UNIVERSIDAD TECNOLÓGICA INDOAMÉRICA

FACULTAD DE INGENIERÍA EN SISTEMAS

ESCUELA DE INFORMÁTICA Y COMPUTACIÓN

TEMA:

INGENIERÍA SOCIAL Y LOS DELITOS INFORMÁTICOS EN LA COMPAÑÍA INSTRUMENTAL Y ÓPTICA CÍA. LTDA.

Trabajo de investigación previo a la obtención del título de Ingeniero en Sistemas

AUTOR:

Joffre Germán Díaz Cobos

ASESOR:

Ingeniero Patricio Lara, M .Sc

Ambato - Ecuador

2016

APROBACIÓN DEL ASESOR

En mi calidad de catedrático Asesor del trabajo de grado previo a la obtención del título de Ingeniero en Sistemas, titulado Ingeniería Social y los delitos informáticos en la compañía Instrumental y Óptica Cía. Ltda. , elaborado por el señor estudiante: Joffre Germán Díaz Cobos. Certifico que dicho proyecto ha sido revisado en todas sus partes y considero que reúne los requisitos y méritos suficientes para ser sometido a la presentación pública y evaluación por parte del tribunal examinador que se designe.

Ambato, abril de 2015

Ingeniero, Patricio Lara, M. Sc.
ASESOR

DECLARACIÓN DE AUTENTICIDAD

El abajo firmante, declara que los contenidos y resultados obtenidos en el presente trabajo, como requerimiento previo para la obtención del título de Ingeniero en Sistemas, son absolutamente originales, auténticos, personales y de exclusiva responsabilidad legal y académica del autor.

Ambato, abril de 2015

Joffre Germán Díaz Cobos
CI: 1715956460

AUTORIZACIÓN POR PARTE DEL AUTOR PARA LA CONSULTA, REPRODUCCION PARCIAL O TOTAL, Y PUBLICACIÓN ELECTRONICA DEL TRABAJO DE TITULACIÓN.

Yo, Joffre Germán Díaz Cobos, declaro ser autor del Proyecto de Tesis titulado Ingeniería Social y los Delitos Informáticos en la compañía Instrumental y Óptica Cía. Ltda. del trabajo como requisito para optar al grado de Ingeniero en Sistemas, autorizo al sistema de Bibliotecas de la Universidad Tecnológica Indoamérica, para que con fines netamente académicos divulgue esta obra a través del Repositorio Digital Institucional (RDI-UTI).

Los usuarios del RDI-UTI podrán consultar el contenido de este trabajo en las redes de información del país y del exterior, con las cuales la Universidad tenga convenios. La Universidad Tecnológica Indoamérica no se hace responsable por el plagio o copia del contenido parcial o total de este trabajo.

Del mismo modo, acepto que los Derechos de Autor, Morales y Patrimoniales, sobre esta obra, serán compartidos entre mi persona y la Universidad Tecnológica Indoamérica, y que no tramitaré la publicación de esta obra en ningún otro medio, sin autorización expresa de la misma. En caso de que exista el potencial de generación de beneficios económicos o patentes, producto de este trabajo, acepto que se deberán firmar convenios específicos adicionales, donde se acuerden los términos de adjudicación de dichos beneficios.

Para constancia de esta autorización, en la ciudad de Ambato, a los 26 del mes de agosto de 2016, firmo conforme:

Autor: Joffre Germán Díaz Cobos

Firma:_____

Número de cédula: 1715956460
Dirección: Pedro Barrios N54-12 y Los Pinos, Quito
Correo Electrónico: joffrediaz@msn.com
Teléfono:0982936738

DEDICATORIA

Con el más profundo amor cariño y respeto, dedico este trabajo a mis padres Germán y Marianita, mis hermanos Rossana y Miguel, mis hijos Andrés, Gabriel e Ismael, mi esposa Sandrita, mis ex alumnos y amigos, en forma muy particular a Cristian Vizuete (†) con quien egresamos de la facultad, pero el Ser Supremo decidió llamarlo a su presencia.

Joffre Germán

AGRADECIMIENTO

Primeramente al Ser Supremo por permitirme gozar de vida, salud, coraje y constancia. A mis padres Germán y Marianita porque con su amor y apoyo incondicional, ellos han sido el pilar fundamental de empuje para poder concluir este trabajo de titulación. A mis hermanos Rossana por su cariño, y a Miguel por ser luz del conocimiento para mí, en este inexplorado camino que requiere templanza. A mi esposa Sandrita porque con su amor, paciencia y respeto ha sido testigo de varias noches de soledad e insomnio. Al Ingeniero Iván Pazmiño gerente general de la empresa Instrumental y Óptica, donde fue desarrollada la presente investigación, razón fundamental de este trabajo de titulación. A mi tutor el Ingeniero Patricio Lara Álvarez, los revisores Ing. Ligia Jácome, Ing. David Castillo e Ing. Francisco Naranjo que con su gran experiencia y conocimiento ha sabido guiarme correctamente en la elaboración y finalización de este trabajo de titulación.

Gracias

ÍNDICE GENERAL

CAPÍTULO I

EL PROBLEMA

CAPÍTULO II

MARCO TEÓRICO

CAPÍTULO III

METODOLOGÍA

CAPÍTULO IV

ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

CAPÍTULO VI

LA PROPUESTA

ÍNDICE DE TABLAS

ÍNDICE DE GRÁFICOS

INTRODUCCIÓN

La investigación corresponde a la Ingeniería Social y los delitos Informáticos en la Compañía Instrumental y Óptica Cía. Ltda. es de relevancia para la compañía ya que la información que maneja es bastante sensible, estos datos son el producto de una estrategia de ventas en el que se involucran clientes, proveedores, inventarios, importaciones, empleados entre otros; la misma que al caer en manos equivocadas podría causar un fuerte perjuicio, poniendo en alto riesgo la estabilidad del negocio.

El documento se compone de seis capítulos, que son:

El Capítulo I, se denomina **EL PROBLEMA**, que contiene, el tema, línea de investigación, planteamiento del problema, contextualización micro, árbol de problemas, análisis crítico, prognosis, formulación del problema, interrogantes de la investigación, delimitación de la investigación, justificación, objetivo general y específicos.

El Capítulo II, se desarrolla el **MARCO TEÓRICO**, que contiene los antecedentes de la investigación, organizador lógico de variables, constelación de ideas, desarrollo de las variables, pregunta directriz, señalamiento de variables.

El Capítulo III, es la **METODOLOGÍA,** donde se describe el enfoque, modalidad, nivel de la investigación, población, operacionalización de variables, técnicas e instrumentos, plan de recolección de datos.

El Capítulo IV, corresponde al **ANÁLISIS E INTERPRETACIÓN DE LOS RESULTADOS**, haciendo uso de cuadros y gráficos fáciles de entender y acompañados por un análisis escrito que sustenta investigación, la interpretación de los datos, y la comprobación de la pregunta directriz.

En el Capítulo V, están las **CONCLUSIONES Y RECOMENDACIONES** de la investigación.

En el Capítulo VI, se presenta **LA PROPUESTA** alternativa como un aporte de esta investigación, que contiene el tema, datos informativos, objetivos y la propuesta de solución al problema.

Finalmente consta la bibliografía y los anexos.

CAPÍTULO I

EL PROBLEMA

TEMA

Ingeniería Social y los delitos Informáticos en la Compañía Instrumental y Óptica Cía. Ltda.

LÍNEA DE INVESTIGACIÓN

Tecnologías de la Información y Comunicación (TIC).- Esta línea de investigación se enmarca en la producción de conocimientos de nuevas tecnología en el campo de la informática y las telecomunicaciones, en donde lo que se busca es la investigación, innovación y desarrollo de estas tecnologías y software libres.

PLANTEAMIENTO DEL PROBLEMA

Contextualización

Macro

La gran necesidad de comunicarnos de hoy en día no conoce fronteras, se ha hecho necesario disponer de correo en todo momento, enviar mensajes a través de redes sociales, traspasar las fronteras geográficas, a cada momento interactuamos con nuestra información sobre internet. Pero la necesidad va acompañada de la inseguridad a la que nos sometemos con ella, no resulta raro que de los correos que se reciben a diario, unos cuantos son no deseados; si tenemos buenas barreras

de protección estos pueden ir directo a la bandeja de correos no deseados, pero sino, podemos ser víctimas de promociones, falsos premios, información de fuentes no confiables, hasta programas de virus y espías. Se conoce de un caso muy particular donde a una persona muy cercana le llegó uno de estos correos "Phishing" el mismo que cayó en la trampa y fue víctima de estafa.

La gran mayoría de personas hacen transacciones bancarias por internet, por facilidad de no hacer filas y ahorrar tiempo, la facilidad de transferir dinero, transacciones por las cuales podemos caer presa de los llamados ciberdelincuentes. Estos delincuentes informáticos siguen inventando formas de atentar contra la privacidad y el patrimonio de las personas, pero con simples estrategias logran engañar a sus víctimas en situaciones que a veces ni una persona entendida en informática puede llegar a darse cuenta.

A nivel mundial el valor que tiene la información en su gran mayoría es poco valorada, pero solo el momento que se afecta la economía se toma cartas en el asunto, por lo general este tipo de delitos cibernéticos trascienden los límites nacionales. Uno de los temas a tratar en La Cumbre Mundial sobre la Sociedad de la Información (Betancourt, 2004) fue crear confianza y seguridad en la utilización de las TIC y como perspectiva resalta que existe ambigüedad en las definiciones de propósitos criminales y terroristas en las políticas, la legislación existente, donde se emerge y se impide el uso de recursos de información para fines legítimos.

(Betancourt, 2004), sostiene que la legítima necesidad de preservar la integridad de la infraestructura no debe estar marcada por una agenda politizada, que se centra básicamente en la integridad del campo militar y el uso de los recursos de información para propósitos criminales y terroristas. Afirma, además, que el derecho de privacidad debe ser defendido en los espacios públicos, en línea, fuera de línea, en el hogar y en el trabajo.

Meso

En el Ecuador los delitos informáticos se han vuelto muy comunes y no es sorprendente saber que nuestro país esté en el décimo lugar en el informe de la OEA y Symantec en la estadística de 2013, donde se reveló las principales

amenazas cibernéticas a las que se enfrentan los gobiernos y cómo la economía la de los ciudadanos está siendo amenazada, este informe revela un ranking con las tendencias país por país, para este caso nos interesa rotundamente nuestro terruño.

Tabla 1 - Actividad maliciosa en América Latina.

Symantec.

Actividad Maliciosa por Fuente en América Latina

País	Ranking Global 2013	Ranking Regional 2013
Brasil	8	1
Argentina	20	2
Perú	21	3
México	27	4
Chile	29	5
Colombia	30	6
Uruguay	40	7
Venezuela	45	8
República Dominicana	69	9
Ecuador	71	10
Puerto Rico	73	11
Bolivia	74	12
Panamá	76	13
Costa Rica	87	14
Trinidad y Tobago	102	15
Jamaica	104	16
Guatemala	109	17
El Salvador	110	18
Bahamas	111	19
Paraguay	114	20

Fuente: (AETECNO, 2015)

En la tabla 1 se identificaron dos impedimentos principales para reducir la ciberdelincuencia; el primero es la falta de leyes adecuadas en esta materia que criminalicen actividades específicas y que definan penas. La segunda es la constante falta de conciencia y de recursos educativos para ciudadanos en relación con el uso responsable de internet y de las TIC, y el uso adecuado de las medidas de seguridad que brindan las redes sociales, los proveedores de servicios de correo electrónico, los sitios de microblogging, etcétera.

Sin ir más lejos, en el 2013, hubo un aumento exponencial en la cantidad de quejas cibernéticas de los ciudadanos hacia las autoridades nacionales. Los casos denunciados estaban relacionados con ataques de interceptación ilegales sobre la integridad de la información, dispositivos que infringen la seguridad de los sistemas, ciberfalsificación, fraude informático, pornografía infantil y delitos contra la propiedad intelectual. Por otra parte, la cantidad de casos que se han presentado y acumulados en el periodo 2008-2013 aumentó 203% y 458%, respectivamente. (Symantec, 2013)

Se puede observar que existe un gran porcentaje en aumento de los delitos informáticos, estos datos pueden servir para hacer referencia a lo que podría estar ocurriendo en el Ecuador, de tal manera que si continúan con estas altas tasas, las pérdidas económicas se elevarían indudablemente y quién pagaría las consecuencias de ello sería la parte más vulnerable, el usuario final, el pueblo.

Las personas no toman suficientes medidas de seguridad al usar dispositivos electrónicos, ahora no sé sabe qué es más seguro, que dejen de usar la tecnología para realizar un pago o que vayan a un banco y que salgan cargados de dinero para que paguen sus cuentas; la respuesta es clara la solución sería que se informen adecuadamente sobre las seguridades que deben tener frente al uso de cualquier medio electrónico bancario.

Si se basan en toda esta inseguridad hay algunas alianzas estratégicas que pueden poner algo de seguridad a toda esta ola de peligros a la que se enfrentan, citando un ejemplo las empresas Spamina e Inforc Ecuador firmaron un acuerdo para distribuir toda la gama de productos de Cloud Email Firewall, Archiving, Encryption & DLP y Web security en arquitectura de public, hybrid y private cloud, incorporándolos a su portafolio de servicios de seguridad. Gracias a este acuerdo, y con la aportación común de la experiencia y conocimientos de ambas empresas, los clientes de Inforc Ecuador obtendrán una avanzada y completa oferta de soluciones de seguridad para garantizar la protección total de su correo electrónico, pudiendo seleccionar el producto o servicio que más se adecúe a sus necesidades. (INFORC_ECUADOR, 2014)

Micro

Dentro de la empresa Instrumental y Óptica se ha podido observar que hay algunos detalles dentro del campo informático y de ingeniería social que no se están tomando en cuenta para mantener a buen recaudo su información, haciendo notar que para esta empresa es muy importante que exista un manejo sigiloso de la misma, porque este pequeño gran descuido podría sobre caer en la pérdida de un negocio, la pérdida de un cliente o lo que es peor, el cierre de la empresa. Y todo va desde estructuras muy básicas como la instalación de una red segura hasta algunos procesos de información donde se manejan compras públicas, razón por la cual han perdido un gran número de negocios habiendo sido presas de individuos que han hecho muy bien su trabajo en cuanto corresponde a la ingeniería social.

El problema va más allá de lo que en realidad parece, porque uno de los nudos críticos que existen en nuestra sociedad es la desinformación de la tecnología informática, esa es una de las debilidades más fuertes al que todos nos enfrentamos, por el simple hecho de que a veces usamos computadores alquilados por horas, desde un teléfono hacemos una transacción bancaria o por no saber manejar bien las seguridades de las redes sociales podemos ser presas de agresión física o que lleguen a amedrentarnos con nuestra familia; otro tipo de problema que podemos mencionar sobre la ausencia de seguridades informáticas dentro de una empresa, es el robo de información de nuestros proveedores, facturación, estados de cuenta, pago de nóminas. Como es muy común actualmente los haberes de los empleados son cancelados a través de una simple transacción electrónica bancaria y la falta de capacitación de quien maneja estas claves hace que sobre caigan en procesos inseguros.

Análisis Crítico

Cuando trabajan con datos en la oficina, la información que manejan es parte de la compañía, lo cual no los hace dueños de ella, aun habiéndola creado, existe un salario que perciben a cambio de generarla. Pero el apoderamiento y el mal manejo de esta, les pueden causar grandes problemas, se ha escuchado contantemente que el desconocimiento de la ley no los exime de culpa. Existe un

marco legal respaldando la información se llama ley de propiedad intelectual. Si alegan que hubo un deficiente control y por ello, inconscientemente existió una tentativa de hurto, el hurto consumado en cualquiera de estos dos casos tiene una conducta sancionable.

Cuando se instala una red para tener facilidad en la obtención de la información, por regla general es de conocimiento que la vamos a compartir. Pero por necesidad han empezado a instalar desmedidamente equipos concentradores de información, routers, hubs y no se sabe quién puede obtener estos datos, lo más seguro es que se vean enfrentados a un grave problema, el mismo del que hace eco la compañía Instrumental y Óptica.

Refiriendo a las contraseñas existentes en la empresa, se puede observar que las hay, ¿Pero cuan seguras son?, no se puede garantizar por la inexistente política para generar contraseñas, hace inseguro los datos existentes que son de gran importancia, de tal manera que todas las computadoras tienen una contraseña de inicio, igual y para acceder al wifi es tan fácil como levantar la vista y obtener la contraseña impresa en una hoja de pared. El problema no es que la contraseña del wifi sea pública, pero es un inconveniente es que el router pertenece a la red interna, la cual carece políticas y permisos definidos, mediante un administrador de red.

Árbol de Problemas

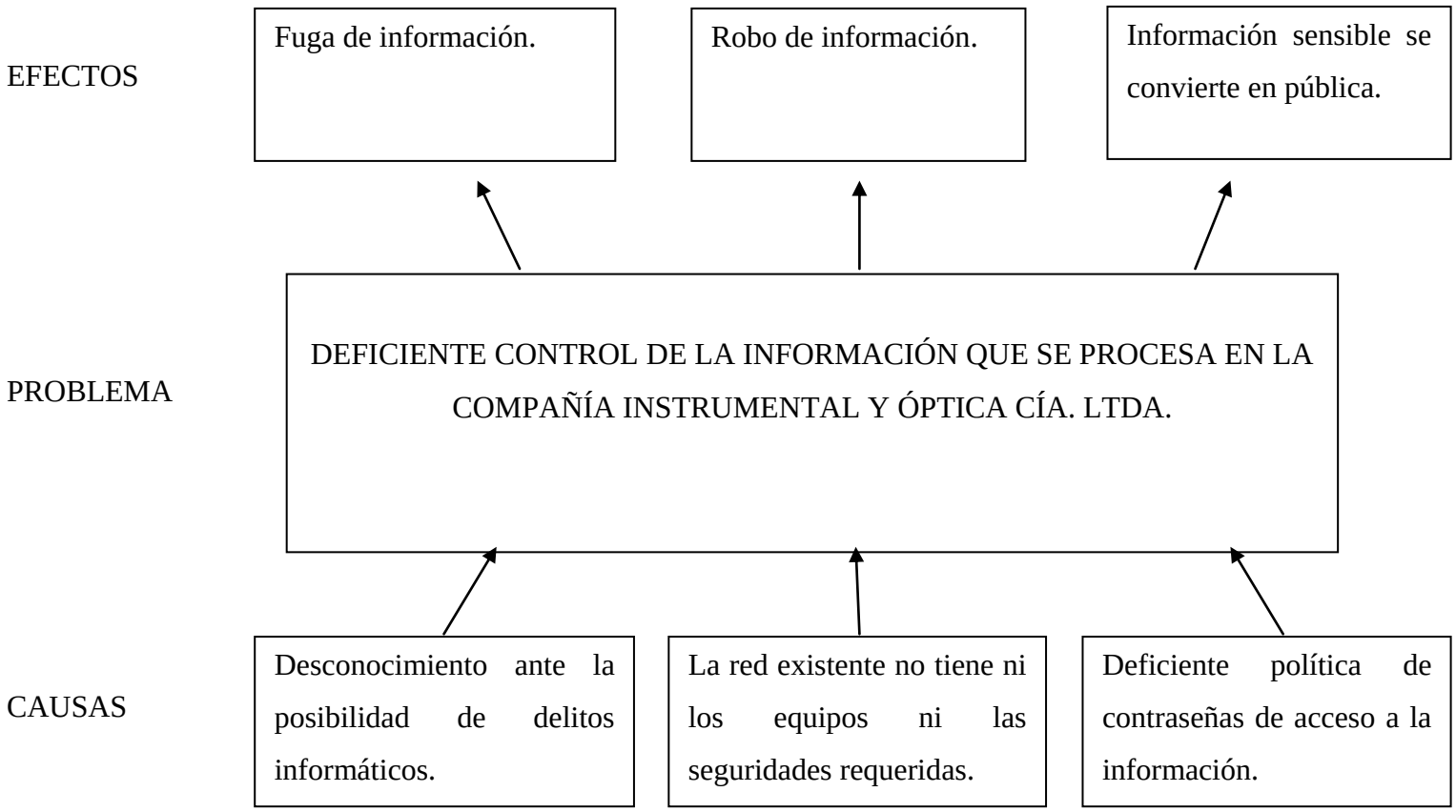


Gráfico 1 - Relación causa efecto
Elaborado por: Joffre Germán Díaz Cobos

Formulación del problema

¿Cómo se maneja los delitos informáticos frente a problemas de ingeniería social en la compañía Instrumental y Óptica?

Preguntas directrices.

- ¿Existen elementos de Ingeniería Social que se pueden evidenciar en la compañía Instrumental y Óptica?
- ¿Se han evidenciado delitos informáticos que han puesto en riesgo la información de la Compañía Instrumental y Óptica?
- ¿De existir un manual de políticas de seguridades informáticas, permitirá un manejo adecuado y seguro de la información?

Prognosis.

Si continúa el problema, en poco tiempo vamos a observar que las ventas han bajado, que las tácticas para ganar una puja ya no son funcionales, y que ahora se tiene más competidores para un proceso de compras públicas, y la razón es tan simple como darle crédito al hurto de información, la falta de controles dieron paso a los intrusos y que los datos más importantes esté en manos de supuestos clientes, que en su momento llegaron a la compañía a preguntar por un equipo, que jamás lo necesitaron, pero a cambio de esa visita obtuvieron información valiosa para la empresa.

Enfrentarnos a una competencia desleal, puede ir generando perdidas de negocios, renuncias intempestivas de excelentes colaboradores, que ahora estarán trabajando en la competencia con un salario más cómodo. Viéndolo de este modo lo que puede llegar a suceder en poco tiempo es que la compañía se vaya abajo, porque lo que era parte de una estrategia de ventas o manejo de personal ahora se hizo público.

DELIMITACIONES DE LA INVESTIGACIÓN

Campo: Informática.

Área: Seguridades Informáticas**.**

Aspecto: Delitos informáticos

Delimitación espacial: La compañía Instrumental y Óptica se encuentra ubicada en Quito, en las calles Av. Cristóbal Colón Oe1-100 y Av. 10 de Agosto.

Delimitación temporal: La siguiente investigación se desarrollará de septiembre 2014 a enero de 2016.

JUSTIFICACIÓN

Importancia: La importancia de esta investigación es proponer una serie de regulaciones y normas que deben existir sobre las seguridades informáticas en la compañía Instrumental y Óptica, dar a conocer a sus colaboradores la ley que regula estos delitos y las penas vigentes por irrumpir en la información de la compañía, dando a denotar que no sólo el delito lo pueden cometer personas externas sino también internas.

Interés y beneficiarios: Inicialmente se obtuvo serias dudas sobre el tema de investigación, si a sus accionistas les interesaría, pero cuando se les entregó varios puntos de vista sobre la importancia de la información, se obtuvo una excelente apertura para desarrollarla, pudieron asimilar cuán importante era, que la información se mantenga reservada y no pública para sus empleados y otros intrusos que no son bienvenidos. Una de las expectativas más notables fue la elaboración de normas y regulaciones para el manejo seguro de la información de la compañía.

Factibilidad: Uno de los puntos más delicados en toda compañía es el acceso a la información, para ello contamos con la total apertura al acceso a la misma y la participación continúa de los dueños. Algunos de los recursos financieros y tecnológicos que usaremos para realizar esta investigación son los siguientes:

Computador Portátil:	$ 900,00
Cámara de fotos	$ 250,00
Grabadora de sonidos	$ 90,00
Impresora	$ 250,00
Disco duro externo	$ 98,00
Material de impresión	$ 80,00
Movilización	$ 200,00
TOTAL	$ 1.868,00

Impactos: Uno de los retos es asignar estratégicamente los recursos para cada equipo informático que intervenga, basándose en el impacto potencial para la compañía, respecto a los diversos incidentes que se deben resolver frente a la problemática planteada, en esta investigación, la idea es desarrollar un manual de seguridad, que se ajuste las necesidades exactas de la compañía frente a sus necesidades para proteger los datos y en un futuro el negocio.

Utilidad práctica: Dentro del producto de esta investigación, cabe destacar que el manual de seguridad desarrollado, será la biblia de uso continuo para cualquier movimiento estratégico en el área de sistemas, aportando reglas claras e inviolables de cómo se debe darle un tratamiento especial, a los repositorios de datos y como resguardar esta información de personas externas e internas, además de tener un sistema de respaldos automáticos y continuos para prevenir futuras perdidas.

OBJETIVOS

Objetivo General

Investigar el impacto de la Ingeniería Social y los posibles delitos informáticos en la Compañía Instrumental y Óptica.

Objetivos Específicos

- Analizar las posibles vulnerabilidades en los sistemas de conexión virtual bancaria, sistema informático de la compañía, redes de comunicación interna y externa y redes sociales que interactúan con la empresa, mediante observación para prevenir posibles delitos informáticos.
- Estudiar los delitos informáticos existentes, asociados con la Ingeniería Social que posiblemente puedan suceder en la compañía.
- Elaborar una alternativa de solución al problema planteado basado en la Metodología de Benson.

CAPÍTULO II

MARCO TEÓRICO

ANTECEDENTES INVESTIGATIVOS

Para la obtención de los antecedentes de esta investigación, se han tomado como referencia las conclusiones de los siguientes trabajos:

En la tesis de Maestría de Sistemas de Información Gerencial (Ureta, 2009) se llega a la conclusión de que "Ecuador ha dado los primeros pasos en el desarrollo de iniciativas que permiten la investigación y sanción de los delitos informáticos, sin embargo, es preciso desarrollar, mejorar e implementar mecanismos que permitan que dichas investigaciones se desarrollen dentro de marcos regulados, controlados y mediante el uso de tecnología apropiada por parte los entes y profesiones dedicados a su investigación. Luego de analizar la realidad de los delitos informáticos en el Ecuador y exponer mecanismos y herramientas existentes para su investigación, se recomienda considerar por sectores: Gubernamental, Marco Legal, formación, tecnología y sociedad"

En la tesis de maestría en redes en la ciudad de Ambato, (Zurita, 2010) concluye que: "Al aplicar los instrumentos de recolección de información al personal de Industrias Catedral, se evidencio, que, aun cuando existen algunas restricciones informáticas, no existen políticas bien definidas de uso y confidencialidad de los recursos informáticos".

Las pocas restricciones informáticas existentes no son conocidas por todos los usuarios. La falta de una cultura informática en los usuarios ha puesto en eminente riesgo la información crítica de la empresa en varias ocasiones

Al no existir un criterio de valoración de los activos informáticos de Industrias Catedral, ha dificultado determinar los activos de mayor importancia para la

empresa, siendo esto un limitante al momento de establecer el impacto que ocasionaría la pérdida de un activo informático."

En la tesis de titulación (Bastidas M. , 2011) concluye que "El hacker, cracker, phishing y el fraude informático constituyen tipos de delitos informáticos, con conceptualizaciones y características propias; una vez diferenciado cada uno de ellos, se puede diferenciar a los sujetos activos, sujetos pasivos, verbos rectores y los bienes jurídicos protegidos; para a su vez poder tipificar y sancionar a los culpables de estos delitos." Al momento de cometer un delito informático es importante llegar a una identificación del actor del mismo, dentro de que tipo caería, de tal manera que no tenga el mismo tipo de sanción un actor intelectual o activo, a la final estos dos deberían tener una sanción fuerte pero quien comete el agravio debe ser sancionado con todo el rigor de la ley. En muchos de los casos este tipo de personas que cometen un fraude informático, no tiene altos estudios en su mayoría, lo cual es un factor importante, para darnos cuenta que jamás recibieron cátedra de ética en las aulas de las universidades. Un nudo crítico en la legislación ecuatoriana, son la ausencia de dureza en las penas por delitos o fraudes informáticos.

Categorías Fundamentales

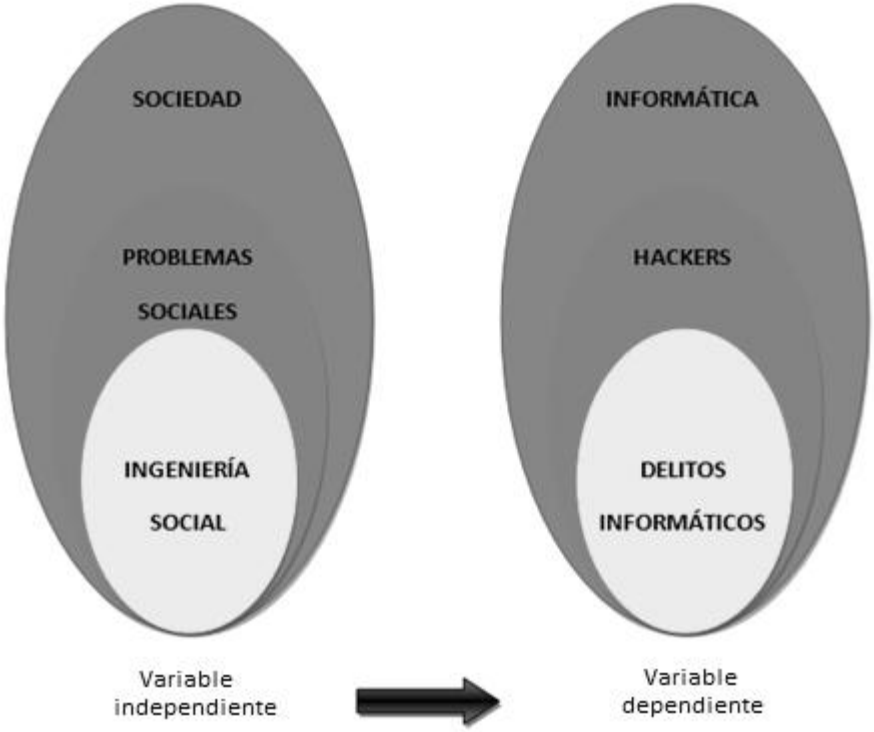


Gráfico 2 - Organizador lógico de variables
Elaborado por: Joffre Germán Díaz Cobos

CONSTELACIONES DE IDEAS VARIABLE INDEPENDIENTE

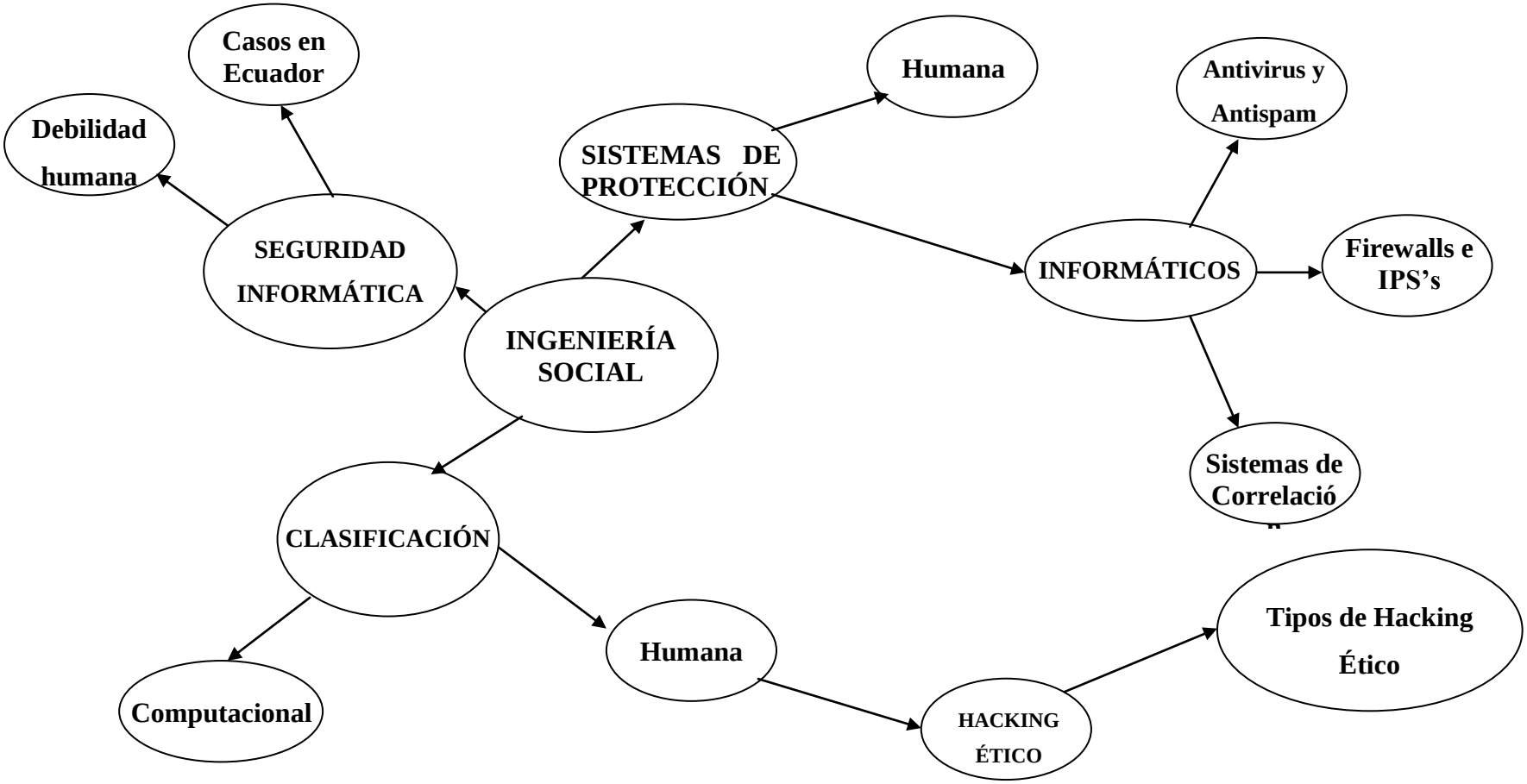


Gráfico 3 - Constelación de ideas variable independiente
Elaborado por: Joffre Germán Díaz Cobos

CONSTELACIONES DE IDEAS VARIABLE DEPENDIENTE

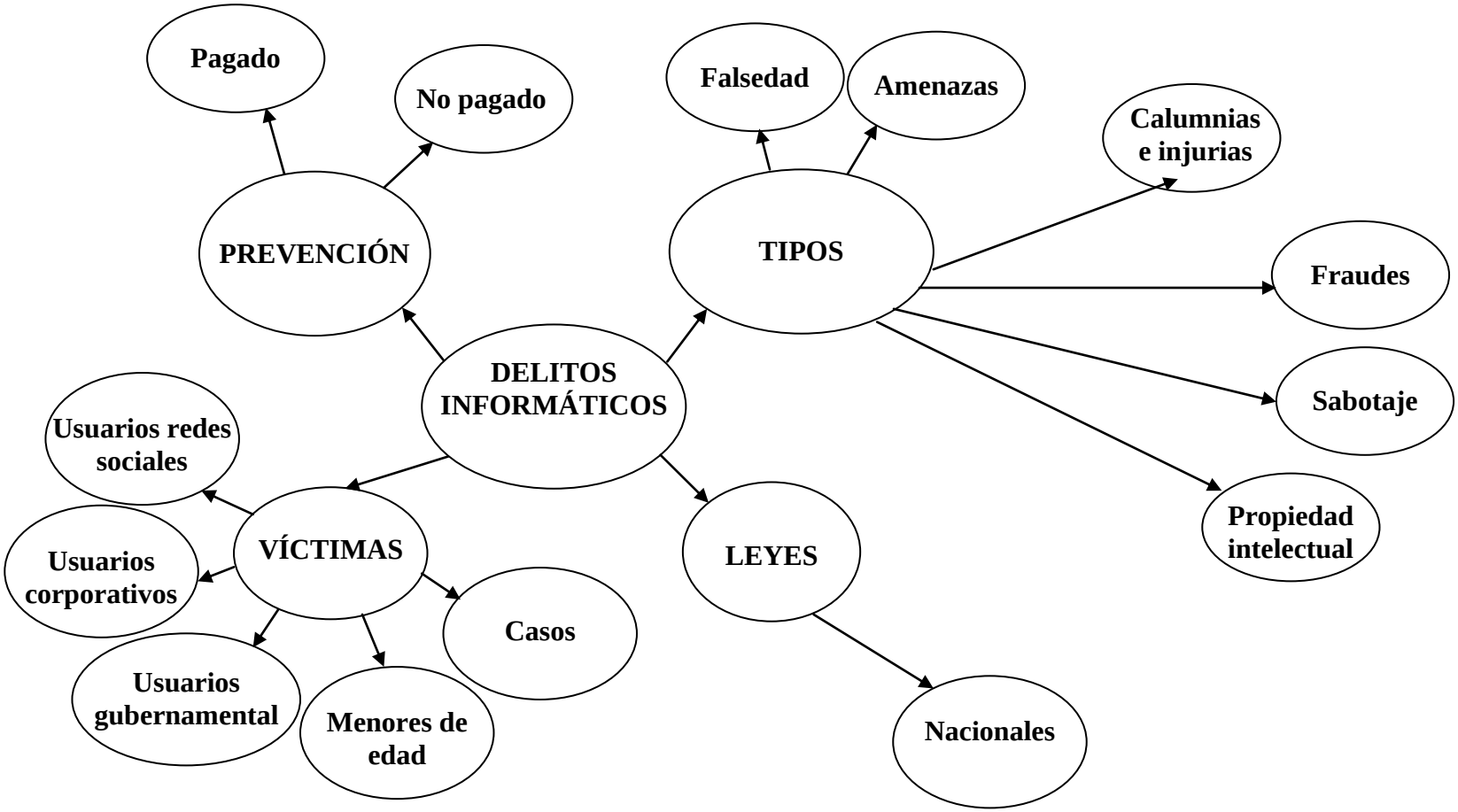


Gráfico 4 - Constelación de ideas variable dependiente
Elaborado por: Joffre Germán Díaz Cobos

DESARROLLO DE LAS CATEGORÍAS FUNDAMENTALES DE LA VARIABLE O LAS VARIABLES

INGENIERÍA SOCIAL

Uno de los eslabones más importantes al hablar de la seguridad informática, es la ingeniería social, pues no es más que el arte de obtener información muy confidencial, manipulando a las personas con fines fraudulentos. Este tipo de individuos llamados ingenieros sociales suelen por lo general, usar la tecnología para mediante engaños poder obtener la información que requieren, y poder violentar la integridad de una persona. Lo más interesante es que de esta manera no deben de usar métodos agresivos para violentar nuestra seguridad ya que nosotros mismos entregamos la información sin saber que estamos siendo presa de fraude. El problema erradica ahí, porque al ser nosotros mismos los que entregamos la información, al dejarnos llevar por estas nuevas técnicas, pues esa es una de las bases de la ingeniería social, aunque ahora en la actualidad hay diversas maneras de poder engañar a la gente, las formas más comunes son por ejemplo enviando un correo electrónico con un archivo adjunto que lleve un script o un spam y de esa manera poder obtener información de páginas que visitas, usuarios y contraseñas de banca electrónica, etc.

