ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

"ESTUDIO SOBRE EL ESTADO DEL ARTE DE LA SEGURIDAD INFORMÁTICA EN EL ECUADOR, Y SUS NECESIDADES REALES."

TESINA DE SEMINARIO

Previa a la obtención del Título de:

INGENIERO EN CIENCIAS COMPUTACIONALES ESPECIALIZACIÓN EN SISTEMAS DE INFORMACIÓN.

INGENIERO EN ELECTRÓNICA Y TELECOMUNICACIONES

Presentada por:

JENNY ALEXANDRA REZABALA TRIVIÑO

LUIS EDISON SOLÓRZANO CADENA

Guayaquil - Ecuador
2011

AGRADECIMIENTO

Gracias a Dios, el centro de nuestras vidas,
A nuestros padres por su apoyo incondicional.

Y a todas las personas que han
contribuido a lograr dicho trabajo.

DEDICATORIA

A todos aquellos que se
Esfuerzan por proveer mejoras y
Dar resultados óptimos.
.

TRIBUNAL DE SUSTENTACIÓN

Ing. Alfonso Aranda

PROFESOR DEL SEMINARIO

Ing. Lenin Freire

PROFESOR DELEGADO POR EL DECANO

DECLARACIÓN EXPRESA

"La responsabilidad del contenido de este Proyecto de Graduación, nos corresponde exclusivamente; y el patrimonio intelectual de la misma, a la Escuela Superior Politécnica del Litoral"

(Reglamento de exámenes y títulos profesionales de la ESPOL)

Jenny Alexandra Rezabala Triviño

Luis Edison Solórzano Cadena

RESUMEN

En el capítulo primero se describe la introducción a la seguridad informática, desde conceptos básicos, objetivos de la seguridad informática, amenazas, técnicas, leyes y organismos, tipos de mercados y los diferentes métodos para la colección de información y la justificación de la técnica de evaluación escogida para el estudio.

En el capítulo segundo se describe el análisis y descripción de los resultados obtenidos durante el estudio;

En el capítulo tercero se describe las conclusiones generales y específicas, comparaciones entre las diferentes consideraciones en el estado de la seguridad informática sobre el manejo eficiente de los recursos que poseen y no, por parte de las empresas.

En la parte de Anexos se describe las encuestas utilizados para los diferentes tipos de mercados.

INDICE DE FIGURAS

ABREVIATURAS

SI	Seguridad Informática
SGSI	Sistema de Gestión de la Seguridad de la Información
IPS	Intrusion Prevention System o Sistema de Prevención de Intrusos.
IDS	Intrusion Detection System o Sistema de Detección de Intrusos.
RAM	Random Access Memory o Memoria de Acceso Aleatorio.
FAT	File Allocation Table o Tabla de Asignación de Ficheros.
DMZ	Demilitarized Zone o Zona Desmilitarizada
PAT	Port Address Translation o Traslación de Direcciones de Puertos.
CERT/CC	Computer Emergency Response Team Coordination Center.
SEI	Software Engineering Institute o Instituto de Ingeniería de Software.
ISP	Internet Service Provider o Proveedor de Servicio de Internet.
SEO	Search Engine Optimization o Posicionamiento en buscadores.

INTRODUCCIÓN

En los últimos tiempos, la seguridad informática ha representado un alto grado de interés dentro de las organizaciones, ya sea a través del cumplimiento de normas y procedimientos; o por desastres informáticos los que han ocasionado la pérdida de grandes cantidades de información.

En una empresa, cuidar de los recursos informáticos, sin duda resulta una tarea ardua para quienes deben resguardar la información; cabe destacar que es una oportunidad para quienes proveen éste tipo de servicio, ya que muchos no cuentan con la infraestructura.

En nuestro estudio, el objetivo es hacer un análisis del estado de seguridad informática que poseen las empresas, dentro de nuestro grupo ecuánime: empresas grandes y Pymes, teniendo como enfoque concienciar acerca del estado que se encuentran, creando una disciplina que permita establecer medidas y éstas a su vez proveen mejoras.

En este trabajo se presenta un análisis basado en un método de evaluación de las encuestas.

CAPÍTULO 1

1. Introducción de Seguridad Informática.

En este capítulo se provee información acerca de los antecedentes sobre los cuáles se plantearon los objetivos, una explicación profunda del problema y la justificación del presente trabajo.

1.1. Definición

La seguridad informática es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta (incluyendo la información). Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información. La seguridad de la información es una sub área de la seguridad informática que se enfoca exclusivamente en la protección de la información, lo que comprende software, bases de datos, metadatos, archivos y todo lo que la organización valore (activo) y signifique un riesgo si ésta llega a manos de otras personas. Este tipo de información se conoce como información privilegiada o confidencial.

1.2. Definición del Estado del Arte

State of the Art, por sus siglas en Inglés, hace referencia al nivel más alto de desarrollo conseguido en un momento determinado sobre cualquier técnica o campo científico.

1.3. Objetivos de la Seguridad Informática

La seguridad informática está concebida para proteger los activos informáticos de la empresa, entre los que se encuentran:

La información

Hoy en día la información se ha convertido en uno de los activos más importantes y valiosos dentro de una organización. La seguridad informática debe velar por que ésta sea administrada según los criterios establecidos por los administradores y supervisores, evitando que usuarios externos y no autorizados puedan acceder a ella sin autorización. De lo contrario la organización corre el riesgo de que la información sea utilizada maliciosamente para obtener ventajas de ella o que sea manipulada, ocasionando lecturas erradas o incompletas de la misma. Otra función de la seguridad informática en esta área es la de asegurar el acceso a la información en el momento oportuno, incluyendo respaldos de la misma en

caso de que esta sufra daños o pérdida producto de accidentes, atentados o desastres.

La infraestructura computacional

Una parte fundamental para el almacenamiento y gestión de la información, así como para el funcionamiento mismo de la organización. La función de la seguridad informática en esta área es velar que los equipos funcionen adecuadamente y prever en caso de falla planes de contingencia que permitan su rápida reposición. También debe asegurar que las redes y toda la infraestructura funcionen correctamente; para ello se deben realizar mantenciones periódicas para detectar posibles fallas en la misma. Por último, la seguridad informática debe asegurar planes de contingencia en caso de robos, incendios, boicot, desastres naturales, fallas en el suministro eléctrico y cualquier otro factor que atente contra la infraestructura informática.

Los usuarios

Son las personas que utilizan la estructura tecnológica, de comunicaciones y que gestionan la información. La seguridad informática debe establecer normas que minimicen los riesgos a la información o infraestructura informática. Estas normas incluyen horarios de funcionamiento, restricciones a ciertos lugares, autorizaciones, denegaciones, perfiles de usuario, planes de emergencia, protocolos y todo lo necesario que permita un buen nivel de seguridad informática minimizando el impacto en el desempeño de los funcionarios y de la organización en general.

Con la finalidad de lograr esto se trazaron los siguientes objetivos:

- Definir el estado de arte actual de la seguridad informática en el Ecuador
- Desarrollar técnicas de evaluación de la madurez en seguridad informática
- Identificar el nivel de aceptación por mercados de los servicios gestionados de seguridad
- Identificar oportunidades de emprendimiento.

1.4. Justificación

La justificación principal para el desarrollo de éste estudio, es la necesidad de identificar las problemáticas actuales dentro de nuestro grupo objetivo, además de poseer datos estadísticos, que nos permitan poder proyectar la tendencia de seguridad de las empresas en un futuro; analizar la estructura y funcionamiento.

1.5. Las Amenazas

Una vez que la programación y el funcionamiento de un dispositivo de almacenamiento (o transmisión) de la información se consideran seguras, todavía deben ser tenidos en cuenta las circunstancias "no informáticas" que pueden afectar a los datos, las cuales son a menudo imprevisibles o inevitables, de modo que la única protección posible es la redundancia (en

el caso de los datos) y la descentralización -por ejemplo mediante estructura de redes- (en el caso de las comunicaciones).

Estos fenómenos pueden ser causados por:

El usuario: causa del mayor problema ligado a la seguridad de un sistema informático (porque no le importa, no se da cuenta o a propósito).

Programas maliciosos: programas destinados a perjudicar o a hacer un uso ilícito de los recursos del sistema. Es instalado (por inatención o maldad) en el ordenador abriendo una puerta a intrusos o bien modificando los datos. Estos programas pueden ser un virus informático, un gusano informático, un troyano, una bomba lógica o un programa espía o Spyware.

Un intruso: persona que consigue acceder a los datos o programas de los cuales no tiene acceso permitido (cracker, defacer, script kiddie o Script boy, viruxer, etc.).

Un siniestro (robo, incendio, inundación): una mala manipulación o una mal intención derivan a la pérdida del material o de los archivos.

El personal interno de Sistemas. Las pujas de poder que llevan a disociaciones entre los sectores y soluciones incompatibles para la seguridad informática **.**

1.6. Tipos de Amenazas

El hecho de conectar una red a un entorno externo nos da la posibilidad de que algún atacante pueda entrar en ella, con esto, se puede hacer robo de información o alterar el funcionamiento de la red. Sin embargo el hecho de

que la red no sea conectada a un entorno externo no nos garantiza la seguridad de la misma, existen 2 tipos de amenazas:

Amenazas internas: Generalmente estas amenazas pueden ser más serias que las externas por varias razones como son:

- Los usuarios conocen la red y saben cómo es su funcionamiento.

- Tienen algún nivel de acceso a la red por las mismas necesidades de su trabajo.

- Los IPS y Firewalls son mecanismos no efectivos en amenazas internas.

Amenazas externas: Son aquellas amenazas que se originan de afuera de la red. Al no tener información certera de la red, un atacante tiene que realizar ciertos pasos para poder conocer qué es lo que hay en ella y buscar la manera de atacarla. La ventaja que se tiene en este caso es que el administrador de la red puede prevenir una buena parte de los ataques externos **.**

1.7. Tipos de Virus

Los virus se pueden clasificar de la siguiente forma:

Virus residentes

La característica principal de estos virus es que se ocultan en la memoria RAM de forma permanente o residente. De este modo, pueden controlar e interceptar todas las operaciones llevadas a cabo por el sistema operativo, infectando todos aquellos ficheros y/o programas que sean ejecutados, abiertos, cerrados, renombrados, copiados, Algunos ejemplos de este tipo de virus son: Randex, CMJ, Meve, MrKlunky.

Virus de acción directa

Al contrario que los residentes, estos virus no permanecen en memoria. Por tanto, su objetivo prioritario es reproducirse y actuar en el mismo momento de ser ejecutados. Al cumplirse una determinada condición, se activan y buscan los ficheros ubicados dentro de su mismo directorio para contagiarlos.

Virus de sobre escritura

Estos virus se caracterizan por destruir la información contenida en los ficheros que infectan. Cuando infectan un fichero, escriben dentro de su contenido, haciendo que queden total o parcialmente inservibles.

Virus de boot o de arranque

Los términos boot o sector de arranque hacen referencia a una sección muy importante de un disco (tanto un disquete como un disco duro respectivamente). En ella se guarda la información esencial sobre las características del disco y se encuentra un programa que permite arrancar el ordenador. Este tipo de virus no infecta ficheros, sino los discos que los contienen. Actúan infectando en primer lugar el sector de arranque de los disquetes. Cuando un ordenador se pone en marcha con un disquete infectado, el virus de boot infectará a su vez el disco duro.

Los virus de boot no pueden afectar al ordenador mientras no se intente poner en marcha a éste último con un disco infectado. Por tanto, el mejor modo de defenderse contra ellos es proteger los disquetes contra escritura y no arrancar nunca el ordenador con un disquete desconocido en la disquetera.

Algunos ejemplos de este tipo de virus son: Polyboot.B, AntiEXE.

Virus de macro

El objetivo de estos virus es la infección de los ficheros creados usando determinadas aplicaciones que contengan macros: documentos de Word (ficheros con extensión DOC), hojas de cálculo de Excel (ficheros con extensión XLS), bases de datos de Access (ficheros con extensión MDB), presentaciones de PowerPoint (ficheros con extensión PPS), ficheros de Corel Draw, etc. Las macros son micro-programa asociado a un fichero, que

sirven para automatizar complejos conjuntos de operaciones. Al ser programas, las macros pueden ser infectadas.

Virus de enlace o directorio

Los ficheros se ubican en determinadas direcciones (compuestas básicamente por unidad de disco y directorio), que el sistema operativo conoce para poder localizarlos y trabajar con ellos.

Virus cifrados

Más que un tipo de virus, se trata de una técnica utilizada por algunos de ellos, que a su vez pueden pertenecer a otras clasificaciones. Estos virus se cifran a sí mismos para no ser detectados por los programas antivirus. Para realizar sus actividades, el virus se descifra a sí mismo y, cuando ha finalizado, se vuelve a cifrar.

Virus polimórficos

Son virus que en cada infección que realizan se cifran de una forma distinta (utilizando diferentes algoritmos y claves de cifrado). De esta forma, generan una elevada cantidad de copias de sí mismos e impiden que los antivirus los localicen a través de la búsqueda de cadenas o firmas, por lo que suelen ser los virus más costosos de detectar.

Virus multipartitos

Virus muy avanzados, que pueden realizar múltiples infecciones, combinando diferentes técnicas para ello. Su objetivo es cualquier elemento que pueda ser infectado: archivos, programas, macros, discos, etc.

Virus de Fichero

Infectan programas o ficheros ejecutables (ficheros con extensiones EXE y COM). Al ejecutarse el programa infectado, el virus se activa, produciendo diferentes efectos.

Virus de FAT

La Tabla de Asignación de Ficheros o FAT es la sección de un disco utilizada para enlazar la información contenida en éste. Se trata de un elemento fundamental en el sistema. Los virus que atacan a este elemento son especialmente peligrosos, ya que impedirán el acceso a ciertas partes del disco, donde se almacenan los ficheros críticos para el normal funcionamiento del ordenador **.**

1.8. Análisis de Riesgos

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

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

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

Los medios para conseguirlo son:

Restringir el acceso (de personas de la organización y de las que no lo son) a los programas y archivos.

Asegurar que los operadores puedan trabajar pero que no puedan modificar los programas ni los archivos que no correspondan (sin una supervisión minuciosa).

Asegurar que se utilicen los datos, archivos y programas correctos en/y/por el procedimiento elegido.

Asegurar que la información transmitida sea la misma que reciba el destinatario al cual se ha enviado y que no le llegue a otro.

Asegurar que existan sistemas y pasos de emergencia alternativos de transmisión entre diferentes puntos.

Organizar a cada uno de los empleados por jerarquía informática, con claves distintas y permisos bien establecidos, en todos y cada uno de los sistemas o aplicaciones empleadas.

Actualizar constantemente las contraseñas de accesos a los sistemas de cómputo **.**

1.9. Elementos de un análisis de riesgo

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

1. Construir un perfil de las amenazas que esté basado en los activos de la organización.

2. Identificación de los activos de la organización.

3. Identificar las amenazas de cada uno de los activos listados.

4. Conocer las prácticas actuales de seguridad.

5. Identificar las vulnerabilidades de la organización.

6. Identificar los requerimientos de seguridad de la organización.

7. Identificación de las vulnerabilidades dentro de la infraestructura tecnológica.

8. Detección de los componentes claves.

9. Desarrollar planes y estrategias de seguridad que contengan los siguientes puntos:

Riesgo para los activos críticos

Medidas de riesgos

Estrategias de protección

Planes para reducir los riesgos.

1.10. Análisis de Impacto al Negocio

El reto es asignar estratégicamente los recursos para equipo de seguridad y bienes que intervengan, basándose en el impacto potencial para el negocio, respecto a los diversos incidentes que se deben resolver. Para determinar el establecimiento de prioridades, el sistema de gestión de incidentes necesita saber el valor de los sistemas de información que pueden ser potencialmente afectados por incidentes de seguridad. Esto puede implicar que alguien dentro de la organización asigne un valor monetario a cada equipo y un archivo en la red o asignar un valor relativo a cada sistema y la información sobre ella. Dentro de los valores para el sistema se pueden distinguir: Confidencialidad de la información, la Integridad (aplicaciones e información) y finalmente la disponibilidad del sistema. Cada uno de estos valores es un sistema independiente del negocio, supongamos el siguiente ejemplo, un servidor Web público pueden poseer los requisitos de confidencialidad de baja (ya que toda la información es pública), pero de alta disponibilidad y los requisitos de integridad. En contraste, un sistema de planificación de recursos empresariales (ERP), sistema puede poseer alta puntaje en los tres variables. Los incidentes individuales pueden variar ampliamente en términos de alcance e importancia**.**

1.11. Puesta en marcha de una política de seguridad

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

Elaborar reglas y procedimientos para cada servicio de la organización.

Definir las acciones a emprender y elegir las personas a contactar en caso de detectar una posible intrusión.

Sensibilizar a los operadores con los problemas ligados con la seguridad de los sistemas informáticos.

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

1.12. Técnicas para asegurar el sistema

Codificar la información: Cristología, Criptografía, Criptociencia, contraseñas difíciles de averiguar a partir de datos personales del individuo.

Vigilancia de red. Zona Desmilitarizada.

Tecnologías repelentes o protectoras: cortafuegos, sistemas de detección de intrusos – antispyware, antivirus, llaves para protección de software, etc. Mantener los sistemas de información con las actualizaciones que más impacten en la seguridad.

Sistema de Respaldo Remoto. Servicio de backup remoto.

Codificar la información

Los sistemas de encriptación tiene como objetivo codificar la información de manera que sea difícil decodificarla si no se conoce la clave pero fácil si se la conoce . Para la codificación de la información existen técnicas como la Cristología que es el estudio de los criptosistemas, sus áreas principales de estudio son la criptografía y el criptoanálisis.

En tiempos recientes, el interés por la cristología se ha extendido asimismo a otras aplicaciones aparte de la comunicación segura de información y, actualmente, una de los más extendidos usos de las técnicas y métodos estudiados por la cristología es la autentificación de información digital (también llamada firma digital) **.**

Tipos de encriptación:

Substitución

Monoalphabetic Substitutions

Gronsfeld

RSA

DES

Chaffing & Winnowing

SKIPJACK

BÍFIDO

WLBYKYAAOTB

Cifrado exponencial

Blowfish

Vigilancia de red. (Zona desmilitarizada)

En seguridad informática, una DMZ o red perimetral es una red local que se ubica entre la red interna de una organización y una red externa, generalmente Internet. El objetivo de una DMZ es que las conexiones desde la red interna y la externa a la DMZ estén permitidas, mientras que las

conexiones desde la DMZ sólo se permitan a la red externa -- los equipos (host) en la DMZ no pueden conectar con la red interna. Esto permite que los equipos (hosts) de la DMZ puedan dar servicios a la red externa a la vez que protegen la red interna en el caso de que intrusos comprometan la seguridad de los equipos (host) situados en la zona desmilitarizada. Para cualquiera de la red externa que quiera conectarse ilegalmente a la red interna, la zona desmilitarizada se convierte en un callejón sin salida.

La DMZ se usa habitualmente para ubicar servidores que es necesario que sean accedidos desde fuera, como servidores de e-mail, Web y DNS.

Las conexiones que se realizan desde la red externa hacia la DMZ se controlan generalmente utilizando port address translation (PAT).

Una DMZ se crea a menudo a través de las opciones de configuración del cortafuego, donde cada red se conecta a un puerto distinto de éste. Esta configuración se llama cortafuegos en trípode (three-legged firewall). Un planteamiento más seguro es usar dos cortafuegos, donde la DMZ se sitúa en medio y se conecta a ambos cortafuegos, uno conectado a la red interna y el otro a la red externa. Esta configuración ayuda a prevenir configuraciones erróneas accidentales que permitan el acceso desde la red externa a la interna. Este tipo de configuración también es llamado cortafuegos de subred monitoreada (screened-subnet firewall).

Obsérvese que los router domésticos son llamados "DMZ host", aunque no es una definición correcta de zona desmilitarizada**.**

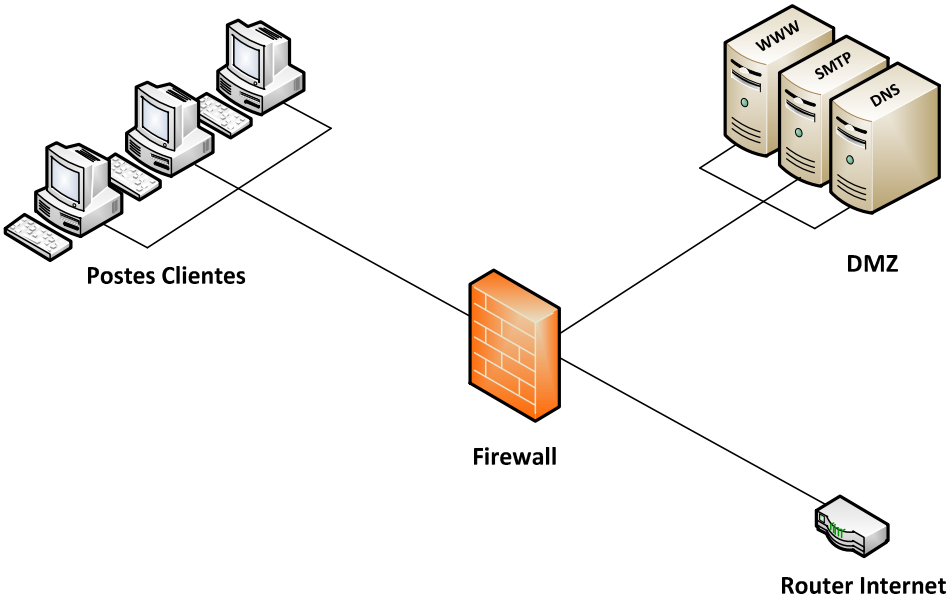

Fig. 1 1 Diagrama de una red típica que usa una DMZ con un cortafuegos de tres patas (three-legged).

Tecnologías repelentes o protectoras.

Dentro de estas tecnologías tenemos a los cortafuegos, sistemas de detección de intrusos – antispyware, antivirus, llaves para protección de software, etc. Mantener los sistemas de información con las actualizaciones que más impacten en la seguridad.

Cortafuegos.

Un muro de fuego (firewall en inglés) es una parte de un sistema o una red que está diseñada para bloquear el acceso no autorizado, permitiendo al mismo tiempo comunicaciones autorizadas. Se trata de un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios.

Los cortafuegos pueden ser implementados en hardware o software, o una combinación de ambos. Los cortafuegos se utilizan con frecuencia para evitar que los usuarios de Internet no autorizados tengan acceso a redes privadas conectadas a Internet, especialmente intranets. Todos los mensajes que entren o salgan de la intranet pasan a través de los cortafuegos, que examina cada mensaje y bloquea aquellos que no cumplen los criterios de seguridad especificados. También es frecuente conectar al cortafuego a una tercera red o Zona desmilitarizada (DMZ), Un cortafuego correctamente configurado añade una protección necesaria a la red, pero que en ningún caso debe considerarse suficiente. La seguridad informática abarca más ámbitos y más niveles de trabajo y protección **.**

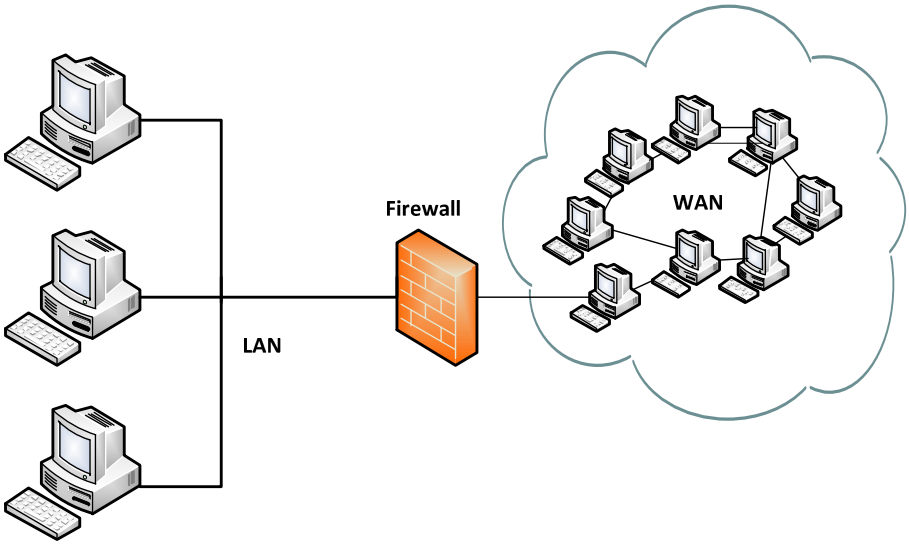

Fig. 1 2 Esquema de una red de computadoras que utiliza un Cortafuegos.

Tipos de Firewall

Filtrado de Paquetes

Proxy-Gateway de Aplicaciones

Dual-Homed Host

Screened Host

Screened Subnet

Inspección de Paquetes

Firewalls Personales

Sistemas de detección de intrusos (IDS)

Un sistema de detección de intrusos (o IDS de sus siglas en inglés Intrusion Detection System) es un programa usado para detectar accesos no autorizados a un computador o a una red. Estos accesos pueden ser ataques de habilidosos hackers, o de Script Kiddies que usan herramientas automáticas.

El IDS suele tener sensores virtuales (por ejemplo, un sniffer de red) con los que el núcleo del IDS puede obtener datos externos (generalmente sobre el tráfico de red). El IDS detecta, gracias a dichos sensores, anomalías que pueden ser indicio de la presencia de ataques o falsas alarmas **.**

Tipos de IDS

HIDS (HostIDS)

NIDS (NetworkIDS)

DIDS (DistributedIDS)

Antispyware

Encargados de evitar o reducir la infiltración de los spyware, los spyware o programa espía es un programa dentro de la categoría malware, que se instala furtivamente en un ordenador para recopilar información sobre las actividades realizadas en éste. La función más común que tienen estos programas es la de recopilar información sobre el usuario y distribuirlo a empresas publicitarias u otras organizaciones interesadas, pero también se han empleado en organismos oficiales para recopilar información contra sospechosos de delitos, como en el caso de la piratería de software. Además pueden servir para enviar a los usuarios a sitios de internet que tienen la imagen corporativa de otros, con el objetivo de obtener información importante. Dado que el spyware usa normalmente la conexión de una computadora a Internet para transmitir información, consume ancho de banda, con lo cual, puede verse afectada la velocidad de transferencia de datos entre dicha computadora y otra(s) conectada(s) a la red.

Los programas espía pueden ser instalados en un ordenador mediante un virus, un troyano que se distribuye por correo electrónico, como el programa Magic Lantern desarrollado por el FBI, o bien puede estar oculto en la instalación de un programa aparentemente inocuo. Algunos programas descargados de sitios no confiables pueden tener instaladores con spyware y otro tipo de malware **.**

Antivirus

Los antivirus son una herramienta simple cuyo objetivo es detectar y eliminar virus informáticos. Nacieron durante la década de 1980.

Con el transcurso del tiempo, la aparición de sistemas operativos más avanzados e Internet, ha hecho que los antivirus hayan evolucionado hacia programas más avanzados que no sólo buscan detectar virus informáticos, sino bloquearlos, desinfectarlos y prevenir una infección de los mismos, y actualmente ya son capaces de reconocer otros tipos de malware, como spyware, rootbits, etc.

Llaves para protección de software

Es un sistema de seguridad basado en hardware el cual brinda protección al software contra la piratería y el uso ilegal, permitiendo el acceso y ejecución únicamente cuando la llave está conectada al PC. Las llaves contienen un motor de cifrado de alta seguridad en el cual todo el proceso se realiza dentro del hardware sin abandonar en ningún momento la llave.

Durante la ejecución, el software protegido envía secuencias cifradas a la llave que las descifra produciendo una respuesta que no se puede emular. Si la respuesta de la llave es correcta la aplicación sigue funcionando. Si la llave no está conectada o la respuesta es incorrecta, la aplicación no se ejecuta.

Una desventaja importante es la parte en la cual es necesaria una llave por cada copia del programa, con esto el precio y costo de fabricación incrementan su valor y pueden surgir problemas de distribución. Por lo tanto las llaves se utilizan sobretodo con programas muy caros y no con shareware.

Respaldo de Información

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

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

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

Continuo

El respaldo de datos debe ser completamente automático y continuo. Debe funcionar de forma transparente, sin intervenir en las tareas que se encuentra realizando el usuario.

Seguro

Muchos software de respaldo incluyen encriptación de datos (128-448 bits), lo cual debe ser hecho localmente en el equipo antes del envío de la información.

Remoto

Los datos deben quedar alojados en dependencias alejadas de la empresa.

Mantención de versiones anteriores de los datos

Se debe contar con un sistema que permita la recuperación de versiones diarias, semanales y mensuales de los datos.

Hoy en día los sistemas de respaldo de información online (Servicio de backup remoto) están ganando terreno en las empresas y organismos gubernamentales. La mayoría de los sistemas modernos de respaldo de información online cuentan con las máximas medidas de seguridad y disponibilidad de datos. Estos sistemas permiten a las empresas crecer en volumen de información sin tener que estar preocupados de aumentar su dotación física de servidores y sistemas de almacenamiento.

1.13. Organismos Oficiales de Seguridad Informática

Existen organismos oficiales encargados de asegurar servicios de prevención de riesgos y asistencia a los tratamientos de incidencias, tales como el CERT/CC (Computer Emergency Response Team Coordination Center) del SEI (Software Engineering Institute) de la Carnegie Mellon University el cual es un centro de alerta y reacción frente a los ataques informáticos, destinados a las empresas o administradores, pero generalmente estas informaciones son accesibles a todo el mundo.

1.14. Leyes y Organismos de Seguridad Informática en el Ecuador

Considerando que la información constituye un valor económico con relevancia jurídico-penal, por ser posible objeto de conductas delictivas (acceso no autorizado, sabotaje o daño informático, espionaje informático, etc.) y por ser instrumento de comisión, falsificación, aseguramiento y calificación de los ilícitos tradicionales, llegando a ser un bien jurídico protegido, susceptible de protección legal propia y específica del ordenamiento jurídico imperante. Desde esa concepción se han de identificar, reconocer y legalizar los procedimientos y herramientas, técnicas especializadas en este tipo de infracciones para asegurar la prueba, otorgarle validez plena y constituirla en el fundamento para la valoración y

decisión judicial, esto está relativamente regulado por la ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.

Ley de Comercio Electrónico y Mensaje de Datos: Esta Ley regula los mensajes de datos, la firma electrónica, los servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos, a través de redes de información, incluido el comercio electrónico y la protección a los usuarios de estos sistemas.

En el Ecuador también existe la resolución JB-2005-834 que expidió la Junta Bancaria en octubre del 2005, que es una relativa a la Gestión del Riesgo Operativo, en la que imparte una serie de disposiciones para propender a que las instituciones del sistema financiero cuenten con un sistema para la gestión del riesgo operativo que les permita identificar, medir controlar / mitigar y monitorear los riesgos derivados de fallas o insuficiencias en los procesos, personas, tecnologías de información y eventos externos incluyendo el riesgo legal.

Esta norma determina que los plazos para que las instituciones del sistema financiero tengan implantados sus sistemas de gestión del riesgo operativo son:

31 de octubre del 2008 para grupos financieros, bancos, sociedades financieras, emisoras y administradoras de tarjetas de crédito y otras.

31 de octubre del 2009 para cooperativas de ahorro y mutualistas.

Además de estas leyes y reglamentos en el Ecuador no existen organismos oficiales encargados de asegurar servicios de prevención de riesgos y asistencia a los tratamientos de incidencias, que funcione como un centro de alerta y reacción frente a los ataques informáticos, cuya información esté disponible y accesible a todo los ecuatorianos.

Esto hace que en la actualidad en el Ecuador no se tengan datos estadísticos de incidentes informáticos, ni conocimiento general del riesgo, esto produce que en general actuemos reactivamente y no proactivamente ante algún problema de seguridad informática.

Es por esto la necesidad de contar con una evaluación que determine en nuestro país cual es el Estado del Arte actual en Seguridad Informática, ya que dará la pauta para la creación de organismos de seguridad informática que velen para que el nivel alcanzado actual mejore o se mantenga.

1.15. Tipos de Mercados en el Ecuador

Para nuestro estudio hemos clasificado al mercado Ecuatoriano en los siguientes grupos.

Corporativos.

Industriales. La actividad primordial de este tipo de empresas es la producción de bienes mediante la transformación de la materia o extracción de materias primas. Las industrias, a su vez, se clasifican en:

Extractivas. Cuando se dedican a la explotación de recursos naturales, ya sea renovable o no renovable. Ejemplos de este tipo de empresas son las pesqueras, madereras, mineras, petroleras, etc.

Manufactureras: Son empresas que transforman la materia prima en productos terminados, y pueden ser:

De consumo final. Producen bienes que satisfacen de manera directa las necesidades del consumidor. Por ejemplo: prendas de vestir, muebles, alimentos, aparatos eléctricos, etc.

De producción. Estas satisfacen a las de consumo final. Ejemplo: maquinaria ligera, productos químicos, etc.

Comerciales. Son intermediarias entre productor y consumidor; su función primordial es la compra/venta de productos terminados. Pueden clasificarse en:

Mayoristas: Venden a gran escala o a grandes rasgos.

Minoristas (detallistas): Venden al menudeo.

Comisionistas: Venden de lo que no es suyo, dan a consignación.

Servicio. Son aquellas que brindan servicio a la comunidad que a su vez se clasifican en:

Transporte

Turismo

Instituciones financieras

Servicios públicos (energía, agua, comunicaciones)

Servicios privados (asesoría, ventas, publicidad, contable, administrativo)

Educación

Finanzas

Salubridad

Carriers.

Empresas autorizadas que proveen servicio de transmisión de datos a otras empresas (ISP) las cuales a su vez distribuyen a baja escala. Son Operadores de telecomunicaciones los cuales son propietarios de las redes troncales de Internet y responsables del transporte de los datos. Proporciona una conexión a Internet de alto nivel.

Item	Operadora	Cobertura
1	CNT	Territorio Nacional
2	CONECEL	Territorio Nacional
3	ECUADORTELECOM S.A.	Territorio Nacional
4	ETAPA	Cantón Cuenca
5	ETAPATELECOM S.A.	Territorio Nacional
6	GRUPO BRAVCO CIA. LTDA.	Territorio Nacional
7	GLOBAL CROSSING	Territorio Nacional
8	MEGADATOS S.A.	Territorio Nacional
9	NEDETEL S.A.	Territorio Nacional
10	OTECEL S.A	Territorio Nacional

11	PUNTONET	Territorio Nacional
12	TRANSELECTRIC	Territorio Nacional
13	TELEHOLDING S.A.	Territorio Nacional
14	TRANSNEXA S.A.	Territorio Nacional
15	SETEL S.A	Territorio Nacional
16	SURATEL S.A.	Territorio Nacional
17	TELCONET S.A.	Territorio Nacional
18	TELECSA S.A	Territorio Nacional

Tabla 1. Operadoras en el Ecuador.

SoHo.

Small Office, Home Office (Pequeña oficina, oficina en casa) o SoHo se asocia con la categoría de negocios que van de 1 a 10 trabajadores. Empresas mayores, que no cuentan con este modelo de división del trabajo, a menudo son llamadas pequeñas y medianas empresas

Home.

Home es el mercado más común, mayoritariamente los usuarios que trabajan y operan desde casa.

