UNIVERSIDAD TÉCNICA PARTICULAR DE LOJA

La Universidad Católica de Loja

TITULACIÓN DE INGENIERO EN INFORMÁTICA

Estudio de Ingeniería Social y su nivel de incidencia en instituciones públicas y privadas de la ciudad de Cariamanga

Trabajo de fin de titulación

AUTORA: Jaramillo Condolo Diana del Rocío

DIRECTORES: Calva Cuenca Daniela Yadira, Ing.

Jaramillo Hurtado Danilo Rubén, Ing.

CENTRO UNIVERSITARIO CARIAMANGA

2013

CERTIFICACIÓN

Ingeniera.

Daniela Yadira Calva Cuenca.

DIRECTORA DEL TRABAJO DE FIN DE TITULACIÓN

C E R T I F I C A:

Que el presente trabajo, denominado: **"**Estudio de Ingeniería Social y su Nivel de Incidencia en las Organizaciones Públicas y Privadas de la Ciudad de Cariamanga**"** realizado por la profesional en formación: Jaramillo Condolo Diana del Rocío; cumple con los requisitos establecidos en las normas generales para la Graduación en la Universidad Técnica Particular de Loja, tanto en el aspecto de forma como de contenido, por lo cual me permito autorizar su presentación para los fines pertinentes.

Loja, Abril del 2013

. . . . . .

Ing. Daniela Calva
DIRECTORA DE TESIS

CERTIFICACIÓN

Ingeniero.

Danilo Rubén Jaramillo Hurtado.

DIRECTOR DEL TRABAJO DE FIN DE TITULACIÓN

C E R T I F I C A:

Que el presente trabajo, denominado: **"**Estudio de Ingeniería Social y su Nivel de Incidencia en las Organizaciones Públicas y Privadas de la Ciudad de Cariamanga**"** realizado por la profesional en formación: Jaramillo Condolo Diana del Rocío; cumple con los requisitos establecidos en las normas generales para la Graduación en la Universidad Técnica Particular de Loja, tanto en el aspecto de forma como de contenido, por lo cual me permito autorizar su presentación para los fines pertinentes.

Loja, Abril del 2013

. . . . . .

Ing. Danilo Jaramillo
DIRECTOR DE TESIS

CESIÓN DE DERECHOS

"Yo, Jaramillo Condolo Diana del Rocío, declaro ser autora del presente trabajo y eximo expresamente a la Universidad Técnica Particular de Loja y a sus representantes legales de posibles reclamos o acciones legales.

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

.....

Autora: Jaramillo Condolo Diana del Rocío

Cédula: 1104613946

DEDICATORIA

Este trabajo va dedicado para las personas más importantes en mi vida, la cuales de cierta forma han estado en las buenas y en las malas junto a mí, aportando con un granito de arena para poder llegar a la meta.

Principalmente se lo dedico de manera especial a mis padres y hermanos quienes son mi fortaleza y motor de vida.

Diana.

AGRADECIMIENTO

Ante todo a Dios, por haberme dado la salud física y mental necesaria para culminar con mis estudios superiores.

A la Universidad Técnica Particular de Loja que por medio dela Escuela de Ciencias de la Computación, que me dio la oportunidad de formarme y preparar la presente investigación.

Así mismo, un profundo reconocimiento de gratitud a los ingenieros Daniela Calva, Directora de Tesis y Danilo Jaramillo, Codirector de Tesis, por haberme brindado su apoyo, dirección y conocimientos durante todo el desarrollo y ejecución del trabajo de investigación.

A todos mis maestros que generosamente me han impartido sus sabios conocimientos.

A mis Padres y hermanos por su apoyo y confianza depositada en mí durante mi carrera universitaria, sobre todo a las palabras sabias que me han iluminado en el periodo de estudio.

Diana.

ÍNDICE DE CONTENIDOS

ÍNDICE DE CUADROS

ÍNDICE DE FIGURAS

ÍNDICE DE GRÁFICOS

RESUMEN EJECUTIVO

La presente investigación trata sobre Ingeniería Social, técnicas y el impacto que estas pueden causar en nuestra sociedad, para tal efecto se procedió a investigar a cinco instituciones de la ciudad de Cariamanga.

Haciendo uso de técnicas de recolección de información en este caso entrevistas, encuestas y observación directa, se ha determinado cuál es el estado actual de las instituciones y así saber con qué tipo de información trabajan, que sistemas informáticos manipulan, cuales son las áreas más vulnerables, etc. A través de la utilización de herramientas informáticas se determinaron las principales vulnerabilidades existentes en los sistemas informáticos y en las redes de datos de cada institución, además se procedió a elaborar políticas de seguridad tomando en consideración las vulnerabilidades y soluciones planteadas en las diferentes instituciones investigadas.

Cabe recalcar que este plan de mejoramiento será presentado al director y gerente de cada institución para su respectiva implementación, así mismo se realizaron jornadas de capacitación a todo el personal de las instituciones investigadas de la ciudad de Cariamanga, con la finalidad de dar a conocer y concientizar sobre los ataques de Ingeniería Social.

OBJETIVOS

Objetivo general

Determinar el nivel de seguridad que tienen las Instituciones públicas y privadas de la ciudad de Cariamanga, con respecto a ataques de Ingeniería Social.

Objetivos específicos

- Analizar las principales técnicas de ataques de Ingeniería Social más frecuentes en la actualidad.
- Conocer que tan vulnerables son las Instituciones de la ciudad de Cariamanga con respecto a los ataques de Ingeniería Social.
- Establecer formas de protección ante las diferentes técnicas de ataque de Ingeniería Social y su difusión a cada una de las instituciones investigadas.
- Especificar políticas de seguridad, las mismas que serán presentadas a las autoridades de las Instituciones investigadas.
- Impartir capacitaciones sobre Ingeniería Social, a los directivos y empleados de las Instituciones investigadas.

CAPITULO I

Introducción a la Ingeniería Social – Estado del Arte

1.1. INTRODUCCIÓN

En la presente investigación se analizarán, casos reales de Ingeniería Social en Instituciones públicas y privadas de la ciudad de Cariamanga, herramientas para combatir el robo de información, leyes que amparan la seguridad informática, planes de seguridad para evitar ser víctimas de Ingenieros Sociales y así mismo se plantearán conclusiones y recomendaciones referentes a la seguridad de la información.

La Ingeniería Social es la forma de obtener información confidencial o sensible de una determinada institución u organismo, además, cabe mencionar que la Ingeniería Social está orientada básicamente en la manipulación de la gente, a través de medios informáticos, sistemas automatizados, telecomunicaciones, etc. Tomando como referencia la publicación realizada en el sitio web Magazcitum [1], se concluye que en la actualidad existen diferentes tipos de ataques asociados al robo de Información, de los cuales a continuación se mencionan los más utilizados:

1.1.1. Ataque tecnológico: Obtención de información a través de medios tecnológicos, como correo electrónico, suplantación de servicios y servidores, medios impresos.

1.1.2. Ataque personal: La persona es engañada para revelar información confidencial, a través de falsos argumentos lo cual demanda cierto sentido de responsabilidad o urgencia.

1.1.3. Ataque sofisticado: Es una combinación de los dos anteriores. Se puede utilizar la tecnología para obtener la información, a través de amigos, compañeros de la víctima, grupos sociales, Web Social, etc. Y después presentar esta información a la víctima, para crear una atmosfera de conocimiento y confianza.

1.2. ANÁLISIS DE INGENIERÍA SOCIAL Y SUS INCIDENCIAS

Actualmente todas las empresas ya sean públicas o privadas, cuentan con infraestructura de última tecnología y personal altamente calificado, lo que hace que tanto la información como cada uno de los procesos que se realizan en la empresa estén seguros y salvaguardados.

Sin embargo la información de las empresas, instituciones u organizaciones están expuestas a un sin número de métodos, técnicas y herramientas que pueden ser utilizadas por un atacante informático para obtener información confidencial y utilizarla a beneficio propio.

Es un error común, pensar que para acceder a un sistema informático u obtener información confidencial de una empresa en particular, es necesario poseer grandes conocimientos técnicos e informáticos. Al contrario, únicamente se requiere astucia, paciencia, habilidades sociales y una buena dosis de psicología, esta técnica es la llamada Ingeniería Social, la cual pretende engañar a los usuarios con el fin de obtener información confidencial. Para una mejor comprensión sobre la definición de Ingeniería Social, a continuación se mencionan conceptos sobre este tema.

Wikipedia define a la Ingeniería Social como:

> “Ingeniería Social es 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 riesgo o abusos” [2].

Definición publicada en Alegsa Diccionario Informático:

> "Ingeniería social es persuadir o manipular a una persona para obtener datos útiles sobre ellos mismos o las empresas en donde trabajan. Suelen utilizarse métodos de engaños para obtener contraseñas o información útil. Pueden emplearse páginas web falsas, programas engañosos o incluso simplemente chatear con una persona ignorante del tema. Increíblemente, la mayoría de las personas son lo suficientemente ilusas como para dar contraseñas a un extraño" [3].

Tomando como referencia las definiciones antes mencionada se puede concluir, que la Ingeniería Social es una técnica eficaz en el robo de información confidencial en instituciones públicas o privadas, robro de contraseñas a personas naturales, suplantación de identidad, información de tarjetas de crédito, etc.

Los atacantes de Ingeniería Social se basan en maniobras y trucos para obtener información sensible de otros usuarios, por ejemplo, mirar por encima del hombro del usuario, enviar correos electrónicos con links maliciosos, mediante llamadas telefónicas o mediante mensajes de texto. A continuación se mencionan algunos ejemplos y técnicas que un Ingeniero Social utiliza para obtener información sin que el usuario se dé cuenta:

- Los Ingenieros Sociales se hacen pasar por empleados de otros departamentos, proveedor de servicios informáticos, operador de telefonía o de acceso a internet.
- A través de una llamada telefónica de un presunto investigador o agente de policía que solicita la contraseña de un empleado para poder llevar a cabo una determinada investigación en la empresa.
- Un supuesto técnico que solicita permiso a un empleado para reparar su ordenador y remplazar el disco duro por otro que trae consigo.

- Correos electrónicos que suplantan la identidad de otra persona u organización, o que incluyen textos o ficheros adjuntos a modo de reclamo.
- Usuarios que utilizan foros y chats en internet para poder tener acceso a determinados ficheros sensibles del sistema.
- Espionaje a los usuarios para obtener su nombre de usuario y contraseña, mediante la observación directa de lo que teclean en el ordenador (técnica de "mirar por encima del hombro").
- Revisar papeles o documentos de la basura y que no son destruidos por completo.
- Puesta en marcha de Websites[1] maliciosos que tratan de engañar a sus usuarios. [4]

Estos son algunos ejemplos que podemos mencionar, los mismos que son utilizados por los atacantes para engañar a los diferentes usuarios. Además es importante destacar la asombrosa facilidad con la que los usuarios de sistemas informáticos y empleados de otras áreas pueden revelar contraseñas o datos sensibles, ya que la mayoría de las veces actúan por ayudar de buena fe, por temor, por codicia o simplemente por cortesía.

Lo cierto es que la Ingeniería Social triunfa como técnica de ataque informático, porque aún no estamos bien capacitados para defender nuestro desempeño y funciones laborales a la hora de presentarse esta técnica de engaño ya sea de forma física o vía internet.

La presente investigación se centra básicamente en determinar cuáles son las instituciones y áreas más propensas a ser víctimas de ataques informáticos; analizar las principales técnicas de ataque utilizadas actualmente por los Ingenieros Sociales, establecer vulnerabilidades y

[1]**Website:** Página web o sitio web registrado en Internet

casos de Ingeniería Social en cada una de las instituciones investigadas, esto a través de herramientas informáticas, las mismas que se describen a continuación:

1.2.1. Nessus: "Sirve para detectar a través de la red vulnerabilidades en un sistema remoto, ya sea un cliente o servidor. También detecta vulnerabilidades del software instalado" [5].

1.2.2. WhoReadMe.- "Es un servicio gratuito online, sirve para saber si los e-mails que se envía son leídos por su destinatario. Sencillamente lo que hace es un seguimiento de los mensajes enviados y nos avisa a través de alertas si un mail que ha sido enviado ha sido leído. Esta herramienta informa sobre la IP del destinatario, su sistema operativo, browser, etc." [6].

1.2.3. PasswordMeter: "Es una utilidad para medir la fuerza de una contraseña que se desea usar en algún sitio web. A medida que se va escribiendo, se visualiza la fuerza de la contraseña, la cual se basa en una serie de atributos clave, con puntaje positivo o negativo. La prueba mide el número de los caracteres de la contraseña, el tipo de caracteres utilizados, y el orden (letras o números secuenciales, por ejemplo, es igual a contraseñas débiles)" [7].

1.3. ANÁLISIS DE TÉCNICAS UTILIZADAS POR ATACANTES INFORMÁTICOS

En la actualidad existen diversas técnicas de Ingeniería Social, pero en esta investigación únicamente nos centraremos en las más utilizadas por los atacantes informáticos, las mismas que se describen a continuación:

1.3.1. Ataque a la persona en forma directa

La víctima es inducida a permitir acciones o a confiar en la información que el atacante le dice con argumentos válidos o demandas, con cierto sentido de responsabilidad o urgencia. Por ejemplo, suplantación de identidad, engaño telefónico, abuso de confianza, visibilidad del entorno de la víctima, ignorancia, etc. El contacto personal es el método más difícil para la obtención de información, ya que el atacante deberá tener el conocimiento de su objetivo, la habilidad y conducta adecuada para no despertar sentimientos de incertidumbre y desconfianza en la victima. A continuación se describen las principales técnicas en forma directa que los Ingenieros Sociales utilizan:

- **Suplantación de identidad.-** La suplantación de identidad adopta muchas formas para engañar a usuarios y convertirlos en sus víctimas. Los atacantes pueden suplantar a miembros de otros departamentos o de empresas asociadas, con la finalidad de ingresar a las áreas más vulnerables de las instituciones y así tener acceso a los sistemas e información confidencial.

- **Observación directa.-** Quizá sea un ataque muy simple pero es muy efectivo, observar el entorno y aprovechar los datos

que están a la vista cuando el sentido común indica que deberían guardarse en un lugar seguro, por ejemplo:

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

- **Surf Hombro.-** El mirar por encima del hombro de una persona es considerado uno de los principales ataques realizados por los Ingenieros Sociales.

  Existen algunas variaciones que permiten apropiarse de información de manera ilícita, como por ejemplo:

  - Usando binoculares o un telescopio de baja potencia para ver quién digita código PIN[2].
  - Recubrimiento del teclado con una fina capa de material ultravioleta de forma que posteriormente puede ver qué teclas pulsa el usuario.
  - Escuchar a un usuario las pulsaciones en el teclado de su contraseña, permitiendo buscar cuantos caracteres pueda poseer su contraseña.

1.3.2. Ataques tecnológicos

Se obtiene información a través de la infraestructura y medios tecnológicos, como correo electrónico, suplantación de servicios y servidores, medios impresos, etc. A continuación se describen las técnicas de ataque más utilizadas por los Ingenieros Sociales haciendo uso de la tecnología:

[2] **PIN.** Número de identificación de la persona

"**Phishing.-** Es un engaño dañino y eficaz, utilizado siempre para fines delictivos. Básicamente consiste en algún e-mail que procede al parecer de un negocio o empresa legítima y digna de confianza (un banco o compañía de crédito) solicitando "verificación" de los datos y advirtiendo sobre consecuencias que traerían si no se hiciera dicha verificación.

Malware.- Programa diseñado para hacer algún daño a un sistema, puede presentarse en forma de virus, gusanos, caballos de Troya, etc., esta técnica de ataque se ejecuta automáticamente sin consentimiento ni conocimiento de la víctima.

Keylogger.- Es un programa que registra y graba la pulsación de teclas y clic del mouse. La información recolectada será utilizada luego por la persona que lo haya instalado. Actualmente existen dispositivos de hardware y aplicaciones (software) que realizan estas tareas.

Sniffing.- Se realiza cuando una persona con conocimientos técnicos accede sin autorización a sistemas y captura paquetes de información que circulan por la red. Al utilizar esta técnica se puede averiguar contraseñas e información confidencial de personas y organizaciones" [8].

Además de las técnicas antes mencionadas, también los Ingenieros Social recolectan información confidencial buscando documentos en la basura los mismos que no han sido destruidos por completo, los cuales suelen contener contraseñas, directorios telefónicos internos, organigramas, memorandos, agendas ejecutivas de eventos o vacaciones, listado de programas (código fuente[3]), impresión de datos sensibles y confidenciales, etc.

[3] **Código Fuente:** Conjunto de instrucciones que debe seguir la computadora para ejecutar un programa. Por lo tanto, en el código fuente de un programa está descrito por completo su funcionamiento.

Las principales técnicas de Ingeniería Social que se van a evaluar en las Instituciones de la ciudad de Cariamanga y herramientas a utilizar, son las que se muestran en el siguiente cuadro:

INSTITUCIÓN	ÁREAS A INVESTIGAR	TÉCNICA A UTILIZAR	HERRAMIENTA A UTILIZAR
Institución Educativa	Secretaría DOBE	Suplantación de identidad (ítem 2.1.1) Observación Robo de información a través del correo electrónico (Phishing), (ítem 2.1.2)	Habilidad y conocimientos de suplantación (ítem 2.1.1) WhoReadMe (ítem 1.2.1)
Institución Pública	Secretaría Financiero		
Centro de Salud	Estadística		
Institución Comercial	Administrativo		
ONG	Secretaria Proyectos		

Cuadro 1.Técnicas de Ingeniería Social a evaluar

1.4. ESTUDIO DE LEYES EN EL ECUADOR REFERENTE A LA INGENIERÍA SOCIAL

En la actualidad las computadoras se utilizan no solo como herramientas auxiliares de apoyo a diferentes actividades humanas, sino como medio eficaz para obtener y conseguir información, lo que las ubica también como un nuevo medio de comunicación tecnológica. “La humanidad no está frente al peligro de la informática, sino frente a la posibilidad real de que individuos mal intencionados, con aspiraciones de obtener el poder de la información, utilicen la tecnología como medio para satisfacer sus propios intereses, a expensas de las libertades individuales y en quebranto de las personas. Así mismo, la amenaza futura será directamente proporcional a los adelantos de las tecnologías informáticas”. [9]

La protección de los sistemas informáticos puede abordarse tanto desde una perspectiva penal como de una perspectiva civil o comercial, e incluso de derecho administrativo. Estas distintas medidas de protección no tienen por qué ser excluyentes unas de otras, sino que, por el contrario, éstas deben estar estrechamente vinculadas. Por eso, dadas las características de esta problemática sólo a través de una protección global, desde los distintos sectores del ordenamiento jurídico, es posible alcanzar una cierta eficacia en la defensa de los ataques a los sistemas informáticos.

Tomando como referencia el Registro Oficial de la Ley de Comercio Electrónico, publicado en el año 2002 [10], a continuación se mencionan los artículos más relevantes de la reforma del código penal:

1.4.1. Código de Procedimiento Penal

Los delitos que se tipifican, mediante reformas del Código Penal se muestran a continuación en la siguiente tabla:

INFRACCIONES INFORMÁTICAS	REPRESIÓN	MULTAS
Delitos contra la información confidencial (Art. 202 CPP) • Violación de claves o sistemas • Información nacional o secretos comerciales o industriales. • Utilización fraudulenta de la información. • Obtención y uso no autorizado de la información.	6 meses a 1 año 1 año a 3 años 3 años a 6 años 2 meses a 2 años	$500 - $1.000 $1.000 - $1.500 $2.000 - $10.000 $1.000 - $2.000
Destrucción mal intencionada de documentos (Art. 262 CPP)	3 años a 6 años	----
Falsificación electrónica (Art. 353 CPP)	3 años a 6 años	----
Apropiación ilícita (Art. 553 CPP) • Uso fraudulento • Usos de medios (claves, tarjetas magnéticas)	6 meses a 5 años 1año a 5 años	$500 a $1.000 $1.000 a $2.000
Estafa (Art. 563 CPP)	5 años	$500 a $1.000

Cuadro 2. Infracciones informáticas, represión y multas

Es evidente, que la persona que violenta claves, sistemas de seguridad para obtener información, lesiona la intimidad y por consiguiente la confidencialidad de la persona jurídica en muchos casos, es sancionada a través de multas y prisión dependiendo de la magnitud del delito informático. Es por esta razón que los Legisladores, deben estar conscientes que la delincuencia informática avanza con pasos agigantados y que las leyes ecuatorianas deben estar acorde con los avances tecnológicos (Anexo 10).

Es oportuno señalar que la informática, no es sólo un fenómeno científico de carácter personal, por el contrario, los ordenadores al permitir un manejo rápido y eficiente de grandes volúmenes de información facilitan la concentración automática de los datos referidos a las personas, convirtiéndose en un verdadero factor de poder, ante el cual es necesario tener las respectivas protecciones de seguridad.

1.4.2. Ley Orgánica de Transparencia y Acceso a la Información Pública.

"El principio general de la Ley Orgánica de Transparencia y Acceso a la Información Pública es la publicidad de información. Es decir, que toda aquella información que poseen las entidades públicas personas jurídicas de derecho privado en directa relación con el Estado, las organizaciones de trabajadores y entidades del Estado e Instituciones de Educación Media y Superior que reciban fondos estatales, es pública" [15].

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

1.4.3. Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos

Los contratos que se generen y perfeccionen en Ecuador por medios electrónicos a través del intercambio de mensajes de datos o comprando en sitios web en Internet sean válidos y de efectos civiles, comerciales y jurídicos en general, idénticos a los actuales contratos por escrito. Que las firmas electrónicas no son un escaneo de una firma o una foto digital de una firma sino un conjunto de algoritmos que cumplen con ciertos requisitos legales establecidos en la Ley se consideren con igual validez jurídica que las firmas manuscritas [15].

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

1.4.4. Ley Especial de Telecomunicaciones

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

Declara que es indispensable proveer a los servicios de telecomunicaciones de un marco legal acorde con la importancia, complejidad, magnitud tecnología y especialidad de servicios, así como también asegurar una adecuada regulación y expansión de los sistemas radioeléctricos, y servicios de telecomunicaciones a la comunidad que mejore de forma permanente la prestación de los servicios existentes [15].

1.5. ESTUDIO DE CASOS REALES DE INGENIERÍA SOCIAL REGISTRADO EN INTERNET

En el estudio de la Ingeniería Social se ha podido identificar y conocer varios casos sobre ataques utilizando diversas técnicas como, observación, suplantación, correo electrónico, cartas, teléfono y otras más que han permitido revelar información sensible o violar políticas de seguridad. En Internet se han registrado varios casos de usuarios que han sufrido ataques informáticos ya sea por descuido o falta de conocimiento.

En la siguiente figura estadística se muestra un informe sobre los principales ataques de Ingeniería Social que se han presentado en los últimos 2 años a nivel de Latinoamérica.

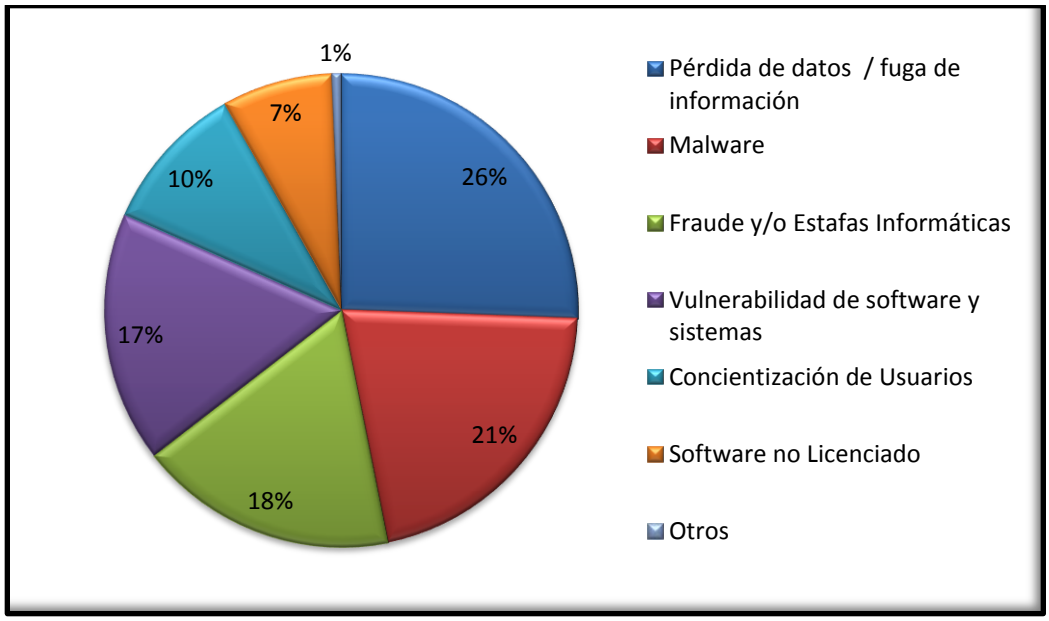


Gráfico 1. Fuente: ESET Security Report Latinoamérica 2011

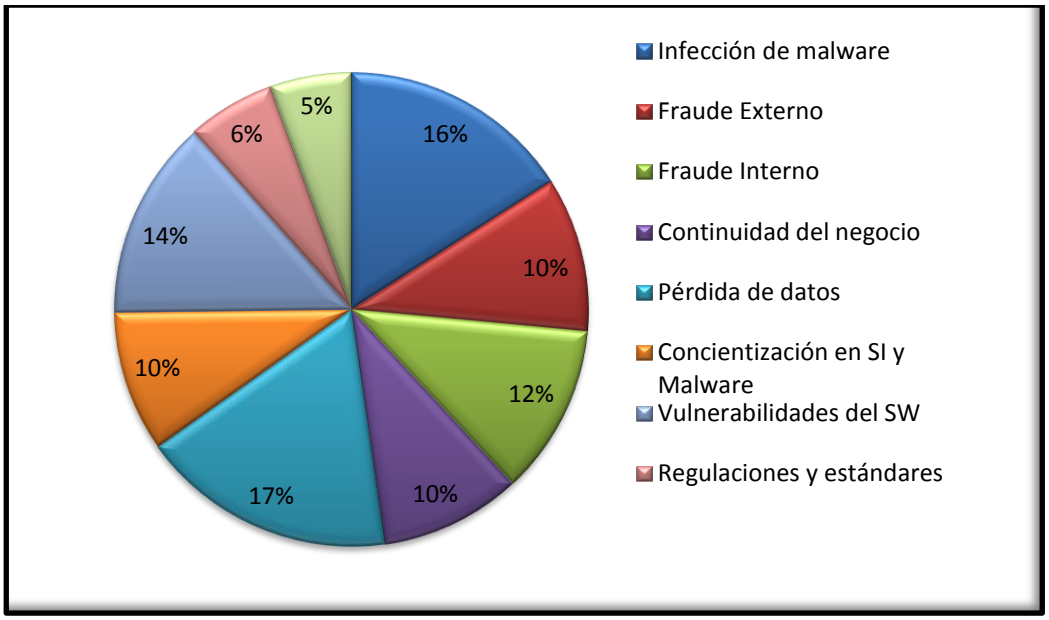


Gráfico 2. Fuente: ESET Security ReportLatinoamérica 2012 [11]

Según las gráficas anteriores se puede concluir que en el año 2011 se han producido en un mayor porcentaje casos mediante infecciones de malware vía web, es decir que estos casos se dan ya que al navegar por la web no se tiene las precauciones necesarias al acceder a diversas páginas y en algunas ocasiones estas son portadoras de virus; así mismo en el año 2012 se han presentado con mayor porcentaje casos de fraudes y/o estafas informáticas, estos ataques se producen debido a la falta de conocimiento sobre Ingeniería Social, es por esto que en diversas ocasiones se revela información confidencial sin saber que esta será usada para realizar estafas o fraudes informáticos.