Erick Lewis Hernández en 2010 cita textualmente lo siguiente sobre este tema: "En estos casos en general, en la ingeniería social el delincuente piensa y anticipa la reacción de la gente para hacerlos caer más fácil, utiliza llamadas telefónicas, correos electrónicos, mensajes de texto, redes sociales, en realidad cualquier medo de comunicación. No hay tecnología capaz de proteger un sistema contra la ingeniería social, realmente como les digo nosotros no sabemos decir que no, si nos alaban, si se nos presenta una persona en la oficina a decirnos que bonitos vinimos hoy, que bonito somos, nos abrimos y ya le damos información que no deberíamos darle y esto se presta no solo en los fraudes informáticos sino en cualquier ámbito de nuestra cultura." (Lewis, 2010)

Clasificación

Tomando en cuenta la clasificación de la información, podemos identificar que se divide en datos públicos y privados y el departamento de sistemas debería

garantizar tres características importantes, como son la disponibilidad, integridad y confiabilidad de la información. En base de esta clasificación podemos decir que, la ingeniería social se clasifica en dos grandes grupos: computacional y humana.

Computacional

Si se habla de la palabra computacional obviamente se está hablando de computadoras y si las nombran tiene que estar inmerso el hardware y software. De tal manera que los computadores deben de tener niveles de permisibilidad muy bajos para que personas no autorizadas no ingresen a la información, se debe mantener los sistemas operativos actualizados para que los spyware no accedan mediante vulnerabilidades, si tienen un buen sistema de defensa y prevención la mayoría de gusanos informáticos, serán eliminados automáticamente.

Adjuntos de correo electrónico

Los archivos que llegan con el correo electrónico forman parte del mismo paquete, el correo puede ir sin un archivo adjunto pero jamás al revés. Los correos institucionales tienen un límite de capacidad para adjuntar archivos, pero en los correos gratuitos se encuentran limitados según el proveedor servicios. (Jiménez, 2014)

De tal manera que si excede el límite, regresa un correo indicando que no pudo ser enviado o simplemente no dejan enviarlo; en ocasiones al enviar un correo electrónico sin enviar ningún archivo adjunto, hay dos opciones: el equipo de donde enviamos el correo está infectado o de manera voluntaria enviamos algún script, virus o programa malicioso para obtener información de ese usuario. Este modo es el más usual de infectarse de virus. De igual forma el problema erradica cuando se abre la ventana de previsualización del mensaje, porque automáticamente el programa malicioso la infecta.

Algunos proveedores de correo electrónico tienen un sistema de protección, denegando o borrando automáticamente el archivo adjunto, pero en muchas ocasiones el usuario acepta verlo; por desconocimiento y se infecta.

Ventanas emergentes

También conocidas como pop-up o ventanas emergentes, suelen aparecer cuando abrimos una página web en nuestro navegador sin que hayamos nosotros elegido

abrirlas, en la mayoría de los casos tienen como finalidad mostrar publicidad y si da clic, se abre otra página y en muchas de las veces se llevan información del computador, por ejemplo: páginas visitadas o cuentas de correos electrónicos que han sido revisas en ese equipo, en otras ocasiones solo se abre una página en blanco, pues el recopilador de información ya está extrayéndola automáticamente. En variadas ocasiones estas páginas no interrumpen la visualización de lo que se estaba buscando, pero por debajo de estas están extrayendo información, estas páginas son llamadas pop-under. Es importante tener bloqueadas las ventanas emergente, pero hay casos como por ejemplo el Banco del Pichincha, cuando ingresan a su portal advierte de tener habilitadas las ventanas emergentes pues ahí se abre el formulario para colocar usuario y contraseña.

Sitios webs falsos o maliciosos

Algo falso puede también identificarse como malicioso o mal intencionado, por citar un ejemplo, si toma un taxi y este lo lleva a un sitio inseguro, lo más acertado es que le suceda algo malo. Estos lugares web mal intencionados son los mismo solo que electrónicamente. Para tener la película aún más clara hagamos de cuenta que usted es una persona que quiere realizar una compra de un libro por internet y el libro lo encuentra en una tienda virtual desconocida, es mas de la cual nunca usted se enteró que existía, pero al momento que usted ingresa al carrito de compras el libro y pretende culminar con la compra, es obvio que usted pagará con tarjeta de crédito y como es obvio deberemos ingresar todos nuestros datos y lo que es más peligroso el numero completo de la tarjeta incluido con el número de seguridad que se encuentra en la parte posterior del esta. Si no recibimos una notificación de la tienda que el libro será entregado en un tiempo determinado, lo más usual es que usted ya fue víctima de estafa. ¿Puede imaginar que puede suceder, si sus identificaciones cayeron en manos equivocadas?

Algo que ayuda en saber cómo se si estoy en un sitio seguro es verificando lo siguiente; cuando estamos en la barra de direcciones y vamos a ingresar datos muy personales, verifiquemos que al momento de ingresar el nombre de la página se antepondrá http:// lo que significa “Hypertext Transfer Protocol o en español protocolo de transferencia de hipertexto” pero cuando la página es segura se

pondrá, https:// lo que significa “Hypertext Transfer Protocol Secure o en español protocolo seguro de transferencia de hipertexto.

Correo no deseado (spam)

Por lo general no es de un remitente conocido y son mensajes que no hemos solicitado y que en muchos de los casos llenan nuestra bandeja de entrada, algunos nuestro proveedor de servicios lo identifica y lo envía directamente a la bandeja de correos no deseados. Actualmente los spam llevan información publicitaria que no es de nuestro interés. ¿Entonces como llegan a nosotros? Muy fácil pues nuestra direcciones de correo electrónico con extraídas, o compradas formando grandes cadenas de mails. Es importante no contestar a estos correo o peor aun enviar un correo de que nuestra dirección se removida de la base de datos de esta publicidad, porque lo único que hacemos es conformarles que la dirección es correcta que está habilitada y que podemos leerla. Lo recomendable es usar un software anti spam que nos ayudará que estos correo sean directamente enviados a los correos no deseados.

Mails falsos

Estos correos falsos o fraudulentos, como la misma palabra lo indica el único fin que tiene es realizar un fraude. Muchas veces se ha escuchado decir “no todo lo que brilla es oro” y para este caso nos queda este dicho exacto, pues en varias ocasiones vemos que nos llega el correo del banco indicando somos los ganadores del sorteo semanal y que para realizar la verificación debemos ingresar a nuestra banca electrónica mediante el enlace y código de operación ganador que nos proporcionan en la parte inferior y así validar nuestra identidad con su dispositivo de seguridad.

Gráfico 5 - Mails falsos
Elaborado por: Joffre Germán Díaz Cobos

Vemos que aparentemente todo está bien pues nos está llevando a un sitio seguro porque la dirección empieza por https, pero si le apuntamos a la dirección web segura que se encuentra subrayada en la barra de estado señala a la verdadera página a dónde iremos, es la siguiente: www.bucarest-hebdo.ro/pic/templates/1/. Pues nada que ver con la pagina del banco. Muchas personas han sido engañadas, hasta yo un momento lo dudé, pero recordé que no tengo cuenta en esa entidad financiera. Imagine de 100 personas a las que les llegue este correo, suponga que 50 tiene cuenta en este banco y que un bajo porcentaje da clic, ahora imagine cuán fácil es que caiga en la trampa por el desconocimiento de la tecnología. Por lo general estos correos son relacionados con entidades financieras, tarjetas virtuales, notificaciones financieras, avisos, noticias, premios, promociones, portales de tarjetas de crédito, etcétera.

Software pirata

Si se remonta a los hechos de la conquista y colonización de América, los piratas eran personas que navegaban sin licencia y su trabajo era asaltar los barcos en alta mar, hablando en términos informáticos los piratas son conocidos como personas de vastos conocimientos en informática y que dedica a duplicar programas que tiene algún valor, puesto por quien lo hizo y deja que la gente acceda ilegalmente aprovechándose del esfuerzo ajeno. No debe ser ingenuo al pensar que alguien

pirateó un software porque no tuvo nada más que hacer, existe un halo invisible que cuando instala estos programas bajados del internet no lo ve, pues por lo general este software tiene código malicioso incluido y cuando lo instala se ejecuta un malware recolectando toda la información importante que tiene en su equipo, de un momento al otro esta información es entregada al pirata y así realiza algún perjuicio con ella.

Humana

Esta variante de ingeniería social humana, habla certeramente de la interacción que existe de persona a persona, razón por la cual no debe ser un experto en informática ni un hacker para cometer un acto ilícito. Prácticamente estas personas llamadas ingenieros sociales son unos expertos en el arte de manipular a las personas. Este tipo de ingeniería sería la base de todo, cuando hablamos del tema de Ingeniería Social, esta existía antes de que las computadoras llegaran a su auge. De esta manera se dice que para estos, el internet fue como una tierra de nadie cuando llegó a ser tan importante, como hacer transacciones bancarias desde la comodidad de su hogar. Anteriormente para obtener dinero fácil, tenían que asaltar un banco o a un transeúnte, etcétera, ahora se aplican técnicas manipuladoras sobre la inocencia de las personas, hoy están a un solo clic del usuario que se dejaba engañar y póstumo a esto ser el estafado.

Hacking Ético.

Para entrar en materia cuando escuchamos la palabra hacker se nos viene a la mente varias cosas, pero una de las cosas que si estamos seguros es el sentimiento de inseguridad. Un hacker es un experto en alguna de las ramas de la informática, sea esta programación, redes, sistemas operativos. Y el hackear viene siendo el aplicar una serie de técnicas de ingenio para obtener algo, de acuerdo a la orientación que este tenga, y en muchos de casos se suelen hacerlo para demostrar su capacidad de invadir la privacidad de las personas. De ahí que esta persona lo haga con maldad, es un tema que requiere mucho cuidado, pues como existen médicos que son preparados para salvar vidas, pues existen algunos que dejan en el piso el juramento Hipocrático y deciden practicar un aborto. De la misma manera si un hacker actúa con maldad, este informático está faltando a su ética.

Para entender de mejor manera que es el hacking ético (Tori, 2008) lo expone este caso:

Para comprender mejor el concepto de hacking ético, analicemos un caso. ¿Es ético ingresar en una casilla de correo electrónico ajena sin conocer su password? Bajo las posibilidades que brinda el ethical hacking, por su puesto. Esa situación puede darse siempre y cuando la casilla de e-mail sea de alguien que nos haya autorizado, como profesional ético, a demostrarle que su organización es vulnerable. Como una casilla es personal (quizás de un gerente o de un administrador de sistemas), posiblemente ese ingreso nos lleve a obtener acceso a determinado lugar o a datos sensibles. Éstos, a su vez, serán utilizados para lograr entrar en un servidor y de allí dirigirnos hacia la red interna, con todo el riesgo que significa para una organización formal altamente informatizada. De ese modo, descubriremos pequeños descuidos que, desde un lugar impensado, pueden exponer a la empresa por completo. Sin embargo, esta vez, ese riesgo pasaría rápido a la historia, ya que estamos hablando de un típico caso de ethical hacking, en donde el problema es intensamente buscado, descubierto, analizado, reportado y por último solucionado a la brevedad.

Tipos

Dentro de algunos tipos de ingeniería social basada en humanos o personas tenemos las más comunes y que de una manera muy inadvertida, pueden afectar a la empresa donde estamos laborando y como personal informático, debemos tenerla muy en cuenta.

Vishing y llamada telefónica

Al igual que algunas prácticas fraudulentas ya antes citadas, vishing, hace uso del protocolo e Voz sobre IP pero a través de ingeniería social. Uno de los objetivos principales es obtener información delicada de la víctima, como número de cédula, cuentas bancarias y contraseñas, pues le hacen creer que alguien ha intentado sacar dinero de su cuenta bancaria o tarjeta de crédito y que ha ingresado una contraseña errada por varias ocasiones, razón por la cual le indica que debe cambiar la clave pero para comprobar que es el usuario con quien habla, le indica que debe ingresar al contraseña anterior. De esta manera pues usted la está dando todos sus datos privados y es ahí cuando se realiza el fraude. El vishing

es una técnica nueva de estafa, teniendo algunas variantes con el phising. Pues es de ahí de donde nace su nombre, en inglés voice y phising.

Se ha nombrado también la llamada telefónica, porque existen personas que llaman por ejemplo al soporte técnico de la compañía que nos presta el servicio de dominio y manejan nuestros correos, haciéndose pasar por un empleado de nuestra compañía y solicitando que resetee la contraseña de una cuenta. Para esto hay algunas mañas de la ingeniería social, como indicar que si no le ayudan de inmediato va a perder su trabajo o será multado, de esta manera la persona de soporte técnico, accede al requerimiento y finalmente cometen el fraude.

Dumpster diving

La traducción al español de estas dos palabras no es más que, recolección urbana. Y cuando se refiere a recolección, no es más que la gente que tiene acceso a la basura de la empresa. Quien podría imaginar que de esta manera tan inusual podríamos afectar a la seguridad de la compañía. Cuando alguna vez fuimos a una oficina y veíamos a una basurero de papeles tan particular que llevaba un cable eléctrico conectado a la pared, pues este es el que evitaba que la información vaya a parar a manos no deseadas, pues ahí es donde van a parar datos impresos muy importantes que era totalmente confidenciales pero porque la hoja se lleno de tinta demás lo votábamos y lo volvía a imprimir.

Piggybacking

Hoy en día está de moda que las personas quieren internet gratis y hacen uso de las redes inalámbricas que están al alcance de un ordenador. Hay muchas herramientas como software gratis en la red que te ayudan a determinar la contraseña de esa red que te aparece en nuestros ordenadores. Esta práctica tiene su inicio con la aparición de las redes inalámbricas, si bien alguien obtiene de forma ilegal nuestra contraseña, pues lo que inmediatamente va hacer es robar internet el problema es que mediante esta técnica ahora el intruso forma parte de nuestra red y de esta manera podría obtener información valiosa para nosotros y así robarla.

Tailgating

Esta es una técnica muy antigua en la sociedad. Se trata de un intruso que ingresa a las instalaciones de la empresa con su identificación, pero no porque la haya

obtenido, sino porque esta persona le hace creer a seguridad que se encuentra con usted o con el gerente de la compañía al ingresar a esta, logrando engañar a todos. Ya dentro de las instalaciones el objetivo es obtener de modo visual tipos de sistemas operativos en las computadoras, sustraer documentos legales importantes para la empresa.

Dejando una carnada

Esta manera tan común va de la mano con la técnica del tailgating, porque al ingresar de una forma engañosa a la empresa lo que simplemente hace es como su nombre mismo lo indica es dejar una carnada, una flash, CD, sobre un escritorio de una forma muy visual no escondida, para que alguien se la encuentre y por la curiosidad de que nadie reclama en la oficina la carnada, la conecte a su computadora o en la de un compañero y automáticamente se ejecute un malware y de esta manera obtener información de esa computadora y sea enviada de forma no visual al delincuente. Los keylogger son los más famosos software instalados en estas carnadas con ello lo que hace es seguir paso a paso lo que se hace en esa máquina.

Pruebas de seguridad

Las pruebas de seguridad son de gran importancia para determinar en qué grado de vulnerabilidad se encuentra nuestro sistema informático, lo cual de acuerdo a los resultados obtenidos, podemos determinar qué estrategia podemos emplear para que nuestro sistema pueda está libre de ataques por intrusos. De acuerdo a varias pruebas que realizan expertos en el tema, podemos determinar donde se encuentran los nudos críticos y poder reorganizar o crear nuevas directivas de seguridad para poder controlar la infiltración indebida de personal no autorizado para entrar en la organización. Obteniendo los resultados de esta evaluación es de suma importancias que el gerente o quien administre el lugar tenga pleno conocimiento del riesgo al que se encuentra expuesta la información delicada y sensible de la empresa debido a las agresiones ofensivas por parte de usurpadores, poniendo en peligro la organización.

Tipos de Hacking Ético

Para que pueda entender los tipos de Hacking Ético es preciso, clasificar los tipos que existen de una manera informática para ello, vamos a colocar cuatro grupos

en los que se los han clasificado, existen organizaciones que prestan este tipo de servicios, para ver cuán vulnerable es el sistema informático de nuestra organización, la clasificación queda de esta manera :

Black Box Hacking

Gray Box Hacking

White Box Hacking

Web Hacking

Ahora explicaremos cada uno de estos:

Black Box Hacking

El modelo de operar de este tipo de hacking, es simular un ataque con total conocimiento del cliente, a la IP pública sin tener un previo conocimiento de la infraestructura d la red, para poder determinar de esta manera hasta donde pueden llegar a penetrar nuestra red interna a través de la externa.

Gray Box Hacking

Habiendo tenido paso a través de la red pública o llamada internet, nos abrimos camino a la red interna o conocida como intranet, y de la misma manera de operación de la black box, sin ningún conocimiento de la infraestructura de la red interna, de esta manera estaríamos simulando que el ataque viene de algún funcionario de la empresa pero que tiene acceso a las inmediaciones de nuestra oficina, para poner de ejemplo, como si nos estuvieran pidiendo acceso al wifi para obtener internet.

White Box Hacking

Para este caso es muy similar a gray box, con la diferencia que para realizar esta evaluación se necesita obtener un punto de red físico y el listado de todas las IP de los equipos que se encuentran en la compañía, lo que se intenta simular aquí, es el ataque de un funcionario interno y que no tiene acceso a ciertos datos de la compañía.

Seguridad Informática

La seguridad informática tiene un principal objetivo principal, resguardar todo elemento físico que se relacione con el sistema informático, de la compañía para este caso puntual, al referirnos de resguardar, se refiere a posibles ataques por personas mal intencionadas, algún software malicioso que trate de violar las

políticas de seguridad de la empresa o de tener un plan de contingencia que garantice que la información está a buen recaudo en un sistema de respaldos continuos sean estos manuales o automáticos por posibles daños electrónicos en los discos duros, pero al hablar de seguridad informática nos referimos a algo utópico definitivamente, porque sabemos que no existe un sistema de seguridad informático cien por ciento seguro.

Debilidad humana

Cuando nos referimos a la debilidad humana nos referimos al gran problema que existe por el desconocimiento de seguridad con el personal de la compañía, pues son el vagón más débil del ferrocarril en cuanto a seguridad, hablaba en el tema anterior de seguridades informáticas, que un sistema informático, está del todo protegido y tiene que ver mucho con el personal humano, pues una falla de alguna persona del interior de la compañía tiene mucho que ver en que el sistema sea violado. Muchos de estos ataques al personal puede darse como el ya tratado en temas anteriores como la ingeniería social, que de por si es uno de los ataques, más complicados de defensa, porque podemos tener equipos muy sofisticados para combatir el ataques de hackers y software que cifre conexiones, pero si un ingeniero social actúa con una sola persona del interior puede ir burlando todo el sistema de seguridad y despedazar las políticas que se pudieron haber instaurado, para dar un buen tratamiento a la información.

Web Hacking

Este tipo de hacking no es muy común realizarlo, pero cuando amerita efectuarlo se hace una evaluación integra, de con qué tipo de seguridades cuenta el servidor web que manejamos, pero a nivel de servicio web o llamado http y el tipo de programación de scripts de tipo SQL injection y Cross Site Scripting.

Sistemas de protección

Los sistemas de protección que podemos obtener de hoy en día, son muchos y variados, pero así mismo son las amenazas a las que nos vemos enfrentados día a día, tomemos en cuenta que la tecnología avanza y cada vez son más, las nuevas plataformas que tenemos disponibles, pues cada día es de suma importancia las necesidades empresariales de tener comunicación de todo tipo, con otras instituciones sean estas clientes o proveedores para el bien común, pues el factor

rapidez es lo que hoy en día le da cierta eficiencia para concretar una venta bien hecha.

Humano

Es importante que se encuentre informado de los pasos que está dando, y estar al día de la tecnología. Para ello es de suma importancia definir políticas de seguridad que serán un lineamiento inviolable a seguir para que pueda estar protegido. Ya se ha mencionado, el riesgo es alto y el no seguir al pie de la letra, las directrices que nos otorgan, sería una desventaja invaluable frente a los problemas que se podrían ocasionar a los intereses de la institución. Para ello es muy importante que el personal, sea correctamente capacitado sobre algunos fraudes electrónicos y generar medidas preventivas para no sea presa fácil de los hackers informáticos.

Informático

Desde el punto informático se debe toma en cuenta, que si bien es cierto cuando el recurso humano ya ha sido capacitado, podemos ya dar el siguiente paso en referencia al tema informático para tomar acciones referentes, a la seguridad informática. Para lo cual debemos de partir de un referente básico, asegurar la información, proteger los datos más importantes y que pueden ser vulnerados y por consiguiente la autenticidad de la misma. Tomando en cuenta la seguridad informática, uno de sus objetivos principales es proteger los datos, evitando que estos sean borrados y llegan a ser modificados por personas inescrupulosas. En cambio el proteger la información lo que nos debe certificar es la integridad y disponibilidad de los datos en cualquier momento y que los datos sean auténticos. Para esto existen algunos programas pagados o libres que nos ayudan, a que gusanos informáticos no deterioren la información; hablaremos de algunos de ellos.

Antivirus/Antispam

Definitivamente cuando se habla de un antivirus, en informática estamos asegurando que es un software que no permite el contagio de un virus, pues el único objetivo de este software en sus inicios, fue detectar y eliminar el virus, con la evolución de las tecnologías sistemas operativos e internet, las técnicas de estos programas ha ido avanzando, pues ahora no solos los borran, son capaces de

neutralizarlos desinfectar el archivo y eliminar el código malicioso, además que son capaces de reconocer algunas otras infecciones que se dan de hoy en día como software espía y los llamados rootkits. No todos los antivirus actúan de la misma manera, pues cada uno de estos se comportan de distintas maneras. Los antivirus que son proactivos y al instante detectan si hay código malicioso utilizan técnicas heurísticas. Aquí podemos observar algunos de los más famosos antivirus que alguna vez hemos ocupado o que tenemos en casa o la oficina usando, donde podemos observar un ranking de los 10 mejores.

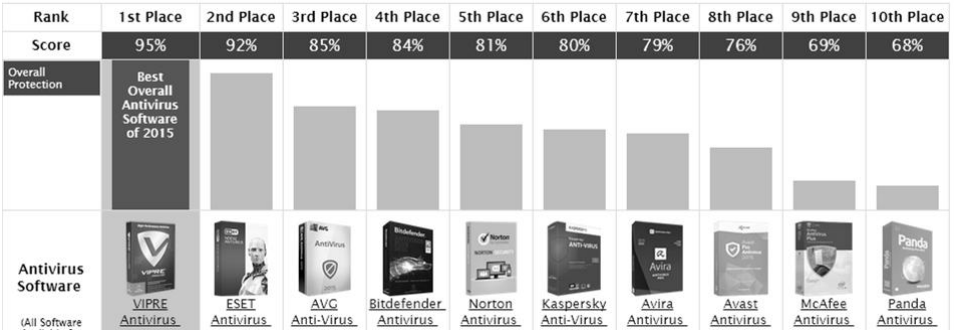


Gráfico 6 – Ranking de antivirus
Fuente (PC antivirus reviews, 2015)

Un antispam se debe diferenciar algunas categorías con las que trabajan; la más usual es de forma automática, y cabe mencionar que los administradores de correo electrónico ya filtran algunos de estos mensajes enviándolos directamente a la bandeja de correos no deseados y si adicional tenemos un software antispam no está demás, también ejecutará lo mismo, pero cuando debe intervenir el usuario es cuando debemos elegir que acción debemos hacer, como elegir si es o no spam.

Firewall e IPS´s

Los firewall o los llamados corta fuegos son dispositivos físicos o software que son especializados en filtrar la entrada y salida de la información, trabajan sobre la capa de red y que como política por defecto el aceptar la comunicación de máquinas entrantes, pero también podemos elegir el bloquear toda entrada y salida y solo dejamos que determinados equipos entren o salgan. Pello Xabier Altadill Izura denota lo siguiente sobre los firewalls "Para que un firewall entre redes funcione como tal debe tener al menos dos tarjetas de red. Esta sería la tipología clásica de un firewall: Esquema típico de firewall para proteger una red local conectada a internet a través de un router. El firewall debe colocarse entre el

router (con un único cable) y la red local (conectado al switch o al hub de la LAN) Dependiendo de las necesidades de cada red, puede ponerse uno o más firewalls para establecer distintos perímetros de seguridad en torno a un sistema". (Izura, 2003)

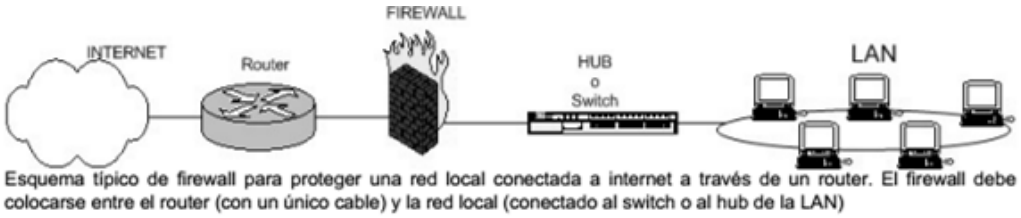


Gráfico 7 – Esquema típico de firewall
Fuente: (Izura, 2003)

Sistemas de Correlación

Los sistemas de correlación se pueden entender como un grupo de sentencias que realizan, ciertas operaciones obteniendo datos de entrada y dando como resultado, un solo dato de salida, pues la información que es obtenida por nuestros servidores, es detectada y analizada, obteniendo un gráfico de espectro de la información que si es importante para nosotros. Pues la relación de correlación que existe entre la información que ingreso y la que en verdad nos sirve es la que podemos aprovechar. Para ellos se puede instalar un sistema para detectar toda la información de una red, esto con la ayuda de una capa de red que nos ayude a trazar un espectro infinito. Un problema elocuente que tenemos con los sistemas de correlación, es la fiabilidad y visibilidad limitada en los detectores de entrada y salida. Estos sistemas de correlación los podemos encontrar en herramientas comerciales como CISCO MARS o herramientas open source SIEM OSSIM. Para este último (Olmos, 2008) redacta un informe de la Universidad Politécnica de Valencia:

Ossim es la abreviatura de Open Source Security Information Management System (Sistema de gestión de la información de seguridad Open Source) desarrollado para gestionar la información de seguridad de una red. Es una distribución que integran más de 22 productos de seguridad todos ellos "Open Source" capaces de correlacionar entre ellos. Ossim es una plataforma compleja pero a su vez potente, ya que integra las soluciones de código libre de seguridad

para la monitorización y detección de patrones de redes más conocidas (Snort, nessus, ntop, nmap, nagios, etc.), integrándolas en una arquitectura abierta que se aprovechará de todas sus capacidades para aumentar la seguridad en las redes.

El objetivo de Ossim ha sido crear un framework capaz de recolectar toda la información de los diferentes plugins, para integrar e interrelacionar entre si y obtener una visualización única del estado de la red y con el mismo formato, con el objetivo de aumentar la capacidad de detección de anomalías, priorizar los eventos según el contexto en el que se producen y mejorar la visibilidad de la monitorización del estado de la red actual.

DELITOS INFORMÁTICOS

En muchas de las ocasiones, nos ponemos a pensar como hemos avanzado tecnológicamente, y el resultado es asombroso, pues cada día sale un nuevo equipo, pero con el avance de esta también existen ciertas personas que avanzan también, en nuevas formas de obtener nuestra información de una manera no tan lícita. Si bien es cierto el avance tecnológico ha contribuido en que tengamos datos más exactos sobre alguna información específica en nuestra empresa, de la misma manera tenemos que avanzar a la par, con mecanismos de defensa con los delitos informáticos que de hoy en día son muy comunes y que cada día existe gente estafada por estos delincuentes informáticos. Ahora bien este tipo de actividades que tiene carácter ilegal, como fraude, estafa, robo, falsificación y sabotaje son considerados delitos informáticos, siempre y cuando tengan que ver con información. El delito informático implica cualquier actividad ilegal que encuadra en figuras tradicionales ya conocidas como robo, hurto, fraude, falsificación, perjuicio, estafa y sabotaje, pero siempre que involucre la informática de por medio para cometer la ilegalidad. La asamblea nacional se ha preocupado por este asunto de tal manera que (Acosta, 2013) en la prensa comunicaron lo siguiente:

La Asamblea Nacional de Ecuador se encuentra en pleno e intenso ajetreo legislativo para conformar el proyecto de Nuevo Código Penal Integral que intentará consolidar toda la jurisdicción penal, tanto adjetiva como procesal, ahora dispersa en varios y múltiples códigos normativos. Sin duda estos esfuerzos en la

formación de la leyes convocan intereses y visiones; de conformidad con ello y con algo de insospechado ejercicio la Policía nacional del Ecuador propone tipificar varios " delitos cibernéticos ", liderando esta iniciativa que parecería ser un patrimonio de otros operadores legales con natural mandato sobre ello (Fiscalía, Consejo nacional de la Judicatura, Facultades de Jurisprudencia de las Universidades). Seguramente habrá mucha discusión , no muy doctrinaria por lo apretado de los tiempos legislativos, acerca del alcance y la relevancia jurídica de las conductas delictivas propuestas para ser tipificadas como delitos, sin embargo llama mucho la atención que un tema tan trascendental y actual en materia penal no sea objeto de ninguna propuesta por parte de las Universidades; en el Ecuador se sigue acumulando deuda y responsabilidad social por parte de la Academia Universitaria en relación con los procesos legislativos de formación legal, una Universidad más activa, creativa y propositiva debe ser el horizonte para la renovación de la Cátedra.

Tipos

Para entender de mejor manera los delitos informáticos, vamos a estudiar los más conocidos, dentro de la literatura algunos autores los clasifican de algunas maneras, aquí veremos los más relevantes:

Falsedad

Dentro de este aspecto, como su nombre lo indica, se trata de todo acto de falsificar algún documento o modificación de datos, en algunos casos se extiende a la falsificación de tarjetas de crédito, se conoce que las que funcionan con banda magnética son muy fáciles de falsificar, por ello ahora las nuevas tecnologías han innovado mediante chip electrónico.

Amenazas

Este tipo de delito consiste en cualquier tipo de amenaza, por cualquier tipo de medio electrónico, en el que la persona o empresa se sienta amedrentada, por este sea correo, o por alguna red social. Si el individuo que esta amedrentando a la persona envía un correo electrónico, este se puede hacer un seguimiento para ver de dónde lo realizó, pero al ser personas con experiencia extrema en estos trabajos, es fácil para ellos realizarlo desde cualquier local de internet, pero aun si

trabajan en conjunto y el correo viene desde el exterior. Se vuelve una odisea y como comúnmente se dice, se convierte en el juego del gato y el ratón.

Fraudes

El fraude es una de las maneras más antiguas de corrupción, tiene como herramienta el engaño a base de mentiras, herramienta muy importante que usan los ingenieros sociales para obtener información, de una persona para manipular datos u obtenerlos de forma ilegítima, para poder lucrar de ellos.

Sabotaje

Esta también es una herramienta muy contundente cuando hablamos de este tipo de delito, pues es muy común y muchas veces proviene, del interior de la compañía, el interrumpir o malograr las bases de datos o información importante de la compañía cuando se la necesite, o dañar equipos. Cualquiera de estas actividades son indicios de sabotaje, lo cual es sancionado en el código penal vigente del Ecuador.

Propiedad intelectual

Dentro de la ley de propiedad intelectual del Ecuador se tipifican algunos artículos que salvaguardan la información que tenemos en nuestros computadores, de tal manera que si somos desarrolladores de software y en nuestra computadora tenemos los archivos fuentes de una aplicación, y alguien utiliza dicho código para generar una aplicación similar o la misma, es objeto de sanción, de igual manera las personas que dentro de una compañía tenga software pirata, también son sancionados.

Víctimas

En nuestra sociedad actual, todas las personas o empresas son víctimas del desconocimiento del manejo de datos y tecnología informática, lo cual conduce a que las que están más atrasadas tecnológicamente, tengan miedo del uso de los recursos tecnológicos, lo cual tiene un efecto causa y un retraso en las empresas de hoy, por el temor a ser engañados, al usar alguno de estos elementos antes mencionados. Todo esto antes descrito se da, por cada vez ha aumentado la proliferación de personas o agrupaciones con intenciones maliciosas, para desarrollar métodos delictivos cada vez más sofisticados. Las víctimas son por lo

general usuarios de redes sociales, corporativos, gubernamentales, menores de edad, entre otros, aquí definiremos los nombrados.

Usuarios de redes sociales

¿Hoy en día quien no está suscrito a una página de redes sociales? La pregunta es un tanto absurda porque la respuesta es obvia, una gran mayoría estamos en redes sociales, pero lamentablemente no conocemos el potencial que tienen al momento de entrar en contacto con nuestros familiares y amigos, pero cuando no manejamos una buena política de privacidad se puede convertir en un verdadero dolor de cabeza. Existen riesgos eminentes a los que nos vemos enfrentados, empezando que cuando ingresamos a darnos de alta en ellas, nos piden una serie de datos personales, dentro de ellos que gustos tenemos, esto es alimentado en una gran base de datos, la cual posteriormente es vendida a grande empresas y llegando a manos equivocadas, puede ocasionar más que un problema.

Según el experto en seguridad (Willems, 2011) de la compañía G DATA, expresa: Los cibercriminales están intensificando el uso de las redes sociales como eficaces propagadoras de malware. Una de sus estafas preferidas es la propagación de código malicioso a través de enlaces posteados en cualquier sitio web y, por supuesto, en las redes sociales. Es frecuente que esos enlaces que en teoría nos dirigen a algún video escandaloso nos lleven directamente a alguna web infectada. Y es complicado que los internautas reconozcamos fácilmente un enlace peligroso pues las direcciones están siempre camufladas, por ejemplo, por alguna herramienta capaz de acortar URLs. Usar una solución de seguridad que incorpore algún tipo de filtro web incrementa la seguridad y, en mi opinión, es obligatoria para cualquiera que valore su seguridad online.

Tabla 2 - Oficinistas que dan clic en el enlace en redes sociales

Los resultados del estudio, por edades y sexo:

¿Pinchas en los enlaces que te llegan en las redes sociales?			
	Sí, en todos	Sí, sólo si vienen de amigos	No
Hombres (18-24)	26,24%	38,02%	35,74%
Hombres (25-34)	25,92%	38,63%	35,45%
Hombres (35-44)	21,09%	33,56%	45,35%
Hombres (45-54)	18,23%	31,10%	50,66%
Hombres (55-64)	15,93%	26,21%	57,86%
Total Hombres	**21,46%**	**33,55%**	**44,99%**
Mujeres (18-24)	21,54%	45,38%	33,08%
Mujeres (25-34)	20,43%	40,92%	38,64%
Mujeres (35-44)	15,41%	35,59%	48,99%
Mujeres (45-54)	13,72%	31,27%	55,01%
Mujeres (55-64)	9,83%	30,48%	59,69%
Total Mujeres	**16,29%**	**36,73%**	**46,99%**
Total	**18,77%**	**35,20%**	**46,02%**

Fuente: (Lewis, 2010)

Usuarios corporativos

Como puede observar en la tabla 2 este tipo de usuarios son los más buscados por los cibernautas para delinquir, la razón es porque son ejecutivos que manejan banca electrónica, pero también los usuarios de los servicios bancarios son presa de estos, gracias a su vocación de ejecutivos no les da tiempo para ir a un banco personalmente, por lo cual optan desde la comodidad de su casa hacer sus pagos, transferencias y no saben que, hay alguien que está siguiendo sus pasos, en muchos de los casos si no sabe manejar con cautela la información puede ser presa de la ingeniería social. De Gouveia dice: "una cadena es tan fuerte como su eslabón más débil y es por ello que además de contar con una solución antivirus con capacidad de detección proactiva, los usuarios deben requieren buenas prácticas para navegar en Internet y así poder reconocer este tipo de correos falsos y engaños. En caso de recibir este tipo de amenazas, es muy importante reportar los correos de phishing".

