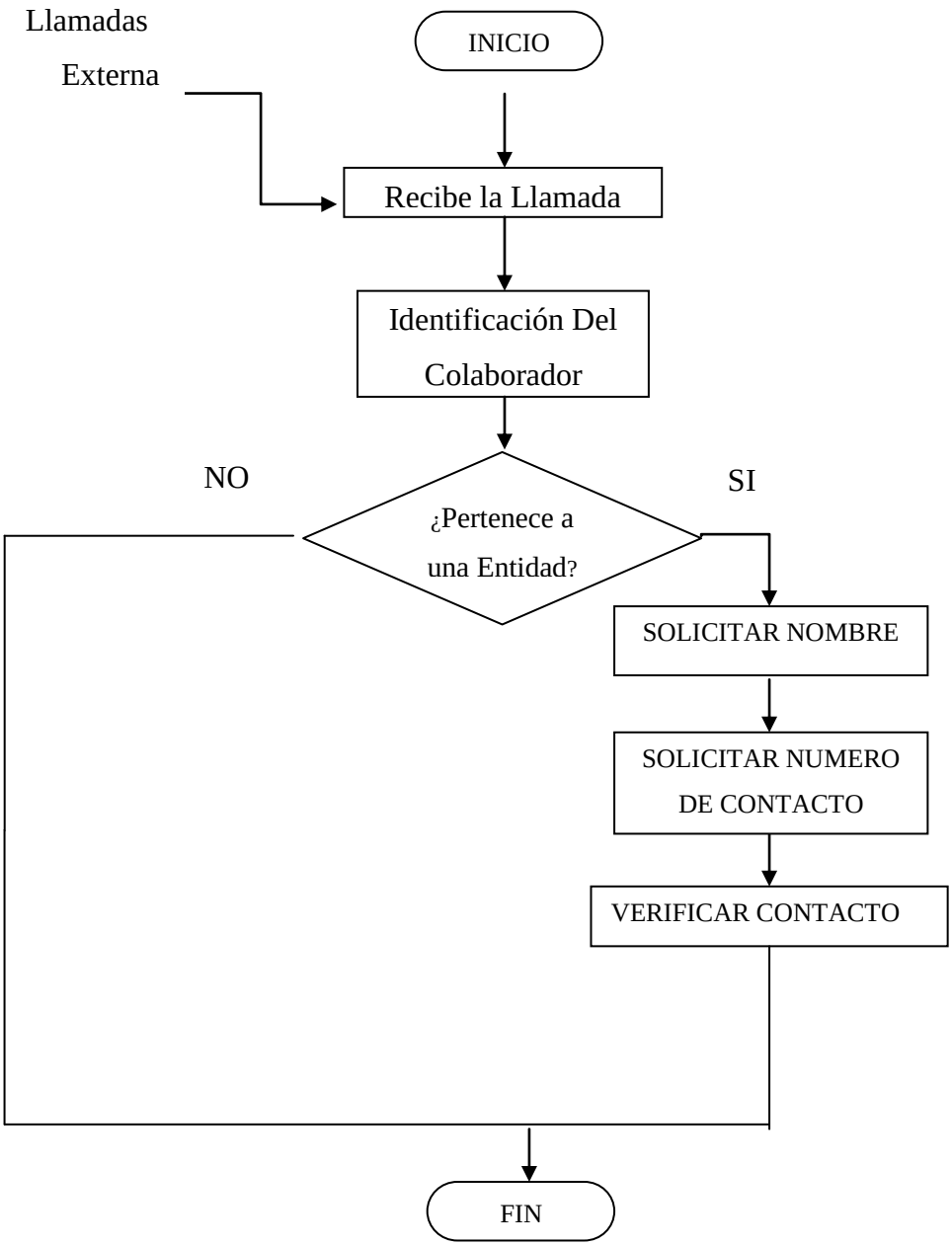
Del Uso del Teléfono

1. Solicitar en cada llamada Nombres e Identidades a las que pertenece la persona que requiere de la ayuda del departamento.

Nombre	Solicitud de Información
Objetivo	Obtener información del usuario
Frecuencia	Eventual

Área	Actividad	Descripción
Departamento de Recursos Humanos	1	Se toma la llamada para lo cual se identifica el departamento, la persona que toma la llamada y finalmente se solicita al usuario que se identifique.
	2	Se solicita al usuario que nos proporcione su Nombre y Apellido.
	3 3.1 3.2 3.3 3.4 3.5	¿El usuario pertenece a alguna entidad específica? <u>En caso de que pertenezca:</u> Solicitar el Nombre de la identidad Solicitar un número de teléfono. Verificar que el número de teléfono corresponda a la entidad. Fin.
	4 4.1	<u>En caso de que no pertenezca:</u> Fin.

FLUJOGRAMA 1



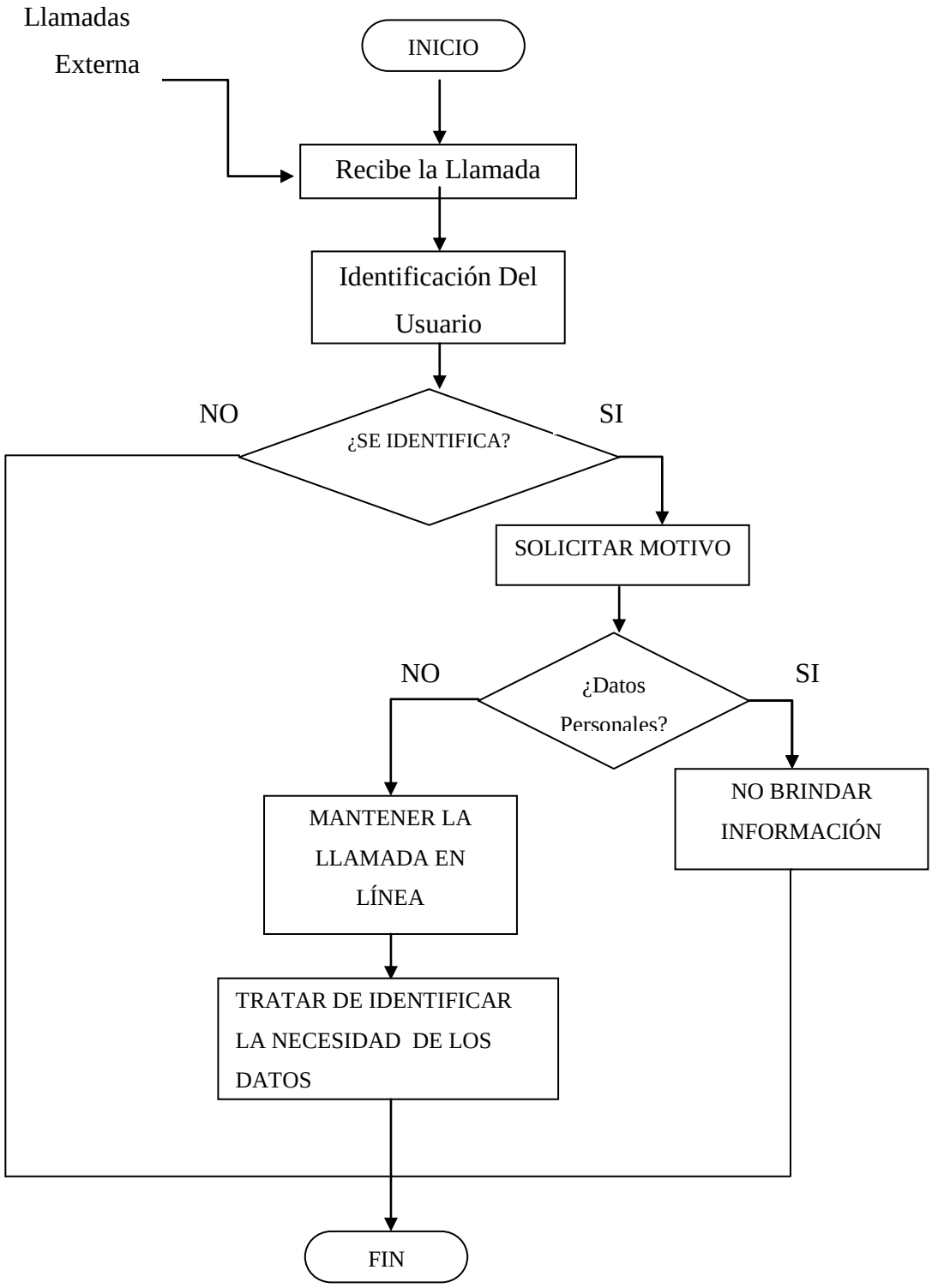
2. Una vez identificada la anomalía dentro de la llamada telefónica. Mantener al usuario en línea hasta poder contactar a un superior que tome control de la situación.