A continuación se presentan algunos ejemplos sobre Ingeniería Social, los mismos que circulan por la web:

1.5.1. Correo electrónico proveniente de una entidad financiera

> "A menudo se recibe correos electrónicos de entidades financieras en las cuales se tiene cuentas bancarias, estos correos contienen mensajes indicando por ejemplo, que la cuenta se ha bloqueado y se

debe actualizar los datos personales, que el número de cuenta ha sido premiada y se debe seguir el link, que existen ofertas o promociones utilizando la cuenta bancaria, etc.” [12]. Son algunos de los textos que los atacantes informáticos utilizan para que los usuarios sigan el link, el mismo que al hacer clic captura toda nuestra información a través de código malicioso.

En la siguiente figura se muestra uno de los correos falsos que los delincuentes informáticos utilizan para acceder a cuentas financieras de los usuarios.

Figura 1. Correo para robar cuentas bancarias

1.5.2. Historia de conversación en mensajería instantánea MSN

"¿Si pudieras leer el historial de conversación de tus amigos de MSN lo harías? ¿Te imaginas descubrir todos los secretos que imaginabas? Estos son algunos de los correos que circulan por la web tratando de engañar a los usuarios, el engaño es rápido y muy tentador para el usuario ya que se envía como un mensaje normal de otro correo donde le informan que únicamente siguiendo el enlace e introduciendo un par de datos se puede ingresar al MSN de un amigo" [13].

Figura 2. Mensaje de historial de conversación de MSN

1.5.3. Facebook una de las redes sociales más atacadas por los delincuentes informáticos

"Los usuarios de la red social Facebook reciben correos falsos o invitaciones para unirse a grupos, al acceder a los links que se presentan automáticamente los Ingenieros Sociales pueden acceder a las cuentas de los usuarios utilizando cualquier tipo de virus, es por

ello que se debe desconfiar de todos estos sitios y jamás dar información confidencial en ellos" [14].

Como técnicas de Ingeniería Social se puede ver el uso del servicio de mensajería instantánea de Facebook, en dónde una víctima potencial recibe un mensaje que lo invita a ver una fotografía para luego ser re-direccionado a una página externa a la red social que cuenta con el mismo diseño, logo y colores para poder llegar a comprometer su equipo. Todo esto en conjunto conlleva a un engaño elaborado por parte del desarrollador del código malicioso con el fin de propagar la amenaza, infectando a la mayor cantidad de usuarios posibles. La siguiente figura muestra un típico mensaje que a menudo circula por la red social Facebook:

Figura 3. Mensaje en Facebook

Es importante remarcar que más allá del uso de una solución antivirus con capacidad de detección proactiva es importante contar con una buena educación por parte de los usuarios, la cual permita identificar estas posibles amenazas, y evitar que se comprometa la seguridad del equipo y la información en él contenida.

1.5.4. Llamadas telefónicas

La voz agradable de un hombre o mujer, que pertenece al soporte técnico de una empresa o de un proveedor de tecnología, que requiere telefónicamente de información para resolver un inconveniente detectado en la red.

1.5.5. La tarjeta de crédito atascada en el cajero automático

Ante la desesperación del usuario porque su tarjeta se atascó, llega una persona “comedida” que se ofrece a ayudar a recuperarla, hasta que finalmente lograr que su víctima digite su código secreto.

Todos los ejemplos anteriormente mencionados son de una u otra forma conocidos por la gente en su totalidad, pero que día a día resultan efectivos al momento de cometer fraudes, la cultura informática en la población de Ecuador, puntualmente citando es escasa ya que en abrir un mail con bonitas frases para reflexionar, amistad, amor etc., que incitan a ser reenviadas pueden contener “espías”, registrando la cuenta para futuros fraudes, al hacer clic en enviar sin la precaución de borrar las direcciones anteriores o reenviándolos con copias ocultas se deja una puerta abierta para los delincuentes informáticos.

CAPITULO II

Ingeniería Social en la Ciudad de Cariamanga

2.1. ESTADO ACTUAL

Considerando los inconvenientes antes mencionados sobre la Ingeniería Social es necesario realizar una investigación exhaustiva en Instituciones de la ciudad de Cariamanga, para determinar cuáles son más propensas a este tipo de ataque, dependiendo de la información que manejan y procesos confidenciales con los que cuentan. A continuación se describe los principales sistemas y actividades informáticas que se realizan en las instituciones, esta información fue recolectada mediante observación directa, encuestas y entrevistas (Anexo 2):

- **Institución Educativa**
  - Sistema de registro de docentes y personal administrativo de la institución.
  - Sistema de expedientes de alumnos y docentes.
  - Sistema financiero.
  - Sistema de base de datos de proyectos.
  - Administración de página web.
  - Instalación y actualización de utilidades de software.
  - Administración de registro de notas, asistencias en forma manual.
  - Mantenimiento físico y lógico de los equipos de cómputo de la institución.

Cabe recalcar que estos sistemas informáticos son administrados por una empresa externa a la institución (Tova Compu[4]). Esta empresa brinda todos los servicios de mantenimiento, configuración, administración y protección de datos de los sistemas que se utilizan en esta institución: Sistema de registro de ingreso del personal, Sistema expedientes de alumnos y docentes.

[4] **Tova Compu:** Empresa ubicada en la ciudad de Loja que brinda los servicios de instalación y mantenimientos de sistemas informáticos a nivel institucional y empresarial.

- **Institución Pública**
  - Sistema de registro de proyectos.
  - Sistema de control de personal.
  - Sistema financiero.
  - Sistemas de cobranza de rubros prediales.
  - Sistema de rentas internas.
  - Mantenimiento y administración de la red, sistemas y equipos.
  - Administración de página web.
  - Copias de seguridad periódicas de las bases de datos.
  - Mantenimiento de sistemas y equipos de cómputo.

  Para administrar estos sistemas la institución cuenta con su personal técnico, el mismo que realiza las actividades de mantenimiento, administración y configuración de todos los sistemas implantados en la Institución, esto con la finalidad de evitar que personas extrañas tengan acceso a los mismos.

- **Centro de Salud**
  - Sistema de ingreso del personal.
  - Sistema de ingreso y búsqueda de historias clínicas.
  - Sistema de registro de hospitalización.
  - Sistema financiero.
  - Sistema contable.
  - Control de subcentros asociados a esta institución.

  Para la administración y configuración de los sistemas informáticos que la Institución maneja, cuentan con los servicios informáticos de la empresa Tova Compu, la cual mediante una persona encarga en la ciudad de Cariamanga realiza las funciones periódicas de administración y mantenimiento a los mismos.

- **Institución Comercial**
  - Procesos de cobro en caja registradora.
  - Administración de base de datos.
  - Control de los sistemas de cámaras de seguridad.
  - Copias de seguridad de los datos.
  - Mantenimiento físico y lógico de los equipos de cómputo.

  Cabe mencionar que las funciones de administración y mantenimiento de los sistemas antes mencionados las realiza una persona externa a la institución, esta persona pertenece a empresa Tova Compu que brinda los servicios de administración de los sistemas en forma semanal.

- **ONG**
  - Sistemas de control de personal.
  - Sistemas de registro y control de proyectos existentes.
  - Sistemas de base de datos de patrocinadores, auspiciantes y afiliados a la institución.
  - Copias de seguridad periódicas.
  - Administración del software utilizado.

Los sistemas antes mencionados son administrados por el personal técnico interno de la institución, esto con la finalidad de preservar de una mejor manera la información de los sistemas

Luego de terminar con la investigación, se realizará una capacitación para todo el personal que labora en las diferentes instituciones en las cuales se tubo apertura, así mismo se presentará un plan de políticas de seguridad (Anexo 1) para proteger la información y dar a conocer los objetivos, técnicas, causas y efectos, que trae consigo la Ingeniería Social, ya que la educación es la única forma de combatirla.

Todas las personas que forman parte de las instituciones, secretarias, administradores, gerentes y demás empleados deben capacitarse en cuanto a las debilidades y métodos de engaño más utilizados por los atacantes para que logren identificarlos y dar aviso de cualquier anomalía que se produzca en el equipo o en determinado ambiente. Esto no significa que deben realizar cursos especializados de seguridad informática, sino que el proceso de capacitación debe formar parte de las Políticas de Seguridad de la Institución. Por otro lado, es muy común que el personal crea erróneamente que su posición dentro de la institución es de poca importancia y por lo tanto no podrían ser objeto de ataque, pero contrariamente, son en realidad las víctimas preferidas por los atacantes.

2.2. ESTUDIO DE CASOS DE INGENIERÍA SOCIAL Y BÚSQUEDA DE PRINCIPALES VULNERABILIDADES EN LAS INSTITUCIONES DE LA CIUDAD DE CARIAMANGA

Considerando los resultados obtenidos en encuestas realizadas al personal que labora en cada una de las Instituciones investigadas, se puede concluir que la mayoría del personal encuestado no tiene conocimiento sobre la Ingeniería Social y los daños que puede causar (gráfico 3). Analizando otros resultados obtenidos hasta la actualidad se han presentado pocos casos de Ingeniería Social en Instituciones de la ciudad de Cariamanga.

A continuación se explican casos reales que se determinaron en cada una de las instituciones, esto fue determinado a través del uso de técnicas de ataque informático como, suplantación de identidad y observación, técnica de Phishing y técnica de llamada telefónica.

Cabe recalcar que estas técnicas fueron aplicadas por igual a todas las instituciones, por lo que se explica todo el procedimiento únicamente en la primera institución y en las siguientes solo se menciona los resultados.

2.2.1. TÉCNICA SUPLANTACIÓN DE IDENTIDAD Y OBSERVACIÓN (Ver anexo 5).

Objetivo

Obtener información confidencial de la institución mediante la suplantación de identidad.

Herramienta

Habilidad y conocimiento sobre técnicas de suplantación de identidad y observación.

Desarrollo

Esta técnica fue ejecutar por separado dependiendo del lugar y la cantidad de personas existentes en el departamento, tal como se explica a continuación:

- Técnica realizada una vez al día en lugares adecuados, en silencio y memorizando la mayor cantidad de información disponible.
- En esta técnica se suplantó al personal de Soporte Técnico, indicando a las secretarias que se iba a dar mantenimiento a los equipos informáticos.
- Las secretarias proporcionaron disponibilidad total de los equipos, mientras ellas se ausentaban del lugar de trabajo.
- Se pudo recolectar información como IP del equipo, usuario y contraseñas (Anexo 6).

La técnica de observación se realizó ingresando de manera particular a cada departamento, con la finalidad de captar la mayor cantidad de información sensible, así mismo la revisión de documentos sobre los escritorios.

INSTITUCIÓN EDUCATIVA

VÍCTIMAS	RESULTADOS	CONCLUSIONES
8 administrativos 2 departamentos	75% si proporcionó información. 25% no proporcionó información	• Fuga de información confidencial, ya que el personal aún no está consiente sobre las diferentes técnicas de robo de información y las consecuencias que esto puede tener. • Para los Ingenieros Sociales se les es fácil suplantar la identidad del personal que labora en la institución, ya que no cuentan con previa identificación.

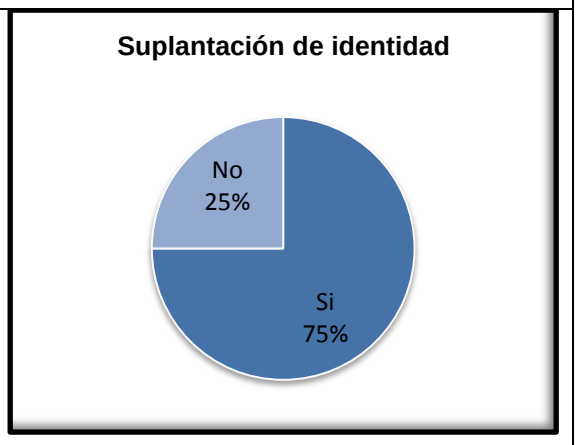
Cuadro 3. Resultados suplantación identidad Institución Educativa

INSTITUCIÓN PÚBLICA

VÍCTIMAS	RESULTADOS	CONCLUSIONES
10 administrativos 2 departamentos	80% si proporcionó información. 20% no proporcionó información	• Fuga de información confidencial, ya que el personal aún no está consiente sobre las diferentes técnicas de robo de información y las consecuencias que esto puede tener. • Para los Ingenieros Sociales se les es fácil suplantar la identidad del personal que labora en la institución, ya que no cuentan con previa identificación.

Cuadro 4. Resultados suplantación identidad Institución Pública

CENTRO DE SALUD

VÍCTIMAS	RESULTADOS	RESULTADOS GRÁFICOS
6 administrativos 1 departamentos	75% si proporcionó información. 25% no proporcionó información	

Cuadro 5. Resultados suplantación identidad Centro de Salud

INSTITUCIÓN COMERCIAL

VÍCTIMAS	RESULTADOS	CONCLUSIONES
5 administrativos 1 departamentos	Información obtenida: • Claves de acceso. • Información con la que trabajan • Datos personales del personal • Información de proveedores • Acceso a las bases de datos	• Fuga de información confidencial, ya que el personal aún no está consiente sobre las técnicas de robo de información y consecuencias que esto puede tener. • Para los Ingenieros Sociales es fácil suplantar la identidad de cualquier persona, ya que para ingresar a esta institución a realizar "prácticas", únicamente se debe tener un argumento y un voto de confianza.

Cuadro 6. Resultados suplantación identidad Centro Comercial

ONG

VÍCTIMAS	RESULTADOS	CONCLUSIONES
20 administrativos 2 departamentos	• Claves de acceso a los sistemas. • Proyectos ejecutados y por ejecutar. • Información que a diario manipulan • Números telefónicos del personal. • Registro de patrocinadores • Registro de personas asociadas a la institución.	• Existe un gran índice de fuga de información dentro de la Institución, ya que la mayoría del personal entrega información confidencial a personas sin pedir ningún tipo de identificación. • Es fácil realizar suplantación ya que actualmente no cuentan con sistemas de seguridad físicas, ni personal técnico dentro de la institución, por lo que personas desconocidas ingresan con facilidad a los departamentos y manipulan los equipos informáticos.

Cuadro 7. Resultados suplantación identidad ONG

2.2.2. TÉCNICA DE PHISHING[5] O ROBO DE INFORMACIÓN MEDIANTE CORREO ELECTRÓNICO

Objetivo

Determinar cuántas personas son víctimas de este ataque.

Herramientas

Para el desarrollo de esta técnica se utilizó la herramienta informática WhoReadMe[6].

Desarrollo

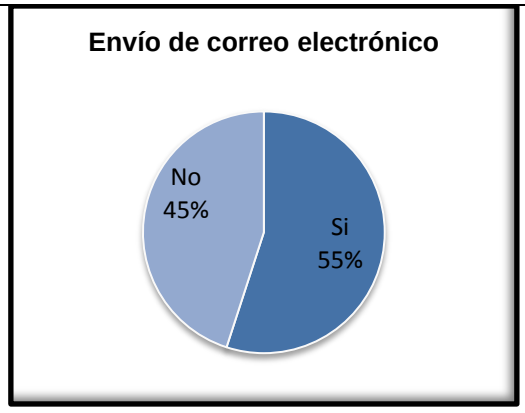
Los correos electrónicos tanto de estudiantes como del personal que labora en la institución, fueron recolectados a través de la técnica de suplantación y observación. Antes de enviar el correo electrónico se analiza la manera en que el mensaje puede ser tentativo para el usuario y de esta manera asegurarse que el destinatario lo abra. El asunto del mensaje fue SUPER OFERTAS POR TEMPORADA desde un correo creado para poder realizar esta técnica de ataque, ofertas_especiales@hotmail.es, en el cual su contenido trataba sobre nuevas ofertas, siendo tentativo para ser abierto por el usuario, el mismo que contiene código que enlaza a la página que contiene incrustada una imagen transparente con un identificador dentro del correo electrónico, el mismo que permite saber si el e-mail ha sido recibido y ejecutado.

Una vez notificado que el correo ha sido abierto y ejecutado el archivo adjunto, se envía los datos de la máquina en donde fue leído el correo (Anexo 7).

[5] **Phishing:** Ver ítem 2.1.2.

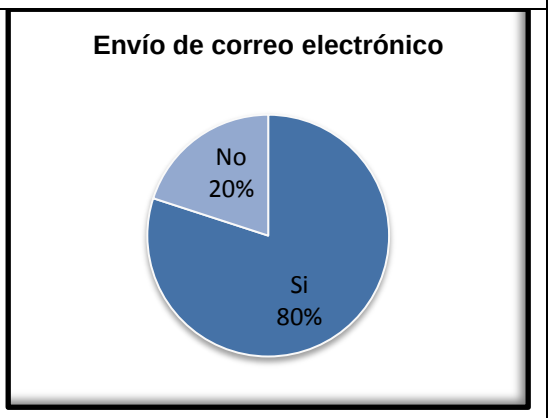
[6] **WhoReadMe:** Es un servicio de seguimiento en línea y permite enviar mensajes de alerta cuando son recibidos y leídos los diferentes correos electrónicos, (ver ítem 1.2.2.).

INSTITUCIÓN EDUCATIVA

VÍCTIMAS	RESULTADOS	RESULTADOS GRÁFICOS
55 administrativos	55% abrieron el correo electrónico. 45% ignoraron el correo electrónico.	

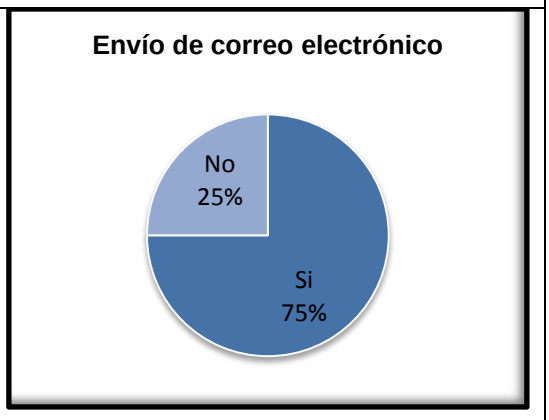
Cuadro 8. Resultados de técnica Phishing Institución Educativa

INSTITUCIÓN PÚBLICA

VÍCTIMAS	RESULTADOS	RESULTADOS GRÁFICOS
10 administrativos 2 departamentos	80% abrieron el correo electrónico. 20% ignoraron el correo electrónico.	

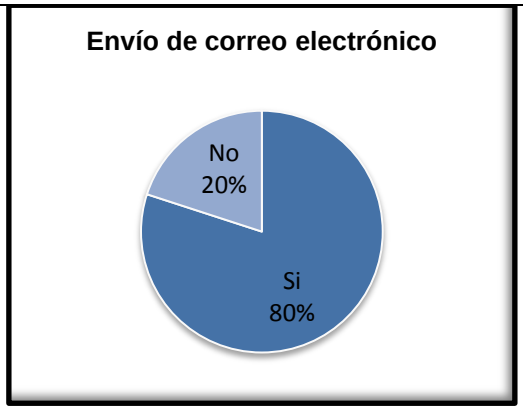
Cuadro 9. Resultados de técnica Phishing Institución Pública

CENTRO DE SALUD

VÍCTIMAS	RESULTADOS	RESULTADOS GRÁFICOS
50 personas que laboran en la Institución	75% abrieron el correo electrónico. 25% ignoraron el correo electrónico.	

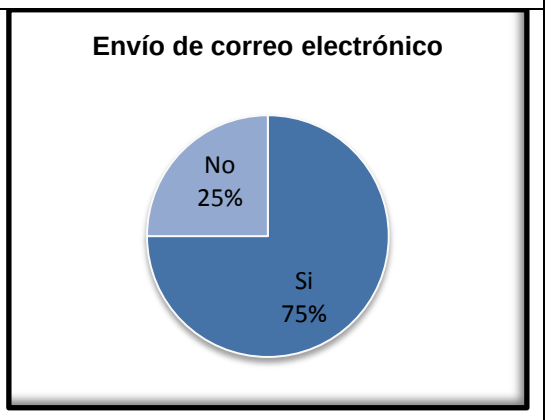
Cuadro 10. Resultados de técnica Phishing Centro de Salud

INSTITUCIÓN COMERCIAL

VÍCTIMAS	RESULTADOS	RESULTADOS GRÁFICOS
12 personas que laboran en la Institución	80% abrieron el correo electrónico. 20% ignoraron el correo electrónico.	

Cuadro 11. Resultados de técnica Phishing Institución Comercial

ONG

VÍCTIMAS	RESULTADOS	RESULTADOS GRÁFICOS
30 personas que laboran en la Institución	75% abrieron el correo electrónico. 25% ignoraron el correo electrónico.	

Cuadro 12. Resultados de técnica Phishing ONG

2.2.3. TÉCNICA DE LLAMADAS TELEFÓNICAS

Esta es una de las técnicas más fáciles de usar para los Ingenieros Sociales, ya que permite tener varias ventajas sobre las víctimas, es decir ocultar el número telefónico y mantener el anonimato, permite actuar a distancia de la víctima lo que proporciona hacer difícil su búsqueda y solicitar información suplantando a personas internas de la empresa. Cuando se realiza llamadas telefónicas es posible que no conteste la persona que estamos buscando o que simplemente no nos brinde información.

Objetivo

Establecer vínculos de relación con los usuarios mediante la técnica de llamadas telefónicas y obtener información confidencial.

Herramienta

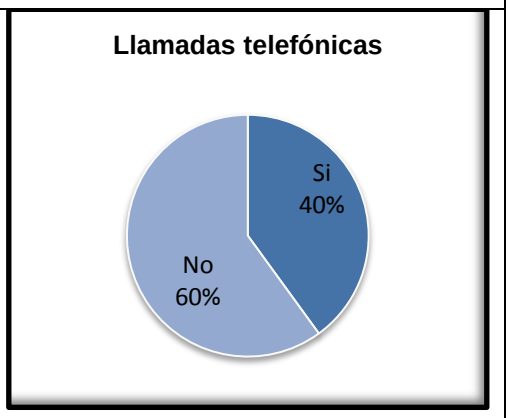
Teléfono.

Desarrollo

Para la ejecución de este ataque por medio del uso telefónico fue fácil la obtención de los números y extensiones telefónicas de las Secretarias y personal administrativo, ya que a través de las técnicas anteriores se pudo determinar este tipo de información.

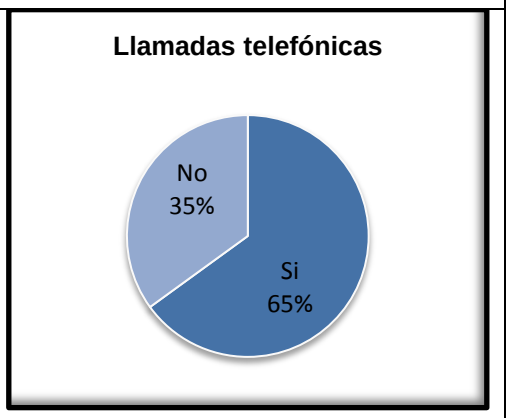
Una vez obtenida esta información, se empezó a realizar las respectivas llamadas al personal originando conversaciones amenas y solicitando de manera cordial información confidencial de su trabajo. Se suplantó a personal de Soporte Técnico, indicando que se necesitaba configurar el antivirus y si nos podía ayudar, dándonos algunos datos del equipo como: dirección IP, usuario, clave, nombres y apellidos, área donde trabajan (Anexo 8).

INSTITUCIÓN EDUCATIVA

VÍCTIMAS	RESULTADOS	RESULTADOS GRÁFICOS
8 administrativos 2 departamentos	40% Si proporcionaron información. 60% ignoraron la llamada telefónica.	