Usuarios gubernamentales

Otro sector que tiene puesto el ojo, es el gubernamental y no solo a nivel de Ecuador sino a nivel mundial, por lo general este tipo de ataques no tiene que ver mucho con lo que respecta a extraer dinero o estafar, van más a instancias de ser detractores de los gobiernos, para que sepan que estas agrupaciones de hackers tiene el poder de irrumpir en una página web estatal, y de pronto colocar una

imagen en la página web de inicio, esto es lo que le sucedió a la página de la presidencia del ecuador , municipios y gobiernos provinciales.

Casos

En el periódico El Telégrafo (Telégrafo, 2011) se da una amplia información de los hackers, llamados Anonymous Iberoamérica se acredita estas intromisiones, llamada operación cóndor libre, debido a una pronunciación de ellos frente a la falta libertad de expresión, a continuación la noticia completa:

Los hackers que se identifican como Anonymous Iberoamérica han publicado información de la Corporación Nacional de Telecomunicaciones CNT, de varios trabajadores del Aeropuerto de Quito, entre otros. A esto lo denominan "sorpresas" y para miércoles se deben esperar más a lo largo del día, según han informado vía Twitter.

La "Sorpresa # 4" fue revelada a las 14:12, dos minutos antes de lo anunciado. La página web de la empresa Hunter para Ecuador (http://www.hunter.com.ec) mostraba en su página principal una imagen de personas enmascaradas en un metro y tenía la leyenda "Somos Anonymous". A la imagen la acompañaba el texto que comenzaba con un "Somos Anonymous y estamos con ustedes pueblo ecuatoriano", que continuaba dirigiéndose directamente al Presidente del Ecuador apuntando que los esfuerzos con Corea del Sur para identificarlos serían inútiles. Terminaban con el conocido lema "Somos Anonymous, somos legión, no perdonamos, no olvidamos, esperadnos", pero lo firmaban Colombianhackers, dando a entender que este ataque había sido realizado con su apoyo. Esto se confirmó con el tweet de Anonymous Iberoamérica (o Anonymous Hispano) que establecían que el ataque llegaba "patrocinado" por los piratas colombianos. La página de Hunter fue restablecida por la empresa tiempo después del ataque.

La "Sorpresa # 3" estaba planeada para las 13:13, pero fue expuesta un minuto tarde. Se publicaron varios links que, supuestamente, llevarían al panel de control del sistema de videoconferencia del Ministerio de Medio Ambiente.

"De hecho esa no era la sorpresa 3 originalmente, pero la web de la sorpresa 3 está offline, cuando se levante se las damos", publicaron los hackers en Twitter.

La "Sorpresa #2" fue la revelación de datos personales de varias personas que trabajan en el Aeropuerto de Quito. Los nombres, apellidos, correos electrónicos,

cargo, teléfonos, números de cédula y usuarios fueron publicados en un boletín de pastebin.com

Asimismo, la "Sorpresa # 1" fue la publicación del diagrama físico de la red de servidores de CNT utilizando la página pastebin.com publicaron un link con el diagrama de los servidores.

Cada una de sus publicaciones tienen agregadas las etiquetas de #Antisec, una operación internacional lanzada por Lulzsec y Anonymous y la etiqueta de #OpCondorLibre de la operación que fue creada para, presuntamente, defender la libertad de expresión en el país.

Este grupo de hackers, que aseguran pertenecer a Anonymous, lanzó la "Operación Cóndor Libre" y desde ayer alertaba, en las redes sociales, de un ataque masivo planeado para las 10:00 de hoy que coincidiría con el inicio del informe del Presidente ecuatoriano a la Nación.

La "Operación Cóndor Libre", presuntamente, pretende defender la libertad de expresión del país tal como lo afirmaba una figura enmascarada en un video colgado en Youtube hace varios días (video adjunto a esta nota).

El pasado lunes, la página web del Municipio de Guayaquil fue víctima de los ataques por estos piratas informáticos y la semana pasada fue vulnerada la web del Municipio de Orellana.

Frente a las amenazas que desde un principio se dieron a los portales gubernamentales, el ministro de Telecomunicaciones, Jaime Guerrero, en días pasados en una entrevista con El Ciudadano dijo que se castigaría "con todo el peso de la ley" a los piratas informáticos que atacaran sitios gubernamentales e informó que cuentan con el apoyo de Corea del Sur para identificarlos.

Páginas gubernamentales saturadas

La mañana de este miércoles las páginas de la Presidencia, el Ministerio de Telecomunicaciones, Vicepresidencia y de la Alcaldía de Quito que se vieron fuera de servicio a las 10:00 coincidiendo con el inicio del informe del Presidente Rafael Correa a la Nación y del ataque masivo de los hackers que se denominan Anonymous Iberoamérica.

El servicio de la página de la Presidencia y la de Telecomunicaciones fueron reactivadas rápidamente y las de la Alcaldía de la capital y Vicepresidencia tardaron más tiempo en volver a su funcionamiento normal.

En el momento de la caída, en la web oficial de la Presidencia se podía ver un mensaje que informaba que el sitio estaba teniendo problemas de mantenimiento.

Prevención

La palabra prevención en el diccionario trata como, medidas que se toma de una manera anticipada, para evitar que alguna situación mala suceda, lamentablemente en el país se ha vuelto más recurrente, y va tomando fuerza de tal manera que las mayoría de compañías se ven envueltas en situaciones, que los lleva a serias pérdidas de dinero, lo cual implica en poner en riesgo la estabilidad económica, porque en la mayoría de casos se ven reflejados en la competitividad por muchos empleados deshonestos, si bien es cierto este tipo de conductas son repetitivas, no son sencillas de poder detectar o prevenir, esto se puede relacionar como un cáncer dentro de las organizaciones, sean estas privadas o públicas, pero al no prevenir estos causales se vuelve más fácil el ataque.

Software pagado

Para que tenga la seguridad de no infectado con malwares, debe tener instalado un software que lo proteja contra el ataque, debido a que cada día aumentan los diferentes virus y programas espías que se propagan por el internet.

Muchas personas para transportar información, sencillamente usan una flash o un disco extraíble externo, pero ¿Sabe si es confiable conectar este dispositivo en su máquina? Es la pegunta que muchas veces no se la plantea, pero en la realidad afecta en gran medida, si no toma las precauciones del caso. Al ser precavido, no dude en tomar medidas comprando un paquete de antivirus con protección de internet, definitivamente tiene muchas más ventajas sobre un software que no es de pago. Entre una de ellas, el software de pago es más eficaz que uno de no pago, por el simple hecho que tiene más características de protección frente a un ataque, por lo general estos son actualizados de forma automática, con todas las últimas definiciones de virus existente hasta el momento, muchos constan con una característica especial, llamados los teclados virtuales, que son más que útiles el momento de usar contraseñas, anulando casi en su totalidad a los programas

espías que generan un log con cada tecla que se ha presionado. En el artículo (PC Word, 2010) la prestigiosa revista no habla sobre este tipo de software contrastando los que hemos mencionado:

Tabla 3 - Top 5 de productos de antivirus pagados

TOP 5 PRODUCTOS ANTIVIRUS PAGADOS DE PC WORLD

	PROGRAMA	Calificación	Detección antivirus y anti-spyware				Limpieza de infecciones		Calificación del diseño
			Detección de código malicioso basado en firmas	Bloqueo de código malicioso del mundo real: ataques totalmente bloqueados	Bloqueo de código malicioso del mundo real: ataques bloqueados parcialmente	Bloqueo de código malicioso del mundo real: ataques no detectados	Limpieza exitosa de componentes activos del código malicioso [1]	Limpieza exitosa de componentes activos e inactivos del código malicioso [2]	
1	Norton Antivirus 2011 US$40 por 1 año/1 PC find.pcworld.com/71019	★★★★½ SUPERIOR	98.7%	96.0%	0.0%	4.0%	80.0%	60.0%	Muy bueno
	▸ Norton Antivirus 2011 es un paquete razonablemente completo que ofrece detección y limpieza de código malicioso sólidos junto con una interfase bien diseñada.								
2	BitDefender Antivirus Pro 2011 US$40 por 1 año/3 PCs find.pcworld.com/71020	★★★★½ SUPERIOR	97.5%	68.0%	20.0%	12.0%	80.0%	70.0%	Superior
	▸ BitDefender Antivirus Pro 2011 hizo un buen trabajo en detectar y eliminar código malicioso, pero su lenta velocidad de exploración y su efecto en el desempeño de la PC lo dejó detrás.								
3	Avast Pro Antivirus 5 US$40 por 1 año/1 PC find.pcworld.com/71021	★★★★ MUY BUENO	94.8%	80.0%	4.0%	16.0%	70.0%	30.0%	Bueno
	▸ En medio de este grupo, el fácil de usar Avast Pro Antivirus 5 explora código malicioso rápidamente y ofrece una detección de código malicioso decente – aunque no impresionante.								
4	G-Data AntiVirus 2011 US$30 por 1 año/1 PC find.pcworld.com/71022	★★★★ MUY BUENO	99.4%	84.0%	4.0%	12.0%	80.0%	60.0%	Aceptable
	▸ En general, G-Data AntiVirus 2011 obtuvo buenas calificaciones en detección y desinfección; es relativamente ligero en características extras pero también cuesta un poco menos.								
5	Kaspersky Anti-Virus 2011 US$40 por 1 año/1 PC find.pcworld.com/71023	★★★★ MUY BUENO	99.8%	53.7%	100.0%	90.0%	100.0%	50.0%	Bueno
	▸ Kaspersky Anti-Virus 2011 es fácil de usar y detiene bien los ataques; sin embargo, el programa afecta el desempeño de una computadora más de los que nos hubiera gustado ver.								

NOTAS: Precios vigentes al 3 de noviembre de 2010. [1] Limpieza de archivos activos del código malicioso. No incluye la eliminación de cambios al Registro o archivos inertes. [2] Prueba realizada con las configuraciones predeterminadas.

Fuente: (PC Word, 2010)

Software no pagado

Por lo general cuando se habla de software gratuito o que simplemente lo hemos descargado del internet, se nos viene algunas ideas a la cabeza, como por ejemplo que no sirve, que está dañado o es una trampa para obtener nuestros datos y posterior poderlo descargar, centrándonos en esta última idea, le deja descargar software para obtener sus datos y lo más importante su correo electrónico y de esta manera alimentar su gran base de datos, para luego ser vendida o ser usada por ellos mismos para promocionar algunos de sus otros productos que ofrece la corporación, este riesgo puede correr al descargar estas herramienta que están libres en la red, pero en realidad son efectivos, con características reducidas frente al que es de pago, lo que puede ocasionar que tenga que descargar herramientas adicionales, para poder estar protegidos de mejor manera, cubriendo las falencias del software de no pago.

Metodología de Políticas de Seguridad de Benson.

(Raggad, 2010, pág. 207) Hace referencia a la política de seguridad de Christopher Benson, en la que se describe claramente el proceso a seguir para definir políticas de seguridad frente a los diferentes eventos que puedan presentarse. Microsoft recoge la información de Benson en su sitio web (Microsoft, 2004):

Esta metodología ayuda a mantener la información siempre a buen recaudo a través de planes de contingencia, por que los datos por lo general están siendo expuestos todo el tiempo en un lugar determinado; existen varias maneras para que la información este expuesta, por ejemplo por casos aislados o su vez porque alguien quiere dañarlos al obtenerlos. Lo más importante cuando tiene información bajo su responsabilidad, es que estos datos se mantengan siempre disponibles, también algo de lo que debe percatarse es que estos sean fiables. Algo que debe tener en cuenta toda institución que maneja información; es quien tiene acceso a ella, pues no todos deben tener los mismos privilegios, pues existen datos de carácter confidencial.

Si usted es un directivo informático debe tener en cuenta que el tratar de implementar una metodología requiere su tiempo, estudio y constantemente debe ser evaluada.

Para iniciar la metodología debe tener claro mediante un boceto el sistema de información que maneja la compañía, de esta manera empiece a analizar cuáles son las vulnerabilidades que tiene esta y de esta manera lograr predecir los posibles ataques en ella; si está preparado ante un atacante y sabe cómo podría comportarse frente a sus debilidades, menor será el impacto del mismo.

Existen varias amenazas que pueden existir dentro de la compañía como colaboradores que no tienen cuidado con sus accesos personales a los sistemas de información, sin tener la mínima intención de hacer daño; fuera de esta siempre habrá gente que desee obtener los datos valiosos para la compañía y que seguramente obteniéndola podrían causar graves perjuicios para esta. Una amenaza que no puede predecir son los desastres naturales, este es un gran motivo por el cual debe tomar sus precauciones. El gráfico 8 nos muestra un resumen de lo expuesto anteriormente.

Gráfico 8 – Amenazas para la seguridad

Fuente: (Raggad, 2010, pág. 207)

Por cada ataque que logre detectar y este afecte a su información debe desarrollarle una metodología de protección.

Para definir una estrategia proactiva debe evaluar que puede ocurrir antes de que el ataque llegue a ser consumado y tener conocimiento de los impactos que este llegue a tener en su sistema de datos. Un punto importante que debe tomar en cuenta es el costo de la pérdida de información versus el costo de la implementación de la metodología, para contrarrestar la amenaza, tome en cuenta que la técnicas que use para bloquear este ataque nunca será efectivo al cien por ciento; y deberá tener un método rápido para recuperar la información perdida o dañada.

Los daños que puede ocasionar pérdida de información pueden ser muchos, desde fallas eléctricas hasta ingeniería social, para ello es importante que conozca que impacto puede tener en la compañía. Para esto se puede montar un pequeño laboratorio de pruebas donde se realicen simulaciones de los posibles ataques que existan en el entorno de trabajo. Esto logrará darle un panorama más claro de lo que sucede y las alternativas de protección.

Es importante tener en cuenta cuáles son los puntos vulnerables, para crear una directiva de seguridad, el mejor método será realizando pruebas reales, ya sea en la red, base de datos o en equipos.

Luego de haber determinado los puntos vulnerables del sistema de información, debe trabajar en reducirlos lo mejor posible, para que no sea ni tan permisible pero tampoco de difícil acceso de tal manera que cause incomodidad a los colaboradores donde implante la metodología de seguridad.

El plan de contingencia es muy importante porque actuará inmediatamente cuando el ataque se ha perpetrado, de tal manera que jamás sea un problema el no disponer de los datos y llegue a bloquear el acceso a la información confiable.

La estrategia reactiva tiene lugar luego de que la estrategia proactiva ha fallado, es importante que la dos vayan de la mano y trabajen conjuntamente. Cuando se aplica una estrategia reactiva se debe documentar en una bitácora para posterior analizarlo y poder modificar la directiva de seguridad.

La evaluación del daño debe realizarla de forma inmediata, si por algún motivo no puede hacerlo, debe aplicar algún plan de contingencia vigente, lo importante es que no detenga la operación de la compañía y disminuir el impacto del daño.

Reparar el daño es una fase que debe realizarla rápidamente, de manera que no afecte al cotidiano desarrollo de la compañía.

Todos estos factores son de suma importancia para evaluar y poder aprender del daño cometido por la amenaza ejecutada, de esta forma podrá evaluar las directivas de seguridad y cambiar las estrategias para predecir posibles ataques.

Luego de un análisis profundo de la directiva debe valorar cuan efectiva es y si es pertinente ajústela.

Pregunta Directriz

¿Existe riesgo de que ocurran delitos informáticos causados por ingeniería social en la compañía Instrumental y Óptica?

SEÑALAMIENTO DE VARIABLES

Variable Independiente: Ingeniería Social

Variable Dependiente: Delitos Informáticos

FUNDAMENTACIÓN LEGAL

Reglamento general a la ley de comercio electrónico, firmas electrónicas y mensajes de datos.

Art. 1.- Incorporación de archivos o mensajes adjuntos.- La incorporación por remisión a que se refiere el artículo 3 de la Ley 67, incluye archivos y mensajes incorporados por remisión o como anexo en un mensaje de datos y a cuyo contenido se accede indirectamente a partir de un enlace electrónico directo incluido en el mismo mensaje de datos y que forma parte del mismo.

La aceptación que hacen las partes del contenido por remisión deberá ser expresada a través de un mensaje de datos que determine inequívocamente tal aceptación. En el caso de contenido incorporado por remisión a través de un enlace electrónico, no podrá ser dinámico ni variable y por tanto la aceptación expresa de las partes se refiere exclusivamente al contenido accesible a través del enlace electrónico al momento de recepción del mensaje de datos.

En las relaciones con consumidores, es responsabilidad del proveedor asegurar la disponibilidad de los remitidos o anexos para que sean accedidos por un medio aceptable para el consumidor cuando éste lo requiera. En las relaciones de otro tipo las partes podrán acordar la forma y accesibilidad de los anexos y remitidos.

Los anexos o remisiones referidas a garantías, derechos, obligaciones o información al consumidor deberán observar lo establecido en la Ley Orgánica de Defensa del Consumidor y su reglamento.

Toda modificación a un anexo o remitido en un mensaje de datos se comunicará al receptor del mismo, a través de un mensaje de datos o por escrito, resaltando las diferencias entre el texto original y el modificado. En el texto modificado se deberá incluir en lugar visible y claramente accesible un enlace al contenido anterior. La comunicación al consumidor acerca de modificaciones no constituye indicación de aceptación de las mismas por su parte. Dicha aceptación deberá ser expresa y remitida por cualquier medio, ya sea éste físico o electrónico.

Cuando las leyes así lo determinen, cierto tipo de información deberá estar directamente incluida en el mensaje de datos y no como anexo o remitido.

Art. 2.- Accesibilidad de la información.- Se considerará que un mensaje de datos, sus anexos y remitidos, son accesibles para consulta posterior cuando se puede recuperar su contenido en forma íntegra en cualquier momento empleando los mecanismos y procedimientos previstos para el efecto, los cuales deberán

detallarse y proporcionarse independientemente del mensaje de datos a fin de garantizar el posterior acceso al mismo.

Art. 3.- Información escrita.- Se entiende que la información contenida en un mensaje de datos es accesible para su posterior consulta cuando:

a) Ha sido generada y puede ser almacenada en un lenguaje electrónico/informático y formato entendibles por las partes involucradas en el intercambio de información y sus respectivos sistemas informáticos de procesamiento de la información, pudiéndose recuperar su contenido y el de los remitidos o anexos correspondientes en cualquier momento empleando los mecanismos previstos y reconocidos para el efecto; y,

b) Se puede recuperar o se puede acceder a la información empleando los mecanismos previstos al momento de recibirlo y almacenarlo, y que deberán detallarse y proporcionarse independientemente del mensaje de datos a fin de garantizar el posterior acceso al mismo.

Las publicaciones que las leyes exijan por escrito, sin perjuicio de lo establecido en dichas leyes, podrán adicionalmente efectuarse en medios electrónicos en forma de mensajes de datos.

Cumplidos los requisitos de accesibilidad, el mensaje de datos tiene iguales efectos jurídicos que los documentos que constan por escrito.

Art. 4.- Información original y copias certificadas.- Los mensajes de datos y los documentos desmaterializados, cuando las leyes así lo determinen y de acuerdo al caso, deberán ser certificados ante un Notario, autoridad competente o persona autorizada a través de la respectiva firma electrónica, mecanismo o procedimiento autorizado.

Los documentos desmaterializados se considerarán, para todos los efectos, copia idéntica del documento físico a partir del cual se generaron y deberán contener adicionalmente la indicación de que son desmaterializados o copia electrónica de un documento físico. Se emplearán y tendrán los mismos efectos que las copias impresas certificadas por autoridad competente.

Art. 5.- Desmaterialización.- El acuerdo expreso para desmaterializar documentos deberá constar en un documento físico o electrónico con las firmas de las partes aceptando tal desmaterialización y confirmando que el documento original y el

documento desmaterializado son idénticos. En caso que las partes lo acuerden o la ley lo exija, las partes acudirán ante Notario o autoridad competente para que certifique electrónicamente que el documento desmaterializado corresponde al documento original que se acuerda desmaterializar. Esta certificación electrónica se la realiza a través de la respectiva firma electrónica del Notario o autoridad competente.

Los documentos desmaterializados deberán señalar que se trata de la desmaterialización del documento original. Este señalamiento se constituye en la única diferencia que el documento desmaterializado tendrá con el documento original.

En el caso de documentos que contengan obligaciones, se entiende que tanto el documento original como el desmaterializado son la expresión de un mismo acuerdo de las partes intervinientes y por tanto, no existe duplicación de obligaciones. De existir multiplicidad de documentos desmaterializados y originales, con la misma información u obligación, se entenderá que se trata del mismo, salvo prueba en contrario.

La desmaterialización de los documentos de identificación personal estará sujeta a las disposiciones especiales y procedimiento que las entidades competentes determinen.

Art. 6.- Integridad de un mensaje de datos.- La consideración de integridad de un mensaje de datos, establecida en el inciso segundo del artículo 7 de la Ley 67, se cumple si dicho mensaje de datos está firmado electrónicamente. El encabezado o la información adicional en un mensaje de datos que contenga exclusivamente información técnica relativa al envío o recepción del mensaje de datos, y que no altere en forma alguna su contenido, no constituye parte sustancial de la información.

Para efectos del presente artículo, se considerará que la información consignada en un mensaje de datos es íntegra, si ésta ha permanecido completa e inalterada, salvo la adición de algún cambio que sea inherente al proceso de comunicación, archivo o presentación.

Art. 7.- Procedencia e identidad de un mensaje de datos.- La verificación de la concordancia entre el emisor del mensaje de datos y su firma electrónica se

realizará comprobando la vigencia y los datos del certificado de firma electrónica que la respalda. En otros tipos de firmas o sistemas de identificación y autenticación, esta verificación se realizará mediante la verificación de los registros acordados o requeridos.

El aviso de un posible riesgo sobre la vulnerabilidad o inseguridad de una firma, su certificado o el mensaje de datos y los anexos relacionados podrá ser realizado por el titular de los mismos, mediante cualquier tipo de advertencia que permita, de manera inequívoca a quien realiza la verificación o recibe un mensaje de datos, tomar las precauciones necesarias para evitar perjuicios y prevenir fallas de seguridad. Este aviso deberá ser realizado antes de iniciar cualquier proceso de transacción comercial negociación, o contratación electrónica.

De acuerdo a las leyes, se podrá recurrir a peritos para determinar la procedencia y otro tipo de relaciones de un mensaje de datos con quien lo remite de modo directo o indirecto.

Art. 8.- Responsabilidad por el contenido de los mensajes de datos.- La prestación de servicios electrónicos de cualquier tipo por parte de terceros, relacionados con envío y recepción de comunicaciones electrónicas, alojamiento de bases de datos, registro electrónico de datos, alojamiento de sitios en medios electrónicos o servicios similares o relacionados, no implica responsabilidad sobre el contenido de los mensajes de datos por parte de quien presta estos servicios, siendo la responsabilidad exclusivamente del propietario de la información.

De acuerdo a la ley y por orden de la autoridad competente, el órgano regulador podrá ordenar la suspensión del acceso a cualquier información en redes electrónicas que se declare ilegal y/o que atente contra las leyes o la seguridad nacionales. El proveedor de servicios electrónicos deberá cumplir con la orden de suspender el acceso al contenido en forma inmediata, y en caso de no hacerlo será sancionado con sujeción a la ley por el CONELEC.

Art. 9.- Prestación de servicios de conservación de mensajes de datos.- La conservación, incluido el almacenamiento y custodia de mensajes de datos, podrá realizarse a través de terceros, de acuerdo a lo que establece el Art. 8 de la Ley 67. Los sistemas, políticas y procedimientos que permiten realizar las funciones de conservación de mensajes de datos se denominan Registro Electrónico de Datos.

Una vez cumplidos los requisitos establecidos en las leyes, cualquier persona puede prestar servicios de Registro Electrónico de Datos que incluyen:

a. Conservación, almacenamiento y custodia de la información en formato electrónico con las debidas seguridades;

b. Preservación de la integridad de la información conservada;

c. Administración del acceso a la información y la reproducción de la misma cuando se requiera;

d. Respaldo y recuperación de información; y,

e. Otros servicios relacionados con la conservación de los mensajes de datos.

La prestación de servicios de Registro Electrónico de Datos se realizará bajo el régimen de libre competencia y contratación. Las partes que intervengan en la contratación de este tipo de servicios, podrán determinar las condiciones que regulan su relación.

La prestación del servicio de Registro Electrónico de Datos deberá observar todas las normas contempladas en la Ley 67, este reglamento y demás disposiciones legales vigentes.

En los procesos de conservación de los mensajes de datos, se debe garantizar la integridad de los mismos al menos por el mismo tiempo que las leyes y reglamentos exijan su almacenamiento.

Por orden de autoridad competente, podrá ordenarse a los proveedores de servicios de Registro Electrónico de Datos mantener en sus sistemas respaldos de los mensajes de datos que tramite por el tiempo que se considere necesario.

Art. 20.- Información al usuario.- La información sobre los programas o equipos que se requiere para acceder a registros o mensajes de datos deberá ser proporcionada mediante medios electrónicos o materiales. En el caso de uso de medios electrónicos se contará con la confirmación de recepción de la información por parte del usuario, cuando se usen medios materiales, los que formarán parte de la documentación que se le deberá entregar al usuario.

Para demostrar el acceso a la información el usuario deberá manifestar expresamente que conoce la información objeto de su consentimiento y que sus sistemas le permiten el acceso tecnológico a la misma.

Art. 21.- De la seguridad en la prestación de servicios electrónicos.- La prestación de servicios electrónicos que impliquen el envío por parte del usuario de información personal, confidencial o privada, requerirá el empleo de sistemas seguros en todas las etapas del proceso de prestación de dicho servicio. Es obligación de quien presta los servicios, informar en detalle a los usuarios sobre el tipo de seguridad que utiliza, sus alcances y limitaciones, así como sobre los requisitos de seguridad exigidos legalmente y si el sistema puesto a disposición del usuario cumple con los mismos. En caso de no contar con seguridades se deberá informar a los usuarios de este hecho en forma clara y anticipada previo el acceso a los sistemas o a la información e instruir claramente sobre los posibles riesgos en que puede incurrir por la falta de dichas seguridades.

Se consideran datos sensibles del consumidor sus datos personales, información financiera de cualquier tipo como números de tarjetas de crédito, o similares que involucren transferencias de dinero o datos a través de los cuales puedan cometerse fraudes o ilícitos que le afecten.

Por el incumplimiento de las disposiciones contenidas en el presente artículo o por falta de veracidad o exactitud en la información sobre seguridades, certificaciones o mecanismos para garantizar la confiabilidad de las transacciones o intercambio de datos ofrecida al consumidor o usuario, el organismo de control podrá exigir al proveedor de los servicios electrónicos la rectificación necesaria y en caso de reiterarse el incumplimiento o la publicación de información falsa o inexacta, podrá ordenar la suspensión del acceso al sitio con la dirección electrónica del proveedor de servicios electrónicos mientras se mantengan dichas condiciones.

Art. 22.- Envío de mensajes de datos no solicitados.- El envío periódico de información, publicidad o noticias promocionando productos o servicios de cualquier tipo observará las siguientes disposiciones:

a. Todo mensaje de datos periódico deberá incluir mecanismos de suscripción y de suscripción (SIC);

b. Se deberá incluir una nota indicando el derecho del receptor a solicitar se le deje de enviar información no solicitada;

c. Deberá contener información clara del remitente que permita determinar inequívocamente el origen del mensaje de datos;

d. A solicitud del destinatario se deberá eliminar toda información que de él se tenga en bases de datos o en cualquier otra fuente de información empleada para el envío de mensajes de datos periódicos u otros fines no expresamente autorizados por el titular de los datos; y,

e. Inmediatamente de recibido por cualquier medio la solicitud del destinatario para suscribirse del servicio o expresando su deseo de no continuar recibiendo mensajes de datos periódicos, el emisor deberá cesar el envío de los mismos a la dirección electrónica correspondiente.

Las solicitudes de no envío de mensajes de datos periódicos, se harán directamente por parte del titular de la dirección electrónica de destino.

Los proveedores de servicios electrónicos o comunicaciones electrónicas, a solicitud de cualquiera de sus titulares de una dirección electrónica afectado por el envío periódico de mensajes de datos no solicitados, procederán a notificar al remitente de dichos correos sobre el requerimiento del cese de dichos envíos y de comprobarse que el remitente persiste en enviar mensajes de datos periódicos no solicitados podrá bloquear el acceso del remitente a la dirección electrónica afectada (SRI, 2002).

Código orgánico integral penal (COIP)

Artículo 212.- Suplantación de identidad.- La persona que de cualquier forma suplante la identidad de otra para obtener un beneficio para sí o para un tercero, en perjuicio de una persona, será sancionada con pena privativa de libertad de uno a tres años (Asamblea Nacional del Ecuador, 2014).

CAPÍTULO III

METODOLOGÍA

ENFOQUE

La presente investigación, se basó en el enfoque crítico-propositivo. Crítico porque cuestiona los esquemas planteados para realizar una investigación lógica instrumental y propositivo porque plantea alternativas de solución en un ambiente proactivo, además se obtiene información de la fuente con todos los actores y se le aplica a un examen estadístico, que determinará el fenómeno causa efecto respaldándola con teoría en el capítulo II (Naranjo, 2010, pág. 18). La metodología es cuantitativa.

MODALIDAD DE INVESTIGACIÓN

De Campo

La investigación fue realizada donde se produce el problema, en la compañía Instrumental y Óptica, para tomar contacto directo con la realidad, de lo que ocurre con las amenazas de ingeniería social y su posible repercusión en delitos informáticos.

Bibliográfico – Documental

Fue importante analizar los resultados de la investigación, para ello se indagó información primordial del marco teórico y libros obtenidos en el internet.

Quasi-Experimental.

Para dar un mayor alcance a la investigación fue necesario, aplicar ciertas variantes que incidan directamente en las variables, por tanto se utilizó también la modalidad de investigación quasi-experimental que permite preparar las

condiciones para que ello suceda. Como lo afirma (Naranjo, 2010) “Investigación quasi-experimental es el estudio en que se manipulan ciertas variables independientes para observar los efectos en las respectivas variables dependientes, con el propósito de precisar la relación causa-efecto.”

TÉCNICAS DE INVESTIGACIÓN

La técnica usada para la investigación fue una encuesta aplicada a colaboradores de la compañía, clientes y proveedores, con preguntas objetivas, que facilitaron recoger la información de las variables objeto de la investigación.

Exploratoria

Se indagó varios escenarios para efectuar la investigación con varios enfoques.

Descriptiva

Basándose en el capítulo II se usó la estadística descriptiva para

Se utilizó la estadística descriptiva para estudiar los datos arrojados por la encuesta e interpretar los resultados.

POBLACIÓN Y MUESTRA

Población

La población para la presente investigación está conformada por 15 colaboradores de la compañía, quienes inciden directamente en los resultados de la misma, aproximadamente 390 clientes activos y 19 proveedores.

Muestra

En base del tipo y número poblacional se ha decidido hacer un muestreo intencional o de conveniencia, el cual permite al investigador seleccionar directa e intencionalmente los individuos de la población.

“En el muestreo intencional todos los elementos muestrales de la población serán seleccionados bajo estricto juicio personal del investigador. En este tipo de muestreo el investigador tiene previo conocimiento de los elementos poblacionales.” (Naghi, 2005, pág. 189)

Las unidades de observación que pueden determinar resultados para la presente investigación son: los colaboradores, clientes y proveedores. De estos grupos de observación los colaboradores son los que mejor información pueden proporcionar a este proyecto investigativo, ya que son los que directamente se relacionan con la información que se procesa; por tal razón se encuestarán al 100% de los colaboradores.

En menos influencia sobre lo que ocurre en la empresa están los clientes y proveedores, por tal razón y en vista del número de los mismos se ha decidido aplicar las encuestas al 50% de estos grupos de información; seleccionando los clientes y proveedores que mayor movimiento tienen con la compañía. Esta información se resume en la siguiente tabla.

Tabla 4 - Distribución de las unidades de observación

Unidades de observación	**No.**	**%**
Colaboradores	15	7,04%
Clientes	188	88,27%
Proveedores	10	4,69%
TOTAL	**213**	**100%**

Elaborado por: Joffre Germán Díaz Cobos

OPERACIONALIZACIÓN DE VARIABLES

Tabla 5 - Variable Independiente: Ingeniería social.

CONCEPTUALIZACIÓN	DIMENSIÓN	INDICADOR	ITEMS	TÉCNICAS E INSTRUMENTOS.
Es una metodología de investigación, de influencias y acciones clandestinas que tiene por objeto comprometer un sistema de información explotando principalmente sus fallos humanos. (Acissi, 2015, pág. 77)	Acciones clandestinas	• Suplantación identidad • Políticas seguridad • Acceso ilegal	¿El personal de la empresa es susceptible a suplantación de identidad? ¿Existen políticas de seguridad para enfrentar acciones de ingreso no autorizado?	Encuesta al personal de la empresa
	Sistema de información	• Tipos de sistemas • Seguridad de acceso • Usuarios	¿Los sistemas de información manejan un nivel jerárquico de usuarios y seguridad de acceso al mismo?	Encuesta al personal de la empresa
	Fallos humanos	• Conocimiento de seguridad informática • Manejo de la información	¿Cuánto conoce el personal sobre seguridad informática? ¿El manejo de la información es el adecuado para enfrentar el comprometimiento de la información?	Encuesta al personal de la empresa

Elaborado por: Joffre Germán Díaz Cobos

Tabla 6 - Variable Dependiente: Delitos informáticos

CONCEPTUALIZACIÓN	DIMENSIÓN	INDICADOR	ITEMS	TÉCNICAS E INSTRUMENTOS.
La realización de una acción que, reuniendo las características que delimitan el concepto de delito, se ha llevado a cabo utilizando un elemento informático, contra los derechos y libertades de los ciudadanos. (Velásquez, 2007, pág. 283)	Delito	• Acto ilegal • Sanciones • Penalidades	¿Conoce de qué manera se produce un delito informático?	Encuesta dirigida al personal de la empresa
	Elemento informático	• Hardware • Software • Redes	¿Cuáles son los elementos informáticos por los cuáles se puede llevar a cabo un delito informático?	Encuesta dirigida al personal de la empresa
	Derechos ciudadanos	• Libre ejercicio de comunicación • Protección de la información	¿Cuáles son los derechos de los ciudadanos frente al manejo de información?	Encuesta dirigida al personal de la empresa

Elaborado por: Joffre Germán Díaz Cobos

Tabla 7 - Plan para la recolección de la información

PREGUNTAS BÁSICAS	EXPLICACIÓN
1. ¿Para qué?	Para obtener la información que nos permita cumplir con los objetivos de esta investigación.
2. ¿A quién?	A todas las personas que trabajan en la compañía Instrumental y Óptica, los cuales serán beneficiados directamente de esta investigación.
3. ¿Sobre qué asunto?	Sobre la ingeniería social y los delitos informáticos.
4. ¿Quién?	Joffre Germán Díaz Cobos
5. ¿Cuándo?	Durante el año 2015
6. ¿Dónde?	En la provincia de Pichincha, cantón Quito.

Elaborado por: Joffre Germán Díaz Cobos

Plan para el Procesamiento de la Información

- Se usó la encuesta de google drive exportando estos datos a una tabla de Excel.

Análisis e Interpretación de Resultados

- Elaboración de tablas y gráficos estadísticos resumidos
- Interpretación de datos obtenidos.
- Analizar los resultados arrojados en las encuestas con las interrogantes.

CAPÍTULO IV

ANÁLISIS E INTERPRETACIÓN DE RESULTADOS

Pregunta No 1 ¿Qué tipo de antivirus tiene la computadora en la que Usted trabaja?

Tabla 8 - Tipos de antivirus que usa.

Antivirus de licencia Pagada	66	30,99%
Antivirus descargado del internet (Gratuito)	109	51,17%
No tiene	17	7,98%
No conozco	21	9,86%
TOTAL	**213**	**100%**

Fuente: Encuesta.