1.16. Métodos para la Colección de Información de Evaluación

Encuesta: La colección de información estandarizada a través de cuestionarios estructurados para generar información cuantitativa. Las encuestas pueden ser enviadas por correo, electrónicamente, contestadas desde lugares remotos o cara a cara. Encuestas de prueba utilizan muestras de probabilidad, al contrario de las encuestas informales.

Entrevistas: Información recolectada al hablar y escuchar a gente, ya sea cara a cara o por teléfono. Pueden ser estructuradas (ej., encuesta) o conversacionales.

Observación: La colección de información a través de la vista y oído. Pueden ser estructuradas y no estructuradas.

Análisis de documentación: El uso de análisis de contenido y otras técnicas para analizar y resumir material impreso y otra información existente.

Caso de estudio: Exanimación profunda de un caso en particular (programa, grupo de participantes, individuo, sitio). Los casos de estudio usan múltiples fuentes de información y métodos que proveen una imagen tan completa posible.

Evaluación de Grupo: Se usa un grupo para recolectar información de valoración como técnicas nominales, grupos de enfoque, Delphi, lluvias de ideas y foros de comunidad.

Experto o peer review: Examinación por un comité o panel de expertos.

Repaso de portafolio: Recopilación de materiales, incluyendo muestras de trabajos que traten el tema del caso siendo estudiado.

Testimonios: Estos los hacen individuos, hablando sobre sus propias experiencias.

Exámenes: Se utilizan estas pruebas para probar la sabiduría, habilidades y funcionamiento de ciertas cosas. Por lo general se conducen en lápiz y pluma.

Fotografías, Filminas o videos: Se utilizan para captar imágenes visuales.

Diarios o periódicos: Reportan eventos desde el punto de vista del autor/ reportero.

Logs: Grabación de eventos cronológicos, generalmente breves y descriptivos.

Técnica de evaluación seleccionada: La Encuesta.

Se seleccionó como técnica de evaluación, la encuesta, en base a que mediante la misma se obtiene datos de diferentes personas (empresas) respecto a un tema, situación o problema; describiendo el funcionamiento que permita comparar situaciones anteriores y las condiciones existentes en el desarrollo de la situación evaluada. La información que se obtiene es un recurso valioso y aplicable a sectores magnos del universo; del cual se obtienen importantes opiniones.

CAPÍTULO 2

2. Análisis de los Resultados

En inferencia estadística se llama estimación al conjunto de técnicas que permiten dar un valor aproximado de un parámetro de una población a partir de los datos proporcionados por una muestra.

En nuestro estudio se ha seleccionado una muestra entre las empresas y los usuarios Home, a los mismos que se les realizará las encuestas; para lo cual se escogió trabajar con un nivel de confianza del 91%, y a su vez; un grado de significancia del 9%.

Se utilizará la siguiente fórmula para calcular el tamaño de la muestra, para el caso de una población infinita:

$$n = \frac{z^2 (p * q)}{e^2}$$

Donde:

n: Tamaño de la muestra.

Z: Porcentaje de datos que se alcanza dado un porcentaje de confianza del 91%.

p: Probabilidad de éxito.

q: Probabilidad de fracaso.

e: Máximo error permisible.

Considerando a p y q como 0,5 y trabajando con el valor de Z correspondiente para este caso, se obtiene:

$$1-\propto= 0.91$$

$$\propto= 0.09$$

$$\frac{\propto}{2} = 0.045$$

$$Z_{0.045} = 1.70$$

$$\frac{1.70^2 * 0.5 * 0.5}{0.09^2} = 89$$

Por ende se trabajará con una muestra de 89 empresas y 120 usuarios Home.

- Hemos efectuado 89 encuestas a empresas dentro del Ecuador de los diferentes sectores económicos, indistintamente del servicio que brinden, el cual nos permitan analizar:
    - Las diferentes tecnologías e información de los servicios actuales que utilizan las empresas.
    - Los dispositivos en el desenvolvimiento diario de las actividades de su empresa.

- Los niveles de seguridad actuales.
- Políticas Globales de Seguridad.
- Agresiones externas y los controles de acceso.
- Mecanismos de Identificación y Autentificación.
- Niveles de Planes de Seguridad y Contingencia.

- Hemos efectuado 120 encuestas a usuarios Home dentro del Ecuador de los diferentes estados de los encuestados, el cual nos permitan analizar:
  - El nivel conocimientos sobre Seguridad Informática que poseen los usuarios.
  - Las ideas sobre sistemas operativos, amenazas, antivirus, uso de la Internet y programas ilegales.

2.1. Empresas

2.1.1. Clasificación de las Empresas

Se decidió clasificar a las empresas en tres grupos: Pequeñas y Medianas Empresas (PYME), Corporativo y Proveedores de Internet. En su totalidad hay una clara mayoría de Empresas Corporativas (54%).

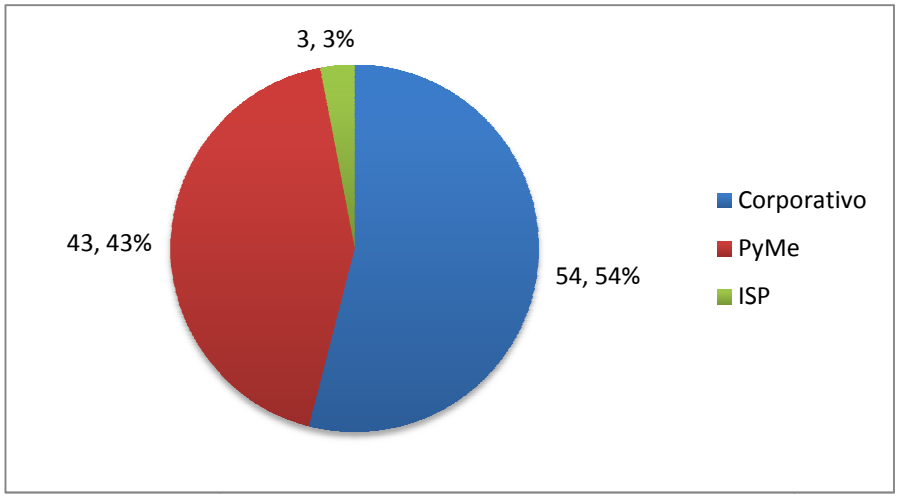

Fig. 2 1 Gráfico de la Clasificación de las Empresas

2.1.2. Número de Empleados

En cuanto al tamaño de las empresas, las cifras muestran que poseen menos de 50 empleados, podemos visualizar en el siguiente gráfico:

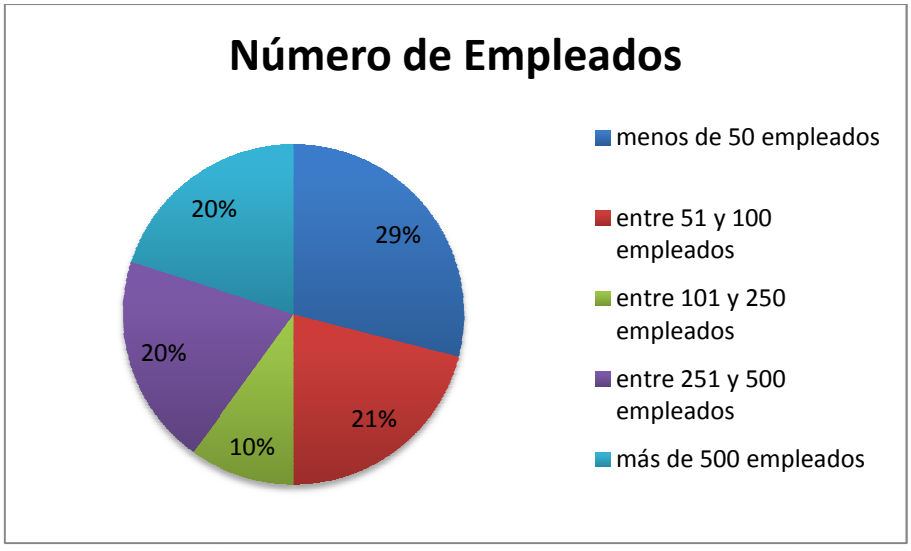

Fig. 2 2 Número de Empleados

2.1.3. Sector

Las cifras muestran que el sector más significativo es el Comercio, seguido del de Servicios y Financiero. Cabe destacar que el 54% aproximadamente se reparte entre los otros sectores.

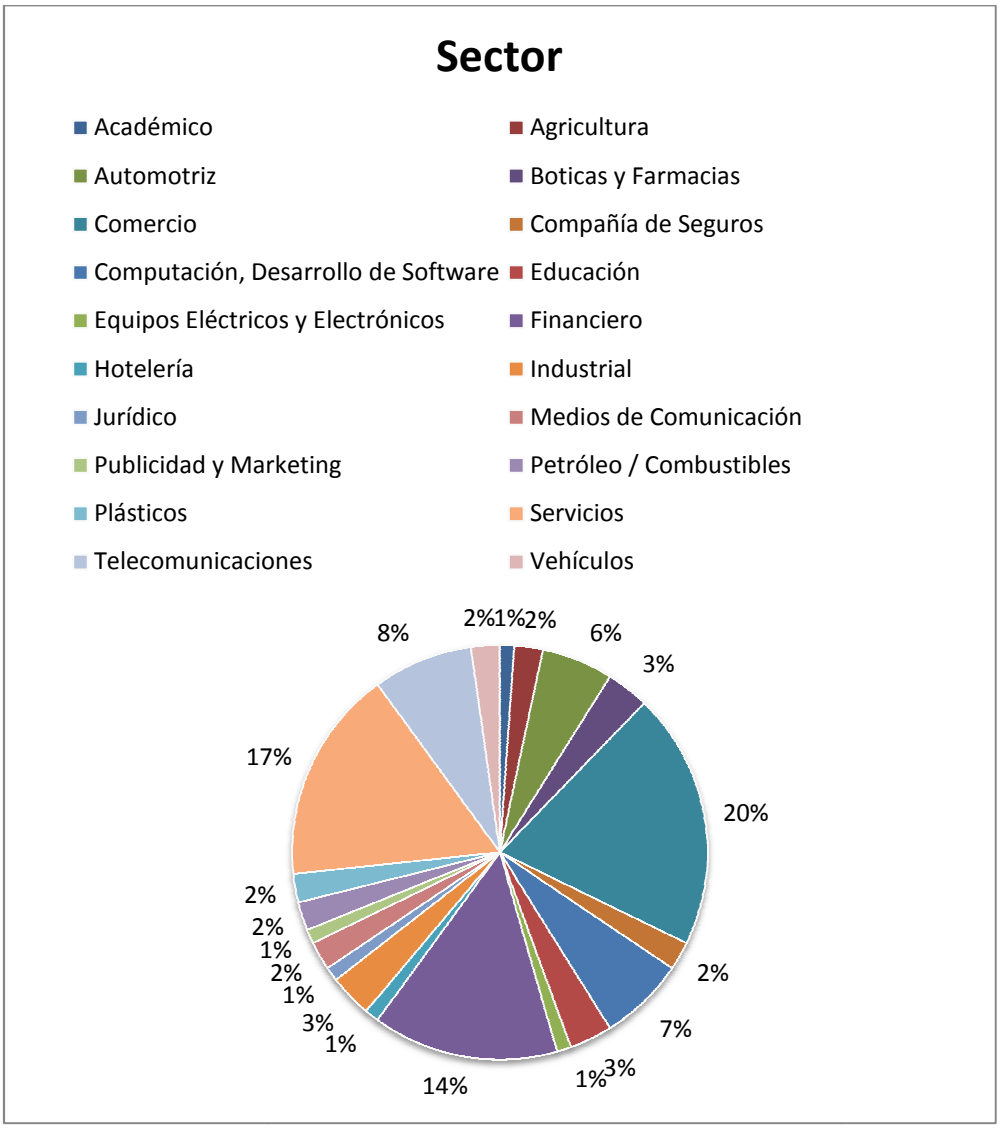

Fig. 2 3 Sector al que pertenecen las diferentes empresas.

2.1.4. Enfoque de las Empresas

Fig. 2 4 Enfoque de las Empresas

2.1.5. Información sobre Servicios Actuales

- **Servicio de Internet**

El internet se ha convertido en algo imprescindible dentro de las organizaciones y podemos observar que en la totalidad de las mismas todos poseen mencionado servicio.

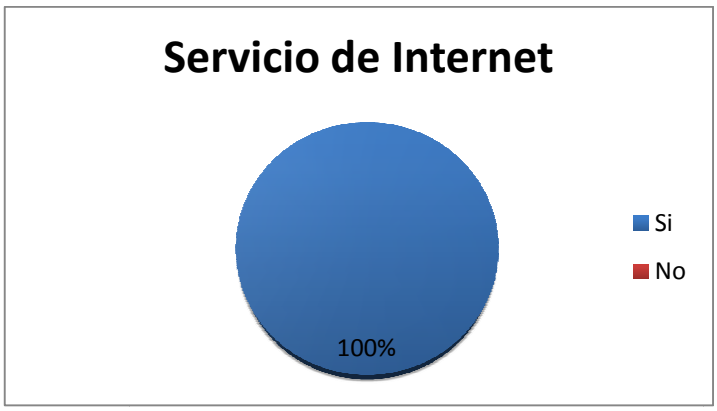

Fig. 2 5 Uso del Servicio de Internet.

- **Número de Usuarios con Acceso a Internet**

En la actualidad hay entre 51 a 250 usuarios con acceso a internet.

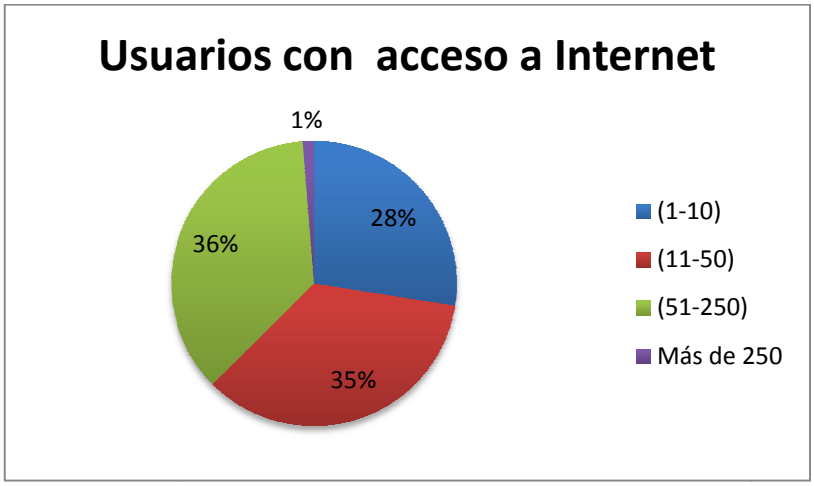

Fig. 2 6 Número de usuarios que tienen acceso a Internet.

- **Servicio de Transmisión de Datos**

En la actualidad es sumamente importante poseer algún servicio de transmisión de datos.

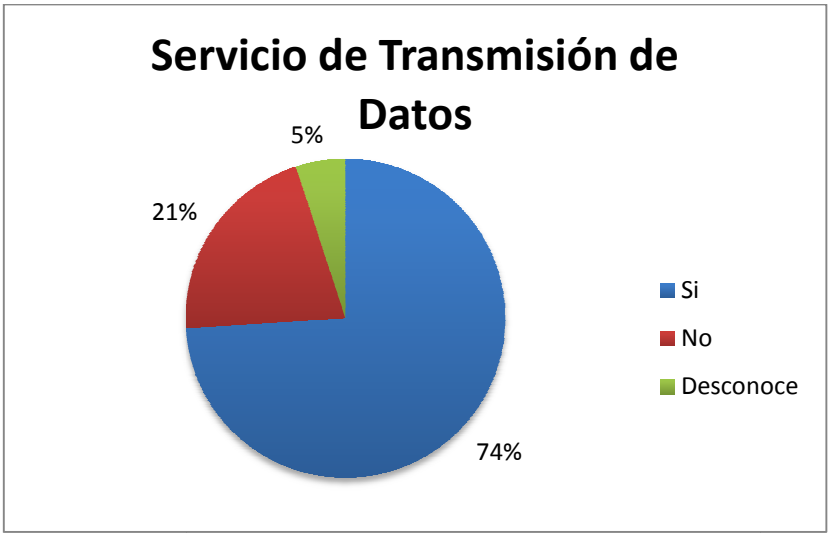

Fig. 2 7 Uso del Servicio de Transmisión de Datos.

- **Número de Usuarios con Servicio de Transmisión de Datos**

En la actualidad hay entre 1 a 10 usuarios con acceso a internet.

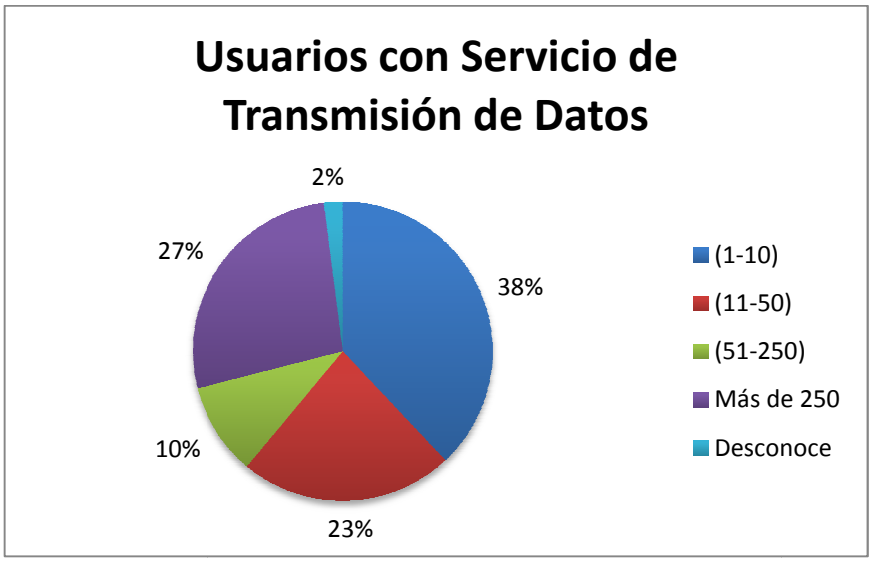

Fig. 2 8 Número de usuarios que tienen Servicio de Transmisión de Datos.

- **Aplicaciones a través del enlace de Internet**

La importancia de interactuar a través de los diferentes espacios que hay en el Internet, y al utilizar aplicaciones que permitan la comunicación y colaboración.

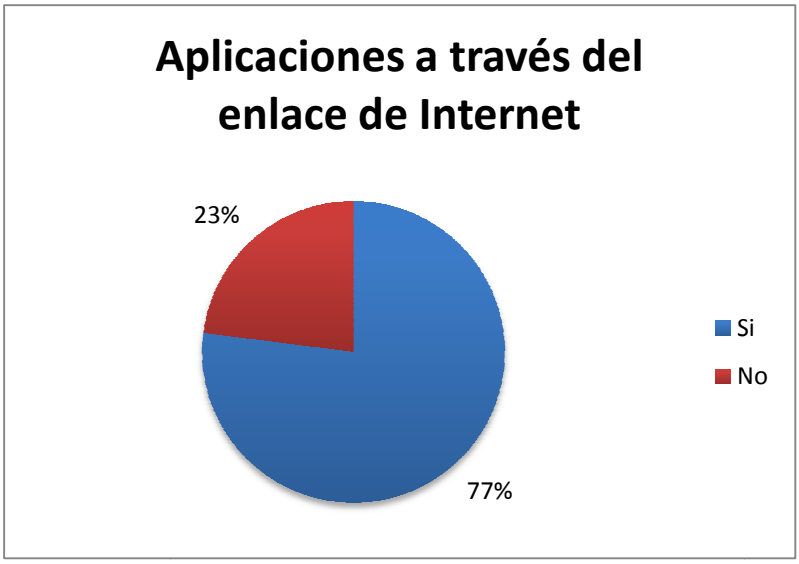

Fig. 2 9 Número de usuarios que tienen Servicio de Transmisión de Datos.

- **Cumplimiento de las Normas de acuerdo al Modelo de Negocio**

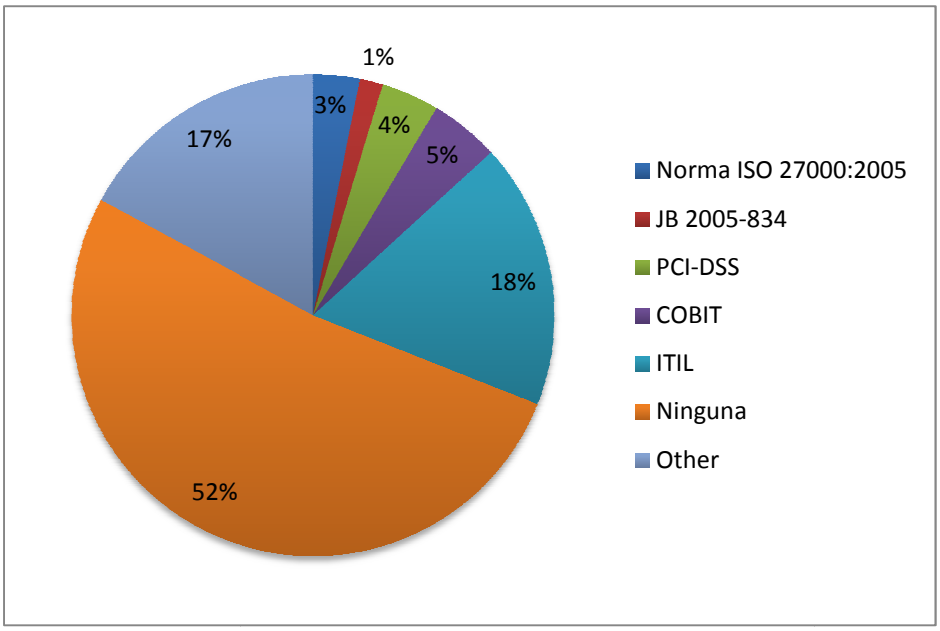

Fig. 2 10 Normas de acuerdo al Modelo de Negocio.

- **Realiza Outsourcing de Seguridad Informática**

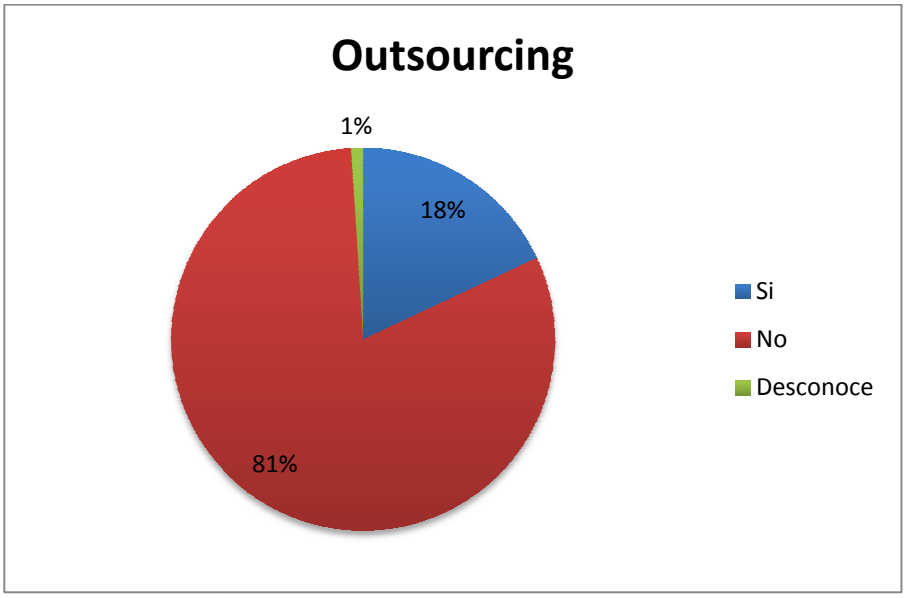

Fig. 2 11 Empresas que realizan Outsourcing de Seguridad Informática

---

2.1.6. Evaluación de la Importancia de la Información

Dentro de la Evaluación de la Importancia de la Información, se considera importante evaluar en base a ciertos dispositivos, donde se ha usado una escala de 1 a 5, donde 1 indica el menor grado de importancia, 3 indica importancia intermedia y el 5 indica el mayor grado de importancia, esto permitirá observar cuáles son los más valiosos para el desenvolvimiento de las actividades diarias dentro de la empresa.

- **Servidor de Correo**

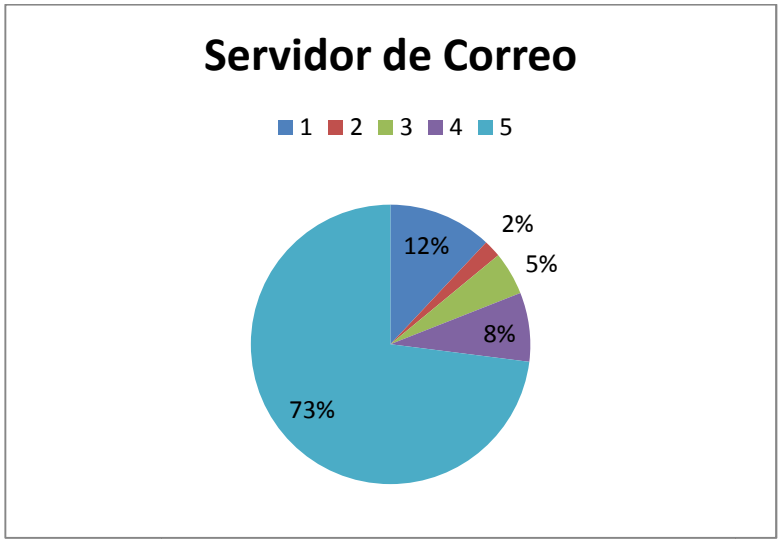

Fig. 2 12 Importancia del Dispositivo Servidor de Correo dentro de las Empresas.

- **Servidor Web**

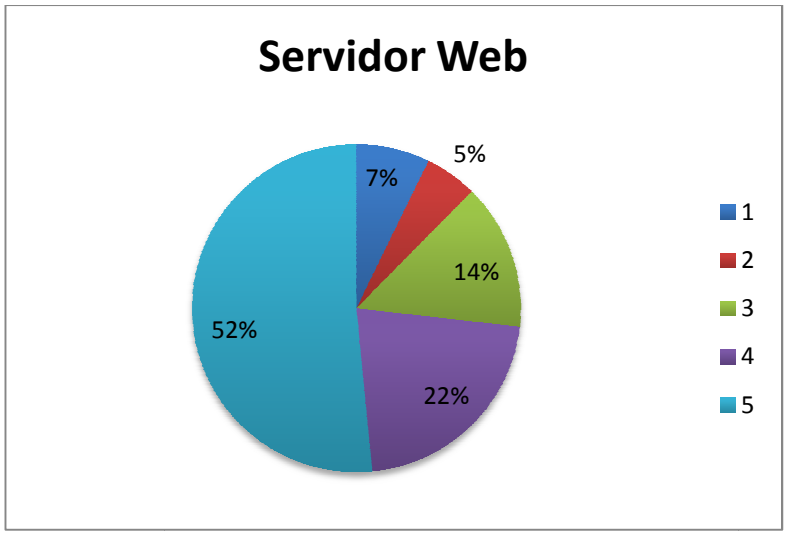

Fig. 2 13 Importancia del Dispositivo Servidor Web dentro de las Empresas.

- **Servidor de Aplicaciones**

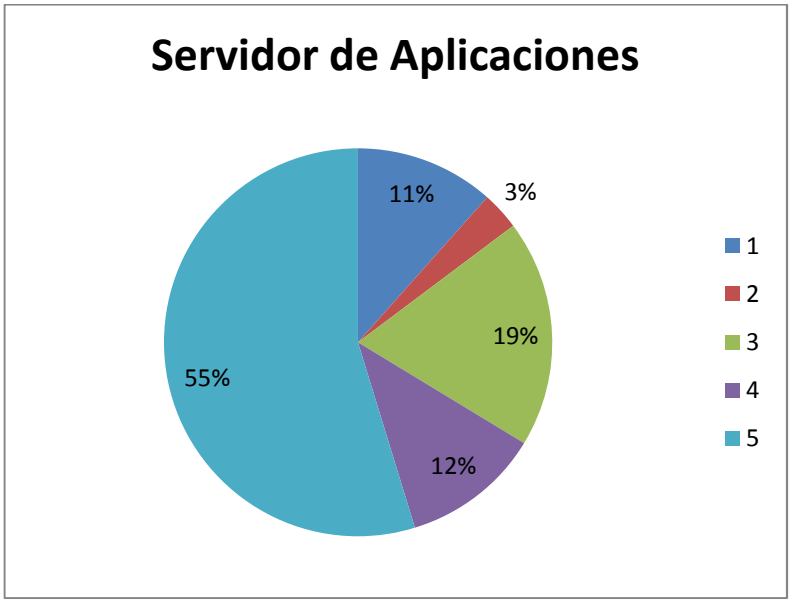

Fig. 2 14 Importancia del Dispositivo Servidor de Aplicaciones dentro de las Empresas.

- **Servidor de Dominios**

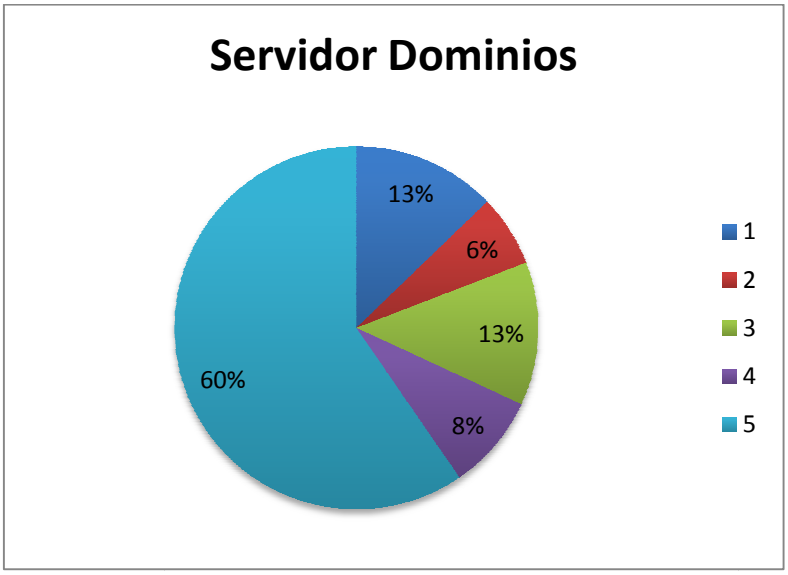

Fig. 2 15 Importancia del Dispositivo Servidor de Dominios dentro de las Empresas.

- **Servidor DNS**

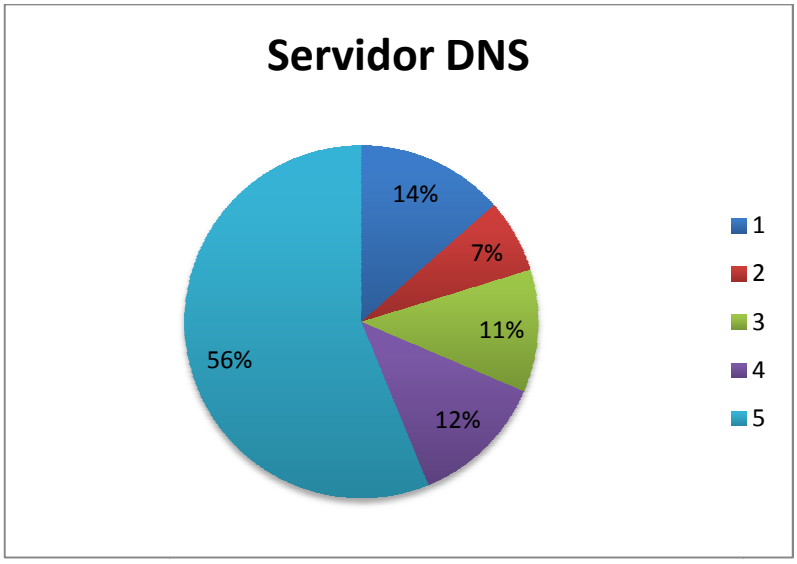

Fig. 2 16 Importancia del Dispositivo Servidor de DNS (Domain Name System) dentro de las Empresas.

- **Servidor Base de Datos**

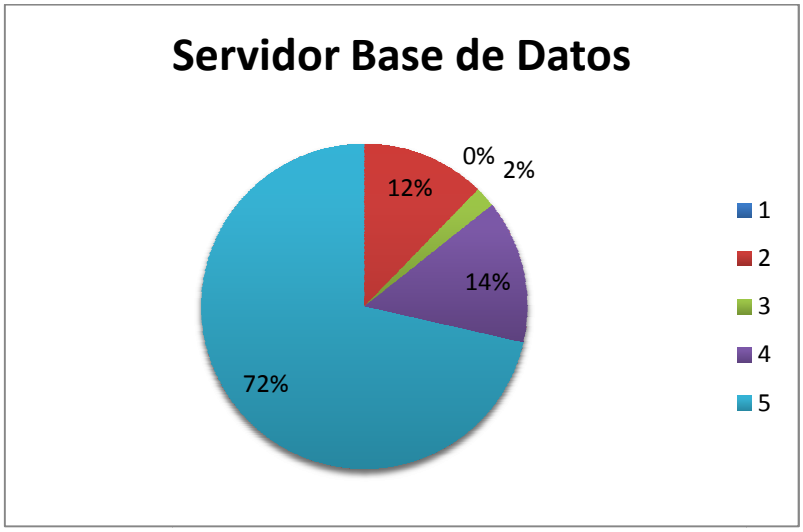

Fig. 2 17 Importancia del Dispositivo Servidor de Base de Datos dentro de las Empresas.

- **Firewall**

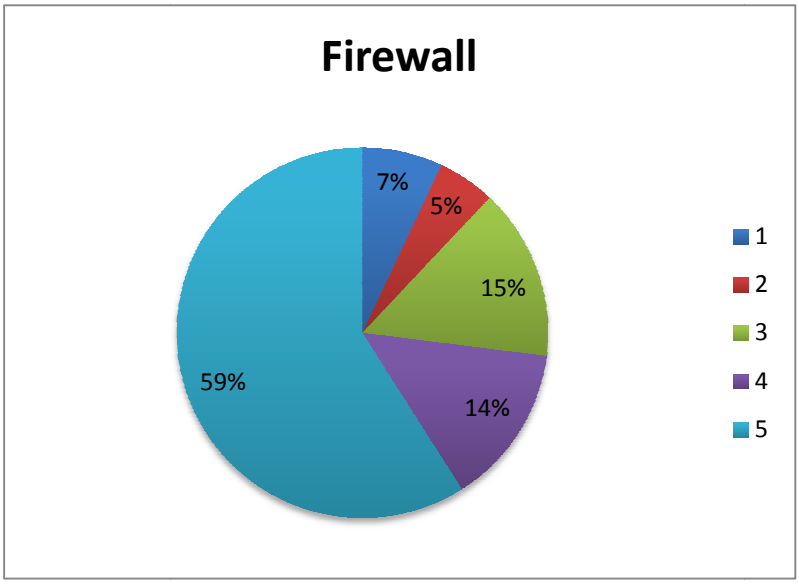

Fig. 2 18 Importancia del Dispositivo Firewall dentro de las Empresas.