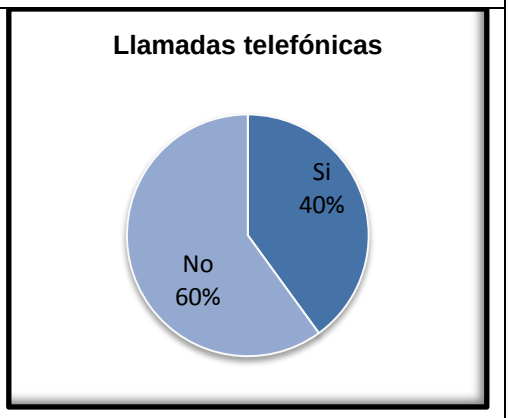
Cuadro 13. Resultados de Llamadas Telefónicas Institución Educativa

INSTITUCIÓN PÚBLICA

VÍCTIMAS	RESULTADOS	RESULTADOS GRÁFICOS
10 administrativos 2 departamentos	65% Si proporcionaron información. 35% ignoraron la llamada telefónica.	

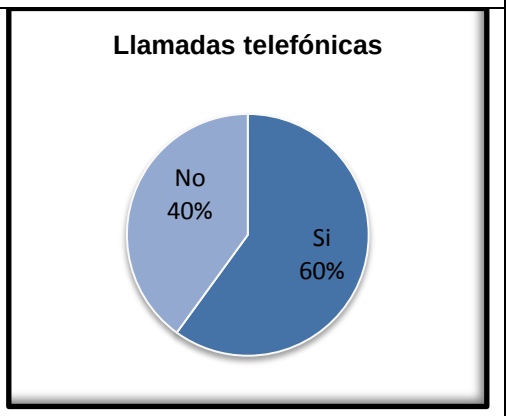
Cuadro 14. Resultados de Llamadas Telefónicas Institución Pública

CENTRO DE SALUD

VÍCTIMAS	RESULTADOS	RESULTADOS GRÁFICOS
6 administrativos 1 departamentos	40% Si proporcionaron información. 60% ignoraron la llamada telefónica.	

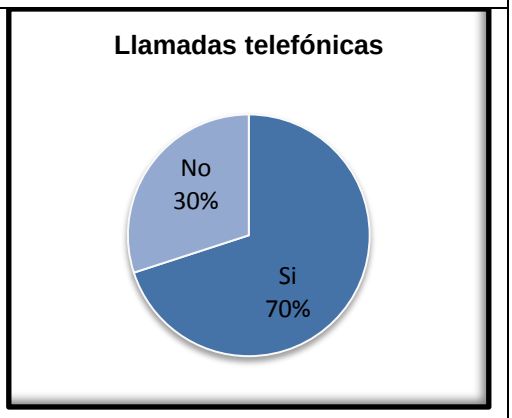
Cuadro 15. Resultados de Llamadas Telefónicas Centro de Salud

INSTITUCIÓN COMERCIAL

VÍCTIMAS	RESULTADOS	RESULTADOS GRÁFICOS
5 administrativos 1 departamentos	60% Si proporcionaron información. 40% ignoraron la llamada telefónica.	

Cuadro 16. Resultados de Llamadas Telefónicas Institución Comercial

ONG

VÍCTIMAS	RESULTADOS	RESULTADOS GRÁFICOS
12 administrativos 2 departamentos	70% Si proporcionaron información. 30% ignoraron la llamada telefónica.	

Cuadro 17. Resultados de Llamadas Telefónicas ONG

Luego de haber analizado las técnicas de Ingeniería Social se puede concluir que en esta institución la mayoría del personal desconoce las diferentes técnicas de ataque para robar información confidencial, por ello se debe realizar campañas de capacitación para concientizar al personal sobre los métodos que actualmente se están utilizando para acceder a los diferentes sistemas de información y sustraer información sensible.

2.2.4. BÚSQUEDA DE VULNERABILIDADES EN LOS SISTEMAS INFORMÁTICOS A TRAVÉS DE HERRAMIENTAS INFORMÁTICAS

Para la búsqueda de vulnerabilidades en los sistemas de información se procedió a utilizar la herramienta Informática NESSUS[7] en todos los sistemas de las Instituciones. Cabe recalcar que las vulnerabilidades encontradas son similares en todas las Instituciones, debido a que en su mayoría los sistemas son administrados por una misma empresa.

Esta herramienta fue implementada para escanear los sistemas Financiero, Registro de personal, de Proyectos y de Cobranza de cada Institución investigada. A continuación se citan las más comunes:

Vulnerabilidades más comunes encontradas en las Instituciones (Anexo 10)

1. **El certificado SSL para este servicio no se puede confiar.**

   El certificado X.509[8] del servidor no tiene una firma de una autoridad de certificación pública conocida. Esta situación puede ocurrir de tres maneras diferentes, como se muestra a continuación:

   En primer lugar, la parte superior de la cadena de certificado enviado por el servidor no podría ser descendiente de una entidad de certificación pública conocida. Esto puede ocurrir cuando la parte superior de la cadena es un desconocido, un certificado auto firmado, o cuando falta los certificados intermedios que conectaría la parte

[7] **Nessus:** Sirve para detectar a través de la red vulnerabilidades en un sistema remoto, ya sea un cliente o servidor. También detecta vulnerabilidades del software instalado

[8] **X.509**: Es un estándar UIT-T para infraestructuras de claves públicas (*Public Key Infrastructure* o PKI). Especifica, formatos estándar para certificados de claves públicas y un algoritmo de validación de la ruta de certificación.'NotBefore'

superior de la cadena de certificados a una autoridad del certificado pública conocida.

En segundo lugar, la cadena de certificados puede contener un certificado que no es válida en el momento de la exploración.

En tercer lugar, la cadena de certificados puede contener una firma que no se corresponde con la información del certificado, o no pudo ser verificada. Las firmas que no pudieron ser verificados son el resultado del emisor del certificado utilizando un algoritmo de firma que NESSUS no es compatible o no reconoce.

Si el host remoto es un sistema público en la producción, que se corte la cadena anula el uso de SSL como cualquiera podría establecer un man-in-the-middle[9] contra la máquina remota.

2. **Firma está deshabilitado en el servidor remoto SMB[10].**

   Firma está deshabilitado en el servidor remoto SMB. Esto puede permitir ataques man-in-the-middle contra el servidor SMB.

3. **Remote puertos abiertos se enumeran a través de SSH.**

   Este plugins se ejecuta 'netstat' en la máquina remota para enumerar puertos abiertos. Consulte 'Opciones' la sección de plugins para su configuración.

   Puertos abiertos (6)

[9] **Man-in-the-middle:** Es un ataque en el que el enemigo adquiere la capacidad de leer, insertar y modificar a voluntad, los mensajes entre dos partes sin que ninguna de ellas conozca que el enlace entre ellos ha sido violado. El atacante debe ser capaz de observar e interceptar mensajes entre las dos víctimas.

[10] **SMB:** Es un Protocolo de red (que pertenece a la capa de aplicación en el modelo OSI) que permite compartir archivos e impresoras (entre otras cosas) entre nodos de una red.

139 /tcp Servicio: smb
8834 /tcp Servicio: www
1241 /tcp Servicio: nessus
1032 /tcp Servicio: www
445 /tcp Servicio: cifs
135 /tcp Servicio: epmap

4. **Un archivo/ servicio compartido de impresoras está escuchando en el host remoto.**

   El servicio remoto entiende las CIFS (Common Internet File System) o bloque de mensajes del servidor (SMB), que se utiliza para proporcionar acceso compartido a archivos, impresoras, etc. Entre los nodos de una red.

5. **El servicio remoto encripta las comunicaciones.**

   Este script detecta que SSL y TLS versiones son compatibles con el servicio remoto para el cifrado delas comunicaciones.

6. **Un servidor web se ejecuta en el host remoto.**

   Este plugins[11] intenta determinar el tipo y la versión del servidor web remoto. El host remoto escucha en el puerto TCP 445 y responde a las peticiones SMB. Mediante el envío de una solicitud de autenticación NTLM SSP es posible obtener el nombre del sistema remoto y el nombre de su dominio.

7. **Conexiones activas se enumeran a través de la 'netstat' comando.**

   Este plugins se ejecuta en 'netstat' en la máquina remota para enumerar todos los activos "establecida" o "escuchar" conexiones TCP / UDP.

[11]**Plugins:** Es una aplicación que se relaciona con otra para aportarle una función nueva y generalmente muy específica. Esta aplicación adicional es ejecutada por la aplicación principal e interactúan por medio de la API.

Luego de analizar los casos de Ingeniería Social presentados en cada una de las Instituciones se pudo constatar que ingresar a los diferentes departamentos y realizar ataques de robo de información, es sumamente fácil debido a que no cuentan con sistemas de seguridad, ni peor aún piden algún tipo de identificación a personas desconocidas, las mismas que acceden a la información argumentando que son de soporte técnico y van a dar mantenimiento a los equipos y sistemas. En el siguiente cuadro se resumen las causas y técnicas más comunes de Ingeniería Social y el impacto que estas han tenido en las instituciones.

CAUSA	TÉCNICA	IMPACTO
Falta de seguridad física.	Suplantación de identidad (ítem 2.4.1) Observación directa	Robo de documentos, contraseñas, proyectos.
Desconocimiento de ataques informáticos	Suplantación de identidad (ítem 2.4.1) Llamadas telefónicas (ítem 2.4.3)	Perdida de contraseñas, correos electrónicos, información confidencial de la institución
Permitir el acceso libre a personas desconocidas sin identificación	Suplantación de identidad (ítem 2.4.1) Llamadas telefónicas (ítem 2.4.3) Observación directa	Perdida de proyectos, información de los equipos informáticos, contraseñas, documentos sensibles.
Abrir correos electrónicos por curiosidad	Phishing(ítem 2.4.2) Suplantación de identidad (ítem 2.4.1)	Perdida de información sobre los equipos informáticos, robo de contraseñas y correos electrónicos.
Firewall de Windows deshabilitado.	Nessus (Anexo 10)	El firewall y el software utilizado están en versiones anteriores, por lo que es fácil para los atacantes informáticos propagar cualquier tipo de código malicioso
Gran cantidad de puertos abiertos	Nessus (Anexo 10)	Acceso a los sistemas mediante códigos maliciosos

innecesariamente		
Los parches de seguridad de Windows desactualizados	Nessus (Anexo 10)	Al tener los parches de seguridad desactualizados los virus y códigos externos pueden afectar el funcionamiento de los sistemas.
Detección de redes y equipos desconocidas	Nessus (Anexo 10)	Acceso a Wireless de la Institución, disminución en el ancho de banda colapso en los sistemas.
Contraseñas fácilmente identificables para los atacantes informáticos.	PasswordMeter (Anexo 9)	Mediante la utilización de una herramienta en línea, se pudo comprobar que tan fuertes son las contraseñas que utilizan los usuarios para acceder a los sistemas.
Robo de información a través de accesos remotos al computador.	Suplantación de identidad (ítem 2.4.1)	Se determinó que la mayoría de los usuarios, al ausentarse de su puesto de trabajo dejan sus equipos de cómputo sin bloquear, por lo que para los atacantes informáticos se les facilita el acceso a los mismos.

Cuadro 18.Técnicas e impacto de Ingeniería Social

A continuación se presenta un resumen estadístico con preguntas relevantes de encuestas realizadas a todo el personal administrativo de cada una de las instituciones, las mismas que permitirán obtener resultados y a partir de estos emitir conclusiones, recomendaciones y comentarios. Los resultados se basan de acuerdo a las respuestas de 50 encuestas realizadas en cada una de las instituciones (Anexo 2):

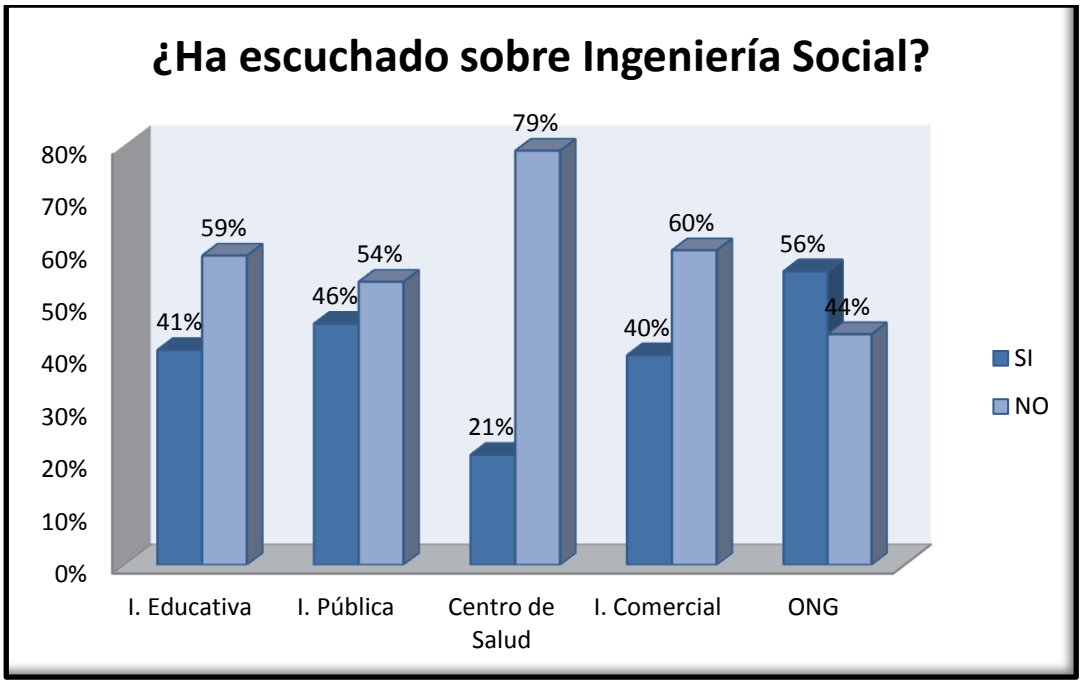


Gráfico 3: Desconocimiento de Ingeniería Social**.**

Gráfico 3: El nivel de conocimiento sobre Ingeniería Social es bajo en todas las instituciones investigadas, es por ello que se debe realizar campañas de capacitación y motivación dirigido a todo el personal que labora en las instituciones.

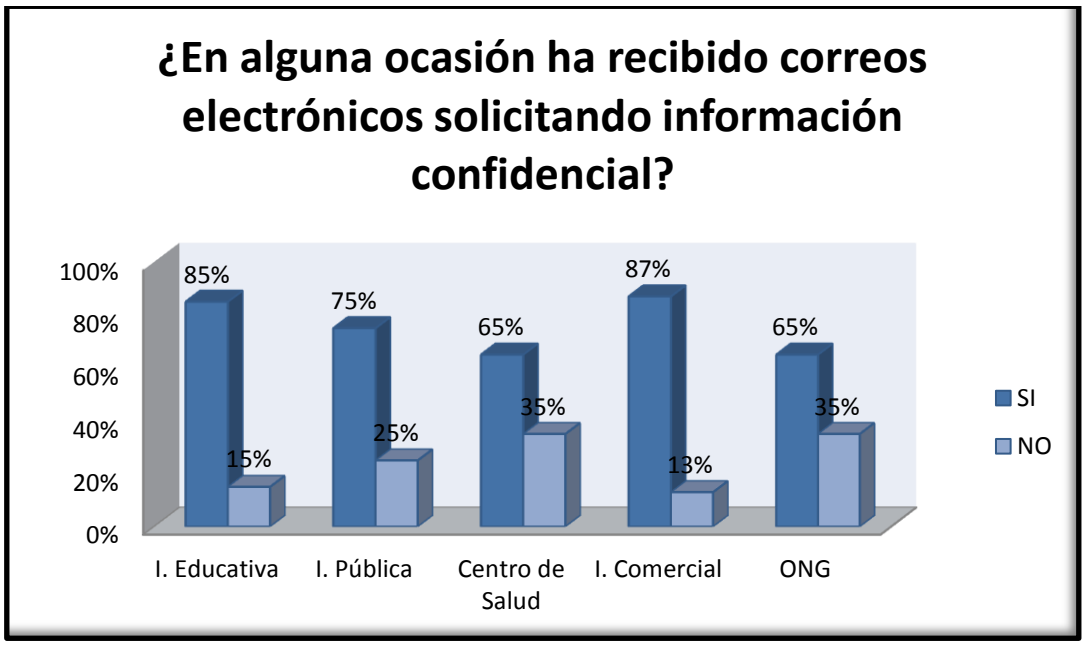


Gráfico 4: Solicitud de información confidencial**.**

Gráfico 4: Las personas encuestadas si reciben correos los cuales solicitan revelar información, en ocasiones los correos electrónicos son eliminados inmediatamente para evitar ser víctimas de estafas o engaños.

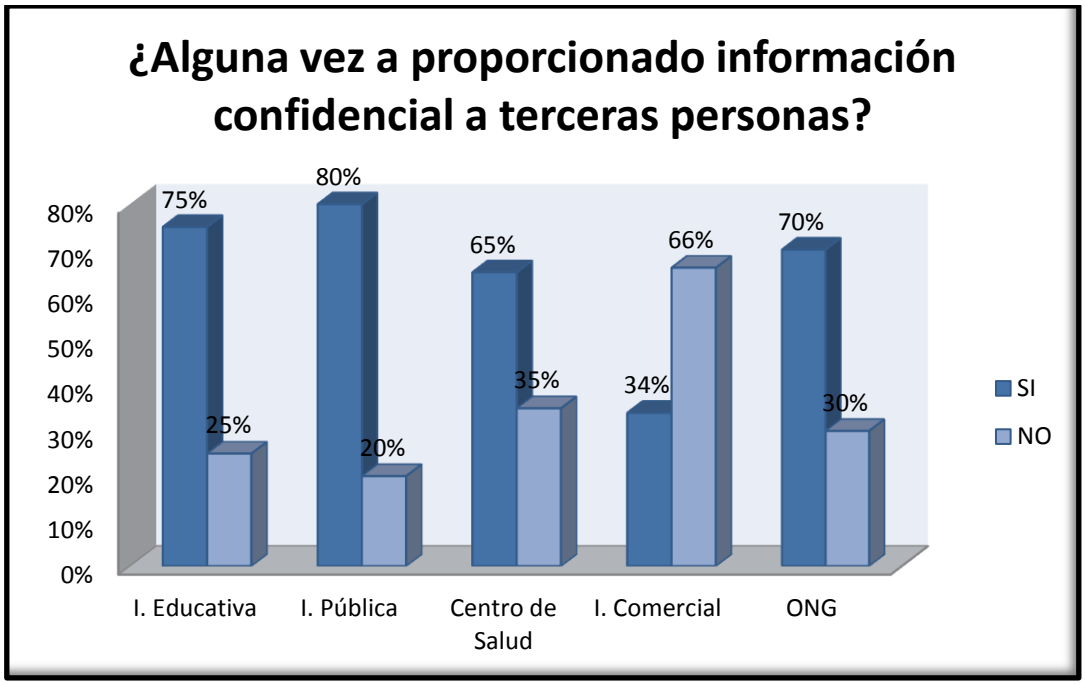


Gráfico 5: Proporcionar información confidencial

Gráfico 5: Las personas encuestadas respondieron en su mayoría que sí han revelado información confidencial, siendo de esta manera víctimas de ataques informáticos.

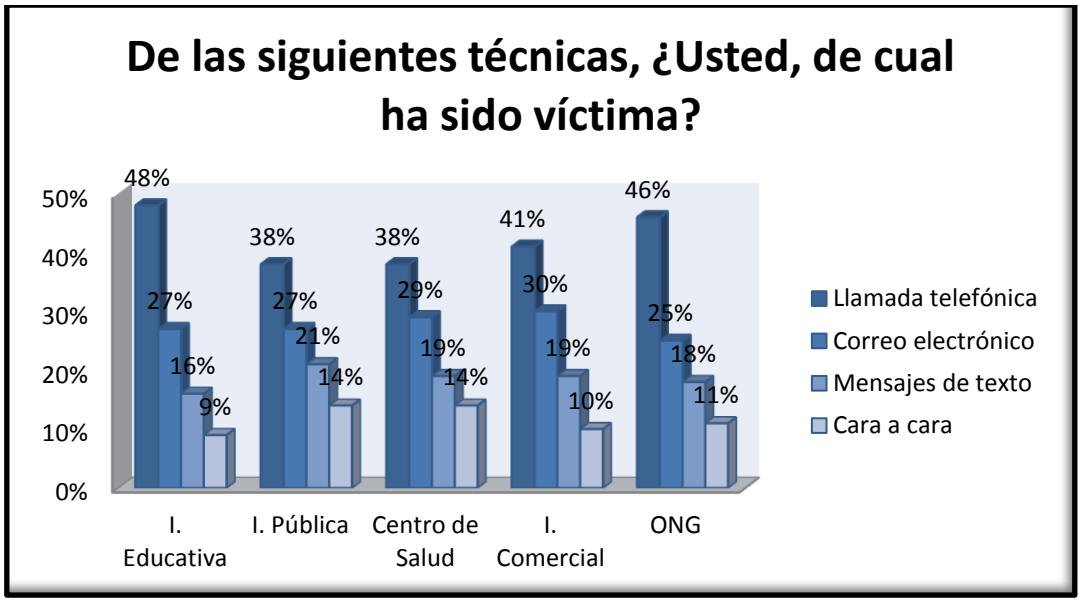


Gráfico 6: Técnicas de las cuales ha sido víctima

Gráfico 6: La mayoría de los encuestados respondieron que revelan información confidencial mediante llamadas telefónicas, ya que los atacantes informáticos se hacen pasar por personal de la institución y manipulan la sicología de la víctima para que revele la información solicitada.

CAPITULO III

Solución

3.1. FORMAS DE PROTECCIÓN CONTRA LAS VULNERABILIDADES ENCONTRADAS EN LAS INSTITUCIONES

En el siguiente cuadro se presenta las soluciones a cada una de las vulnerabilidades encontradas en las instituciones investigadas, el personal debe seguir las siguientes recomendaciones para evitar ser víctima de las trampas de la Ingeniería Social:

VULNERABILIDAD	SOLUCIÓN
Falta de seguridad física.	Para solucionar esta vulnerabilidad es necesario implementar cámaras de seguridad en los departamentos principales, ya que es aquí en donde se manipula mayor cantidad de información confidencial, además es indispensable contratar los servicios de un guardia de seguridad, el mismo que llevará un registro mediante el siguiente procedimiento: solicitar y registrar número de cédula de ciudadanía, nombres y apellidos completos, motivo por el que ingresa al departamento, hora de ingreso y hora de salida, (ver anexo 1- política 1.1)
Desconocimiento de ataques informáticos	Todo el personal que labora en la institución fue capacitado sobre temas relacionados con técnicas de robo de información (Ingeniería Social), esto con la finalidad de concientizar a los usuarios y evitar ser víctimas de los Ingenieros Sociales, semestralmente se reforzará los conocimientos sobre Ingeniería Social mediante capacitaciones continuas (ver anexo 13 y anexo 1- política 1.9).
Permitir el acceso libre a personas desconocidas sin identificación	Se estableció como política de seguridad el bloquear siempre el computador al ausentarse del puesto de trabajo, así mismo la utilización adecuada de contraseñas seguras (anexo 1- política 1.2, 1.3 y 1.7).
Contraseñas fácilmente identificables para los atacantes informáticos.	Se estableció como política de seguridad el uso de contraseñas seguras, combinando letras, números, signos y con un mínimo de 6 dígitos y de esta manera evitar que otras

	personas descubran con facilidad las contraseñas (anexo 1- política 1.3).
Robo de información a través de accesos remotos al computador.	Se estableció como política de seguridad el bloquear siempre el computador al ausentarse del puesto de trabajo, así mismo la utilización adecuada de contraseñas seguras (anexo 1- política 1.3 y 1.7).
Firewall de Windows deshabilitado.	En todos los equipos informáticos de los departamentos investigados, se procedió a habilitar el servicio de firewall, ya que de esta forma los equipos están protegidos ante cualquier amenaza de virus o código malicioso que pueda poner en riesgo la información que allí se almacena. Además se procedió a actualizar el software, utilizando las últimas versiones. Los encargados de realizar este proceso son las personas del departamento informático ya que ellos son los responsables directos del mantenimiento tanto del software como del hardware.
Gran cantidad de puertos abiertos innecesariamente.	Se realizó mantenimiento físico y lógico a los equipos informáticos con la finalidad de cerrar todos los puertos que no sean utilizados y de esta forma evitar que intrusos accedan a los equipos con códigos maliciosos.
Los parches de seguridad de Windows desactualizados.	Mediante una política de seguridad quedó establecido la actualización mensual de los parches de seguridad del sistema operativo de cada Institución y de esta forma contrarrestar los códigos maliciosos.
Detección de redes y equipos desconocidas.	Se procedió a investigar la procedencia de las redes inalámbricas conectadas al servidor de la institución, obteniendo la dirección IP y deshabilitando del servicio.
La información que envía a través de la redes de datos no cuenta con los estándares necesarios de seguridad.	Cifrar la información enviada a través de las redes informáticas, para preservar la confidencialidad, integridad y autenticación de la misma. Cifrando la información enviada se evita que los intrusos intercepten los mensajes enviados ya que debe contar con una clave y un algoritmo para cifrar y descifrar (anexo 1- política 1.2).
Copias de seguridad incompletas, por lo que en caso de pérdida de	Mediante la política de seguridad se estableció que las copias de seguridad deben realizarse en forma diaria y es de vital importancia la verificación de su correcto funcionamiento

información importante no tiene como recuperarla.	y asegurar que los dispositivos físicos que contengan las copias de seguridad sean custodiados de forma adecuada. (Anexo 1- política 1.5).