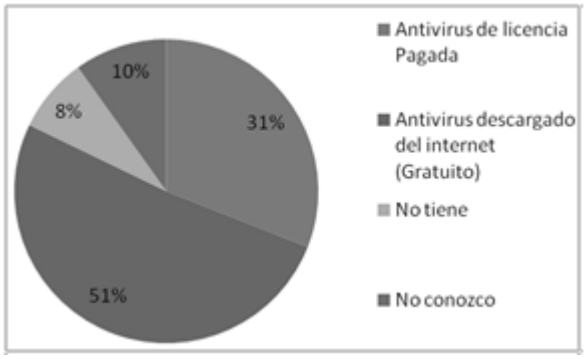


Gráfico 9- Tipos de antivirus que usa.
Elaborado por: Joffre Germán Díaz Cobos

Interpretación.

El 31% de los encuestados contestaron que el antivirus con el que trabajan tiene una licencia pagada, un 8% que no conoce, 51% indica que es descargado del internet o gratuito y un 10% no conoce. Si existe una protección en los equipos instalados, pero la décima parte de los encuestados indican que no conocen.

Pregunta Nro. 2.- ¿Con qué periodicidad se realiza mantenimiento en las computadoras de la empresa donde usted trabaja?

Tabla 9 - Periodicidad del mantenimiento.

Una vez al año	95	44,60%
Dos veces al año	49	23,00%
Tres veces al año	40	18,78%
Nunca	29	13,62%
TOTAL	**213**	**100%**

Fuente: Encuesta.

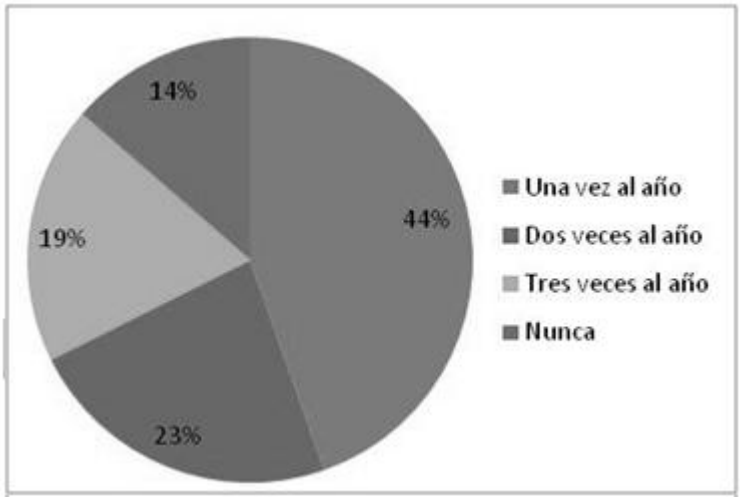


Gráfico 10- Periodicidad del mantenimiento.
Elaborado por: Joffre Germán Díaz Cobos

Interpretación.

Un 44% de los encuestados respondieron que los mantenimientos en las computadoras de la compañía se realizan una vez al año, 19% tres veces al año y 14% indica que nunca se realiza. Los datos recogidos son preocupantes porque podemos concluir que esos equipos, solo van a pasar con daños y el problema es que eso afecta a la economía de la compañía, además que la perdida de información es bastante posible, al llegar a quemarse el disco duro por algún sobre calentamiento de la fuente.

Pregunta Nro. 3.- ¿Usted descarga en la computadora de su trabajo, música, películas o programas?

Tabla 10 - Descarga de música, películas o programas.

Nunca	62	29,11%
A veces	107	50,23%
Usualmente	44	20,66%
TOTAL	**213**	**100%**

Fuente: Encuesta realizada.

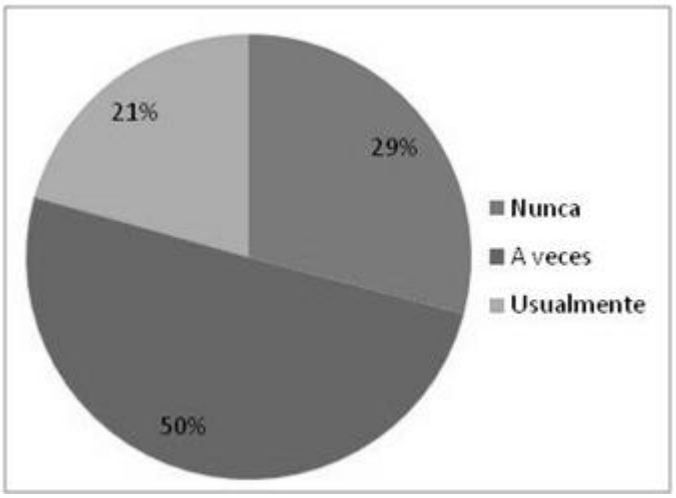


Gráfico 11- Descarga de música, películas o programas.
Elaborado por: Joffre Germán Díaz Cobos

Interpretación.

El 29% de los encuestados ha contestado que nunca han descargado en la computadora de la compañía música, películas o programas, 50% a veces y 21% usualmente. Realizando una sumatoria de estos dos valores nos deja observar que más de la mitad de los encuestados ocupa la banda de internet para asuntos que no tienen carácter laboral, ocasionando que el internet se vuelva lento y poco eficiente para las personas que si lo ocupan para investigar o desarrollar su trabajo habitual. Esto se puede convertir en un grave problema porque por lo general al bajar software, música y películas suelen descargarse malwares, que puede bajar el rendimiento de la computadora y poner en riesgo la información de su diario trabajo.

Pregunta Nro. 4.- ¿Con qué frecuencia le han solicitado a usted o algún colaborador la clave de la red inalámbrica, por parte de personas que visitan la empresa donde usted trabaja?

Tabla 11 - Solicitud clave inalámbrica por visitantes a la empresa.

Nunca	79	37,09%
De vez en cuando	75	35,21%
A menudo	40	18,78%
Siempre	19	8,92%
TOTAL	**213**	**100%**

Fuente: Encuesta.

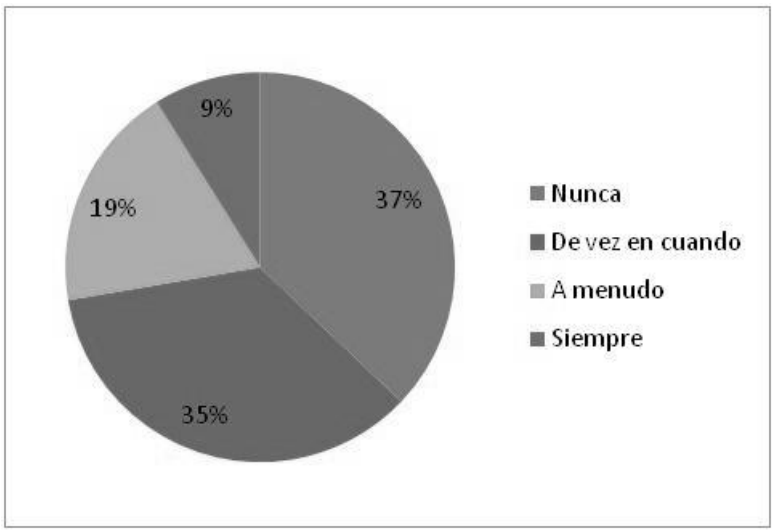


Gráfico 12- Solicitud de clave inalámbrica por visitantes a la empresa.
Elaborado por: Joffre Germán Díaz Cobos

Interpretación.

El 37% de los encuestados han contestado que nunca les han pedido la clave de la red inalámbrica, pero al contrastar con los encuestados que contestaron de vez en cuando, a menudo y siempre el porcentaje es 63% muy por encima del porcentaje de personas que contestaron que nunca les ha solicitado la clave. Es evidente que si la red inalámbrica pertenece a la misma red de trabajo de sus oficinas, la información puede estar expuesta a intrusos que puede usurpar datos sensibles para la compañía.

Pregunta Nro. 5.- ¿La computadora que usa en su trabajo, tiene protección contra la pérdida de información en el caso de fallos de energía (UPS)?

Tabla 12 - Uso de UPS en la computadora.

Si	84	39,44%
No	75	35,21%
No se	54	25,35%
TOTAL	**213**	**100%**

Fuente: Encuesta.

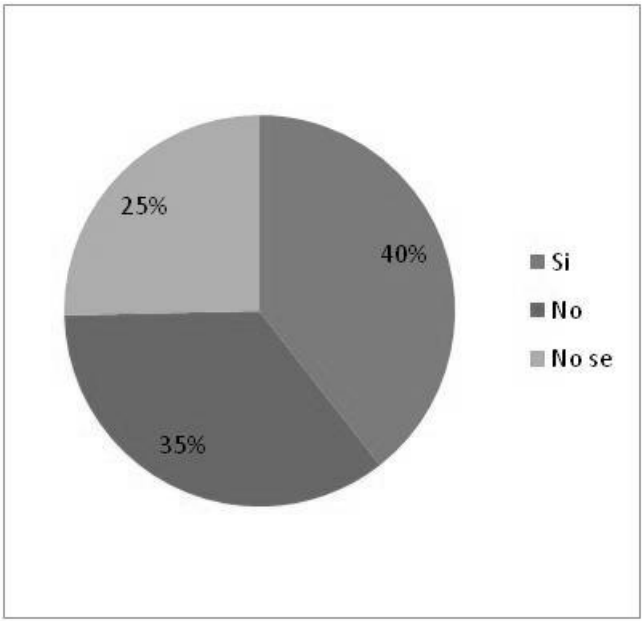


Gráfico 13- Uso de UPS en la computadora.
Elaborado por: Joffre Germán Díaz Cobos

Interpretación.

Un 40% de encuestados han contestado, que si tienen, un equipo que provee de energía continua, el 35% que no tienen y un 25% no sabe. La gran parte de empresas pierden sus datos o dañan motores de bases de datos por incumplir con esta normativa que debería ser general para todas las compañías, si bien es cierto no va a permitirles seguir trabajando por mucho tiempo por lo menos, va a permitirles que guarden los documentos en los que estaba trabajando, salir del sistema y apagar de una forma correcta y no abrupta.

Pregunta Nro. 6.- ¿El trabajo que usted realiza, requiere de conexión a internet?

Tabla 13 - Uso de internet en el trabajo.

Nunca	2	0,94%
De vez en cuando	51	23,94%
Siempre	160	75,12%
TOTAL	**213**	**100%**

Fuente: Encuesta.

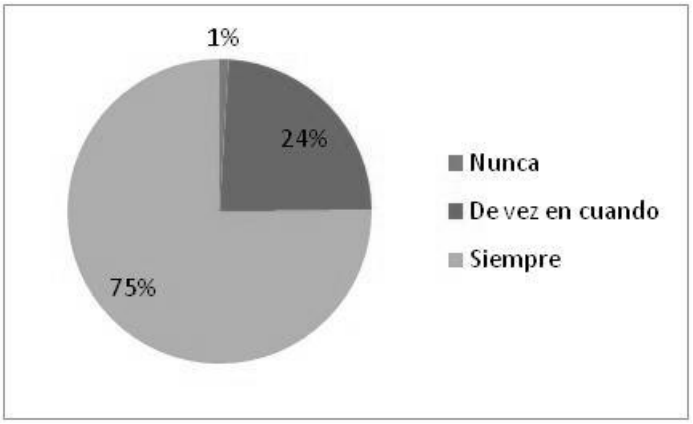


Gráfico 14- Tipo Uso de internet en el trabajo.
Elaborado por: Joffre Germán Díaz Cobos

Interpretación.

El 75% de los encuestados manifiesta que el trabajo que realizan requiere internet. Lo que nos muestra que lo equipos debe estar protegidos con software (antivirus) y hardware (firewall). Queda en total evidencia que la gran mayoría usa constantemente o regularmente internet porque solo un 1% de los encuestados ha indicado que nunca necesitan internet, es importante tomar juicios de protección.

Pregunta Nro. 7.- ¿De qué manera respalda la información que usted maneja en la empresa donde usted trabaja?

Tabla 14 – Manera de respaldar la información.

CD, DVD, Flash memory.	77	36,15%
En la misma computadora.	57	26,76%
En la nube.	25	11,74%
Personal técnico se encarga de respaldar la información.	37	17,37%
No se respalda.	17	7,98%
TOTAL	**213**	**100%**

Fuente: Encuesta.

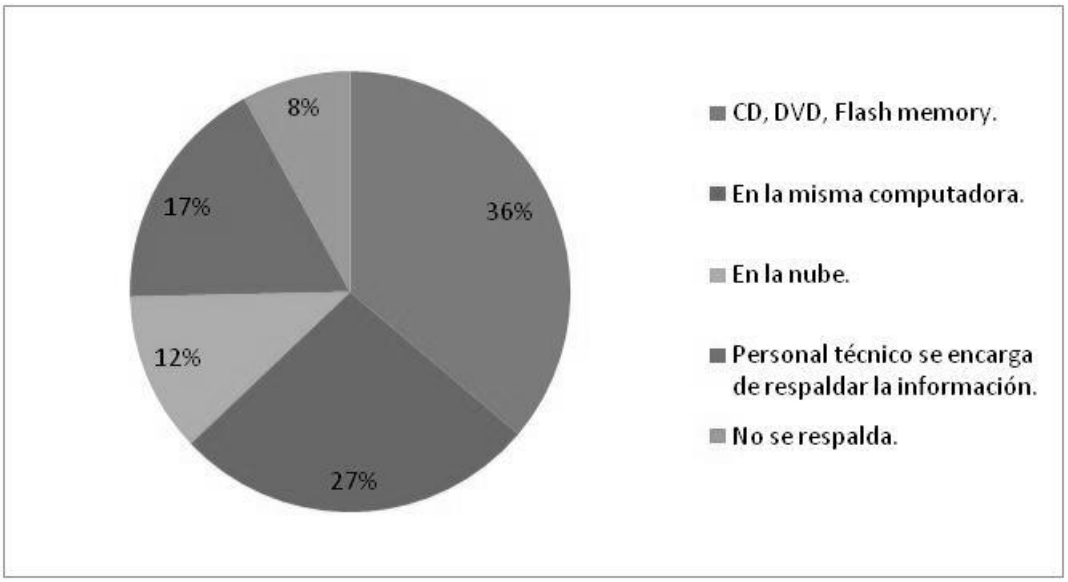


Gráfico 15- Manera de respaldar la información.
Elaborado por: Joffre Germán Díaz Cobos

Interpretación.

El 36% de los encuestados ha contestado que respaldan la información en CD, DVD, flash memory, un 27% en la misma computadora, 12% en la nube, el 17% personal técnico y un 8% no respalda. Solo un 12% toma muy enserio su información guardándola en la nube, pero hay dos respuestas que suman 35%, más de la cuarta parte de la encuesta y este resultado obtenido es alarmante, porque están asegurando que el respaldo se realiza en la misma computadora y otro gran grupo dice que no se respalda, con lo cual podemos concluir que no se cuenta con respaldo de la información.

Pregunta Nro. 8.- ¿Tiene conocimiento acerca del uso de la firma electrónica en el Ecuador?

Tabla 15 - Conocimiento de la firma electrónica en el Ecuador.

No conozco	133	62,44%
Poco conocimiento	63	29,58%
Si conozco completamente.	17	7,98%
TOTAL	**213**	**100%**

Fuente: Encuesta.

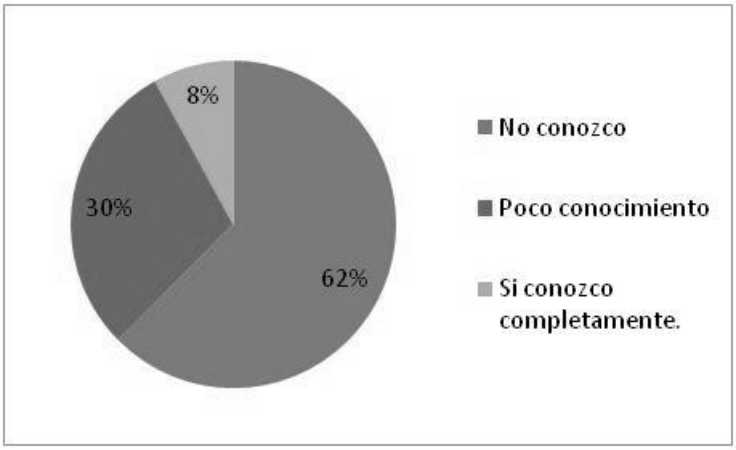


Gráfico 16- Conocimiento de la firma electrónica en el Ecuador.
Elaborado por: Joffre Germán Díaz Cobos

Interpretación.

Más de la mitad de encuestados ha contestado que no tiene conocimiento acerca de la firma electrónica, un 30% tiene poco conocimiento pero un 8% no conoce. El comercio digital hoy en día es tan variado e importante que casi cualquier pago se logra hacer a través del internet, lo cual si no se tiene un entero conocimiento, las personas pueden ser presa de la delincuencia informática.

Pregunta Nro. 9.- ¿Ingresa dispositivos de almacenamiento masivo (flash memory, discos duros externos o memorias SD), en la computadora que usted usa en la empresa, proveniente de personas externas a esta?

Tabla 16 - Uso de dispositivos de almacenamiento masivo que provienen de personal externo.

Nunca	58	27,23%
De vez en cuando	110	51,64%
Siempre	45	21,13%
TOTAL	**213**	**100%**

Fuente: Encuesta.

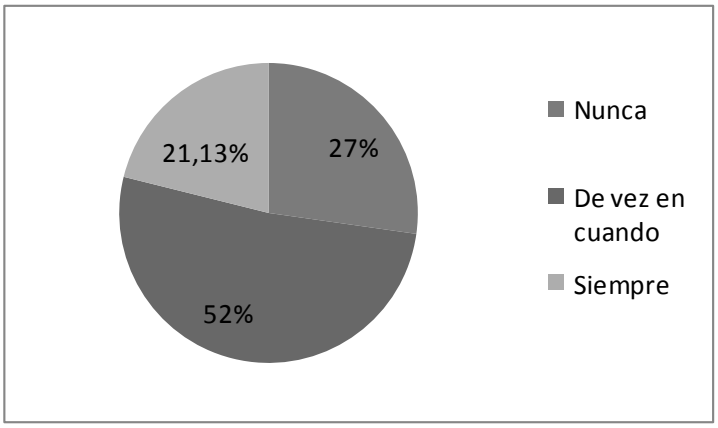


Gráfico 17- Uso de dispositivos de almacenamiento masivo que provienen de personal externo.
Elaborado por: Joffre Germán Díaz Cobos

Interpretación.

Un 27% de los encuestados indica que nunca ingresa dispositivos de almacenamiento, masivo, 52% de vez en cuando y 22% indica que siempre. El riesgo es alto, al hablar que alrededor del 70% la usa de vez en cuando y siempre, puesto que estos dispositivos son los más contaminados con malwares y podrían dañar la información o enviar información sensible a personal fuera de la empresa y poner en riesgo la estabilidad del equipo como la de la compañía.

Pregunta Nro. 10.- ¿Cuándo tiene qué generar una contraseña que usa?

Tabla 17 - Generación de contraseñas.

La misma para varias cosas	73	34,27%
Sus nombres o apellidos o de sus hijos o número de cédula	11	5,16%
Fechas importantes	15	7,04%
Una contraseña segura que nadie podría acertar con ella	114	53,52%
TOTAL	**213**	**100%**

Fuente: Encuesta.

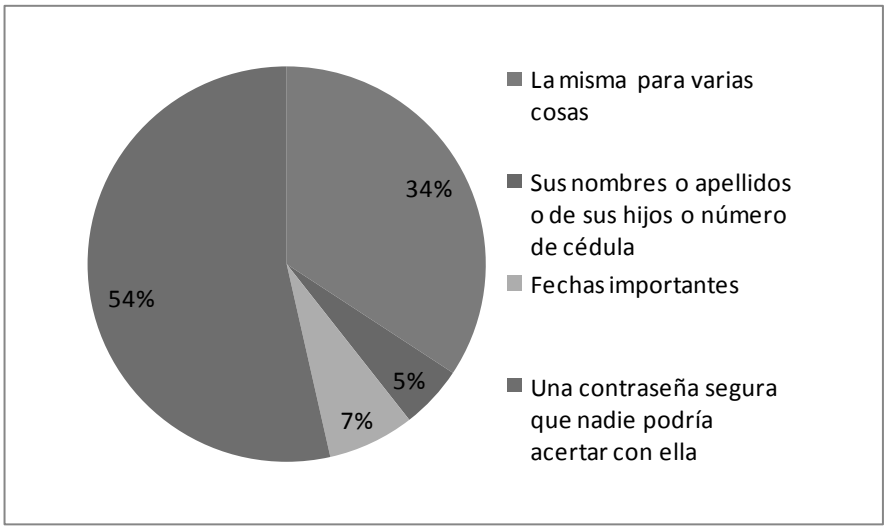


Gráfico 18- Generación de contraseñas.
Elaborado por: Joffre Germán Díaz Cobos

Interpretación.

Más de la mitad de encuestados, usan la misma contraseña para varias cosas, solo el 5% usa sus nombres o apellidos o de sus hijos o número de cédula, un 7% usa fechas importantes y más de la mitad de los encuestados usa contraseña segura que nadie podría acertar con ella. Es evidente que no es para nada seguro que usemos la misma contraseña, puesto que si algún hacker, logra adivinarla podríamos estar en serios problemas al tener expuestos nuestros datos. Si somos personas en la compañía que usamos datos delicados como banca electrónica, por ningún motivo debería ser nuestra contraseña igual a las otras.

Pregunta Nro. 11.- ¿Con que frecuencia se cambia la contraseña de la computadora que usa en su oficina?

Tabla 18 - Frecuencia de cambio de contraseñas.

No tiene clave	62	29,11%
Nunca se cambia	73	34,27%
Frecuentemente	78	36,62%
TOTAL	**213**	**100%**

Fuente: Encuesta.

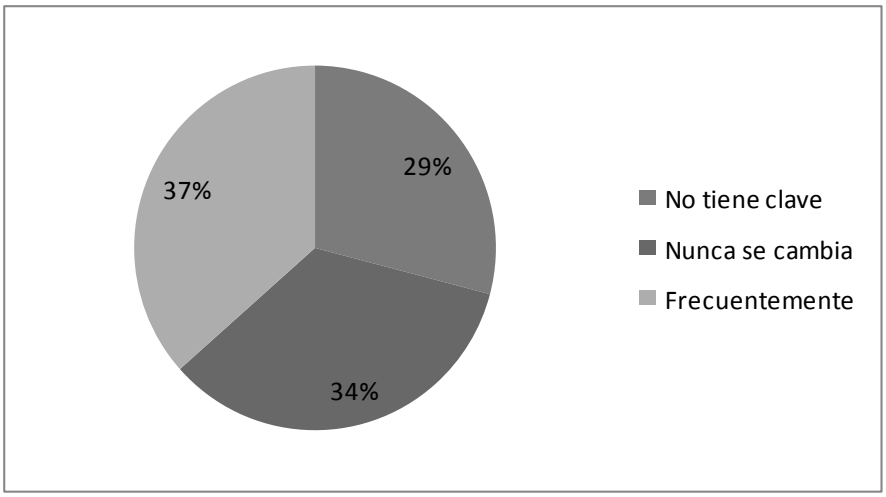


Gráfico 19- Frecuencia de cambio de contraseñas.
Elaborado por: Joffre Germán Díaz Cobos

Interpretación.

El 29% de los encuestados indican que la computadora que usan en la compañía no tiene clave, el 34% nunca cambia y un 37% cambia frecuentemente. Interpretando los datos obtenidos en la encuesta, claramente se observa que casi las tercera parte nunca cambia la contraseña, este caso conlleva a tener varios problemas de seguridad puesto que los datos son más propensos a ser expuestos. Cuando tenemos información muy delicada en nuestros computadores es importante que nuestra contraseña sea segura. Si la contraseña es segura, es alfanumérica, mayúsculas, minúsculas, números y caracteres especiales; la persona interesada puede en un tiempo prolongado obtenerla pero será bastante complicada dar con ella.

Pregunta Nro. 12.- En la actualidad, en internet abundan correos de dudosa procedencia solicitando información personal, bancaria o que se oriente a una posible estafa. ¿Con que frecuencia usted o alguien cercano ha recibido, solicitudes de este tipo?

Tabla 19 - Frecuencia de recepción de correos de dudosa procedencia.

Nunca	65	30,52%
De vez en cuando	114	53,52%
Siempre	34	15,96%
TOTAL	**213**	**100%**

Fuente: Encuesta.

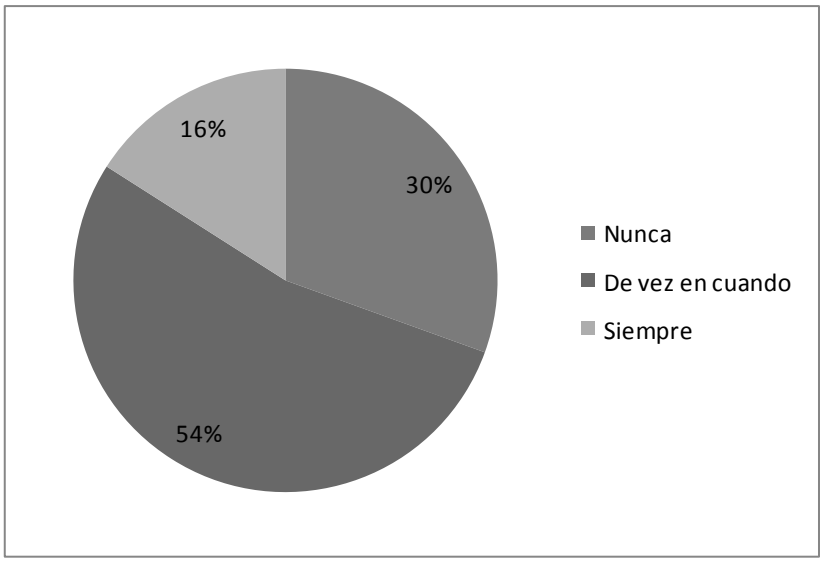


Gráfico 20- Frecuencia de recepción de correos de dudosa procedencia.
Elaborado por: Joffre Germán Díaz Cobos

Interpretación.

El 30% nunca ha recibido correo no deseado o de dudosa procedencia, un 54% de vez en cuando y un 16% siempre recibe este tipo de correos. En nuestra sociedad es casi normal recibir correos de dudosa procedencia, los porcentajes presentados por los encuestados, son verdaderamente alarmantes porque más de la mitad son equipos expuestos de vez en cuando y siempre. Si las personas no tienen una buena cultura informática, diferenciando que es un correo no deseado de un correo publicitario, podrían caer fácilmente en alguna estafa.

Pregunta Nro. 13.- ¿Tiene conocimiento si las leyes del Ecuador sancionan los delitos informáticos?

Tabla 20 - Conocimiento de leyes que sancionan delitos informáticos en el Ecuador.

Si	77	36,15%
No	76	35,68%
No se	60	28,17%
TOTAL	**213**	**100%**

Fuente: Encuesta.

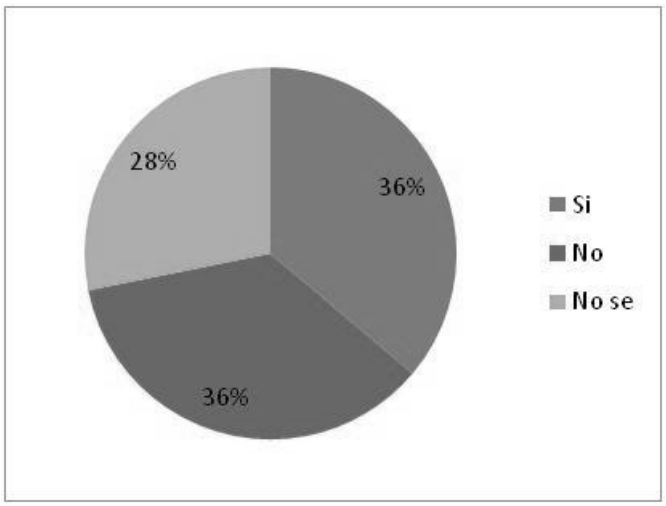


Gráfico 21- Conocimiento de leyes que sancionan delitos informáticos en el Ecuador.
Elaborado por: Joffre Germán Díaz Cobos

Interpretación.

El 36% de los encuestados conoce sobre las leyes del Ecuador sancionan los delitos informáticos, pero un 36% no conoce y un 28% duda sobre si conoce. Aquí se refleja algo importante al sumar los porcentajes de los encuestados que dudan de conocer y los que no conocen la ley que sanciona los delitos informáticos en Ecuador, más de la mitad de encuestados 72%, una cantidad bastante notable y considerable, la problemática incide en que si no se conoce la ley, no la podemos aplicar ni defendernos al ser víctimas y el desconocimiento de la ley no exime a nadie sobre su sanción.

Pregunta Nro. 14.- ¿Con qué frecuencia usa la banca electrónica?

Tabla 21 - Frecuencia de uso de la banca electrónica

No uso banca electrónica	98	46,01%
Una vez al mes	54	25,35%
Una vez por semana	38	17,84%
A diario	23	10,80%
TOTAL	**213**	**100%**

Fuente: Encuesta.

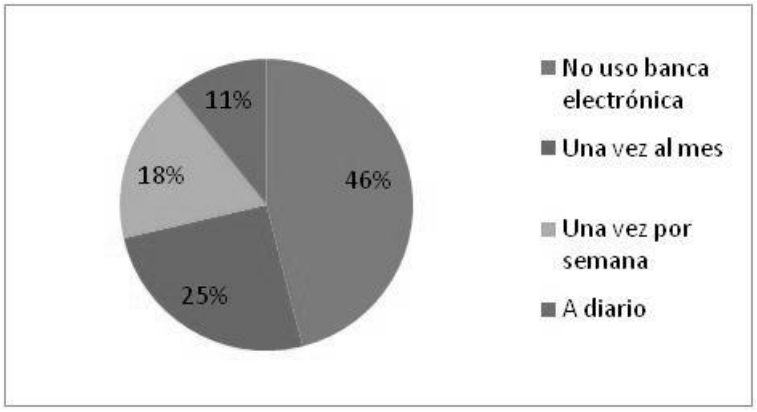


Gráfico 22- Frecuencia de uso de la banca electrónica
Elaborado por: Joffre Germán Díaz Cobos

Interpretación.

Los encuestado ha contestado que un 46% no usa banca electrónica, 25% una vez por mes, 18% una vez por semana y un 11% a diario, claramente deberíamos realizar un enfoque sobre los encuestados que usan una vez al mes, una vez por semana y a diario ellos son el 54% de los encuestados, razón por la cual hay una alta incidencia de ser atacados y por ende engañados. Las estafas bancarias son las más frecuentadas hoy en día por personas que delinquen de esta manera, no hay que ser ingeniero para poder usar técnicas que faciliten el delito, el hecho de estar revisando la banca electrónica denota primeramente que tenemos una cuenta bancaria y si es frecuentemente, nos dice que las transacciones también son frecuentes.

Pregunta Nro. 15.- ¿Conoce mecanismos de seguridad para manejo de banca electrónica?

Tabla 22 - Conocimiento de mecanismos de seguridad con la banca electrónica

No conozco	104	48,83%
Poco conocimiento	76	35,68%
Si, conozco completamente	33	15,49%
TOTAL	**213**	**100%**

Fuente: Encuesta.

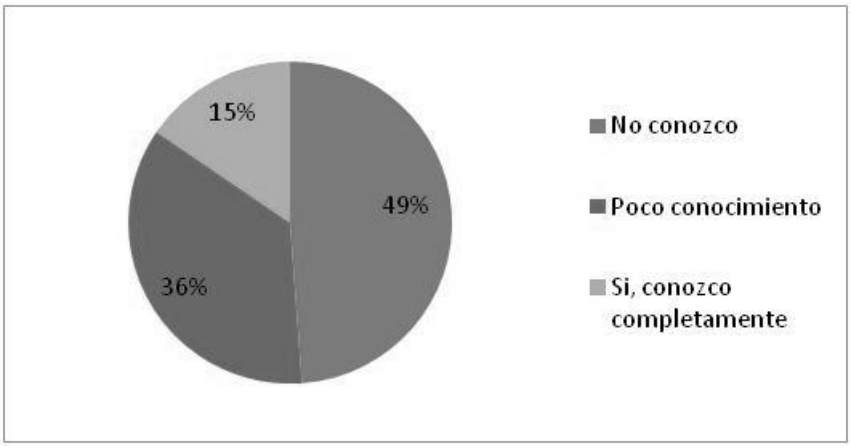


Gráfico 23- Conocimiento de mecanismos de seguridad con la banca electrónica
Elaborado por: Joffre Germán Díaz Cobos

Interpretación.

Un 49% no conoce mecanismos de seguridad para el manejo de la banca electrónica, un 36% tiene poco conocimiento y solo un 15% conoce completamente estos mecanismos de seguridad, lo que indica que muy pocos encuestados no se encontrarían expuestos a ser estafados, pero un 85% entre los que no conocen y los que algo conocen, lo que refleja que un alto porcentaje de encuestados no lo usan o son presa fácil para los delincuentes de cuello blanco, hay que tomar en cuenta que un alto porcentaje de personas tiene una cuenta bancaria donde son depositados sus salarios o mantiene los ahorros de toda su vida, lo cual se convierte en un negocio muy rentable para los que se dedican a delinquir.

Pregunta Nro. 16.- ¿En alguna ocasión le han clonado a usted la tarjeta de débito o crédito?

Tabla 23 - Clonación de tarjetas de débito y crédito.

No tengo tarjetas	62	29,11%
Nunca	135	63,38%
Si	16	7,51%
TOTAL	**213**	**100%**

Fuente: Encuesta.

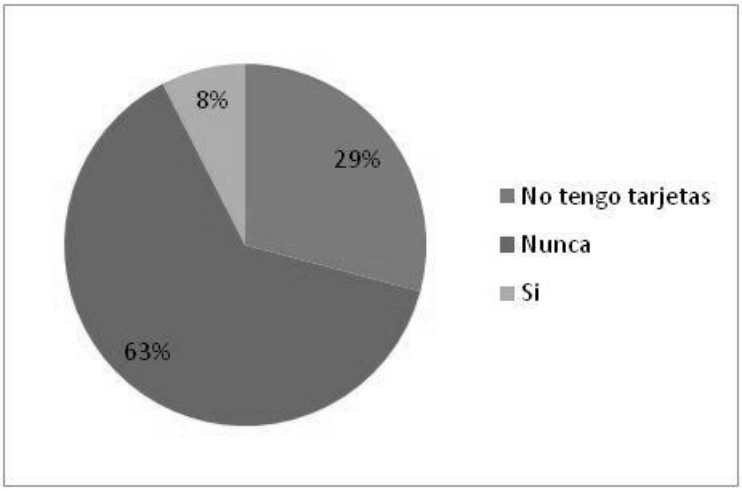


Gráfico 24- Clonación de tarjetas de débito y crédito.
Elaborado por: Joffre Germán Díaz Cobos

Interpretación.

El 63% de encuestados nunca le han clonado la tarjeta de débito o crédito, un 29% no tiene y un 8% si le han clonado. El negocio de la banca tuvo que ver algunas alternativas para no quedarse sin clientes que consumían con tarjeta, y una de ellas fue el incorporar un chip inteligente de seguridad, que no permite la clonación, tanto como lo facilitaba la banda magnética. Interpretando las respuestas es más que seguro que ese 7% que si le clonaron la tarjeta solo tenía banda magnética.

Pregunta Nro. 17.- En la definición de contraseñas para el acceso a la banca electrónica u otros sitios que son de riesgo frente amenazas de delitos informáticos, como las conforma:

Tabla 24 - Definición de contraseñas.

Con 6 o menos caracteres	21	9,86%
Con más de 6 caracteres	35	16,43%
Está compuesta solamente por números	17	7,98%
Está compuesta solamente por letras	4	1,88%
Combinación de números y letras	72	33,80%
Combinación de números y letras añadiendo caracteres especiales como + - * ? u otros	64	30,05%
TOTAL	**213**	**100%**

Fuente: Encuesta.

Gráfico 25- Definición de contraseñas.
Elaborado por: Joffre Germán Díaz Cobos

Interpretación.

Un 10% de los encuestados usan contraseñas de menos de 6 caracteres, el 16% con más de 6 caracteres, 8% está compuesta solo por números, 2% de los encuestados ha indicado que está compuesta solo por letras, un 34% entre números y letras y un 30% combina números, letras y caracteres especiales. Podemos observar que un gran porcentaje de los encuestados maneja contraseñas seguras al momento de ingresar a la banca electrónica, pero la explicación es muy sencilla, los bancos de alto prestigio así lo exigen, pero personas que tienen manejan dinero en cooperativas las exigencias no son muy altas, ellos son foco para software que escanea contraseñas para poder adivinar mediante algoritmos.

Pregunta Nro. 18.- ¿Qué tipo de precaución tiene cuando usa una tarjeta de débito o crédito?

Tabla 25 - Precauciones al usar tarjetas de débito o crédito.

No tengo tarjetas	75	35,21%
No pierdo de vista a la persona que entrego la tarjeta	48	22,54%
Compro en lugares seguros	90	42,25%
TOTAL	**213**	**100%**

Fuente: Encuesta.