Nombre	Anomalías de Llamadas telefónicas externas
Objetivo	Mantener en la línea telefónica al usuario en línea hasta contactar a un superior que tome control de la situación.
Frecuencia	Eventual

Área	Actividad	Descripción
Departamento de Recursos Humanos	1	Se toma la llamada para lo cual se identifica el departamento, la persona que toma la llamada y finalmente se solicita al usuario que se identifique.
	2	Se solicita al usuario que nos proporcione su nombre y apellido.
	3 3.1	¿El usuario no se identifica? Se debe proceder a cerrar la llamada Fin.
	4	Se debe solicitar al usuario que identifique el motivo de su llamada.
	5	Una vez tomada la solicitud del usuario se debe analizar los diferentes tipos de información a brindar.
	6	¿La información solicitada por el usuario de la línea telefónica solicita datos personales?
	7	<u>En caso de que el usuario solicita datos personales:</u>

	7.1 7.2 Fin.	Mantener al usuario en la línea y solicitar a un superior que monitoree la llamada, pero nunca dar datos personales. Identificado el direccionamiento de la llamada se debe proceder a cerrarla.
	8 8.1 8.2 Fin.	<u>En caso de que el usuario no solicite datos personales o confidenciales:</u> Identificar la información requerida Proporcionar la información solicitada

FLUJOGRAMA 2



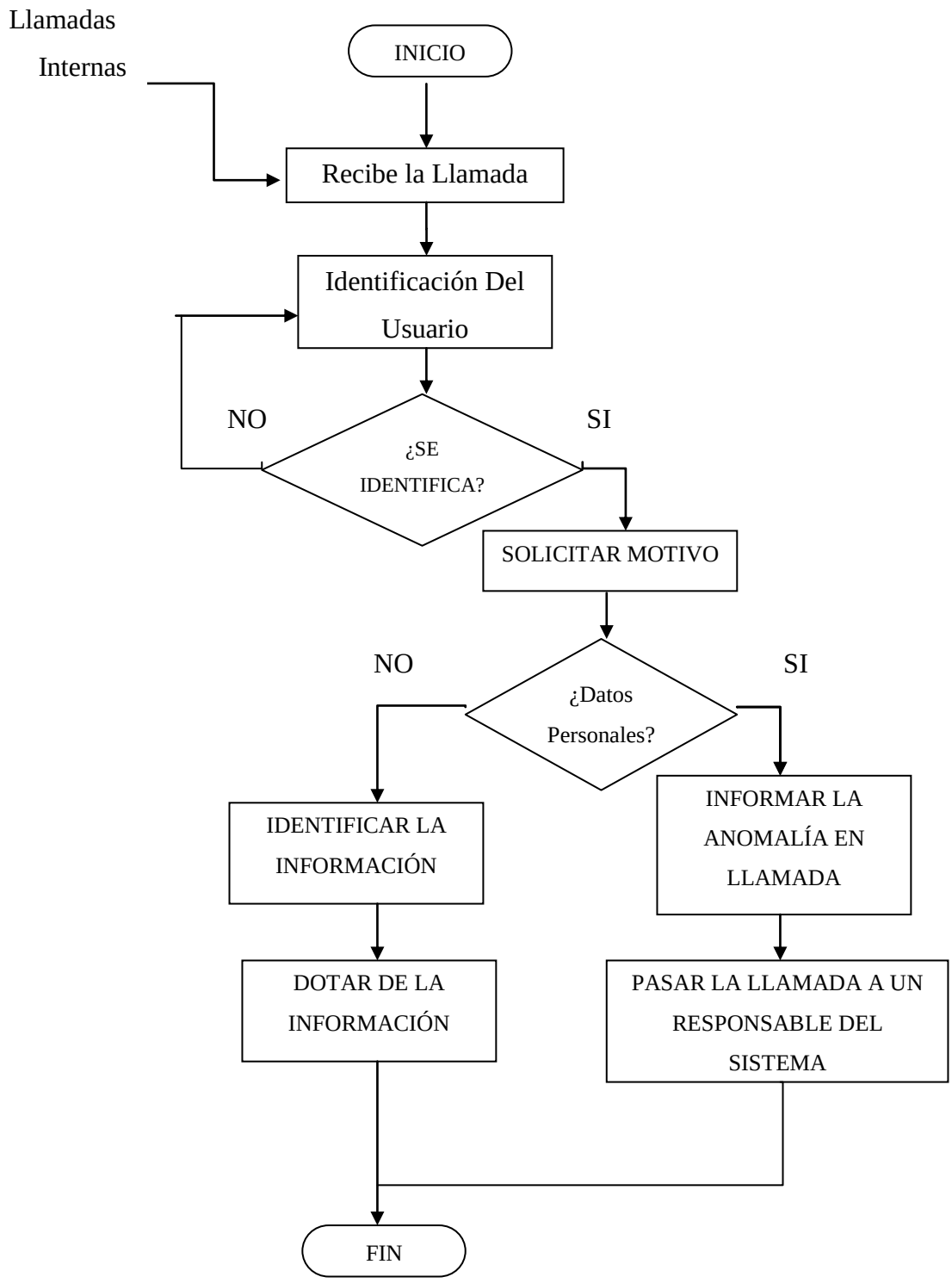
3. Si la llamada proviene de una oficina que se ubica dentro de la institución se deberá proceder a informar al Responsable de la misma sobre la llamada recibida con diversas anomalías.

Nombre	Anomalías de Llamadas telefónicas internas
Objetivo	Identificar llamadas anomalías que traten de obtener información confidencial
Frecuencia	Eventual

Área	Actividad	Descripción
Departamento de Recursos Humanos	1	Se toma la llamada para lo cual se identifica el departamento, la persona que toma la llamada y finalmente se solicita al usuario que se identifique.
	2	Se verifica que la persona pertenezca al departamento que menciona
	3 3.1 3.2 3.3 3.4 3.5 3.6	¿El usuario pertenece al departamento identificado? Se debe proceder a identificar el requerimiento solicitado. ¿Solicita que se le proporcione algún tipo de información no autorizada para acceder a la información? <u>En caso de que se solicita esta información:</u> Informar al superior que se está solicitando información confidencial. Identificar al usuario que solicita la llamada. Pasar la llamada al encargado del sistema de información para que tome control de la situación Fin. <u>En caso de no se solicite este tipo de información:</u>

	3.7	Identificar la información requerida. Proporcionar la información Fin.
	4	<u>En caso de que no se identifique al usuario dentro del departamento descrito:</u> Solicitar nuevamente que se identifique Fin.

FLUJOGRAMA 3



Del Sitio de Trabajo

4. Realizar un control de las personas mediante un Registro en el cual se incluirá el Nombre, Número de Cédula, Motivo de Visita, Hora de Ingreso, Hora de Salida y una Firma de la persona Visitante. **Formato de Registro Anexo 1.**