Cuadro 19. Formas de protección

3.2. SEGURIDAD DE LA INFORMACIÓN

Modelo PDCA

Dentro de una institución el tema de la seguridad de la información es muy importante, requiere dedicarle tiempo y recursos. La organización debe plantearse un Sistema de Gestión de la Seguridad de la Información (SGSI).El objetivo de un SGSI es proteger la información y para ello lo primero que debe hacer es identificar los 'activos de información' que deben ser protegidos y en qué grado.

Luego debe aplicarse el plan **PDCA** (**'PLAN – DO – CHECK – ACT**'), es decir Planificar, Hacer, Verificar, Actuar y volver a repetir el ciclo.

Se entiende la seguridad como un proceso que nunca termina ya que los riesgos nunca se eliminan, pero se pueden gestionar. De los riesgos se desprende que los problemas de seguridad no son únicamente de naturaleza tecnológica, y por ese motivo nunca se eliminan en su totalidad. Un Sistema de Gestión de Seguridad siempre cumple cuatro niveles repetitivos que comienzan por Planificar y terminan en Actuar, consiguiendo así mejorar la seguridad.

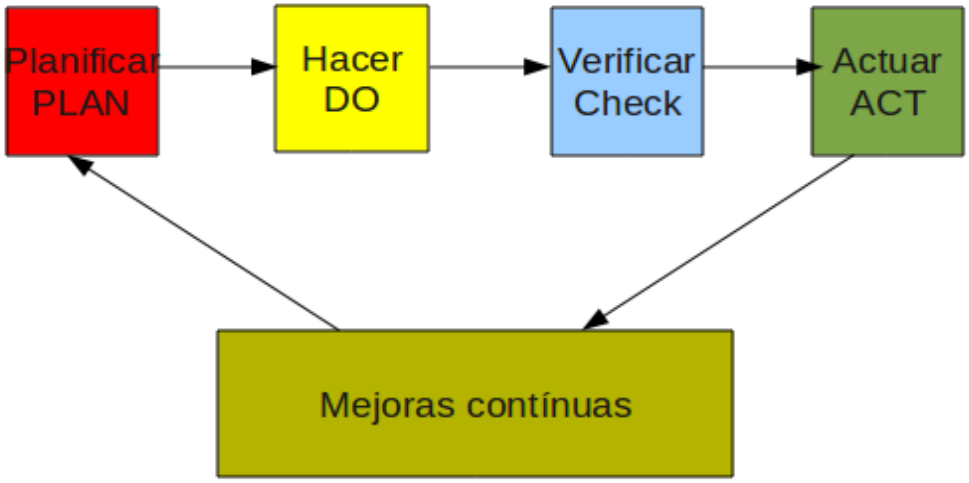


Figura 4: Modelo PDCA

PLANIFICAR (Plan): consiste en establecer el contexto en él se crean las políticas de seguridad, se hace el análisis de riesgos, se hace la selección de controles y el estado de aplicabilidad

HACER (Do): consiste en implementar el sistema de gestión de seguridad de la información, implementar el plan de riesgos e implementar los controles.

VERIFICAR (Check): consiste en monitorear las actividades y hacer auditorías internas.

ACTUAR (Act): consiste en ejecutar tareas de mantenimiento, propuestas de mejora, acciones preventivas y acciones correctivas.

MECANISMOS BÁSICOS DE SEGURIDAD

Autenticación: Definimos la Autenticación como la verificación de la identidad del usuario, generalmente cuando entra en el sistema o la red, o accede a una base de datos. Normalmente para entrar en el sistema

informático se utiliza un nombre de usuario y una contraseña. Pero, cada vez más se están utilizando otras técnicas más seguras.

Es posible autenticarse de tres maneras:

1. Por lo que uno sabe (una contraseña)
2. Por lo que uno tiene (una tarjeta magnética)
3. Por lo que uno es (las huellas digitales)

La utilización de más de un método a la vez aumenta las probabilidades de que la autenticación sea correcta. Pero la decisión de adoptar más de un modo de autenticación por parte de las empresas debe estar en relación al valor de la información a proteger. La técnica más usual (aunque no siempre bien) es la autenticación utilizando contraseñas. Este método será mejor o peor dependiendo de las características de la contraseña. En la medida que la contraseña sea más grande y compleja para ser adivinada, más difícil será burlar esta técnica.

Además, la contraseña debe ser confidencial. No puede ser conocida por nadie más que el usuario. Muchas veces sucede que los usuarios se prestan las contraseñas o las anotan en un papel pegado en el escritorio y que puede ser leído por cualquier otro usuario, comprometiendo a la empresa y al propio dueño, ya que la acción/es que se hagan con esa contraseña es/son responsabilidad del dueño.

Autorización: Definimos la Autorización como el proceso por el cual se determina qué, cómo y cuándo, un usuario autenticado puede utilizar los recursos de la organización. El mecanismo o el grado de autorización pueden variar dependiendo de qué sea lo que se está protegiendo. No toda la información de la organización es igual de crítica. Los recursos en general y los datos en particular, se organizan en niveles y cada nivel debe tener una autorización.

En el caso de los datos, la autorización debe asegurar la confidencialidad e integridad, ya sea dando o denegando el acceso en lectura, modificación, creación o borrado de los datos. Por otra parte, solo se debe dar autorización a acceder a un recurso a aquellos usuarios que lo necesiten para hacer su trabajo y si no se le negará. Aunque también es posible dar autorizaciones transitorias o modificarlas a medida que las necesidades del usuario varíen.

Administración: Definimos la Administración como la que establece, mantiene y elimina las autorizaciones de los usuarios del sistema, los recursos del sistema y las relaciones usuarios-recursos del sistema. Los administradores son responsables de transformar las políticas de la organización y las autorizaciones otorgadas a un formato que pueda ser usado por el sistema. Normalmente todos los sistemas operativos que se precian disponen de módulos específicos de administración de seguridad. Y también existe software externo y específico que se puede utilizar en cada situación.

Auditoría y registro: Definimos la Auditoría como la continua vigilancia de los servicios en producción y para ello se recaba información y se analiza. Este proceso permite a los administradores verificar que las técnicas de autenticación y autorización utilizadas se realizan según lo establecido y se cumplen los objetivos fijados por la organización.

Definimos el Registro como el mecanismo por el cual cualquier intento de violar las reglas de seguridad establecidas queda almacenado en una base de eventos para luego analizarlo. Monitorear la información registrada o auditar se puede realizar mediante medios manuales o automáticos, y con una periodicidad que dependerá de lo crítica que sea la información protegida y del nivel de riesgo.

Mantenimiento de la integridad: Definimos el Mantenimiento de la integridad de la información como el conjunto de procedimientos establecidos para evitar o controlar que los archivos sufran cambios no autorizados y que la información enviada desde un punto llegue al destino inalterada. Dentro de las técnicas más utilizadas para mantener (o controlar) la integridad de los datos están: uso de antivirus, encriptación y funciones 'hash'.

3.3. POLÍTICAS DE SEGURIDAD A IMPLEMENTAR EN LAS INSTITUCIONES PARA EVITAR LA INGENIERÍA SOCIAL

La principal defensa contra Ingeniería Social es educar y entrenar a los usuarios en el uso de políticas de seguridad y asegurarse de que estas sean cumplidas. La seguridad informática ha tomado gran auge, debido a las cambiantes condiciones y nuevas plataformas tecnológicas disponibles, la posibilidad de interconectarse a través de redes, ha abierto nuevos horizontes a las empresas para mejorar su productividad y poder explorar más allá de las fronteras nacionales, lo cual lógicamente ha traído consigo, la aparición de nuevas amenazas para los sistemas de información.

Estos riesgos que se enfrentan han llevado a que muchas desarrollen documentos y directrices que orientan en el uso adecuado de estas destrezas tecnológicas y recomendaciones para obtener el mayor provecho de estas ventajas, y evitar el uso indebido de las mismas, lo cual puede ocasionar serios problemas a los bienes, servicios y operaciones de la empresa. En este sentido, las políticas de seguridad informática surgen como una herramienta organizacional para concientizar a los colaboradores de la organización sobre la importancia y sensibilidad de la información y servicios críticos que permiten a la empresa crecer y mantenerse competitiva. Ante esta situación, el proponer o identificar una política de seguridad requiere un alto compromiso con la organización, agudeza técnica para establecer fallas y debilidades, y constancia para renovar y

actualizar dicha política en función del dinámico ambiente que rodea las organizaciones modernas.

A continuación se enumeran las políticas de seguridad que se recomienda implementar en cada una de las Instituciones analizadas:

- POLÍTICA DE SEGURIDAD FÍSICA
- POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN
- POLÍTICA DE CAMBIO DE CONTRASEÑA
- POLÍTICA DE DESTRUCCIÓN DE INFORMACIÓN OBSOLETA
- POLÍTICA DE COPIAS DE SEGURIDAD
- POLÍTICA DE PROTECCIÓN CONTRA SOFTWARE MALICIOSO
- POLÍTICA DE CONTROL DE ACCESO A SISTEMAS Y APLICACIONES
- POLÍTICA DE AUDITORIAS
- POLÍTICAS DE CAPACITACIÓN CONTINUA
- POLÍTICA DE LICENCIAMIENTO DE SOFTWARE
- POLÍTICA DE ADQUISICIÓN Y MANTENIMIENTO DE EQUIPOS INFORMÁTICOS
- POLÍTICA DE CUMPLIMIENTO

CAPITULO IV

Capacitaciones

4.1. CAPACITACIÓN SOBRE PREVENCIÓN DE INGENIERÍA SOCIAL

Para proteger efectivamente la información de cada una de las instituciones investigadas y minimizar el tiempo perdido por problemas en los equipos, es importante asegurar el punto más débil de la infraestructura, el personal.

OBJETIVO

Dar a conocer los diferentes tipos de ataques informáticos para el robo de información y cómo se puede combatir este tipo de ataque.

TEMAS

- Ingeniería Social
- Técnicas utilizadas por los Ingenieros Sociales
- Ejemplos de Ingeniería Social
- Formas de protección contra la Ingeniería Social

METODOLOGÍA DE TRABAJO

a. Reunión con los directivos de cada una de las instituciones (Institución Educativa, Institución Pública, Centro de Salud, Institución Comercial, ONG), para establecer prioridades generales de información y operación.

b. Evaluación de las políticas de seguridad actuales en cada institución.

c. Diseño y armado de las capacitaciones presenciales necesarias.

d. Charla general sobre metodologías comunes y pautas preventivas de seguridad de la información.

e. Capacitación general para todo el personal de las instituciones investigadas.

RESULTADOS

En cada institución investigada se realizó las capacitaciones al personal administrativo y de servicios, los cuales manifestaron su satisfacción en cuanto a los temas tratados en la misma, de igual forma se presentó ante cada uno de los directivos un plan de políticas de seguridad (anexo 1- ítem 1.2), el mismo que servirá para mejorar la seguridad de la información que a diario manejan. Adicional se hizo entrega de trípticos informativos, en los cuales se menciona conceptos de Ingeniería Social, técnicas utilizadas, ejemplos y formas de protección (Anexo 12).

Mediante encuestas realizadas a todo el personal capacitado (Anexo 5), se puede analizar los siguientes resultados:

En la segunda pregunta de la encuesta realizada a todas las instituciones se obtiene los siguientes porcentajes respectivamente:

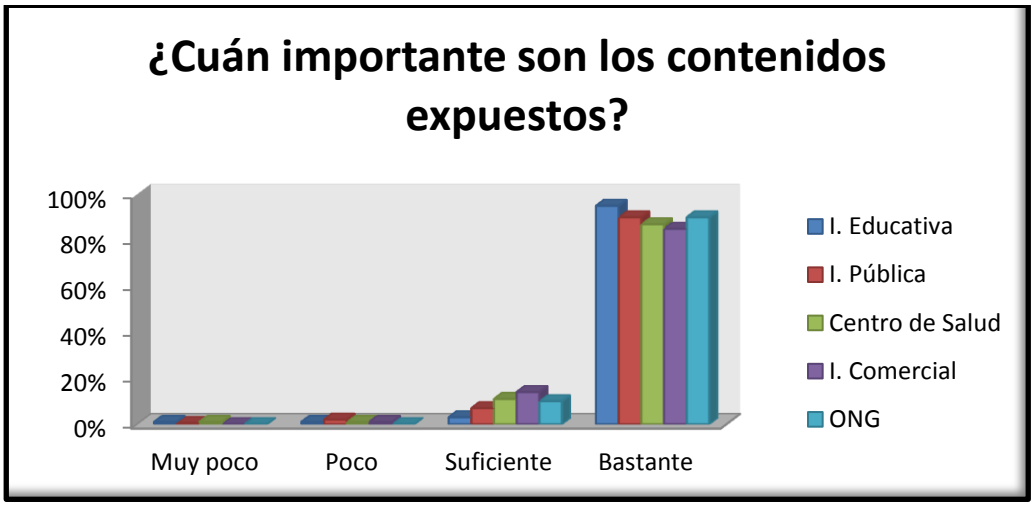


Gráfico 7. Contenidos expuestos

De acuerdo con estos resultados se puede concluir que los temas expuestos respecto a la Ingeniería Social han sido satisfactorios generalmente en un 95%. Es decir los contenidos expuestos sobre Ingeniería Social y sus diferentes técnicas de ataques han causado un gran impacto al personal de las instituciones, considerando que los temas y

medidas preventivas respecto a la Ingeniería Social, son útiles en el trabajo cotidiano de cada institución.

En la tercera pregunta se obtiene los siguientes porcentajes:

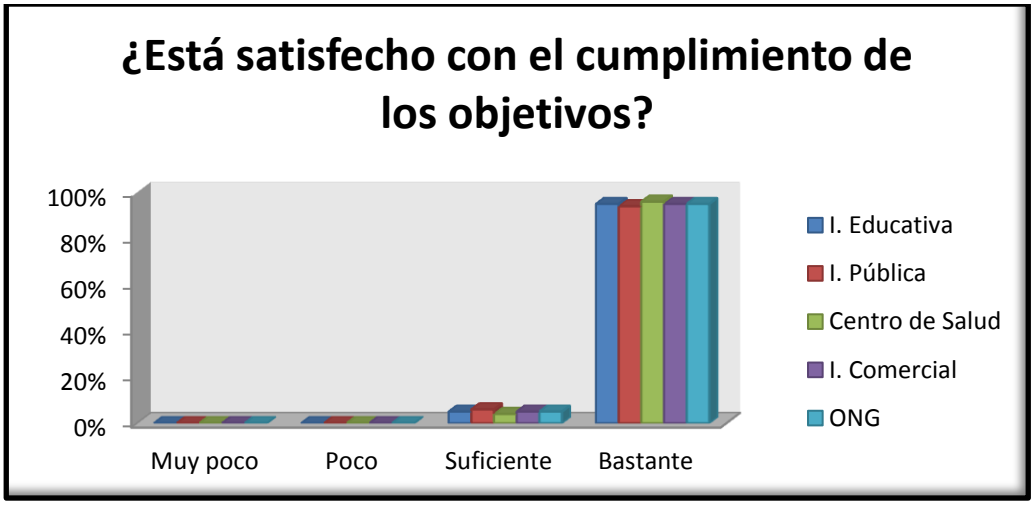


Gráfico 8. Cumplimiento de objetivos

En esta pregunta se obtiene los mismos resultados en cuanto a la satisfacción de los objetivos de la capacitación y del tema expuesto. Todo el personal capacitado de las diferentes instituciones, presenta un alto grado de satisfacción, por lo tanto se puede concluir que todos los temas investigados respecto a la Ingeniería Social en el mejoramiento de la seguridad de la información.

En la pregunta cuatro de la encuesta realizada se obtienen los siguientes resultados:

Gráfico 9. Superación de expectativas

Considerando estos porcentajes se concluye que los participantes de las capacitaciones, han superado las expectativas acerca de la ingeniería social en un 99% generalmente.

Como conclusión final, se obtiene que esta investigación si aporta en el mejoramiento de las instituciones, ya que con la encuesta realizada al personal de cada institución, se ha podido obtener altos porcentajes de satisfacción respecto a los temas de Ingeniería Social.

4.2. DISCUSIÓN

La Ingeniería Social se basa en engaños, estafas, fraudes y manipulación de personas mediante habilidades psicológicas, con el principal objetivo de obtener información confidencial como, contraseñas, números telefónicos, información confidencial, números de cuentas bancarias, documentos importantes de una institución, proyectos, etc.

Los Ingenieros Sociales utilizan diversas técnicas como: llamadas telefónicas, accesos no autorizados a sistemas, mirar por encima del hombro, buscar documentación en la basura, mediante correos

electrónicos, suplantación de identidad o utilizando diversas herramientas informáticas.

En esta investigación se analizó las técnicas más utilizadas de Ingeniería Social y las incidencias que pueden tener en nuestra sociedad. Se ha analizado cinco instituciones de la ciudad de Cariamanga, Institución Educativa, Institución Pública, Centro de Salud, Institución Comercial, ONG. Al utilizar técnicas de Ingeniería Social en las instituciones, se pudo constatar un alto grado de desconocimiento referente a robo de información en las diferentes áreas de la Institución.

Como resultado de encuestas, entrevistas, herramientas informáticas, técnicas de Ingeniería Social, se pudo recolectar información sobre las principales vulnerabilidades que actualmente tienen las instituciones y de esta forma poder emitir soluciones para contribuir con la seguridad de la información. El siguiente cuadro muestra las vulnerabilidades más comunes encontradas en las diferentes Instituciones en las cuales se realizó la investigación y sus respectivas soluciones:

VULNERABILIDADES MÁS COMUNES

VULNERABILIDAD	SOLUCIÓN
Falta de seguridad física y lógica en los departamentos.	Para solucionar esta vulnerabilidad es necesario implementar cámaras de seguridad principalmente en los departamentos de secretaría y financiero, ya que es aquí en donde se manipula mayor cantidad de información confidencial, además es indispensable contratar los servicios de un guardia de seguridad, el mismo que llevará un registro de todas las personas que ingresan a los departamentos.
Firewall de Windows deshabilitado.	En todos los equipos informáticos de los departamentos investigados, se procedió a habilitar el servicio de firewall, ya que de esta forma los equipos están protegidos ante cualquier amenaza de virus o código malicioso que pueda

	poner en riesgo la información que allí se almacena. Además se procedió a actualizar el software utilizando las últimas versiones
Contraseñas fácilmente identificables para los atacantes informáticos.	Se estableció como política de seguridad el uso de contraseñas seguras, combinando letras, números, signos y con un mínimo de 6 dígitos y de esta manera evitar que otras personas descubran con facilidad las contraseñas.
Falta de seguridad física.	Para solucionar esta vulnerabilidad se establecieron políticas d seguridad, en las cuales se menciona los diferentes procedimientos y puntos importantes que se deben considerar para preservar la seguridad de la información.
Desconocimiento de ataques informáticos	Todo el personal que labora en la Institución fue capacitado sobre temas relacionados con técnicas de robo de información (Ingeniería Social), esto con la finalidad de concientizar a los usuarios y evitar ser víctimas de los Ingenieros Sociales, semestralmente se reforzará los conocimientos sobre Ingeniería Social mediante capacitaciones continuas (ver anexo 13 y anexo 1- política 1.9).

Cuadro 20. Vulnerabilidades obtenidas mediante Nessus y suplantación de identidad (Anexo 9)

Al practicar cada una de estas soluciones se puede mejorar los servicios que ofrecen las instituciones y de igual forma se mejora el nivel de seguridad de la información.

Para contribuir con la seguridad de la información se realizaron capacitaciones dirigidas al personal de cada institución, mediante la cual se logró concientizar sobre las diversas formas de ataque informático para robar información, así mismo se presentó un plan de políticas de seguridad el mismo que será implementado en cada institución.

4.3. RESULTADOS

Como resultado del presente trabajo se obtiene que el tema de Ingeniería Social en las diversas Instituciones se dé con frecuencia en la actualidad ya que, para este tipo de ataque no es necesario contar con la mejor tecnología implementada o tener un alto nivel de conocimientos informáticos para acceder a una Institución y sustraer la información.

Actualmente la mayoría de los atacantes informáticos roban cualquier tipo de información únicamente haciendo uso de técnicas de engaño, soborno o ingenuidad de los usuarios, ya que la sociedad aun no esta capacitada ni tiene los suficientes conocimientos con respecto a técnicas de robo de información ni las formas de protección.

La seguridad de la información consiste en proteger la confidencialidad, integridad y disponibilidad de la misma, mediante políticas de mejoramiento, configuraciones de sistemas seguras y software actualizado. A través de estas técnicas de protección se puede preservar los datos almacenados en los diversos sistemas de información.

4.4. CONCLUSIONES

- El nivel de seguridad que tienen las Instituciones de la ciudad de Cariamanga es de 40%(porcentaje promedio obtenido mediante encuestas, entrevistas, técnicas de Ingeniería Social y herramientas informáticas) es decir que las Instituciones están propensas a sufrir ataques de Ingeniería Social esto se lo ha determinado mediante la aplicación de técnicas de Ingeniería Social y herramientas informáticas (capítulo 3).
- Considerando el estudio mostrado en el Capítulo 2 se concluye que en la actualidad los ataques más frecuentes se dan a través de llamadas telefónicas (42,2%) haciendo uso de la suplantación de identidad, también mediante el internet, a través de correos electrónicos (27,6%) y redes sociales.

- Mediante encuestas realizadas al personal que labora en cada institución se pudo determinar que un 59,2 % no tienen conocimiento en cuanto a la Ingeniería Social y sus diferentes formas de robar información, mientras que un 40,8% si conoce sobre la Ingeniería Social.
- Haciendo uso técnicas de Ingeniería Social, se accedió a departamentos importantes dentro de las instituciones, en donde se recolectó información sensible como contraseñas, información sobre el personal, información sobre los equipos informáticos, etc. Esto fue posible mediante la suplantación de identidad, observación directa, llamadas telefónicas, Phishing y herramientas informáticas (NESSUS).
- Una de las mejores formas de protección ante ataques de Ingeniería Social es la concientización o educación del personal esto mediante capacitaciones continuas.
- Se pudo determinar que en la nueva constitución de nuestro país constan artículos que penalizan los ataques y fraudes informáticos (Anexo 4).
- A través de la presente investigación se determinó que es de suma importancia implementar políticas de seguridad en las Instituciones de la ciudad de Cariamanga. Este manual de políticas fue entregado a cada directivo de las Instituciones (Anexo 15).
- Mediante capacitaciones impartidas a todo el personal de las Instituciones se da a conocer sobre las diferentes técnicas de ataque para el robo de información (ítem 4.1 y Anexo 12).
- Con este trabajo de investigación se concluye que los Ingenieros Sociales pueden hacer uso de diversas técnicas psicológicas, como: engaños, sobornos, amenazas, extorsión, etc., para obtener cualquier tipo de información de una institución.

- No hace falta tener altos conocimientos técnicos para tener acceso a los sistemas informáticos y en sí a la información que en ellos se manipula.

4.5. RECOMENDACIONES

- Educar al personal de cada una de las instituciones sobre las diferentes técnicas de robo de información, especialmente sobre Ingeniería Social y fomentar el uso de políticas de seguridad para evitar estos ataques (anexo 1- política 1.2.).
- Realizar auditorías para dar seguimiento al plan de mejoramiento de seguridad de la información presentado a los directivos de las instituciones.
- En las instituciones investigadas mantener el software, actualizado, ya que de esta forma se puede hacer frente a los efectos que puede provocar la ejecución de archivos con códigos maliciosos.
- Periódicamente hacer uso de las herramientas informáticas implementadas en cada una de las instituciones para determinar vulnerabilidades e identificar el grado de riesgo de las mismas.
- Mediante actividades de simulación de ataques y técnicas de Ingeniería Social verificar el grado de concientización del personal de las instituciones.
- Verificar previamente la veracidad de la fuente que solicite cualquier información sobre la red, equipo, información de la institución, etc., su localización y las personas que se encuentran al frente de la misma.
- Revisar periódicamente la configuración de los sistemas informáticos, sistema operativo, antivirus, firewall, aplicaciones, etc., con la finalidad de evitar el ingreso de códigos maliciosos (virus).
- Implementar las Políticas de Seguridad, las mismas que servirán para mejorar la seguridad de la información y disminuir los riesgos de robo de información en las instituciones.

ANEXOS

ANEXO 1: Políticas de Seguridad

MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

LOJA 2013

Este manual constituye las Políticas de Seguridad de la Información, aprobadas por cada uno de los principales dirigentes de las Instituciones en las cuales se realizó la investigación.

Es responsabilidad de todos quienes forman parte de cada una de las instituciones tanto públicas como privadas, cumplir con cada una de las políticas establecidas en este manual.

1.1. POLÍTICA DE SEGURIDAD FÍSICA

Objetivo

Mantener la adecuada protección de los equipos informáticos y conservación de la información de la Institución.

Alcance

Esta política rige para todos quienes conforman la institución, ya sea administradores, personal de servicio, personal de apoyo, etc.

Descripción de la política

La institución debe contar con un estándar específico para los departamentos en donde se manipula gran cantidad de información confidencial (Secretaría, Depto. Financiero, Depto. De Proyectos), tomando en consideración los siguientes puntos:

- Implementación de cámaras y alarmas de seguridad en los departamentos en donde se maneja información confidencial.
- Control de registro de todas la personas particulares que ingresan a la Institución, (número de cédula, nombres completos, departamento al que se dirige, motivo por el cual ingresa, hora de ingreso y hora de salida).

El área técnica de la Institución, físicamente debe considerar los siguientes puntos:

- La institución debe contar con un cuarto de comunicaciones, destinado únicamente para el área técnica, en el cual estarán ubicados todos los equipos de red (servidores, Reuters[12], switch[13], controles de energía, puntos de red).
- El cableado de red de datos y cableado eléctrico debe ser organizado y debidamente etiquetado.