- **Routers**

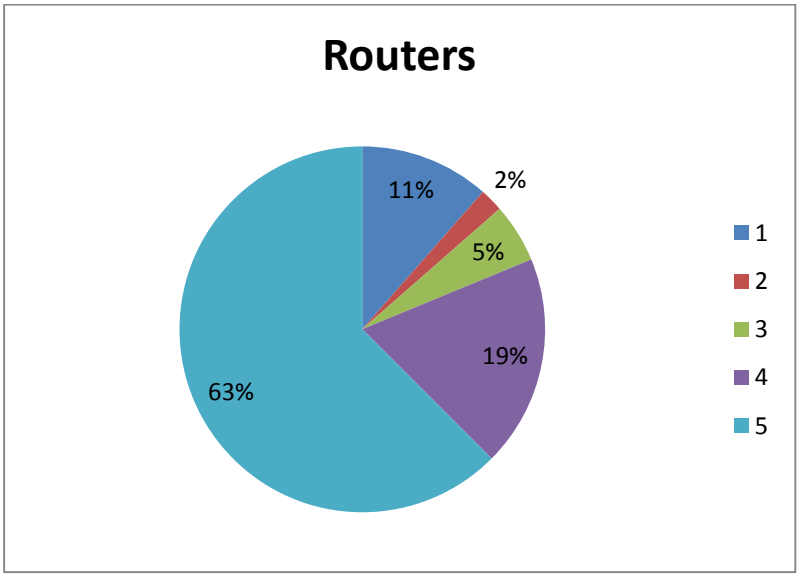

Fig. 2 19 Importancia del Dispositivo Routers dentro de las Empresas.

- **Otros**

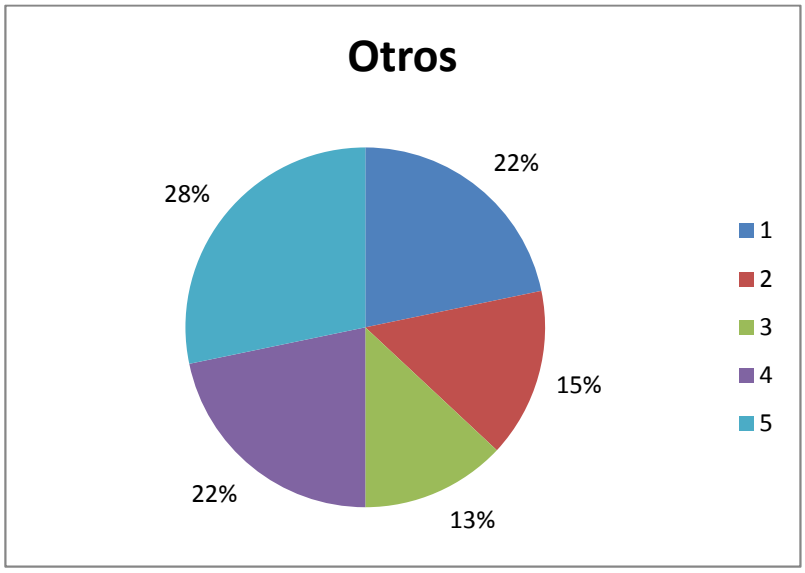

Fig. 2 20 Importancia de Otros Dispositivos dentro de las Empresas.

- **Identificación de los procesos más críticos del Negocio.**

Se puede indicar que la gran mayoría tiene identificado los procesos más críticos de su empresa, cabe destacar que eso varía según el sector al que pertenece, entre ellos podríamos mencionar Soporte a Usuarios, Facturación, Venta, Manejo de Calidad de Servicio, Transferencia de Datos, Seguimiento de Información, Plan de Continuidad de Negocio, DataWarehouse, Respaldo de Información, Monitoreo de Servicios y Sistemas de Información.

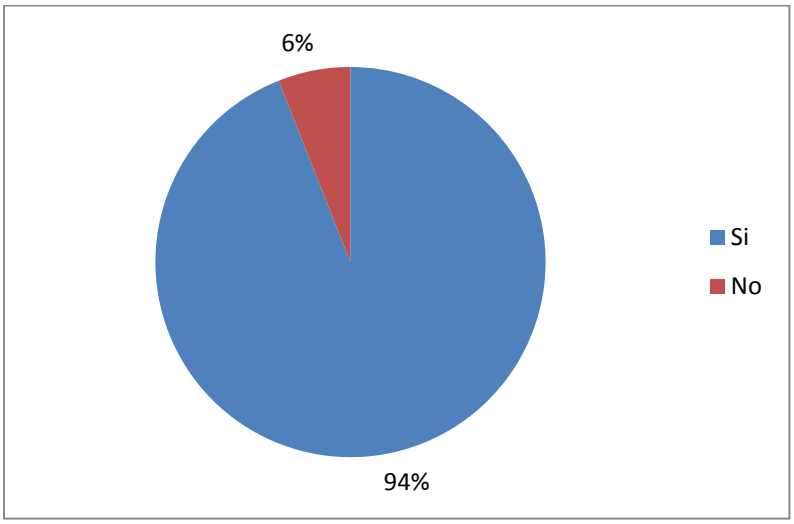

Fig. 2 21 Identificación de los Procesos Críticos de las Empresas.

- **Personal que proporcione soporte a la Empresa.**

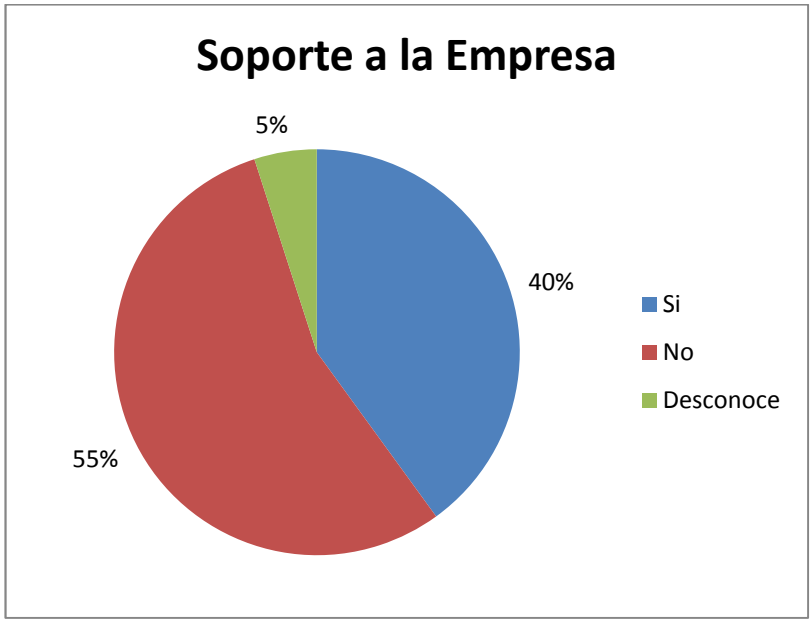

Fig. 2 22 Personal que proporcione Soporte a las Empresas.

2.1.7. Evaluación de Niveles de Seguridad Actuales.

- **Dispositivos de Seguridad Perimetral**

Entre los dispositivos de seguridad perimetral, el 50% de las empresas poseen un Firewall, luego un 66% de las mismas poseen además un IDS.

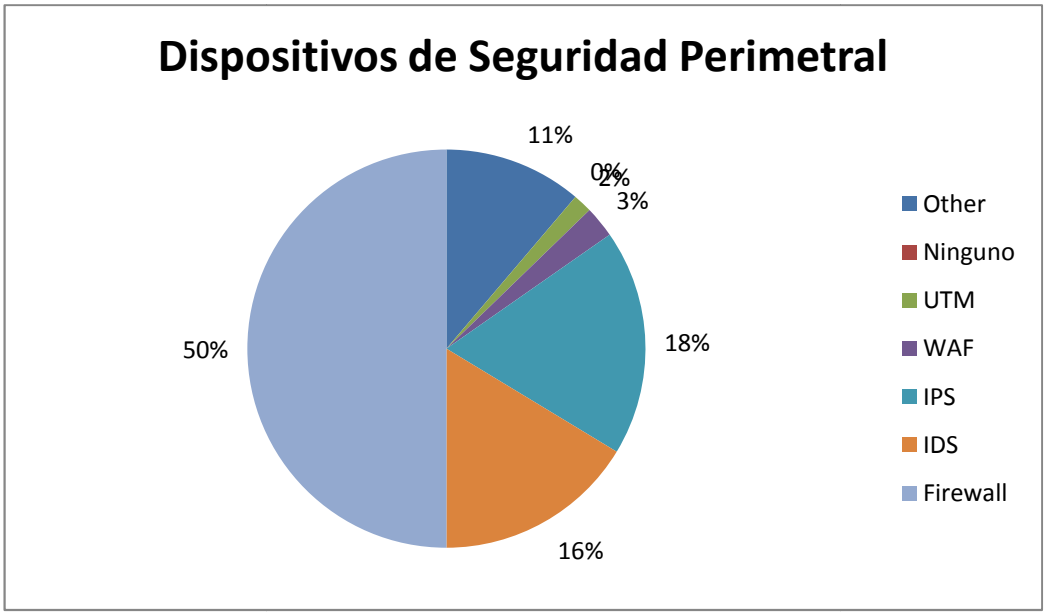

Fig. 2 23 Dispositivos de Seguridad Perimetral que poseen las Empresas.

2.1.8. Política Global de Seguridad

Esta política definiría ciertos criterios y lineamientos a seguir dentro de la organización.

- **¿Ha tenido en cuenta la posibilidad de perder información, que te roben, que no sea correcta?**

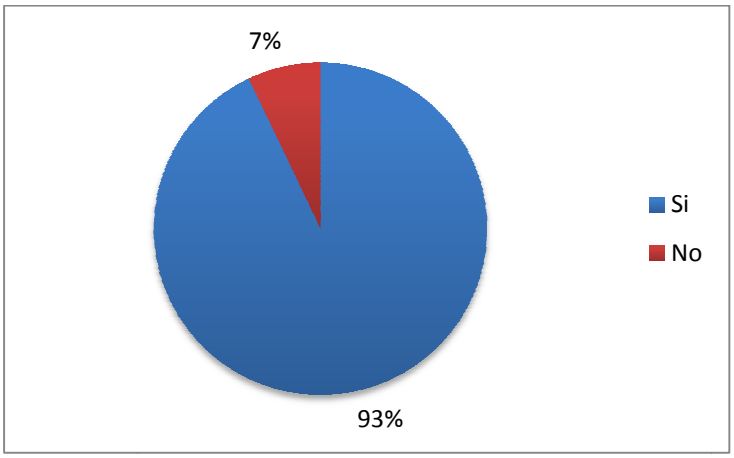

Fig. 2 24 Personal que proporcione Soporte a las Empresas.

- **¿Se ha definido una política global de seguridad en la empresa?**

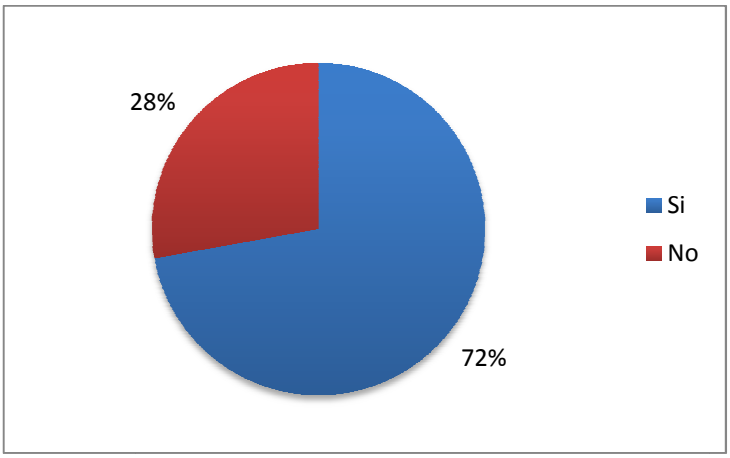

Fig. 2 25 Política Global de Seguridad definida en la Empresa.

- **¿Poseen un área de Seguridad Informática?**

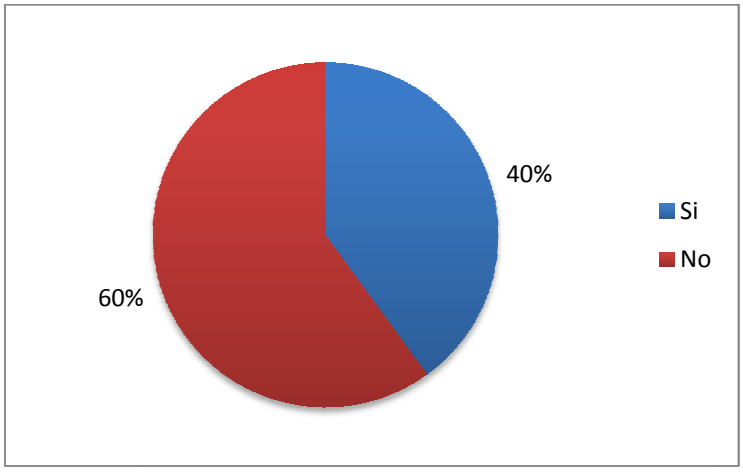

Fig. 2 26 Área de Seguridad Informática definida en la Empresa.

- **¿Se hace algún tipo de revisión del sistema de información de forma periódica?**

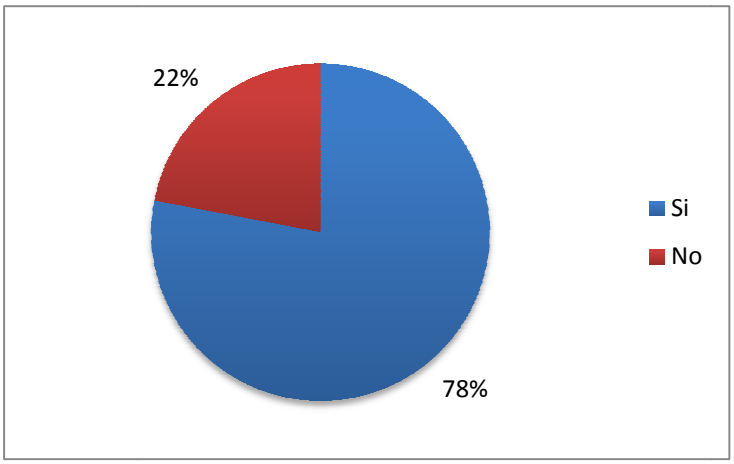

Fig. 2 27 Revisión del Sistema de Información de forma periódica.

- **Considera Ud. ¿Qué posee un alto nivel de Seguridad de Información?**

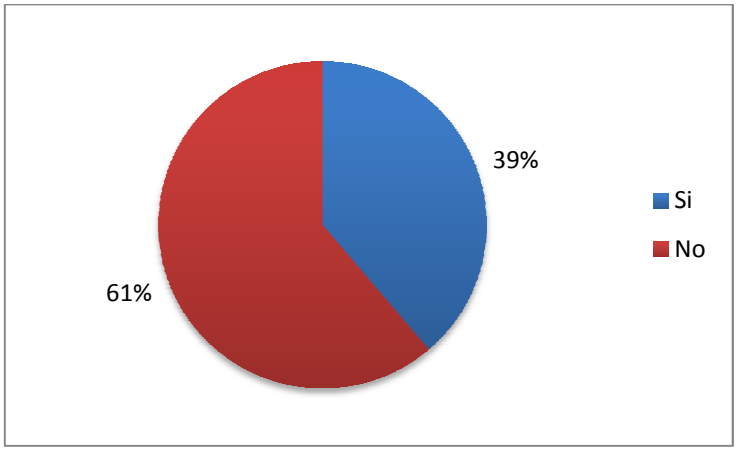

Fig. 2 28 Alto nivel de Seguridad de Información.

- **¿Existen controles que detecten posibles fallos en la seguridad?**

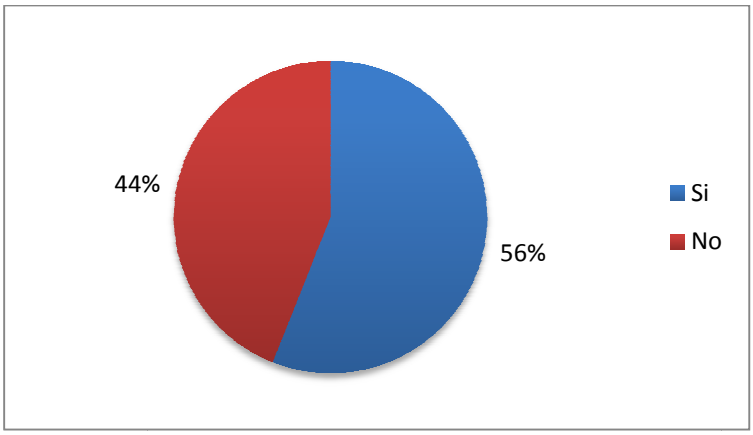

Fig. 2 29 Controles que detecten posibles fallos de seguridad.

- **¿Se ha definido el nivel de acceso de los usuarios?, es decir, a qué recursos tienen acceso y a que recursos no.**

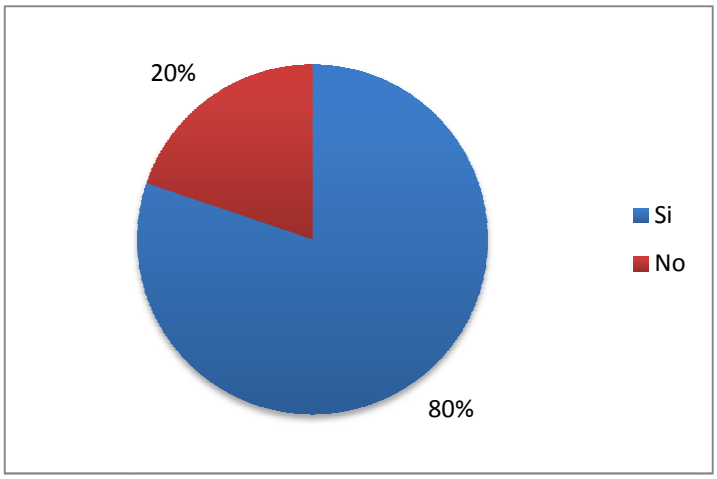

Fig. 2 30 Definición del Nivel de Acceso a los Usuarios.

2.1.9. Agresiones Físicas Externas

- **¿Existen filtros y estabilizadores eléctricos en la red eléctrica de suministro a los equipos?**

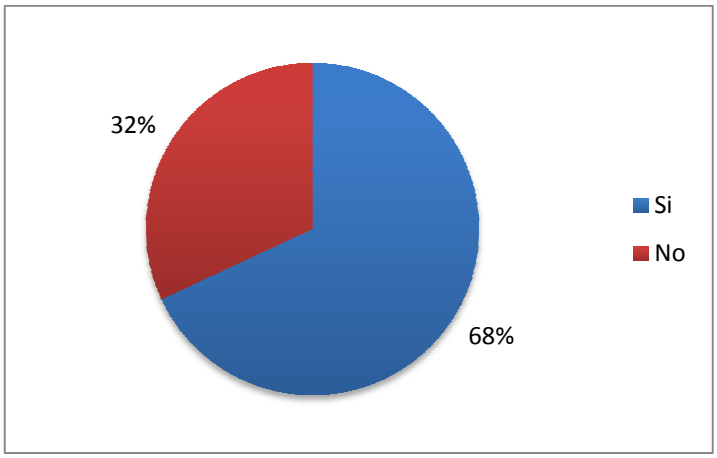

Fig. 2 31 Definición del Nivel de Acceso a los Usuarios.

- **¿Tienen instaladas fuentes de alimentación redundantes?**

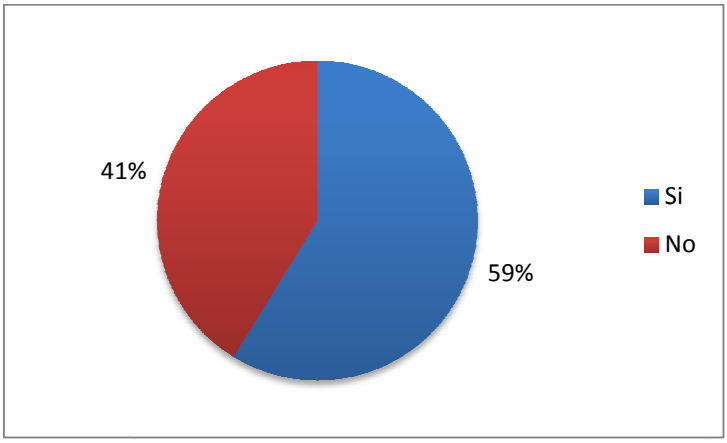

Fig. 2 32 Fuentes de alimentación redundantes instaladas.

- **¿Tienen instalados Sistemas de Alimentación Ininterrumpida?**

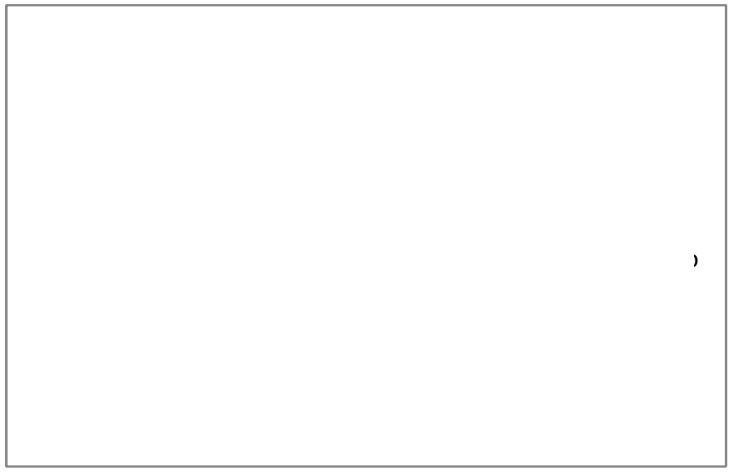

Fig. 2 33 Sistemas de Alimentación Ininterrumpida.

2.1.10. Controles de Acceso Físico

- **¿Existe algún control que impida el acceso físico a los recursos a personal no autorizado? (Puertos de Seguridad, alarmas, controles de acceso mediante tarjetas).**

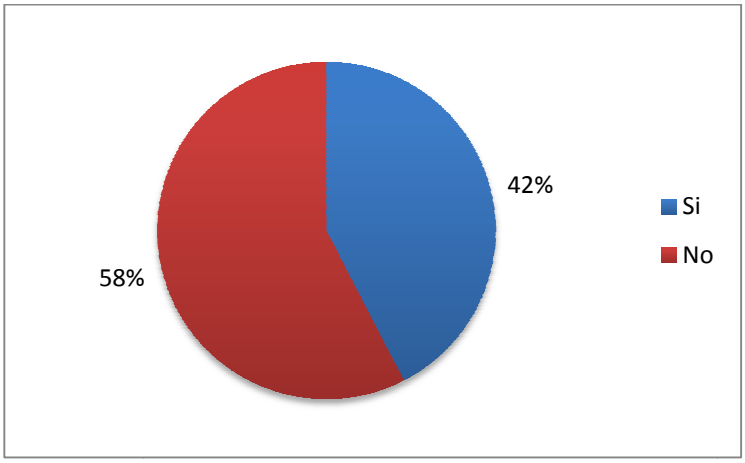

Fig. 2 34 Controles que impida el acceso físico a los recursos no autorizados.

- **¿Existe algún mecanismo físico que impida el uso de los sistemas de información a mecanismos no autorizados?**

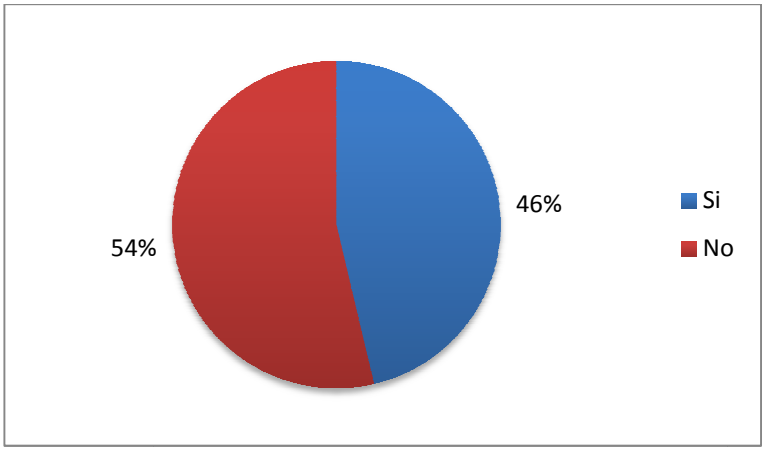

Fig. 2 35 Mecanismo físico que impida el uso de los sistemas de información a mecanismos no autorizados.

2.1.11. Servidores

- **¿Posee servidor web?**

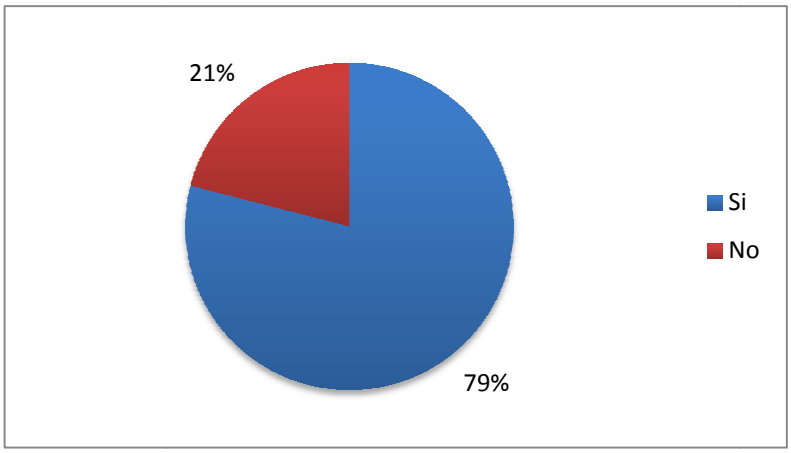

Fig. 2 36 Servidor Web que posee la Empresa.

- **¿Alguna vez ha sido víctima de ataques?**

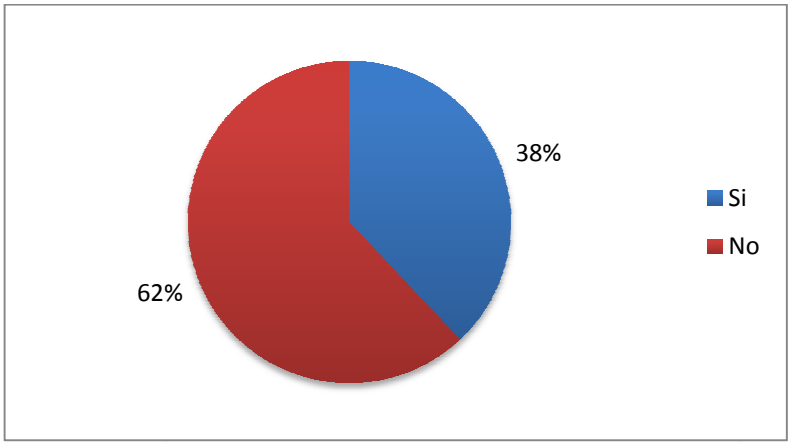

Fig. 2 37 Víctima de algún ataque.

- **Escoja:**

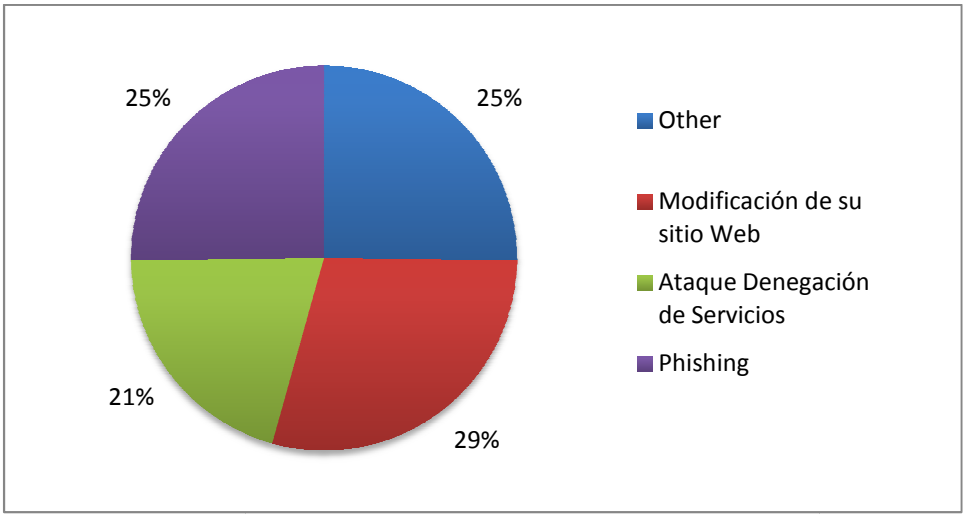

Fig. 2 38 Ataques que sufren las organizaciones.

- **¿Existen sistemas operativos servidores que impiden el acceso a los datos a los usuarios no autorizados?**

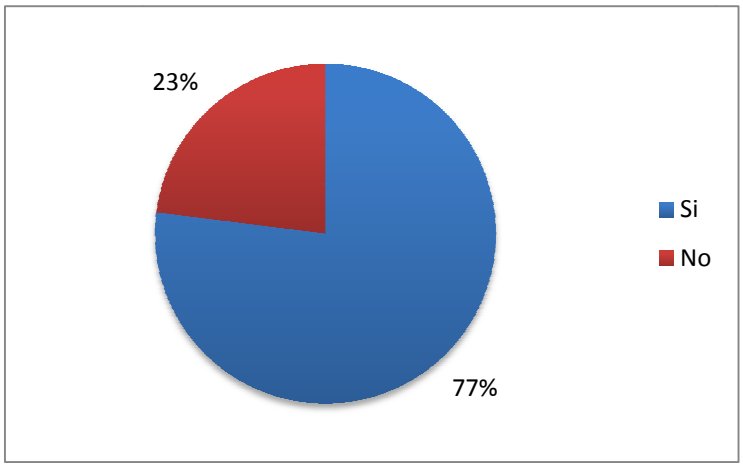

Fig. 2 39 Sistemas Operativos servidores que impiden el acceso a los datos a los usuarios no autorizados.

- **¿Están los servidores protegidos en cuanto a inicio de sesión y accesos a través de la red?**

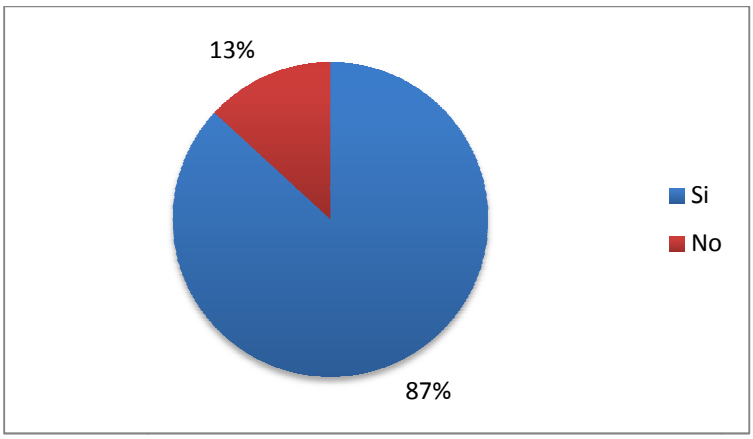

Fig. 2 40 Servidores protegidos en cuanto a inicio de sesión y accesos a través de la red.

- **¿Tienen instalados fuentes de alimentación redundantes?**

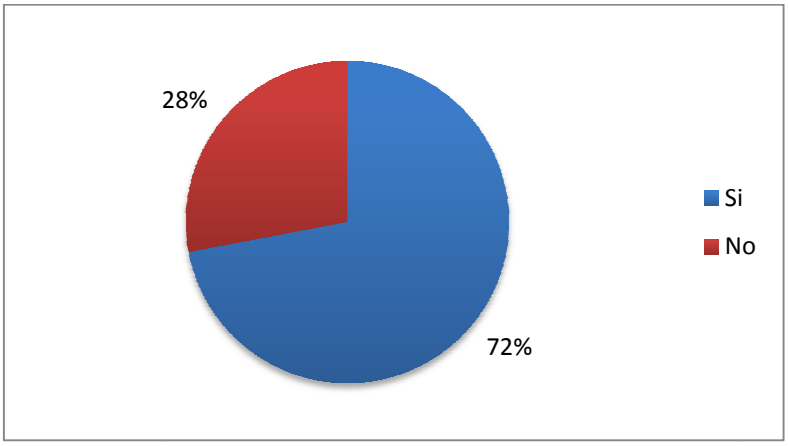

Fig. 2 41 Fuentes de alimentación redundantes instalados.

- **¿Tienen instalados Sistemas de Alimentación Ininterrumpida?**

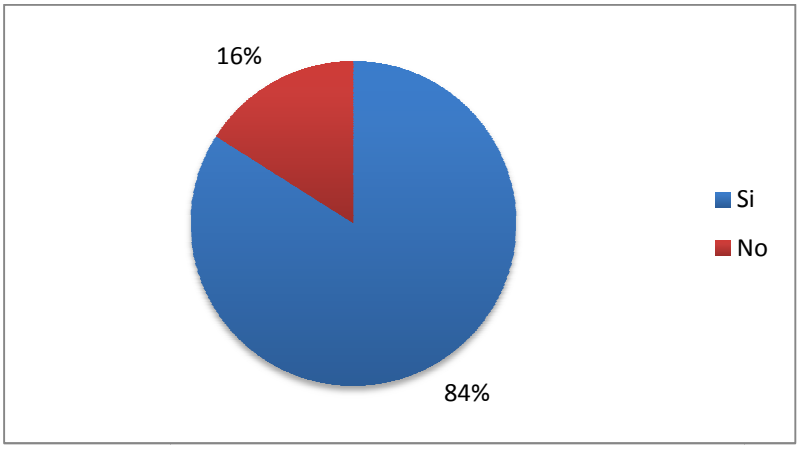

Fig. 2 42 Sistemas de alimentación ininterrumpida instalados.

- **¿Tienen aplicado un Sistema RAID?**

Fig. 2 43 Aplica Sistema RAID.

2.1.12. Copias de Seguridad

- **¿Se realizan copias de los datos?**

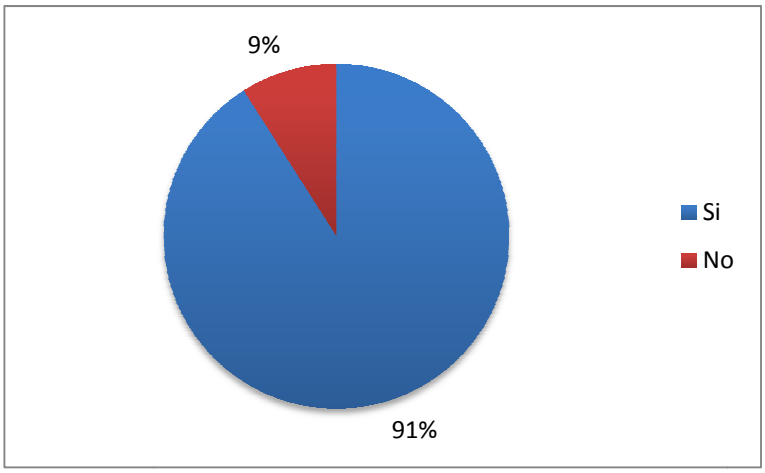

Fig. 2 44 Copia de los Datos.