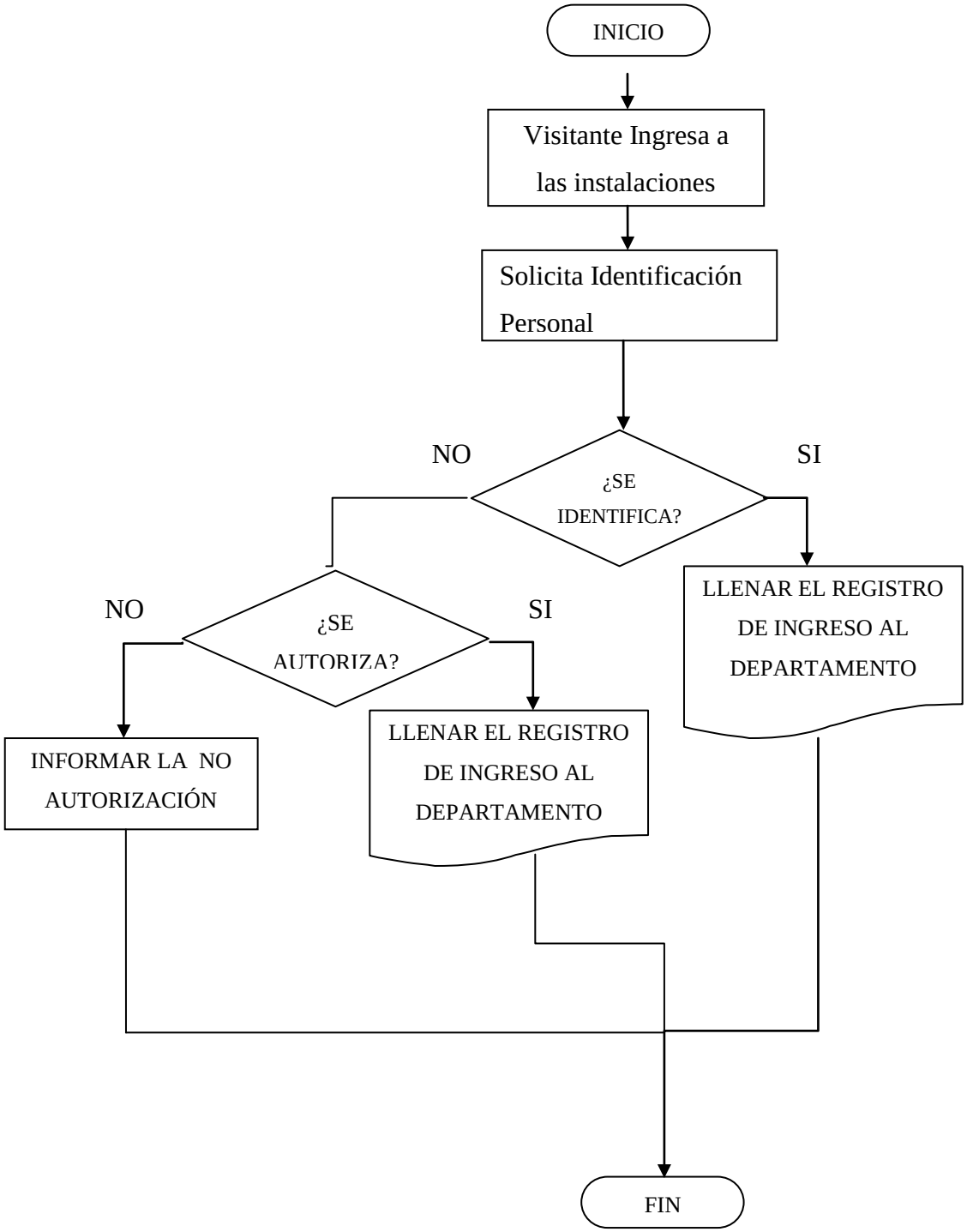
5. Verificar que el nombre de la persona corresponda al visitante que se registra

Nombre	Control de Ingreso al Departamento
Objetivo	Registrar a los visitantes del departamento mediante un formato de Registro de Ingresos
Frecuencia	Eventual

Área	Actividad	Descripción
Seguridad de la Institución	1	Se solicita un documento de identificación a la persona visitante
	2	¿El visitante posee alguna identificación?
	3 3.1 3.2	**<u>En caso de que se presente identificación:</u>** Llenar el Formato de Registro "**FORMATO DE CONTROL DE INGRESO DE VISITANTES**", para el cual se llenarán todas las columnas de este registro. Fin.
	4 4.1 4.2 4.3	**<u>En caso de que no se presente la identificación:</u>** El personal de seguridad debe anunciar a la persona ¿Se afirma el paso del visitante? <u>En caso de que se afirme el paso del visitante:</u> Llenar el Formato de Registro "**FORMATO DE**

	4.4	**CONTROL DE INGRESO DE VISITANTES**", para el cual se llenarán todas las columnas de este registro. Fin. <u>En caso de que se niegue el paso del visitante:</u> Informar la No Autorización del ingreso. Fin.

FLUJOGRAMA 4



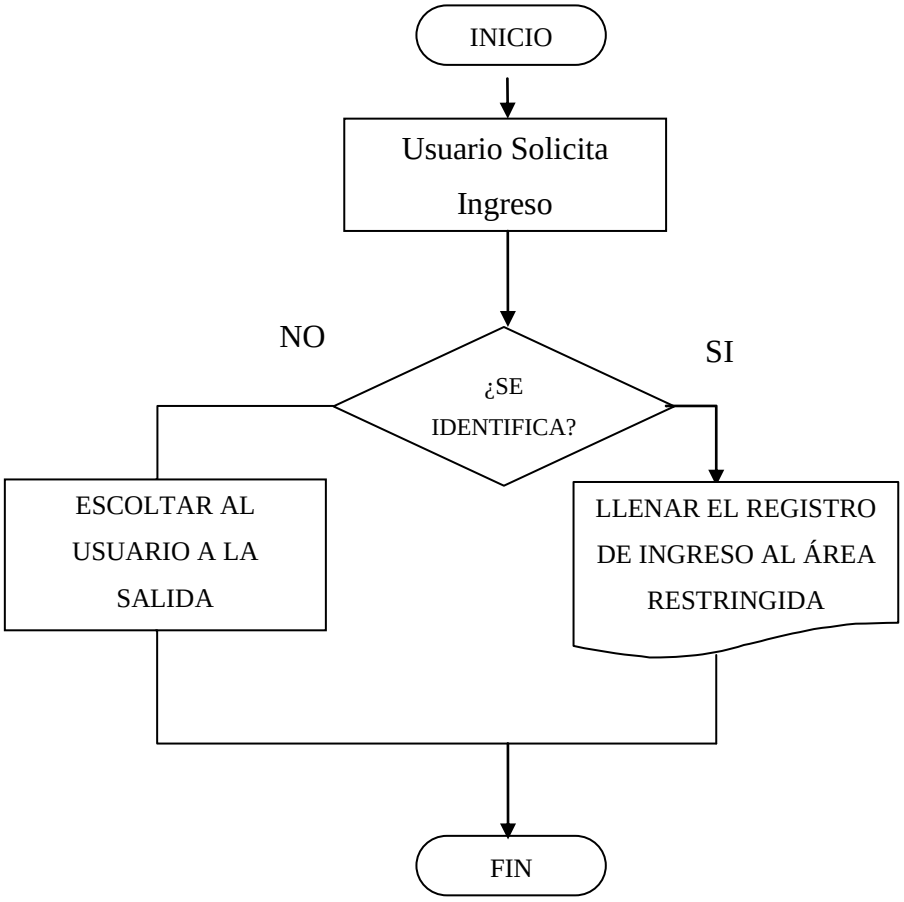
6. Evitar que las personas ajenas al Departamento ingresen a los sitios de acceso restringido, el acceso a estos debe ser únicamente autorizado por el Director de Recursos Humanos en casos de primordial importancia.

7. Si se detecta alguna persona que no posea la autorización y se encuentre dentro de un sitio restringido se debe dar aviso a su superior con la brevedad posible.

Nombre	Control de Ingreso a Áreas Restringidas
Objetivo	Controlar el acceso a áreas restringidas
Frecuencia	Eventual

Área	Actividad	Descripción
Director de Recursos Humanos	1	Se solicita acceso al área restringida especificando las actividades a realizarse y el motivo.
	2	¿Se autoriza el ingreso al área restringida?
	3 3.1	**<u>En caso de que se autorice:</u>** Llenar el Formato de Registro "**FORMATO DE CONTROL DE INGRESO A CUARTO DE ACCESO NO AUTORIZADO**", para el cual se llenarán todas las columnas de este registro. Fin.
	4 4.1	**<u>En caso de que no se autorice:</u>** Un colaborador del Departamento de Recursos Humanos de la Universidad Técnica de Ambato debe acompañar al visitante hacia la salida. Fin.

FLUJOGRAMA 5



De la Basura

8. Evitar desechar archivos, documentos o medios de almacenamiento sin realizar la previa destrucción de los mismos para evitar que se esta se pueda recuperar una vez desechados.

9. Si se detecta alguna persona que no posea la autorización y se encuentre dentro de un sitio restringido se debe dar aviso a su superior con la brevedad posible.