[12]**Router.** Se trata de un producto de hardware que permite interconectar computadoras que funcionan en el marco de una red**.**
[13]**Switch:** Es el dispositivo analógico que permite interconectar redes, funcionando como un puente que transmite datos de un segmento a otro.

- Colocación de suficientes puntos eléctricos (toma corriente, interruptor de luz, UPS[14])
- Todo equipo informático deberá estar conectado a un UPS para regular la energía eléctrica.
- En caso de presentarse un incidente físico (incendios, inundaciones, destrucción del lugar), este debe ser reportado e investigado inmediatamente por el personal técnico de la Institución. Se debe identificar la severidad del caso para la toma de las medidas pertinentes.

En caso de requerir movilización de equipos se deberá regirse al siguiente estándar:

- Para la movilización de cualquier equipo informático, deben existir procedimientos formales por parte del responsable del área técnica y el dirigente de la Institución.
- Deben existir procedimientos formales para la movilización o adquisición de equipos informáticos.
- En caso de requerir movilizar los equipos informáticos fuera de la Institución se deberá registrar la fecha y hora de salida, datos del responsable de los equipos y datos de la persona de quien firmó la autorización para la movilización.

El recurso humano debe regirse al siguiente estándar:

- El personal técnico debe permanecer en su lugar de trabajo durante los horarios establecidos por la Institución, cumpliendo sus funciones respectivas.
- El personal técnico de la Institución deberá realizar revisiones semestrales al cableado eléctrico y de red, definiendo su respectiva organización.

[14] **UPS:** Es una fuente de suministro eléctrico que posee una batería con el fin de seguir dando energía a un dispositivo en el caso de interrupción eléctrica.

- Los administradores y personal en general no deben portar información sensible de la institución en medios extraíbles como: discos, flash memory's, celulares, discos duros portátiles, etc., fuera de las instalaciones de la Institución.
- Se prohíbe el ingreso de bebidas y alimentos a lugares en donde se manipule equipos informáticos.
- Las conexiones a las redes internas deben cumplir con los estándares de la Institución sobre servicios de red y control de accesos
- La arquitectura de la red de la Institución debe considerar la separación de redes que requieran distintos niveles de seguridad. Esta separación debe realizara de acuerdo al tipo de información almacenada en los sistemas que constituyen la red.

Responsabilidades

Los principales responsables para el cumplimiento de esta política son: Personal del departamento técnico, personal administrativo y personal en general que labore en la Institución.

Control de cumplimiento y sanciones

En caso de existir incumplimiento con alguno de los puntos antes mencionados en la presente política, por parte de un trabajador de la Institución, se comunicará inmediatamente a la Dirección General de la institución para que se tomen las medidas respectivas de sanción por incumplimiento, considerando las políticas institucionales internas.

1.2. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Objetivo

Establecer puntos importantes los cuales sirvan para preservar la seguridad de la información.

Alcance

Esta política rige para todos quienes conforman la institución, ya sea administradores, personal de servicio, personal de apoyo, etc.

Descripción de la política

Para preservar la seguridad de la información en la parte física, se debe cumplir con el siguiente estándar:

- Los equipos y sistemas informáticos deben contener la respectiva seguridad física y lógica (contraseñas, antivirus, firewall[15]), para preservar la seguridad de la información y evitar el acceso no autorizado a los mismos.
- Mediante un control de registro de personal autorizado para acceder a los diferentes departamentos e información confidencial, se evitará casos de suplantación de identidad tanto de personal como de recursos informáticos.
- Todo dispositivo digital que contenga información de la Institución (CD, flash memory's, etc.), debe presentar una etiqueta con la clasificación correspondiente.
- Desactivar puntos de red innecesarios en la misma.

Para mantener la seguridad de la información, lógicamente se debe cumplir con los puntos que se detallan a continuación:

[15]**Firewall:** Sirve para impedir que extraños accedan a su PC desde Internet. Los Firewalls pueden ser de dos tipos, de software o de hardware, y proporcionan una frontera de protección que ayuda a mantener fuera a los invasores no deseados de Internet.

- Toda la información debe ser clasificada y archivada como restringida, de uso interno, de uso general. Esta clasificación debe ser documentada por el responsable del departamento y aprobada por el Director de la Institución.
- La información y procedimientos tanto manuales como automatizados, deben estar disponibles en el momento necesario para el personal autorizado por la dirigencia de la Institución.
- Asegurar que la información y procedimientos institucionales, sean utilizados únicamente para fines laborales dentro de la Institución.
- Los programas de antivirus deben estar habilitados y actualizados en todos los equipos de cómputo. En caso de detectar fallas en el funcionamiento del programa estas deben ser comunicadas inmediatamente al personal técnico de la Institución.
- Todos los archivos adjuntos en los correos electrónicos, deben ser revisados por un antivirus antes de ser ejecutados.
- Toda la información enviada a través debe ser cifrada utilizando claves y algoritmos al momento de enviar y receptar el mensaje, para proteger la información ante accesos no autorizados

Responsabilidades

El personal del área técnica y administradores de la Institución, son los responsables del cumplimiento de esta política de seguridad, ya que son quienes deben revisar y aprobar las debidas autorizaciones para la manipulación tanto de equipos informáticos como de información confidencial, adicional a ello se debe supervisar periódicamente el cumplimiento de esta política. El director de cada departamento será el encargado de notificar al personal, sobre sus responsabilidades y cumplimiento de las políticas de seguridad de la información.

Control de cumplimiento y sanciones

En caso de existir incumplimiento con alguno de los puntos antes mencionados en la presente política, por parte de un trabajador de la Institución, se comunicará inmediatamente a la Dirección General de la institución para que se tomen las

medidas respectivas de sanción por incumplimiento, considerando las políticas institucionales internas.

1.3. POLÍTICA DE CAMBIO DE CONTRASEÑA

Objetivo

Proteger la información de la Institución mediante el uso adecuado de contraseñas.

Alcance

Esta política de seguridad rige para todos quienes conforman la Institución sin excepción alguna y su cumplimiento es de carácter obligatorio.

Descripción de la política

- Aplicación de un estándar para la creación de contraseñas seguras, para el acceso a los diferentes sistemas informáticos y servidores de la Institución.
    - ❖ La contraseña debe tener una longitud mínima de seis caracteres.
    - ❖ Debe ser una combinación de letras mayúsculas y minúsculas, números y caracteres especiales (EJEMPLO &Calvas_2013&).
    - ❖ No debe contener nombres personales, palabras comunes, referencias o datos de la institución a la que pertenece.
- Los sistemas informáticos deben estar configurados para que el usuario cambie su contraseña en forma obligatoria, cuando acceda al mismo por primera vez.
- Bloquear el usuario de la cesión de la aplicación, luego de 5 intentos fallidos.
- Cambiar la contraseña en un tiempo máximo de seis (6) meses o dependiendo de la criticidad de la información, en caso de no realizarse durante este periodo de tiempo, no podrá acceder al equipo y sus respectivos sistemas informáticos. En casos de existir este tipo de bloqueo en el equipo, se deberá presentar por escrito la respectiva solicitud para su respectiva activación, la misma que será entregada al personal técnico y Director de la Institución.

- Cambiar inmediatamente la contraseña al existir sospecha de sabotaje de la misma.
- Todos los equipos de cómputo deben ser configurados con un protector de pantalla con contraseña.
- Para preservar la seguridad de la información se debe seguir las siguientes instrucciones:
    - ❖ Bajo ninguna circunstancia se debe escribir las contraseñas en papel o almacenarlas en medios digitales.
    - ❖ No se debe divulgar las contraseñas a ninguna persona, salvo el pedido del Director de la Institución. En caso de divulgar la contraseña esta debe ser cambiada inmediatamente.
    - ❖ Los sistemas no deben mostrara las contraseñas en pantalla o en impresiones.

Responsabilidades

El personal técnico será el encargado de verificar que esta política y los aspectos que en ella se mencionan se cumplan a cabalidad, con la finalidad de preservar la seguridad de la información.

Control de cumplimiento y sanciones

En caso de existir incumplimiento con alguno de los puntos antes mencionados en la presente política, por parte de un trabajador de la Institución, se comunicará inmediatamente a la Dirección General de la institución para que se tomen las medidas respectivas de sanción por incumplimiento, considerando las políticas institucionales internas.

1.4. POLÍTICA DE DESTRUCCIÓN DE INFORMACIÓN OBSOLETA

Objetivo

Asegurar la confidencialidad de la información, mediante la destrucción absoluta de documentación obsoleta.

Alcance

Esta política comprende los diferentes tipos de soporte: papel, CD, archivos generales, etc.

Descripción de la política

- Para la destrucción absoluta de documentación se debe informar y solicitar al director de la Institución.
- Evitar arrojar documentación importante en los desechos de basura.
- Toda información almacenada en documentos impresos, se debe proceder a incinerar la misma, con la finalidad de destruir por completo la misma.
- Los dispositivos de almacenamiento móviles que contengan información de la Institución serán dados de baja y se procederá a incinerar los mismos.

Responsabilidad

Para el correcto funcionamiento de esta política, todo el personal administrativo y de servicio debe estar consciente de los efectos que ocurrirían en caso de dejar información confidencial de la Institución dentro de los botes de basura. Es por esto que todo el personal que conforma la Institución debe cumplir a cabalidad esta política.

Control de cumplimiento y sanciones

En caso de existir incumplimiento con alguno de los puntos antes mencionados en la presente política, por parte de un trabajador de la Institución, se comunicará inmediatamente a la Dirección General de la institución para que se tomen las medidas respectivas de sanción por incumplimiento, considerando las políticas institucionales internas.

1.5. POLÍTICA DE COPIAS DE SEGURIDAD

Objetivo

Salvaguardar la de los datos y software en general mediante el empleo de copias de seguridad que permitan garantizar la continuidad de las operaciones en la Institución.

Alcance

Política dirigida a toda información sensible y necesaria para la continuidad de los procesos en la Institución.

Descripción de la política

- Realizar un estudio sobre la información sensible de la Institución, para identificar: que tan crítico resulta para la Institución, que tanto cambia la información con el tiempo, volumen de la información que se maneja, etc.
- Establecer como medida de seguridad informática la necesidad de realizar copias de respaldo periódicamente en los equipos de cómputo administrativos y servidores.
- El personal técnico de la Institución es el responsable de asegurar que se generen copias de respaldo de la información de los sistemas informáticos y su administración segura.
- Trimestralmente se deben efectuar pruebas para verificar la capacidad de restauración de la información en caso de ser necesario, las mismas que se deben realizar en un ambiente diferente a al Institución.

- El personal del departamento técnico o sus delegados deben almacenar en un lugar seguro los dispositivos en donde se almacena la información sensible d la Institución.

Responsabilidad

Es responsabilidad del personal técnico administrar las copias de seguridad y así minimizar los riesgos ante la presencia de alguna catástrofe natural.

Es responsabilidad de todo el personal velar por el cumplimiento de esta política, ya que son ellos quienes deben realizar estas copias de seguridad con toda la información que a diario manipulan.

Control de cumplimiento y sanciones

En caso de existir incumplimiento con alguno de los puntos antes mencionados en la presente política, por parte de un trabajador de la Institución, se comunicará inmediatamente a la Dirección General de la institución para que se tomen las medidas respectivas de sanción por incumplimiento, considerando las políticas institucionales internas.

1.6. POLÍTICA DE PROTECCIÓN CONTRA SOFTWARE MALICIOSO

Objetivo

Evitar la infección de código malicioso en los sistemas informáticos y preservar la seguridad de los mismos.

Alcance

Política establecida para todos los equipos informáticos de trabajo y sistemas en ellos implementados.

Descripción de la política

- El software procedente de empresas no reconocidas o acreditadas como no confiables, no tendrá valor alguno para la Institución siempre que esta sea en formato ejecutable.
- El personal técnico supervisará la instalación y correcta configuración de software antivirus en todas y cada una de las estaciones de trabajo de la Institución.
- En caso de infección se procederá a determinar el origen del virus para eliminarlo y de esta forma evitar la reinfección en los equipos y sistemas.
- Prohibido el uso de dispositivos de almacenamiento como discos, flash memory's, disquetes, etc., ajenos a la Institución, a excepción de los provenientes de los proveedores o administradores técnicos los cuales necesariamente deben pasar por un procesos de verificación y control por el área técnica de la Institución.

- Para evitar la infección de código malicioso en los equipos de trabajo, el personal de la Institución no debe hacer uso de software que no haya sido analizado y autorizado por el área técnica.
- En caso de existir sospecha por infección de virus en el computador, se debe dejar de usar e informar inmediatamente al personal técnico, el mismo que verificará y erradicará el virus.

Responsabilidad

El personal que labora en la Institución es responsable de evitar contagiar el equipo de trabajo con códigos maliciosos o virus, los mismos que pueden estar incrustados en correos electrónicos o dispositivos móviles conectados al equipo.

Es de responsabilidad de departamento técnico o sus responsables del cumplimiento y control de la presente política.

Control de cumplimiento y sanciones

En caso de existir incumplimiento con alguno de los puntos antes mencionados en la presente política, por parte de un trabajador de la Institución, se comunicará inmediatamente a la Dirección General de la institución para que se tomen las medidas respectivas de sanción por incumplimiento, considerando las políticas institucionales internas.

1.7. POLÍTICA DE CONTROL DE ACCESO A SISTEMAS Y APLICACIONES

Objetivo

Evitar el acceso no autorizado a los sistemas informáticos y de esta forma preservar la seguridad de la información

Alcance

Esta política debe ser aplicada en todos los sistemas informáticos de la Institución.

Descripción de la política

Administradores

- El Administrador de Seguridad proporcionará toda la documentación necesaria para agilizar la utilización de los sistemas, referente a formularios, guías, controles, etc.
- Cualquier petición de información, servicio o acción proveniente de un determinado usuario o departamento, se deberá efectuar siguiendo los canales de gestión formalmente establecidos por la institución, para realizar dicha acción.

Usuarios finales

- Se asignará una cuenta de acceso a los sistemas, siempre y cuando se identifique previamente el objetivo de su uso o permisos explícitos a los que accederá, junto a la información personal del usuario.

- El acceso a la red por parte de terceros es estrictamente restrictivo y permisible únicamente mediante firma impresa y documentación de aceptación de confidencialidad hacia la institución y comprometido con el uso exclusivo del servicio para el que le fue provisto el acceso.
- No se proporcionará el servicio solicitado por un usuario, departamento o facultad, sin antes haberse completado todos los procedimientos de autorización necesarios para su ejecución.
- El usuario será responsable del uso que haga de su cuenta de acceso y contraseña de los sistemas o servicios informáticos.

Responsabilidad

Para dar cumplimiento de la presente política, los responsables son los miembros del departamento técnico o responsables de la administración de los sistemas y aplicaciones informáticas.

Control de cumplimiento y sanciones

Si no se da cumplimiento a esta política, se debe realizar los siguientes aspectos:

a. Negar por completo la ejecución de la acción o servicio.
b. Informe completo dirigido a comité de seguridad, mismo será realizado por la persona o el departamento al cual le es solicitado el servicio.
c. Sanciones aplicables por autoridades de nivel superior, previamente discutidas con el comité de seguridad.

En caso de existir incumplimiento con alguno de los puntos antes mencionados en la presente política, por parte de un trabajador de la Institución, se comunicará inmediatamente a la Dirección General de la institución para que se tomen las medidas respectivas de sanción por incumplimiento, considerando las políticas institucionales internas.

1.8. POLÍTICA DE AUDITORIAS

Objetivo

Realizar auditorias periódicas dentro de la Institución, sobre el cumplimiento de la normas y procedimientos asociados a la seguridad de la información.

Alcance

Esta política rige para todos los departamentos que conforman la Institución, sin excepción alguna.

Descripción de la política

Protección de las herramientas de la auditoria

- Todos los programas, aplicaciones, documentos y papeles de trabajo requeridos para la auditoría de sistemas deben protegerse ante las diferentes amenazas a las que pueda ser sometido.

Controles de auditorías

- Se realizará auditorías institucionales anualmente o cuando la Institución lo requiera.
- Las auditorías deben evaluar la confidencialidad y calidad de los sistemas utilizados, integridad y disponibilidad de los datos y cumplimiento de las especificaciones de este manual aprobadas por la Dirección de la Institución.
- Los resultados de las auditorías deberán ser eliminados periódicamente (transcurridas tres auditorías), para que no afecten el rendimiento de los servicios.
- Mediante las auditorías se determinará el cumplimiento de las medidas de seguridad incorporadas en sistemas informáticos, departamentos y sí a nivel de toda la Institución.

Responsabilidad

Para el cumplimiento de esta política el Director de la Institución deberá contratar los servicios especiales de un Auditor especializado y con experiencia, y de esta forma preservar la seguridad de la información.

Control de cumplimiento y sanciones

En caso de existir incumplimiento con alguno de los puntos antes mencionados en la presente política, por parte de un trabajador de la Institución, se comunicará inmediatamente a la Dirección General de la institución para que se tomen las medidas respectivas de sanción por incumplimiento, considerando las políticas institucionales internas.

1.9. POLÍTICAS DE CAPACITACIÓN CONTINUA

Objetivo

Concientizar al personal de la Institución sobre los diferentes ataques de Ingeniería Social, mediante charlas educativas periódicas.

Alcance

Esta política rige para todo el personal de la Institución.

Responsabilidad

El personal técnico de la Institución o sus delegados serán los encargados de realizar las capacitaciones en forma anual o cuando así lo requiera.

Descripción de la política

- Realizar charla general sobre metodologías comunes y pautas preventivas de seguridad de la información.
- Fomentar e innovar las capacitaciones con pautas específicas para mejorar la seguridad de la información.
- Periódicamente emplear diversos métodos de concientización como afiches, llaveros, mensajes de log-in, etc., los cuales recuerden al usuario el

papel importante que cumplen en la preservación de la seguridad de la información.

Control de cumplimiento y sanciones

En caso de existir incumplimiento con alguno de los puntos antes mencionados en la presente política, por parte de un trabajador de la Institución, se comunicará inmediatamente a la Dirección General de la institución para que se tomen las medidas respectivas de sanción por incumplimiento, considerando las políticas institucionales internas.

1.10. POLÍTICA DE LICENCIAMIENTO DE SOFTWARE

Objetivo

Regular y controlar, el uso y gestión de licencias de software utilizado en la Institución.

Nivel de responsabilidad o funciones

Personal técnico

- Mantener documentación respectiva de licencias de software existentes en la Institución, licencias entregadas a usuarios, y licencias disponibles.
- Generar reportes periódicos sobre la gestión de licencias
- Ejecutar procesos de concienciación e información a los usuarios finales, sobre ventajas y desventajas del uso adecuado de licenciamiento de software.
- Monitorear periódicamente el uso, instalación y gestión de licencias de software en los equipos utilizados en la Institución.
- Presentar al departamento de Dirección, informes semestrales sobre el estado de licencias existencias.

Usuario final

- Cumplir a cabalidad política de licenciamiento de software.
- Mantienen la responsabilidad de cuidar el software instalado en su equipo de trabajo.

Descripción de la política

- En caso de requerir instalación de software en los equipos informáticos de la Institución, el usuario debe solicitar por escrito al departamento técnico, su respectiva instalación previa autorización del Director de la Institución.
- En caso de existir software sin licencia, no regularizado o no registrado como aprobado por la Dirección de la Institución, la responsabilidad y sanciones respectivas recaerán sobre el usuario que labore con dicho software.
- Está estrictamente prohibido el uso de software que obtiene mediante otras fuentes (descargas de Internet, discos con copias), ya que esto puede implicar amenazas en la seguridad de la información de la Institución.
- El personal de técnico de la Institución no está autorizado para realizar instalaciones de software en otros equipos que no estén registrados en el inventario de activos fijos de la Institución.
- Informe inmediato al personal administrativo de la Institución, en caso de detectarse software no regularizado dentro de la misma.
- Todo equipo informático asignado al personal de la Institución, debe utilizarlo única y exclusivamente él, cumpliendo las normativas y responsabilidades de esta política de licenciamiento de software.

Restricciones para esta política

- Instalación y utilización de software sin licencia en los equipos informáticos de la Institución.
- Instalación y utilización de programas de generación de códigos de licenciamiento.
- Instalación y utilización de software de propiedad de la Institución, en equipos computacionales ajenos a la misma.

1.11. POLÍTICA DE ADQUISICIÓN Y MANTENIMIENTO DE EQUIPOS INFORMÁTICOS

Objetivo

Definir y documentar los procedimientos que se aplicaran durante el ciclo de vida de los activos

Alcance

Esta política de seguridad se aplica para todos los equipos informáticos adquiridos por la Institución.

Descripción de la política

- Cualquier adquisición que se realice debe estar debidamente registrada y documentada por el responsable del departamento técnico como del director de la Institución.
- Todos los equipos de cómputo y sistemas informáticos deben autenticarse en el registro oficial de activos fijos, en Dirección de la Institución.
- Difundir las disposiciones mencionadas en esta política de adquisición de hardware y sanciones a tomar en caso de que se incumpla con la misma.

Antes de realizar cualquier adquisición de equipos informáticos, se debe tomar en consideración los siguientes puntos:

- Definir las funciones del equipo, valorar las necesidades de las aplicaciones, es decir, en qué departamento será utilizado o para que funciones se demandan.
- Considerar el posible crecimiento o proyección de las aplicaciones, esto en capacidad de trabajo como en capacidad de proceso y almacenamiento.

- Tomar en cuenta las garantías y valor agregado, es decir, todo aquello que el proveedor pueda ofrecer por el producto (garantía, soporte técnico, soporte en línea, reemplazo de equipo, etc.)

Responsabilidad

Para el cumplimiento de esta política el personal encargado será el departamento técnico bajo la debida autorización y aprobación del Director de la Institución.

Control de cumplimiento y sanciones

En caso de existir incumplimiento con alguno de los puntos antes mencionados en la presente política, por parte de un trabajador de la Institución, se comunicará inmediatamente a la Dirección General de la institución para que se tomen las medidas respectivas de sanción por incumplimiento, considerando las políticas institucionales internas.

1.12. POLÍTICA DE CUMPLIMIENTO

Objetivo

Cumplir con las disposiciones legales establecidas en la constitución del país, con la finalidad de evitar sanciones administrativas a la Institución o al empleado que incurra en responsabilidad civil o penal como resultado de su incumplimiento.

Alcance

Esta política se aplica para los sistemas de información, procedimientos, documentación y en general a todo el personal de la Institución.

Descripción de la política

- La Institución está sujeta al cumplimiento y respeto de las leyes y normativas establecidas en la constitución del Ecuador, en especial:
  - ❖ Derechos de propiedad intelectual
  - ❖ Código de trabajo
  - ❖ Código tributario

- Establecer normativas y procedimientos que definan el uso legal de productos informáticos y software.
- Divulgar las políticas de adquisición de software y hardware y notificar la determinación de tomar acciones disciplinarias contra el personal de las incumpla.
- Todo tipo de hardware y software utilizado por la Institución debe tener su respectivo registro de licencia.
- La Institución puede obviar algunas de las políticas de seguridad definidas en este documento, únicamente cuando se ha demostrado que existen impactos negativos para la Institución. Toda excepción de políticas debe ser documentada y aprobada por el Director de la Institución detallando el motivo por el que justifica el no-cumplimiento de la misma.

Responsabilidad

Los encargados de preservar la seguridad de la información son todos quienes forman parte de la Institución.

Control de cumplimiento y sanciones

En caso de existir incumplimiento con alguno de los puntos antes mencionados en la presente política, por parte de un trabajador de la Institución, se comunicará inmediatamente a la Dirección General de la institución para que se tomen las medidas respectivas de sanción por incumplimiento, considerando las políticas institucionales internas.

ANEXO 2: Encuesta realizada a los directivos de cada institución.

Objetivo: Conocer qué tipo de sistemas manipulan y determinar el perfil administrativo y de servicios de la institución.

1. **¿A qué sector pertenece la institución?**
   ☐ Sector Público ☐ Sector Privado

2. **¿Cuántos departamentos o áreas conforman la institución?**
   ☐ 1 ☐ 4
   ☐ 2 ☐ 5
   ☐ 3 ☐ 6
   Cuáles son: _____

3. **¿Qué tipo de información manipulan?**
   _____
   _____

4. **¿Qué procesos realizan en cada departamento?**
   _____
   _____

5. **¿Con qué sistemas informáticos cuenta la institución?**
   _____
   _____

6. **¿La institución cuentan con personal técnico especializado para la manipulación de los diferentes sistemas informáticos?**
   ☐ Si ☐ No
   Porque: _____
   _____

7. **¿Cómo resguardan la seguridad de la información?**
   _____
   _____

8. **¿Los sistemas informáticos y software que utiliza la institución, cada que tiempo lo actualizan?**
   _____
   _____

ANEXO 3: Encuestas realizadas a todo el personal administrativo de cada una de las Instituciones.

Objetivo: Medir su nivel de conocimiento sobre la Ingeniería Social y su impacto en nuestra comunidad.

1. **¿Ha escuchado sobre Ingeniería Social?**

   Si ( ) No ( )

2. **¿Qué tipo de servidor de correo electrónico utiliza?**
   ( ) Hotmail
   ( ) Yahoo
   ( ) Gmail
   ( ) Otros: _____

3. **¿Cada qué tiempo utiliza su correo electrónico?**
   ( ) Todos los días
   ( ) Dos veces por semana
   ( ) Una vez al mes
   ( ) Casi nunca

4. **¿Con qué frecuencia cambia sus contraseñas?**
   ( ) Nunca ( ) Cada mes

5. **¿Cree usted que el correo electrónico es seguro? ¿Por qué?**
   ( ) Si ( ) No
   ¿Por qué?_____

6. **¿En alguna ocasión ha recibido correos electrónicos solicitando información confidencial?**
   ( ) Si ( ) No

7. ¿Envía cadenas de correos? ¿A cuántas personas?