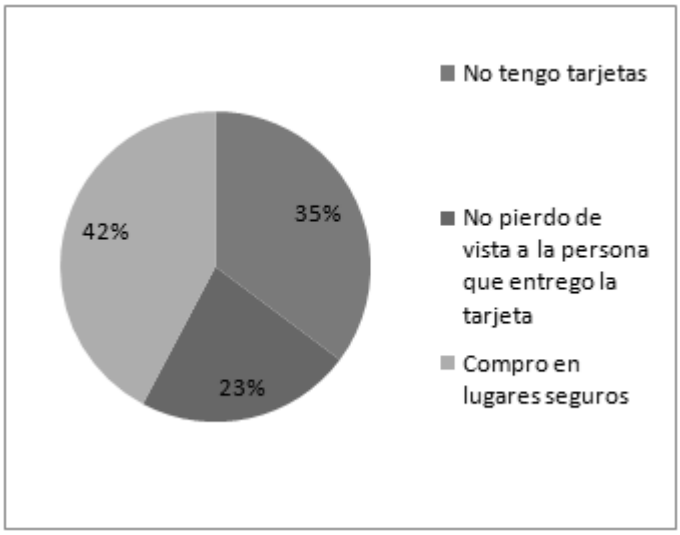


Gráfico 26- Precauciones al usar tarjetas de débito o crédito.
Elaborado por: Joffre Germán Díaz Cobos

Interpretación.

El 35% de los encuestados no manejan tarjetas de crédito, 23 de estos no pierden de vista a la persona que entregó la tarjeta y un 42% compra en lugares seguros. Es evidente que más de la mitad de encuestados tiene una buena cultura de manejo seguro de su tarjeta de débito o crédito. El no perder de vista a la persona que le entrega la tarjeta es de suma importancia, porque ayuda a que este individuo no trate de hacer transacción ilegales o anote los número de seguridad de la tarjeta que se encuentran en la parte posterior de esta, o pueda imprimir la tarjeta en un boucher manual.

Pregunta Nro. 19.- ¿Conoce que significan phishing, hacker, cracker?

Tabla 26 - Conocimiento de phishing, hacker, cracker.

No conozco	50	23,47%
Poco conocimiento	108	50,70%
Si, conozco completamente	55	25,82%
TOTAL	**213**	**100%**

Fuente: Encuesta.

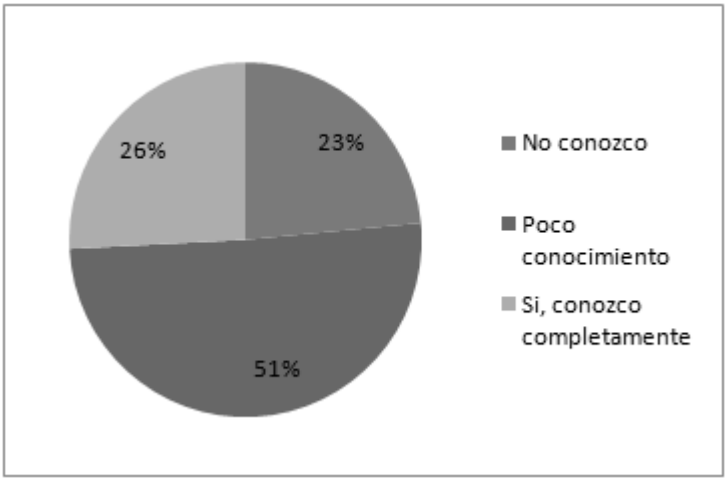


Gráfico 27- Tipo Conocimiento de phishing, hacker, cracker.
Elaborado por: Joffre Germán Díaz Cobos

Interpretación.

El 23% de encuestados indica que no tiene conocimiento del significado de phishing, hacker, cracker, casi la mitad de los encuestados conoce algo sobre su significado, y el 20% afirma conocer. Si totalizamos entre los que no conocen y tiene poco conocimiento suma el 74% de encuestados, un porcentaje bastante considerable que pueden ser atacados por phishing, un hacker o cracker, aunque estos prefieren los peces gordos, porque el trabajo de estos es mas de resistencia, no hay que descuidarse.

Pregunta Nro. 20.- De existir un manual de referencia con prevenciones de seguridad informática. ¿Usted haría uso de este?

Tabla 27 - Uso del manual de seguridad informática.

Nunca	13	6,10%
De vez en cuando	95	44,60%
Siempre	105	49,30%
TOTAL	**213**	**100%**

Fuente: Encuesta.

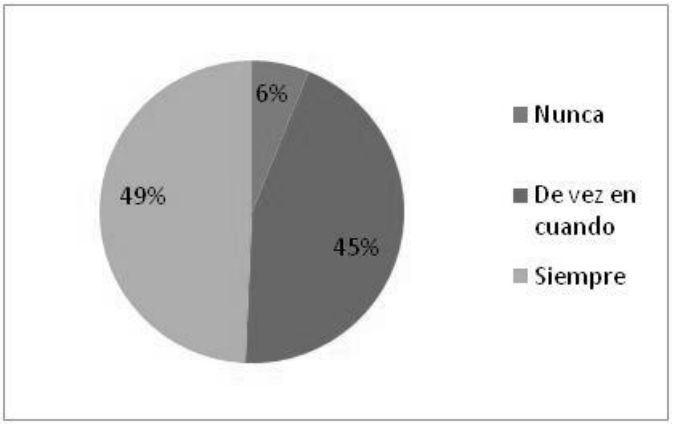


Gráfico 28- Uso del manual de seguridad informática.
Elaborado por: Joffre Germán Díaz Cobos

Interpretación.

La encuesta arroja que el 49% usaría, el 45% de vez en cuando, y el 6% nunca los usaría. Solo sería cuestión de tiempo y capacitación a los encuestados en la compañía, para que comprendan el porqué deberían usar siempre este manual. Definitivamente un manual de seguridad informática orientado a la compañía sería de gran ayuda para poder reducir el riesgo de pérdida de información, los dueños de la compañía deben entender que seguir al pie de la letra el manual al inicio será un poco complicado, pero si es amigable y des complicado, muy pronto se hará un hábito, y un habito bueno lleva a buenos resultados.

Comprobación de la Pregunta Directriz

Para comprobar la pregunta directriz: ¿Existe riesgo de que ocurran delitos informáticos causados por ingeniería social en la compañía Instrumental y Óptica? Se realiza un análisis bajo enfoque mixto de la aplicación de los instrumentos a los colaboradores de la compañía.

Interrogante N° 1: ¿Existen elementos de Ingeniería Social que se pueden evidenciar en la compañía Instrumental y Óptica?

De las encuestas aplicadas a los colaboradores en las preguntas 4, 9, 10, 11 se afirma que existen elementos de ingeniería social que se pueden evidenciar en la compañía Instrumental y Óptica.

Por lo que se infiere que, en la compañía Instrumental y Óptica si existen elementos de ingeniería social, al momento que personas ajenas a la compañía llegan a solicitar la clave de la red inalámbrica interna, o ingresando dispositivos de almacenamiento masivo infectados con algún keylogger que les permitirá obtener usuarios y claves, igualmente cuando se genera una contraseña son tan simples y la frecuencia de cambiarla es nula.

Interrogante N° 2: ¿Se han evidenciado delitos informáticos que han puesto en riesgo la información de la Compañía Instrumental y Óptica?

De las encuestas aplicadas a los colaboradores en las preguntas 3, 6, 12, 19 se alega que si se han evidenciado delitos informáticos que han puesto en riesgo la información de la Compañía Instrumental y Óptica.

Por lo que se concluye que, en la compañía Instrumental y Óptica si se han evidenciado delitos informáticos que han puesto en riesgo la información, cuando al descargar música, películas o programas se han descargado en paralelo otros programas que intentan instalarse solos, lo que supone una salida ilegal de información por medio del internet. Se pudo comprobar también que la compañía recibía correos electrónicos de dudosa procedencia, solicitando proformas de equipos y copias de facturas de clientes, compras de proveedores. Adicional a ello se pudo comprobar que alguien no autorizado extrajo manuales técnicos de una manera ilegal.

Interrogante N° 3: ¿De existir un manual de políticas de seguridades informáticas, permitirá un manejo adecuado y seguro de la información?

De las encuestas aplicadas a los colaboradores en las preguntas 2, 7, 15, 17, 20 de existir un manual de políticas de seguridades informáticas, si permitirá un manejo adecuado y seguro de la información.

Por lo que se puede deducir en que la utilización de un manual como el que se está planteando ayudará en el correcto manejo del hardware, software y cuidados en la seguridad de la información que se procesa en la compañía.

CAPÍTULO V

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

La información que se procesa en la compañía es vulnerable, por la inexistencia de políticas de seguridad, frente a equipos de personal externo que visita la compañía, llevando información con dispositivos de almacenamiento masivo que son conectados en cualquier computador sin realizar un escaneo del mismo o ingresa a la red para usar el internet, así también por la frecuencia con la que se realizan transacciones electrónicas usando la banca, también se pudo observar que el personal que brinda asistencia en el software administrativo contable lo hace de forma remota sin supervisión.

La estructura de la red y transferencia de datos es poco confiable, mediante información directamente obtenida por el investigador, la cablería de red es antigua, existen cables que tienen la protección rota, así también los cables pasan conjuntamente con cables de electricidad, además que se opera la red con dispositivos descontinuados hubs que tienen algunos puertos están quemados, adicional hacen varias cascadas innecesarias, ocasionando pérdidas de paquetes al momento de realizar una transferencia de datos y causando también que el internet sea lento particular que se evidencia al momento de realizar una oferta pública con el estado.

Los equipos de red no son de última tecnología y no presentan las seguridades necesarias frente al ataque de organismos externos.

RECOMENDACIONES

Instaurar el departamento de informática, que encargue de supervisar, mantener, mejorar la estructura tecnológica y brindar el soporte necesario a los funcionarios de la compañía.

Reestructurar la red informática con cableado estructurado logrando certificar los puntos de red, así también colocando equipos de última tecnología que permitan bloquear ataques externos y garantizar la correcta transferencia de datos.
Planificar capacitaciones periódicas que tengan que ver con temas tecnológicos y sobre todo de la seguridad informática.

Elaborar un manual de políticas de seguridad informática que sirva de referencia o guía para el adecuado manejo de la información que se procesa en la compañía.
Socializar el manual y fomentar el uso en los diferentes niveles jerárquicos dentro de la compañía.

CAPÍTULO VI

LA PROPUESTA

TÍTULO DE LA PROPUESTA

Manual de políticas de seguridad informática para la compañía Instrumental y Óptica.

DATOS INFORMATIVOS

Localización: La compañía Instrumental y Óptica se encuentra ubicada en Quito, en las calles Av. Cristóbal Colón Oe1-100 y Av. 10 de Agosto.
Beneficiarios: El número de beneficiarios de la compañía son 20 personas.

ANTECEDENTES

El presente manual detalla algunas políticas de seguridad que deberán de ser cumplidas por el personal de la compañía Instrumental y Óptica, y ha sido desarrollado en base a la problemática que existe frente a la seguridad de la información que maneja y aun estudio investigativo por parte del Joffre Germán Díaz Cobos y reflejado en las encuestas aplicadas a colaboradores, clientes y proveedores, de tal manera que ayuden a precautelar el correcto uso del recurso informático y tener a buen recaudo la información de la compañía.

JUSTIFICACIÓN

Debido a los altos índices de inseguridad que vemos reflejados en la tabulación de las encuestas, es de carácter obligatorio, que tanto el recurso informático y de

datos se protejan de varias maneras, unas de estas es aplicando cambios en el manejo de estos, porque debemos darnos cuenta que el eslabón más frágil de una cadena, es el recurso humano, pues podemos tener varios controles de software, pero si uno de ellos declina ante algo tan simple o se salta de alguna de estas políticas de seguridad propuestas, lo más posible es que se vea afectada la compañía con importantes pérdidas. Por ello lo más destacable es instaurar una cultura de protección, ante los delitos a los que nos enfrentamos, incluso de esta manera se lleva un orden con respecto a la manipulación del hardware y tener a buen recaudo la información, para que estos siempre estén disponibles.

OBJETIVOS

Objetivo General

Elaborar un manual de políticas de seguridad, para un manejo adecuado de los elementos informáticos, de tal manera que la información esté siempre segura y confiable.

Objetivos Específicos

Determinar la influencia de la ingeniería social para instaurar normas que minimicen sus riesgos.

Seleccionar las normas de seguridad que mejor se ajusten para garantizar el buen manejo de la información.

Desarrollar el manual de políticas de seguridad informática

Resultados esperados

Se espera minimizar en un 80% la incidencia de la ingeniería social.

Se desarrolló las políticas de seguridad en base de la Metodología de Benson.

Se desarrolló el 100% del manual de políticas de seguridad informática

ANÁLISIS DE FACTIBILIDAD

Factibilidad Operativa

El desarrollo de la propuesta basada en la Metodología de Benson, prestará grandes beneficios a la empresa, ya que el personal de la misma contará con un manual de políticas de seguridad que le permita guiarse frente a cualquier evento, relacionado con el manejo diario de equipos informáticos.

Factibilidad Técnica

El investigador, se ha inmerso en la problemática de la empresa Instrumental y Óptica, y ha establecido una serie de políticas de seguridad basado en la metodología antes descrita; por tanto es la persona idónea como para diseñar y elaborar el manual de políticas de seguridad propuesto. El investigador tiene la aprobación de empresa para la impresión y socialización del mismo e incluso hacer una verificación posterior que permita determinar su eficacia. Basado en lo anterior se puede concluir que la propuesta es técnicamente factible.

PRESUPUESTO DE LA PROPUESTA

Computador Portátil:	$ 900,00
Impresora	$ 250,00
Servicio de imprenta	$ 400,00
Movilización	$ 100,00
Capacitación	$ 100,00
TOTAL	$ 1.750,00

DISEÑO DE LA PROPUESTA

Bocetaje del manual

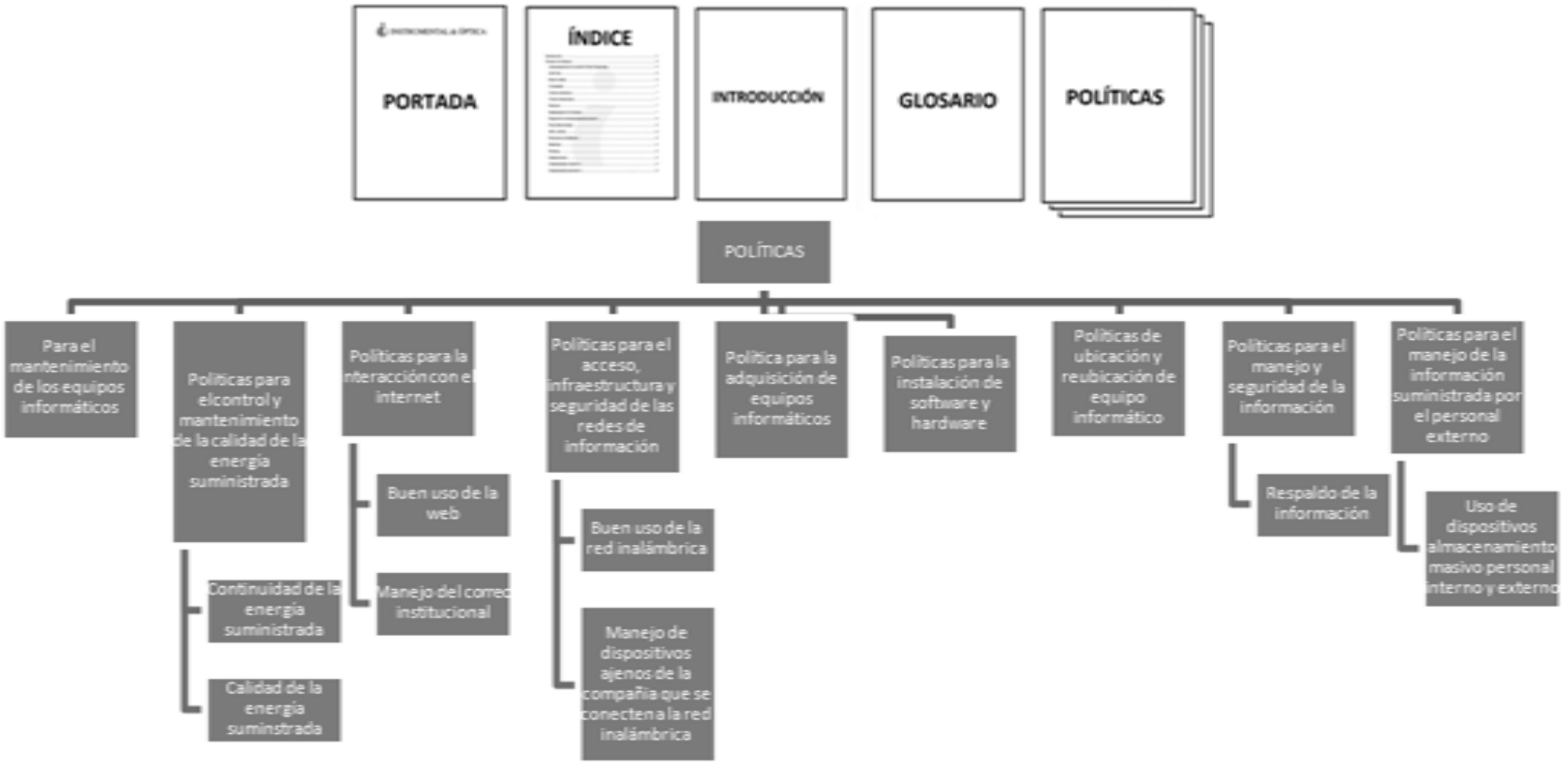


Gráfico 29 – Bocetaje del manual
Elaborado por: Joffre Germán Díaz Cobos

DESARROLLO DE LA PROPUESTA

En el siguiente gráfico puede observar la estructura que debe tener la metodología de Benson, para poder generar estrategias de seguridad y eliminar las vulnerabilidades del sistema de datos ante ataques de cualquier tipo.

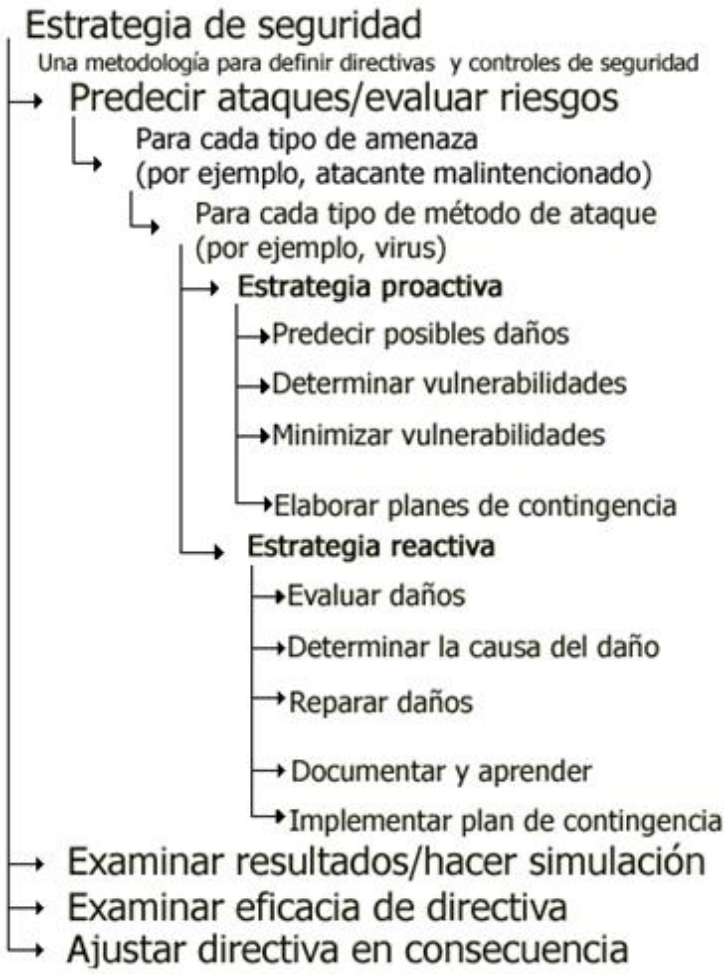


Gráfico 30- Estrategia de seguridad.
Fuente: (Raggad, 2010, pág. 207)

Desarrollo de las directivas de seguridad informática según Metodología de Benson:

Directivas de seguridad informática física.

Políticas para el mantenimiento del los equipos informáticos.

Estrategia de seguridad

Predecir ataques/evaluar riesgos

Daños parcial o total de los equipos informáticos. Los equipos no se pueden usar para el trabajo de la compañía.

Para cada tipo de amenaza

Consumo de alimentos en las estaciones de trabajo.

Presencia de polvo, smog ceniza volcánica y humo de cigarrillo.

Para cada tipo de método de ataque

Contaminar los equipos con residuos de comida y bebida.

Ubicación de la oficina frente a un parte y una avenida de alto tráfico.

Estrategia proactiva

Predecir posibles daños

El teclado y componentes de los equipos informáticos pueden verse seriamente afectados por la presencia de residuos de comida y líquidos.

Si la fuente de poder se atasca por exceso de polvo y smog, puede emitir voltajes errados que llevan al mal funcionamiento del equipo.

Determinar vulnerabilidades

No hay señales de prevención para el cuidado de los equipos.

Oficina alfombrad, sistema de ventilación inadecuado.

Minimizar vulnerabilidades

Colocar rotulación adecuada.

Reemplazar las alfombras por materiales que no atrapen polvo y mejorar el sistema de ventilación para reducir la contaminación externa.

Elaborar planes de contingencia

Disponer de partes y piezas para poder reemplazar en caso de daños.

Estrategia reactiva

Evaluar daños

Pérdida de producción

Determinar la causa del daño

Los equipos informáticos dejan de funcionar por amenazas humanas y ambientales.

Repara daños

Realizando un mantenimiento correctivo de los equipos afectados.

Documentar y aprender

Llevar una bitácora donde registre el problema ocasionado y que sirva de aprendizaje para futuros eventos.

Planes de contingencia

Reemplazo de periféricos afectados o colocar un equipo provisional hasta que el equipo afectado sea reparado.

Examinar resultados

Pérdida de producción

Examinar eficacia de la directiva

Políticas para el mantenimiento del los equipos informáticos.

Ajustar directiva en consecuencia

Políticas de ubicación y reubicación de equipos informático.

Estrategia de seguridad

Predecir ataques/evaluar riesgos

Daños físicos y/o lógicos por reubicar equipo.

Los equipos no se pueden usar para el trabajo de la compañía.

Para cada tipo de amenaza

Movimiento no autorizado de los equipos dentro o fuera de la compañía.

Para cada tipo de método de ataque

Los usuarios toman prestado periféricos de otros equipos para uso dentro de su estación de trabajo o fuera de él.

Estrategia proactiva

Predecir posibles daños

Rotura de periféricos.

Pérdida de información.

Hurto del equipo.

Determinar vulnerabilidades

Ausencia de controles para movimiento de equipo informático dentro y fuera de la compañía.

Minimizar vulnerabilidades

Establecer formas para la ubicación y reubicación de equipo informático.

Capacitar al personal de seguridad para el control adecuado de la salida de equipo.

Elaborar planes de contingencia

Disponer de partes y piezas para poder reemplazar en caso de daños.

Estrategia reactiva

Evaluar daños

Pérdida de producción

Pérdida de equipo informático.

Determinar la causa del daño

Los equipos informáticos se destruyen por el manejo inadecuado, en un traslado no autorizado, incluso perderse.

Repara daños

Reposición total o parcial del equipo afectado.

Documentar y aprender

Llevar una bitácora donde registre el problema ocasionado y que sirva de aprendizaje para futuros eventos.

Planes de contingencia

Reemplazo de periféricos afectados.

Examinar resultados

Pérdida de producción

Examinar eficacia de la directiva

Políticas de ubicación y reubicación de equipos informático.

Ajustar directiva en consecuencia

Directivas de seguridad de la red.

Política para el buen uso de la red inalámbrica.

Estrategia de seguridad

Predecir ataques/evaluar riesgos

Robo de información.

Baja velocidad de conexión a internet en los equipo de la compañía.

Saboteo de la red.

Para cada tipo de amenaza

Conexión de dispositivos móviles.

Para cada tipo de método de ataque

El intruso ingresa mediante un dispositivo inalámbrico.

Estrategia proactiva

Predecir posibles daños

Extracción de información delicada para la compañía.

Des configuración de la red para dejarla vulnerable para propósitos ilícitos.

Delincuentes ingresan a la red y obtiene claves bancarias que desembocan en pérdidas económicas.

Determinar vulnerabilidades

Contraseña es accesible para todos los visitantes de la compañía.

La red inalámbrica es visible y accesible fuera de la empresa.

El sistema de protección de la red inalámbrica es débil.

La red inalámbrica para visitantes forma parte de la misma red de transferencia de archivos internos y del sistema informático.

Minimizar vulnerabilidades

Limitar el acceso de la red inalámbrica a los usuarios de la compañía.

Usar encriptación para el acceso a la red.

Separa la red de datos y sistema informático de la red inalámbrica.

Elaborar planes de contingencia

Cambio de usuarios y claves de acceso en routers, servidor y terminales.

Estrategia reactiva

Evaluar daños

Pérdida de producción

Pérdida de información.

Pérdidas económicas.

Determinar la causa del daño

Existe pérdida de información, daños económicos e inseguridad en la red inalámbrica.

Reparar daños

Recuperar respaldo de configuración de router.

Evaluar pérdidas y reclamar a las compañías de seguros por el siniestro causado.

Documentar y aprender

Llevar una bitácora donde registre el problema ocasionado y que sirva de aprendizaje para futuros eventos.

Planes de contingencia

Respaldar configuraciones.

Contratar seguros que cubra pérdida de información y dinero a causa de delitos informáticos.

Examinar resultados

Pérdidas económicas.

Pérdidas de información.

Examinar eficacia de la directiva

Políticas de ubicación y reubicación de equipos informático.

Ajustar directiva en consecuencia

Políticas para la seguridad de la red informática.

Estrategia de seguridad

Predecir ataques/evaluar riesgos

Robo de información.

Saboteo de la red.

Accesos externos.

Para cada tipo de amenaza

Personas no autorizadas pueden conectarse a la red de la compañía.

Para cada tipo de método de ataque

Personas no autorizadas ingresa a la red con solo conectarse a un punto de la misma.

Mediante el uso de keyloggers cualquier usuario de la compañía abre las puertas de la información a todo el mundo.

Mediante la IP pública usuarios pueden ingresar a la red mediante puertos abiertos.

Estrategia proactiva

Predecir posibles daños

Mal funcionamiento de los equipos.

Extracción de información delicada para la compañía.

Des configuración de la red para dejarla vulnerable para propósitos ilícitos.

Delincuentes ingresan a la red y obtiene claves bancarias que desembocan en pérdidas económicas.

Determinar vulnerabilidades

Puntos de red de fácil acceso para el propósito ilícitos.

Puertos del router abiertos innecesariamente, permiten el acceso externo.

El sistema de configuración lógica de red es DHCP.

El desconocimiento de los usuarios frente a, cómo actuar frente a amenazas en la red.

Minimizar vulnerabilidades

Usar un sistema de configuración lógica de red mediante proxy,

Usar encriptación para el acceso a la red.

Separar la red de datos y sistema informático de la red inalámbrica.

Capacitar al usuario sobre seguridades que deben tener dentro de una red.

Elaborar planes de contingencia

Cambio de usuarios y claves de acceso en routers, servidor y terminales.

Estrategia reactiva

Evaluar daños

Pérdida de producción

Pérdida de información.

Pérdidas económicas.

Determinar la causa del daño

Existe pérdida de información, daños económicos e inseguridad en la red.

Reparar daños

Recuperar respaldos de configuración e información.

Evaluar pérdidas y reclamar a las compañías de seguros por el siniestro causado.

Documentar y aprender

Llevar una bitácora donde registre el problema ocasionado y que sirva de aprendizaje para futuros eventos.

Planes de contingencia

Respaldar configuraciones.

Respaldar información

Contratar seguros que cubra pérdida de información y dinero a causa de delitos informáticos.

Examinar resultados

Pérdidas económicas.

Pérdidas de información.

Examinar eficacia de la directiva

Políticas para la seguridad de la red informática.

Ajustar directiva en consecuencia

Manejo de dispositivos ajenos a la compañía que se conecten a la red inalámbrica.

Estrategia de seguridad

Predecir ataques/evaluar riesgos

Robo de información.

Saboteo de la red.

Accesos externos.

Para cada tipo de amenaza

Personas no autorizadas pueden conectarse a la red de la compañía.

Para cada tipo de método de ataque

Personas no autorizadas ingresa a la red inalámbrica.

Mediante el explorador de red pueden acceder a la información sensible para la compañía.

Estrategia proactiva

Predecir posibles daños

Mal funcionamiento y des configuración de red.

Extracción de información delicada para la compañía.

Delincuentes ingresan a la red y obtiene claves bancarias que desembocan en pérdidas económicas.

Determinar vulnerabilidades

Puertos del router abiertos innecesariamente, permiten el acceso externo.

El sistema de configuración lógica de red es DHCP.

El desconocimiento de los usuarios frente a, cómo actuar frente a amenazas en la red.

Minimizar vulnerabilidades

Usar un sistema de configuración lógica de red mediante proxy,

Usar encriptación para el acceso a la red.

Separar la red de datos y sistema informático de la red inalámbrica.

Capacitar al usuario sobre seguridades que deben tener dentro de una red.

Elaborar planes de contingencia

Cambio de usuarios y claves de acceso en routers, servidor y terminales.

Estrategia reactiva

Evaluar daños

Pérdida de producción

Pérdida de información.

Pérdidas económicas.

Pérdida de velocidad en banda ancha.

Determinar la causa del daño

Existe pérdida de información, daños económicos e inseguridad en la red.

Reparar daños

Recuperar respaldos de configuración e información.

Evaluar pérdidas y reclamar a las compañías de seguros por el siniestro causado.

Documentar y aprender

Llevar una bitácora donde registre el problema ocasionado y que sirva de aprendizaje para futuros eventos.

Planes de contingencia

Respaldar configuraciones.

Respaldar información

Contratar seguros que cubra pérdida de información y dinero a causa de delitos informáticos.

Examinar resultados

Pérdidas económicas.

Pérdidas de información.

Examinar eficacia de la directiva

Manejo de dispositivos ajenos a la compañía que se conecten a la red inalámbrica.

Ajustar directiva en consecuencia

Directivas de seguridad de los datos.

Política para el respaldo de la información.

Estrategia de seguridad

Predecir ataques/evaluar riesgos

Robo de información.

Saboteo de la información.

Pérdida de información.

Para cada tipo de amenaza

Personal interno o externo extraen información sensible de la compañía.

Personal de la compañía con o sin intención borran información importante.

El disco duro del servidor de archivos se daña.

Para cada tipo de método de ataque

Personas no autorizadas ingresa al servidor de archivos con intenciones fraudulentas.

Mediante un computador conectado a la red se borra la información.

La falta de mantenimiento en el proveedor de regulación de energía eléctrica quema el disco duro.

Estrategia proactiva

Predecir posibles daños

Extracción de información delicada para la compañía.

Pérdidas económicas.

Determinar vulnerabilidades

Puertos del router abiertos innecesariamente, permiten el acceso externo.

No hay un proceso de respaldos de información.

El personal no se encuentra capacitado para manejar la información desde una red.

Minimizar vulnerabilidades

Usar un sistema de configuración lógica de red mediante proxy,

Sacar respaldos periódicos.

Capacitar al usuario del correcto manejo de la información en la red.

Elaborar planes de contingencia

Tener un respaldo actualizado y fiable.

Estrategia reactiva

Evaluar daños

Pérdida de producción

Pérdida de información.

Pérdidas económicas.

Determinar la causa del daño

Existe pérdida de información, daños económicos e inseguridad en la red.

El usuario no maneja correctamente el computador.

Mala regulación del sistema eléctrico.

Reparar daños

Recuperar respaldos

Reparar o cambiar disco duro dañado.

Documentar y aprender

Llevar una bitácora donde registre el problema ocasionado y que sirva de aprendizaje para futuros eventos.

Planes de contingencia

Respaldar información

Contratar seguros que cubra pérdida de información y dinero a causa de delitos informáticos.

Examinar resultados

Pérdidas económicas.

Pérdidas de información.

Examinar eficacia de la directiva

Política para el respaldo de la información.

Ajustar directiva en consecuencia

Políticas para el uso de mensajería electrónica y uso de redes sociales.

Estrategia de seguridad

Predecir ataques/evaluar riesgos

Robo de información.

Virus.

Ingeniería Social

Para cada tipo de amenaza

Información sensible se fuga por correo electrónico.

Software dañino daña el computador

Datos importantes de la compañía se filtran.

Para cada tipo de método de ataque

Personal de la compañía mediante el correo electrónico envía proformas de la compañía a la competencia.

Abriendo correos de personas no conocidas el computador es contagiado de troyanos.

A través de una supuesta encuesta que llega al correo electrónico extraen información de la compañía.

Estrategia proactiva

Predecir posibles daños

Perdida de información sensible.

El computador deja de ser operativo y se vuelve un medio de contagio masivo mediante la red.

Entrega de datos sensibles ocasionan perjuicios económicos.

Determinar vulnerabilidades

Falta de restricción de revisión de correos personales.

Desconocimiento de Ingeniería Social.

Minimizar vulnerabilidades

Bloquear redes sociales y correos personales.

Capacitación de seguridad informática.

Elaborar planes de contingencia

Capacitaciones continúas sobre seguridades informáticas y ética profesional.

Estrategia reactiva

Evaluar daños

Pérdida de producción

Pérdida de información.

Pérdidas económicas.

Determinar la causa del daño

Existe pérdida de información, daños económicos e inseguridad en la red.

Reparar daños

Recuperar respaldos de configuración e información.

Evaluar pérdidas y reclamar a las compañías de seguros por el siniestro causado.

Documentar y aprender

Llevar una bitácora donde registre el problema ocasionado y que sirva de aprendizaje para futuros eventos.

Planes de contingencia

Respaldar configuraciones.

Respaldar información

Contratar seguros que cubra pérdida de información y dinero a causa de delitos informáticos.

Examinar resultados

Pérdidas económicas.

Pérdidas de información.

Examinar eficacia de la directiva

Políticas para el uso de mensajería electrónica y uso de redes sociales.

Ajustar directiva en consecuencia

Monitoreo de computadora (s) por parte de soporte externo.

Estrategia de seguridad

Predecir ataques/evaluar riesgos

Robo de información.

Robo o cambio de partes y piezas de equipos.

Para cada tipo de amenaza

Extracción de información delicada

Intervenir equipos sin ser necesario

Para cada tipo de método de ataque

Conectar dispositivos de almacenamiento masivo.

Llevarse equipos o abrir equipos.

Estrategia proactiva

Predecir posibles daños

Al sacar información sensible esta se vende o se entrega a la competencia ocasionando grande pérdidas económicas.

Mal funcionamiento o bajo rendimiento del equipo informático.

Determinar vulnerabilidades

No existe personal de sistemas que supervise las acciones que está realizando el personal de soporte externo.

Minimizar vulnerabilidades

Solicitar al personal de sistemas que atienda al personal de soporte externo, vigilando continuamente las acciones que va a tomar con el equipo informático.

Elaborar planes de contingencia

Tener todos los datos de la empresa, persona que ejecuta el soporte externo.

Evaluar pérdidas y reclamar a las compañías de seguros por el siniestro causado.

Estrategia reactiva

Evaluar daños

Pérdida de producción

Pérdida económica.

Determinar la causa del daño

Los equipos informáticos dejan de funcionar correctamente por partes y piezas cambiadas.

Repara daños

Realizar un reclamo de manera formal a la empresa que realizó el soporte.

Documentar y aprender

Llevar una bitácora donde registre el problema ocasionado y que sirva de aprendizaje para futuros eventos.

Planes de contingencia

Reemplazo de periféricos afectados o colocar un equipo provisional hasta que el equipo afectado sea reparado.

Examinar resultados

Pérdida de producción

Examinar eficacia de la directiva

Políticas para el monitoreo de computadora (s) por parte de soporte externo.

Ajustar directiva en consecuencia

Cuidados para el manejo de la banca electrónica

Estrategia de seguridad

Predecir ataques/evaluar riesgos

Robo de contraseñas bancarias.

Robo de dinero.

Para cada tipo de amenaza

Personas no autorizadas pueden conocer contraseñas bancarias.

Delincuentes informáticos extraen dinero de cuentas bancarias o realizan compras con tarjetas de crédito de la compañía.

Para cada tipo de método de ataque

Mediante el uso de keyloggers enviado vía correo o insertando un dispositivo de almacenamiento masivo en el equipo donde se realizan las transacciones bancarias, el delincuente puede saber todos los movimientos de la máquina, páginas visitadas, usuarios, contraseñas bancarias.