- **¿Con qué periodicidad se realizan copias de los datos?**

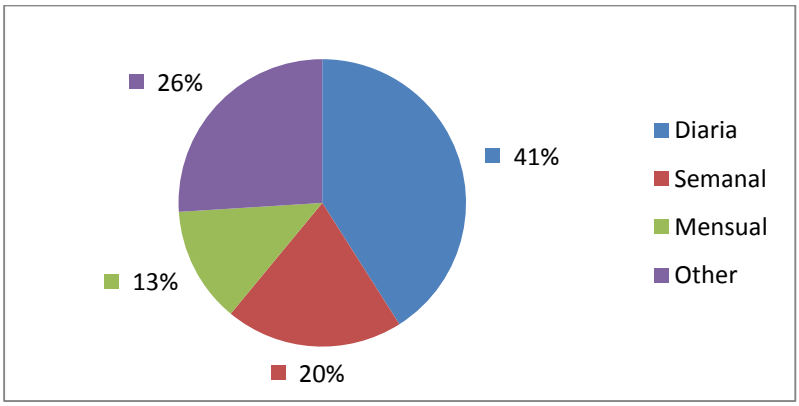

Fig. 2 45 Copia de los Datos, periodicidad.

- **¿Existe un procedimiento de copia de seguridad?**

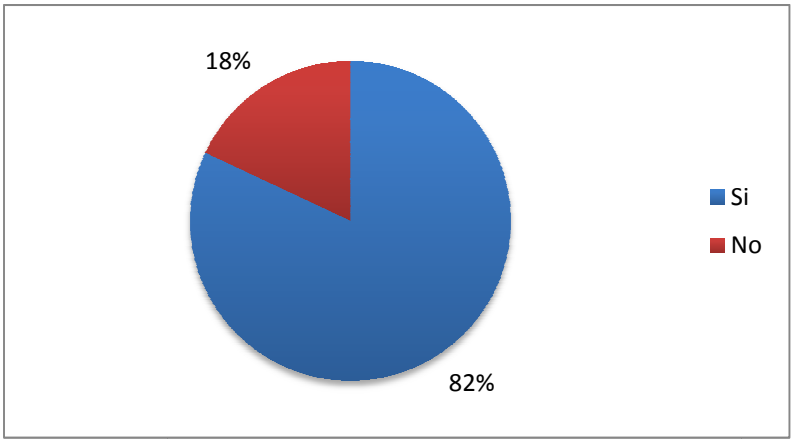

Fig. 2 46 Procedimiento de Copia de Seguridad.

- **¿Está automatizado?**

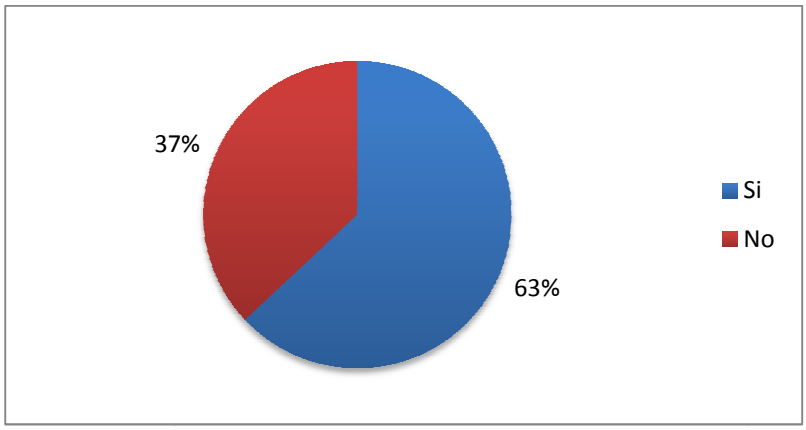

Fig. 2 47 Proceso que está automatizado.

- **¿Se almacenan las copias de seguridad en un lugar de acceso restringido?**

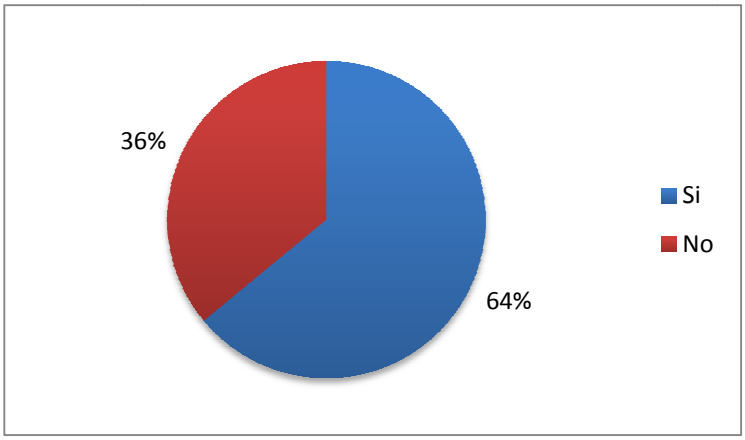

Fig. 2 48 Almacenamiento en lugares de acceso restringido.

- **¿Se almacena alguna copia fuera de los locales de trabajo?**

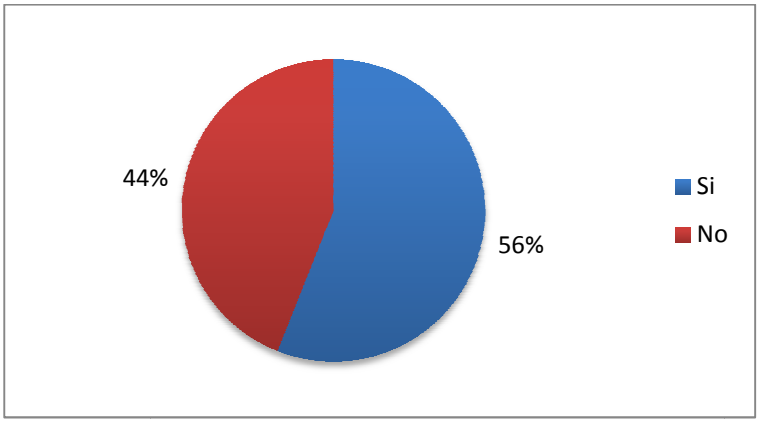

Fig. 2 49 Almacenamiento de copia fuera del lugar de trabajo.

- **¿Ha probado restaurar alguna copia de seguridad?**

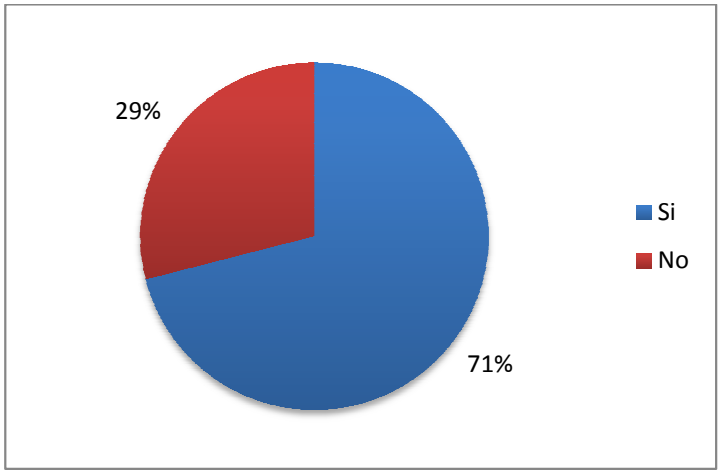

Fig. 2 50 Ha restaurado Copias de Seguridad.

2.1.13. Mecanismos de Identificación y Autenticación

- **¿Existe un procedimiento de Identificación?**

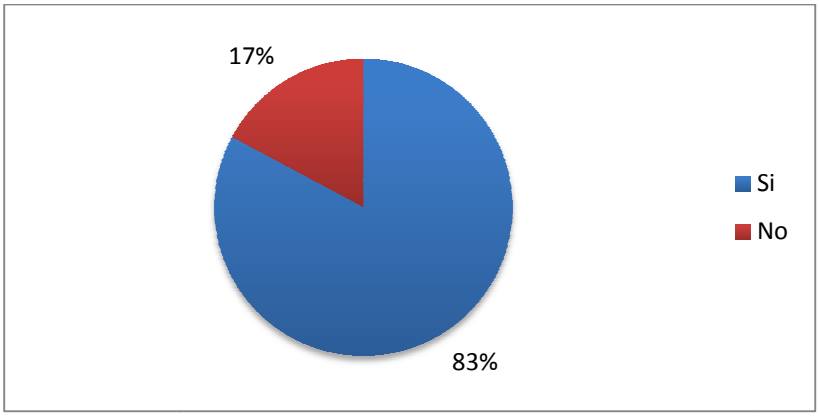

Fig. 2 51 Procedimiento de Identificación.

- **¿Existe un procedimiento de Autentificación?**

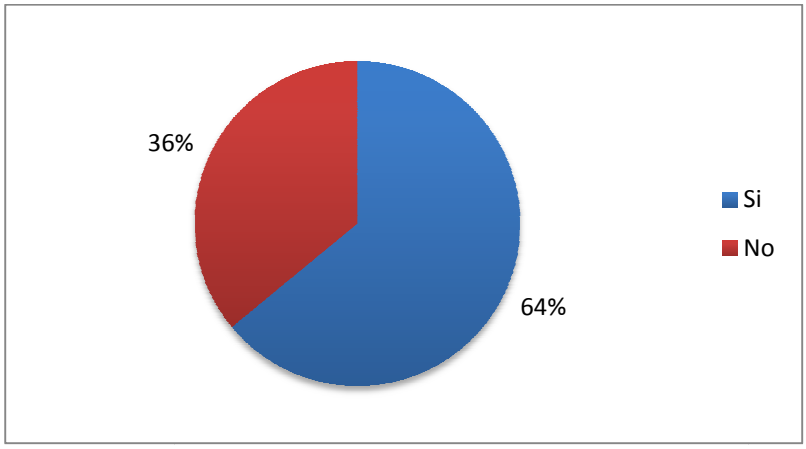

Fig. 2 52 Procedimiento de Autentificación.

- **¿Existe un procedimiento de Accounting?**

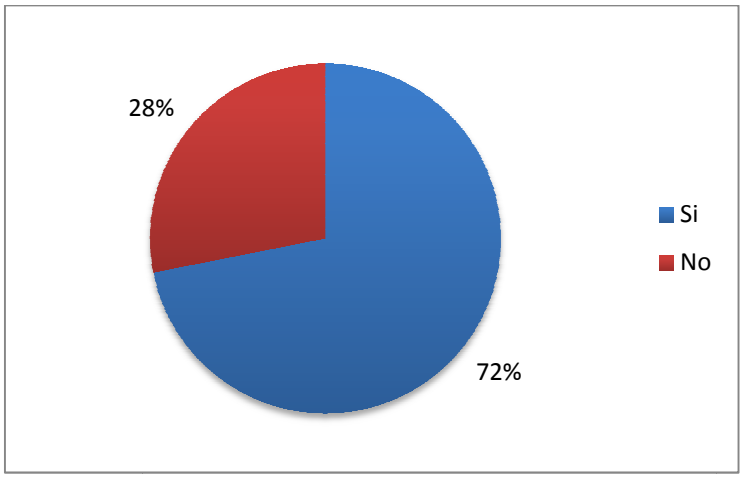

Fig. 2 53 Procedimiento de Accounting.

- **¿Las contraseñas se asignan de forma automática por el servidor?**

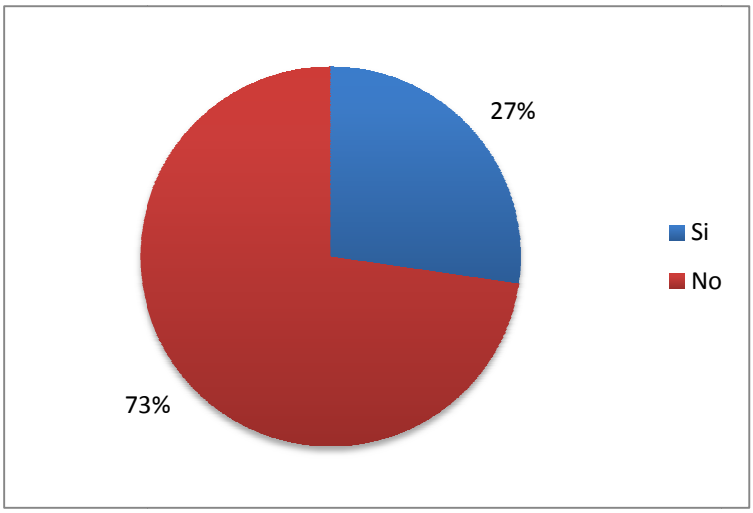

Fig. 2 54 Se asignan contraseñas de forma automática por el servidor.

- **¿Existe un procedimiento de cambio de contraseñas?**

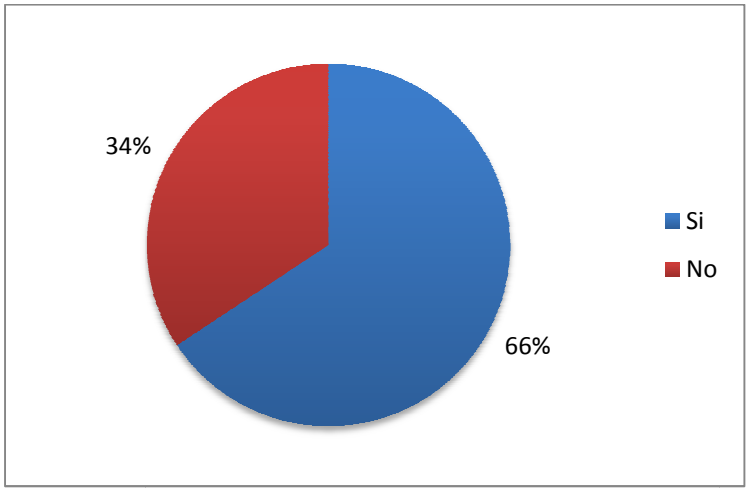

Fig. 2 55 Procedimiento de Cambio de Contraseñas.

2.1.14. Controles de Acceso (Físico)

- **¿Existen controles para el acceso a los recursos?**

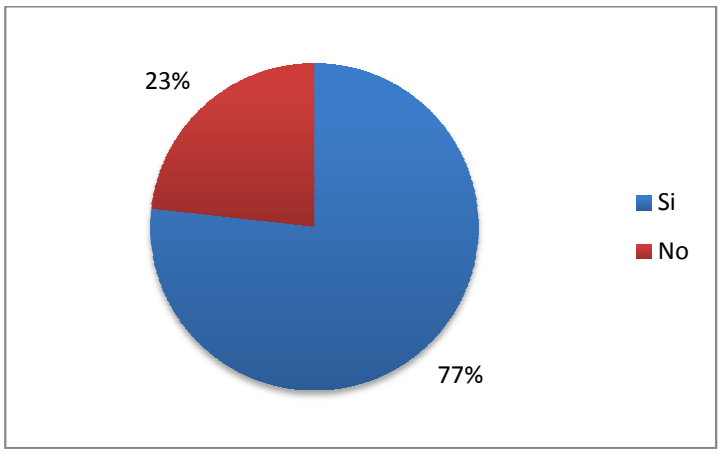

Fig. 2 56 Controles para el acceso a los recursos.

- **¿Existen ficheros de log o similares que registren los accesos autorizados y los intentos de acceso ilícitos?**

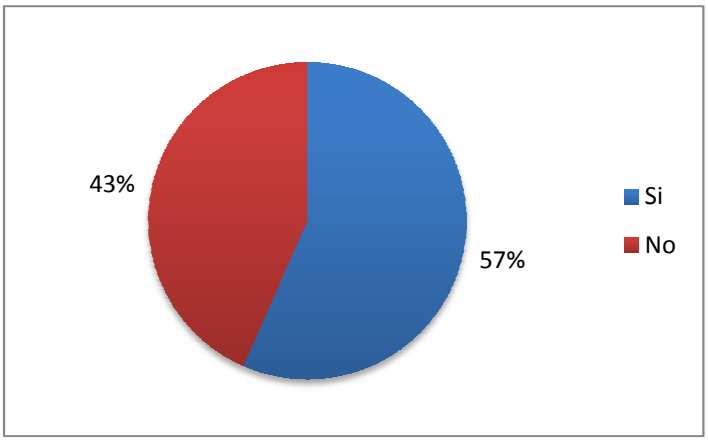

Fig. 2 57 Registran los accesos autorizados y los intentos de acceso ilícitos.

- **Una vez pasados los filtros de identificación, ¿Se han separado los recursos a los que tiene acceso cada usuario?**

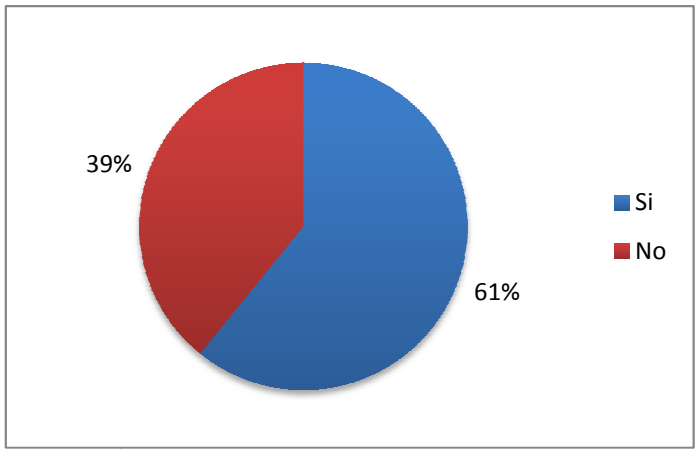

Fig. 2 58 Separación de los recursos a los que tiene acceso cada usuario.

2.1.15. Virus

- **¿Tiene cuentas de correo electrónico de Internet?**

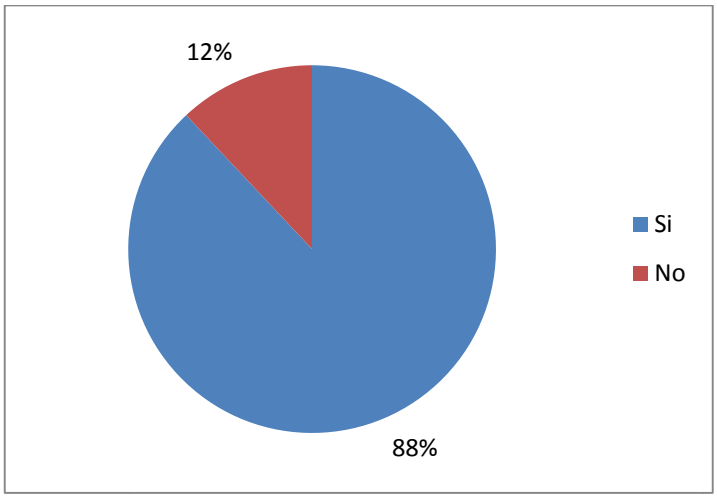

Fig. 2 59 Los Usuarios poseen cuentas de correo electrónico de Internet.

- **¿Tiene antivirus corporativo?**

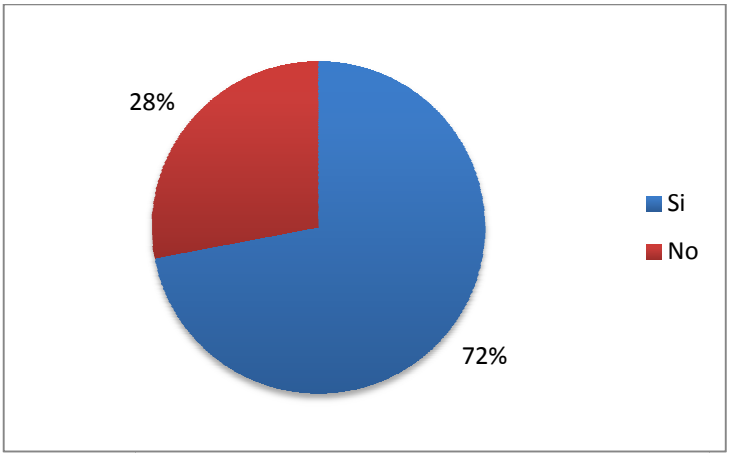

Fig. 2 60 Poseen Antivirus Corporativo.

- **¿Protege su antivirus los correos electrónicos y la descarga de archivos vía Web?**

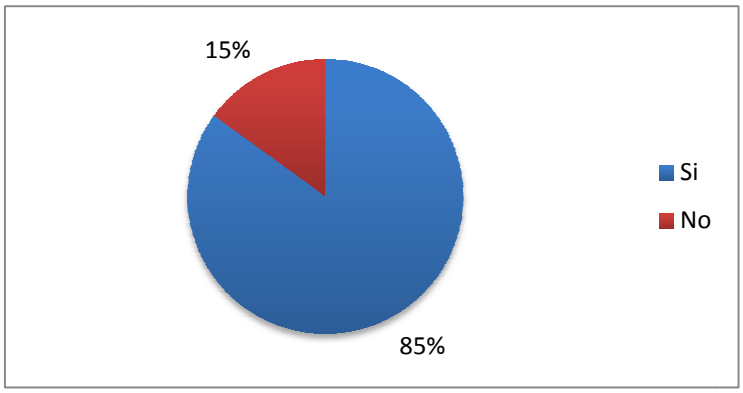

Fig. 2 61 Protege su antivirus los correos electrónicos y la descarga de archivos vía Web.

- **¿Actualiza regularmente el antivirus?**

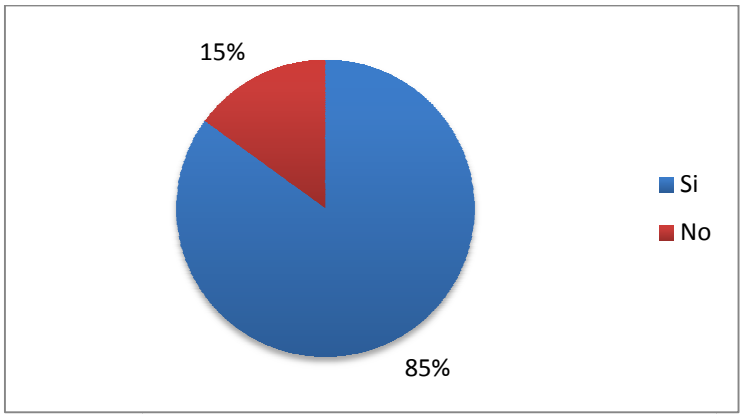

Fig. 2 62 Actualiza regularmente el antivirus.

- **¿Alguna vez ha experimentado inconvenientes con algún virus en su sistema?**

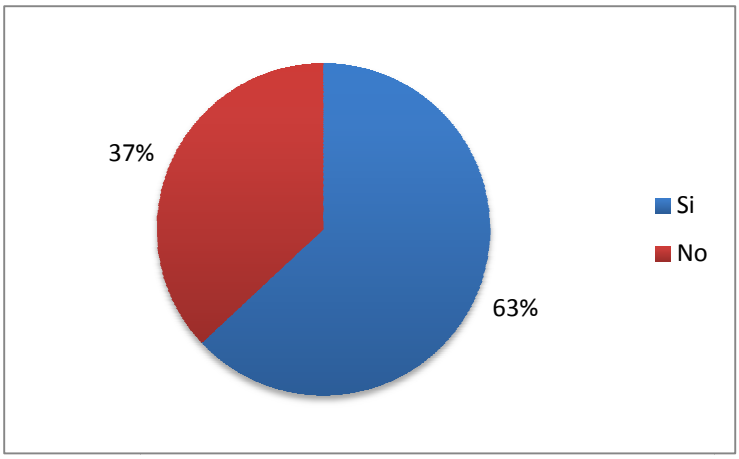

Fig. 2 63 Experimentó inconvenientes con algún virus en el Sistema.

- **¿Es el SPAM un problema para Ud. actualmente?**

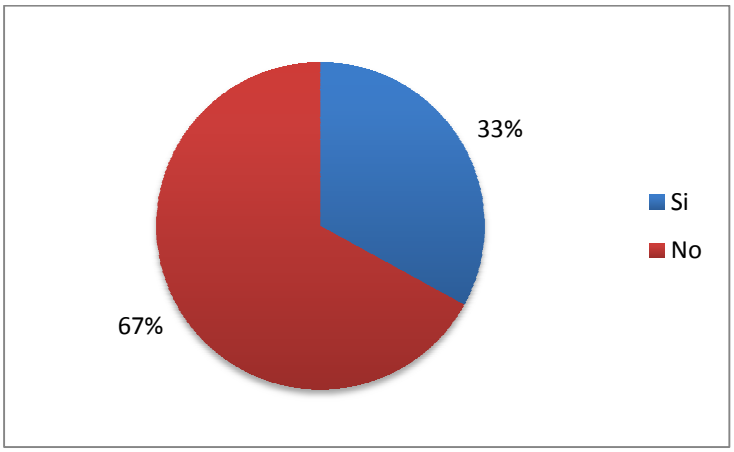

Fig. 2 64 El SPAM es un problema actualmente.

2.1.16. Planes de Seguridad y Contingencias

- **¿Se ha elaborado un plan de seguridad?**

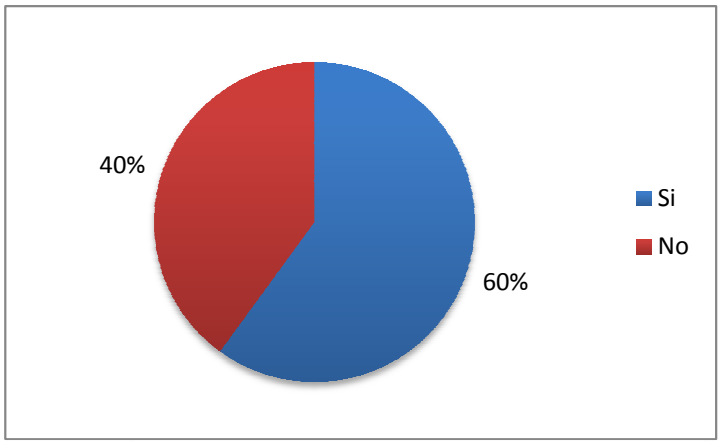

Fig. 2 65 Elaboración de un Plan de Seguridad.

- **¿Existe un responsable o responsables que coordinen las medidas de seguridad aplicables?**

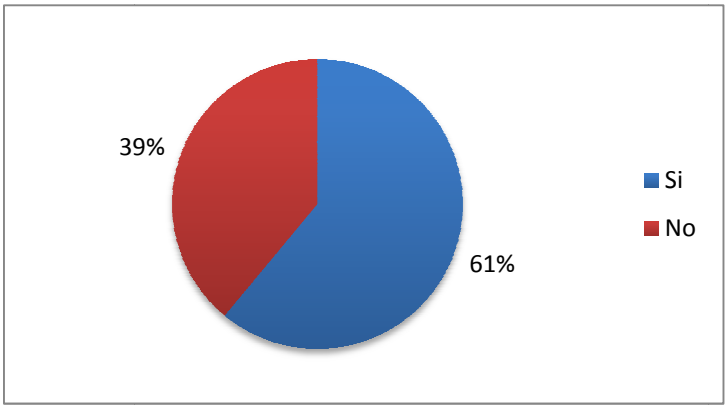

Fig. 2 66 Responsables que coordinen las medidas de seguridad aplicables.

- **¿Existe un plan de contingencias?**

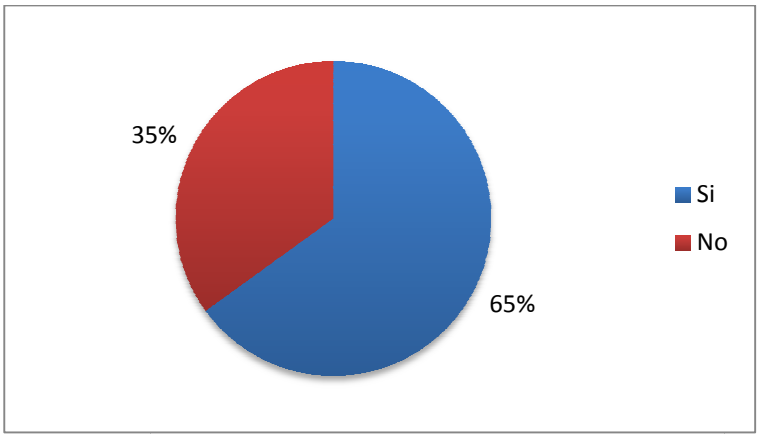

Fig. 2 67 Plan de Contingencias.

- **¿Existe un presupuesto asignado para la seguridad en la empresa?**

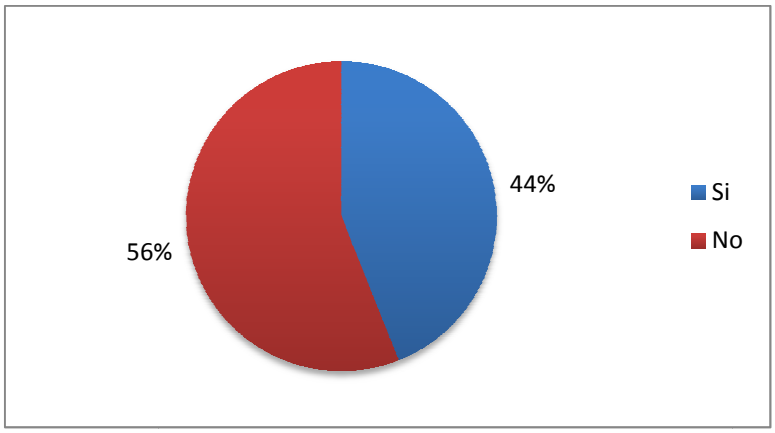

Fig. 2 68 Presupuesto asignado para la seguridad en la Empresa.

- **¿Se han incluido en el mismo los aspectos relacionados con las comunicaciones?**

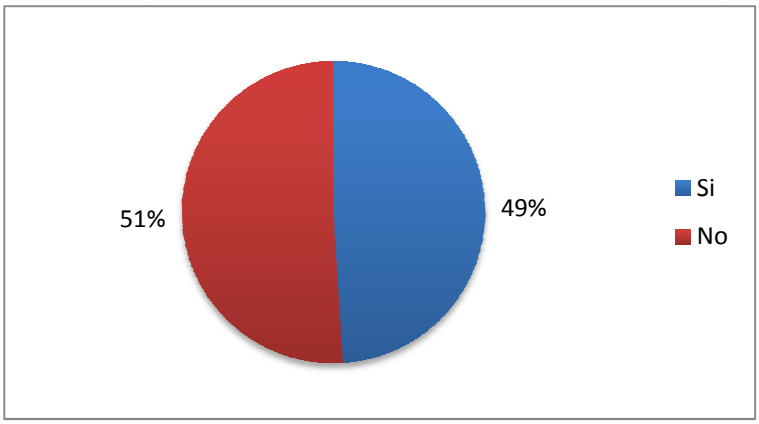

Fig. 2 69 Se han incluido los aspectos relacionados con las comunicaciones

---

- **¿Realiza el seguimiento del plan de seguridad personal de la empresa?**

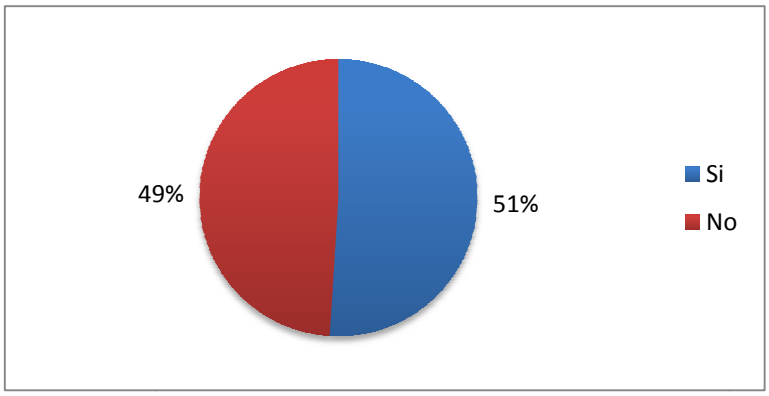

Fig. 2 70 Seguimiento del plan de seguridad personal de la empresa.

- **¿Existe un contrato de mantenimiento en el que se priorice la seguridad y el plan de contingencia?**

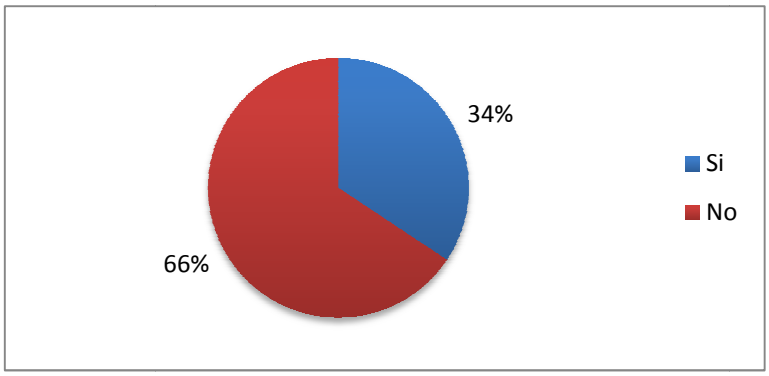

Fig. 2 71 Contrato de mantenimiento en el que se priorice la seguridad y el plan de contingencia.

- **¿Dispone de personal informático involucrado directamente con la seguridad del sistema?**

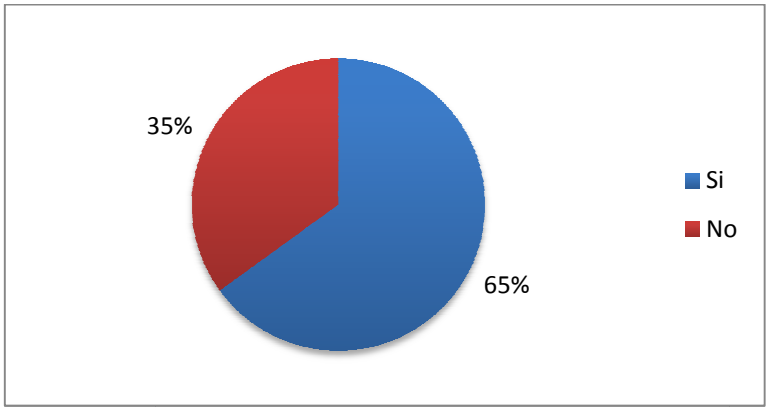

Fig. 2 72 Dispone de personal informático involucrado directamente con la seguridad del sistema.

2.1.17. Cifrado de las Comunicaciones

- **¿Existe un procedimiento de cifrado de las comunicaciones?**

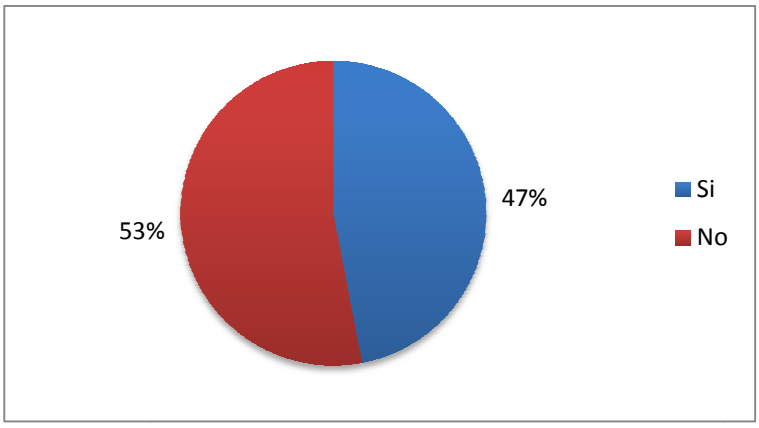

Fig. 2 73 Procedimiento de Cifrado de las Comunicaciones.