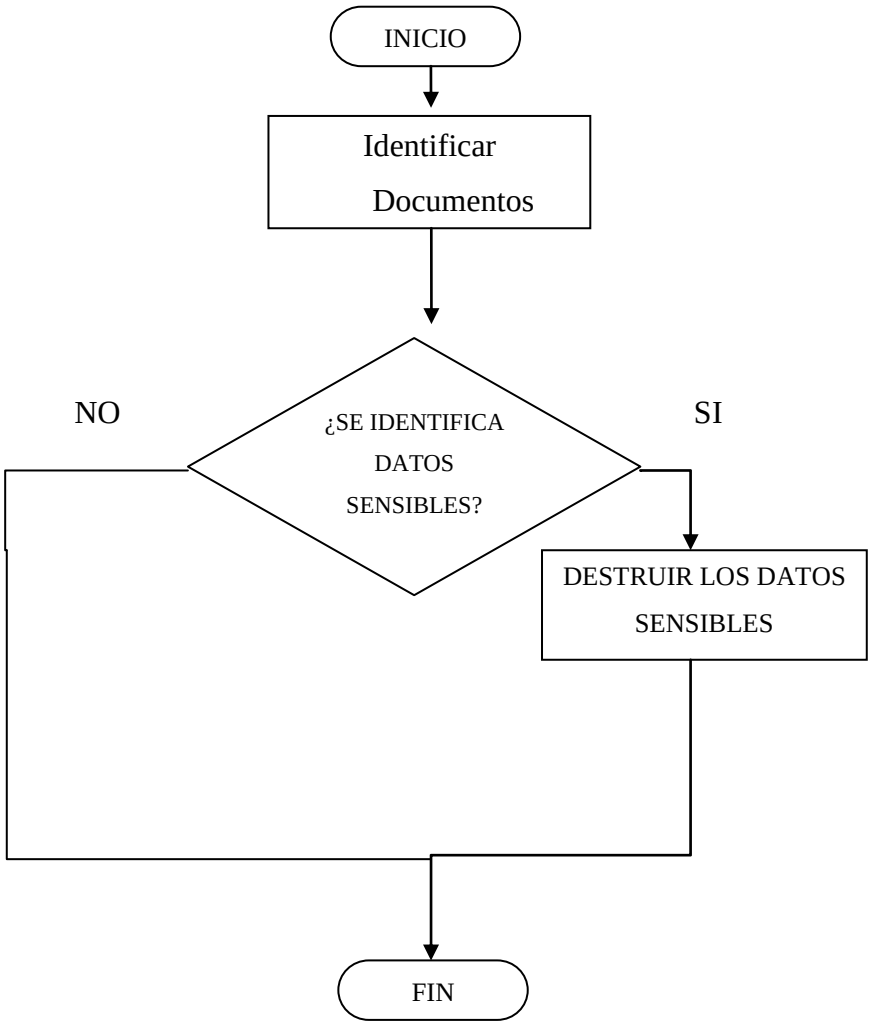
10. Verificar que los archivos en físicos que se vayan a desechar estén correctamente cortados o a su vez tachar los campos o datos de información personal o confidencial.

Nombre	Control de Documentos Desechados
Objetivo	Controlar el desecho de documentos que contengan datos confidenciales
Frecuencia	Eventual

Área	Actividad	Descripción
Director de Recursos Humanos	1	Identifican archivos a desechar
	2	Verificar los datos obtenidos dentro del mismo
	3	¿Se encuentran datos sensibles en los documentos?
	4 4.1	**<u>En caso de que se identifique este tipo de datos:</u>** Proceder a destruir por completo los documentos, utilizando; corte de los documentos, tachado de los datos o el quemado de los mismos.

		Fin.
	5 5.1	**<u>En caso de que no se identifique este tipo de datos:</u>** Proceder a desecharlo. Fin.

FLUJOGRAMA 6



De la Intranet

11. Evitar compartir o divulgar las contraseñas. Las contraseñas son de uso personal e intransferibles

12. Formar una cultura de confidencialidad dentro del Departamento con las claves personales asignadas a cada uno de los equipos.

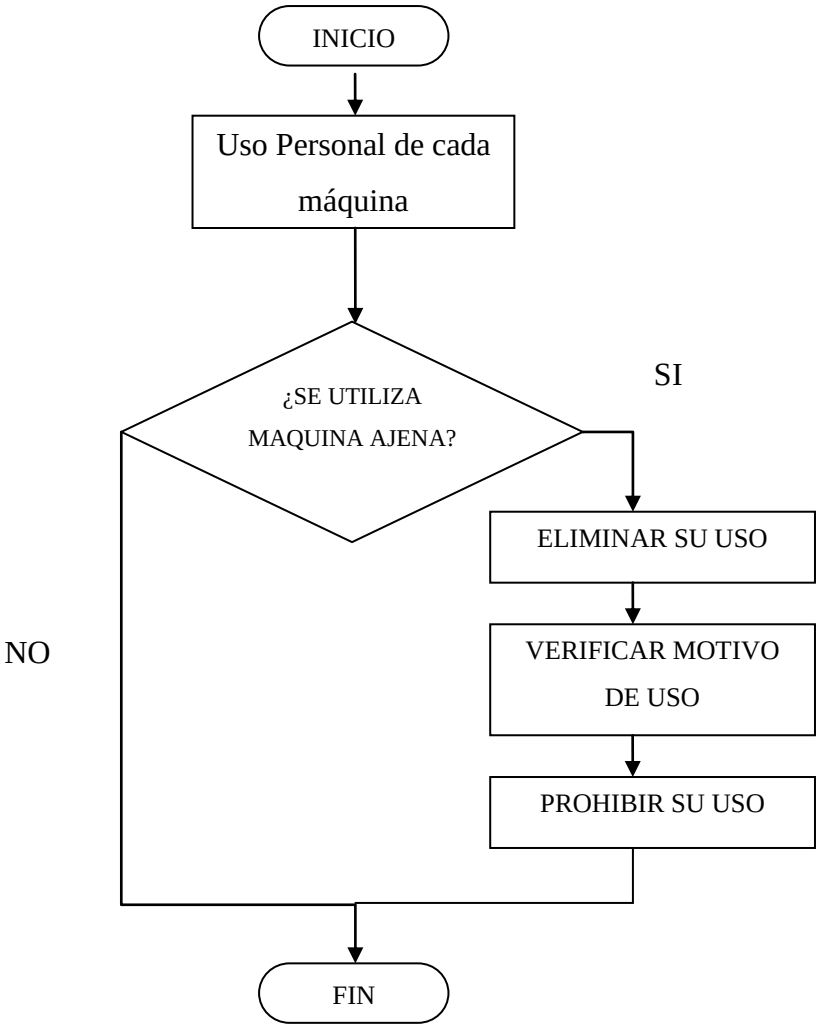
13. Si se detecta que algún colaborador usa una máquina o contraseña ajena sin autorización y supervisión del colaborador, se debe dar conocimiento a su jefe inmediato superior; y este a su vez, debe informar al departamento de Sistemas sobre el suceso encontrado.

Nombre	Control de confidencialidad de Contraseñas
Objetivo	Evitar el control de uso de contraseñas ajenas en máquinas del departamento
Frecuencia	Eventual

Área	Actividad	Descripción
Personal de Recursos Humanos de la UTA	1	Verificar que cada usuario utilice únicamente su contraseña en su máquina
	2	¿Se utiliza máquinas de otros colaboradores sin supervisión del mismo?
	3	**<u>En caso de que se identifique este tipo de anomalías:</u>**
	4.1	Proceder a eliminar el uso de la misma.
	4.2	Verificar los motivos de uso de la máquina.
	4.3	Prohibir el uso de la máquina sin supervisión.
		Fin.

	5 5.1	**<u>En caso de que no se identifique este tipo de anomalías:</u>** Fin.

FLUJOGRAMA 7



Del Comportamiento Humano

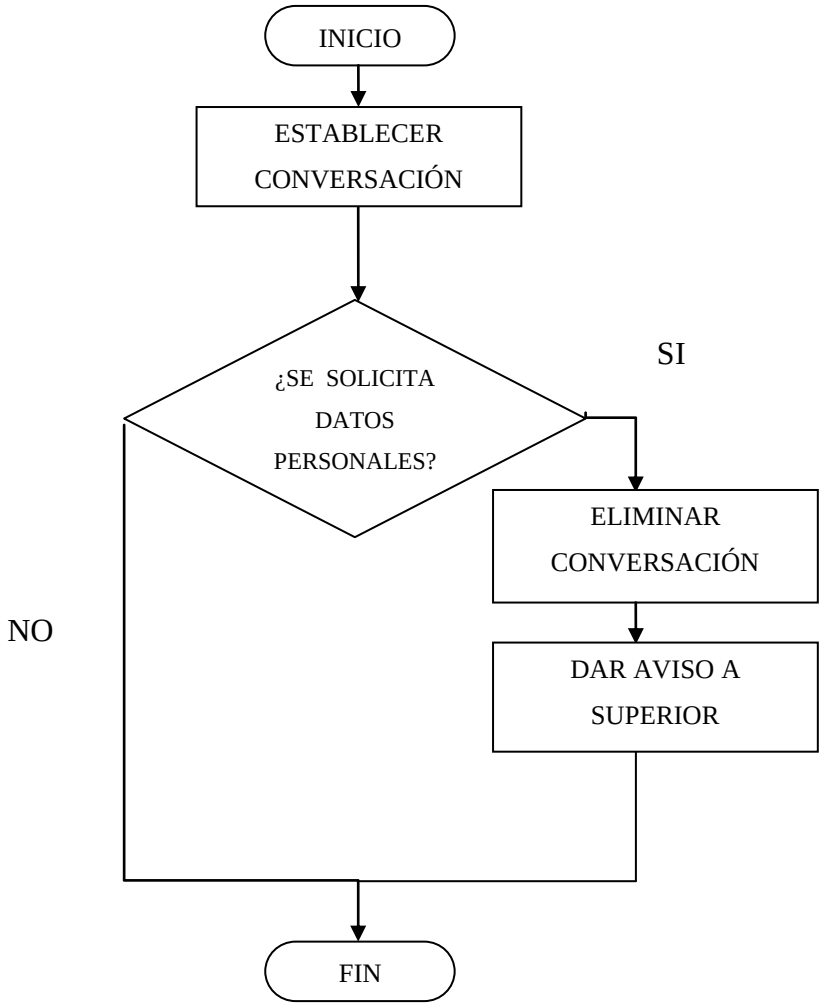
14. Cada uno de los colaboradores debe evitar establecer conversaciones personales con los visitantes del departamento, para evitar identificar información personal del colaborador que pueda comprometer la seguridad de la información.