Estrategia proactiva

Predecir posibles daños

Lentitud en el funcionamiento de los equipos.

Extracción de información delicada para la compañía.

Pérdidas económicas.

Determinar vulnerabilidades

Varios usuarios tienen accesos a la computadora donde se realizan las transacciones bancarias.

Se conectan todo tipo de dispositivos de almacenamiento masivo en la computadora donde se realizan las transacciones bancarias.

Minimizar vulnerabilidades

Usar una sola computadora donde se realicen las transacciones bancarias.

La computadora donde se realicen las transacciones bancarias debe ser la de gerencia administrativa.

El manejo de contraseñas debe estará cargo de la gerencia administrativa.

Capacitar al usuario sobre seguridades que debe mantener al momento de realizar una transacción bancaria.

Elaborar planes de contingencia

Cambio de usuarios y contraseñas de acceso a computador y portales bancarios.

Informar a las autoridades y entidades bancarias sobre el delito cometido.

Estrategia reactiva

Evaluar daños

Pérdidas económicas.

Determinar la causa del daño

Existe pérdida de dinero por falta de políticas de seguridad en la compañía y la falta de información del personal a cargo.

Reparar daños

Evaluar pérdidas y reclamar a las compañías de seguros por el siniestro causado.

Documentar y aprender

Llevar una bitácora donde registre el problema ocasionado y que sirva de aprendizaje para futuros eventos.

Planes de contingencia

Contratar seguros que cubra pérdida de información y dinero a causa de delitos informáticos.

Examinar resultados

Pérdidas económicas.

Pérdidas de información.

Examinar eficacia de la directiva

Cuidados para el manejo de la banca electrónica

Ajustar directiva en consecuencia

Planes y pruebas de contingencias y de recuperación de desastres.

Política para el control y mantenimiento de la calidad de la energía eléctrica suministrada.

Estrategia de seguridad

Predecir ataques/evaluar riesgos

Daños parcial o total de los equipos informáticos.

Pérdida de información.

Para cada tipo de amenaza

Variaciones de voltaje.

Voltajes incorrectos en los equipos informáticos.

Para cada tipo de método de ataque

Conectar los equipos informáticos en tomas de corriente no apta para los equipos.

Estrategia proactiva

Predecir posibles daños

Fuentes de alimentación de CPUs, impresoras adaptadores de voltaje de computadores portátiles pueden verse seriamente afectados por la presencia de picos de voltaje o corrientes.

Las placas principales contaminadas por corrientes elevadas transmiten corrientes incorrectas a discos duros provocando que estos dispositivos se quemen y dejen de funcionar y perder la información.

Determinar vulnerabilidades

No hay señales de prevención para conectar en lugares apropiados los equipos informáticos.

No hay reguladores y UPS.

Minimizar vulnerabilidades

Colocar rotulación adecuada.

Reemplazar antiguo sistema de red eléctrico.

Colocar reguladores y UPS´s.

Elaborar planes de contingencia

Constar de un seguro para los equipos informáticos.

Tener respaldos actualizados.

Disponer de partes y piezas para poder reemplazar en caso de daños y resolver el problema de forma inmediata.

Estrategia reactiva

Evaluar daños

Pérdida de producción

Pérdidas económicas.

Pérdida de información.

Determinar la causa del daño

Los equipos informáticos dejan de funcionar por shocks eléctricos y falta de capacitación de los usuarios.

Repara daños

Realizando un mantenimiento correctivo de los equipos afectados.

Documentar y aprender

Llevar una bitácora donde registre el problema ocasionado y que sirva de aprendizaje para futuros eventos.

Planes de contingencia

Reemplazo de periféricos afectados o colocar un equipo provisional hasta que el equipo afectado sea reparado.

Examinar resultados

Pérdida de producción.

Examinar eficacia de la directiva

Política para el control y mantenimiento de la calidad de la energía eléctrica suministrada.

Ajustar directiva en consecuencia

Política de uso de dispositivos de almacenamiento masivo personal interno, externo

Estrategia de seguridad

Predecir ataques/evaluar riesgos

Robo de información.

Saboteo de la información.

Pérdida de información.

Para cada tipo de amenaza

Personal interno o externo extraen información sensible de la compañía.

Personal de la compañía con o sin intención borran información importante.

El dispositivo de almacenamiento masivo esta contagiado de troyanos.

Para cada tipo de método de ataque

Personas no autorizadas roban información con intenciones fraudulentas.

Mediante un dispositivo almacenamiento masivo se puede dañar o borra la información.

Estrategia proactiva

Predecir posibles daños

Extracción de información delicada para la compañía.

Pérdidas económicas.

Determinar vulnerabilidades

Puertos de conexión para dispositivos de almacenamiento masivo abiertos innecesariamente, permiten el acceso.

Los respaldos no deben hacerse con dispositivos de almacenamiento masivo por personal no autorizado.

El personal saca respaldos en memorias flash.

Minimizar vulnerabilidades

Configuración de puertos.

Sacar respaldos periódicos por personal informático de la empresa.

Capacitar al usuario del correcto manejo de la información.

Elaborar planes de contingencia

Tener un respaldo actualizado y fiable.

Estrategia reactiva

Evaluar daños

Pérdida de producción

Pérdida de información.

Pérdidas económicas.

Determinar la causa del daño

Existe pérdida de información, daños económicos e inseguridad en la red.

El usuario no maneja correctamente el computador.

Mala regulación del sistema eléctrico.

Reparar daños

Recuperar respaldos

Documentar y aprender

Llevar una bitácora donde registre el problema ocasionado y que sirva de aprendizaje para futuros eventos.

Planes de contingencia

Respaldar información

Contratar seguros que cubra pérdida de información y dinero a causa de delitos informáticos.

Examinar resultados

Pérdidas económicas.

Pérdidas de información.

Examinar eficacia de la directiva

Política de uso de dispositivos de almacenamiento masivo personal interno, externo.

Ajustar directiva en consecuencia

Directivas de administración y coordinación de la seguridad informática.

Políticas para el manejo del correo institucional.

Estrategia de seguridad

Predecir ataques/evaluar riesgos

Robo de información.

Virus.

Ingeniería Social

Para cada tipo de amenaza

Información sensible se fuga por correo electrónico.

Software dañino daña el computador

Datos importantes de la compañía se filtran.

Para cada tipo de método de ataque

Personal de la compañía mediante el correo electrónico envía proformas de la compañía a la competencia.

Abriendo correos de personas no conocidas el computador es contagiado de troyanos.

A través de una supuesta encuesta que llega al correo electrónico extraen información de la compañía.

Estrategia proactiva

Predecir posibles daños

Perdida de información sensible.

El computador deja de ser operativo y se vuelve un medio de contagio masivo mediante la red.

Entrega de datos sensibles ocasionan perjuicios económicos.

Determinar vulnerabilidades

Falta de restricción de revisión de correos personales.

Desconocimiento de Ingeniería Social.

Minimizar vulnerabilidades

Bloquear redes sociales y correos personales.

Capacitación de seguridad informática.

Elaborar planes de contingencia

Capacitaciones continúas sobre seguridades informáticas y ética profesional.

Estrategia reactiva

Evaluar daños

Pérdida de producción

Pérdida de información.

Pérdidas económicas.

Determinar la causa del daño

Existe pérdida de información, daños económicos e inseguridad en la red.

Reparar daños

Recuperar respaldos de configuración e información.

Evaluar pérdidas y reclamar a las compañías de seguros por el siniestro causado.

Documentar y aprender

Llevar una bitácora donde registre el problema ocasionado y que sirva de aprendizaje para futuros eventos.

Planes de contingencia

Respaldar configuraciones.

Respaldar información

Contratar seguros que cubra pérdida de información y dinero a causa de delitos informáticos.

Examinar resultados

Pérdidas económicas.

Pérdidas de información.

Examinar eficacia de la directiva

Políticas para el manejo del correo institucional.

Ajustar directiva en consecuencia

Políticas para el uso el buen uso de la web.

Estrategia de seguridad

Predecir ataques/evaluar riesgos

Robo de información.

Virus.

Ingeniería Social

Para cada tipo de amenaza

Información sensible se fuga por páginas espías.

Software dañino daña el computador

Datos importantes de la compañía se filtran.

Para cada tipo de método de ataque

Personal de la compañía la web abren páginas no autorizadas.

Abriendo páginas no autorizadas, desconocidas, descargar software pirata el computador es contagiado de troyanos.

A través de una supuesta encuesta que solicita una página web extraen información de la compañía.

Estrategia proactiva

Predecir posibles daños

Perdida de información sensible.

El computador deja de ser operativo y se vuelve un medio de contagio masivo mediante la red.

Entrega de datos sensibles ocasionan perjuicios económicos.

Determinar vulnerabilidades

Falta restricción de páginas web.

Desconocimiento de Ingeniería Social.

Minimizar vulnerabilidades

Autorizar estrictamente solo las páginas que van a ser usadas en cada computador.

Capacitación de seguridad informática.

Elaborar planes de contingencia

Capacitaciones continúas sobre seguridades informáticas y ética profesional.

Estrategia reactiva

Evaluar daños

Pérdida de producción

Pérdida de información.

Pérdidas económicas.

Determinar la causa del daño

Existe pérdida de información, daños económicos e inseguridad en la red.

Reparar daños

Recuperar respaldos de configuración e información.

Evaluar pérdidas y reclamar a las compañías de seguros por el siniestro causado.

Documentar y aprender

Llevar una bitácora donde registre el problema ocasionado y que sirva de aprendizaje para futuros eventos.

Planes de contingencia

Respaldar configuraciones.

Respaldar información

Contratar seguros que cubra pérdida de información y dinero a causa de delitos informáticos.

Examinar resultados

Pérdidas económicas.

Pérdidas de información.

Examinar eficacia de la directiva

Políticas para el uso el buen uso de la web.

Ajustar directiva en consecuencia

Política para la adquisición de equipos informáticos.

Estrategia de seguridad

Predecir ataques/evaluar riesgos

Adquirir un equipo inadecuado.

Pérdidas económicas.

Para cada tipo de amenaza

Personal sin conocimiento técnico frente a la adquisición de equipos.

Para cada tipo de método de ataque

Adquisición de equipo informático

Estrategia proactiva

Predecir posibles daños

Equipo no responde a necesidades de la empresa.

Determinar vulnerabilidades

No disponer de personal técnico.

Minimizar vulnerabilidades

Disponer del asesoramiento adecuado.

Elaborar planes de contingencia

Estrategia reactiva

Evaluar daños

Pérdida producción.

Determinar la causa del daño

Se adquiere equipo inadecuado.

Repara daños

Acondicionar equipo para el trabajo.

Documentar y aprender

Llevar una bitácora donde registre el problema ocasionado y que sirva de aprendizaje para futuros eventos.

Planes de contingencia

Examinar resultados

Pérdida económica y productividad.

Examinar eficacia de la directiva

Examinar la directiva para la adquisición de equipos informáticos.

Ajustar directiva en consecuencia

Política para la selección y mantenimiento del software antivirus.

Estrategia de seguridad

Predecir ataques/evaluar riesgos

Pérdida total o parcial de la información

Mal funcionamiento del software

Para cada tipo de amenaza

Los usuarios sin intención introducen virus en el equipo.

Personas mal intencionadas introducen virus.

Para cada tipo de método de ataque

El correo electrónico infectado con virus.

Ingreso de dispositivos con virus

Mal uso del interne.

Estrategia proactiva

Predecir posibles daños

Pérdida total o parcial de la información.

Pérdida de productividad.

Contagiar a otros equipos de la red.

Determinar vulnerabilidades

Uso de software antivirus ilegal o ausencia del mismo.

Minimizar vulnerabilidades

Instalación de software antivirus de buena calificación con licenciamiento.

Mantener actualizada la base de datos del antivirus.

Elaborar planes de contingencia

Respaldar periódicamente la información.

Estrategia reactiva

Evaluar daños

Pérdida de información y pérdidas económica para la compañía.

Determinar la causa del daño

El mal funcionamiento del equipo por virus

Repara daños

Usar software alternativo para corregir el problema.

Restaurar información de respaldos.

Documentar y aprender

Llevar una bitácora donde registre el problema ocasionado y que sirva de aprendizaje para futuros eventos.

Planes de contingencia

Respaldos periódicos

Examinar resultados

Pérdida de información.

Examinar eficacia de la directiva

Examinar la directiva para el mantenimiento del software antivirus.

Ajustar directiva en consecuencia

Políticas para establecer contraseñas.

Estrategia de seguridad

Predecir ataques/evaluar riesgos

Accesos no autorizados

Para cada tipo de amenaza

Acceso a información confidencial.

Perjuicios económicos.

Para cada tipo de método de ataque

El usuario escribe contraseñas débiles.

Ingeniería social.

Estrategia proactiva

Predecir posibles daños

Si se roba información confidencial hay pérdida de beneficios.

Al ingresar a sistema bancario hay pérdidas económicas.

Determinar vulnerabilidades

No existe una política para establecer contraseñas.

Minimizar vulnerabilidades

Implementando políticas para establecer contraseñas seguras.

Elaborar planes de contingencia

Acuerdo de confidencialidad.

Estrategia reactiva

Evaluar daños

Pérdida de beneficios e información confidencial.

Determinar la causa del daño

Contraseñas débiles.

Repara daños

Capacitar al personal para definir contraseñas fuertes.

Documentar y aprender

Llevar una bitácora donde registre el problema ocasionado y que sirva de aprendizaje para futuros eventos.

Planes de contingencia

Examinar resultados

Pérdida económicas y de información.

Examinar eficacia de la directiva

Examinar la directiva para establecer contraseñas.

Ajustar directiva en consecuencia

Políticas para la instalación de hardware.

Estrategia de seguridad

Predecir ataques/evaluar riesgos

Equipo informático con daño parcial o total.

Para cada tipo de amenaza

Los usuarios instalan inadecuadamente el hardware.

Para cada tipo de método de ataque

Los usuarios abren los equipos informáticos.

Conectar equipos en tomacorrientes inadecuados para los equipos informáticos

Estrategia proactiva

Predecir posibles daños

Si el usuario abre el equipo la estática puede dañar los componentes electrónicos.

Si se conecta en un tomacorriente inadecuado el equipo sufre daños severos.

Determinar vulnerabilidades

No hay señales de identificación en tomas de corriente.

No existe una capacitación a los usuarios del correcto manejo de los equipos.

Minimizar vulnerabilidades

Identificar los tomacorrientes.

Capacitar a los usuarios en el correcto uso de los equipos informáticos.

Elaborar planes de contingencia

Disponer de partes y piezas para poder reemplazar en caso de daños ocasionados por el usuario.

Estrategia reactiva

Evaluar daños

Pérdida de información, pérdidas económicas para la compañía y/o el usuario.

Determinar la causa del daño

El usuario manipuló o conectó indebidamente el equipo.

Repara daños

Realizando un mantenimiento correctivo o reemplazo de los equipos afectado.

Prohibir a los usuarios la manipulación interna del equipo.

Documentar y aprender

Llevar una bitácora donde registre el problema ocasionado y que sirva de aprendizaje para futuros eventos.

Planes de contingencia

Reemplazo de periféricos afectados o colocar un equipo provisional hasta que el equipo afectado sea reparado.

Examinar resultados

Pérdida de producción

Examinar eficacia de la directiva

Examinar la directiva para la instalación de hardware.

Ajustar directiva en consecuencia

VALIDACION DE LA PROPUESTA EN EL CONTEXTO REAL.

Para determinar que el manual de políticas de seguridad desarrollado constituye un aporte positivo para la institución, se aplicó la siguiente encuesta a los colaboradores de la empresa Instrumental y Óptica (15 personas).

Obteniendo los siguientes resultados:

Tabla 28 - Encuesta estructurada para colaboradores.

Nro.	Preguntas	Mucho	Poco	Nada
1	¿La capacitación recibida para uso del manual de políticas de seguridad fue satisfactoria?	12	3	0
2	¿Con qué frecuencia usted acude al manual cada vez que tiene que usar equipos informáticos?	5	8	2
3	¿Cree qué ha mejorado la navegación del internet, respecto a publicidades no deseadas, correos de dudosa procedencia?	9	5	1
4	¿Antes de conectar en su computador un dispositivo de almacenamiento masivo toma en cuenta las recomendaciones del manual de políticas de seguridad?	12	3	0
5	¿Basada en la política de seguridad para establecer contraseñas, piensa que la contraseña actual es más segura que las usadas anteriormente?	15	0	0
6	¿Le ha servido la sección del glosario del manual, para informarse respecto a palabras de seguridad que usted desconocía?	13	2	0
7	¿Ha mejorado el rendimiento del computador de su puesto de trabajo?	8	5	2
8	¿La navegación en internet ahora es más fluida y segura?	10	4	1
9	¿Cuando llega un cliente a solicitarle la clave de la red inalámbrica, se remite a la política de seguridad respectiva en el manual de políticas de seguridad?	12	2	1
10	¿La empresa ha tomado acciones al no uso del manual de políticas de seguridad?	4	10	1

Fuente: Encuesta aplicada a los colaboradores de Instrumental y Óptica

ANÁLISIS E INTERPRETACIÓN DE RESULTADOS DE LA VALIDACION DE LA PROPUESTA.

Con base en las respuestas obtenidas en la Tabla 28 - Encuesta estructurada para colaboradores, se puede afirmar que el personal de la compañía Instrumental y Óptica utiliza el manual de manera frecuente, ya sea para establecer contraseñas así como para consultar palabras que desconoce y en uso general relacionado con los equipos informáticos; también aseguran que la navegación sobre internet es más fluida y segura.

Aunque la compañía no ha puesto condicionamientos para el uso del manual de políticas de seguridad, los usuarios acuden al mismo ante eventos que ponga en riesgo la seguridad de la información. Por lo tanto, el usarlo sí muestra un aporte significativo dentro de la institución.

Conclusiones

Luego de haber escrito este manual se ha podido determinar que han existido vulnerabilidades en la compañía a nivel informático y que pueden ser evitadas.

La parte estructural informática y lo que depende de esta, dentro de este manual, se concluye que el equipo informático no estaba cumpliendo su función específica o era inexistente o descuidado.

Debido a que la tecnología y los equipos informáticos tienen avances tecnológicos muy rápidos, algunas políticas podrían ser modificadas.

Recomendaciones:

Apegarse a las políticas de este manual para evitar la pérdida de información, recursos informáticos y no ocasionar perjuicios a la compañía.

Toda la estructura tecnológica debe ser sometida a una auditoria informática, por lo menso una vez al año.

La revisión y actualización de este manual de seguridad, se lo hará cada que lo amerite, por lo tanto puede ser cambiado en base a nuevos lineamientos, dados por la compañía, actualización tecnológica u otras consideraciones que así lo demanden.

BIBLIOGRAFÍA

Acissi. (2015). *Seguridad Informática - Hacking Ético.* Madrid: Ediciones ENI.

Acosta, A. (16 de 08 de 2013). DELITOS " CIBERNETICOS " EN PROYECTO DE CODI GO INTEGRAL PENAL EN EL ECUADOR. *El Comercio* .

AETECNO. (Enero de 2015). Recuperado el 10 de Agosto de 2015, de http://tecno.americaeconomia.com/noticias/seguridad-y-cibercrimen-en-latinoamerica-que-tan-seguro-es-mi-pais

Agencia de regulación y control de las telecomunicaciones. (2002). *ARCOTEL*. Recuperado el 02 de 03 de 2015, de https://www.google.com.ec/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CBwQFjAA&url=http%3A%2F%2Fwww.regulaciontelecomunicaciones.gob.ec%2Fwp-content%2Fplugins%2Fdownload-monitor%2Fdownload.php%3Fid%3D557&ei=gSP1VNXFAcTmsAS_rIGACw&usg=AFQj

Asamblea Nacional del Ecuador. (10 de Febrero de 2014). *Registro oficial*. Obtenido de http://www.asambleanacional.gob.ec/es/system/files/document.pdf

Bastidas, D. A. (16 de Agosto de 2013). DELITOS " CIBERNETICOS " EN PROYECTO DE CÓDIGO INTEGRAL PENAL EN EL ECUADOR.

Bastidas, M. (2011). *ANÁLISIS CRÍTICO DEL TRATAMIENTO JURÍDICO DE LAS TIPOLOGÍAS EN LA LEY PENAL RESPECTO DE LA PROTECCIÓN DE LA INFORMACIÓN INFORMÁTICA EN EL ECUADOR.* Quito.

Betancourt, V. (2004). *Red de Información para el Tercer Sector (RITS) y la Fundación Heinrich.*

Bonifaz, G. (2015). Obtenido de http://www.monografias.com/trabajos/departservi/departservi.shtml

Borghello. (4 de Enero de 2008). *ESET*. Recuperado el 6 de Enero de 2015, de http://www.eset-la.com/centro-prensa/articulo/2008/eset-informa-falsos-perfiles-myspace-codigos-maliciosos/1708

Catalunya, U. d. (2015). *Universidad de Catalunya*. Obtenido de http://www.uoc.edu/portal/es/tecnologia_uoc/infraestructures/index.html

Convenio sobre ciberdelincuencia. (2001). Budapest: Serie de tratados europeos Nro. 185.

Definición de. (2008). Obtenido de http://definicion.de/correo-electronico/

El equipo de Definición ABC. (2015). *Definición ABC*. Obtenido de www.definicionabc.com

El Universo. (20 de 06 de 2011). Recuperado el 18 de 02 de 2015, de Web de la Presidencia de Ecuador sufrió ataque informático: http://www.eluniverso.com/2011/06/20/1/1355/pagina-internet-presidencia-ecuatoriana-sufrio-ataque-informatico.html

El Universo. (17 de 11 de 2014). Recuperado el 18 de 02 de 2015, de Ataques web podrian aumentar: http://www.eluniverso.com/noticias/2014/11/17/nota/4226966/

INFORC_ECUADOR. (2014). *INFORC ECUADOR*. Recuperado el 05 de Noviembre de 2014, de INFORC ECUADOR: http://www.inforc.ec/

Informática moderna. (2008). Obtenido de http://www.informaticamoderna.com/Disp_almacen.htm

Informática moderna. (2008). Obtenido de http://www.informaticamoderna.com/Disp_almacen.htm

ISO. (2013). *ISO*. Recuperado el 02 de 03 de 2015, de http://www.iso27000.es/download/doc_iso27000_all.pdf

Izura, P. X. (02 de agosto de 2003). *IPTABLES tutorial práctico de firewall*. Recuperado el 05 de febrero de 2015, de Pello: http://www.pello.info/filez/firewall/iptables.html

Jiménez, R. (17 de Septiembre de 2014). *Soluciones WEB*. Recuperado el 5 de Enero de 2015, de http://www.solucionweb.co/help-desk/hosting/489-limite-envio-adjuntos-correo-electronico

Leica. (2015). *Leica*. Obtenido de http://www.leica-geosystems.es/es/Redes-de-Estaciones-de-Referencia-GNSS_53982.htm

León, M. (2004). *Diccionario de informática, telecomunicaciones ciencias afines.* Madrid: Babel.

Lewis, E. (2010). *Ciberseguridad en Costa Rica.* Costa Rica: Impresión Gráfica del Este S.A.

Mas adelante. (1999). Obtenido de https://www.masadelante.com/faqs/base-de-datos

Mas adelante. (2015). Obtenido de https://www.masadelante.com/faqs/dominio

Metro. (20 de 09 de 2011). Recuperado el 18 de 02 de 2015, de Ataques informáticos aumentaron 500% en dos años en latinoamérica: http://www.metroecuador.com.ec/15989-ataques-informaticos-aumentaron-500-en-dos-anos-en-latinoamerica.html

Microsoft. (2014). Obtenido de http://windows.microsoft.com/es-xl/windows-vista/what-is-a-password

Microsoft. (20 de Julio de 2004). *TechNet Estrategias de seguridad*. Recuperado el 20 de Noviembre de 2015, de https://www.microsoft.com/spain/technet/recursos/articulos/2005.aspx

Naghi, M. (2005). *Metodología de la Investigación.* México: Limusa.

Naranjo, G. (2010). *Tutoría de la investigación científica.* Ambato: Gráficas Corona Quito.

Olmos, A. P. (01 de 12 de 2008). *Sistema de gestión de la información.* Recuperado el 18 de 02 de 2015, de https://riunet.upv.es/

PC antivirus reviews. (01 de 01 de 2015). Recuperado el 05 de febrero de 2015, de http://www.pcantivirusreviews.com/Comparison/

PC Word. (3 de 11 de 2010). *Antivirus gratuitos y pagados, frente a frente*. Recuperado el 02 de 03 de 2015, de http://www.pcworld.com.mx/Articulos/11744.htm

Pesantes, K. (2013). Anonymous hecho en Ecuador . *VISTAZO* , 15.

Raggad, B. G. (2010). *Information Security Management: Concepts and Practice.* Boca Raton: CRC Press.

Rojas, G. (2010). Manual de sistemas de puesta a tierra. En I. G. Rojas, *Manual de sistemas de puesta a tierra* (pág. 35).

Seguridad y cibercrimen en latinoamerica. (Enero de 2014). Recuperado el 10 de 08 de 2015, de http://tecno.americaeconomia.com/noticias/seguridad-y-cibercrimen-en-latinoamerica-que-tan-seguro-es-mi-pais

SRI. (17 de Abril de 2002). *SRI*. Obtenido de http://www.sri.gob.ec/DocumentosAlfrescoPortlet/descargar/69c4134c-204a-4b35-a702-428a07711b34/ReglamentoComercioElectronico.doc

Sucuzhañay, W. (2015). *PROPUESTA DE GUÍA DE PROCEDIMIENTOS PARA EL LEVANTAMIENTO CATASTRAL DEL CONSORCIO BARRIDOS PREDIALES EC.* Cuenca.

Symantec, O. y. (2013). *Seguridad y cibercrimen en Latinoamérica: ¿Qué tan seguro es mi país?*

Telégrafo, E. (10 de 10 de 2011). Ataques hacker a redes de Ecuador. Guayaquil, Guayas, Ecuador.

Tori, C. (2008). *Hacking Ético.* Argentina: Mastroianni Impresiones.

Ureta, L. (2009). *Retos a superar en la administración de justicia ante los delitos informáticos del Ecuador.* Guayaquil.

Velásquez, J. (2007). *El estudio de caso en las relaciones jurídicas internacionales.* México: Unam.

Wikipedia. (2014). Obtenido de http://es.wikipedia.org/wiki/Fase_(onda)

Willems, E. (13 de 10 de 2011). *G DATA*. Recuperado el 20 de 02 de 2015, de https://www.gdata.es/security-labs/news/news-details/2379-un-20-de-los-usuarios-de-rede

Zurita, S. (2010). Políticas de seguridad y los riesgos informáticos en la Industria Catedral S.A. de la ciudad de Ambato. Ambato.

GLOSARIO

Adware: Es un programa que difunde publicidad a través de banners, ventanas emergentes, etc. mientras está funcionando.

Alfanumérico: Cualquier combinación de números, letras y símbolos.

Ancho de banda: Es la máxima cantidad de información simultánea que se puede transferir por un canal en cada unidad de tiempo.

Antivirus: Programas que se utilizan con el fin de prevenir y detectar posibles infecciones producidas por virus y todo tipo de programas maliciosos, y reparar los daños que éstas hayan podido causar.

Aplicación: Se puede considerar sinónimo de programa o software.

Archivo: Sinónimo de fichero. Paquete de información (textos, gráficos, programas...)identificado por un nombre en los sistemas informáticos.

Backup: Copia de seguridad de los ficheros o programas del disco duro que se duplican en otro soporte de almacenamiento.

Bajar (download): Proceso que consiste en transferir un archivo de un ordenador remoto a nuestro propio ordenador.

Base de datos: Sistema de almacenamiento de datos muy flexible que te permite utilizar la información en función de diversos criterios.

Clave: Es una señal que ha sido expresada en código mezclado con fines de seguridad.

Cookie: Pequeño segmento de datos que entrega el servidor de HTTP al navegador WWW del usuario cuando se conecta a una determinada página, para que éste lo guarde

Correo electrónico (e-mail): Sistema para enviar mensajes entre ordenadores conectados telemáticamente. A los mensajes se les pueden adjuntar archivos de todo tipo.

Cortafuegos (firewall): Son programas que protegen una red de otra red. El cortafuego permite el acceso de un ordenador de una red local a Internet, pero la Red no ve más allá del "firewall".

Delitos informáticos: La realización de una acción que, reuniendo las características que delimitan el concepto de delito, se ha llevado a cabo utilizando un elemento informático, contra los derechos y libertades de los ciudadanos.

Gusano: Los gusanos o worms son programas con características similares a las de los virus, aunque a diferencia de éstos, son capaces de realizar copias de sí mismos

Keylogger: Programa o dispositivo que registra las combinaciones de teclas pulsadas por los usuarios, y las almacena para obtener datos confidenciales como contraseñas, contenido de mensajes de correo, etc. La información almacenada se suele publicar o enviar por internet.

Ingeniería Social: Es una metodología de investigación, de influencias y acciones clandestinas que tiene por objeto comprometer un sistema de información explotando principalmente sus fallos humanos.

Link: En una página web es un hiperenlace que permite acceder directamente a otra página.

Login: Nombre o identificador de un usuario de un sistema remoto en una red.

Hacker: Amañador, mañoso; intruso, pirata informático

Hardware: Equipo físico de máquina

Malware: El término Malware (Acrónimo en inglés de: "Malcious software") engloba a todos aquellos programas "maliciosos" (troyanos, virus, gusanos, etc.) que pretenden obtener un determinado beneficio, causando algún tipo de perjuicio al sistema informático

Manual de usuario: Es una guía de consulta que permite al usuario la mejor utilización del sistema de información.

Navegador (browser): Programa que se emplea pata acceder a la información contenida en la World Wide Web y visualizarla.

Navegar: Desplazarse por las páginas web de Internet mediante un navegador.

Página web: Documento electrónico escrito con lenguaje HTML para la World Wide Web.

Password: Palabra clave que puede ser necesaria para acceder a algún servicio o aplicación informática.

Periféricos: Son los elementos mediante los cuales el ordenador se comunica con el exterior.

Phishing: Es la contracción de "password harvesting fishing" (cosecha y pesca de contraseñas).Las técnicas denominadas "phishing" consisten en el envío de correos electrónicos, en los cuales el usuario cree que el remitente se trata de una entidad reconocida y seria.

Pirata informático: Persona que copia software ilegalmente y lo comercializa sin licencia.

Programa: Conjunto de instrucciones escritas con un lenguaje de programación que los ordenadores interpretan y facilitan a los usuarios la realización de tareas concretas.

Red: Infraestructura normalmente de cable que permite la interconexión entre los ordenadores ya sea a nivel local, nacional o mundial.

Resetear (reinicializar): Tecnicismo que se utiliza cuando se apaga el ordenador mediante la tecla «reset» (o la combinación «Ctrl+Alt+Supr») al quedarse colgado.

Router: Dispositivo para conectar redes telemáticas y encaminar los paquetes de información hacia su destino. Controla el tráfico en la red.

Servidor: Ordenador central de una red de ordenadores que suministra programas y servicios(impresora, disco duro, conexión a Internet) a otros ordenadores menores llamados clientes.

Sistema operativo: Es el conjunto de programas que nos permiten comunicarnos con el ordenador y ordenarle la ejecución de determinadas tareas: ver lo que hay en un disco, copiar y transferir datos, ejecutar programas.

Software: Es el término que hace referencia a los programas y técnicas de informática propiamente dicha.

Spam o correo no deseado: Todo tipo de comunicación no solicitada, realizada por vía electrónica.

USB (Universal Serial Bus): Bus que permite la conexión de todo tipo de periféricos.

Virus: Programa de ordenador que puede infectar otros programas o modificarlos para incluir una copia de sí mismo.

WEB: Forma abreviada de designar la World Wide Web.

Wi-Fi : Red inalámbrica por microondas.

(León, 2004)

ANEXOS

Anexo 1- Certificado de la implementación de la propuesta.

INSTRUMENTAL
& OPTICA

Quito, 25 de enero de 2016

CERTIFICADO

Por medio de la presente certifico que el Sr. Joffre Díaz Cobos con número de cédula 1715956460 ha culminado exitosamente la socialización e implementación del Manual de Políticas de Seguridad en nuestra empresa. Es todo cuanto puedo decir a la verdad. El suscrito puede hacer uso del presente para los fines pertinentes.

Atentamente,

INSTRUMENTAL Y OPTICA
Representaciones M. P. Cía. Ltda

Ingeniero Iván Pazmiño
GERENTE GENERAL

Anexo 2 - Manual de políticas de seguridad

INSTRUMENTAL & ÓPTICA

MANUAL DE POLÍTICAS DE SEGURIDAD

AGOSTO DE 2016

INDICE

Introducción.

El presente manual detalla algunas políticas de seguridad que deberán de ser cumplidas por el personal de la compañía Instrumental y Óptica, y ha sido desarrollado en base a la problemática que existe frente a la seguridad de la información que maneja y aun estudio investigativo por parte de Joffre Germán Díaz Cobos y reflejado en las encuestas aplicadas a colaboradores, clientes y proveedores, de tal manera que ayuden a precautelar el correcto uso del recurso informático y tener a buen recaudo la información de la compañía.

Debido a los altos índices de inseguridad que vemos reflejados en la tabulación de las encuestas, es de carácter obligatorio, que tanto el recurso informático y de datos se protejan de varias maneras, unas de estas es aplicando cambios en el manejo de estos, porque debemos damos cuenta que el eslabón más frágil de una cadena, es el recurso humano, pues podemos tener varios controles de software, pero si uno de ellos declina ante algo tan simple o se salta de alguna de estas políticas de seguridad propuestas, lo más posible es que se vea afectada la compañía con importantes pérdidas. Por ello lo más destacable es instaurar una cultura de protección, ante los delitos a los que nos enfrentamos, incluso de esta manera se lleva un orden con respecto a la manipulación del hardware y tener a buen recaudo la información, para que estos siempre estén disponibles.

Glosario de términos

Almacenamiento en la nube (Cloud Computing)

Con el trabajo en la nube (Cloud Computing), físicamente el usuario no manipula el dispositivo, sino que por medio de una conexión a Internet, tiene la capacidad de utilizar los datos disponibles en servidores dedicados a ello (esto no quiere decir que los medios de almacenamiento final no existan).Ejemplos de lo anterior es el uso de datos almacenados en el correo electrónico Yahoo®, el uso de suites ofimáticas como Microsoft® Office bajo la plataforma de Microsoft® Hotmail, el uso de antivirus como Panda Cloud® que tienen las firmas de virus no instaladas en el equipo sino en varios servidores, almacenamiento de archivos como Google® Drive, etc. Fuente: (Informática moderna, 2008)

Antivirus

Un antivirus es un programa informático que tiene el propósito de detectar y eliminar virus y otros programas perjudiciales antes o después de que ingresen al sistema. Fuente: (El equipo de Definición ABC, 2015)

Base de datos

Una base de datos es el conjunto de datos informativos organizados en un mismo contexto para su uso y vinculación. Se le llama base de datos a los bancos de información que contienen datos relativos a diversas temáticas y categorizados de distinta manera, pero que comparten entre sí algún tipo de vínculo o relación que busca ordenarlos y clasificarlos en conjunto. Una base de datos puede ser de diverso tipo, desde un pequeño fichero casero para ordenar libros y revistas por clasificación alfabética hasta una compleja base que contenga datos de índole gubernamental en un Estado u organismo internacional. Recientemente, el término base de datos comenzó a utilizarse casi exclusivamente en referencia a bases construidas a partir de software informático, que permiten una más fácil y rápida organización de los datos. Las bases de datos informáticas pueden crearse a partir de software o incluso de forma online usando Internet. En cualquier caso, las funcionalidades disponibles son prácticamente ilimitadas. Fuente: (El equipo de Definición ABC, 2015)

Contraseña

Una contraseña es una cadena de caracteres que se puede usar para iniciar sesión en un equipo y obtener acceso a archivos, programas y otros recursos. Las contraseñas ayudan a garantizar que no se pueda obtener acceso a un equipo si no se tiene la autorización para hacerlo. En Windows, una contraseña puede estar formada por letras, números, símbolos y espacios. Las contraseñas de Windows también distinguen mayúsculas de minúsculas. Para ayudar a mantener protegida la información en el equipo, no debe comunicar su contraseña a nadie, ni anotarla en un lugar donde otros puedan verla. Fuente: (Microsoft, 2014)

Correo electrónico

El correo electrónico o email es un servicio que sirve para enviar y recibir mensajes en forma rápida y segura a través de un canal electrónico o informático. En informática, el correo electrónico es un servicio de red que permite que dos o más usuarios se comuniquen entre sí por medio de mensajes que son enviados y recibidos a través de una computadora o dispositivo afín. El correo electrónico es una de las funcionalidades más utilizadas de Internet, ya que contribuye a comunicaciones veloces, confiables y precisas. (El equipo de Definición ABC, 2015)

Correo institucional

Es muy similar al correo electrónico, con la diferencia que se usa para asuntos de índole comercial, haciendo referencia a dominio de la compañía.