2.1.18. Correo Electrónico

- **¿Posee servidor de correo?**

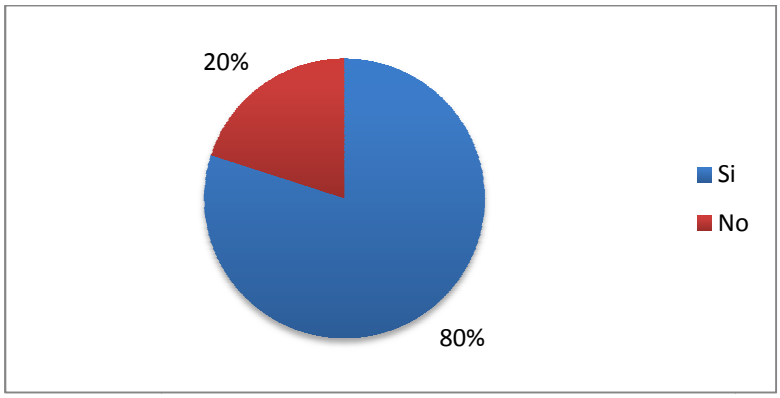

Fig. 2 74 Dispone de Servidor de Correo.

- **¿Tiene alguna solución para la protección de su correo electrónico?**

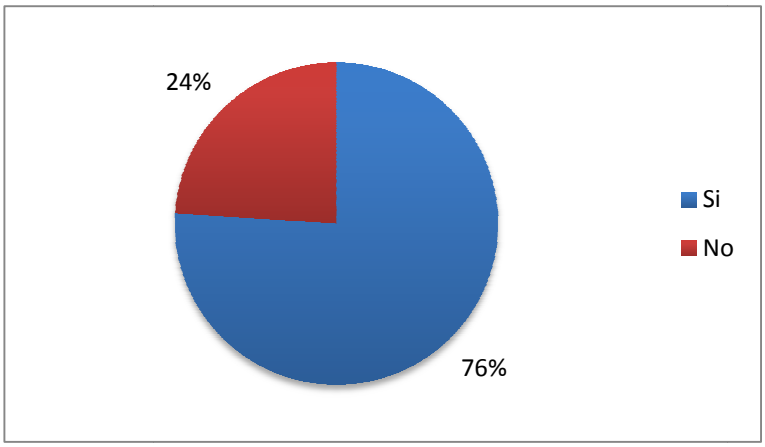

Fig. 2 75 Dispone de alguna solución para la protección de su correo electrónico.

- **¿Cuál?**

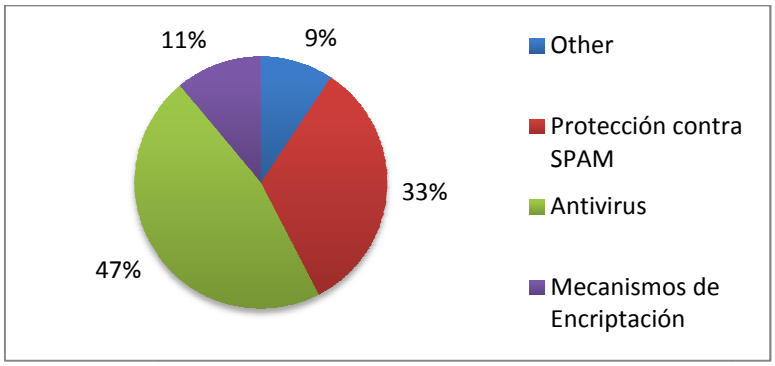

Fig. 2 76 Soluciones para la protección del Correo Electrónico.

- **¿Su servidor de correo ha estado en listas negras (RBL)?**

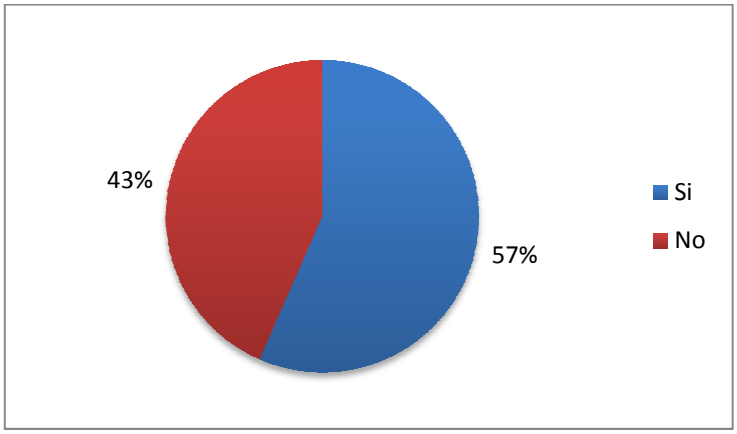

Fig. 2 77 Servidor de Correo que ha estado en listas negras (RBL).

- **¿Quién solucionó el inconveniente de RBL?**

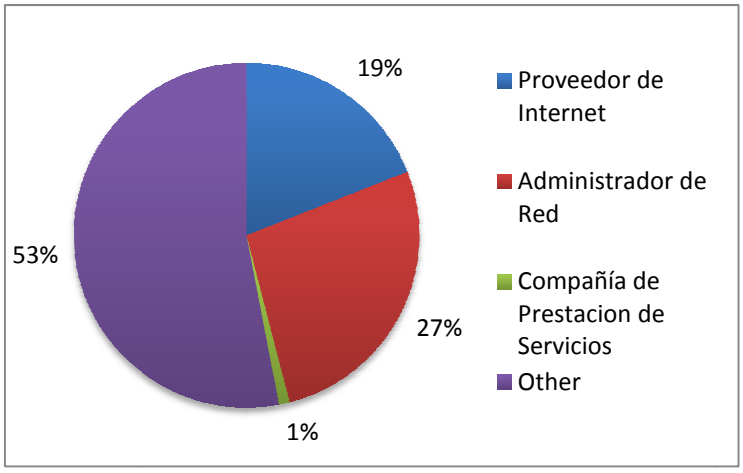

Fig. 2 78 Quienes han solucionado los inconvenientes RBL

- **¿Quien administra su servidor de correo?**

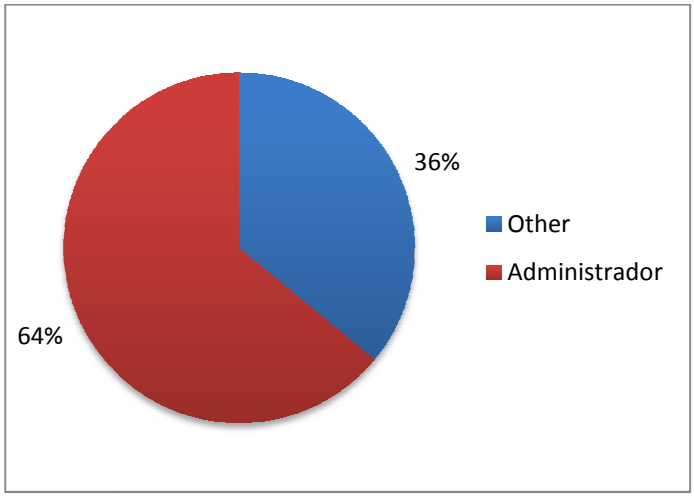

Fig. 2 79 Administradores del Servidor Correo.

- **¿Quien administra su servidor de dominio?**

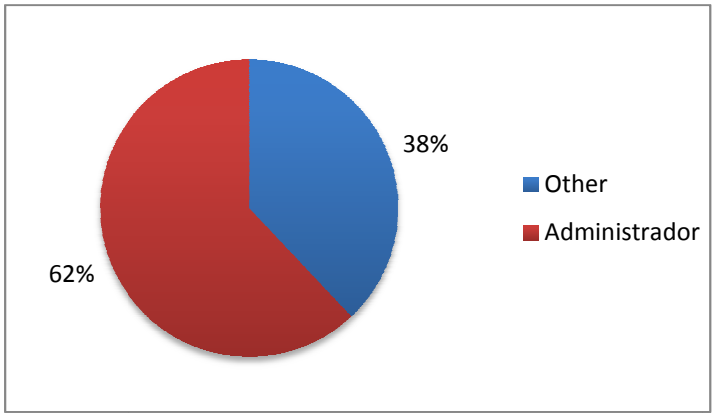

Fig. 2 80 Administradores del Servidor de Dominio.

- **¿Disponen de correo electrónico todos los usuarios?**

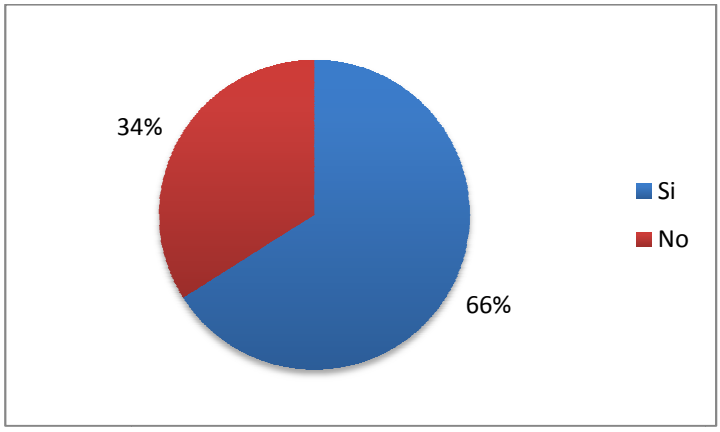

Fig. 2 81 Disponen de correo electrónico los Usuarios.

- **De aquellos que disponen, ¿Se les ha informado de la política de la empresa en cuanto a su uso?**

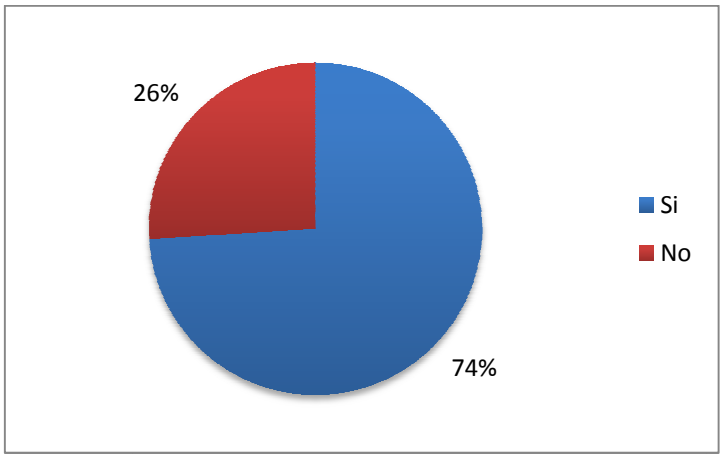

Fig. 2 82 Conocen la política de la empresa en cuanto al uso del correo electrónico.

- **¿Existe algún control sobre los mensajes que se envían y/o reciben?**

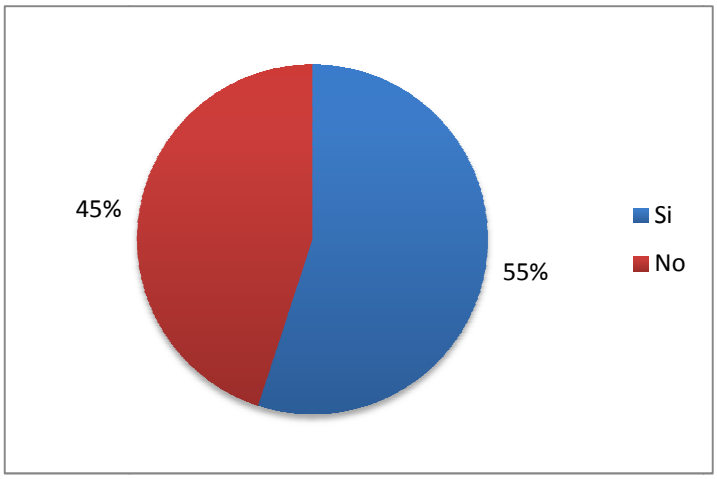

Fig. 2 83 Existe un Control sobre los mensajes que se envían y/o reciben.

2.1.19. Acceso a Internet

- **¿Existe una política definida para los accesos a Internet?**

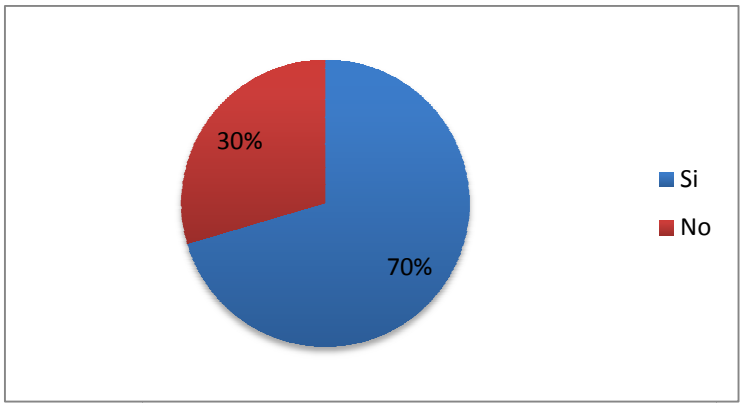

Fig. 2 84 Existe una Política definida para los accesos a Internet.

- **¿Se ha explicado claramente a los trabajadores de la empresa?**

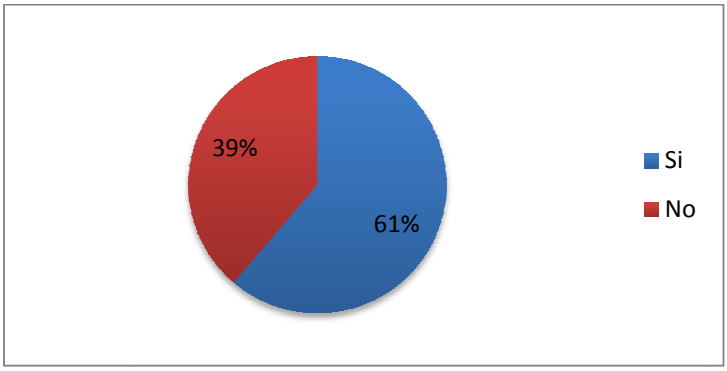

Fig. 2 85 Los trabajadores tienen conocimiento que existe una política definida para los accesos a Internet.

- **¿Existe un acceso a Internet Corporativo?**

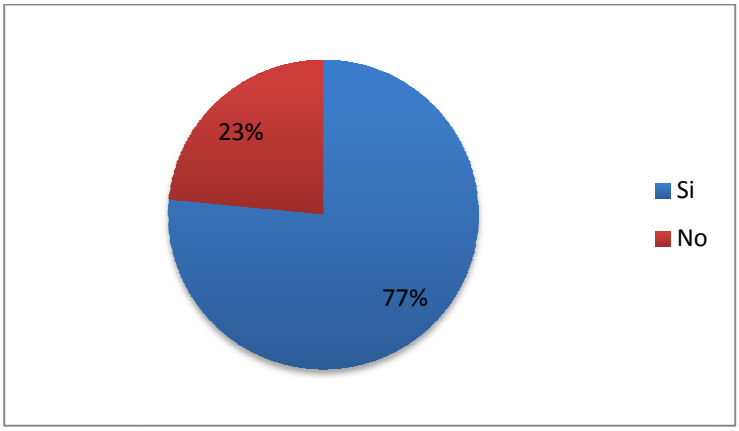

Fig. 2 86 Existe un acceso a Internet Corporativo.

- **¿Está limitado el acceso por cargo?**

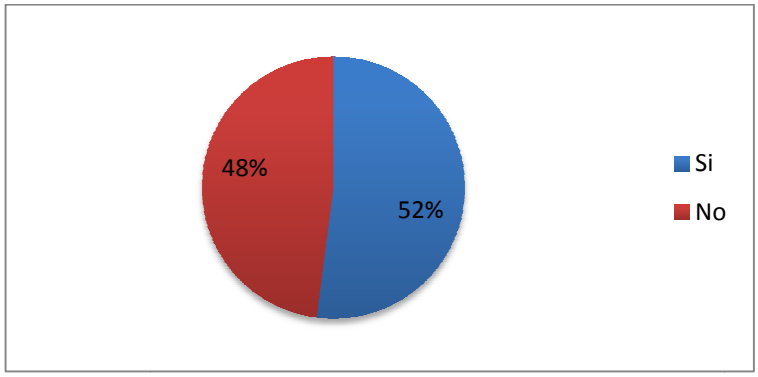

Fig. 2 87 El acceso está limitado por cargo.

- **¿Está limitado el acceso por usuario?**

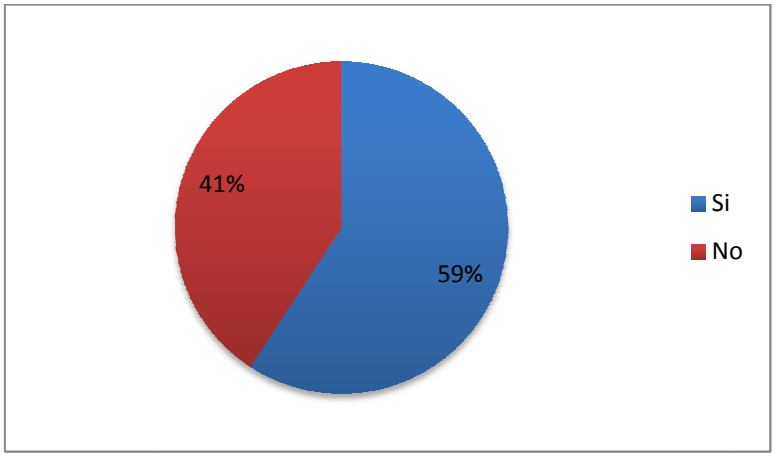

Fig. 2 88 El acceso está limitado por usuario.

- **¿Existen controles sobre las páginas accedidas por cada Puesto o Usuario?**

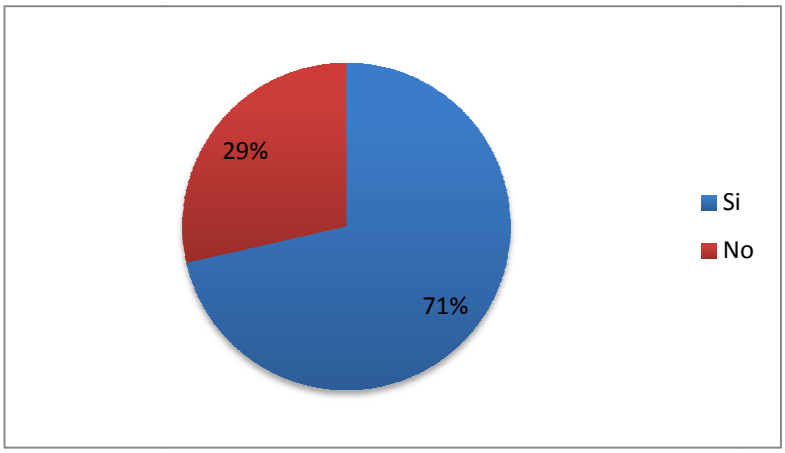

Fig. 2 89 Existen controles sobre las páginas accedidas por cada puesto o usuario.

2.1.20. Web Site

- **¿Dispone de Web Site empresarial?**

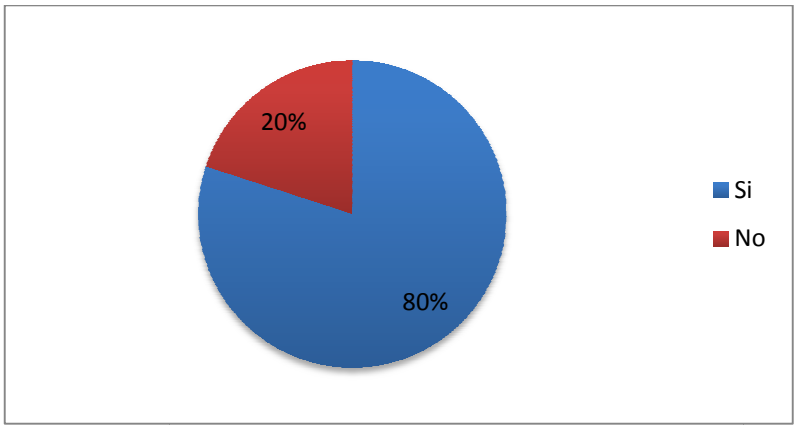

Fig. 2 90 Dispone de Web Empresarial.

- **¿Se ha contratado el hosting a una empresa externa?**

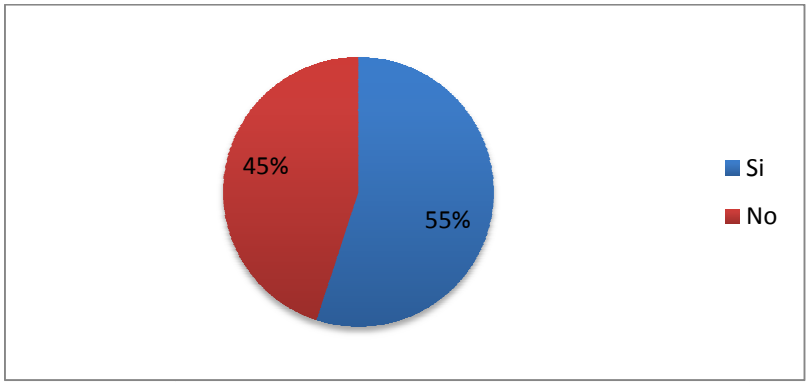

Fig. 2 91 Contratación de Hosting a una Empresa Externa.

- **¿Se realiza el mantenimiento por personal de la propia empresa?**

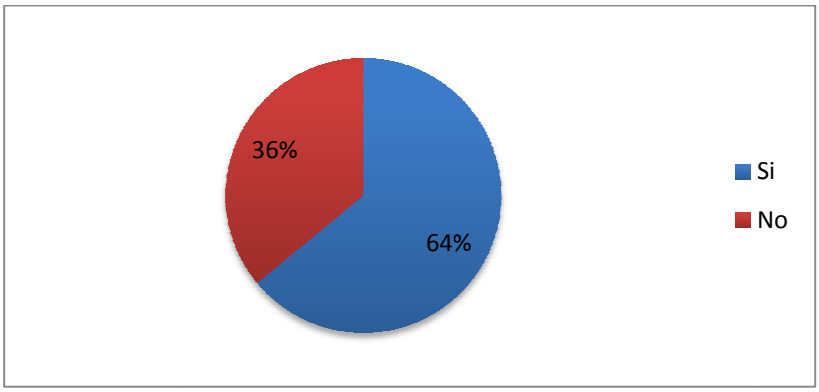

Fig. 2 92 Realiza el mantenimiento por personal de la propia empresa.

- **¿Está alojado en la red empresarial el Servidor de Web?**

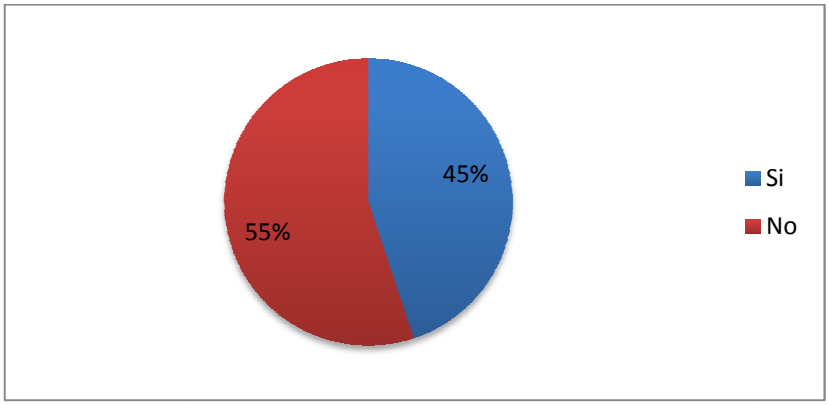

Fig. 2 93 Está alojado en la red empresarial el Servidor de Web.

- **¿Se ha contratado personal informático para que diseñe la protección?**

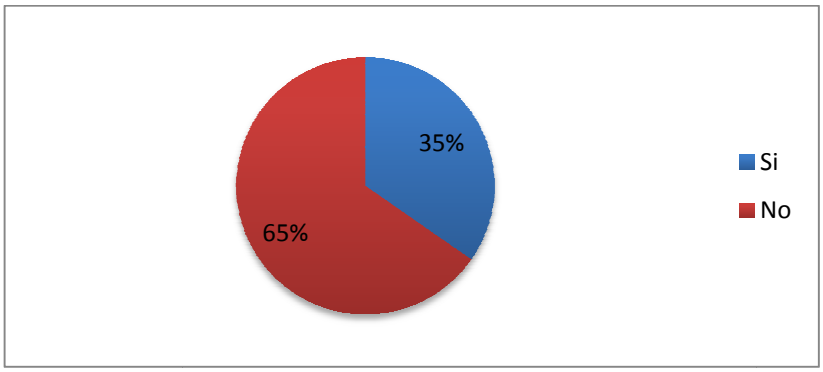

Fig. 2 94 Existe personal informático para que diseñe alguna protección.

- **¿Dispone de firewall?**

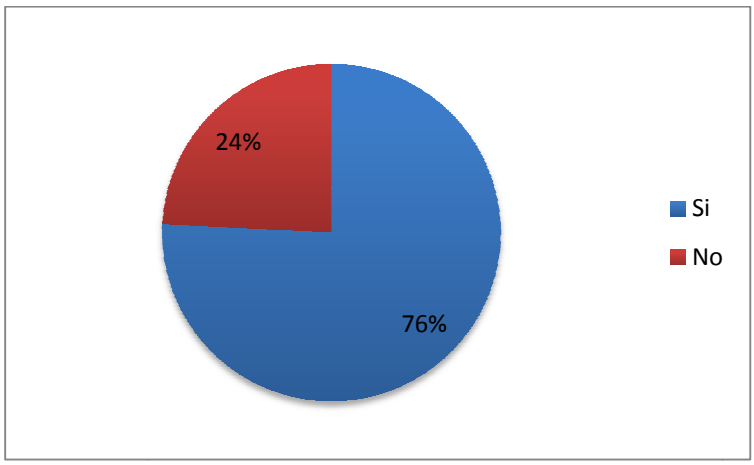

Fig. 2 95 Dispone de Firewall

- **¿Dispone de herramientas que auditen intentos de acceso externos?**

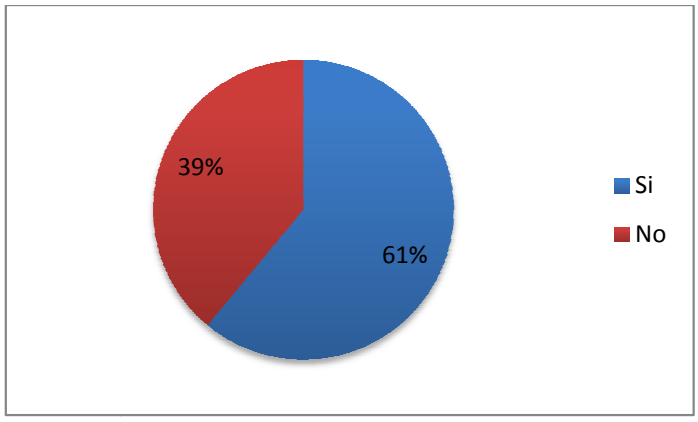

Fig. 2 96 Dispone de Herramientas que auditen intentos de accesos externos.

2.1.21. General

- **¿Alguno de los problemas presentados anteriormente ha ocasionado la interrupción de algún proceso de la empresa?**

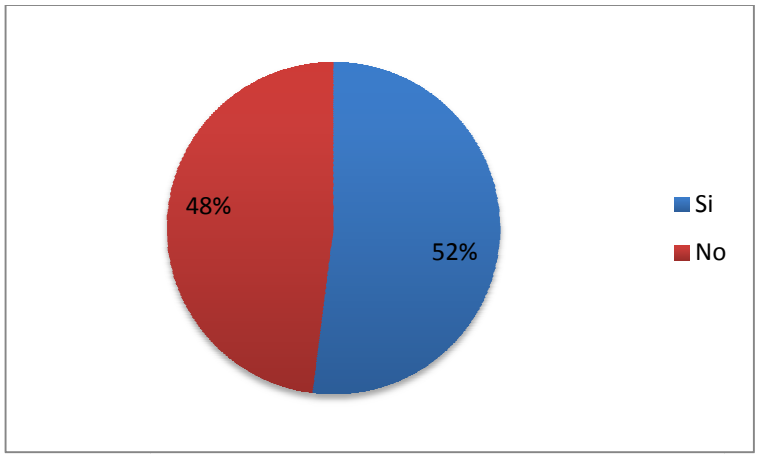

Fig. 2 97 Los problemas presentados anteriormente han ocasionado la interrupción de algún procesos de la empresa.

- **¿Durante cuánto tiempo?**

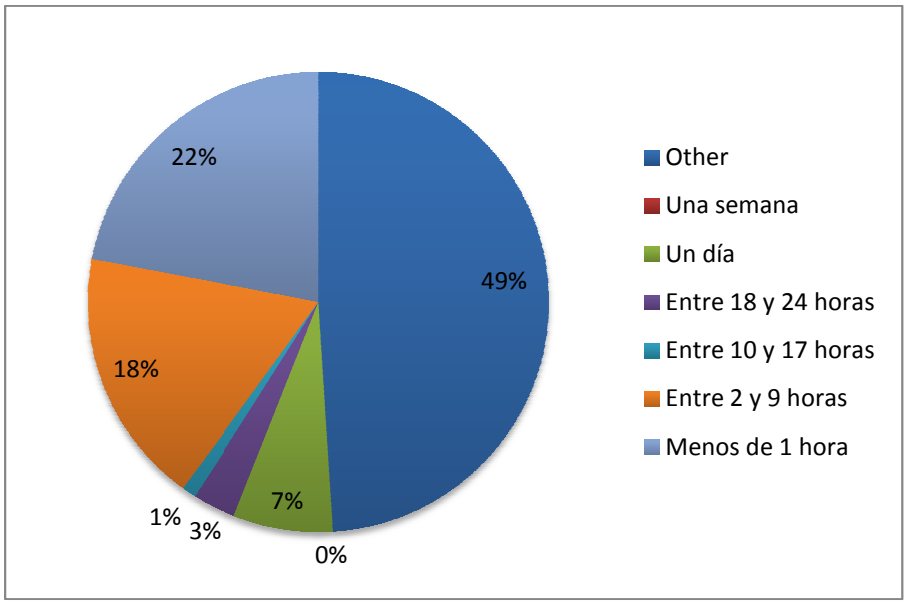

Fig. 2 98 Existe personal informático para que diseñe alguna protección.

- **¿Cree Ud. que en el Ecuador, el Área de Seguridad Informática se ha fortalecido en los últimos años?**

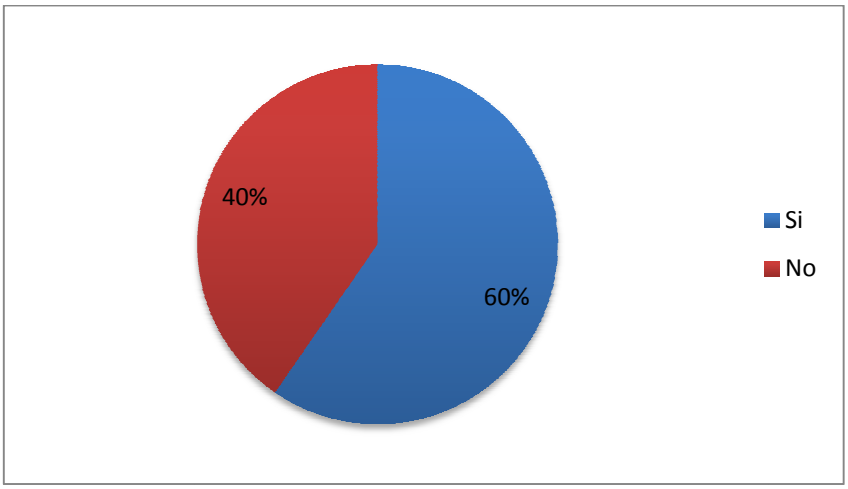

Fig. 2 99 Se considera que el Área de Seguridad Informática se ha fortalecido en los últimos años.

En la **Figura 2.99** podemos observar los resultados finales sobre la Seguridad Informática dentro del Ecuador. Evidentemente se considera que el área se ha fortalecido en los diversos sectores por la implementación de normas y políticas dentro de las organizaciones.

- **Opinión sobre la Seguridad Informática en el Ecuador.**

Muchas personas consideran que la seguridad, aún está lejos de tener buenas prácticas como cambios periódicos de claves e incluso que éstas sean complejas. Se enfatiza la capacitación en Normas Internacionales, implementación de auditorías y otras herramientas impartidas en las capacitaciones antes descritas. Definir roles de los usuarios e incluir en presupuesto de las empresas una asesoría anual al menos en este tema.

Un apoyo gerencial, la política de seguridad no le compete meramente al Departamento de Sistemas, es y debe ser siempre una política empresarial. Sin embargo, es difícil de comprender a nivel empresarial. En seguridad para empresas medianas y pequeñas el costo de esta seguridad es un factor decisivo. En la actualidad hay muchas soluciones a bajo o alto costos, pero las cifras siguen siendo altas para una buena solución.

Mientras la mayoría de gerentes de empresas de este país, no tengan claramente asociado que una empresa es vulnerable a ataques internos como externos, y que eso afectará las finanzas de sus empresa, no se dará la prioridad, ni relevancia y menos los recursos suficientes que se requieren para dar seguridad a la infraestructura TIC del negocio.

Home

2.1.22. Estado de los Encuestados

- **Género de los Encuestados**

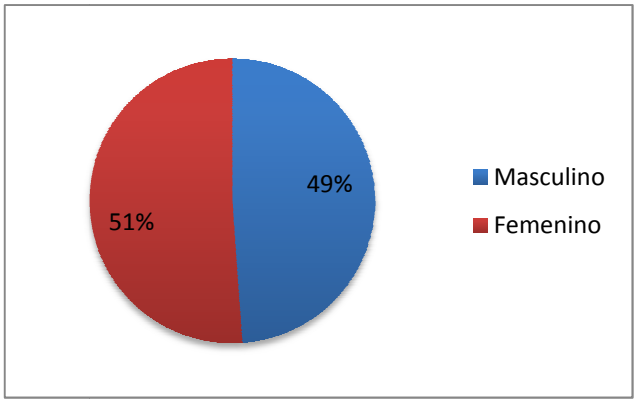

Fig. 2 100 Género de las personas encuestadas.

En la Figura 2.100 hemos obtenido un equilibrio entre el género de los encuestados ya que están repartidos con equitativamente con el 50% entre hombres y mujeres.