( ) Si ( ) No

( ) 5 a 10 personas

( ) 10 a 20 personas

( ) 20 a 35 personas

( ) Más de 35 personas

8. ¿Cuál es su actitud frente a correos electrónicos en los que le aparece un mensaje que podría contener virus?

( ) Elimina los correos electrónicos

( ) No les presta atención

( ) Verifica si es confiable y abre el correo electrónico

( ) Abre el correo sin prestar atención

9. ¿En alguna ocasión ha olvidado sus contraseñas en lugares visibles?

Si ( ) No ( )

10. ¿Alguna vez ha proporcionado información confidencial a terceras personas?

Si ( ) No ( )

11. De las siguientes técnicas ¿Usted, de cual ha sido víctima?

( ) Llamada telefónica

( ) Correo electrónico

( ) Mensaje de texto

( ) Cara a cara

ANEXO 4: Encuesta realizada al Director y Gerente de cada una de las instituciones investigadas, para determinar si en las Instituciones de la ciudad de Cariamanga ha existido casos de Ingeniería Social y cuáles son las técnicas más utilizadas por los atacantes informáticos.

1. **¿La institución ha sido víctima de Ingeniería Social?**

   ( ) SI ( ) NO

2. **¿Mediante qué técnica han actuado los Ingenieros Sociales?**

   ( ) Teléfono
   ( ) Cara a cara
   ( ) Messenger MSN
   ( ) Mensaje de texto

3. **¿En qué áreas se han registrado más casos de ataques informáticos?**

   ( ) Área técnica
   ( ) Área financiera
   ( ) Área contable
   ( ) Área de recursos humanos
   ( ) Área gerencial

4. **¿Qué tipo de información fue manipulada por los atacantes informáticos?**

   ( ) Transacciones bancarias
   ( ) Correos electrónicos
   ( ) Accesos a sistemas
   ( ) Archivos de la institución

5. **¿Ha sufrido algún tipo engaño, amenaza o extorción, de personas desconocidas con la finalidad de revelar información confidencial?**

   ( ) SI ( ) NO

Especifique:

_____

_____

6. **¿Qué inconvenientes o consecuencias ha tenido, debido a la perdida de información a través de Ingeniería Social?**

   ( ) Sociales

   ( ) Legales

   ( ) Económicos

   ( ) Otros: _____

7. **¿Cuáles serían sus recomendaciones respecto a los ataques informáticos?**

   _____

   _____

ANEXO 5: Encuesta realizada a todo el personal capacitado de cada institución investigada de la ciudad de Cariamanga.

OBJETIVO: Es importante conocer el concepto que tiene acerca de la capacitación que ha recibido, por esta razón se le solicita que responda la presente encuesta.

Fecha: _____

Institución: _____ Cargo: _____

1. **Califique el expositor en los siguientes aspectos: (Favor marcar con una x)**

	Excelente	Bueno	Regular	Malo
Profundidad en el manejo del tema				
Orden de la presentación				
Claridad de la exposición				
Capacidad para motivar				
Material didáctico utilizado				
Aclaración de dudas				
Puntualidad				
Manejo del tiempo				

2. **En la práctica, ¿Qué tan útiles considera que son los contenidos expuestos**?

Muy poco	Poco	Suficiente	Bastante

3. ¿Está usted satisfecho con el cumplimiento de los objetivos de la capacitación y tema expuesto?

	Muy poco	Poco	Suficiente	Bastante
Capacitación				
Tema				

¿Por qué?

_____

_____

4. ¿Se superaron las expectativas respecto a los temas tratados?

Sí ____ No ____

¿Por qué? _____

_____

5. El siguiente espacio es para sus comentarios y sugerencias.

_____

_____

ANEXO 6: Técnica de suplantación de identidad y observación

Una de las técnicas más utilizadas por los atacantes informáticos es la suplantación de identidad y observación, es por ellos que para determinar casos reales de Ingeniería Social fue ejecutada en cada una de las instituciones investigadas de la ciudad de Cariamanga.

Para la ejecución de estas técnicas se utilizó únicamente hacer uso de habilidades, conocimientos y aptitudes para identificar las víctimas e iniciar con la recolección de información confidencial. Tanto la suplantación como la observación fueron ejecutadas en conjunto, es decir, al suplantar al personal técnico se pudo acceder a los diferentes sistemas e información sensible de cada institución y mediante la observación se revisó en forma directa documentación sobre los escritorios y la memorización de la mayor cantidad de información que circulaba en el departamento. Estas técnicas fueron ejecutadas de la siguiente manera y se obtuvo información confidencial como:

INSTITUCIÓN EDUCATIVA

Departamento de Secretaría
Secretaria: Ing. Hilda Vega
Descripción

- En este departamento disponen de un computador individual en donde se accedió al usuario HildaMaría, así mismo se obtuvo la dirección IP del equipo 200.107.x.x
- Se obtuvo información confidencial a través de una conversación en la cual se le preguntó que procesos realizaba en su computador y que información almacenaba en la misma.
- Parte de la información que se recolectó fueron antecedentes de los docentes, registros de asistencias del personal, futuros proyectos para la institución.

- En los escritorios se observó solicitudes, oficios, programadores de la institución, los mismos que estaban dirigidos al Dr. Wilson Bravo, rector de la institución en los que se visualizó nombre y números de cédula.
- Adicional se tuvo acceso a información confidencial de los docentes de la institución, nombres completos, correos electrónicos, números de cédula, números telefónicos, números de cuentas bancarias.

Conclusión

- La secretaria no pidió ningún tipo de identificación para acceder al departamento y a los equipos informáticos.
- Dejar el computador a disposición sin emitir ningún tipo de restricción

Departamento de DOBE

Secretaria: Lic. Aura Flores

Descripción

- Se tuvo acceso al sistema mediante el usuario aflores, de igual forma se obtuvo la dirección IP del equipo 200.107.x.x
- Parte de la información que se recolectó fueron antecedentes de los estudiantes con calificaciones, asistencias, permisos.
- En los escritorios se observó solicitudes, oficios, programadores de la institución.

Conclusión

- La secretaria no pidió ningún tipo de identificación para acceder al departamento y a los equipos informáticos.
- Otorgar información confidencial en presencia de terceras personas.

INSTITUCIÓN PÚBLICA

Departamento de Secretaría

Secretaria: Lic. Amparito Ruiz

Descripción

- Disposición de un computador individual en donde se accedió al usuario aruiz, así mismo se obtuvo la dirección IP del equipo 168.24.x.x
- Se obtuvo información confidencial a través de conversaciones, mediante las cuales se recolecto información sobre el sistema, proyectos, información que a diario manipula.
- En los escritorios se observó solicitudes, oficios, programadores de la institución.
- Adicional se tuvo acceso a información confidencial de todo el personal de la institución, nombres completos, correos electrónicos, números de cédula, números telefónicos, números de cuentas bancarias.

Conclusión

- La secretaria no pidió ningún tipo de identificación para acceder al departamento y a los equipos informáticos.
- Dejar el computador a disposición sin emitir ningún tipo de restricción.

Departamento Financiero

Secretaria: Lic. Gladys Bravo

Descripción

- Se tuvo la dirección IP del equipo 168.24.x.x
- Parte de la información que se recolectó fueron estados de cuenta de la institución.
- En los escritorios se observó proyectos, oficios, los mismos que contenían información como correos electrónicos, nombres, números telefónicos.

Conclusión

- La secretaria no pidió ningún tipo de identificación para acceder al departamento y a los equipos informáticos.
- Otorgar información confidencial en presencia de terceras personas.

CENTRO DE SALUD

Departamento de Estadística

Secretaria: Lic. Elizabeth Cueva

Descripción

- Para acceder al sistema de historias clínicas se utilizó el usuario cuevaEli, así mismo se obtuvo la dirección IP del equipo 178.64.x.x
- Se recolectó información confidencial del personal médico, registro de los pacientes, actividades de centros asociados a la institución.
- En los escritorios se observó historias clínicas impresas, informes médicos, registros de pacientes.

Conclusión

- La secretaria no pidió ningún tipo de identificación para acceder al departamento y a los equipos informáticos.
- Dejar el computador a disposición sin emitir ninguna restricción

INSTITUCIÓN COMERCIAL

Departamento Administrativo

Secretaria: Ing. Nancy Castillo

Descripción

- Se obtuvo información confidencial a través de una conversación en la cual se le preguntó que procesos realizaba en su computador e información que a diario manipulan.
- La información que se recolectó fueron datos confidenciales del personal, información de los proveedores, información de los productos.
- Se tuvo acceso a la base de datos de productos en la cual se pudo observar nombres, cantidad de productos existentes, valor económico, códigos de seguridad.

- En los escritorios se observó facturas de proveedores, solicitudes.

Conclusión

- La secretaria no pidió ningún tipo de identificación para acceder al departamento y a los equipos informáticos.
- Dejar el computador a disposición sin emitir ningún tipo de restricción

ONG

Departamento de Secretaría

Secretaria: Lic. Susana Torres

Descripción

- Se accedió al usuario torresSusana
- La información que se recolectó fueron proyectos por ejecutar y en ejecución, nombres de auspiciantes, registro de patrocinadores, registro del personal de la institución.
- En el escritorio se observó documentación como, oficios, proyectos, solicitudes.

Conclusión

- La secretaria no pidió ningún tipo de identificación para acceder al departamento y a los equipos informáticos.
- Dejar el computador a disposición sin emitir ningún tipo de restricción
- La secretaria digitó la contraseña en presencia de otras personas y no se percató que la estaban observando.

Departamento de Proyectos

Secretaria: Lic. Ángel Jiménez

Descripción

- Se tuvo acceso al sistema mediante el usuario jimenez12.

- Se recolectó información como nombres de patrocinadores, estado de los proyectos, informes de actividades.
- Informe de información confidencial mediante diálogo.
- En los escritorios se observó solicitudes, oficios, programadores de la institución.

Conclusión

- Para ingresar no pidió ningún tipo de identificación ya sea al departamento o equipos informáticos.
- Otorgar información confidencial en presencia de terceras personas.

ANEXO 7: Técnica de envío de correo electrónico o Phishing

El correo electrónico es una forma de acercamiento hacia la víctima que permite introducirse disfrazado de muchas formas, ya sea que la dirección de correo electrónico resulte familiar o el asunto del e-mail produzca un impacto de curiosidad, avaricia, compasión o miedo y es donde el usuario se vuelve susceptible a abrirlo. A continuación se presenta un informe de los ataques realizados a direcciones de correo electrónico del personal administrativo, docente y personal de servicio, haciendo uso de la herramienta en línea WhoReadMe.

INFORME

Se empezó a formular un mensaje llamativo para atraer la atención de los usuarios y este abra y ejecute el archivo adjunto. A continuación se presenta la imagen del mensaje enviado a los distintos usuarios:

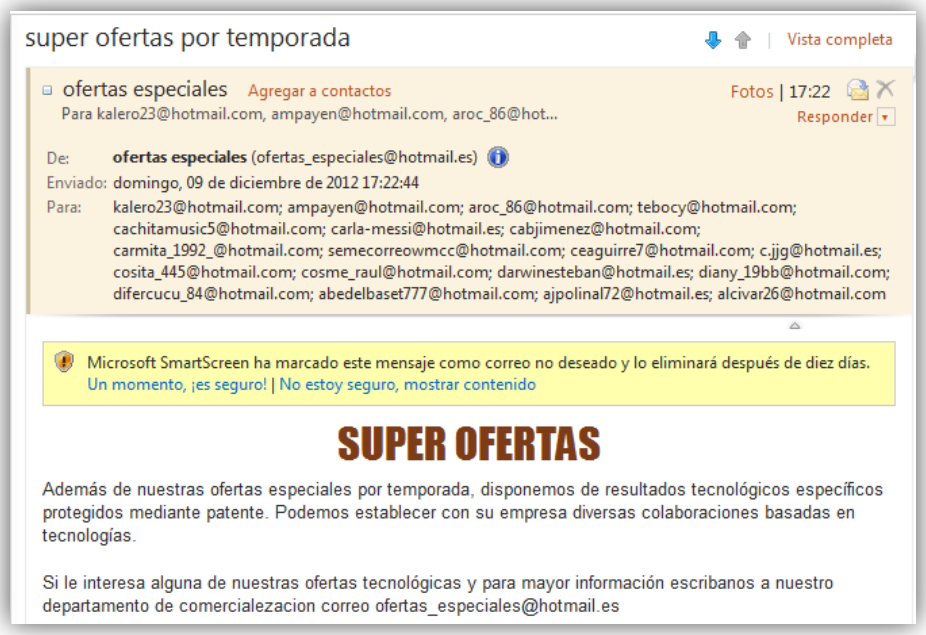


Figura 5. Interfaz de correo enviado

Cuando el mensaje es recibido y abierto el archivo adjunto, inmediatamente se recibe una notificación con los datos del equipo en donde fue abierto el email.

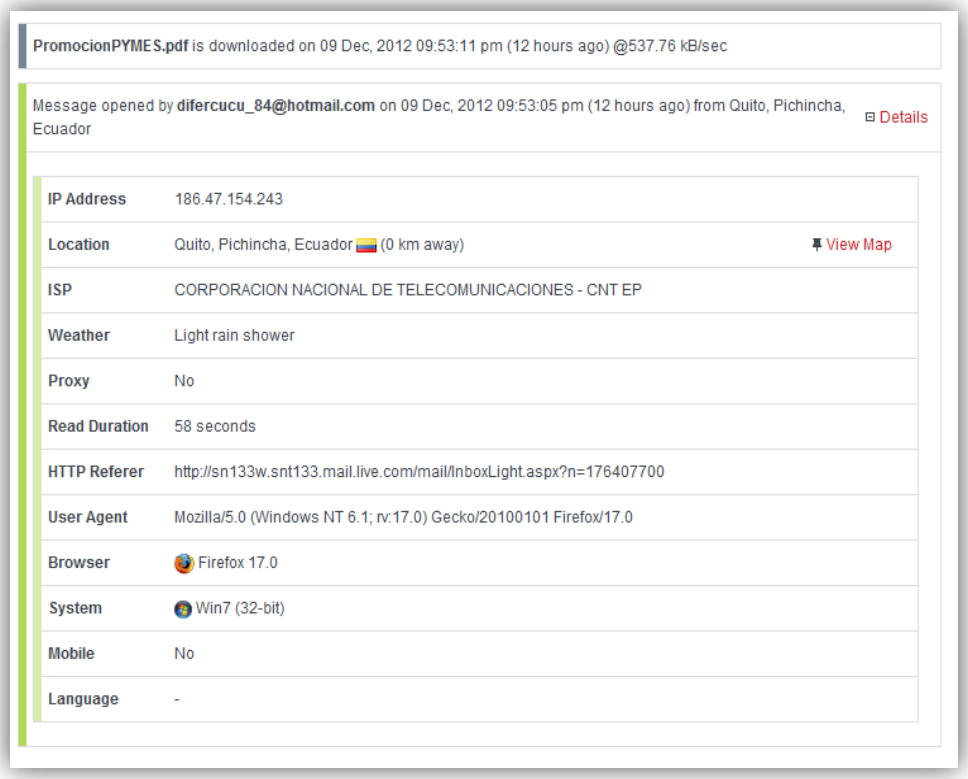


Figura 6. Informe del equipo

Conclusión

- Mediante esta herramienta se puede conocer datos del equipo y sistema en donde fue abierto el correo.
- Pueda que no todos abran el correo, pero los usuarios que si lo hacen tienden a poner en riesgo la seguridad de su información.

ANEXO 8: Técnica de llamada telefónica

Esta es una de las técnicas más fáciles de utilizar pero en ocasiones no se obtiene los resultados como se esperaba, debido a que la persona no dé la información requerida o que simplemente no conteste. Al realizar llamadas telefónicas se puede ocultar el número y mantener el anonimato, permite actuar a distancia de la víctima y persuadirla sicológicamente, para obtener la información requerida.

Esta técnica de Ingeniería Social fue aplicada al personal de instituciones de la ciudad de Cariamanga en los cuales se profundizó en habilidades sicológicas manteniendo la educación, hablar claro en forma fluida para ganar la confianza de la víctima. A continuación se presenta el formato de la llamada telefónica, la misma que fue realizada a los administrativos de cada institución respectivamente. Cabe recalcar que en todos los departamentos e instituciones se utilizó el mismo formato, por lo que el presente informe es a nivel general.

Informe

Al utilizar esta técnica primeramente se indicó se técnicos de soporte y era necesario realizar actualizaciones del antivirus, para lo cual se requiere conocer algunos datos importantes del equipo y sistema informático, además se obtiene más información de la requerida ya que últimamente se han presentado inconvenientes técnicos con el equipo.

Detalle de la llamada

- Buenos días, ¿Con quién tengo el gusto?
  - *Con.....*
- Soy del departamento técnico y me gustaría hablar con……..
  - *Soy yo mismo*
- Mi llamada tiene que ver con las actualizaciones de antivirus de la máquina y queremos que usted mismo nos ayude desde su equipo, realizando las modificaciones, para ello yo le iré indicando por teléfono los pasos de manera rápida y sencilla.

- *Está bien*

- Primeramente ayúdeme abriendo el ícono del antivirus, pero antes de eso debe indicarme el IP de su equipo, usuario y contraseña para poder enviarle las actualizaciones de la fecha.
  - *Espere un momento……..haber es……..*
- Ahora si ya estoy enviándole las actualizaciones solo espere unos minutos, mientras ayúdeme con unos datos para poder llenar el registro de actualización. Solo usted manipula el equipo…….. que tipo de información maneja……. con que tipo de sistemas trabaja……..
- Bueno he terminado, disculpe la molestia, gracias por su colaboración, para cualquier inquietud comuníquese con soporte técnico, estamos para servirle.
  - *Ok. Gracias*

ANEXO 9: Herramienta para comprobar la fiabilidad de la contraseña

Para determinar la fortaleza de las contraseñas, se utilizó el programa en línea PasswordMeter, el cual permitió determinar qué tan seguras son las contraseñas que actualmente utiliza el personal de cada una de las instituciones investigadas. En las siguientes imágenes se muestra claramente los resultados en cuanto a la combinación de caracteres en las contraseñas:

COMPRUEBA LA FIABILIDAD DE TU CONTRASEÑA

Prueba tu Contraseña		Requerimientos recomendados
Contraseña:	••••••••••••••	Tamaño mínimo de 8 caracteres Contener al menos 3-4 de las siguientes cosas: - Letras en Mayúsculas - Letras en Minúsculas - Números - Símbolos
Ocultar:	☑	
Resultado:	72%	
Complejidad:	Fuerte	

Adiciones		Tipo	Ratio	Contador	Puntos
✓	Número de Caracteres	Fijo	+(n*4)	14	+ 56
✗	Letras Mayúsculas	Cond/Incr	+((len-n)*2)	0	0
✓	Letras minúsculas	Cond/Incr	+((len-n)*2)	8	+ 12
✓	Números	Cond	+(n*4)	4	+ 16
✓	símbolos	Fijo	+(n*6)	2	+ 12
✓	Mitad Números o símbolos	Fijo	+(n*2)	5	+ 10
✓	Requerimientos	Fijo	+(n*2)	4	+ 8
Deducciones					
✓	Solo Letras	Fijo	-n	0	0
✓	Solo Números	Fijo	-n	0	0
!	Caracteres Repetidos (No sensible)	Incr	-(n(n-1))	4	- 4

Figura 7. Resultado del escaneo de contraseñas seguras

COMPRUEBA LA FIABILIDAD DE TU CONTRASEÑA

Prueba tu Contraseña		Requerimientos recomendados
Contraseña:	••••••••••••	Tamaño mínimo de 8 caracteres Contener al menos 3-4 de las siguientes cosas: - Letras en Mayúsculas - Letras en Minúsculas - Números - Símbolos
Ocultar:	☑	
Resultado:	50%	
Complejidad:	Buena	

Adiciones		Tipo	Ratio	Contador	Puntos
✓	Número de Caracteres	Fijo	+(n*4)	12	+ 48
✗	Letras Mayúsculas	Cond/Incr	+((len-n)*2)	0	0
✓	Letras minúsculas	Cond/Incr	+((len-n)*2)	8	+ 8
✓	Números	Cond	+(n*4)	4	+ 16
✗	símbolos	Fijo	+(n*6)	0	0
✓	Mitad Números o símbolos	Fijo	+(n*2)	4	+ 8
✗	Requerimientos	Fijo	+(n*2)	3	0
Deducciones					
✓	Solo Letras	Fijo	-n	0	0
✓	Solo Números	Fijo	-n	0	0
!	Caracteres Repetidos (No sensible)	Incr	-(n(n-1))	4	- 4

Figura 8. Resultados del escaneo de contraseñas

Conclusión

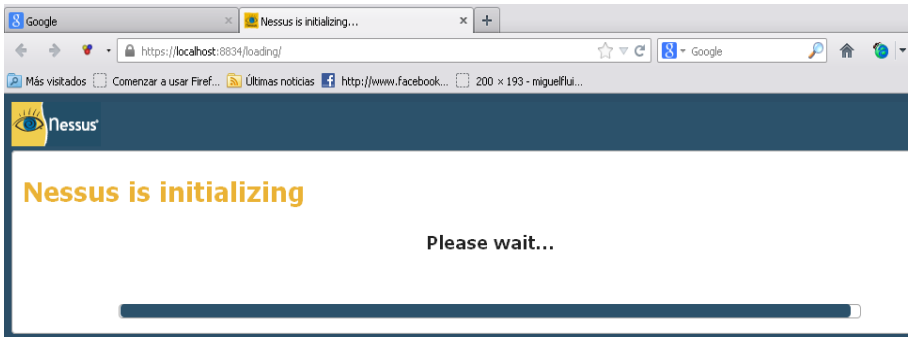
- Las contraseñas en las cuales se utiliza nombres propios, técnicamente no son seguras ya que están más propensas a ser descubiertas con facilidad.
- La mayoría del personal de las instituciones utiliza contraseñas débiles, es decir utiliza nombres de familiares, mascotas, fechas de nacimiento, números de cédula o números telefónicos.