15. Si se observa algún comportamiento de autoridad e insistencia en la obtención de información tanto personal como confidencial se deberá informar a su jefe inmediato superior sobre el acontecimiento encontrado y a la vez se deberá evitar dar acceso al mismo a algún dispositivo de almacenamiento proveniente del visitante o usuario.

Nombre	Control de divulgación de Información
Objetivo	Evitar la divulgación de datos personales o confidenciales de la empresa
Frecuencia	Eventual

Área	Actividad	Descripción
Personal de Recursos Humanos de la UTA	1	Verificar los temas de conversación
	2	¿Se solicitan datos personales o confidenciales?
	3	**En caso de que se identifique este tipo de anomalías:**
	4.1	Proceder a terminar la conversación.
	4.2	Dar aviso a superior sobre el hecho ocurrido
		Fin.
	5	**En caso de que no se identifique este tipo de anomalías:**
	5.1	Fin.

FLUJOGRAMA 8



CONTRAMEDIDAS

EL TELÉFONO

La utilización del teléfono es un blanco perfecto para los ataques de la Ingeniería Social estos pueden alcanzar su objetivo al 100% con tan solo realizar una suplantación de identidad, y de este modo vulnerar la seguridad de cualquier institución.

Contramedidas:

- Ser muy celoso con los datos personales e institucionales.
- No entregar información sensible a nadie.
- Sospechar de llamadas telefónicas no solicitadas.
- No suministrar información personal o empresarial sin estar seguro.

DEL SITIO DE TRABAJO

Realizar un control mínimo sobre las personas que ingresan a las oficinas del Departamento de Recursos Humanos de la Universidad Técnica de Ambato puede minimizar en gran medida la amenaza de un ataque que vulnere la Seguridad Informática.

Contramedidas:

- No ser tan confiado. No es necesario llegar a la paranoia, pero sí es importante tener presente que estos hechos cada día son más habituales y es vital estar atentos.

LA BASURA

No es para nada raro ver en los escritorios de los empleados papeles de todo tipo revelando información más que útil para cualquier atacante que quiera utilizar algunos de los métodos antes descritos, se pueden encontrar desde Números de teléfonos útiles, claves de acceso a bancos, claves de acceso a portales tributarios, web mails, etc.

Muchos de estos papeles, generalmente van a parar a la basura y posteriormente a la calle donde el atacante tiene un acceso directo a ellos.

Esta también es una práctica de la ingeniería social, y aunque en la mayoría de los casos no se revelen datos útiles como números de pines y claves, si se revela información valiosa para entender el funcionamiento de la empresa, por ejemplo: mails impresos, agendas con números telefónicos, datos de personas, reuniones, bancos en uso, etc.

Si se tiene acceso a esos datos, es probable que el atacante gane conocimiento necesario para aplicar, por ejemplo, la técnica de Ingeniería Social Inversa.

Contramedidas:

- Como primera medida, evite usar el papel común para anotar claves, pines o números (mucho menos pegarlo en el costado del monitor o dejarlo a la vista de cualquier persona). Utilice herramientas (a veces en formato software) destinadas para estas tareas, por ejemplo: USB Tokens, Smart Cards, sistemas de almacenamiento de claves, etc.

- No deseche información sensible en papeles grandes y legibles, utilice trituradoras de papel antes de echarlos a la basura.

LA INTRANET

PHISHING

Esta técnica a pesar de no realizar interacción personal con la víctima permite realizar el uso de la Ingeniería Social mediante el engaño en cuanto a las páginas y los textos que se muestran al usuario.

Gráfica. 6. 8. Gráfica de Página Falsa de Phishing

Gráfica. 6. 9. Gráfica de Solicitud de Datos con Phishing

Contramedidas:

Como principales contramedidas con referencia a los ataques de PHISHING:

- Los bancos e instituciones financieras nunca y en ningún caso solicitan datos personales, números o códigos de tarjetas. Si llegado al caso se llega a recibir este tipo de emails, se debe proceder a eliminarlo.

- Cuando se ingrese a la página de Internet de su banco o institución financiera, se debe revisar los siguientes parámetros básicos de seguridad:

- Que la URL o dirección de la página comience con https:// y no con el http://
- Asegurarse que la dirección sea la correcta y no con alteraciones
- Se puede verificar el certificado de seguridad con el cual las páginas de seguridad vienen firmados para hacer legítima la seguridad del sitio Web donde se ingresa para realizar las transferencias.
- Evitar ingresar a sitio de instituciones financieras o realizar compras en línea en Cibercafés o computadoras públicas.
- Si se posee dudas al respecto se recomienda acercarse a la institución financiera o llamar a un número que se posea de la misma con anterioridad.

INGENIERÍA SOCIAL INVERSA

Esta técnica aplica a grandes organizaciones, donde no todos se conocen entre sí, y consiste en que el atacante contacta a un empleado significativo para el fin (algún administrativo con acceso a cuentas, algún sysadmin, etc.) haciéndose pasar por un alto directivo de la empresa y solicitándole datos sensibles (claves, números de pin, etc.) de manera urgente.

Muchas veces, los mismos servidores de e-mail de la empresa cuentan con una mala configuración que permite enviar mails en nombre de otros. Esto es un ambiente propicio para perpetrar estos ataques.

Por supuesto que estos actos delictivos deben ser planificados y estudiados por el atacante, que deberá conocer de la mecánica interna de la organización, pero aún así, cuenta con grandes oportunidades de conseguir información valiosa.

Contramedidas*:*

- El usuario que posea información sensible, por política de la empresa, no debe divulgar dicha información a nadie que no esté autorizado. De hacerlo, deberá existir un procedimiento para proporcionarla de manera segura y se pueda comprobar la identidad del solicitante.

Presentación del manual al director y personal del Departamento de Recursos Humanos de la Universidad Técnica de Ambato.

Culminada la creación del Manual bajo la base de la metodología de la administración de Riesgo Tecnológicos, se procede a realizar la presentación del Manual al Director del Departamento de Recursos Humanos.

Para lo cual se redacta una solicitud de recepción del Manual de Políticas, Procedimientos y Contramedidas de Seguridad Informática referentes a la Vulnerabilidad Humana la cual llevara en la parte frontal del mismo:

- Sellos y nombre de la Universidad.
- Ciudad y Fecha de Emisión.
- Nombre y Firma del Director de Recursos Humanos de la UTA.
- Sello del Departamento de Recursos Humanos.
- Nombre y Firma en la parte inferior derecha del documento de la persona que entrega el manual al Director del Departamento de Recursos humanos de la Universidad Técnica de Ambato.

Anexo 5. Solicitud de Presentación del Manual de Políticas, Procedimientos y Contramedidas.

Evidencia de Entrega del Manual al Director de Recursos Humanos:

Gráfico 6.10. Entrega de Manual 1

Gráfico 6.11. Entrega de Manual 2

Gráfico 6.12. Entrega de Manual 3

Gráfico 6.13. Entrega de Manual 4

6.7.3. CONCLUSIONES

- La presente investigación ha permitido identificar la efectividad de la extracción de información; tanto a nivel personal como departamental, mediante la aplicación de las técnicas de Ingeniería Social afirmando que las debilidades humanas son un gran riesgo a nivel de Seguridad Informática.