- **Edad de los Encuestados**

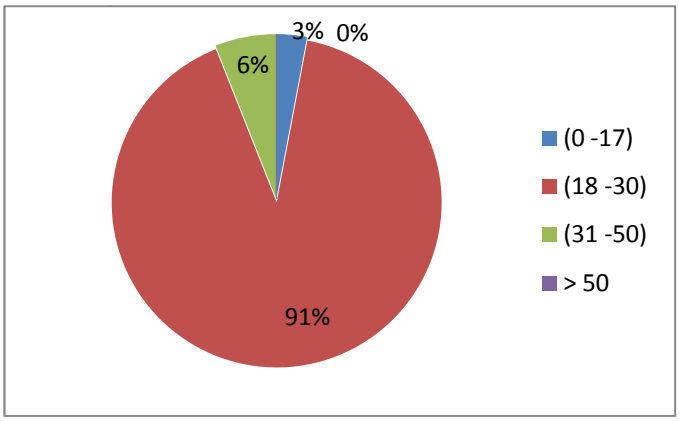

Fig. 2 101 Edad de las personas encuestadas.

- **Ocupación de los encuestados**

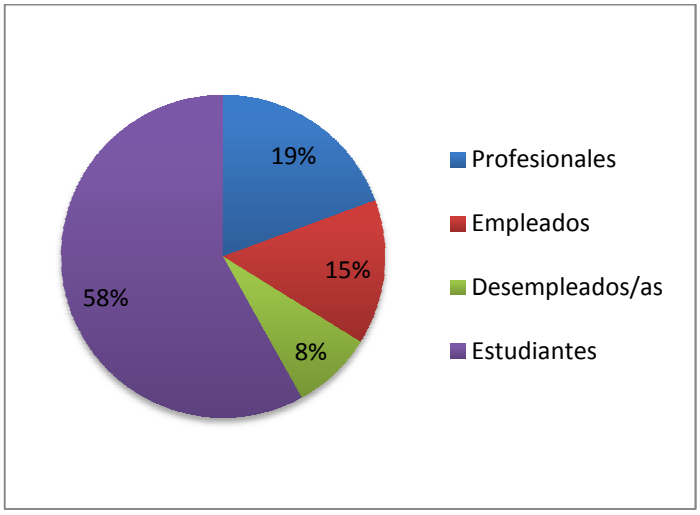

Fig. 2 102 Ocupación de los encuestados.

- **Nivel de estudio de los encuestados**

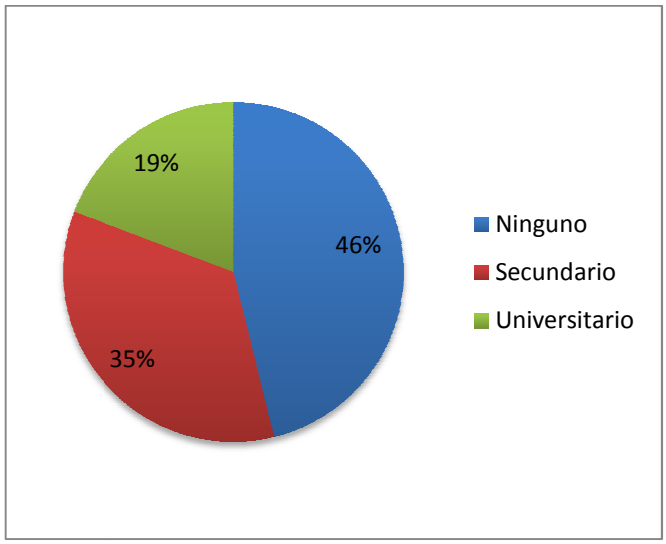

Fig. 2 103 Nivel de estudio de los encuestados.

- **¿Está preparado para realizar esta encuesta?**

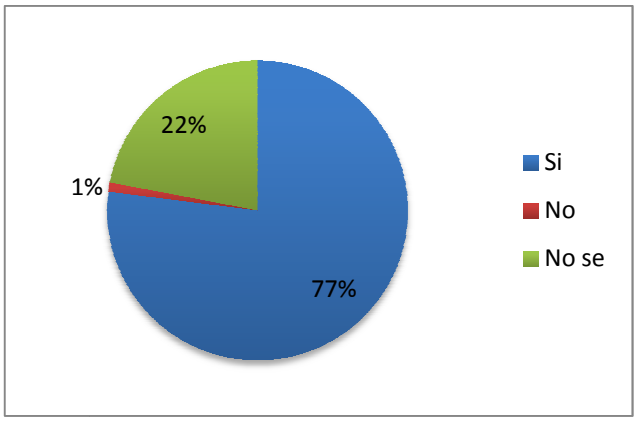

Fig. 2 104 Porcentaje de preparación para realizar la encuesta.

- **Interés por lo relacionado a la seguridad informática**

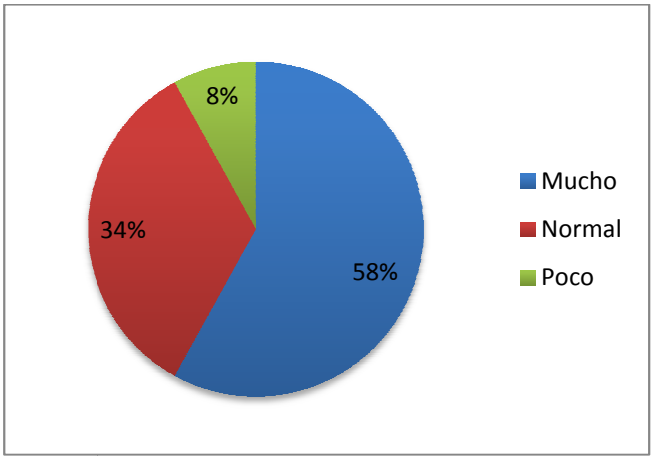

Fig. 2 105 Interés relacionado a la seguridad informática.

2.1.23. Conocimiento sobre Seguridad Informática de los Encuestados

- **¿Sabes cuánto impacto tiene la seguridad informática en el mercado laboral?**

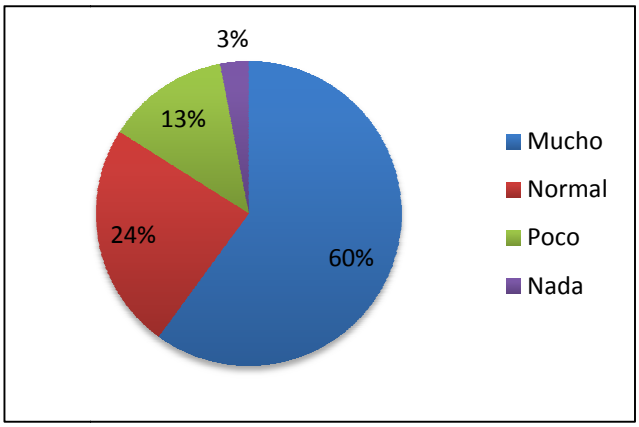

Fig. 2 106 Impacto de la seguridad informática en el mercado laboral.

- **¿Sabes qué la integridad, confidencialidad y autenticidad de datos es sólo una parte de la protección de datos?**

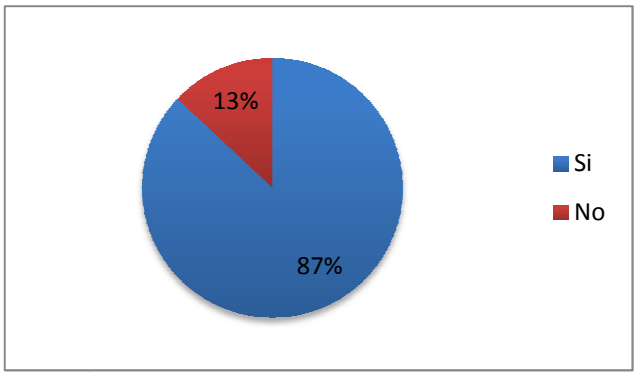

Fig. 2 107 Conocimiento de Integridad, Confidencialidad y Autenticidad como parte de protección de los datos.

- **Tus datos y tu información son privados**

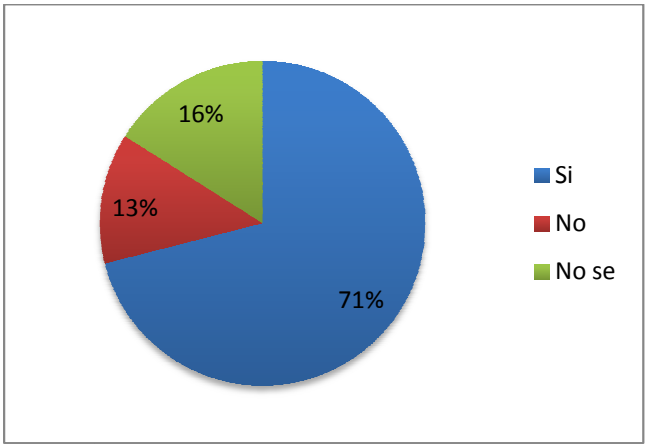

Fig. 2 108 Considera los datos e información como privados.

- **¿Existe la posibilidad de que el encargado de las computadoras de los Cybers puedan afectarnos sin que lo sepamos?**

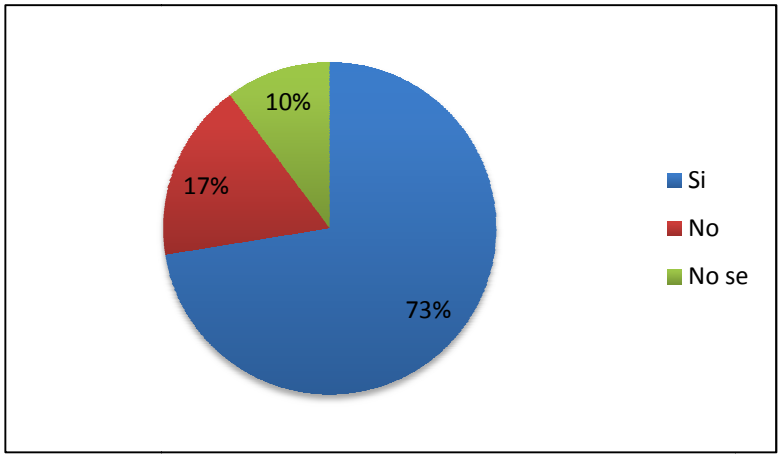

Fig. 2 109 El encargado de las computadoras de los Cybers pueda afectarle sin Ud. tener conocimiento.

- **Personas que realizan operaciones de dinero o se conectan a páginas con cuentas que tengan que disponer de contraseñas**

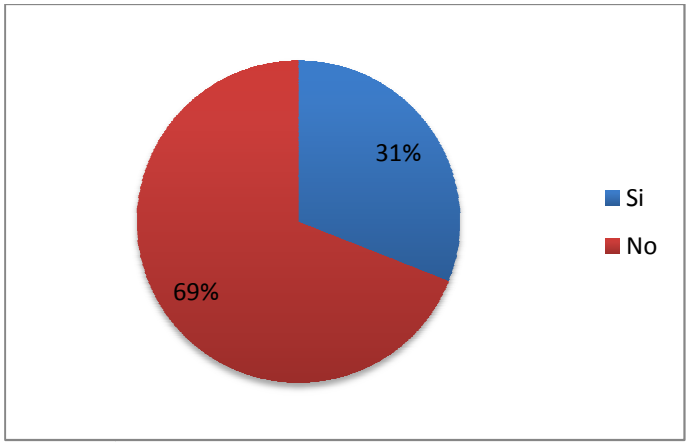

Fig. 2 110 Porcentaje de personas que realizan operaciones de dinero o se conectan a páginas que tengan que disponer de contraseñas.

- **Personas que saben que existe la posibilidad de que el encargado del cyber pueda recolectar las cuentas y contraseñas**

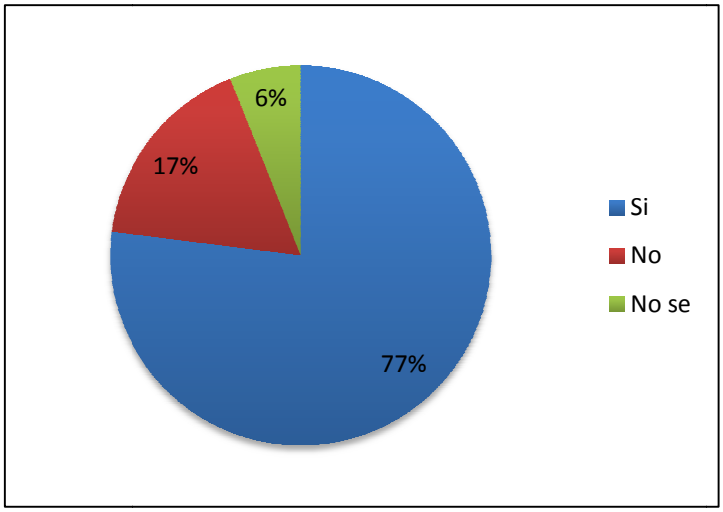

Fig. 2 111 Posee conocimiento que el encargado del Cyber pueda hacer uso de sus cuentas y contraseñas.

- **Método de espionaje que la gente cree que usa el encargado de un Cyber para recolectar datos o información privada se sus clientes**

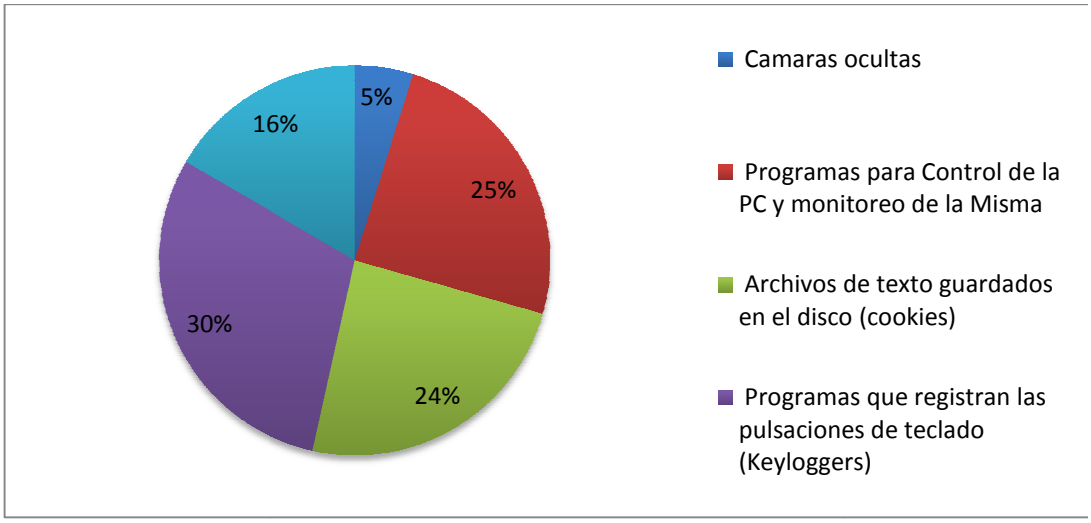

Fig. 2 112 Métodos de espionaje que Ud. considere que use el encargado de un Cyber para recolectar información privada de sus clientes.

- **¿Cuánto conocen las personas de las amenazas que rodea la inseguridad informática?**

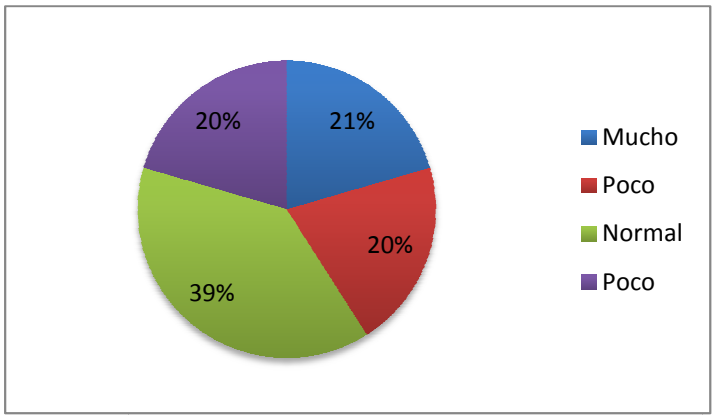

Fig. 2 113 Conocimiento de las amenazas de la inseguridad informática.

- **¿Cuántos saben que la principal amenaza somos los seres humanos?**

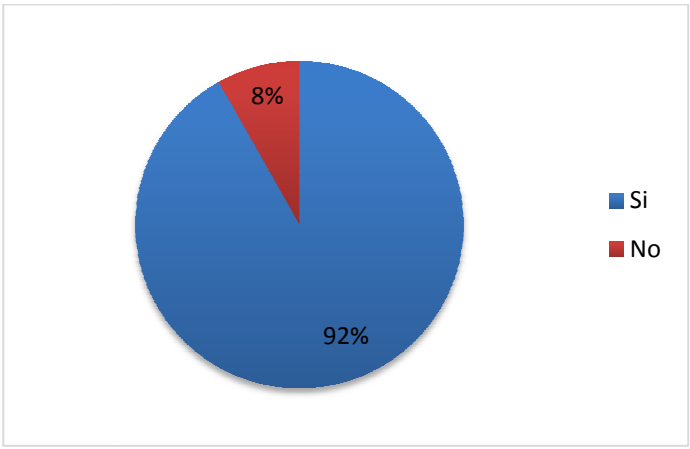

Fig. 2 114 Conocen que la principal amenaza somos los seres humanos.

2.1.24. Sistemas Operativos

- **¿Conoce Ud. lo que es un Sistema Operativo?**

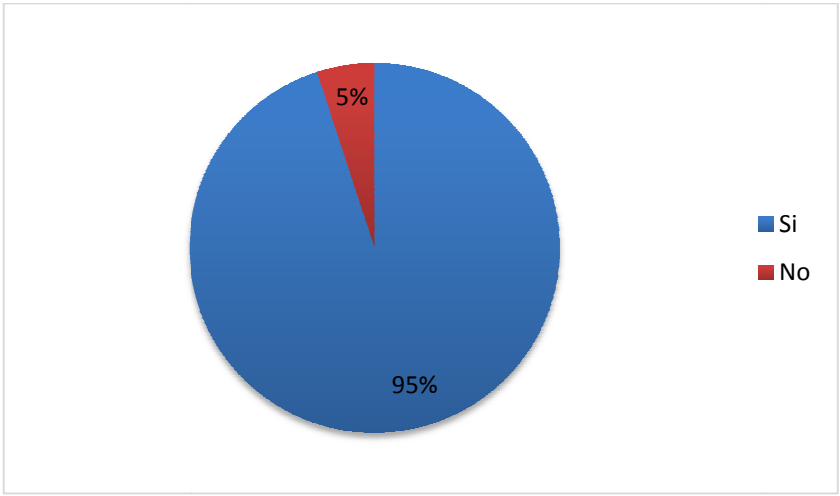

Fig. 2 115 Porcentaje de Personas que tienen conocimiento acerca de un sistema operativo.

- **Mencione Sistemas Operativos que utilice.**

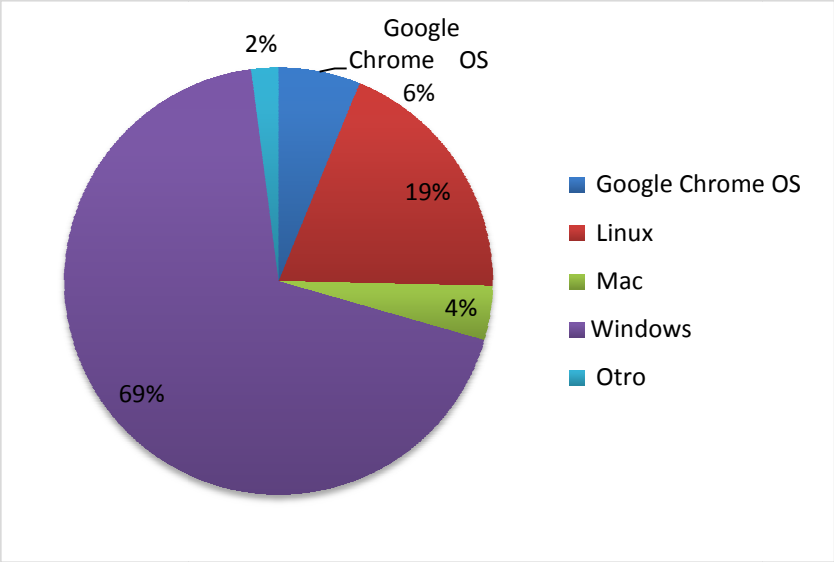

Fig. 2 116 Porcentaje de Uso de los diferentes Sistemas Operativos

---

- **¿Sabe Ud. que ésta inseguridad les puede causar graves daños?**

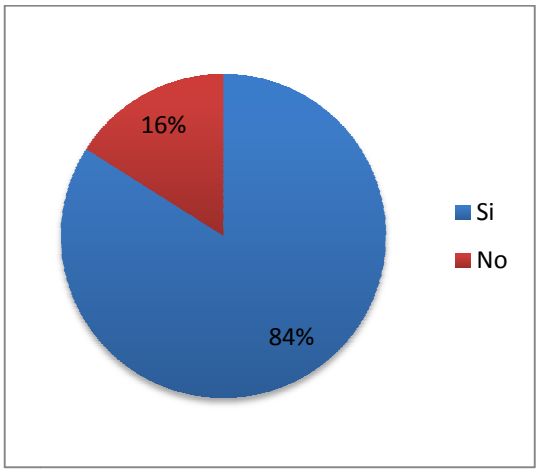

Fig. 2 117 Conocimiento sobre la inseguridad, la misma que puede causar graves daños.

- **¿Está Ud. consciente de que su Sistema Operativo no es 100% seguro?**

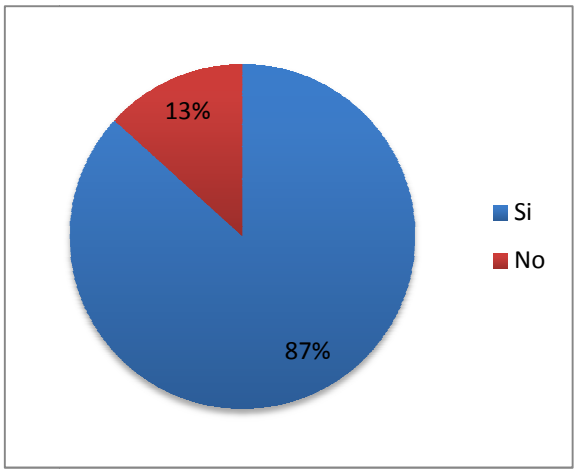

Fig. 2 118 Considera que su Sistema Operativo no fiable.

2.1.25. Amenazas

- **Conocen las personas los diferentes métodos de ser atacado por una amenaza**

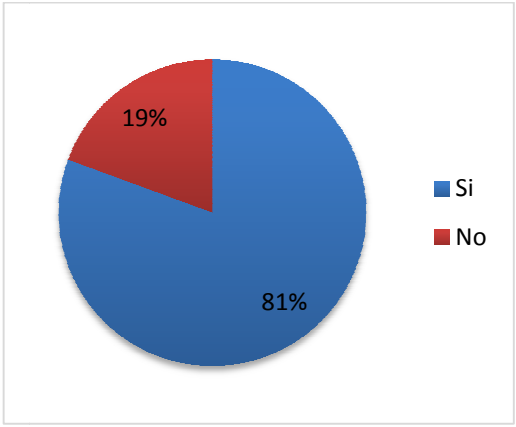

Fig. 2 119 Conocimiento sobre los diferentes métodos de amenazas.

- **Métodos que la gente conoce de ser atacado por una amenaza**

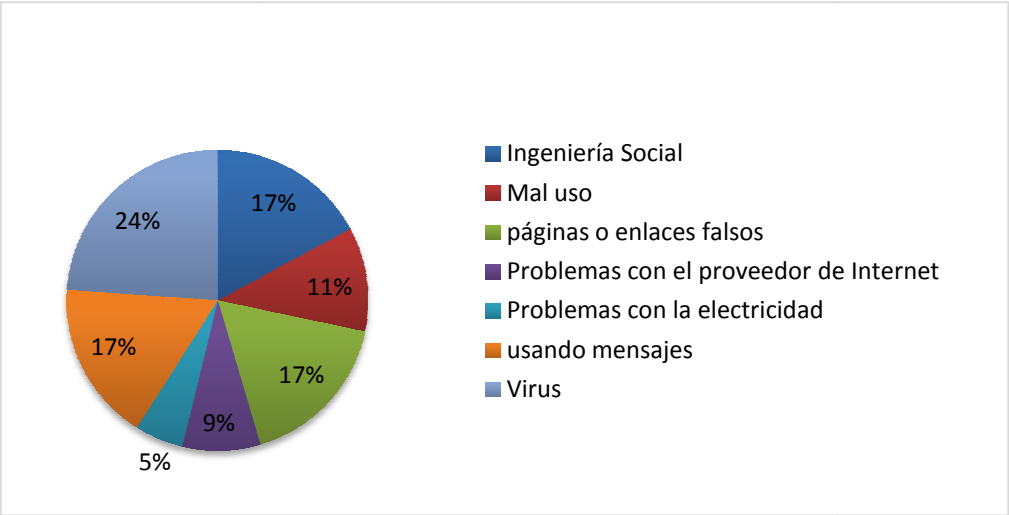

Fig. 2 120 Métodos

- **Saben las personas cómo actuar ante una posible amenaza**

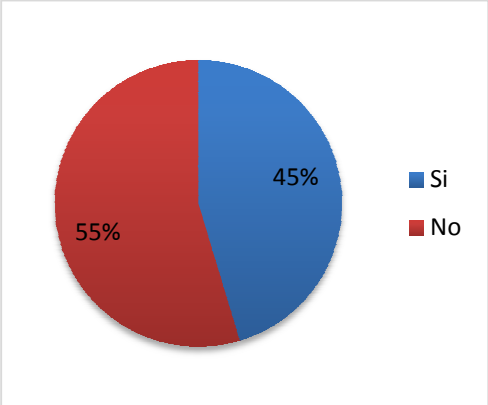

Fig. 2 121 Las personas saben actuar ante una amenaza.

- **Utilizan las personas alguna técnica para proteger tus datos**

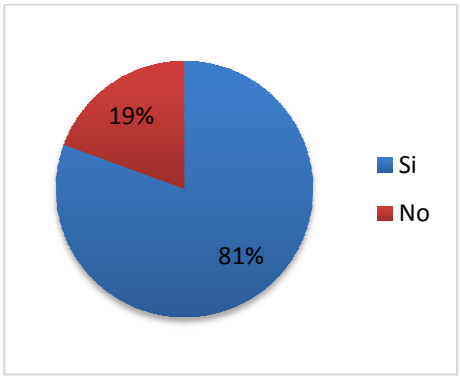

Fig. 2 122 Utilizan alguna técnica para proteger los datos.

- **Técnicas que la gente conoce para protegerse de una amenaza**

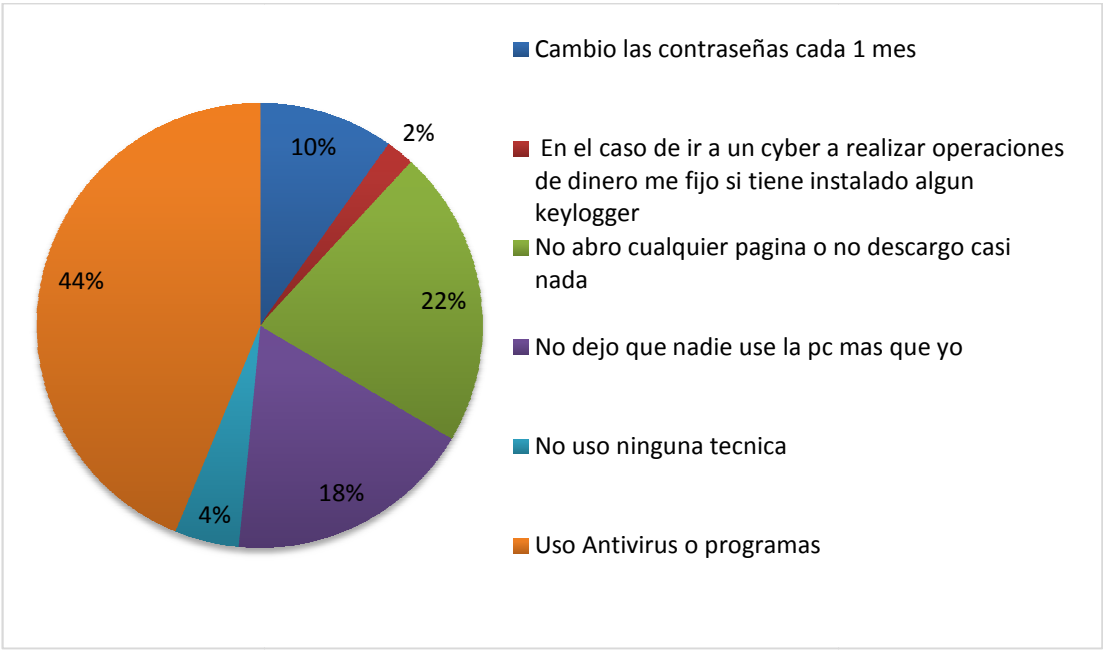

Fig. 2 123 Técnicas

2.1.26. Antivirus

- **¿Sabe Ud. qué es un antivirus?**

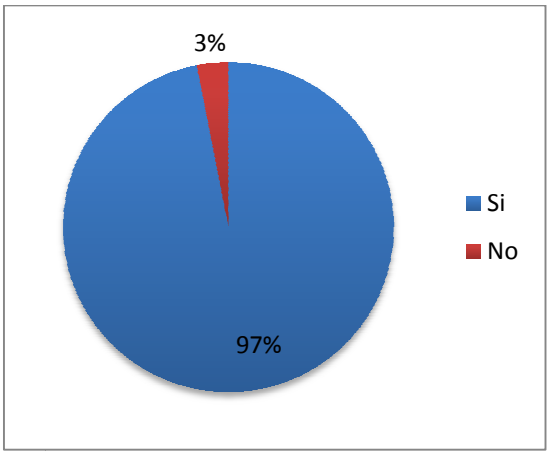

Fig. 2 124 Conocimiento sobre Antivirus.

- **¿Sabe Ud. para qué sirve un antivirus?**

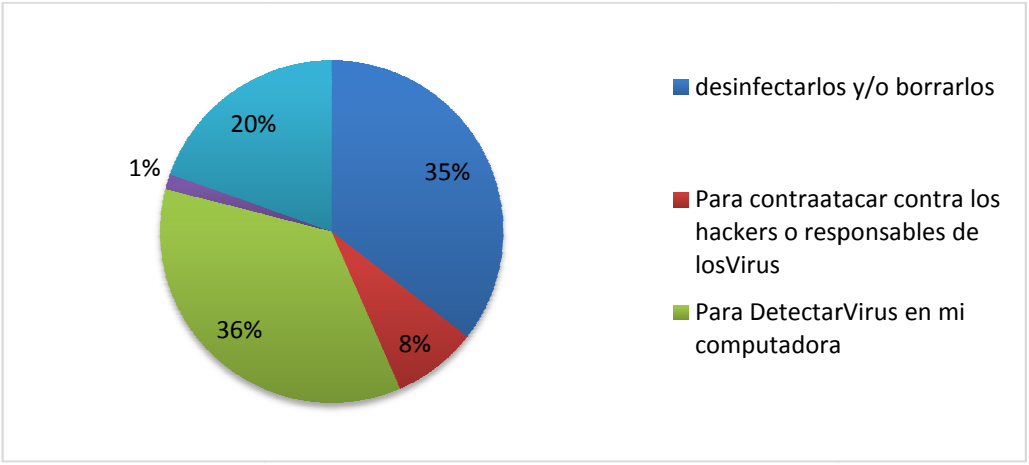

Fig. 2 125 Conocimiento para qué sirve un Antivirus.

- **¿Usa algún Anti-Virus?**

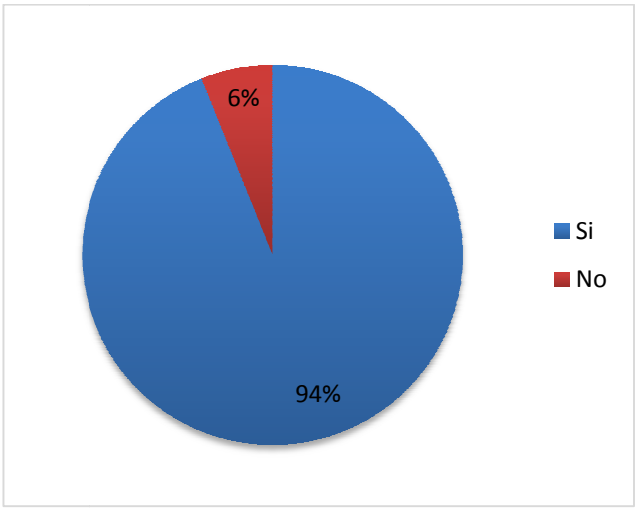

Fig. 2 126 Utiliza algún Antivirus.

- **Mencione los Antivirus que utiliza.**

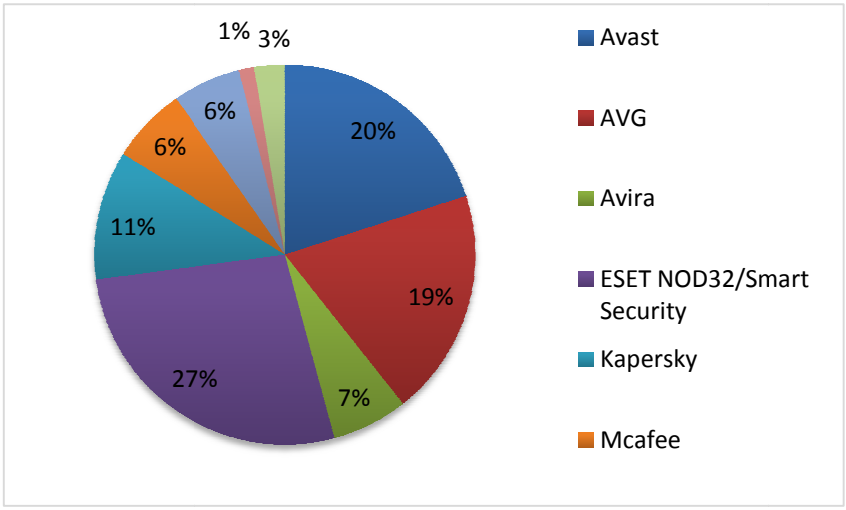

Fig. 2 127 Diferentes Antivirus que se utilizan.

- **¿Ud. Actualiza su Antivirus con frecuencia?**

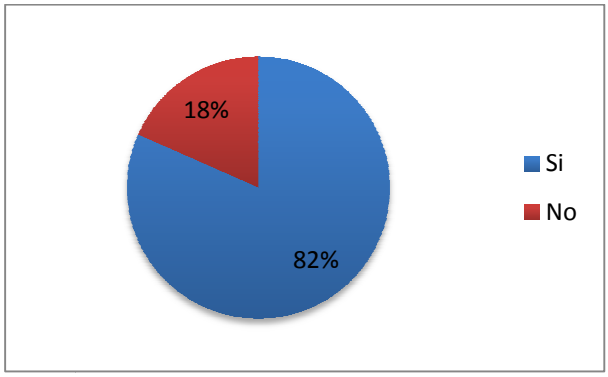

Fig. 2 128 Personas que contestaron que actualizan su Anti-Virus con frecuencia

---

- **¿Considera Ud. que las empresas que fabrican los antivirus son las mismas que fabrican algunos de esos Virus?**

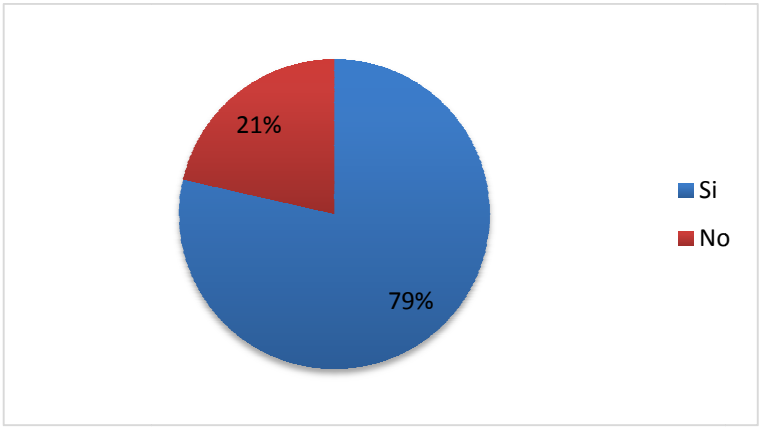

Fig. 2 129 Personas que creen que las empresas que fabrican los antivirus son las mismas que fabrican algunos de esos Virus.