ANEXO 10: Utilización de herramienta Nessus

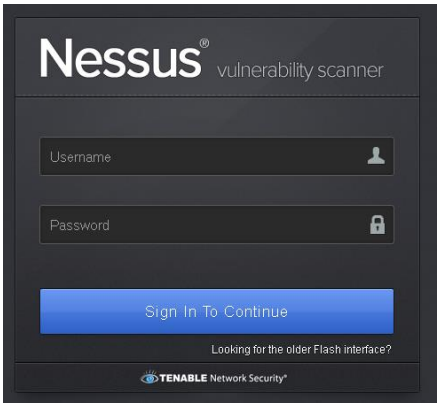
Es una herramienta para escanear vulnerabilidades. Se caracteriza por tener alta velocidad de descubrimiento, auditoria en la configuración de aplicaciones, descubrimiento de datos sensibles y análisis de vulnerabilidades de la red. NESSUS puede estar distribuido a lo largo de toda una empresa, incluyendo la DMZ (Zona Desmilitarizada) y demás redes físicamente separadas. NESSUS soporta los siguientes tipos de auditorías de seguridad: Escanear puertos o Escanear vulnerabilidades en la red o Auditoria en la configuración de plataformas Windows y Unix o Pruebas de vulnerabilidad sobre aplicaciones web embebidas Auditoria en la configuración de bases de datos SQL

Para poder realizar un escaneo a través de la herramienta ***NESSUS 5*** se realizó los siguientes pasos:

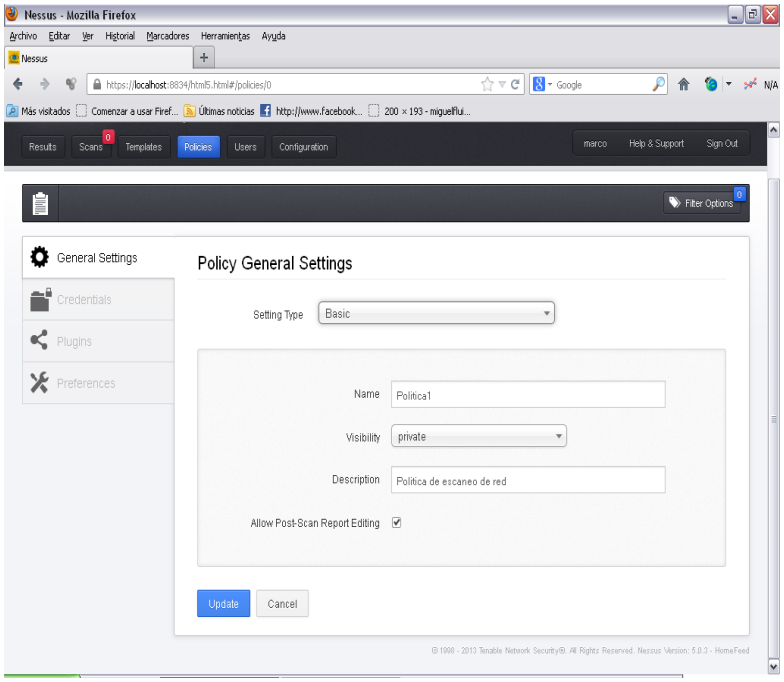
1) Inicialización del programa



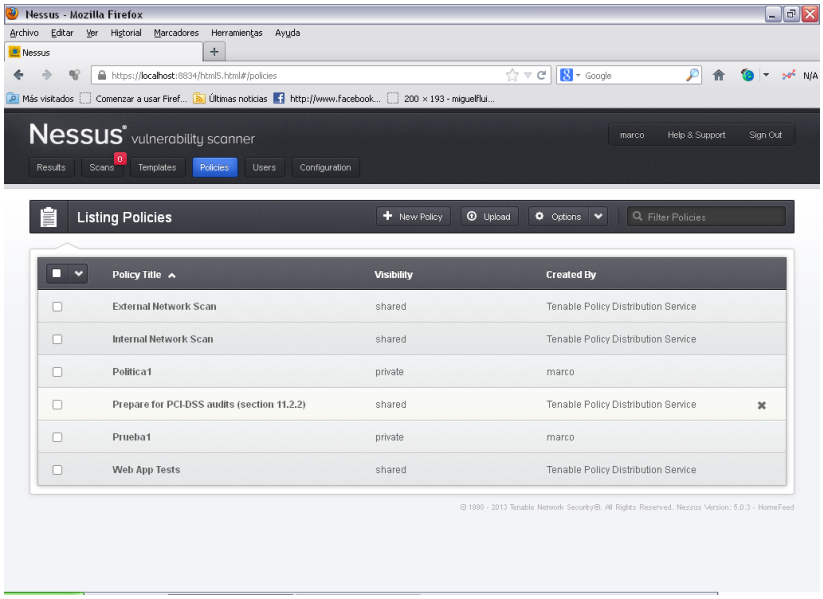
2) Usuario y Contraseña



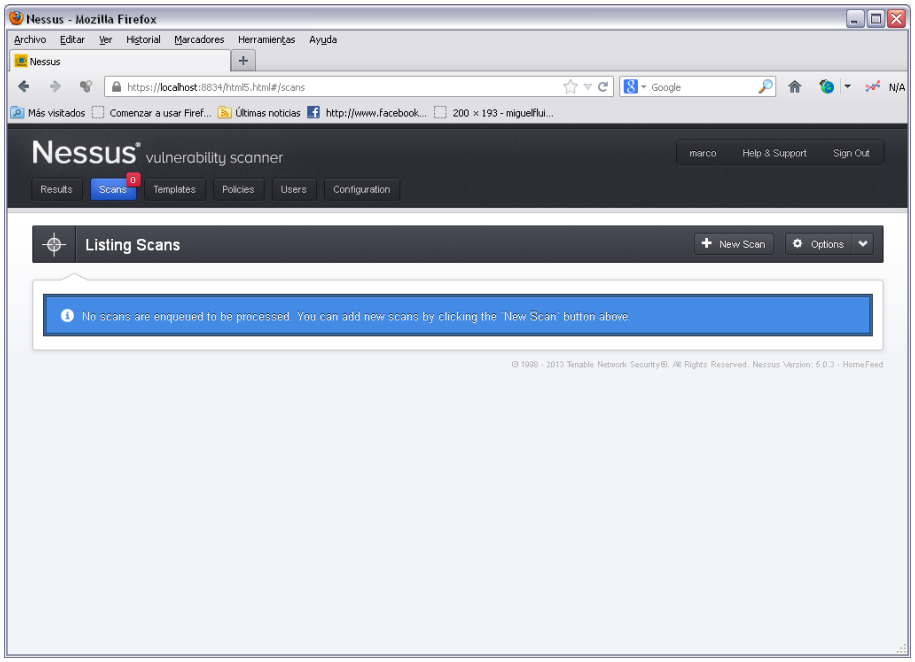
3) Creación de una política de escaneo



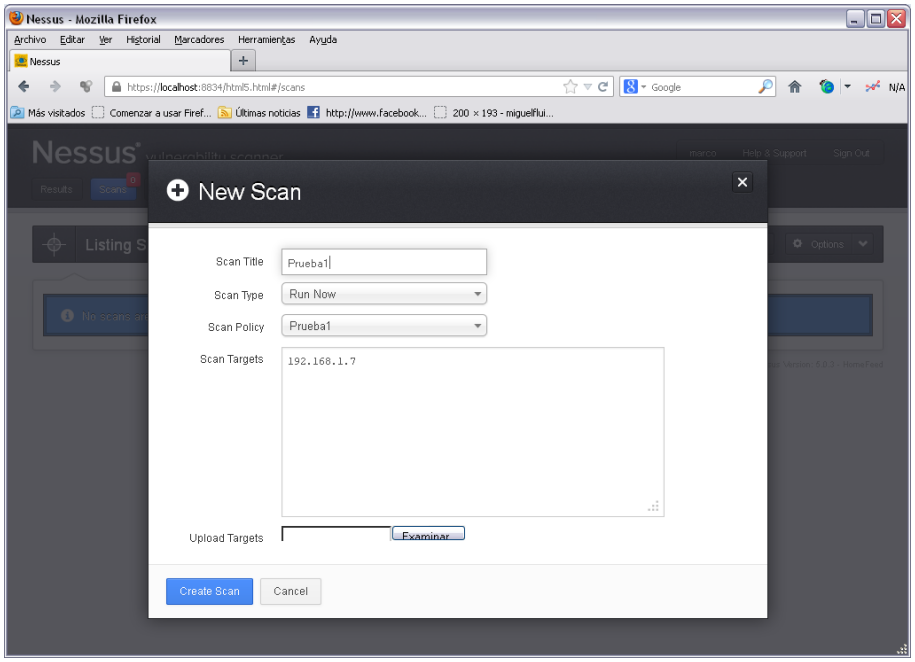
Tendrá por nombre Prueba1



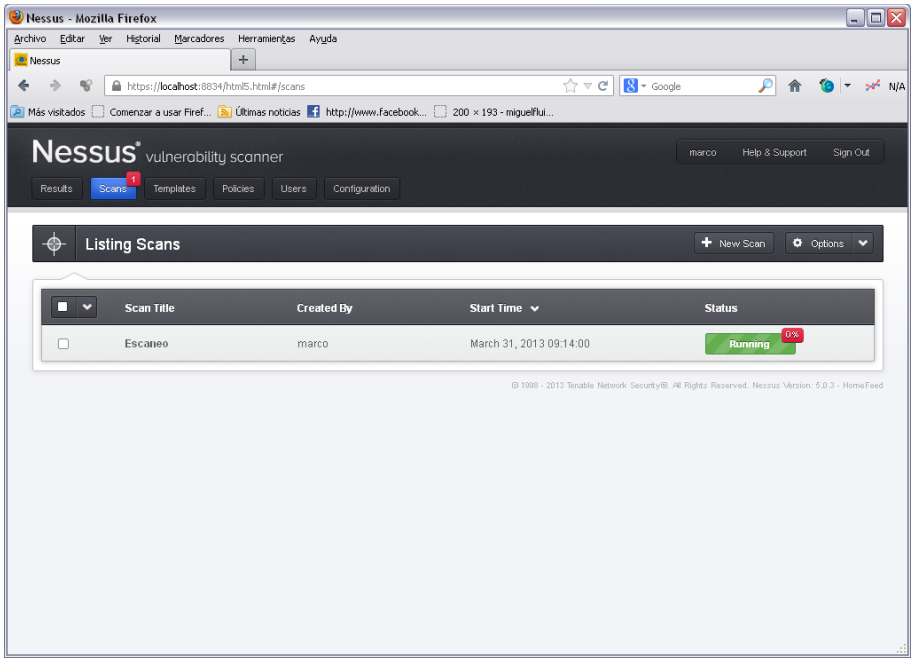
4) **Realizamos un nuevo escaneo aplicando la política creada en este caso Prueba1**



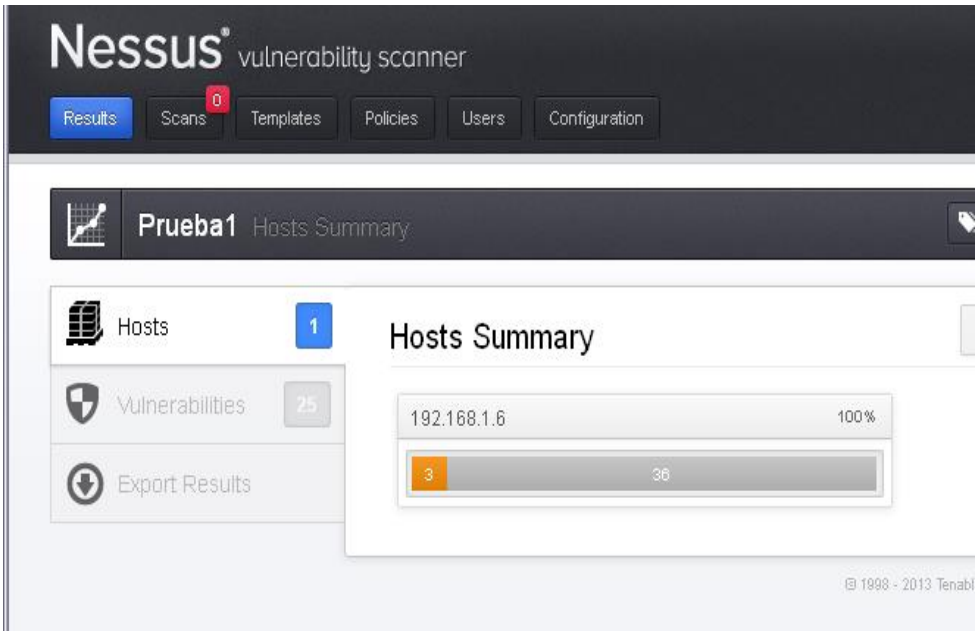
Debemos colocar un nombre para el escaneo, escoger la política que vamos a tomar en cuenta para el escaneo y por ultimo colocamos la dirección del host que vamos a escáner en este caso el host con dirección IP 192.168.1.6

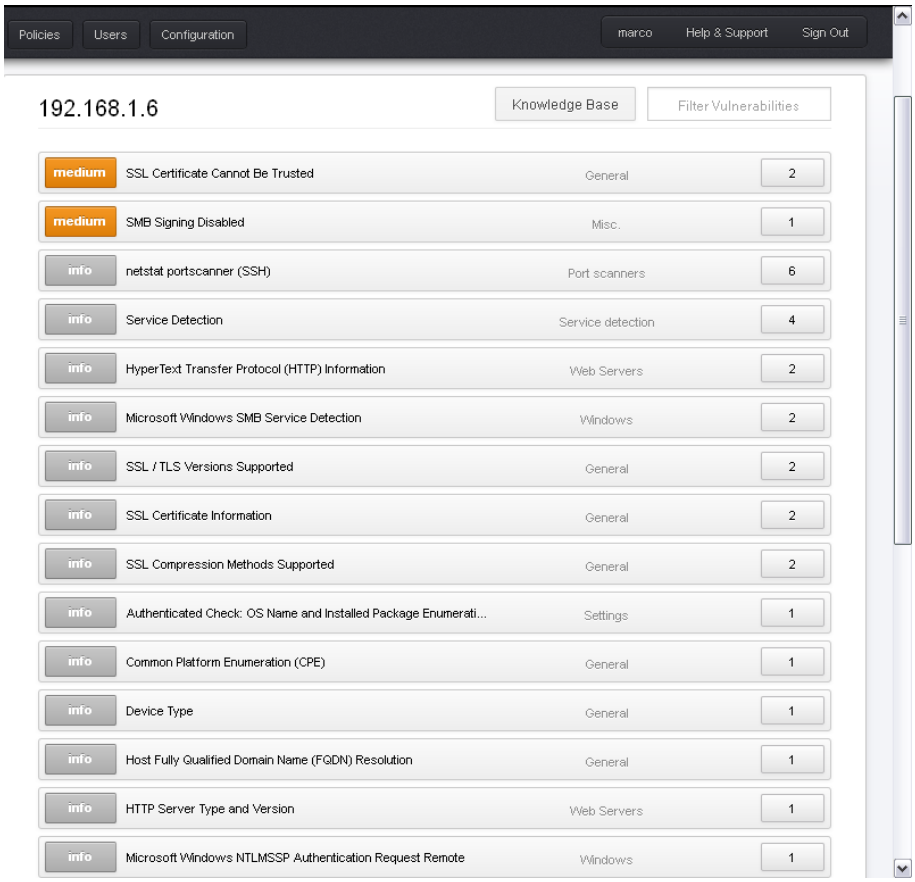


5) **Tomará algunos minutos el escaneo de la maquina**

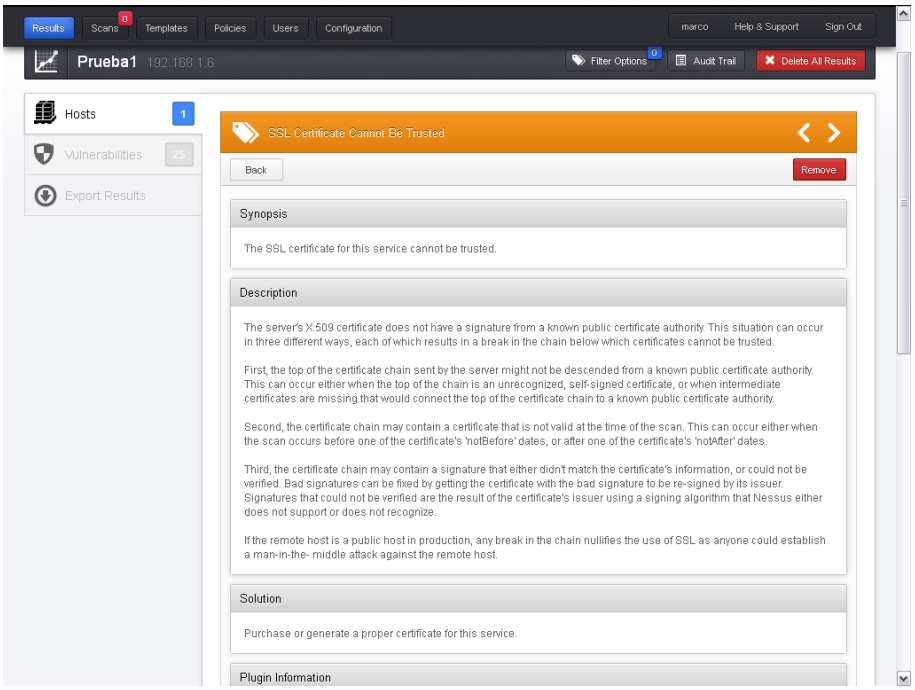


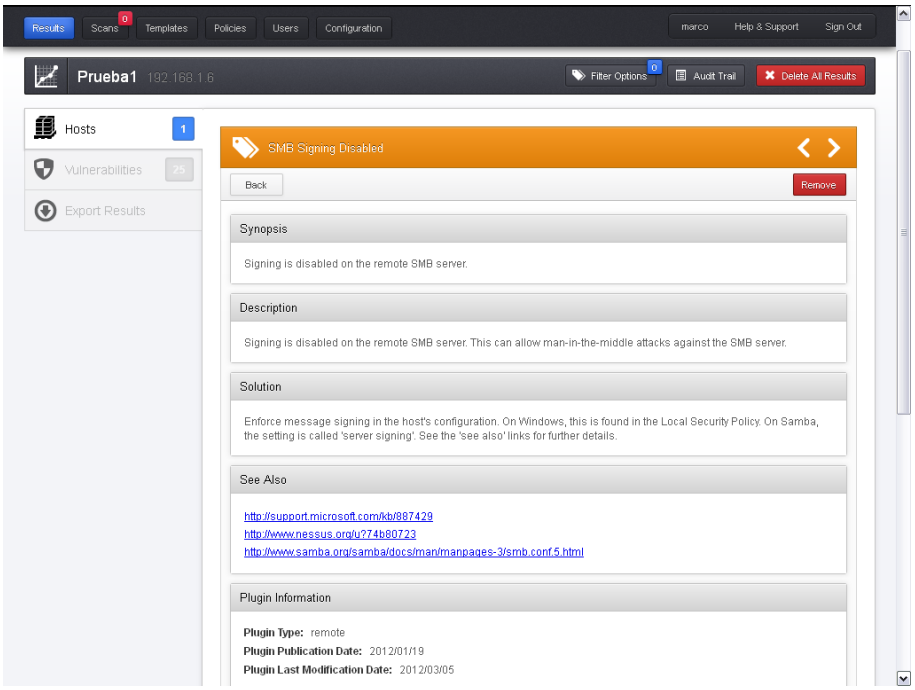
6) **Una vez terminado el escaneo tenemos los siguiente resultados**

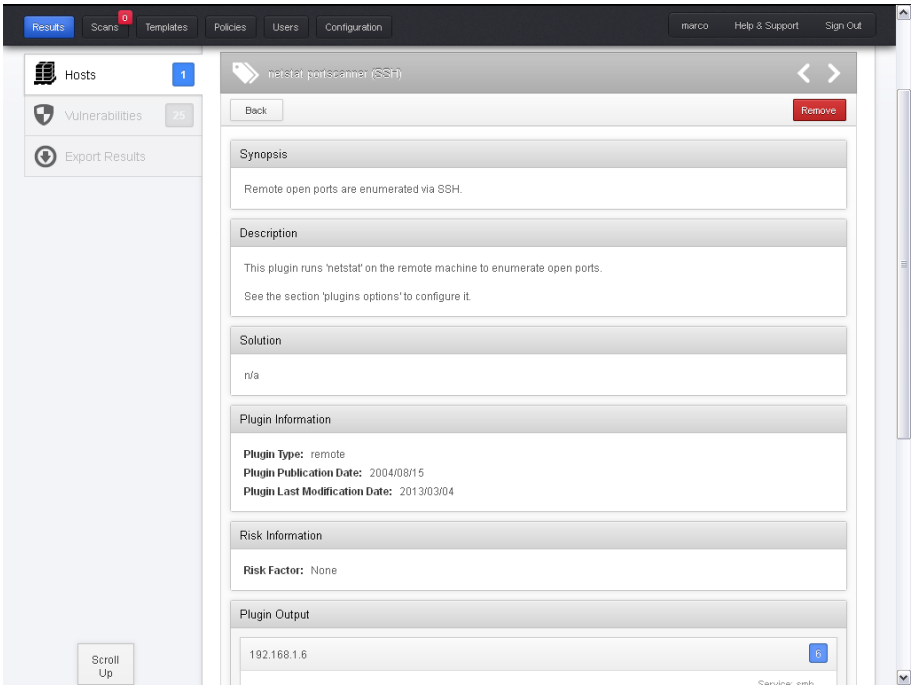


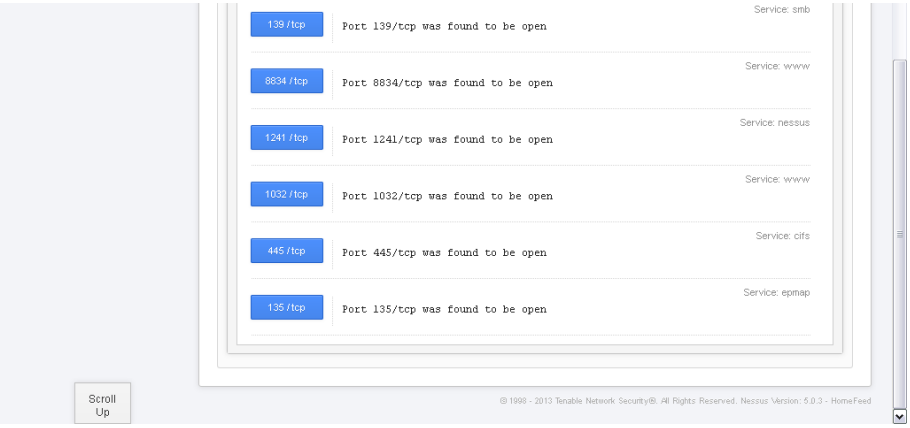


7) Detalle de los resultados




Results
Scans
Templates
Policies
Users
Configuration
marco
Help & Support
Sign Out
Prueba1 192.168.1.6
Filter Options
Audit Trail
Delete All Results
Hosts 1
Vulnerabilities 25
Export Results
SMB Signing Disabled
Back
Remove
Synopsis
Signing is disabled on the remote SMB server.
Description
Signing is disabled on the remote SMB server. This can allow man-in-the-middle attacks against the SMB server.
Solution
Enforce message signing in the host's configuration. On Windows, this is found in the Local Security Policy. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.
See Also
http://support.microsoft.com/kb/887429
http://www.nessus.org/u?74b80723
http://www.samba.org/samba/docs/man/manpages-3/smb.conf.5.html
Plugin Information
Plugin Type: remote
Plugin Publication Date: 2012/01/19
Plugin Last Modification Date: 2012/03/05


Results
Scans
Templates
Policies
Users
Configuration
marco
Help & Support
Sign Out
Hosts 1
Vulnerabilities 25
Export Results
netstat portscanner (SSH)
Back
Remove
Synopsis
Remote open ports are enumerated via SSH.
Description
This plugin runs 'netstat' on the remote machine to enumerate open ports.
See the section 'plugins options' to configure it.
Solution
n/a
Plugin Information
Plugin Type: remote
Plugin Publication Date: 2004/08/15
Plugin Last Modification Date: 2013/03/04
Risk Information
Risk Factor: None
Plugin Output
192.168.1.6
6
Scroll Up



CONCLUSIONES

- Se determinaron vulnerabilidades de prioridad media e informativa.
- Según los resultados obtenidos podremos decir que el sistema cuenta con vulnerabilidades teniendo un estado de seguridad bajo.
- Se tiene 6 puerto abiertos, que generan mayor preocupación para la seguridad de la información.
- De acuerdo al plugins “netstat” podemos determinar que direcciones remotas están tratando con nuestro PC.
- La herramienta NESSUS nos permite realizar un escaneo a una máquina en la cual no esté instalada y conozcamos su dirección o alias.

RECOMENDACIONES

- Después de realizar un escaneo, tomar en cuenta los resultados que la herramienta NESSUS lanza, así como las soluciones que propone para cada vulnerabilidad.
- Realizar un escaneo periódico, para determinar las vulnerabilidades a tiempo y poder evitar perdida, ataque o fuga de información de acuerdo sea el caso.
- Tener abierto solo los puertos que necesariamente lo ameriten y dar permiso solo a conexiones que sean seguras.
- Realizar las actualizaciones del sistema operativo, ya que traen muchas ventajas a la hora de la seguridad de la información. Si no se tiene activada

la opción de actualizaciones automáticas, realizarlas manualmente de forma periódica.

- Mantener el Firewall activado ayuda a mejorar la seguridad de la información y evita ataques de terceras personas.
- Crear una política de escaneo de acuerdo a las necesidades de cara individuo o institución.

Además, podemos navegar dentro de cada vulnerabilidad, dónde Nessus nos reporta un informe sobre la peligrosidad de la misma y datos orientativos de explotar los fallos de seguridad encontrados, webs de referencia.

ANEXO 11: Artículos que amparan la seguridad de la información en nuestro país

Artículo 41º. Sanciones. La Superintendencia de Telecomunicaciones, impondrá de oficio o a petición de parte, según la naturaleza y gravedad de la infracción, a las entidades de certificación de información acreditadas, a sus administradores y representantes legales, o a terceros que presten sus servicios, las siguientes sanciones:

Amonestación escrita;

Multa de quinientos a tres mil dólares de los Estados Unidos de Norteamérica; Suspensión temporal de hasta dos años de la autorización de funcionamiento de la entidad infractora, y multa de mil a tres mil dólares de los Estados Unidos de Norteamérica; y, revocatoria definitiva de la autorización para operar como entidad de certificación acreditada y multa de dos mil a seis mil dólares de los Estados Unidos de Norteamérica;

REFORMAS AL CÓDIGO PENAL

Artículo 58º. A continuación del artículo 202, inclúyanse los siguientes artículos innumerados:

Artículo...- El que empleando cualquier medio electrónico, informático o afín, violentare claves o sistemas de seguridad, para acceder u obtener información protegida, contenida en sistemas de información; para vulnerar el secreto, confidencialidad y reserva o simplemente vulnerar la seguridad, será reprimido con prisión de seis meses a un año y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica.

Artículo...- Obtención y utilización no autorizada de información. La persona o personas que obtuvieren información sobre datos personales para después cederla, publicarla, utilizarla o transferirla a cualquier título, sin la autorización de

su titular o titulares, serán sancionadas con pena de prisión de dos meses a dos años y multa de mil a dos mil dólares de los Estados Unidos de Norteamérica"

Artículo 59º. Sustitúyase el artículo 262º por el siguiente:

"**Artículo...-** 262. Serán reprimidos con tres a seis años de reclusión menor, todo empleado público y toda persona encargada de un servicio público, que hubiere maliciosa y fraudulentamente, destruido o suprimido documentos, títulos, programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, de que fueren depositarios, en su calidad de tales, o que les hubieren sido encomendados sin razón de su cargo".

Artículo 60º. A continuación del artículo 353º, agréguese el siguiente artículo innumerado:

"**Art.…** Falsificación electrónica. Son reos de falsificación electrónica la persona o personas que con ánimo de lucro o bien para causar un perjuicio a un tercero, utilizando cualquier medio; alteren o modifiquen mensajes de datos, o la información incluida en éstos, que se encuentre contenida en cualquier soporte material, sistema de información o telemático, ya sea:

Alterando un mensaje de datos en alguno de sus elementos o requisitos de carácter formal o esencial; Simulando un mensaje de datos en todo o en parte, de manera que induzca a error sobre su autenticidad; Suponiendo en un acto la intervención de personas que no la han tenido o atribuyendo a las que han intervenido en el acto, declaraciones o manifestaciones diferentes de las que hubieren hecho.

Artículo 61º. A continuación del artículo 415º del Código Penal, inclúyanse los siguientes artículos innumerados:

"**Artículo...** Daños informáticos. El que dolosamente, de cualquier modo o utilizando cualquier método, destruya, altere, inutilice, suprima o dañe, de forma temporal o definitiva, los programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, será reprimido con prisión de seis meses a tres años y multa de sesenta a ciento cincuenta dólares de los Estados Unidos de Norteamérica. La pena de prisión será de tres a cinco años y multa de doscientos a seiscientos dólares de los Estados Unidos de Norteamérica, cuando se trate de programas, datos, bases de datos, información o cualquier mensaje de datos contenido en un sistema de información o red electrónica, destinada a prestar un servicio público o vinculado con la defensa nacional.