- Al realizar la investigación sobre las vulnerabilidades humanas referentes a la Seguridad Informática, ayudó a las personas a conocer sobre este tipo de ataques y analizar que los ataques para la realización de fraude informático no se limita únicamente a tecnologías de información sino que puede afectar tanto a usuarios como sistemas de información en general.

- La generación de un documento que permita conocer los procesos para minimizar los ataques enfocados a la vulnerabilidad humana provee al Departamento de Recursos Humanos, una gran herramienta de la cual se pueden desprender nuevos conceptos sobre Seguridad de la Información.

- La utilización de la metodología MAGERIT para la identificación de riesgos tecnológicos ayudó a determinar de una manera minuciosa la existencia de cada una de las vulnerabilidades que el investigador tuvo que determinar mediante el desarrollo de algunas técnicas de Ingeniería Social, para de esta manera realizar los controles necesarios para mitigar y minimizar el riesgo y así salvaguardar la confidencialidad, integridad y disponibilidad de la información.

- Se concluye que la única manera de combatir los ataques informáticos referentes a las vulnerabilidades humanas es la educación de los usuarios, para generar una cultura de concientización y seguridad en la relación establecida entre usuario y máquina.

6.7.4. RECOMENDACIONES

- Realizar la socialización del manual, el cual reposa en el Departamento de Recursos Humanos de la Universidad Técnica de Ambato, para capacitar al personal sobre los principales riesgos a los cuales se encuentran expuestos y dar a conocer los controles, procesos y medidas preventivas a tomar contra los ataques informáticos enfocados a las Vulnerabilidades Humanas.

- Generar una cultura de seguridad de la información a nivel departamental para realizar el control y regularizar el flujo de información, permitiendo clasificarla y salvaguardarla de mejor manera.

- Aplicar los formatos de registro de visitantes a nivel general y para el acceso a cuartos de acceso restringido del Departamento de Recursos Humanos de la Universidad Técnica de Ambato.

7. BIBLIOGRAFÍA

- AGUILERA, Purificación (2010). Seguridad Informática. 22, 10 2011. Disponible y Accesible (http://books.google.com.ec/books?id=Mgvm3AYIT64C&printsec=frontcover&dq=seguridad+informatica&hl=es&ei=-_qiTqv-G8KztwfW_fmlBQ&sa=X&oi=book_result&ct=result&resnum=1&ved=0CDQQ6AEwAA#v=onepage&q&f=false). Seguridad Informática.
- ALEGSA (2009). Diccionario de Informática: Definición de Usuario. 21/03/2012. Disponible y Accesible (http://www.alegsa.com.ar/Dic/usuario.php). Usuario.
- ALEGSA, Diccionario General de Español- Definición de Información 17/12/2010. 28/11/2012 11:46 am. Disponible y accesible (http://www.alegsa.com.ar/Definicion/de/informacion.php). Información.
- ALEGSA, Diccionario General de Español– Definición de módulo (programación). 17/12/2010. 28/11/2012 11:46 am. Disponible y accesible (http://www.alegsa.com.ar/Dic/modulo.php). Módulos del Sistema.
- ÁLVAREZ, Martín (2006). Manual para Elaborar Manuales de Políticas y Procedimientos. 09/03/2012. Disponible y accesible (http://books.google.com.ec/books?id=YnhdFdUDnVIC&printsec=frontcover&dq=manual+de+politicas&hl=es&sa=X&ei=KkNnT82oJKj-sQKW0cS2Dw&ved=0CC0Q6AEwAA#v=onepage&q=manual%20de%20politicas&f=false). Manual de Políticas y Procedimientos.
- AMUTIO GÓMEZ, Miguel Ángel (Octubre 2012). Magerit v.3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I – Método, Libro II- Catalogo de Elementos, Libro III- Guía de Técnicas. 15/11/2012. Disponible y Accesible (http://administracionelectronica.gob.es/?_nfpb=true&_pageLabel=

P800292251293651550991&langPae=es&detalleLista=PAE_1276529683497133). Metodología de Magerit

- ANÓNIMO (Abril 2004). Amenazas Tecnológicas. 21, 10, 2011; Disponible y accesible (http://cidbimena.desastres.hn/docum/crid/Abril2004/pdf/spa/doc10869/doc10869-a.pdf). Amenazas Tecnológicas y Vulnerabilidad.
- ANÓNIMO (desconocido). Definición de Manual. 04/02/2012. Disponible como una definición y accesible (http://www.definicion.org/manual). Manual.
- ANÓNIMO (desconocido). Definición de manual de políticas. 09/03/2012. Disponible y accesible (http://www.mitecnologico.com/Main/ManualesDePoliticas). Manual de Políticas.
- ANÓNIMO (desconocido). Definición de Proceso. 29, 10, 2012. Accesible y Disponible (http://www.definicionabc.com/general/proceso.php). Proceso
- ANÓNIMO, Medios Magnéticos. No disponible, 28/11/2012 11:56 am. Disponible y accesible (http://www.cavsi.com/preguntasrespuestas/que-son-medios-magneticos/). Medios Magnéticos.
- ANÓNIMO, Seguridad Física. No disponible, 28/11/2012 11:04 am. Disponible y accesible (http://www.uv.es/~sto/cursos/icssu/html/ar01s04.html). Acceso Físico.
- ANÓNIMO. Vulnerabilidad. 27, 10, 2011; Solamente páginas seleccionadas 4-6 disponible (http://www.cne.go.cr/CEDO-CRID/CEDO-CRID%20V4/pdf/spa/doc1420/doc1420-1d.pdf). Vulnerabilidad tecnológica.
- CAIRE, Ramiro (Junio 2010). AltoSecBlog 25, 09, 2012; Disponible y Accesible (http://blog.altosec.com.ar/2009/06/ingenieria-social-moderna/). Contramedidas de Seguridad.
- CISTERNA, Miguel (Enero 2011). InfoWeek On Line - Contramedidas de Seguridad para la Ingeniería Social. 25, 09,

2012; Disponible y Accesible (http://www.infoweek.biz/la/2011/01/contramedidas-de-ingenieria-social). Contramedidas de Ingeniería Social.

- CLEARSWIFT, Fuga de Información: la amenaza invisible. 04,01,2012; Archivo descargable PDF disponible (http://www.google.com.ec/url?sa=t&rct=j&q=tipos+de+fuga+de+informaci%C3%B3n+&source=web&cd=5&ved=0CDcQFjAE&url=http%3A%2F%2Fwww.inteco.es%2Ffile%2FU9sVYROlKPh506ZWcHTKRg&ei=MiYGT5iZKYiJtwfHm5zQBg&usg=AFQjCNEFlAUP-QzDzbP9ri6rvIBRxFkleQ). Fuga de Información y Tipos de Fuga.
- DEFINCIÓN.DE. Definición de Dato. No disponible. 28/11/2012 11:25 am. Disponible y accesible (http://definicion.de/datos/). Datos
- DEFINCIÓN.DE. Definición de Dispositivos de Almacenamiento. No disponible. 28/11/2012 11:44 am. Disponible y accesible (http://definicion.de/dispositivos-de-almacenamiento/). Dispositivos de Almacenamiento.
- DEFINCIÓN.DE. Definición de Documentos. No disponible. 28/11/2012 11:44 am. Disponible y accesible (http://definicion.de/documento/). Documentos.
- DEFINCIÓN.DE. Definición de Módulos. No disponible. 28/11/2012 11:59 am. Disponible y accesible (http://definicion.de/modulo/). Módulos del Sistema.
- DEFINCIÓN.DE. Definición de Política. No disponible. 28/11/2012 11:59 am. Disponible y accesible (http://definicion.de/politica/). Política.
- DEFINICIÓN.DE, Definición de Usuario. 21/03/2012; Disponible y Accesible (http://definicion.de/usuario/). Usuario.
- DEFINICIÓN.ORG, Definición de Acceso. 21/03/2012; Página Web Disponible y Accesible (http://www.definicion.org/acceso). Acceso.
- DÍAZ MONTENGERO QUIESNEL, Silvia (Junio 2009). Metodología de Definición de Procesos. 25, 10, 2012. Accesible y Disponible

(http://oa.upm.es/1698/1/PFC_SYLVIA_DIAZ_MONTENEGRO_QUESNEL_SH.pdf). Tipos de Procesos.