2.1.27. Uso de la Internet

- **¿Usa la Internet adecuadamente?**

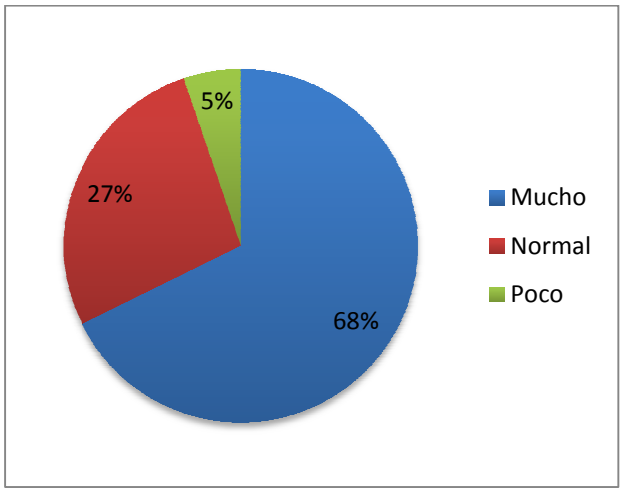

Fig. 2 130 Personas que indican que usan Internet adecuadamente.

- **Personas que indican que frecuentemente realizan descargas desde Internet.**

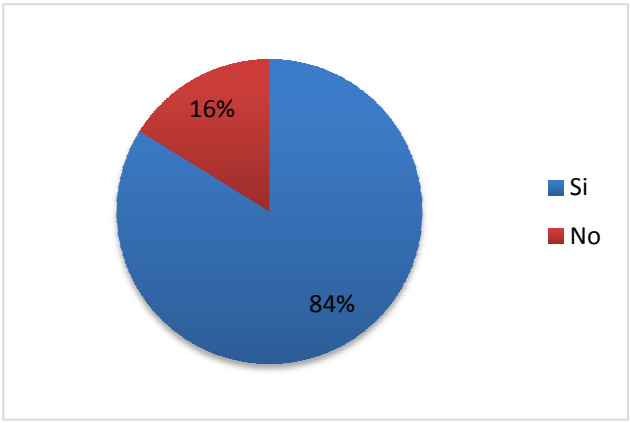

Fig. 2 131 Personas que indican que frecuentemente realizan descargas desde Internet.

- **Personas que indican saber donde se almacenan esos rastros y que tipos de archivos son**

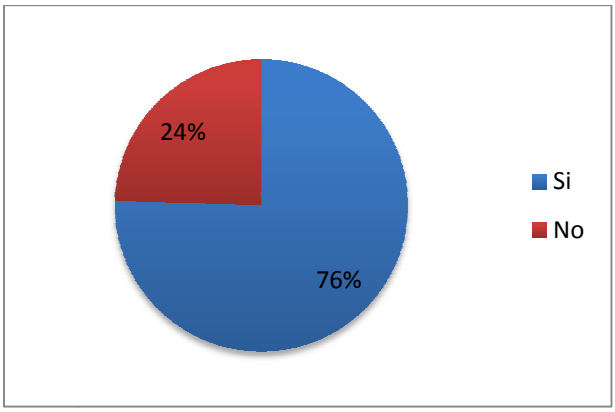

Fig. 2 132 Personas que indican saber donde se almacenan esos rastros y que tipos de archivos son.

- **¿Cuándo Ud. navega en la web, deja algún rastro?**

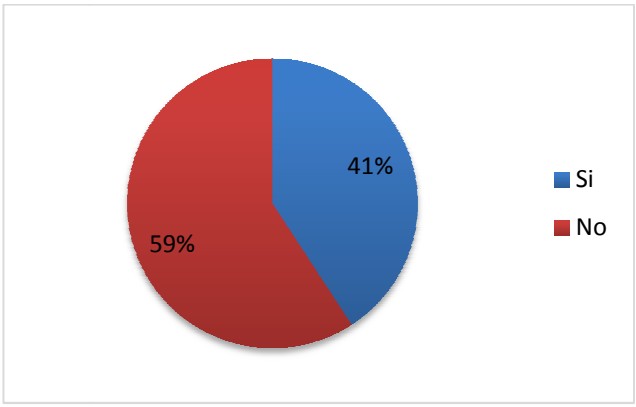

Fig. 2 133 Personas que indican saber que cuando navegas siempre dejas rastros.

- **Personas que indican que se actualizas con las noticias, cosas o programas que más impacten en la seguridad informática**

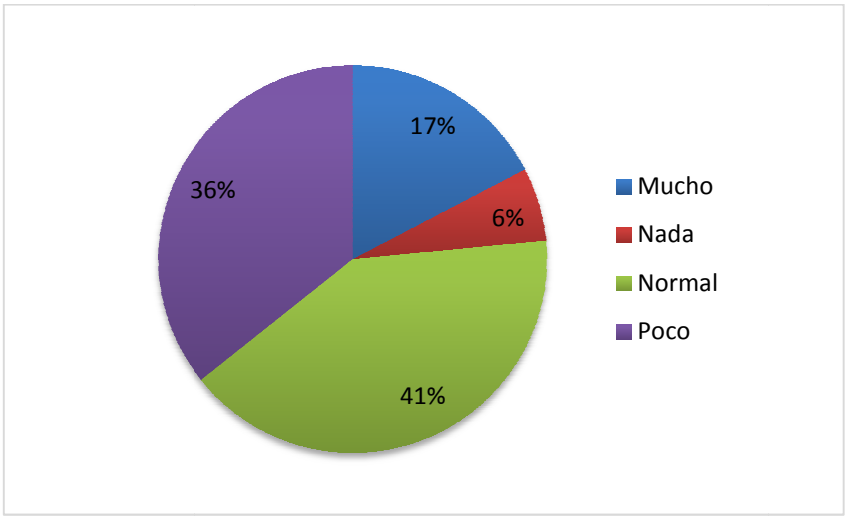

Fig. 2 134 Personas que indican que se actualizas con las noticias, cosas o programas que más impacten en la seguridad informática.

2.1.28. Uso de programas ilegales

- **¿Ud. sabe que los programas que utiliza diariamente son originales o ilegales?**

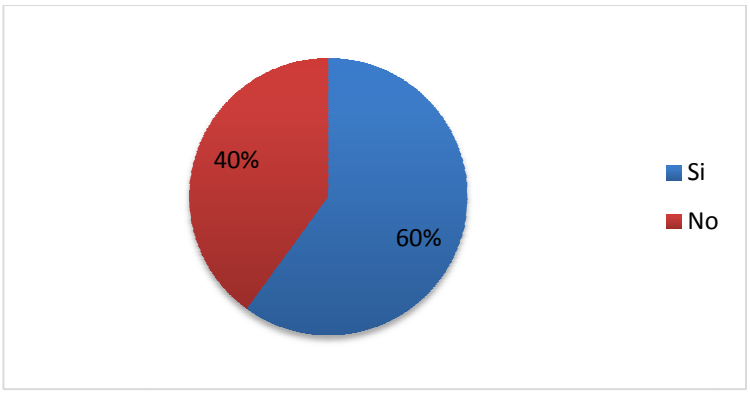

Fig. 2 135 Personas que indican saber si los programas que utilizas diariamente son originales o ilegales (piratas o truchos)

- **¿Qué tipo de programas ilegales utilizan?**

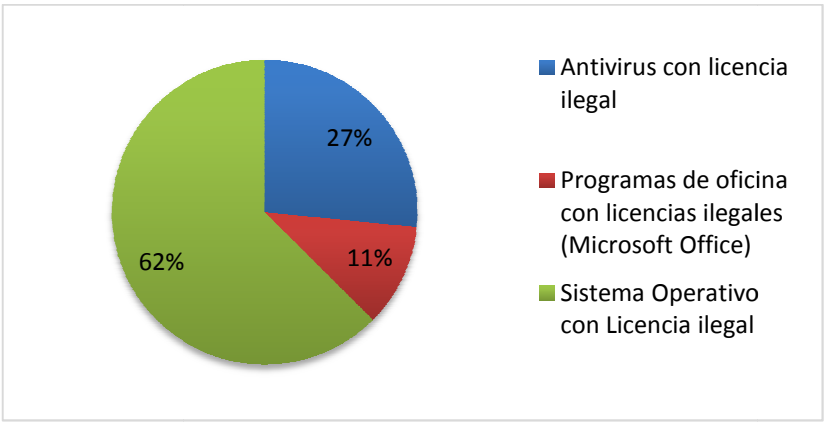

Fig. 2 136 Diferentes programas ilegales que utilizan.

- **¿Ud. considera que algunos de esos programas truchos pueden contener o atraer amenazas informáticas?**

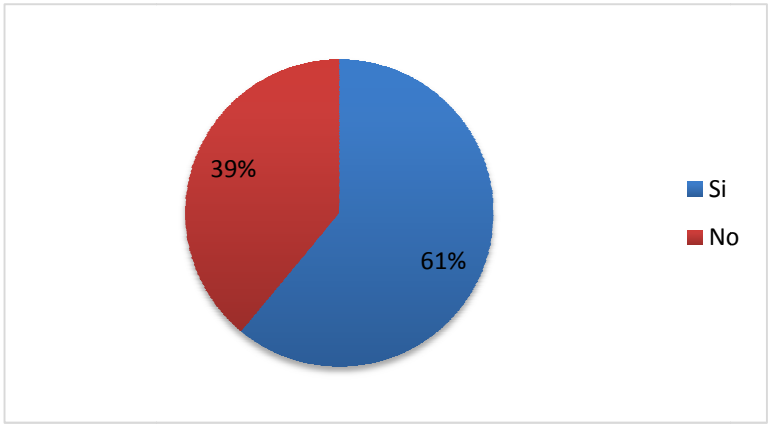

Fig. 2 137 Personas que indican saber que algunos de esos programas truchos pueden contener o atraer amenazas informáticas.

- **¿Te sientes más informado sobre la seguridad informática al haber realizado esta encuesta?**

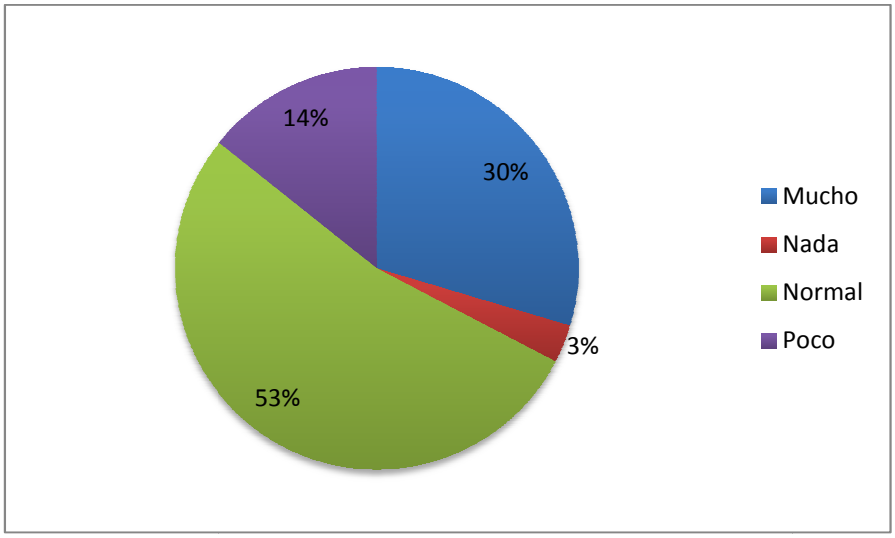

Fig. 2 138 Se siente más informado con la realización de dicha encuesta.

CAPÍTULO 3.

3. Tendencias de la Seguridad Informática y Productos

Para este capítulo veremos los detalles acerca de las nuevas tendencias y posibles productos que se puedan ofrecer dentro de las organizaciones.

Tendencias en Seguridad informática a nivel global.

En esta sección hacemos una recopilación de las tendencias en seguridad informática para este año, la misma es extraída de las principales empresas dedicadas al desarrollo y servicio de productos de seguridad informática a nivel mundial, cabe mencionar que el Ecuador no estará excluido de estas tendencias ya que somos participes de un mundo ya globalizado.

Entre las principales tendencias tenemos al Ciberterrorismo, ataques a dispositivos móviles y ciberprotestas, entre otras, las empresas que hemos

escogido para este análisis de tendencias son Eset, Fortinet, Imperva, Kaspersky Labs, M86 Security, Panda, Segu-Info News, Symantec, Trendmicro, Websense y Zscarler, las mismas fueron escogidas por estar con una posición muy aceptada en el mercado mundial.

Basados en los informes de estas empresas mencionaremos las tendencias que más se destacan en cada uno de ellos.

El Ciberespionaje y Ciberterrorismo.

La mayoría de los informes de estas empresas coinciden que a raíz del éxito del sabotaje con el famoso virus Stuxnet, los incidentes provocados por este tipo de malware y cuyo enfoque es al control de las infraestructuras criticas, tendera a aumentar en el 2011 de forma significativa.

Con la aparición del virus Stuxnet se ha abierto el camino a los ataques dirigidos, enfocados y especializados que podrían poner en alerta a un país mediante el ataque a infraestructuras que controlan elementos necesarios y básicos como el agua, la energía, e incluso centrales nucleares.

Con este tipo de ataques se debe de ampliar la defensa del terrorismo ya que cualquiera puede ser el enemigo, por lo que los gobiernos de todos los países tendrán que concentrar y coordinar esfuerzos para proteger sus activos críticos ya que cada vez hay más amenazas.

También serán objetivo de estos ataques, al igual que las infraestructuras críticas y las grandes empresas, las medianas empresas según el informe de Trendmicro.

Ciberprotestas

Las ciberprotestas es una tendencia en aumento, esto comenzó con la Operación Payback del grupo Anonymous, cuyos objetivos en primera instancia fue de atacar a empresas gubernamentales que estaban en contra de la piratería y que luchan contra ella.

Luego y con el escándalo de Wikileaks se realizaron operaciones parecidas basadas en ataques distribuidos de denegación de servicio DDoS, estos ataques son proporcionados por múltiples usuarios cuyas herramientas son provistas por los grupos que organizan el ataque.

Según Informe de Zscarler dos hemos tomado nota del poder de activismo político en la era de las redes sociales dónde no es necesario disponer de una organización para promover y coordinar rápidamente un ataque desde un relativo anonimato.

Ataques a dispositivos móviles.

Existe una gran aumento en los dispositivos móviles, vemos como el puesto de trabajo ha experimentado una clara tendencia hacia la movilidad, por lo que se hace casi inevitable proteger estos dispositivos igual como los de escritorio.

Los dispositivos móviles en la actualidad disponen de gran capacidad de almacenamiento y pueden contener una alta cantidad de datos sensibles, por lo que se prevé que podrán ser objetivo de campañas masivas de malware.

Otro problema que presentan con respecto a la confidencialidad de la información que contienen es que al poder ser perdidos o substraídos con facilidad pueden ocasionar importantes fugas de información de una organización.

Aunque casi todos los informes coinciden en esta tendencia, el informe de Panda indica no se espera para 2011 que el malware contra estos dispositivos despegue de forma significativa.

Vulnerabilidades del Día Cero en aumento

En el año 2010 se produjo un aumento en el numero de vulnerabilidades del Día-Cero que han sido descubiertas, y esto parece indicar que el 2011 este crecimiento aumentara, esto traerá como consecuencia que los sistemas con estas vulnerabilidades se puedan ver afectados mientras no se desarrolle el parche que soluciona el problema.

El informe de Kaspersky Labs señala la vigencia y crecimiento de este método de ataque cibernético.

Cloud Computing y Virtualización

La seguridad en la nube y la virtualización se menciona en la mayoría de los informes aunque con diferentes enfoques.

De forma resumida

Imperva indica que habrá una tendencia creciente de implementación de aplicaciones de seguridad en la nube

Según Symantec, con el aumento de infraestructuras cloud se prevé una tendencia al alza de soluciones para la protección de los servicios que se prestan en la nube.

M86 Security, entre otros, se dará una tendencia de aumento en la utilización de entornos *cloud* para el alojamiento de organizaciones criminales en lo que se podría denominar como *Malware As A Service*

Ataques malware más sofisticados

Se estima que durante el 2011 el malware evolucionara no tanto en la forma de propagación, que seguirá siendo mayoritariamente vía email y web, sino en las capacidades, el malware contara con capacidades remotas de actualización para evadir los controles de las soluciones de seguridad.

Las formas de propagación de las Botnets también evolucionarán siendo la tendencia a incrustar el código malicioso en archivos multimedia interactivos. Como predice Websense se difundirán rápidamente a través de las redes sociales.

Ingeniería social, ataques enfocados en redes sociales

Se estima que las redes sociales serán un nuevo foco de transmisión masiva de malware dado que la navegación de los usuarios por ellas suele ser más relajada. Mediante las técnicas de *Blackhat SEO*, de posicionamiento web ilícito, se intentará derivar al usuario a páginas fraudulentas o infectadas por malware. Según el informe de Eset, la red social *Facebook* se verá especialmente afectada.

Control de la información sensible

Como ya se ha hablado durante mucho tiempo las principales fugas de información se gestan desde dentro de la empresa por los propios

empleados, ya sea de forma intencionada o no. La tendencia que se espera ante este problema en 2011 es que las empresas comenzarán a cuidar esa información sensible con mayor mimo y tratarán de instaurar controles tanto físicos como lógicos para evitar este tipo de fugas que tanto perjudica a una empresa. Esto es según Segu-info News la asignatura pendiente de las empresas.

Aumento de esfuerzos globales contra el cibercrimen

Dada la deslocalización del negocio del malware, los gobiernos tendrán que unir esfuerzos y posturas para durante el año 2011 poder dar duros golpes a las organizaciones delictivas que controlan el negocio. Así lo resaltan los informes de Fortinet e Imperva.

Esto se supone básico para poder cercar a las organizaciones criminales que operan en todo el mundo de forma remota, ya que las infraestructuras que poseen suelen estar replicadas en diferentes lugares, por lo tanto la coordinación será esencial si se quiere mejorar la efectividad de las actuaciones contra el cibercrimen.

Consolidación de las organizaciones criminales

Para el 2011 también se prevé que las organizaciones criminales comenzarán a fusionarse o unirse ya sea de forma temporal o permanente. La explicación se basa que la persecución a la que están sometidas provoca que tengan que realizar inversiones importantes para mejorar sus

técnicas evasivas, y no todas estas organizaciones delictivas tienen la capacidad económica para realizar dicha inversión por lo que se prevé que las grandes tenderán a absorber otras de menor tamaño y de esa forma aumentar su negocio.

Seguridad informática en la Nube

Problema de Malware

En la actualidad el malware o virus debido a su evolución a través de los anos sigue siendo uno de los principales objetivos a ser contrarrestada por los desarrolladores de productos de seguridad informática, conocemos que el malware tiene como objetivo introducirse en el sistema para dañarlo o capturar información sin el conocimiento o consentimiento nuestro.

En los últimos 20 años han cambiado las técnicas y tecnologías de la información tanto a nivel de PC como de sistemas, el er trasladaba hasta su oficina o empresa el cual era un entorno controlado, hasta el 2004 los ataques de malware proporcionados por los hacker tenían un objetivo que se hablara de ellos, mejorar o subir su reputación dependiendo de la efectividad del ataque, hoy recordamos que a nivel mundial se hablaba en un noticiero de un hacker cuando lograba romper toda barrera de seguridad y penetrar en un entorno protegido.

Con el crecimiento del internet a partir del 2004 las empresas vieron la necesidad de salir de estos entornos protegidos y expandir sus servicios y productos a través de la nube generando la movilidad de sus usuarios, esto es visto por los creadores de malware como un entorno de oportunidades para realizar sus acciones delictivas y obtener grandes beneficios económicos, ya el objetivo no es la reputación si no el beneficio económico, ahora se trata de pasar lo mas desapercibido posible.

Fig. 3 139 Cambios en los últimos veinte años.

Las oportunidades de negocio que ofrece Internet son cada vez mayores para personas y empresas, pero hay quienes encuentran en Internet una plataforma ideal para llevar a cabo sus acciones maliciosas y obtener grandes beneficios económicos.

Estadísticamente está demostrado que en la actualidad hay muchos más malware o virus que hace algunos anos, este cada vez son más profesionalizado, menos visible y más inesperado.

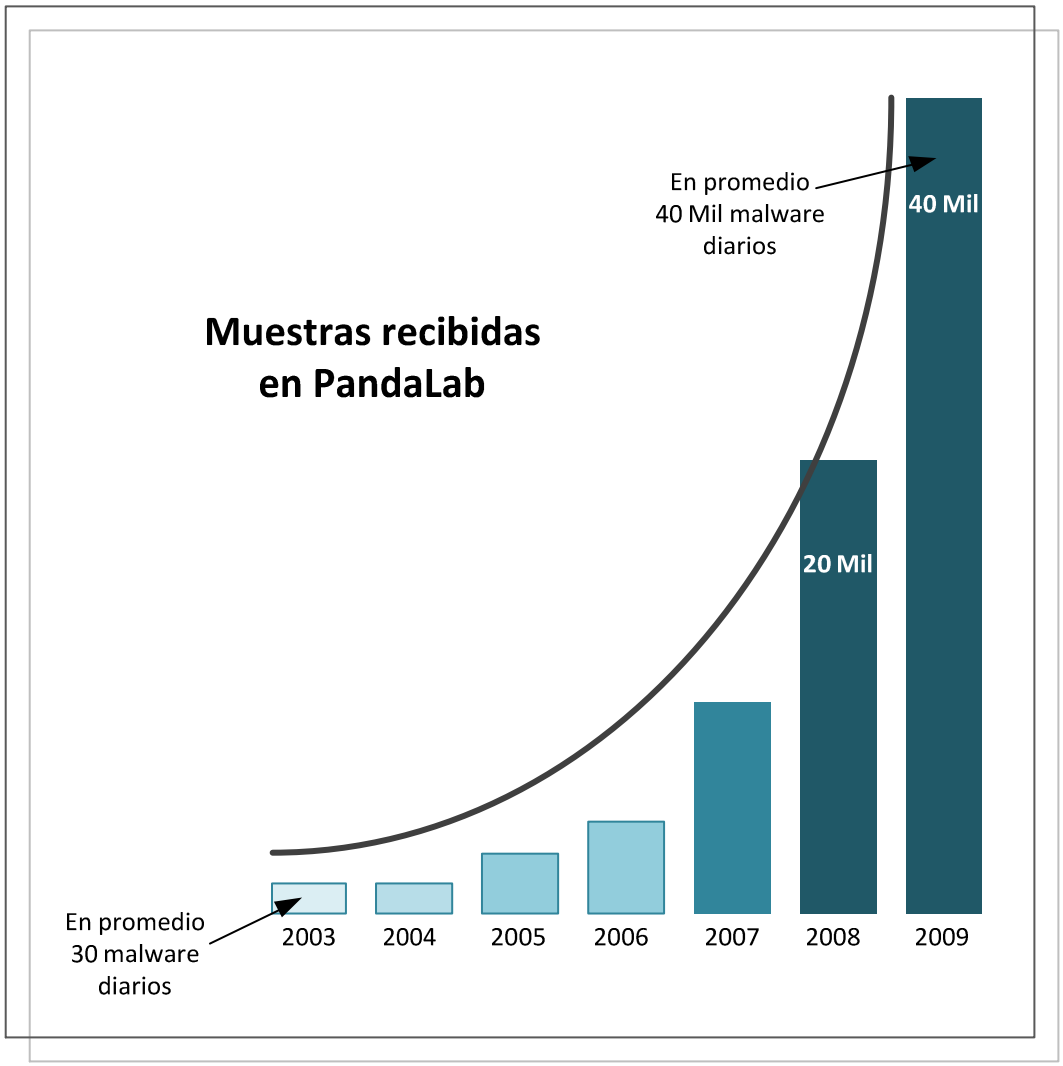

Fig. 3 140 Muestras de Malware detectado en PandaLabs 2003 - 2009

Como podemos ver en el grafico desde el 2003 hasta el 2009 los malware detectados en al laboratorio de la empresa Panda han aumentado exponencialmente, de recibir o detectar 30 malware diarios ha pasado a 40 mil en el 2009 y mucho más en la actualidad hace que sea necesario

cambiar los métodos y sistemas de detección, los mismos deben ser métodos muy sofisticados ya que los malware han evolucionado y aumentado en los últimos años.

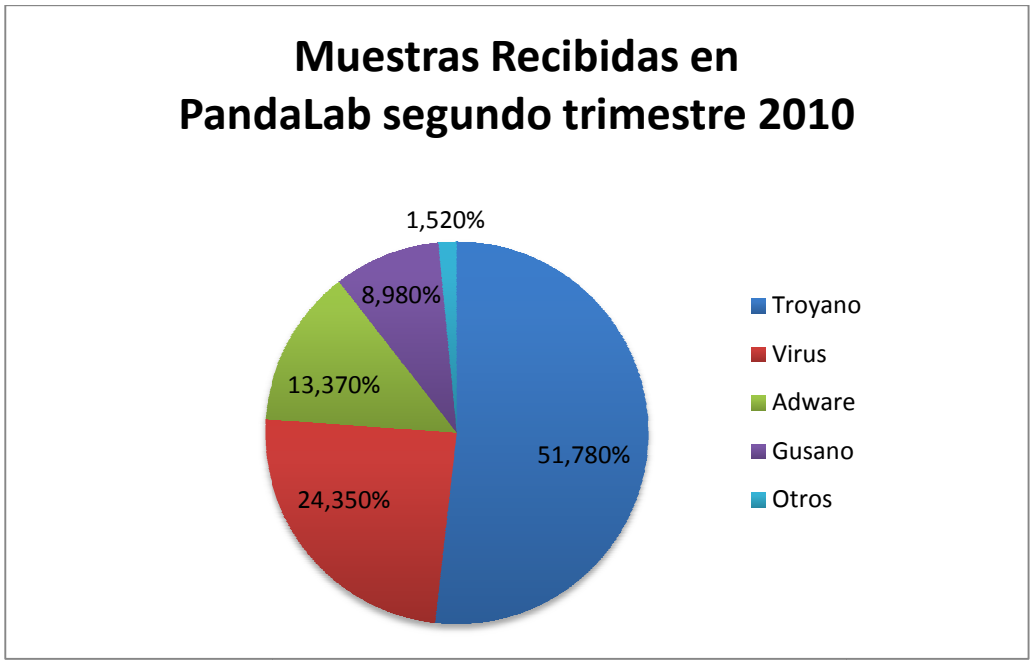

Fig. 3 141 Muestras de tipos de Malware detectados en PandaLabs segundo trimestre 2010

Como podemos notar en la grafica e los últimos tiempos el malware más común o mas detectado es el Troyano o Caballo de Troya con más del cincuenta por ciento entre los tipos de malware, un troyano en un software que está alojado en el cliente el cual se encuentra en forma latente hasta que un administrador del malware de forma remota lo activa con diferentes fines, envió de spam, captura de datos, etc., con esto podemos decir que en muchos casos el usuario cree aparentemente que tiene el control del equipo que por atrás hay alguien que realmente tiene el control de la máquina.

Los troyanos son los malware ideales para crear las botnets o redes de bots, estas consisten en infectar a las maquinas con un troyano el mismo que será actualizando remotamente por el botmaster para no perder la comunicación y para que el antivirus no lo detecte, de esta forma botmaster crea una gran red de maquinas infectas a las cuales se las conoce como ordenadores zombis, de esta forma el botmaster al poseer esta red la puede usar para diferentes fines.

El botmaster puede vender o alquilar parte de esta red, la cual puede ser utilizada para generar ataques Spam, captura de datos bancarios o de tarjetas, envió de troyanos y ataques de denegación de servicio DOS.

Estas redes de bots se propagan de forma muy efectiva a través de redes P2P, dispositivos USB y enlaces MSM, entre otros.

El Caso Mariposa

El caso Mariposa (BotNets), es el más representativo como muestra de la peligrosidad de las redes de Bots, las cifras de infección obtenidas hasta abril del 2010 suman 13 millones de ordenadores infectados a nivel mundial, los botmaster de esta red tenían datos de 800 mil personas en 190 países, entre las víctimas de encontraban más de la mitad de las mil

mayores empresas del mundo, se calcula que los daños ascienden a varios millones de dólares.

El hecho de tener a más de la mitad de las mayores empresas del mundo, que en teoría tienen sistemas de protección bastante avanzados, es un factor que demuestra la capacidad de expansión de este tipo de troyano, los cuales se promociona libremente por internet ya que existe un vacío legal en cual no lo impide hacer, contribuyendo de manera directa a la proliferación del Cibercrimen que en la actualidad es más rentable que el tráfico de heroína, según el diario El País de España.

Fig. 3 142 El Cibercrimen que en la actualidad es más rentable que el tráfico de heroína, según el diario El País de España. Esta red ya fue desmantelada en un trabajo conjunto de la Guardia Civil Española con el FBI y Panda Security.

Situación del Mercado

Actualmente las empresas dedicadas a la industria del antivirus se encuentran saturadas por la gran cantidad de amenazas existentes y cuya complejidad cada vez es superior, esto ha hecho que se busquen mecanismos para poder alcanzar a registrar esta gran cantidad de malware.

Inteligencia Colectiva

Debido a esta gran afluencia de amenazas las industrias han desarrollado un amanera de recaudación de información llamada Inteligencia Colectiva, la misma que consiste en tener en la nube un gran número de servidores a nivel mundial, los mismos que están en tiempo real recopilando datos de los diferentes malware ya se de PCs, honeypots, URLs, etc., manteniendo un feedback constante.

En esta gran base de datos actualizada casi en tiempo real se realiza con la tecnología de inteligencia colectiva el análisis de los malware para catalogarlos de forma automática y poder sacar el fichero o la medicina para la infección

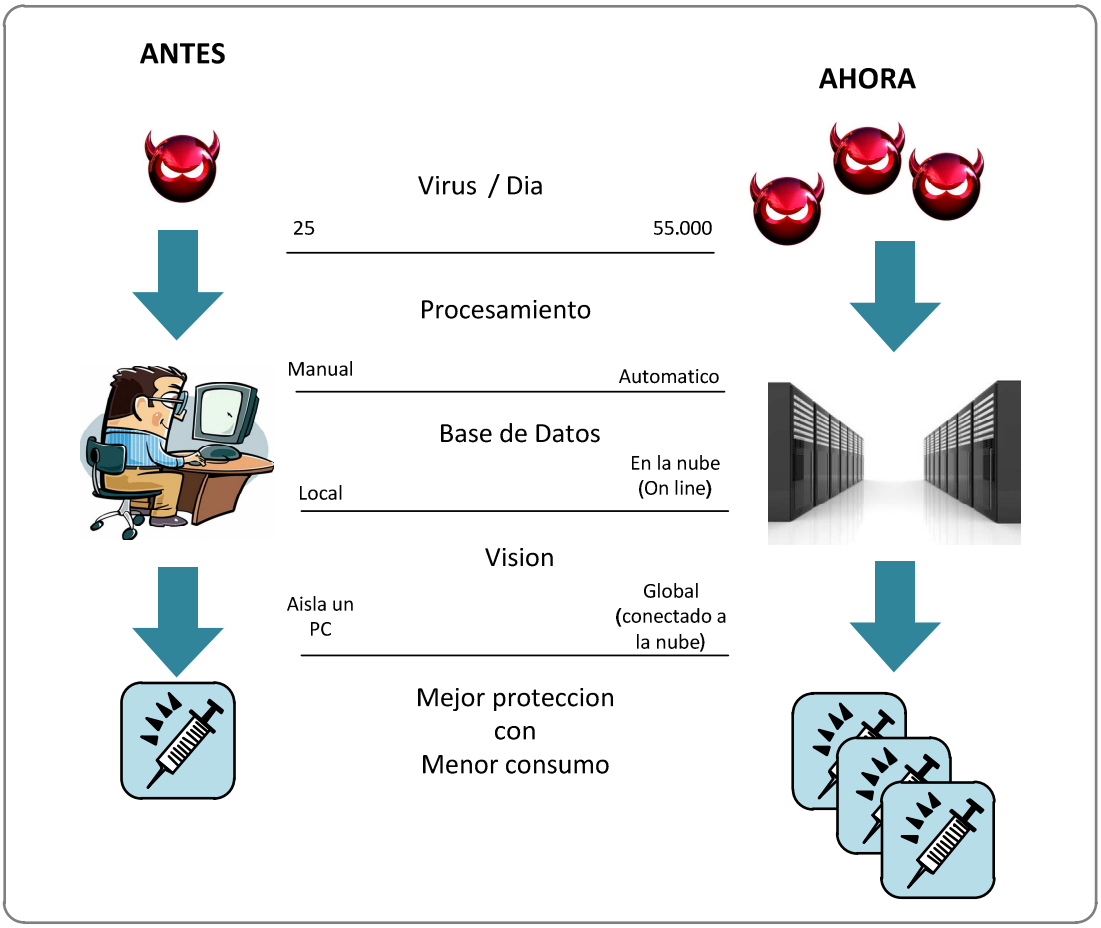

Fig. 3 143 Comparación de detección de malware

Como podemos ver en el grafico antes se recibían o se detectaban pocos malware, alrededor de 25, hoy en día se detectan alrededor de 55 mil, antes el procedo para encontrar el fichero para la cura era manual, ahora es automático con el sistema Inteligencia Colectiva, de igual forma la base de datos ha pasado de ser local a estar en la nube, la visión que se tenía antes era para aislar un PC, ahora es algo Global, con la virtualización o cloud computing, la visión es dar seguridad en la nube.

La tecnología de inteligencia colectiva permite poder catalogar a los programas sospechosos como malware o goodware, en caso de ser un

malware se bloquearan en la nube sus acciones protegiendo de manera más eficiente a los usuarios.

Situación del mercado y Necesidades a Cubrir

En la actualidad la gran mayoría del malware que entra a los sistemas es a través de los siguientes tres medios:

A través de e-mails

A través de tráfico Web

A través del PC (Pendrive, CD-ROM, etc.)

Lo ideal es que toda empresa corporativa tenga protegido estos tres elementos, para poder garantizar en un alto porcentaje la seguridad informática.

Soluciones de Seguridad en la Nube (Cloud Protection)

Debido a la situación actual del mercado donde la tendencia es al Cloud computing y movilidad de los usuarios, los productos deben estar en capacidad bajo estar circunstancias de poder proteger las tres mayores entradas de malware como ya lo hemos mencionado antes, internet, e-mail y PC o endpoint.