Dominio

Un dominio o nombre de dominio es el nombre que identifica un sitio web o empresa. Cada dominio tiene que ser único en Internet. Por ejemplo, "www.instrumentalyoptica.com.ec" es el nombre de dominio de la página web de la compañía Instrumental y Optica. Un solo servidor web puede servir múltiples páginas web de múltiples dominios, pero un dominio sólo puede apuntar a un servidor. Fuente: (El equipo de Definición ABC, 2015)

Departamento de Sistemas

El Departamento de Sistemas es el que ofrecen la mayoría de las soluciones informáticas, sin embargo es llamado también Departamento de informática por ser

precisamente el proveedor de información. El trabajo medular de un Departamento de sistemas, es conocer los sistemas de información que abarca tanto perspectivas técnicas como conductuales, destacando la conciencia de las dimensiones de administración, organización y tecnológicas de los mismos. Los sistemas de información definen cinco retos claves para los administradores de hoy día: el reto del negocio estratégico; el reto de la globalización, el reto de la arquitectura de la información; el reto de la inversión en sistemas de información y el reto de la responsabilidad y control. Fuente: (Bonifaz, 2015)

Dispositivos de almacenamiento masivo

Se trata de cualquier dispositivo electromecánico ó electrónico, capaz de guardar a largo plazo información generada por los usuarios, sin importar su origen u objetivos de tales datos. Actualmente existe una gran gama de productos destinados a este fin, clasificados de acuerdo a sus principios de almacenamiento, tales como mecánicos, magnéticos, digitales, ópticos y mixtos. Fuente: (Informática moderna, 2008)

Fase (Electricidad)

A instancias de la electricidad, las fases, corresponden a cada uno de los circuitos en una corriente alterna, siendo el caso que presenta una corriente de tipo polifásica, es decir, que ostenta varias fases en lugar de una sola. Fuente: (El equipo de Definición ABC, 2015)

GPS y GNSS

Las siglas GPS se corresponden con "Global Positioning System" que significa Sistema de Posicionamiento Global (aunque sus siglas GPS se han popularizado el producto en el mundo comercial. En síntesis podemos definir el GPS como un Sistema Global de Navegación por Satélite (GNSS) que nos permite fijar a escala mundial la posición de un objeto, una persona, un vehículo o una nave. Fuente: (Sucuzhañay, 2015)

Estaciones de referencia

Una estación de referencia proporciona al usuario los datos diferenciales necesarios para obtener la precisión requerida en nuestro equipo móvil, ya sea para postproceso o para tiempo real. La mayoría de los usuarios montan en el campo su estación de referencia GNSS cada día, pero éste es un esfuerzo innecesario con las estaciones de referencia GNSS permanentes. Fuente: (Leica, 2015)

Hardware

Literalmente, "hardware" significaría "mercancía dura". Con este concepto se intenta designar a todos los componentes tangibles en un sistema electrónico, es decir, lo que podemos tocar: teclado, mouse, monitor, chips, placas, impresoras, etc. Se podría realizar una analogía con el ser humano y decir que el software es el pensamiento, mientras que el hardware es el cuerpo. Fuente: (El equipo de Definición ABC, 2015)

Hosting

En los últimos años, el término de hosting cobró presencia relevante en el ámbito de la informática y las nuevas tecnologías dado que allí se lo utiliza para designar al servicio que una empresa ofrece a los usuarios de internet para que almacenen información sobre su página web, por ejemplo, entre otros contenidos, imágenes, documentos, videos, entre otros. El servidor dispone de toda esa información y es posible su acceso a través de internet. Vale mencionarse que a este servicio se lo denomina también como alojamiento web. Fuente: (El equipo de Definición ABC, 2015)

Infraestructura

Es el conjunto de hardware y software sobre el que se asientan los diferentes servicios que la compañía necesita tener en funcionamiento para poder llevar a cabo toda su actividad de negocios, investigación o de gestión interna. Fuente: (Catalunya, 2015)

Mantenimiento correctivo

El concepto de mantenimiento designa a aquellas acciones, actividades, que tienen como finalidad la mantención de un aparato, una maquinaria, un producto, entre otros, o en su defecto la restauración de alguno de éstos para que el mismo pueda desplegar su funcionalidad de modo satisfactorio. Fuente: (El equipo de Definición ABC, 2015)

Mantenimiento preventivo

Y en el mantenimiento preventivo, como su denominación ya nos lo anticipa, lo que se realiza es una comprobación que garantice el funcionamiento del equipo para evitar la sucesión de la falla. Fuente: (El equipo de Definición ABC, 2015)

Navegadores GPS

Un navegador GPS, un sistema de guía en tiempo real capaz de llevarnos a un determinado lugar, gracias a las indicaciones verbales y visuales que facilita. Un Navegador GPS planifica y analiza las posibles rutas hacia un determinado destino y establece el camino más indicado, de acuerdo a unos criterios más o menos definibles. (Leica, 2015)

Neutro (Electricidad)

Es el punto necesario por donde retorna la corriente que es enviada por la fase, que alimenta la carga y cierra el circuito.

Personal interno

Personas que son colaboradoras de la empresa o que trabajan en esta para un fin económico.

Personal externo

Personas que son colaboradoras de la empresa que no trabajan dentro de ella, sean estos clientes, proveedores, etc.

Rack

Rack es un término inglés que se emplea para nombrar a la estructura que permite sostener o albergar un dispositivo tecnológico. Se trata de un armazón metálico que, de acuerdo a sus características, sirve para alojar una computadora, un router u otro tipo de equipo. (Definición de, 2008)

Red

La red informática nombra al conjunto de computadoras y otros equipos interconectados, que comparten información, recursos y servicios. Puede a su vez dividirse en diversas categorías, según su alcance (red de área local o LAN, red de área metropolitana o MAN, red de área amplia o WAN, etc.), su método de conexión (por cable coaxial, fibra óptica, radio, microondas, infrarrojos) o su relación funcional (cliente-servidor, persona a persona), entre otras. (Definición de, 2008)

Red inalámbrica - Wifi

Las redes WiFi resultan especialmente útiles en los casos que no admiten el uso de cables; por ejemplo, son muy usadas en salas de conferencia y exhibiciones internacionales,

y también son ideales para edificios considerados monumentos históricos, donde sería inaceptable realizar el cableado necesario para el uso de Internet. (Definición de, 2008)

Regulador

Los reguladores permiten mantener el voltaje de la salida fijo independiente de las variaciones de carga o ondulación de la entrada. Las características se especifican a través del porcentaje de regulación. (Informática moderna, 2008)

Servidor

Los servidores suelen utilizarse para almacenar archivos digitales. Los clientes, por lo tanto, se conectan a través de la red con el servidor y acceden a dicha información. En ocasiones, un ordenador puede cumplir con las funciones de servidor y de cliente de manera simultánea. (Definición de, 2008)

Software

El software es una palabra que proviene del idioma inglés, pero que gracias a la masificación de uso, ha sido aceptada por la Real Academia Española. Según la RAE, el software es un conjunto de programas, instrucciones y reglas informáticas que permiten ejecutar distintas tareas en una computadora. (Definición de, 2008)

Software downgrade

Significa devolver el software a una antigua versión. A menudo, programas complejos pueden necesitar ser downgradeados para eliminar partes con fallos, y para incrementar velocidad y/o facilidad de uso.

Software upgrade

Significa ascender al software a una versión superior. A menudo, programas complejos pueden necesitar ser actualizaos para eliminar partes con fallos, y para incrementar velocidad y/o facilidad de uso.

Soporte técnico topográfico.

La Real Academia Española da como definición "persona que profesa el arte de la topografía o tiene en ella especiales conocimientos". Entendiendo por topografía: "arte de describir y delinear detalladamente la superficie de un terreno; conjunto de particularidades

que presenta un terreno en su configuración superficial." Entonces es el personal especializado en dar soluciones en este ámbito.

Toma a tierra

El propósito de aterrar los sistemas eléctricos es limitar cualquier voltaje elevado que pueda resultar de rayos, fenómenos de inducción o de contactos no intencionales con cables de voltajes más altos. Esto se realiza mediante un conductor apropiado a la corriente de falla a tierra total del sistema, como parte del sistema eléctrico conectado al planeta tierra. (Rojas, 2010)

UPS

Sistema de alimentación ininterrumpida (SAI), en inglés uninterruptible power supply (UPS), es un dispositivo que gracias a sus baterías u otros elementos almacenadores de energía, puede proporcionar energía eléctrica por un tiempo limitado y durante un apagón eléctrico a todos los dispositivos que tenga conectados. Otras de las funciones que se pueden adicionar a estos equipos es la de mejorar la calidad de la energía eléctrica que llega a las cargas, filtrando subidas y bajadas de tensión y eliminando armónicos de la red en el caso de usar corriente alterna. (Informática moderna, 2008)

Usuario

Un usuario es «aquél que usa algo» o «que usa ordinariamente algo». Es preferible, por tanto, hablar de actores, sujetos, ciudadanos, etc. para referirse a las personas que interactúan en las redes digitales

Virus informático

Son programas que pueden replicarse y ejecutarse por sí mismo. En su accionar, suelen reemplazar archivos ejecutables del sistema por otros infectados con el código maligno. Los virus pueden simplemente molestar al usuario, bloquear las redes al generar tráfico inútil o, directamente, destruir los datos almacenados en el disco duro del ordenador. (Definición de, 2008)

Políticas para el mantenimiento del los equipos informáticos.

- El jefe del departamento de sistemas se encargará de realizar una planificación para los mantenimientos del equipo informático.
- Las únicas personas autorizadas para realizar un mantenimiento en los equipos informáticos, son los técnicos del departamento de sistemas.
- El departamento de sistemas le notificará al usuario, con una semana de antelación cuando se vaya a realizar un mantenimiento en su equipo.
- Si en el equipo hay que realizar un mantenimiento correctivo, el técnico asignado se encargará de obtener los respaldos correspondientes.
- El mantenimiento de equipos informáticos y rack se lo realizará fuera de las horas de trabajo.
- El personal del departamento de sistemas será el responsable de realizar una actualización mensual del sistema operativo.
- Si el caso amerita de enviar el equipo informático, con personal externo para el reemplazo de piezas, se deberá tomar las siguientes medidas:
    - Sacar respaldo de toda la información de ser posible.
    - Entregar un equipo provisional y recuperar la información del usuario.
    - Borrar toda la información de los discos o disco duro.
    - De no ser posible sacar respaldo de la información, por daños en el disco, extraer el disco duro y no entregar a el personal externo.
    - Solicitar una credencial y una orden de trabajo del equipo donde consten todos los accesorios y números de series de los componentes de equipo o equipos entregados.
    - Solicitar una proforma de los costos generados de dicho daño.
    - El jefe de sistemas debe solicitar la autorizar con la gerencia administrativa, de dicha proforma para proceder con la reparación.
    - Cuando el equipo regrese a la compañía el personal del departamento de sistemas deberá entregar totalmente operativo el equipo informático.

    - El departamento de sistemas será el encargado de trasladar la información del equipo temporal al equipo entregado al usuario.
- Si el equipo tiene fallas y debe ser revisado, notificarlo con el jefe de sistemas.
- El rack debe contener un sistema de ventilación, el cual será chequeado periódicamente.
- El personal del departamento de sistemas no hará mantenimientos preventivos ni correctivos sobre los equipos informático que pertenezcan a los colaboradores de la compañía.

Política para el control y mantenimiento de la calidad de la energía eléctrica suministrada.

Calidad de la energía suministrada

- El cableado que llegue a cada punto de toma eléctrica deberá llevar tres cables, uno de la fase, neutro y tierra.
- Los cables deberán respetar la siguiente norma de color, rojo para el cable de fase, negro para el neutro y verde o verde con anillos amarillos para el de tierra.
- La toma eléctrica o tomacorriente deberá ser de dos polos (fase, neutro) y tierra.
- Los cables serán conectados al tomacorriente en forma ordenada para que la toma alimente correctamente y el circuito este debidamente polarizado.
- El circuito de tomacorrientes para el equipo informático será independientemente de los demás.
- El tablero principal será conectado un UPS con regulador, para no permitir el corte abrupto de energía eléctrica, dando tiempo para apagar los equipos informáticos.
- Los tomacorrientes donde se conectan los equipos informáticos, serán exclusivamente para conectar estos, está prohibido conectar cualquier dispositivo diferente a ellos, para prevenir riesgos laborales y en los equipos.

- Los tomacorrientes serán debidamente rotulados con un código de identificación y mostrar el valor nominal de voltaje que proveen.
- La toma a tierra será instalada con una caja de revisión.
- La voltaje a tierra será medida continuamente por el personal del departamento de sistemas.

Continuidad de la energía suministrada

- El sistema de UPS será usado exclusivamente para equipos informáticos (computadoras) con excepción de impresoras.
- El sistema UPS da un tiempo máximo de operación de 15 minutos.
- Si existe un corte de energía el equipo UPS no tiene la utilidad de alargar su jornada de trabajo, solo le permitirá guardar su trabajo que estaba realizando en ese momento y apague sus equipos.

Políticas para la interacción sobre el internet

Manejo del correo institucional.

- La configuración del correo institucional estará a cargo del personal del departamento de sistemas.
- El correo institucional será usado para fines de comunicación interna y externa estrictamente laboral.
- El correo institucional no será usado como chat personal.
- Es de responsabilidad del usuario el depurar el correo institucional de correos no deseados, publicidad inservible, pues esto ocasiona acumulación de información en los servidores de respaldos.
- El correo institucional ha sido creado en función de la estructura de la empresa, haciendo alusión en varios casos a nombre y apellido del usuario, por lo tanto será de responsabilidad del usuario el buen uso de este.

- No se usará el correo institucional para emitir algún comentario o documento que contenga palabras groseras o con el afán de calumniar, acosar ni amenazar al personal interno y externo relacionado con la compañía.
- El correo institucional es de derecho intransferible, por lo tanto nadie más que el usuario debe conocer el usuario y contraseña.
- Todos los documentos adjuntos que se emitan por medio del correo institucional serán enviados en un formato no editable.
- No se permite que los usuarios envíen correos electrónico no solicitado o cadenas de spam, con propósitos comerciales, personales, informativos, publicitarios, políticos y religiosos entre otros.
- Es obligación del usuario de revisar periódicamente su correo institucional, en los días y horarios hábiles.

Buen uso de la web.

- El internet debe ser usado solo con fines investigativos y de consulta.
- En los exploradores no se abrirá páginas web de contenidos de dudosa procedencia tales como sitios pornográficos, religioso, medios de comunicación o violencia ni nada que no tenga que ver con los intereses de la empresa.

Uso de mensajería electrónica y uso de redes sociales.

- El uso de la mensajería electrónica será habilitada siempre y cuando así lo requiera su trabajo y previamente autorizado por el jefe inmediato.
- El uso de redes sociales será permitido para el usuario y equipo informático que así lo requiera, exclusivamente para manejar cuentas de redes sociales de la compañía.

Políticas para el acceso, infraestructura y seguridad de las redes informáticas.

Buen uso de la red inalámbrica.

- Los equipos que se conecten a la red inalámbrica de la oficina, deberán ser autorizados por la gerencia administrativa, para posterior a esto ingresar a la red.

- No es permitido que los colaboradores de la empresa se conecten a la red inalámbrica mediante computadores portátiles, teléfonos inteligentes u otros dispositivos de su propiedad, que puedan bajar la banda del servicio.
- El conocimiento de la clave de la red inalámbrica de la oficina es de uso exclusivo del jefe del departamento de sistemas.

Manejo de dispositivos ajenos a la compañía que se conecten a la red inalámbrica.

- Los dispositivos ajenos a la compañía (clientes, colaboradores, etc.) podrán conectarse a la red inalámbrica "usuarios", que ha sido creada para este fin.
- Para el ingreso de un dispositivo ajeno a la compañía será notificado al jefe de sistemas, para poder ingresar el dispositivo en la base de datos y otorgar permiso de conexión.
- La clave de la red inalámbrica para dispositivos ajenos a la compañía, será cambiada cada que lo amerite.
- Por ningún motivo un dispositivo ajeno a la compañía podrá formar parte de la red interna, y transferir archivos.

Política para la adquisición de equipos informáticos.

- El departamento de sistemas será quien valide las especificaciones técnicas de los equipos que van a ser adquiridos en base a la necesidad del usuario y eficiencia del trabajo.
- Los costos del equipo informático que va a ser adquirido deberán de ser conforme al costo de mercado.
- Los equipos adquiridos serán de marca conocida en el mercado.
- Los equipos adquiridos constarán en el de una garantía técnica de no menos de 1 año.
- El proveedor donde se adquieran los equipos, deberá tener un tiempo de operación en el mercado de no menos de 10 años.
- El proveedor deberá ser distribuidor exclusivo de la marca del equipo a adquirirse.

Políticas para la instalación de software.

- Si se requiere comprar un software, lo hará el departamento de adquisiciones, con la respectiva aprobación de jefe inmediato, para posteriormente ser instalado por el personal del departamento de sistemas.
- Todo el software será instalado por el personal del departamento de sistemas.
- Si un equipo requiere ser reinstalado este deberá contar con las licencias vigentes.
- El software que se instalará en las computadoras deberán tener su respectiva licencia.
- El jefe de sistemas deberá tener en un lugar seguro las licencias de todos los equipo y realizar una base de datos de estas licencias respectivamente codificadas.
- De la misma manera los upgrades y downgrades serán llevados por el jefe de sistemas en la base de datos de licenciamiento.
- Anualmente el departamento de sistemas deberá realizar un inventario del software instalado en los equipos informático.
- Si el software o actualización instalada no es de conocimiento para el usuario, este deberá solicitar mediante correo electrónico a su jefe inmediato copia al jefe del departamento de sistemas la capacitación de uso de este. Posterior a la aprobación, se realizará una planificación para la respectiva capacitación, de tal manera de convertir este software en una herramienta potencial de su trabajo.
- Si nota que existe algún software que no usa o que ha sido instalado automáticamente, de manera inmediata debe ser reportado al departamento de sistemas.
- Ninguna de las personas que conforman el departamento de sistemas, está autorizada a instalar, software sin licencia e ilegal en los equipos de la compañía.
- El personal del departamento de sistemas no hará instalaciones de software legal o pirata sobre los equipos informáticos que pertenezcan a los colaboradores de la compañía.

Políticas para la instalación de hardware.

- Los equipos de escritorio y portátiles deberán ser instalados por personal del departamento de sistemas.
- Los equipos de escritorio y portátiles deben ser configurados e ingresados a la red por el personal del departamento de sistemas.
- Los equipos de escritorio y portátiles deberán estar colocados en un lugar seco y fuera de humedad.
- El departamento de sistemas realizará una base de datos con la ubicación, características y usuario del equipo.

Políticas de ubicación y reubicación de equipos informático.

- Solo el personal del departamento de sistemas será el encargado de desconectar, movilizar y reubicar el equipo informático.
- En el caso que un equipo de escritorio o portátil deba salir de las instalaciones de la compañía, el jefe del departamento de sistemas será el encargado de realizar una constancia de entrega del equipo en el estado que se encuentra, junto a una acta de responsabilidad por daños, perdida de información o mal uso de esta, previo a la autorización del jefe inmediato.
- Para que un equipo informático sea dado de baja, deber ser justificado por el informe del jefe de sistemas, conjuntamente con la autorización por escrito de la gerencia administrativa.

Políticas para el manejo y seguridad de la información

Respaldo de la información.

- Los usuarios están en la obligación de realizar los respaldos correspondientes a su información, como el departamento de sistemas se lo indique.
- Si el usuario envía la computadora al departamento de sistemas, para su respectivo mantenimiento correctivo o preventivo, deberá primeramente realizar un respaldo

de la información más sensible o importante, si es posible, en dvd´s, de ninguna manera el respaldo deberá ser alojado en el mismo disco duro.

- Los respaldos en dvd´s deben ser entregados a la jefe del departamento de sistemas de manera oportuna, de ninguna manera deberán llevarse fuera de la oficina.
- Será responsabilidad del departamento de sistemas realizar un respaldo manual de la información cada fin de mes, sin interrumpir las labores diarias.
- El departamento de sistemas será el encargado de realizar el respaldo manual y semanal de las bases de datos del sistema de gestión contable y facturación.
- El personal del departamento de sistemas se encargará de instaurar un método, para que los respaldos de cada computadora sean sacados de forma automática cada mes y subidos al dispositivo cloud, para su permanencia en la nube.
- La información del correo institucional será respaldará en el mismo hosting por un período de seis meses.
- Si algún dvd de respaldos es encontrado, debe reportarlo de manera inmediata al jefe del departamento de sistemas.
- Si algún dvd se ha dañado el momento de grabarlo, debe destruirlo antes de botarlo a la basura.
- Es de responsabilidad de cada usuario el mantener a buen recaudo la información de equipo informático y la confidencialidad de la misma.

Políticas para el manejo de la información suministrada por personal externo a la compañía.

Uso de dispositivos de almacenamiento masivo personal interno

- Se debe analizar con el antivirus vigente, todo dispositivo de almacenamiento masivo proveniente por el personal interno de la compañía.
- No se permite el uso de dispositivos de almacenamiento masivo en el interior de la compañía, o la transferencia de datos por estos medio.
- Los discos duros externos serán de uso exclusivo por el personal de soporte técnico topográfico.

- Los cd's y dvd's serán de uso solo para respaldar información no para transferir datos de un equipo informático a otro.

Uso de dispositivos de almacenamiento masivo personal externo

- Se debe analizar con el antivirus vigente, todo dispositivo de almacenamiento masivo proveniente por el personal externo a la compañía.
- Los únicos equipos informáticos que tendrán acceso para usar dispositivos de almacenamiento masivo es el personal del soporte técnico topográfico, con el afán de transferir solamente archivos de estaciones de referencia, navegadores y equipos GPS.
- Se permite el uso de dispositivos de almacenamiento masivo, estrictamente para transferir trabajos realizados por parte de la compañía, hacia el cliente en mención.

Política para la selección y mantenimiento del software antivirus.

- El software antivirus será seleccionado por el jefe del departamento de sistemas, en base a un análisis técnico y crítico sobre las prestaciones, ventajas y desventajas.
- El software antivirus será instalado siempre y cuando tenga una licencia y funcionará de acuerdo al criterio del jefe de sistemas, en red o de forma individual en cada equipo.
- El usuario del equipo de cómputo de ninguna manera deshabilitará el antivirus, ni hará caso omiso, a las advertencias de detección de virus.
- Si por algún motivo el antivirus no puede eliminar automáticamente el virus detectado, inmediatamente se acercará al departamento de sistemas para solicitar soporte.
- Al notar que en su equipo informático o de algún compañero, el antivirus se ha deshabilitado automáticamente, de manera inmediata debe ser reportado al departamento de sistemas.
- Si equipo informático de alguna forma se ha vuelto lento o sospecha que está infectado, debe repórtalo al departamento de sistemas.

- El usuario está en la obligación de por lo menos una vez a la semana realizar un escaneo de la información mediante el antivirus, si nota alguna irregularidad, notifíquelo al departamento de sistemas.
- Dentro de un periodo de treinta días el personal del departamento de sistemas, revisará el estado de funcionamiento, actualizaciones automáticas y bóveda de virus dentro del software antivirus vigente.

Políticas para el monitoreo de computadora (s) por parte de soporte externo.

- Si el soporte es presencial, una persona del departamento de sistemas hará el acompañamiento del personal de soporte externo, para solventar alguna duda, permisos del equipo o salvaguardar la información encontrada en el equipo.
- Si el soporte es virtual, una persona del departamento de sistemas se encontrará en el equipo informático intervenido, para solventar alguna duda, permisos del equipo o salvaguardar la información encontrada en el equipo.
- Por ningún motivo se dará soporte virtual, cuando no exista personal del departamento de sistemas presente, o fuera de horas de oficina.
- Si se requiere tener acceso a los equipos informáticos virtualmente o presencialmente fuera de los horarios de oficina, se los realizará con carta de autorización a la gerencia administrativa y el jefe del departamento de sistemas asignará un técnico para que se encuentre en la intervención.

Políticas para establecer contraseñas

- Es responsabilidad del jefe de sistemas la creación de contraseñas y de mantener de una forma segura un banco de todas las contraseñas de forma encriptada.
- La contraseña es de uso único e intransferible, no podrá de ninguna manera ser igual a la de otro usuario.
- Las contraseñas tendrán un tiempo de vigencia de tres meses, y no podrán volverá ser las mismas al momento de cambiar y estará a cargo del departamento de sistemas.

- La contraseña deberá tener al menos 8 caracteres y máximo 16.
- Los caracteres que deben ocupar para la creación de contraseñas serán: alfanumérica, usando mayúsculas y minúsculas además de caracteres especiales ejm: Y3m8A-9e*\5JhI
- Si usted sospecha que su contraseña ha sido adivinada o copiada debe solicitar el cambio al jefe de sistemas.
- Jamás use fechas importantes, nombres de parientes o el suyo, lugares de nacimiento, cargo que desempeña para generar una contraseña.
- Si olvida la contraseña solicite al jefe de sistemas que le reinicie y le otorgue otra.
- No colocar la contraseña en cuadernos, agendas o notas.

Cuidados para el manejo de la banca electrónica

- Si usted tiene a su cargo una tarjeta de coordenadas debe guardarla en un lugar seguro, por ningún motivo debe entregarla a nadie.
- Si llega un correo de parte del banco solicitando alguna coordenada de la tarjeta, sin que usted haya realizado ninguna transacción, reporte inmediatamente el correo al departamento de sistemas, para su verificación.
- De ninguna manera deberá mantener un documento dentro de su equipo informático, que contenga usuarios y contraseñas de los bancos que maneje.
- Si usted va a ingresar a la banca virtual desde su teléfono inteligente, recuerde bajar el software de sitios seguros como App Store, App World o Google Play.
- Si usted duda del lugar de donde el banco le solicita descargar la aplicación, diríjase al departamento de sistemas.
- De llegarle un correo electrónico del banco, solicitándole usuario, contraseña, usuario biométrico o actualizar los datos, solicite asistencia al departamento de sistemas para verificar la autenticidad de la página visitada o el correo que lo solicita, por lo general los bancos nunca requieren este tipo de información.
- Es de suma importancia que en el celular donde va a instalar la aplicación bancaria tenga un antivirus instalado y certificado por el departamento de sistemas.

- Solo el gerente financiero tendrá acceso a generar una nueva clave bancaria.
- Al momento de registrar el correo en el banco, el correo deberá ser el institucional y del gerente financiero.
- Las transferencias bancarias se realizarán en una sola computadora de preferencia de escritorio y debe operarla el gerente financiero, de esta manera registrar el IP de la computadora en el banco.

Anexo 3 - Encuesta sobre delitos Informáticos, clientes, proveedores.

Esta encuesta es completamente anónima y forma parte de una investigación sobre delitos informáticos, estos resultados serán tabulados para ofrecer soluciones a esta problemática y de esta manera generar una propuesta para corregir los problemas de inseguridad, en la compañía donde se desarrolla esta investigación.

Favor leer las preguntas y contestar con una sola opción, luego al final dele clic en el botón Enviar:

*Obligatorio

1.- ¿Qué tipo de antivirus tiene la computadora en la que Usted trabaja?

- Antivirus de licencia Pagada
- Antivirus descargado del internet (Gratuito)
- No tiene
- No conozco

2.- ¿Con qué periodicidad se realiza mantenimiento en las computadoras de la empresa donde usted trabaja?

- Una vez al año
- Dos veces al año
- Tres veces al año
- Nunca

3.- ¿Usted descarga en la computadora de su trabajo, música, películas o programas?

- Nunca
- A veces
- Usualmente

4.- ¿Con qué frecuencia le han solicitado a usted o algún colaborador la clave de la red inalámbrica, por parte de personas que visitan la empresa donde usted trabaja?

- Nunca
- De vez en cuando
- A menudo
- Siempre

5.- ¿La computadora que usa en su trabajo, tiene protección contra la pérdida de información en el caso de fallos de energía (UPS)?

- Si
- No
- No se

6.- ¿El trabajo que usted realiza, requiere de conexión a internet?

- Nunca
- De vez en cuando
- Siempre

7.- ¿De qué manera respalda la información que usted maneja en la empresa donde Usted trabaja?

- CD, DVD, Flash memory.
- En la misma computadora.
- En la nube.
- Personal técnico se encarga de respaldar la información.
- No se respalda.

8.- ¿Tiene conocimiento acerca del uso de la firma electrónica en el Ecuador?

- No conozco

- Poco conocimiento
- Si conozco completamente.

9.- ¿Ingresa dispositivos de almacenamiento masivo (flash memory, discos duros externos o memorias SD), en la computadora que usted usa en la empresa, proveniente de personas externas a esta?

- Nunca
- De vez en cuando
- Siempre

10.- ¿Cuándo tiene qué generar una contraseña que usa?

- La misma para varias cosas
- Sus nombres o apellidos o de sus hijos o número de cédula
- Fechas importantes
- Una contraseña segura que nadie podría acertar con ella

11.- ¿Con que frecuencia se cambia la contraseña de la computadora que usa en su oficina?

- No tiene clave
- Nunca se cambia
- Frecuentemente

12.- En la actualidad, en internet abundan correos de dudosa procedencia solicitando información personal, bancaria o que se oriente a una posible estafa. ¿Con que frecuencia usted o alguien cercano ha recibido, solicitudes de este tipo?

- Nunca
- De vez en cuando
- Siempre

13.- ¿Tiene conocimiento si las leyes del Ecuador sancionan los delitos informáticos?

- Si
- No
- No se

14.- ¿Con qué frecuencia usa la banca electrónica?

- No uso banca electrónica
- Una vez al mes
- Una vez por semana
- A diario

15.- ¿Conoce mecanismos de seguridad para manejo de banca electrónica?

- No conozco
- Poco conocimiento
- Si, conozco completamente

16.- ¿En alguna ocasión le han clonado a usted la tarjeta de débito o crédito?

- No tengo tarjetas
- Nunca
- Si

17.- En la definición de contraseñas para el acceso a la banca electrónica u otros sitios que son de riesgo frente amenazas de delitos informáticos, como las conforma:

- Con 6 o menos caracteres
- Con más de 6 caracteres
- Está compuesta solamente por números
- Está compuesta solamente por letras

- ○ Combinación de números y letras
- ○ Combinación de números y letras añadiendo caracteres especiales como + - * ? u otros

18.- ¿Qué tipo de precaución tiene cuando usa una tarjeta de débito o crédito?

- ◉ No tengo tarjetas
- ○ No pierdo de vista a la persona que entrego la tarjeta
- ○ Compro en lugares seguros

19.- ¿Conoce que significan phishing, hacker, cracker?

- ○ No conozco
- ○ Poco conocimiento
- ○ Si, conozco completamente

20.- De existir un manual de referencia con prevenciones de seguridad informática. ¿Usted haría uso de este?

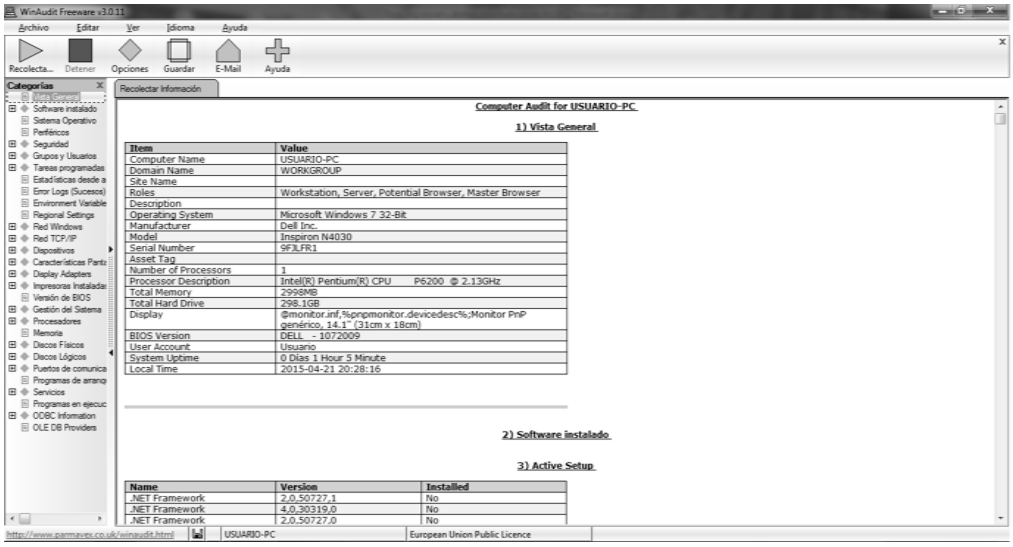
- ○ Nunca
- ○ De vez en cuando
- ◉ Siempre

Anexo 4 – Software Winaudit para auditar los computadores de la compañía Instrumental y Óptica.

1. Es importante tener un control del inventario informático que posee la compañía, para ello hacemos uso del software libre Winaudit. Para ello entramos en la página principal del software https://winaudit.codeplex.com y procedemos a lo descargarlo.

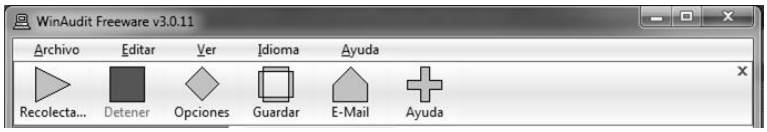
2. Luego le damos doble clic en la aplicación que se descargó, una utilidad de este software es que no se debe instalar, solo se ejecuta.

3. Al momento que lo ejecutamos automáticamente empieza hacer un escaneo de todo el equipo, tal y como se puede observar en el gráfico.



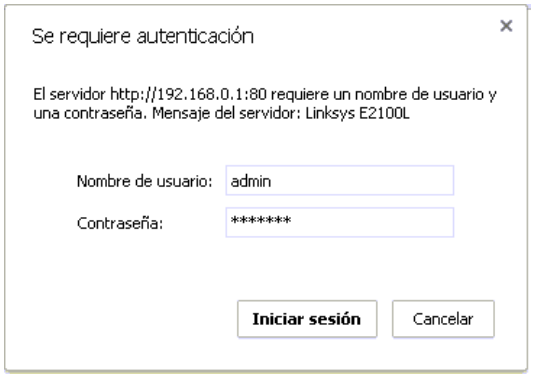
4. En el gráfico anterior se puede observar una vista general del equipo donde se pude observar si usamos las demás opciones del panel izquierdo el software instalado, sistema operativo, periféricos, seguridad, grupos y usuarios, tareas programadas, red Windows, red TCP/IP, Dispositivos, características y pantalla, adaptadores y displays, impresoras instaladas, gestión del sistema, procesadores, discos físicos, lógicos, puertos de comunicación, servicios e información ODBC.

5. Adicional a ello para mantener en una base de datos esta información se puede elegir la opción de guardar en formatos .csv, rtf y html.

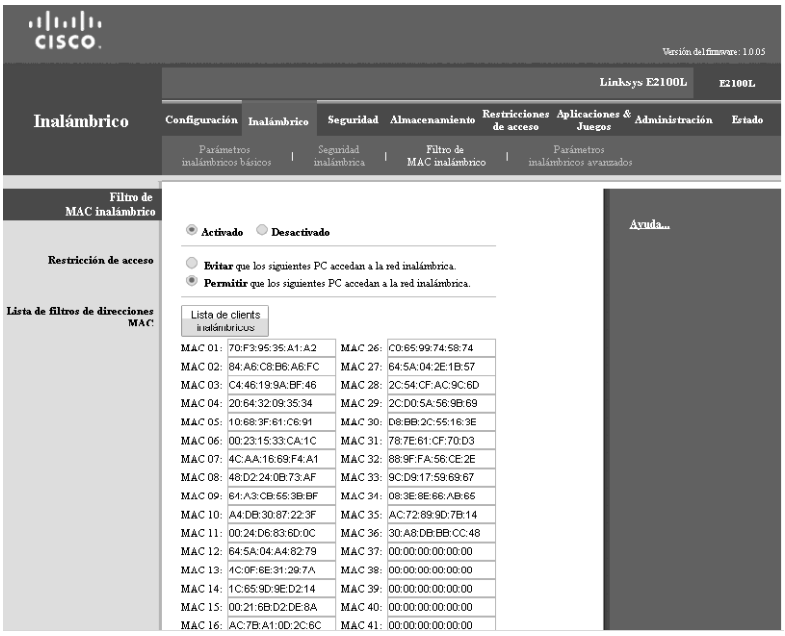


Anexo 5 – Software del Router Cisco Linksys E2100L para poder limitar las conexiones de los dispositivos inalámbricos que se conectan a la red de la compañía Instrumental y Óptica y tener un control.

1. Para ingresar al router ingresamos a la siguiente dirección: 192.168.0.1
2. A continuación nos abre una ventana de autentificación donde ingresamos usuario y contraseña, como lo muestra el gráfico.