- ESPASA, Calpe. Diccionario de la Lengua Española – Salvaguardar. 2005. 28/11/2012 12:15 pm. Disponible y accesible (http://www.wordreference.com/definicion/salvaguardar). Salvaguardar.
- ESTRUCPLAN (2000). Políticas de la Empresa: ¿para qué sirven? 22, 03, 2012; Disponible y accesible (http://www.estrucplan.com.ar/Articulos/verarticulo.asp?IDArticulo=375). Políticas.
- INTERBUSCA, Código ASCII, No disponible, 28/11/2012 11:12 am. Disponible y accesible (http://antivirus.interbusca.com/glosario/ASCII.html). Caracteres Especiales.
- MasAdelante.com. ¿Qué es un disco Duro? - Definición de un Disco Duro. No disponible, 28/11/2012 11:43 am. Disponible y Accesible (http://www.masadelante.com/faqs/disco-duro). Disco Duro.
- MARCO GALINDO, María Jesús; MARCO SIMÓ, Josep María; PRIETO BLÁZQUEZ, Josep; "et al". (2010). Escaneando al Informática. 22,10,2011. Páginas bloqueadas y accesible (http://books.google.com.ec/books?id=svpzjkMpdiUC&pg=PA15&dq=que+es+la+inform%C3%A1tica&hl=es&ei=vOmiTsLxN8aEtgfkoPCoBQ&sa=X&oi=book_result&ct=result&resnum=1&ved=0CCsQ6AEwAA#v=onepage&q=que%20es%20la%20inform%C3%A1tica&f=false). Informática.
- MIERES, Jorge (2009). Ataques Informáticos: Debilidades de seguridad Comúnmente explotadas. 27, 10,2011. Disponible y accesible (https://www.evilfingers.com/publications/white_AR/01_Ataques_informaticos.pdf). Ataques informáticos e Ingeniería Social.
- NEPOMUCENO, Ángel; QUESADA, José F.; SALGUERO Francisco (2001). Información: Tratamientos y representación. 22, 10,2011. Páginas bloqueadas y accesible (http://books.google.com.ec/books?id=Q1BSlLveu7wC&printsec=

frontcover&dq=informaci%C3%B3n&hl=es&ei=tQOjTpb2GMaWtwf0wKCUBQ&sa=X&oi=book_result&ct=result&resnum=1&ved=0CCsQ6AEwAA#v=onepage&q&f=false). Información.

- NETMEDIA (Noviembre 2011). Ingeniería Social: el arte de hacernos mensos (segunda parte). 25, 09, 2012. Accesible y disponible (
- http://www.bsecure.com.mx/opinion/ingenieria-social-el-arte-de-hacernos-mensos-segunda-parte/). Fundamentos de la Ingeniería Social.
- PALMA, José (2006). Manual de procedimiento. 04/02/2012. Disponible y accesible (http://www.monografias.com/trabajos13/mapro/mapro.shtml). Manual de Procedimientos.
- PERGAMINOVIRTUAL. Definición Password. No disponible, 28/11/2012 12:08 am. Disponible y Accesible (http://www.pergaminovirtual.com.ar/definicion/Password.html). Password.
- REVISTA RED (2002). Seguridad Informática ¿Qué, Por Qué y Para Qué? 28, 10, 2011. Accesible y disponible (http://www.ciberhabitat.gob.mx/museo/cerquita/redes/seguridad/intro.htm). Seguridad Informática.
- RUIZ OLAYA, Andrés. Implementación de una Red MODBYS/TCP. 2002, 28/11/2012 11:13 am. Disponible y Accesible (http://es.scribd.com/doc/51762490/57/Definicion-de-caracteres-especiales). Caracteres especiales.
- TELLES ARAUJO, Pedro (2010). Seguridad Informática. 22, 10,2011. Disponible y Accesible (http://www.slideshare.net/Tcherino/seguridad-informatica-3143924). Seguridad Informática.
- OLMEDO, José Joaquín-Hermoso; MONTERO NAVARRO, Antonio; MARTÍN, Santiago; "et al". (2000). Informática Aplicada a la Gestión de Empresas. 22, 10, 2011. Páginas bloqueadas y accesible (http://books.google.com.ec/books?id=nrXvTg2nNroC&pg=PA9&

dq=inform%C3%A1tica&hl=es&ei=KtWiToTcFsjngQfs6um7BQ&sa=X&oi=book_result&ct=result&resnum=3&ved=0CDwQ6AEwAg#v=onepage&q&f=false). Informática.

- PACHECO, Federico. Fuga de información: ¿una amenaza pasajera? 28, 10, 2011. Disponible y accesible (http://www.eset-la.com/pdf/prensa/informe/fuga_de_informacion.pdf). Información confidencial y Amenazas Tecnológicas.
- RUIZ, Fernando (Agosto 2010). Simbología de los Diagramas de Flujo. 25, 10, 2012. Accesible y disponible (http://es.scribd.com/doc/36469069/SIMBOLOGIA-DIAGRAMAS-DE-FLUJO). Simbología de Diagramación.
- UTA. Estatuto de la Universidad Técnica de Ambato. 22, 03, 2012. Disponible y accesible (http://www.uta.edu.ec/v2.0/pdf/estatuto.pdf). Director de Recursos Humanos.
- WIKIPEDIA, Confidencialidad. 24/08/2012. 28/11/2012 11:20 am. Disponible y Accesible (http://es.wikipedia.org/wiki/Confidencialidad). Confidencialidad.
- WIKIPEDIA (Octubre 2012). Diagrama de Flujo. 29, 10, 2012. Disponible y Accesible (http://es.wikipedia.org/wiki/Diagrama_de_flujo). Diagramas de Procesos.
- WIKIPEDIA, Disco Duro. 18/05/2011. 28/11/2012 11:41 am. Disponible y Accesible (http://es.wikipedia.org/wiki/Disco_duro). Disco Duro.
- WIKIPEDIA (2011). Ingeniería Social (seguridad informática). 27, 10,2011. Disponible y accesible (http://es.wikipedia.org/wiki/Ingenier%C3%ADa_social_(seguridad_inform%C3%A1tica). Ingeniería Social.
- WIKIPEDIA, Intranet. 19/02/2008. 28/11/2012. Disponible y accesible (http://es.wikipedia.org/wiki/Intranet). Intranet.
- WIKIPEDIA (2011).Manual de procedimientos. 04/02/2012. Disponible y accesible

(http://es.wikipedia.org/wiki/Manual_de_procedimientos). Manual de procedimientos.

- WIKIPEDIA, Política. 18/06/2010. 28/11/2012 12:11 pm. Disponible y Accesible (http://es.wikipedia.org/wiki/Pol%C3%ADtica). Políticas.
- WIKIPEDIA (Octubre 2012). Proceso (Informática). 29, 10, 2012. Disponible y Accesible (http://es.wikipedia.org/wiki/Procesos). Procesos.

Referencias:

1. BISCIONE, Carlos A. Ingeniería Social para No Creyentes. 28, 10, 2011. Disponible y accesible (http://www.acis.org.co/fileadmin/Base_de_Conocimiento/V_Jornada_de_Seguridad/IngenieraSocial_CarlosBiscione.pdf). Ingeniería Social.
2. EMM, David (2010). Arreglando las vulnerabilidades humanas. 22,10, 2011. Disponible y accesible (http://www.viruslist.com/sp/analysis?pubid=207271063). Vulnerabilidad humana y Amenazas. Help Net Security (2011). Estadísticas de Amenazas. 15, 10,2011. Disponible y accesible (http://www.net-security.org/secworld.php?id=11665&utm_source=Help+Net+Security+Daily+News&utm_campaign=bf208140c5-RSS-hns&utm_medium=email).

ANEXOS

Anexo 1. Modelo de Encuesta aplicada al Personal del Departamento de Recursos Humanos de la UTA:

UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL

Departamento de Recursos Humanos de la Universidad Técnica de Ambato

Objetivo: La presente encuesta como fin conocer los tipos de amenazas informáticas a las que el personal se encuentra expuesto.

Señores, su veracidad en las respuestas permitirá al investigador desarrollar un trabajo real y efectivo.

Agradezco su colaboración y garantizó absoluta reserva de su información.