Artículo...- Si no se tratare de un delito mayor, la destrucción, alteración o inutilización de la infraestructura o instalaciones físicas necesarias para la transmisión, recepción o procesamiento de mensajes de datos, será reprimida con prisión de ocho meses a cuatro años y multa de doscientos a seiscientos dólares de los Estados Unidos de Norteamérica.".

Artículo 62º. A continuación del artículo 553º del Código Penal, añádanse los siguientes artículos innumerados:

"**Artículo...-** Apropiación ilícita. Serán reprimidos con prisión de seis meses a cinco años y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica, los que utilizaren fraudulentamente sistemas de información o redes electrónicas, para facilitar la apropiación de un bien ajeno, o los que procuren la transferencia no consentida de bienes, valores o derechos de una persona, en perjuicio de ésta o de un tercero, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas informáticos, sistemas informáticos, telemáticos o mensajes de datos.

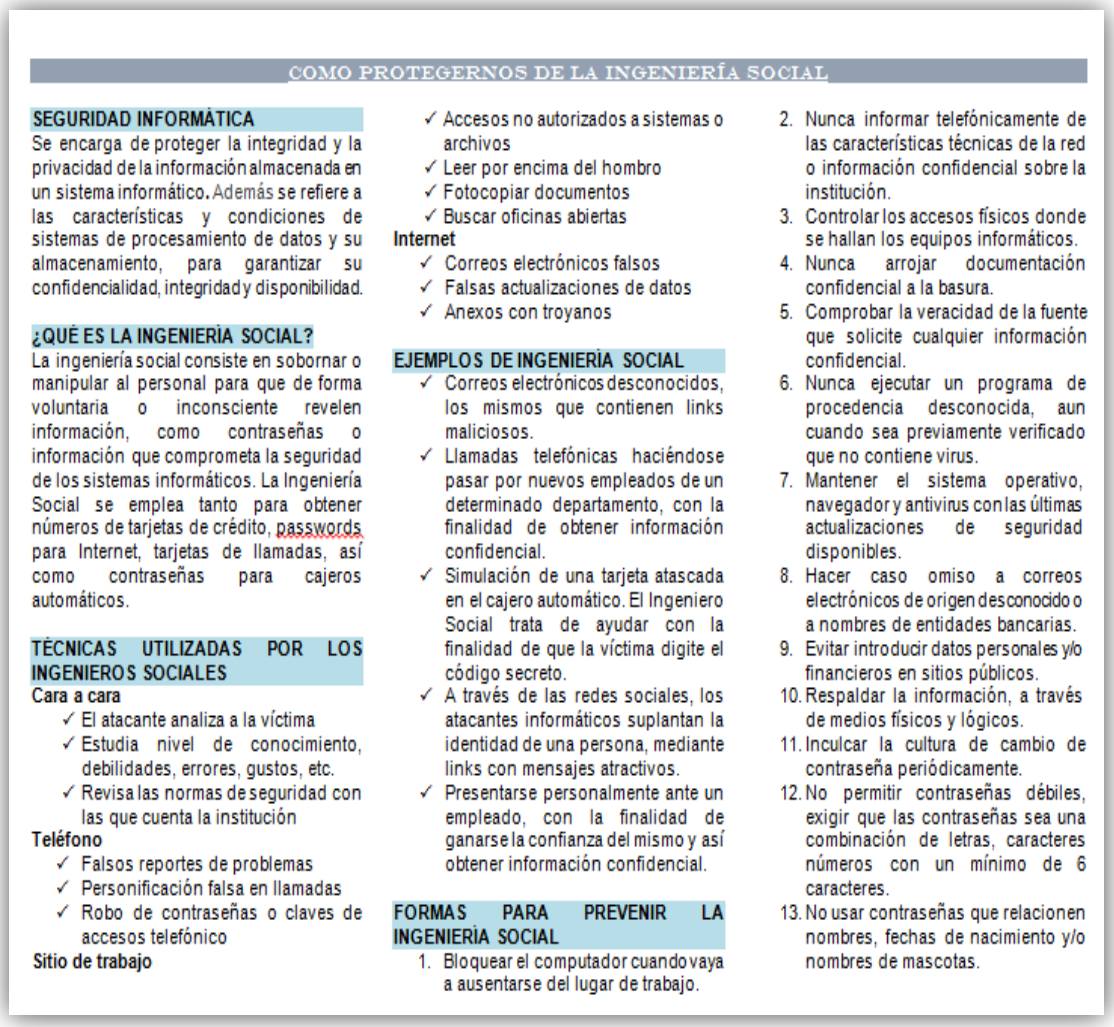
Artículo...- La pena de prisión de uno a cinco años y multa de mil a dos mil dólares de los Estados Unidos de Norteamérica, si el delito se hubiere cometido empleando los siguientes medios:

- Inutilización de sistemas de alarma o guarda;
- Descubrimiento o descifrado de claves secretas o encriptados;
- Utilización de tarjetas magnéticas o perforadas;
- Utilización de controles o instrumentos de apertura a distancia; y,
- Violación de seguridades electrónicas, informáticas u otras semejantes.".

Artículo 63º. Añádase como segundo inciso del artículo 563º del Código Penal, el siguiente:

"Será sancionado con el máximo de la pena prevista en el inciso anterior y multa de quinientos a mil dólares de los Estados Unidos de Norteamérica, el que cometiere el delito utilizando medios electrónicos o telemáticos.".

ANEXO 12: Capacitación



COMO PROTEGERNOS DE LA INGENIERÍA SOCIAL

SEGURIDAD INFORMÁTICA

Se encarga de proteger la integridad y la privacidad de la información almacenada en un sistema informático. Además se refiere a las características y condiciones de sistemas de procesamiento de datos y su almacenamiento, para garantizar su confidencialidad, integridad y disponibilidad.

¿QUÈ ES LA INGENIERÌA SOCIAL?

La ingeniería social consiste en sobornar o manipular al personal para que de forma voluntaria o inconsciente revelen información, como contraseñas o información que comprometa la seguridad de los sistemas informáticos. La Ingeniería Social se emplea tanto para obtener números de tarjetas de crédito, passwords para Internet, tarjetas de llamadas, así como contraseñas para cajeros automáticos.

TÉCNICAS UTILIZADAS POR LOS INGENIEROS SOCIALES

Cara a cara

- ✓ El atacante analiza a la víctima
- ✓ Estudia nivel de conocimiento, debilidades, errores, gustos, etc.
- ✓ Revisa las normas de seguridad con las que cuenta la institución

Teléfono

- ✓ Falsos reportes de problemas
- ✓ Personificación falsa en llamadas
- ✓ Robo de contraseñas o claves de accesos telefónico

Sitio de trabajo

- ✓ Accesos no autorizados a sistemas o archivos
- ✓ Leer por encima del hombro
- ✓ Fotocopiar documentos
- ✓ Buscar oficinas abiertas

Internet

- ✓ Correos electrónicos falsos
- ✓ Falsas actualizaciones de datos
- ✓ Anexos con troyanos

EJEMPLOS DE INGENIERÌA SOCIAL

- ✓ Correos electrónicos desconocidos, los mismos que contienen links maliciosos.
- ✓ Llamadas telefónicas haciéndose pasar por nuevos empleados de un determinado departamento, con la finalidad de obtener información confidencial.
- ✓ Simulación de una tarjeta atascada en el cajero automático. El Ingeniero Social trata de ayudar con la finalidad de que la víctima digite el código secreto.
- ✓ A través de las redes sociales, los atacantes informáticos suplantan la identidad de una persona, mediante links con mensajes atractivos.
- ✓ Presentarse personalmente ante un empleado, con la finalidad de ganarse la confianza del mismo y así obtener información confidencial.

FORMAS PARA PREVENIR LA INGENIERÌA SOCIAL

1. Bloquear el computador cuando vaya a ausentarse del lugar de trabajo.
2. Nunca informar telefónicamente de las características técnicas de la red o información confidencial sobre la institución.
3. Controlar los accesos físicos donde se hallan los equipos informáticos.
4. Nunca arrojar documentación confidencial a la basura.
5. Comprobar la veracidad de la fuente que solicite cualquier información confidencial.
6. Nunca ejecutar un programa de procedencia desconocida, aun cuando sea previamente verificado que no contiene virus.
7. Mantener el sistema operativo, navegador y antivirus con las últimas actualizaciones de seguridad disponibles.
8. Hacer caso omiso a correos electrónicos de origen desconocido o a nombres de entidades bancarias.
9. Evitar introducir datos personales y/o financieros en sitios públicos.
10. Respaldar la información, a través de medios físicos y lógicos.
11. Inculcar la cultura de cambio de contraseña periódicamente.
12. No permitir contraseñas débiles, exigir que las contraseñas sea una combinación de letras, caracteres números con un mínimo de 6 caracteres.
13. No usar contraseñas que relacionen nombres, fechas de nacimiento y/o nombres de mascotas.

Figura 9. Tríptico impartido en la capacitación

OBJETIVO

Dar a conocer los diferentes tipos de ataques informáticos para el robo de informacion y como podemos combatir este tipo de ataque.

TEMAS

- Seguridad informática
- Ingeniería Social
- Técnicas utilizadas por los Ingenieros Sociales
- Ejemplos de Ingeniería Social
- Formas de protección contra la Ingeniería Social

INTRODUCCIÓN

La educación es la única forma de combatir los ataques informáticos, es decir, para evitar ser victimas de cualquier ataque informático se debe conocer sobre las principales técnicas de robo de información. Por ello a través de capacitaciones se pretende concientizar al personal y de esta forma reducir el índice de robo de información.

Los temas a tratarse en esta capacitación, son sobre Ingeniería Social que es la práctica de obtener información confidencial a través de engaños, suplantación de identidad, manipulación, etc. Esto lo pueden realizar mediante correos electrónicos, mensajes de texto, observación directa, mirar por encima del hombro, llamadas telefónicas, etc.

RESULTADOS ESPERADOS

- Concientizar al personal de la institución sobre los principales ataques de robo de información.
- Conocer si en alguna ocasión han sido victimas de Ingeniería Social.
- Definir estrategias internas de seguridad para combatir los ataques informáticos.
- Resolver todas las inquietudes presentadas por parte de los participantes.

RECOMENDACIONES

- Capacitar al personal de la institución periódicamente.
- Los encargados de realizar las capacitaciones posteriores serán los del departamento de informática, ya que ellos están más inmersos en el tema de seguridad informática.
- A través de encuestas realizadas al personal capacitado, medir el nivel de concientización sobre ataques informáticos.

Figura 10. Temas a tratar en capacitación

ANEXO 13: Propuesta para capacitación continua

OBJETIVO

Capacitar constantemente a los usuarios, sobre los diferentes tipos de ataques informáticos para el robo de información y cómo podemos accionar ante este tipo de situación.

TEMAS RECOMENDADOS

- Análisis de las políticas de seguridad en la institución.
- Estudio de los resultados de las auditorías realizadas en la institución.
- Medidas de protección contra técnicas de robo de información.
- Ejemplos actualizados sobre Ingeniería Social.
- Análisis de los Ingenieros Sociales más reconocidos a nivel nacional.
- Concientizar a los usuarios sobre el uso de software actualizado y con licencia de seguridad.

ANEXO 14: Autorizaciones

Cariamanga, 23 de Marzo del 2011

[redacted]

Ciudad.

Mediante la presente me dirijo a su digna persona deseándole éxitos en las labores que día a día realiza en beneficio de ésta institución y en sí de toda la ciudadanía Calvence. Así mismo le manifiesto lo siguiente, como es de su conocimiento todo estudiante antes de obtener su título de profesional debe realizar un proyecto de tesis, es por ello que, yo **Diana Jaramillo** alumna de la **UTPL Ext. Cariamanga**, del décimo ciclo de la carrera de **Ingeniería en Informática**, debo realizar una investigación en las Empresas e Instituciones de esta ciudad, mediante el siguiente tema "Estudio de Ingeniería Social y su nivel de incidencia en las organizaciones públicas y privadas de la ciudad de Cariamanga".

Por consecuente me dirijo a usted para solicitarle que se me de la respectiva autorización para realizar la investigación pertinente en los diferentes departamentos de esta institución, ya que al desarrollar el tema antes mencionado en la empresa que usted éticamente dirige, se podrá obtener un sinnúmero de beneficios.

Segura de obtener una respuesta positiva a la presente desde ya le antelo mis más sinceros agradecimientos.

Atentamente.

Diana del Rocío Jaramillo Condolo
C.I. 1104613946

Vto. Bueno.
22-03-2011.

Cariamanga, 23 de Marzo del 2011

[redacted]
Ciudad.

Mediante la presente me dirijo a su digna persona deseándole éxitos en las labores que día a día realiza en beneficio de ésta institución y en sí de toda la ciudadanía Calvence. Así mismo le manifiesto lo siguiente, como es de su conocimiento todo estudiante antes de obtener su título de profesional debe realizar un proyecto de tesis, es por ello que, yo **Diana Jaramillo** alumna de la **UTPL Ext. Cariamanga**, del décimo ciclo de la carrera de **Ingeniería en Informática**, debo realizar una investigación en las Empresas e Instituciones de esta ciudad, mediante el siguiente tema "Estudio de Ingeniería Social y su nivel de incidencia en las organizaciones públicas y privadas de la ciudad de Cariamanga".

Por consecuente me dirijo a usted para solicitarle que se me de la respectiva autorización para realizar la investigación pertinente en los diferentes departamentos de esta institución, ya que al desarrollar el tema antes mencionado en la empresa que usted éticamente dirige, se podrá obtener un sinnúmero de beneficios.

Segura de obtener una respuesta positiva a la presente desde ya le antelo mis más sinceros agradecimientos.

[redacted] DEL CANTÓN CALVAS
INGRESADO Día 23
FOLIOS 09 HORA 11:59
LO CERTIFICO:

entamente.

Diana del Rocío Jaramillo Condolo
C.I. 1104613946

Presentada el día 29 de marzo del 2011, en la secretaria del plantel.- Lo certifico.

[redacted]
Secretaria

Vista la solicitud que antecede, autorizo a la Srta. DIANA JARAMILLO, realizar el trabajo de investigación en los departamentos de Secretaría y DOBE, del [redacted]

Cariamanga, 29 de marzo del 2011

[redacted]
Rector

Cariamanga, 23 de Marzo del 2011

[redacted]

Ciudad.

Mediante la presente me dirijo a su digna persona deseándole éxitos en las labores que día a día realiza en beneficio de ésta institución y en sí de toda la ciudadanía Calvence. Así mismo le manifiesto lo siguiente, como es de su conocimiento todo estudiante antes de obtener su título de profesional debe realizar un proyecto de tesis, es por ello que, yo **Diana Jaramillo** alumna de la **UTPL Ext. Cariamanga**, del décimo ciclo de la carrera de **Ingeniería en Informática,** debo realizar una investigación en las Empresas e Instituciones de esta ciudad, mediante el siguiente tema "Estudio de Ingeniería Social y su nivel de incidencia en las organizaciones públicas y privadas de la ciudad de Cariamanga".

Por consecuente me dirijo a usted para solicitarle que se me de la respectiva autorización para realizar la investigación pertinente en los diferentes departamentos de esta institución, ya que al desarrollar el tema antes mencionado en la empresa que usted éticamente dirige, se podrá obtener un sinnúmero de beneficios.

Segura de obtener una respuesta positiva a la presente desde ya le antelo mis más sinceros agradecimientos.

Atentamente.

[redacted]
AUTORIZA A: DIANA JARAMILLO
REALIZAR: INVESTIGACIÓN DE TEMA DE TESIS
DEL: 23 MARZO
F:

Diana del Rocío Jaramillo Condolo
C.I. 1104613946

Cariamanga, 23 de Marzo del 2011

[redacted]

Ciudad.

Mediante la presente me dirijo a su digna persona deseándole éxitos en las labores que día a día realiza en beneficio de ésta institución y en sí de toda la ciudadanía Calvence. Así mismo le manifiesto lo siguiente, como es de su conocimiento todo estudiante antes de obtener su título de profesional debe realizar un proyecto de tesis, es por ello que, yo **Diana Jaramillo** alumna de la **UTPL Ext. Cariamanga**, del décimo ciclo de la carrera de **Ingeniería en Informática,** debo realizar una investigación en las Empresas e Instituciones de esta ciudad, mediante el siguiente tema "Estudio de Ingeniería Social y su nivel de incidencia en las organizaciones públicas y privadas de la ciudad de Cariamanga".

Por consecuente me dirijo a usted para solicitarle que se me de la respectiva autorización para realizar la investigación pertinente en los diferentes departamentos de esta institución, ya que al desarrollar el tema antes mencionado en la empresa que usted éticamente dirige, se podrá obtener un sinnúmero de beneficios.

Segura de obtener una respuesta positiva a la presente desde ya le antelo mis más sinceros agradecimientos.

Atentamente.

Cariamanga

Diana del Rocío Jaramillo Condolo
C.I. 1104613946

Presentada el día 23 de enero del 2012, en la secretaría del plantel.- Lo certifico.

[redacted]
Secretaria

Vista la solicitud que le antecede, autorizo a la Srta. Diana Jaramillo, realizar campañas de capacitación al personal administrativo, docentes y estudiantes del [redacted]

Cariamanga, 23 de enero del 2012

[redacted]
Rector

Cariamanga, 15 de Mayo del 2012

[redacted]

Ciudad.

Mediante la presente me dirijo a su digna persona deseándole éxitos en las labores que día a día realiza en beneficio de ésta institución y en sí de toda la ciudadanía Calvence. Como es de su conocimiento actualmente me encuentro culminando la investigación sobre casos de Ingeniería Social en esta prestigiosa institución de la ciudad de Cariamanga, para la cual me dirijo a usted para solicitarle se me de la respectiva autorización para realizar campañas de capacitación a todo el personal que labora en esta institución que usted tan acertadamente dirige, en la cual se tratarán temas relacionados con la seguridad de la información, los mismos que anexos a este documento.

Segura de obtener una respuesta positiva a la presente desde ya le antelo mis más sinceros agradecimientos.

Atentamente.

[redacted] DEL CANTÓN CALVAS
INGRESADO DÍA 3/2011
DE
A LAS
LO CERTIFICO

Diana Jaramillo
C.I. 1104613946

Cariamanga, 15 de Mayo del 2012

[redacted]

Ciudad.

Mediante la presente me dirijo a su digna persona deseándole éxitos en las labores que día a día realiza en beneficio de ésta institución y en sí de toda la ciudadanía Calvence. Como es de su conocimiento actualmente me encuentro culminando la investigación sobre casos de Ingeniería Social en esta prestigiosa institución de la ciudad de Cariamanga, para la cual me dirijo a usted para solicitarle se me de la respectiva autorización para realizar campañas de capacitación a todo el personal que labora en esta institución que usted tan acertadamente dirige, en la cual se tratarán temas relacionados con la seguridad de la información, los mismos que anexos a este documento.

Segura de obtener una respuesta positiva a la presente desde ya le antelo mis más sinceros agradecimientos.

Atentamente.

Cariamanga

Diana Jaramillo
C.I. 1104613946

Cariamanga, 15 de Mayo del 2012

[redacted]

Ciudad.

Mediante la presente me dirijo a su digna persona deseándole éxitos en las labores que día a día realiza en beneficio de ésta institución y en sí de toda la ciudadanía Calvence. Como es de su conocimiento actualmente me encuentro culminando la investigación sobre casos de Ingeniería Social en esta prestigiosa institución de la ciudad de Cariamanga, para la cual me dirijo a usted para solicitarle se me de la respectiva autorización para realizar campañas de capacitación a todo el personal que labora en esta institución que usted tan acertadamente dirige, en la cual se tratarán temas relacionados con la seguridad de la información, los mismos que anexos a este documento.

Segura de obtener una respuesta positiva a la presente desde ya le antelo mis más sinceros agradecimientos.

Atentamente.

[redacted]
AUTORIZA A: DIANA JARAMILLO
REALIZAR: CAPACITACIONES DE SEGURIDAD INFORMÁTICA
DEL: 20-05 AL: 21-05-2012
F:

Diana Jaramillo
C.I. 1104613946

Anexo 15. Certificaciones

[redacted]

Mediante el presente documento, CERTIFICO, que la Sta. DIANA JARAMILLO con número de cédula 1104613946, realizó una campaña de Capacitación a todo el personal de esta Unidad Educativa, sobre temas de Seguridad de la Información las mismas que tuvieron una duración de dos (2) horas, las mismas que se realizaron los días 26 y 27 de enero del 2012. Cabe recalcar que además de las capacitaciones también se recibió el MANUAL DE POLÍTICAS DE SEGURIDAD, las cuales serán implementadas en esta Institución.

Es todo cuanto puedo mencionar con respecto a este tema y autorizo a la señorita antes mencionada para que haga uso de este documento como ella crea conveniente

Cariamanga 22 de Marzo del 2013

[redacted]

RECTOR

CERTIFICADO EMITIDO EN GERENCIA DE [redacted]

Cariamanga, 20 de Marzo del 2013

Mediante el presente certifico que, Diana Jaramillo con número de cédula 1104613946, realizó capacitaciones con temas de seguridad informática dirigidas a todo el personal, estas capacitaciones se realizaron los días 23 y 24 de marzo del 2012. Indico también que la señorita antes mencionada hizo la entrega del MANUAL DE POLÍTICAS DE SEGURIDAD, el mismo que será implementado en la Institución con la finalidad de preservar la seguridad de la información.

Lic. [redacted]

[redacted]

[redacted]

Cariamanga, 22 de Marzo del 2013

Yo, JUVENAL JARAMILLO certifico, que la Sta. DIANA DEL ROCÍO JARAMILLO CONDOLO con número de cédula 1104613946, realizó capacitaciones los días 20 y 21 de mayo del 2012. En estas capacitaciones se trataron temas de seguridad de la información las mismas que fueron dirigidas a todo el personal que conforma la Institución.

Cabe recalcar que además la Sta., mencionada anteriormente procedió a entregar el Manual de Políticas de Seguridad, las mismas que ya se analizaron anteriormente.

Atentamente.

[redacted]
C.I. [redacted]
DIRECTOR [redacted] CARIAMANGA

Ministerio de Salud Pública

[redacted]

[redacted]

Certifica que:

Diana Jaramillo, realizó capacitaciones a todo el personal que labora en esta Institución 12 y 13 de febrero del 2012, dichas capacitaciones tuvieron una duración de dos horas. Además de lo mencionado anteriormente la Sta., antes mencionada entregó el Manual de Políticas de Seguridad para su análisis y posterior implementación en esta Casa de Salud.

Es todo cuanto puedo certificar en honor a la verdad.

Cariamanga, 21 de Marzo del 2013

Dra. [redacted]
Directora [redacted]

Cariamanga, 19 de Marzo del 2013

[redacted] mediante el presente certifica que:

Diana Jaramillo estuvo en la Institución los días 22 y 23 de febrero del 2012 realizando capacitaciones al personal que labora en esta Institución, con la finalidad de concientizar sobre las diferentes técnicas que actualmente son utilizada para robar información, estas capacitaciones tuvieron una duración de una hora por día. Además a esto, se procedió la recepción del MANUAL DE POLÍTICAS DE SEGURIDAD, el mismo que fue analizado y posteriormente se implementará en la Institución.

Es todo cuanto puedo certificar en honor a la verdad.

[redacted]

BIBLIOGRAFÍA

[1] MAGAZCITUM, ROMO S. Eduardo. Publicado el 23 de Junio del 2010, disponible en http://www.magazcitum.com.mx/?p=313

[2]WIKIPEDIA, disponible en http://es.wikipedia.org/wiki/Ingenier%C3%ADa_social_%28seguridad_inform%C3%A1tica%29

[3] DICCIONARIO DE INFORMÁTICA http://www.alegsa.com.ar/Dic/ingenieria%20social.php

[4] GÓMEZ, A. (2007): Enciclopedia de la Seguridad Informática. México: AlfaOmega Grupo Editor.

[5] THE NESSUS PROJECT, Página Oficial. Recuperado el 25 de septiembre del 2012 de http://www.nessus.org

[6]ZONAWINDOWS, publicado el 6 junio 2009. Disponible en http://www.zonawindows.com.ar/whoreadme-servicio-gratuito-para-saber-si-tus-e-mails-son-leidos/

[7] TECNOLOGÍA, CUEVA Jimmy. Publicado el 24 de Noviembre del 2011, disponible en http://tecnologia21.com/49413/password-meter-medir-fuerza-contrasenas

[8] ÁLVAREZ, G., PÉREZ, P. (2004). Seguridad Informática Para Empresas y Particulares. Madrid. McGraw-Hill.

[9] MUNDO DEL TUTORIAL, publicado domingo, 2 de Enero del 201, disponible en http://mundodelturorial.blogspot.com/2011/01/programacion-bash.html

[10] REGISTRO OFICIAL. Órgano del Gobierno del Ecuador. 2002. Ley de comercio electrónico. Publicado 17 de abril del 2002. Disponible en http://www.cetid.abogados.ec/index.php?p=boletin_mostrar&id=128&ide=55

[11] ESET Security Report Latinoamérica 2012. http://seguridad-informacion.blogspot.com/2012/08/eset-security-report-latinoamerica-2012.html

[12] GRUPO DE INVESTIGACIONES TECNOLÓGICAS, disponible en http://www.delitosinformaticos.gov.co/node/62

[13] SOFTZONE, GÓMEZ Hugo, MSN Historiales, un nuevo ejemplo de ingeniería social con el objetivo de robar cuentas MSN, disponible en http://www.softzone.es/2009/02/28/msn-historiales-un-nuevo-ejemplo-de-ingenieria-social-con-el-objetivo-de-robar-cuentas-msn/

[14] NOBOSTI, Facebook ingeniería social, disponible en, http://www.nobosti.com/spip.php?article1336

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