3. Hemos ingresado al router, posterior a ellos vamos a buscar la pestaña Inalámbrico y dentro de este, clic donde dice filtro inalámbrico MAC. Aquí podemos ver los equipos que están autorizados a conectarse de manera inalámbrica, esta validación se realiza mediante el MAC address, de esta manera tenemos un control de los equipos inalámbricos que están en la red, tal y como lo muestra el gráfico.

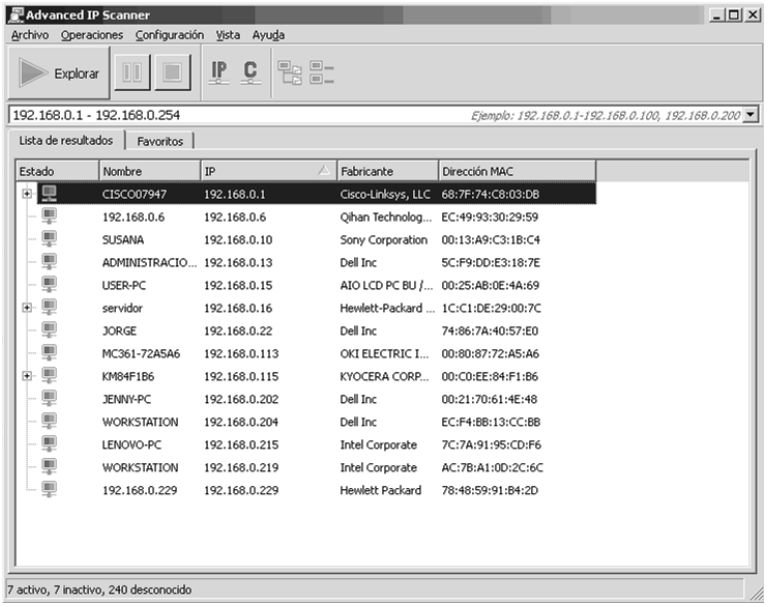


Anexo 6 – Software Advanced IP Scanner permite explorar los dispositivos, computadoras que se encuentran conectados a la red local de la compañía Instrumental y Óptica de esta manera podemos monitorear que intrusos no invadan nuestra red y robar archivos.

1. Para obtener este software gratuito debemos ingresar a la siguiente página: http://www.advanced-ip-scanner.com/es y posterior a esto le damos clic en el botón descargar, posterior a esto se baja el software y se muestra de esta manera, observemos el gráfico.

2. Este software tiene la prestaciones de explora una red, detecta cualquier dispositivo de red, explorar puertos y encontrar recursos HTTP, HTTPS, FTP, RDP y carpetas compartidas, conectarse a ordenadores ejecutando Radmin Server, apagar ordenadores de forma remota, listar favoritos para una administración sencilla de la red. Adicional a esto este software no se instala se lo puede ejecutar desde el disco duro o un dispositivo de almacenamiento masivo de lectura y escritura.

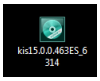
3. Una prestación que tiene es que no es necesario instalarlo, al momento de ejecutarlo se muestra de esta manera dándonos los equipos conectados a nuestra red.



Anexo 7 – Software Kaspersky Internet Security 2015 además de ser un antivirus permite poner controles de páginas web que no se desea que visiten ciertos usuarios y si han intentado entrar a alguna de estas, quedan registradas en un base de datos imposible borrar para el usuario.

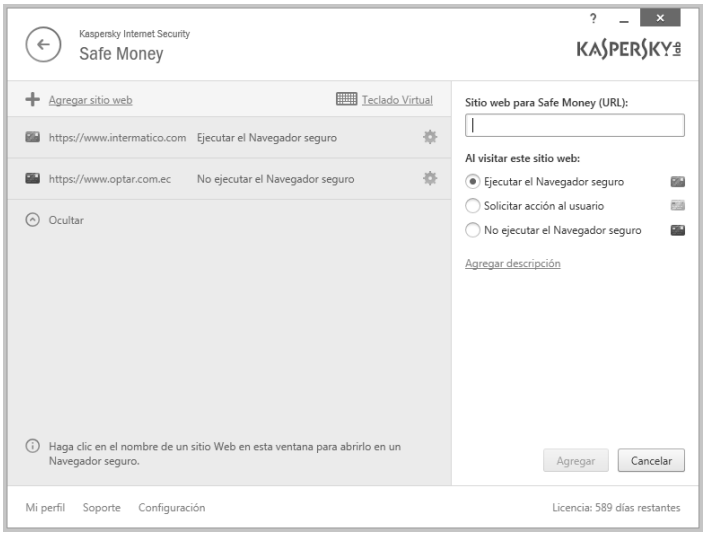
1. A diferencia de los otros programas vistos anteriormente, este si es un software de licencia pagada, pero para bajar un demo por 30 días podemos ingresar en la página http://latam.kaspersky.com/descargas/versiones-de-prueba/internet-security/descargar. Colocamos nuestro correo y le damos clic en el botón Download, para este caso elegimos protección para PC Windows.

2. Esta software es necesario instalarlo

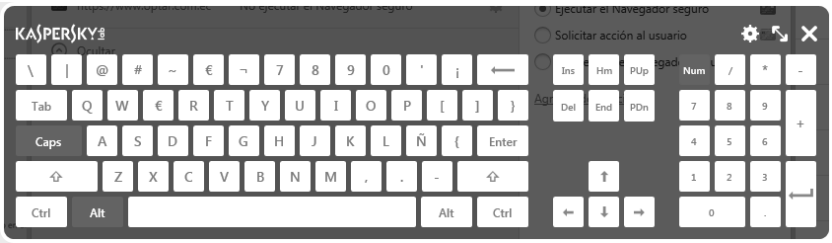


3. Al iniciar el software tenemos el siguiente ambiente, así como lo muestra el gráfico.

4. En el gráfico anterior tenemos claramente un icono que nos ayuda a controlar las páginas de los bancos sean seguras y podemos agregarlas, la opción se llama Safe Money.

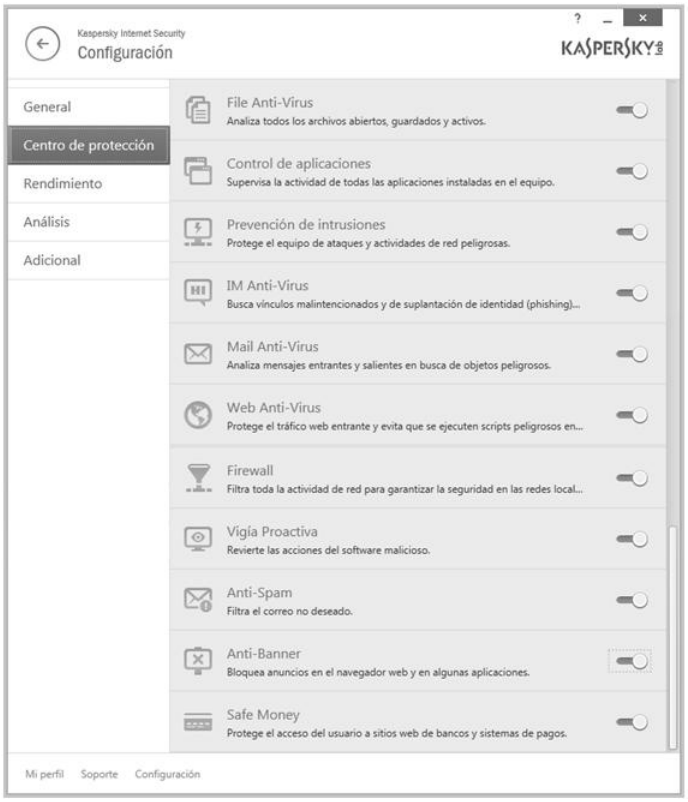


5. Para darnos aún más seguridad contra software que detecta las teclas que nosotros digitamos, podemos abrir el teclado virtual que cuando estemos en una página web y debemos colocar una contraseña, automáticamente se abrirá el teclado virtual.

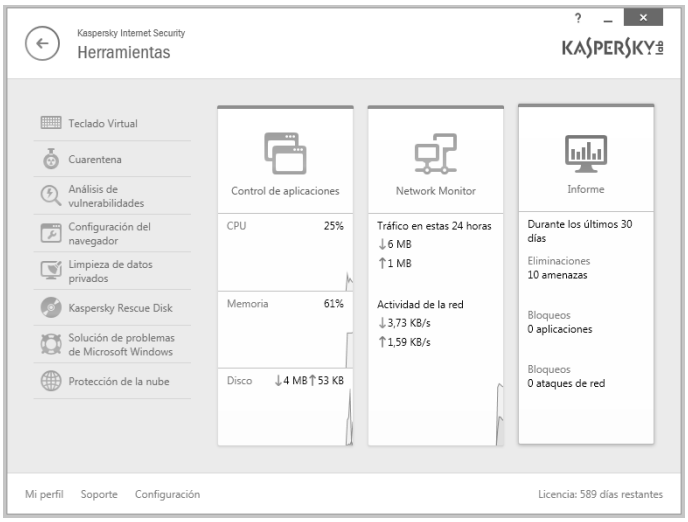


6. Dentro de la configuración podemos configurar el centro de protección, chequear el rendimiento de equipo, análisis y adicional tal y como se muestra en el gráfico.

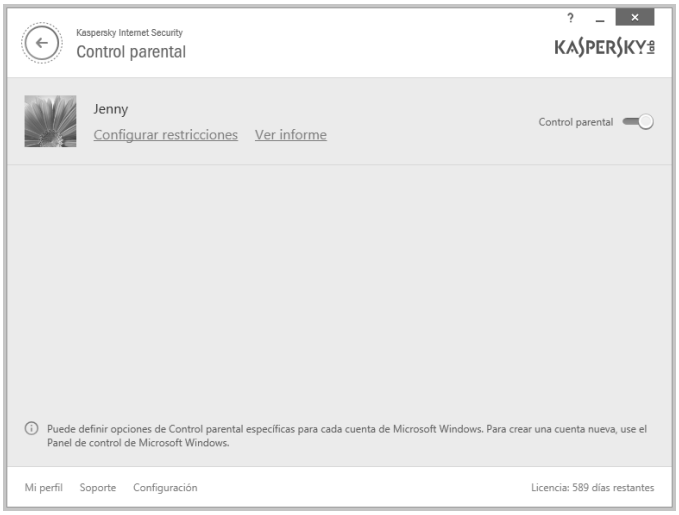
7. Si revisamos el centro de protección podemos observar que hay algunas opciones de seguridad que podemos habilitar o deshabilitar, por defecto están todas las protecciones deshabilitadas, así como muestra el gráfico.



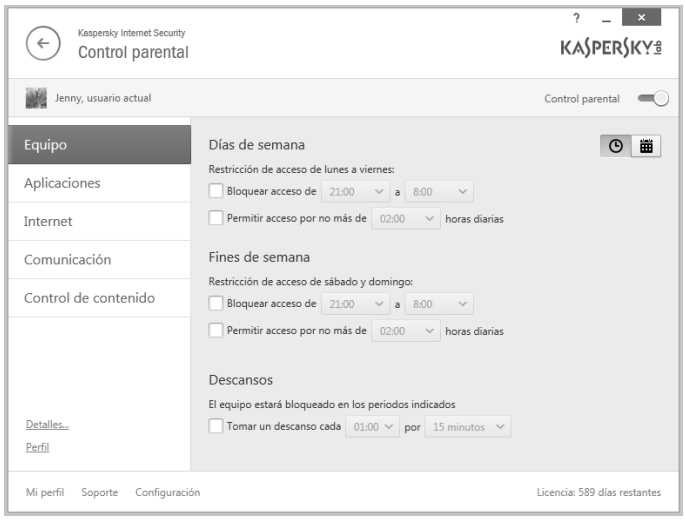
8. Dentro de la opción herramientas tenemos algunas opciones de monitoreo de las aplicaciones bloqueadas, bloqueos de red y las últimas 10 amenazas que han sido eliminadas.



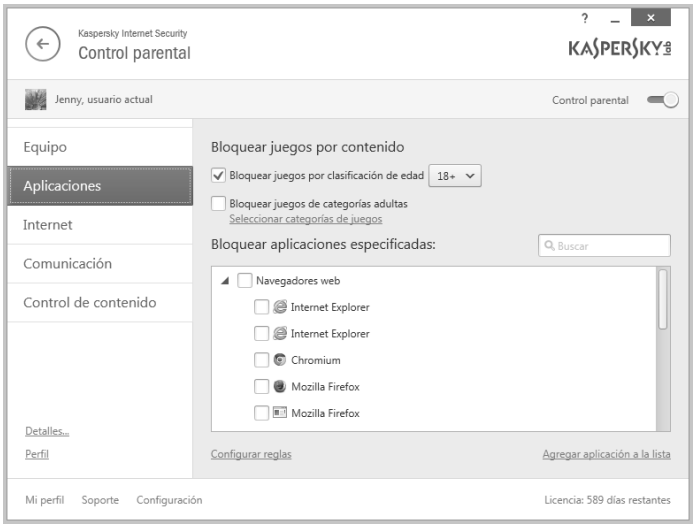
9. En el menú principal tenemos el control parental, el cual es completamente configurable, además que podemos colocar una contraseña para que el usuario no cambie ni se borren los historiales.



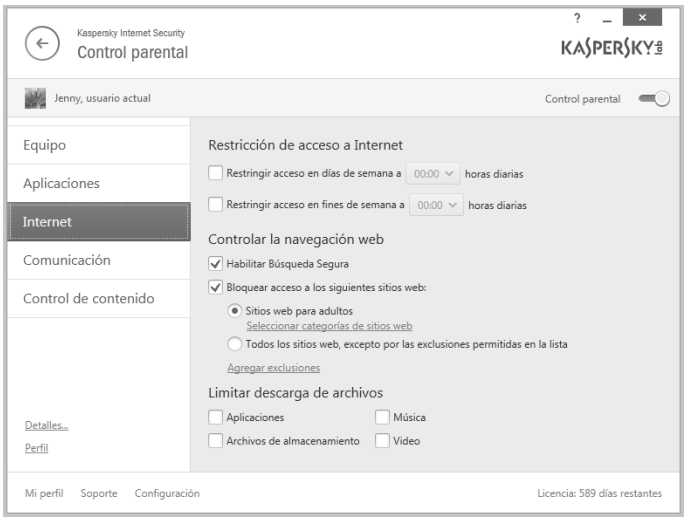
10. Dentro del control parental podemos configurar el equipo, la frecuencia de tiempo con la que puede contar con internet, por ejemplo podemos habilitar o deshabilitar el internet con su respectivo horario en días de las semana, fines de semana, descansos.



11. Se puede bloquear juegos por edad o contenido y los navegadores en los que podrían entrar.

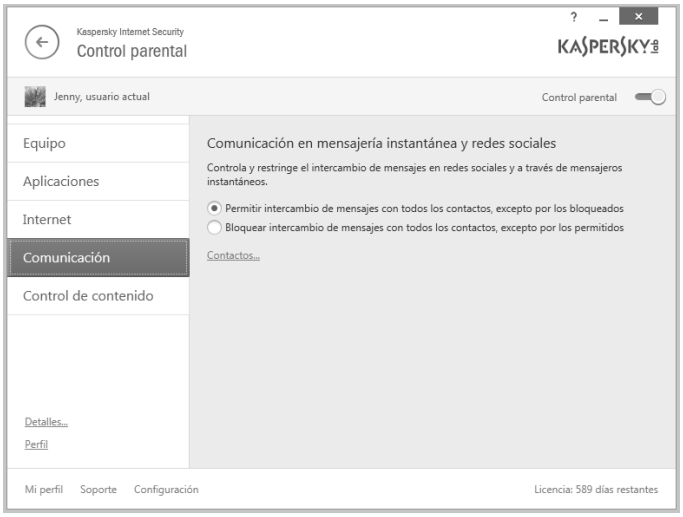


12. En la opción de internet se puede restringir el acceso a la navegación web, limitar la descarga de archivos de software, almacenamiento, música y videos.

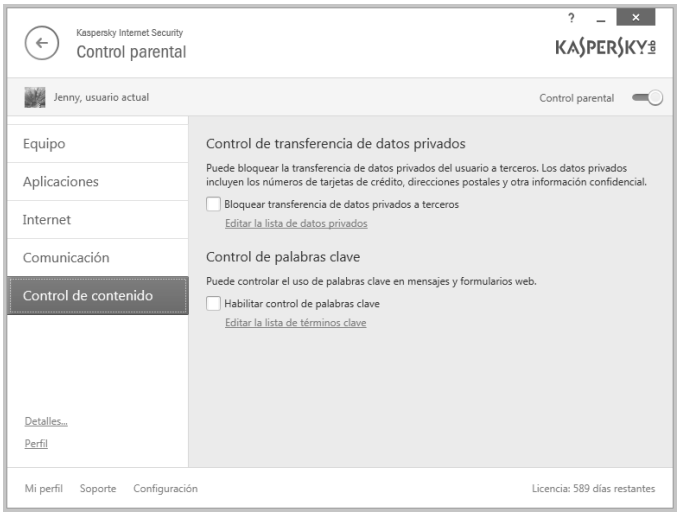


13. Dentro de las virtudes de este software podemos destacar también el bloqueo por categorías tal y como lo muestra el gráfico.

14. Si de nuestro interés es bloquear la comunicación de mensajería instantánea o redes sociales también podemos hacerlo, tal y como lo muestra el gráfico.



15. De igual manera podemos bloquear la transferencia de datos privados y controlar la transferencia con palabras clave, que nosotros podemos configurar.



Anexo 8 –Squid se encuentran entre los programas más populares de proxy y SARG es un complemento permitiéndoles obtener reportes por IP de los sitios. Herramienta que se usará para poder llevar una auditoría completa de las páginas web que los usuarios de la red visitan.

1. Para poder bajar Squid debemos entrar a la página oficial en la zona de descargas (download), que para este manual de instalación se descargará la versión 2.7 para Windows. http://www.squid-cache.org/

2. Una vez descargado el software descomprimimos la carpeta squid-2.7.STABLE8-bin.zip y la copiamos en el disco C:

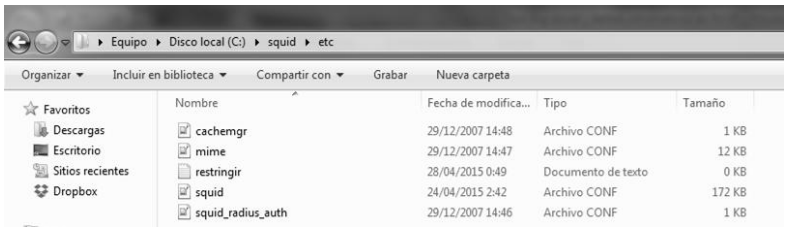
3. Entramos en la siguiente dirección “C:\squid\etc” mediante el explorador de Windows, y renombramos estos archivos, borrando la extensión .default de cada uno de ellos:

- squid.conf.default
- mime.conf.default
- cachemgr.conf.default
- squid_radius_auth.conf.default

Por:

- squid.conf
- mime.conf
- cachemgr.conf
- squid_radius_auth.conf

4. A continuación creamos un documento de tipo .txt con el nombre restringir.txt, resultándonos de la siguiente manera. Este documento de texto nos servirá para poder colocar las páginas web que deseamos restringir. Las páginas a restringir las configuraremos más adelante.



5. A continuación vamos a abrir el archivo squid de la misma ubicación anterior con notepad ++ y haremos los siguientes cambios, dentro de las líneas de programación.

6. Buscamos la siguientes líneas de código:

acl localnet src 10.0.0.0/8 # RFC1918 possible internal network

acl localnet src 172.16.0.0/12# RFC1918 possible internal network

acl localnet src 192.168.0.0/16 # RFC1918 possible internal network

Y procedemos a comentarlas porque por defecto el servidor proxy tiene habilitada la navegación, quedando de la siguiente manera:

#acl localnet src 10.0.0.0/8 # RFC1918 possible internal network

#acl localnet src 172.16.0.0/12 # RFC1918 possible internal network

#acl localnet src 192.168.0.0/16 # RFC1918 possible internal network

7. Ahora buscamos el método acl CONNECT method CONNECT, y debajo de este colocamos las siguientes líneas de código:

acl localnet src 192.168.1.0/255.255.255.0

Donde le indicamos que mi red tendrá ese rango de IP´s y máscara de subred, después agregamos la siguiente sentencia:

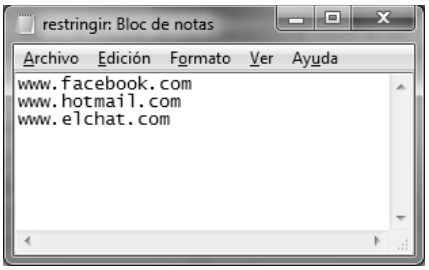
acl restringir url_regex "c:\Squid\etc\restringir.txt"

Aquí creamos la variable restringir y almacenamos la ruta donde está el grupo de páginas que restringiremos el acceso. Dentro de este documento de texto es donde colocaremos las páginas que deseamos bloquear, para este caso bloquearemos:

www.facebook.com

www.hotmail.com

www.elchat.com



8. Luego verificamos que el puerto del proxy sea el 3128, buscando http_port, debiendo dejar la sentencia de esta manera:

http_port 3128

9. Después buscamos cache_mem 8 MB y la cambiamos por 16MB dejando la sentencia de esta manera:

cache_mem 16 MB

10. Buscamos la siguiente línea de código cache_dir ufs c:/squid/var/cache 100 16 256 donde 100 es el número de megas que va a ocupar, como es una compañía que tiene alto tráfico le cambiaremos a 50000 para que no haya problemas de lentitud. De esta manera nos queda la sentencia:

cache_dir ufs c:/squid/var/cache 50000 16 256

11. A continuación buscaremos la sentencia access_log, aquí es donde le direccionaremos al log de squid, para entender mejor, es donde se almacenarán las páginas visitadas por todos los equipos informáticos que pasan por el proxy. La sentencia debe quedar de la siguiente manera para este caso:

access_log c:/squid/var/logs/access.log squid

12. Luego guardamos el archivo squid que modificamos y abrimos el símbolo del sistema en modo de administrador y entramos al directorio c:\squid\sbin y ejecutamos el comando squid –z, posterior a ello vemos que se crearon los directorios correctamente.

13. Al final de las líneas de código le colocamos la siguiente instrucción para indicar el nombre del equipo donde corre el servidor proxy:

visible_hostname Servidor

14. A continuación guardamos el archivo.

15. Abrimos el símbolo del sistema y ejecutamos la siguiente instrucción:

cd\

cd squid

cd sbin

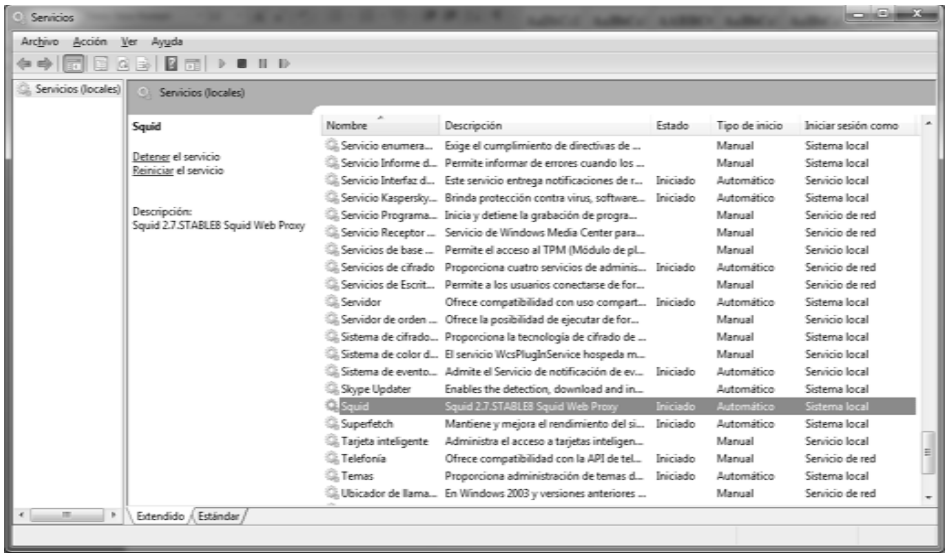
squid –z

Hacemos esto para crear los directorios necesarios de squid.

16. Después vamos a crear el servicio squid e iniciando colocando la siguiente sentencia:

squid –i

17. Luego verificamos si el servicio ha sido creado e iniciado correctamente en Inicio\Panel de control\Sistema y seguridad\Herramientas administrativas\Servicios

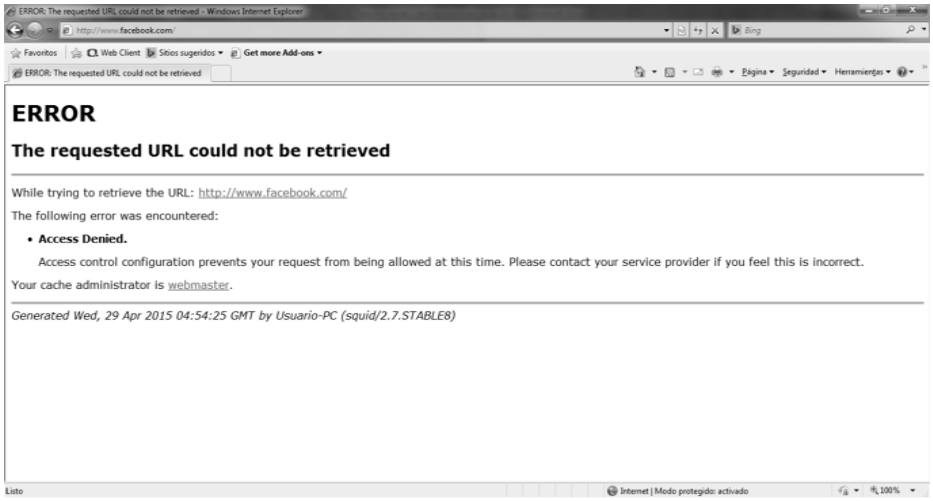


18. Ahora debemos ir a configurar el servidor proxy en el navegador, siguiendo la siguiente secuencia, abrimos internet explorer\opciones de internet\conexiones\configuración LAN y habilitamos el servidor proxy, en dirección colocaremos 192.168.1.115 y el puerto el 3128 y aceptamos.

19. Ahora abriremos el internet explorer y navegaremos en dos páginas una que tiene libre acceso y una que está bloqueada (documento de texto llamado restringir.txt).

Para este ejemplo ingresaremos en www.google.com.

Ahora para el siguiente ejemplo ingresaremos a www.facebook.com. (página bloqueada), y podemos visualizar que el proxy ha denegado el acceso.



Con lo que verificamos que las páginas que están dentro del documento de texto restringir.txt no tendrán acceso a la navegación.

20. Luego de ello lo que nos resta es poder instalar SARG para poder tener nuestros reportes, para lo cual ingresamos en la siguiente dirección: http://sourceforge.net/projects/sarg. y bajamos la versión SARG 2.2

21. Luego de haber bajado SARG 2.2 para Windows descomprimimos el archivo y lo copiamos al disco C:

22. Dentro de la carpeta SARG vamos a crear una carpeta que se llame Reportes, esta carpeta nos va a servir posteriormente para que aquí se almacenen los reportes que extraigamos de squid.

23. Ahora lo que vamos hacer es editar el archivo sarg.conf con notepad++ y realizaremos los siguientes cambios.

24. Buscaremos en el código lo siguiente con al afán que nuestro reporte salga en español:

#language English

Y cambiamos por

language Spanish

Sin el signo de numeral para que la sentencia se ejecute.

25. Después buscamos la siguiente sentencia para colocar el nombre de a carpeta que creamos (Reportes) donde se almacenaran los informes que generemos con SARG.

output_dir c:/sarg/report

Y la cambiamos por:

output_dir c:/sarg/reportes

26. Luego abrimos el símbolo del sistema y digitamos las siguientes sentencias:

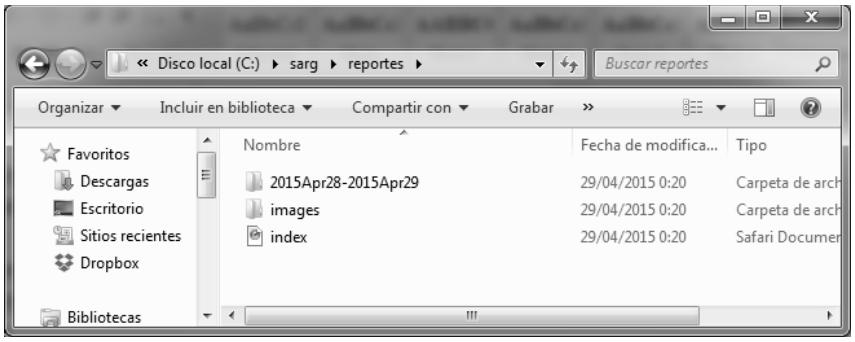
cd\

cd sarg

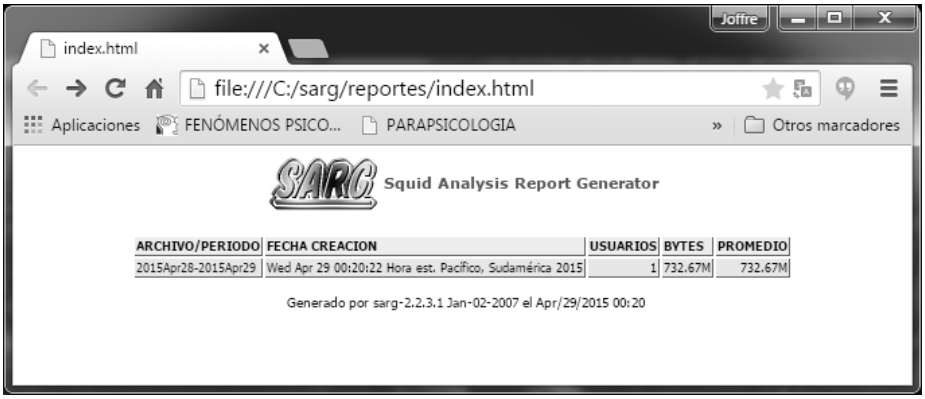
cd sbin

sarg

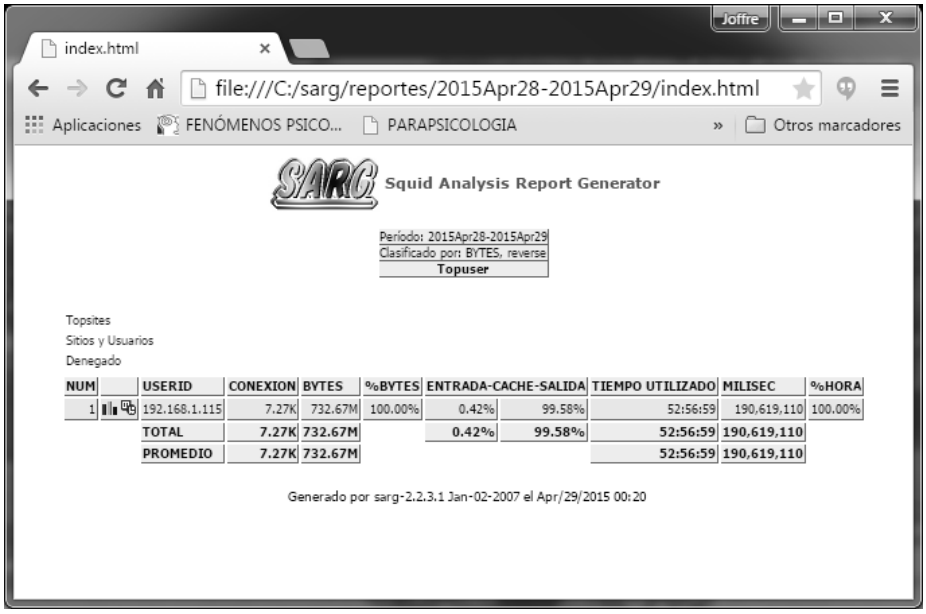
27. A continuación abrimos el explorador de Windows y ubicamos la carpeta reportes dentro de la carpeta SARG que se encuentra en el disco c:



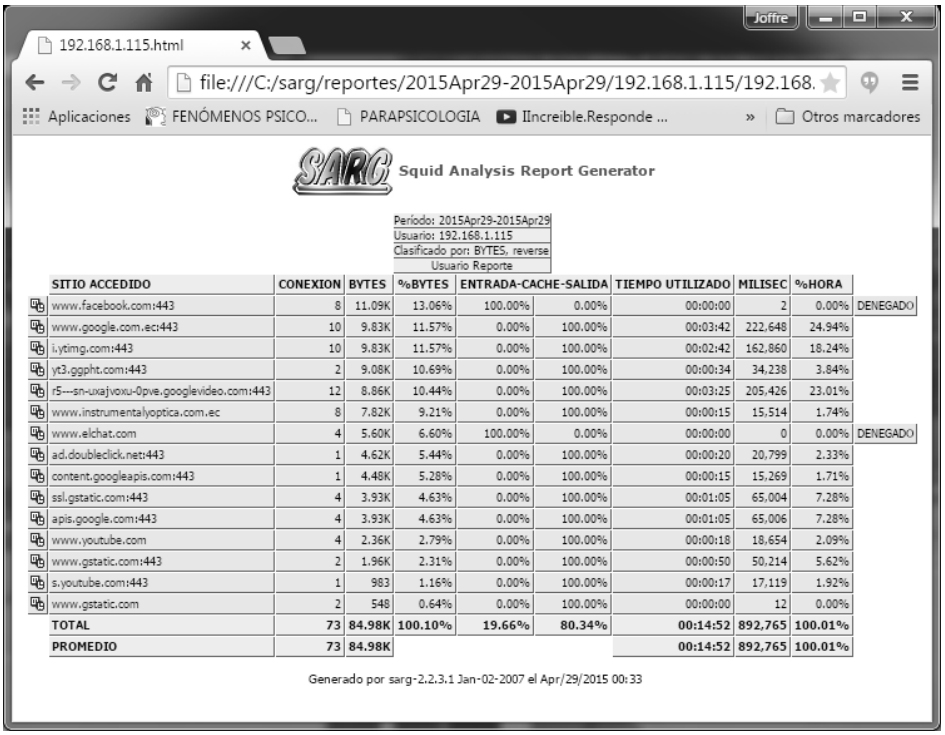
28. Ahí encontraremos el archivo index, le damos doble clic y tenemos nuestro reporte de páginas visitadas ordenadas por el IP de los equipos que navegaron a internet.



Le damos clic en el achivo/período y tenemos lo siguiente:



A continuación le damos clic en el UserID que es la IP del equipo que ha registrado navegación y podemos observar las páginas que ha visitado, páginas permitidas y bloqueadas de navegación.



SITIO ACCEDIDO	CONEXION	BYTES	%BYTES	ENTRADA-CACHE-SALIDA		TIEMPO UTILIZADO	MILISEC	%HORA	
www.facebook.com:443	8	11.09K	13.06%	100.00%	0.00%	00:00:00	2	0.00%	DENEGADO
www.google.com.ec:443	10	9.83K	11.57%	0.00%	100.00%	00:03:42	222,648	24.94%	
i.ytimg.com:443	10	9.83K	11.57%	0.00%	100.00%	00:02:42	162,860	18.24%	
yt3.ggpht.com:443	2	9.08K	10.69%	0.00%	100.00%	00:00:34	34,238	3.84%	
r5---sn-uxajvoxu-0pve.googlevideo.com:443	12	8.86K	10.44%	0.00%	100.00%	00:03:25	205,426	23.01%	
www.instrumentalyoptica.com.ec	8	7.82K	9.21%	0.00%	100.00%	00:00:15	15,514	1.74%	
www.elchat.com	4	5.60K	6.60%	100.00%	0.00%	00:00:00	0	0.00%	DENEGADO
ad.doubleclick.net:443	1	4.62K	5.44%	0.00%	100.00%	00:00:20	20,799	2.33%	
content.googleapis.com:443	1	4.48K	5.28%	0.00%	100.00%	00:00:15	15,269	1.71%	
ssl.gstatic.com:443	4	3.93K	4.63%	0.00%	100.00%	00:01:05	65,004	7.28%	
apis.google.com:443	4	3.93K	4.63%	0.00%	100.00%	00:01:05	65,006	7.28%	
www.youtube.com	4	2.36K	2.79%	0.00%	100.00%	00:00:18	18,654	2.09%	
www.gstatic.com:443	2	1.96K	2.31%	0.00%	100.00%	00:00:50	50,214	5.62%	
s.youtube.com:443	1	983	1.16%	0.00%	100.00%	00:00:17	17,119	1.92%	
www.gstatic.com	2	548	0.64%	0.00%	100.00%	00:00:00	12	0.00%	
TOTAL	**73**	**84.98K**	**100.10%**	**19.66%**	**80.34%**	**00:14:52**	**892,765**	**100.01%**	
PROMEDIO	**73**	**84.98K**				**00:14:52**	**892,765**	**100.01%**	

Generado por sarg-2.2.3.1 Jan-02-2007 el Apr/29/2015 00:33