CUESTIONARIO

1. ¿Conoce sobre los ataques de Ingeniería Social?
    - Si
    - No
2. ¿Conoce usted cuáles son los procedimientos de seguridad que debe seguir en caso de que exista un ataque informático o de Ingeniería Social dentro del departamento?
    - Si
    - No
3. ¿Cree usted que la tecnología y los equipos tecnológicos que existen dentro del departamento son suficientemente seguros y no sufrirán un ataque de Ingeniería Social?
    - Si
    - No

4. Para el acceso a su computadora destinada para sus labores diarias en su lugar de trabajo, utiliza usted:
    - Contraseña de Seguridad
    - No existe ningún tipo de restricciones para el acceso
    - Necesita un administrador para el acceso
5. ¿Cree usted que se encuentra propenso a algún tipo de ataque de Ingeniería Social?
    - Si
    - No
6. ¿Utiliza usted una misma contraseña se seguridad para acceder a todas sus cuentas personales?
    - Si
    - No
7. ¿Ha compartido alguna vez su contraseña con alguna persona de su confianza?
    - Si
    - No
8. ¿Qué parámetros utiliza en su contraseña?
    - Número
    - Letras Minúsculas
    - Letras Mayúsculas
    - Símbolos o Caracteres especiales
9. En su clave de seguridad utiliza:
    - Nombres
    - Apellidos
    - Fechas Importantes
    - Placa de Auto
    - Número de Cédula
10. ¿Alguna vez ha sido víctima de algún robo informático?
    - Si
    - No

11. ¿Se utiliza algún tipo de seguridad física para los visitantes cuando ingresan al departamento o las instalaciones?
    - Si
    - No
12. ¿Con qué frecuencia reciben a las personas dentro del departamento?
    - Muy Frecuente
    - Frecuente
    - Poco Frecuente
13. ¿Según su criterio como clasificaría usted la importancia de la información que maneja?
    - Muy Importante
    - Importante
    - Medianamente Importante
    - Poco Importante

Gracias por su colaboración

Firma:……

Fecha:……

Investigador: Gabriela Cortez

Anexo 2. Modelo de Encuesta aplicada al Administrador del Sistema

UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL

Departamento de Recursos Humanos de la Universidad Técnica de Ambato

Objetivo: La presente encuesta tiene como fin conocer los tipos de amenazas informáticas a las que el personal se encuentra expuesto.

CUESTIONARIO

1. ¿Qué tipo de sistema se utiliza dentro del departamento de RRHH de la UTA?
    - Contable
    - Transaccional
    - Apoyo a las Decisiones
    - Control de Personal
    - Información
2. ¿Cómo se encuentra actualmente el sistema?
    - Funcional
    - Necesita actualizaciones
    - Poco Funcional
3. ¿Qué tipo de información se maneja en el departamento?
    - Información de Docentes
    - Financiera
    - De Estudiantes
    - De Proyectos
    - Otro Cuál?.....

4. ¿La información del departamento es considerada importante?
    - Si
    - No
5. ¿La información es guardada de manera física?
    - Si
    - No
6. ¿Se realizan respaldos de la información?
    - Si
    - No
7. ¿Con que frecuencia se realizan los respaldos?
    - Diariamente
    - Semanalmente
    - Mensualmente
    - Semestralmente
    - Anualmente
8. ¿Se han registrado ataques informáticos dentro del departamento?
    - Si
    - No
9. ¿Existen seguridades aplicadas dentro del departamento?
    - Si
    - No

Gracias por su colaboración

Firma:……

Fecha:……

Investigador: Gabriela Cortez

Anexo 3. FORMATO DE CONTROL DE VISITANTES AL DEPARTAMENTO DE RECURSOS HUMANOS DE LA UNIVERSIDAD TÉCNICA DE AMBATO

FORMATO DE CONTROL DE INGRESO DE VISITANTES

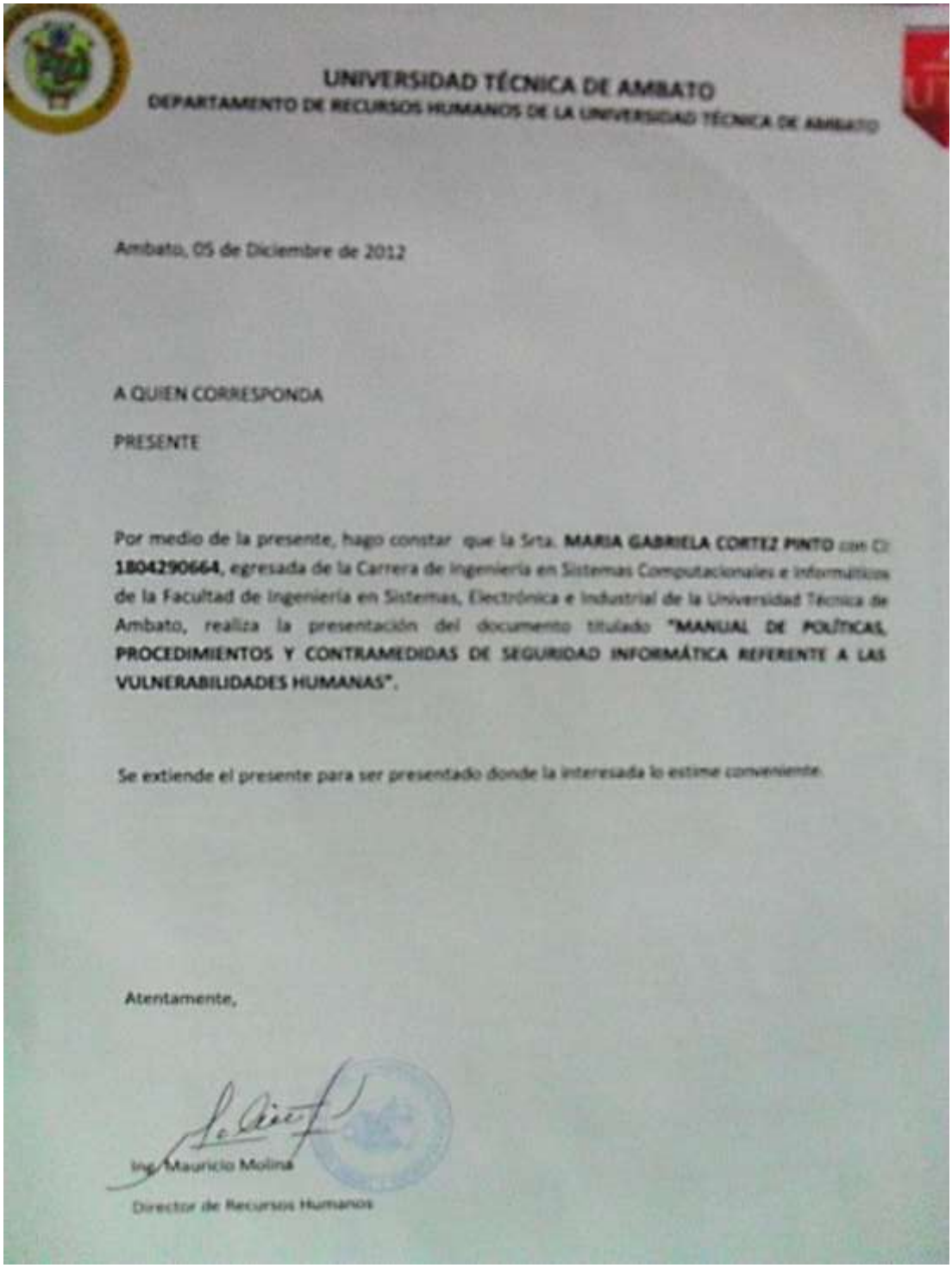
NOMBRE	IDENTIFICACIÓN	MOTIVO	INGRESO	SALIDA	FIRMA

Anexo 4. FORMATO DE CONTROL DE INGRESOS A CUARTO DE ACCESO RESTRINGIDO

FORMATO DE CONTROL DE INGRESO A CUARTO DE ACCESO NO AUTORIZADO

NOMBRE	IDENTIFICACIÓN	MOTIVO	INGRESO	SALIDA	FIRMA	AUTORIZADO POR

Anexo 5. Solicitud de Presentación del Manual de Políticas, Procedimientos y Contramedidas de Seguridad Informática referente a las Vulnerabilidades Humanas.



UNIVERSIDAD TÉCNICA DE AMBATO

DEPARTAMENTO DE RECURSOS HUMANOS DE LA UNIVERSIDAD TÉCNICA DE AMBATO

Ambato, 05 de Diciembre de 2012

A QUIEN CORRESPONDA

PRESENTE

Por medio de la presente, hago constar que la Srta. **MARIA GABRIELA CORTEZ PINTO** con CI **1804290664**, egresada de la Carrera de Ingeniería en Sistemas Computacionales e Informáticos de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial de la Universidad Técnica de Ambato, realiza la presentación del documento titulado **"MANUAL DE POLÍTICAS, PROCEDIMIENTOS Y CONTRAMEDIDAS DE SEGURIDAD INFORMÁTICA REFERENTE A LAS VULNERABILIDADES HUMANAS"**.

Se extiende el presente para ser presentado donde la interesada lo estime conveniente.

Atentamente,

Ing. Mauricio Molina

Director de Recursos Humanos