Fig. 3 144 Cloud Protection

Cloud Internet Protection.

La mayoría de las empresas que poseen oficinas centrales, remotas y usuarios móviles tienen sistemas de filtrado de tráfico hacia internet desde su red internas, esto mantiene el control de tráfico y de las amenazas, pero cuando los usuarios móviles están fuera de las empresas y acceden a internet no existe control alguno sobre este tráfico pudiéndose así infectarse y por ende al estar dentro de la empresa y conectar su PC al sistema interno puede infectarlo aprovechando alguna vulnerabilidad.

La solución para este tipo de problema es el sistema **Cloud Internet Protection**, el cual consiste en tener un proxy en la nube y de esta manera controlar todo el tráfico hacia internet ya sea de la oficina central, remota o de los usuarios móviles, este proxy o consola en la nube puede ser administrada por personal calificado de la empresa, de esta manera se resuelve el tema de la movilidad y posible infección de los usuarios.

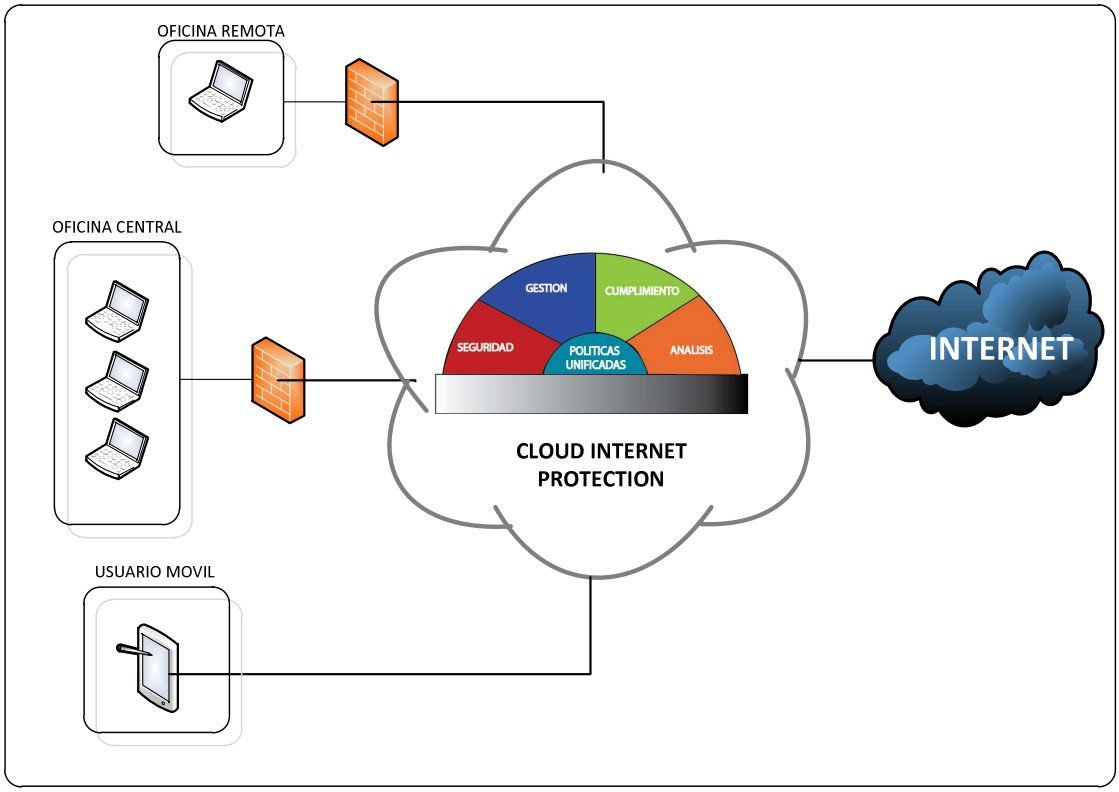

Fig. 3 145 Esquema para Cloud Internet Protection

La figura muestra el esquema para Cloud internet protection, en el mismo podemos encontrar Antivirus, Antispyware, protección avanzada contra amenazas, control de acceso a Internet, filtrado de URL y aplicaciones Webs, prevención de pérdida de información DLP, etc.

Cloud Email Protection.

Estadísticamente se conoce que un 90% de los email que recibe una empresa promedio son Spam, solo el 10% es correo útil, por lo tanto el ancho de banda destinado para el correo esta se ve desperdiciado en un 90%, ancho de banda que puede ser destinado para otro uso.

En cloud email protection lo que se hace es usar un Relay en la nube el cual recibe todos los email destinado para la empresa y mediante un proceso solo permite el paso del trafico limpio, bloquea el paso de spam y por ende reduciendo en consumo de ancho de banda en los correos para la empresa.

Cloud Endpoint Protection.

Actualmente las empresas al tener varias delegaciones ha conllevado a que tengan un servidor de gestión del antivirus por cada una de ellas, esto hace que el administrador este periódicamente actualizando cada uno de ellos cada vez que el fabricante indique alguna mejora o actualización, otro problema que se da en este modelo es que los equipos móviles, que hoy en día son más, hacen la actualización del antivirus directamente por la red con el fabricante, de esta manera el administrador no recibe lo logs de los eventos que se suscitaron en esta dispositivo, perdiendo de alguna manera el control del mismo

Con Cloud EndPoint Protection, lo que se hace es tener una consola de gestión del antivirus centralizado en la nube, en el mismo se registran todos los dispositivos de la empresa y por lo tanto de tendrá el control de los mismos independientemente de su ubicación, realizando actualización, recibiendo los eventos suscitados en cada uno de ellos, y poder realizar el cambio de las políticas de protección de los equipos.

Beneficios Cloud Protection vs Modelo Tradicional

Beneficios	Modelo Tradicional	Cloud Protection
No hay inversión en infraestructura	Infraestructura en casa del cliente	Infraestructura en la nube
No necesita personal especializado	Gestión y monitorización por personal propio	Software y Hardware en la nube, gestionado por el proveedor
No hay costes de mantenimiento	Mantenimiento a cargo del cliente	Mantenimiento por parte del proveedor
Ahorra Tiempo, no requiere personal dedicado	Consume tiempo, instalación compleja.	Instalación fácil y rápido vía web

Tabla 2. Beneficios Cloud Protection vs Modelo Tradicional

En base a las tendencias podemos ver que la vitalización o computación en la nube es algo que prolifera a nivel mundial sin excluir al Ecuador, en nuestro país en el mercado corporativo en los últimos cinco años hemos visto una tendencia a la implementación de un data-center bien

estructurado, especialmente en el segmento financiero, desde el 2008 en el Ecuador la Junta Bancaria mediante resolución JB 2005-834, exige que las empresas financieras implemente soluciones para la disminución del riesgo operativo, este incluye la continuidad en el servicio en caso de desastres ya sea naturales o provocados en el centro de computo, a partir de esto las empresas financieras se vieron en la necesidad de implementar centros de computo alternos para cumplir con la norma, pocas son las empresas que cuentas con suficiente recursos económicos para la implantación de un centro de computo alterno que cumpla con las exigencias tecnológicas del mismo, la gran mayoría no cuenta con estos recursos, unas optaron por adquirir el servicio de Colocation, el cual es el alquiler de espacio físico en un datacenter para colocar los servidores con conectividad a internet las 24 horas todos los días del año, otras optaron por la virtualización, lo cual consiste en alquilar servidores virtuales que pueden ser accedidos vía internet, esta tendencia debe cubrir una necesidad importante que es la seguridad informática, para esto debemos conocer cuál es la situación actual del mercado corporativo en el Ecuador con respecto a seguridad informática.

Situación actual de la Seguridad Informática del mercado corporativo en el Ecuador

De las encuestas realizadas un porcentaje mayor al cincuenta por ciento corresponde al mercado corporativo, las mismas que superan en más del

50% los 250 empleados catalogándose así como grandes empresas, los sectores que predomina en estas son Comercio y Financiero con un 20 y 22 % respectivamente, con un alcance a nivel nacional de cada una de ellas.

Del grupo de las empresas corporativas tenemos que un 57% abarcan el territorio nacional, entiéndase así que tienen presencia en las principales ciudades del Ecuador, aquí también podemos notar la importancia en la actualidad del Internet para el negocio ya que de este mismo grupo en un 100% tienen contratado servicio de Internet y un 74% usa aplicación usa aplicaciones a través de este medio, además un 83% tiene enlaces de transmisión de datos como medio dedicado de comunicación entre sucursales y empresas. Este uso masivo del Internet en el mercado corporativo Ecuatoriano nos indica que la Seguridad Informática es una pieza fundamental para el desarrollo de las empresas, ya que sin las mismas serian muy vulnerables.

Esto hace que las mayoría de las empresas del mercado corporativo tengan que cumplir con ciertas normas de seguridad informática ya sea impuestas por entes reguladores de acuerdo a su modelo de negocio o servicio, dentro de las principales normas que cumple el mercado corporativo tenemos a ITIL en su gran mayoría con un 35%, COBIT con un 12 %, PCI-DSS con un 10%, JB 2005-834 con un 4%, especial para el mercado financiero y ISO 27001 con un 4%.

ITIL (del inglés Information Technology Infrastructure Library) es una de las normas que el mercado corporativo indica que mas cumple con un 35%, a nuestro parecer esto se debe a que ITIL independientemente del modelo de

negocio da descripciones detalladas de un extenso conjunto de procedimientos de gestión ideados para ayudar a las organizaciones a lograr calidad y eficiencia en las operaciones de TI, que es si es lo que toda organización busca.

Siguiendo con nuestro análisis de mercado Corporativo tenemos que solo un 24% realiza outsourcing de seguridad informática a pesar de que solo el 50% tiene posee un área de seguridad informática dentro de la organización, esto indica que no se está poniendo en un primer plano la seguridad informática dentro de ciertas empresas.

El firewall sigue siendo un elemento casi por default dentro de la organizaciones para la protección de la seguridad perimetral con un nivel de presencia de un 96% dentro del mercado corporativo seguidos por los dispositivos IDS e IPS con u 52 y 52% respectivamente, muy atrás quedan los dispositivos WAF con un 4% de presencia, esto es lógico ya que no aplica su uso a todos los modelos de negocios.

En lo concerniente a políticas de Seguridad un 80% indica que tiene definidas políticas globales de seguridad a pesar de que el 98 % está consciente de que existe la posibilidad de perder información, ya sea por robo, algo preocupante es que solo el 39% cree que cuenta con un alto nivel de seguridad informática.

En lo concerniente a las agresiones físicas externas al sistema eléctrico se muestra que existe preocupación por mantener un buen desempeño del mismo, ya que un 70% indica que cuenta con sistemas de alimentación redundante y un 83% indica que cuenta con sistemas de alimentación

ininterrumpida, no así con los sistemas de control de acceso físico ya que solo un 52% menciona que cuentan con sistemas que impiden el acceso físico a los recursos a personal no autorizado y un 54% indica que cuenta con mecanismos físicos que impiden el uso de los sistemas de información a mecanismos no autorizados.

En lo que respecta a los servidores de aplicaciones un 41% ha indicado que ha sido víctima de al menos un ataque donde los tres ataques más recurrentes son DoS con un 32%, Modificación de su sitio web con un 27% y Phishing con un 23%, DoS o Ataque de Denegación de Servicio sigue siendo uno de los principales ataques generados por el cibercrimen.

La información sigue siendo el activo más importante de las empresas, pudiendo verse afectada por muchos factores tales como robos, incendios, fallas de disco, virus u otros, y la medida más eficiente para la protección de los datos es determinar una buena política de copias de seguridad o backups, el mercado corporativo nos indica que el 94% realizan copias de seguridad y casi en su totalidad cuentan con procedimiento para realizar dichas copias, el problema ha este buen procedimiento se da a que solo el 69% de estas copias es automatizada, el resto es propensa al error humano, además solo el 59% es guardada en un lugar de acceso restringido, solo el 65% de estas copias son guardadas fuera del lugar de trabajo, y solo el 80% ha probado en restaurar una copias de estas.

Los mecanismos de identificación y autenticación son muy importante dentro de una organización ya que es un modo de asegurar de que los usuarios son quienes dicen que ellos son, que el usuario que intenta realizar

funciones en un sistema es de hecho el usuario que tiene la autorización para hacer así, esto el mercado corporativo Ecuatoriano lo está controlando en su mayoría ya que se indica que el 83% cuenta con procedimientos de identificación y el 89% con procedimientos de autenticación.

La mayoría de los ataques físicos generalmente ocurren cuando una persona tiene acceso a las dependencias, los intrusos pueden ser personas ajenas a la organización o bien personal interno como empleados o contratistas. Cuando un intruso es capaz de acceder a un físicamente a un sistema informático, por lo general puede dejarlo fuera de funcionamiento, es por esta razón que los controles de acceso físico deben estar bien definidos por una organización, en nuestro mercado corporativo el 89% de las empresas indican que cuentan con controles de acceso, esto es un alto porcentaje que nos da a conocer la importancia a la protección de los recursos, el 67% nos indica que cuentan con log o ficheros que les indican los accesos autorizados y los intentos de acceso ilícitos, con la finalidad de detectar intrusos, un 63% de estas empresas indican tener separados los recursos a los que pueden acceder los usuarios autorizados una vez que pasaron los filtros de seguridad, esto es una buena práctica en medida de protección a los recursos.

Los datos obtenidos contra el virus son muy favorables para el sector financiero, ya que un 87% indica contar con herramientas de antivirus corporativo, 85% que su antivirus protege los correos electrónicos y las descargas vía web, como buena práctica el 89% indica que actualiza regularmente su antivirus, esta puede ser una razón para que solo el 69% haya indicado que alguna vez ha experimentado inconvenientes con algún

tipo de virus, ya que todos conocemos que con la gran cantidad de virus existente que difícil no ser víctima al menos una vez de ellos, además puede ser una razón más para que solo el 30% indique que el SPAM actualmente es un problema para su organización.

Los planes de seguridad y contingencia son procesos calves dentro del plan de negocio de una organización para la continuidad del mismo, el mercado corporativo ecuatoriano nos indica que en 72% que cuenta con un plan de seguridad y 78% con un plan de contingencia, estos son números favorables para nuestro mercado.

Correo electrónico, hoy en día uno de los pilares principales en las comunicaciones de una organización, y por ello debe de contar con las debidas protecciones de seguridad informática, en nuestro mercado un 83% indica contar son su propio servidor de correos, esto hace que tengan que contar con soluciones de protección del correo, pero solo 76% lo tiene, y entre los principales tipos de protección de utilizan están los antivirus, anti-SPAM y mecanismos de encriptación, algo importante de notar es que el 57% de estos ha estando en lista negra (RBL)

Acceso a internet, una de las principales causas en problemas de seguridad informática, es difíciles poder controlar en su totalidad el acceso ya que son los usuarios los que deciden que paginas visitar, es por esta razón que las organizaciones crean políticas para que minimicen el acceso a paginas no seguras que puedan atentar contra la seguridad informática de la organización, en nuestro mercado nos indican que un 83% cuenta con políticas definidas para el acceso a internet, y que un 70% han explicado

claramente a sus trabajadores de las mismas, además un 78% cuenta con políticas corporativas para el acceso a internet, y las mismas son limitadas por cargos y por usuarios.

Web Site, hoy en día si no están en internet simplemente no existes para el mundo, es por esto que el 0% del nuestro mercado corporativo cuenta con web site empresarial, y debido a que se maneja data sensible solo un 54% ha decidido alojar su web site en una empresa externa, el resto lo maneja localmente en su red, notamos también que hay un porcentaje considerable que no dispone de herramientas que auditen intentos de acceso a externos.

En general tenemos que solo un 52% cree que el área de la seguridad informática se ha fortalecido en los últimos anos, esto es algo que debe ser considerado y analizado ya que como hemos visto anteriormente las amenazas y los diferentes ataques que existen han aumentado y evolucionado considerablemente, entonces podríamos indicar que la seguridad informática en el Ecuador no está siguiendo el ritmo impuestos por todos los actores que atentan contra ella.

Productos de Seguridad Informática en el Ecuador

La empresas ecuatorianas dedicadas a la venta de servicios y productos de tecnología, se han dado cuenta que ante el acelerado desarrollo de la tecnología que se da a nivel mundial y ante el aumento del acceso a internet por parte de los usuarios en el ecuador, donde las empresas casi

en un 100% tienen contratado servicio de internet con un porcentaje considerable de los empleados con acceso a este medio y donde los portales web para transacciones online están proliferando, ven la necesidad de ofrecer productos de seguridad informática que vayan a la par con este desarrollo, esto por esto que muchas empresas ya cuentan con un portafolio de productos de seguridad informática entre sus soluciones para ofrecer a los clientes, además están surgiendo empresas jóvenes dedicadas a ofrecer este tipo de soluciones.

Entre los productos de seguridad informática que podemos encontrar en el Ecuador notamos que predominan las marcas de Cisco, Fortinet y Checkpoint con sus equipos que seguridad y control.

Productos de seguridad informática que se ofrecen en el Ecuador.

- Seguridad Perimetral Gestionada
- Análisis de Trafico
- Análisis del Riesgo
- Test de Penetración
- **Ethical Hacking**
- Informática Forense
- Diagnostico de Seguridad de los Sistemas
- Diagnostico de Vulnerabilidades y Riesgos

- Planeación y Administración de la Seguridad Informática
- Planeación Estratégica de Sistemas de Información
- **Asesoría Implantación ISO 27001**
- **Auditorías de Seguridad de Información**
- Auditoria IT
- Software de Seguridad Informática
- Planes para Contingencias y Seguridad de la información
- **Capacitación**
- **Seguridad en Redes**

OPORTUNIDAD DE NEGOCIO

Como hemos podido notar a lo largo del desarrollo del documento el Ecuador no está excluido del desarrollo y avance tecnológico, la globalización hace que cada día la brecha que existía en tecnología entre nuestro país y el resto del mundo sea más estrecha, la Fibra Óptica ha hecho que las distancias se acorten a milisegundos, por ende las empresas en el Ecuador como las del resto del mundo han visto que es inevitable no relacionar su negocio con el Internet, cada día este medio entra a mas y mas a formar parte del desarrollo diario de miles de negocios, esto es muy favorable pero así mismo acarrea consigo nuevas amenazas no

necesariamente provenientes del Ecuador sino de nivel mundial, por lo tanto las precauciones que se deben tomar en lo concerniente a la seguridad informática deben considerar estas amenazas.

El escenario para los emprendedores en el negocio de la seguridad informática es favorable, los segmentos de clientes están definidos, sabemos que cuentan vulnerabilidades, las amenazas están latentes no descansan, cada día son más sofisticadas, por lo tanto podemos decir que la necesidad existe solo que somos una sociedad que solo reacciona ante eventualidades por ende el desafío esta en concientizar y crear un conciencia proactiva en las empresas para adopten medidas de protección y empiecen a equiparse y adquirir los productos de seguridad informática que logren reducir sus vulnerabilidades.

Además es momento de que las empresas entiendan que es importante invertir en seguridad informática para resguardar y garantizar la integridad de la información de la compañía, además que se considere a la seguridad informática como un activo muy importante ya que un buen sistema de protección de datos trae mejores resultados en producción, mejora la gestión de sus trabajadores y otorga mayor calidad al negocio.

Vemos que hoy en día las grandes empresas corporativas están ya pensando e invirtiendo en movilidad, en vitalización, en computación en la nube, entonces eso abre un nicho de mercado por explotar en lo concerniente a seguridad informática, esto es algo que ya se está dando y no es algo que puede pasar, por lo tanto la protección de Internet en la nube, de email en la nube y de endpoints en la nube se vuelve inevitable,

entonces esta es una buena oportunidad para empezar un negocio ya que la computación en la nube, movilidad, vitalización, mejora la productividad de las empresas y la gran mayoría optaran por contar con estos productos y como ya hemos dicho contar con un buen sistemas de seguridad informática no será una opción sino una obligación para estas empresas.

Los Pymes hoy en día se han constituido en una fuerza de producción importante para el Ecuador, pero su poco presupuesto ha sido un factor importante para no implementar las correctas medidas de seguridad informática para aquellas que quieren protegerse, es por esta razón que surge la necesidad de crear servicios de seguridad gestionada que sean capaz de cubrir las necesidades de seguridad de los Pymes sin que tengan que incurrir en grandes gastos de entrada ya sea en adquisición de equipos, personal, implementación, etc.

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

De los resultados obtenidos por las encuestas podemos concluir de manera general lo siguiente:

1. La seguridad informática en el Ecuador aún no alcanza un nivel de madurez que garantice y brinde confianza a los actores del negocio sobre el resguardo de la información, la cual hoy en día constituye uno de los activos más importantes en la organizaciones, y cada día con el avance tecnológico y la penetración del internet en el país están más expuesta a ser víctima del cibercrimen.
2. El mercado corporativo sigue marcando la diferencia en lo concerniente a tecnología pero seguido muy de cerca de las Pymes, ambos tienen un porcentaje de uso del internet de un 100%, esto indica que el riesgo de ser víctimas del cibercrimen mundial ha aumentado ya que cuentan con la conexión al mundo globalizado.
3. El uso de aplicaciones a través de internet por parte de los usuarios que forman parte de una empresa en la actualidad representa un alto porcentaje del 77%, ante éste porcentaje si no se cuenta con las debidas protecciones de seguridad informática podría acarrear un grave problema a la seguridad de la información de las empresas.
4. El servidor de correos se considera hoy en día uno de los dispositivos de aplicaciones más importantes por las empresas para el desenvolvimiento de las actividades diarias, seguido por el dispositivo de base de datos y el servidor de dominios, de aquí podemos mencionar que el hecho de que el correo se haya convertido en una herramienta muy valiosa para una empresa, debe considerarse en los planes de seguridad informática tanto para su confidencialidad, integridad y disponibilidad; el uso masivo de este medio por los usuarios hace que en muchos casos se dependa del uso de las buenas prácticas que los mismos apliquen, no obstante las empresas no deben esperar que esto se dé por parte de los usuarios, y deben implementar medidas de

seguridad informática que garanticen la confidencialidad, integridad y disponibilidad del correo.

5. En el Ecuador se sigue considerando que el mantener el buen desempeño de los dispositivos que permiten el flujo de datos en la red es suficiente para garantizar un buen desenvolvimiento de las actividades, dejando así en otro plano a la seguridad informática.
6. Los dispositivos de seguridad perimetral más usados o aplicados son Firewall IDS e IPS respectivamente, esto ha prevalecido durante ya algún tiempo.
7. Las Empresas Ecuatorianas aun creen que no deben mantener un área dentro de la misma con personal especializado, es tanto así que en el sector financiero podemos encontrar en mayor porcentaje solo una persona a cargo de la seguridad informática, es por esta razón que a nivel ejecutivo no está contemplado la asignación de un presupuesto para el área de Seguridad Informática.
8. La encuesta para este documento fue realizada al personal técnico involucrado directamente con el mantenimiento de la red, éstas personas en un alto porcentaje indicaron estar conscientes de que no poseen un alto nivel de seguridad de la información, sus respuestas nos da a conocer que el problema para la no asignación de los suficientes recursos a la seguridad informática esta en mayor parte del lado ejecutivo de la empresa, a pesar de esto se están comenzando a implementar políticas se seguridad informática que contribuyan a mantener la confidencialidad, integridad y disponibilidad de la información.
9. Las empresas ecuatorianas se han preocupado en mantener un sistema de protección eléctrica ininterrumpida y de alta disponibilidad, pero no así con los sistemas de control de acceso físico a los recursos, ya que la mayoría no cuenta con ellos, ni con mecanismos físicos que impidan el uso de los sistemas de información a mecanismos no autorizados.
10. El mantener copias de seguridad de la información es algo que las empresas en su mayoría lo practican, esto es una buena práctica ya que le garantiza ante alguna pérdida de información ya sea por robo o desastre poder contar con el respaldo de la última copia, el problema

que notamos en éste proceso es debido a que un porcentaje considerable de empresas no cuenta con un procedimiento automatizado para la obtención de las copias de seguridad, existe ausencia de mecanismos criptográficos; haciendo que las mismas estén propensas al error humano, además no cuentan con un lugar interno o externo de acceso restringido para el almacenamiento.

11. Las empresas han llegado a comprender la importancia de los mecanismos de identificación y autenticación, ya que esto les garantiza que solo los usuarios autorizados puedan hacer uso de los sistemas de la empresa, es por esto que notamos que un alto porcentaje cuenta con estas políticas de buenas prácticas dentro de las empresas ecuatorianas, de igual manera a estos controles se suman los controles de acceso físico.
12. Las estadísticas nos indican que en nuestro país, ITIL es el estándar, la misma que define qué hacer y qué no hacer, las buenas prácticas que están en las áreas de la seguridad de la información y en los departamentos de tecnología, eso se debe a que ITIL independientemente del modelo de negocio ayuda a las organizaciones a lograr la calidad y eficiencia en las operaciones de TI.
13. El virus, el desafío de todos los sistemas de seguridad informática, el cual paso de ser el juego de un hacker a convertirse en la principal arma del cibercrimen, actualmente las empresas ecuatorianas han tomado medidas contra este mal, lamentablemente no siempre las medidas que se toman son las más adecuadas.
14. Hoy en día es conocido a nivel global que el cifrado en la comunicación es un buen método ante el robo de información, sin embargo ésta no es una práctica que menos del cincuenta por ciento de las empresas en el ecuador la práctica, al parecer se conoce de su uso pero no se hace conciencia de su importancia.
15. Es notorio decir que el poco entendimiento de la seguridad informática y la falta de apoyo que se le da a la misma por parte de los directivos, no puede ser excusa para no avanzar en un sistema de gestión de seguridad, conocemos que la inversión en seguridad es costosa pero los daños materiales que puede causar la inseguridad serían mucho mayor.

RECOMENDACIONES

1. Como ya lo hemos mencionado antes, los nuevos emprendedores en el negocio de la seguridad informática tienen como desafío hacer que las empresas comiencen a entender la importancia de la seguridad informática, se debe culturizar a los entes relacionados con la seguridad de la información, comenzando por los directivos de las organizaciones.
2. La capacitación dentro de las empresas en seguridad informática tiene que convertirse en el primer paso para el entendimiento de la importancia de la misma, ésta es una oportunidad de negocio que va de acorde a las tendencias actuales y futuras.
3. La seguridad informática gestionada se convertirá en la primera alternativa para las pequeñas empresas por ende hay que poner gran atención es esta oportunidad de negocio.
4. El Ecuador no cuenta con un organismo de control, monitoreo y regulación de la seguridad informática, esta es algo que se hace emergente implementar a corto plazo, sin duda ayudará en el fortalecimiento de la seguridad informática en el país y por ende la empresas se podrán apoyar en este organismo.
5. Ya es hora de pensar en forma globalizada y dejar de creer que el cibercrimen o ciberterrorismo no puede pasar aquí en nuestro país, una vez mencionamos que los problemas de seguridad informática son globalizados y por ende las medidas de protección que debemos tomar deben ser de igual magnitud.
6. La penetración del internet en el mercado HOME está en aumento, las redes sociales crecen junto con sus usuarios, los mismos que proporcionan más datos personales, en contraparte la ingeniería social lo hace de igual manera, por lo tanto la protección en nuestros hogares no es una opción, todos los miembros del hogar tienen un computador con acceso internet, por lo cual deben contar con el conocimiento necesario en protección y navegar a la defensiva.

ANEXOS

1.1 Encuesta utilizada: Empresas

ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

FACULTAD DE INGENIERIA EN ELECTRICIDAD Y COMPUTACIÓN

Encuesta:

Estudio sobre el Estado del Arte de la Seguridad Informática en el Ecuador, y sus necesidades reales

Estimado: A continuación se muestra un conjunto de preguntas, cuyas respuestas contribuirán con el Estudio del Estado del Arte de la Seguridad Informática en el Ecuador.

Importante: El contenido de éste documento será utilizado con fines académicos, los resultados se mostrarán en porcentajes y no se publicaran los nombres de las empresas participantes.

1 - Totalmente en desacuerdo
2 - En desacuerdo
3 - Ni en acuerdo, ni en desacuerdo
4 - De acuerdo
5 - Totalmente de acuerdo

Nombre de la Empresa:
Clasificación de la empresa:
Número de Empleados:

Sector al que Pertenece:

Su empresa se enfoca en:

◉ Ciudad Local

○ Territorio Nacional

Ciertas Ciudades

Internacional

Información sobre servicios actuales

¿Posee servicio de Internet?

Si No

Número de usuarios con acceso a Internet

1 - 10 ( ) 11 - 50 ( ) 51 - 250 ( ) Mas de 250 ( )

¿Posee servicio de transmisión de Datos?

Si No

Número de usuarios

1 - 10 ( ) 11 - 50 ( ) 51 - 250 ( ) Mas de 250 ( )

¿Utilizan aplicaciones los usuarios a través del enlace de internet?

Si No

Actualmente, ¿Cumplen alguna norma de acuerdo a su modelo de Negocio?

Norma ISO 27001:2005 (SGSI)

JB 2005-834

PCI-DSS

COBIT

ITIL

Ninguna

Other

¿Realiza Outsourcing de Seguridad Informática?

Si No

Evaluación de la importancia de la información

Evalúe los dispositivos, más valiosos para el desenvolvimiento de las actividades diarias de su empresa.

1-Totalmente en desacuerdo 2-En desacuerdo 3-Ni en acuerdo, ni en desacuerdo 4-De acuerdo 5-Totalmente de acuerdo

	1	2	3	4	5
Servidor de Correo					
Servidor Web					
Servidor de Aplicaciones					
Servidor de Dominios					
Servidor DNS					
Servidor de Base de Datos					
Firewall					
Routers					
Otros.					

¿Tiene claramente identificados cuales son los procesos más críticos de su empresa?

Si No

¿Podría mencionar uno de ellos? _____

¿Existe alguna persona especializada en seguridad que proporcione soporte a su empresa?

Si No

Evaluación de niveles de seguridad actuales

¿Posee algún dispositivo de seguridad perimetral para su red?

Firewall

IDS

IPS

WAF

UTM (Unified Threat Management)

Ninguno

Other

Política Global de Seguridad

Responda:

	Si	No
¿Ha tenido en cuenta la posibilidad de perder información, que te roben, que no sea correcta?		
¿Se ha definido una política global de seguridad en la empresa?		
¿Poseen un área de Seguridad Informática?		
¿Se hace algún tipo de revisión del sistema de información de forma periódica?		
Considera Ud. ¿Qué posee un alto nivel de Seguridad de Información?		
¿Existen controles que detecten posibles fallos en la seguridad?		
¿Se ha definido el nivel de acceso de los usuarios?, es decir, a qué recursos tienen acceso y a que recursos no.		

Agresiones Físicas Externas

Responda:

	Si	No
¿Existen filtros y estabilizadores eléctricos en la red eléctrica de suministro a los equipos?		
¿Tienen instaladas fuentes de alimentación redundantes?		
¿Tienen instalados Sistemas de Alimentación Ininterrumpida?		

Controles de Acceso Físico

Responda:

	Si	No
¿Existe algún control que impida el acceso físico a los recursos a personal no autorizado? (Puertos de Seguridad, alarmas, controles de acceso mediante tarjetas.		
¿Existe algún mecanismo físico que impida el uso de los sistemas de información a mecanismos no autorizados?		

Servidores

Responda:

	Si	No
¿Posee servidor web?		
¿Alguna vez ha sido víctima de ataques?		

Escoja:

¿Posee algún dispositivo de seguridad perimetral para su red?

- Phishing
- Ataque Denegación de Servicios
- Modificación de su sitio web
- Other

Responda:

	Si	No
¿Existen sistemas operativos servidores que impiden el acceso a los datos a los usuarios no autorizados?		
¿Están los servidores protegidos en cuanto a inicio de sesión y accesos a través de la red?		

	Si	No
¿Tienen instalados fuentes de alimentación redundantes?		
¿Tienen instalados Sistemas de Alimentación Ininterrumpida?		
¿Tienen aplicado un Sistema RAID?		

Copias de Seguridad

Responda:

	Si	No
¿Se realizan copias de los datos?		

¿Con qué periocidad?

- Diaria
- Semanal
- Mensual
- Other

Responda:

	Si	No
¿Existe un procedimiento de copia de seguridad?		
¿Está automatizado?		
¿Se almacenan las copias de seguridad en un lugar de acceso restringido?		
¿Se almacena alguna copia fuera de los locales de trabajo?		
¿Ha probado a restaurar alguna copia de seguridad?		

Mecanismos de Identificación y Autenticación

Responda:

	Si	No
¿Existe un procedimiento de Identificación?		
¿Existe un procedimiento de Autentificación?		
¿Existe un procedimiento de Accounting?		
¿Las contraseñas se asignan de forma automática por el servidor?		
¿Existe un procedimiento de cambio de contraseñas?		

Controles de Acceso Físico

Responda:

	Si	No
¿Existen controles para el acceso a los recursos?		
¿Existen ficheros de log o similares que registren los accesos autorizados y los intentos de acceso ilícitos?		
Una vez pasados los filtros de identificación, ¿Se han separado los recursos a los que tiene acceso cada usuario?		

Virus

Responda:

	Si	No
¿Tiene cuentas de correo electrónico de Internet?		

	Si	No
¿Tiene antivirus corporativo?		
¿Protege su antivirus los correos electrónicos y la descarga de archivos vía Web?		
¿Actualiza regularmente el antivirus?		
¿Alguna vez ha experimentado inconvenientes con algún virus en su sistema?		
¿Es el SPAM un problema para Ud. actualmente?		

Planes de seguridad y contingencias

Responda:

	Si	No
¿Se ha elaborado un plan de seguridad?		
¿Existe un responsable o responsables que coordinen las medidas de seguridad aplicables?		
¿Existe un plan de contingencias?		
¿Existe un presupuesto asignado para la seguridad en la empresa?		
¿Se han incluido en el mismo los aspectos relacionados con las comunicaciones?		
¿Realiza el seguimiento del plan de seguridad personal de la empresa?		
¿Existe un contrato de mantenimiento en el que se priorice la seguridad y el plan de contingencia?		

	Si	No
¿Dispone de personal informático involucrado directamente con la seguridad del sistema?		

Cifrado de las Comunicaciones

Responda:

	Si	No
¿Existe un procedimiento de cifrado de las comunicaciones?		

Correo Electrónico

Responda:

	Si	No
¿Posee servidor de correo?		
¿Tiene alguna solución para la protección de su correo electrónico?		

¿Cuál?

- Mecanismos de Encriptación
- Antivirus
- Protección contra Spam
- Other

Responda:

	Si	No
¿Su servidor de correo ha estado en listas negras (RBL)?		

¿Quién solucionó el inconveniente de RBL?

- Proveedor de Internet
- Administrador de Red

Compañia de Prestación de Servicios

Other

¿Quién administra su servidor de correo?

Administrador

Other

¿Quién administra su servidor de dominio?

Administrador

Other

Responda:

	Si	No
¿Disponen de correo electrónico todos los usuarios?		
De aquellos que disponen, ¿Se les ha informado de la política de la empresa en cuanto a su uso?		
¿Existe algún control sobre los mensajes que se envían y/o reciben?		

Acceso a Internet

Responda:

	Si	No
¿Existe una política definida para los accesos a Internet?		
¿Se ha explicado claramente a los trabajadores de la empresa?		
¿Existe un acceso a Internet Corporativo?		
¿Está limitado el acceso por cargo?		
¿Está limitado el acceso por usuario?		

	Si	No
¿Existen controles sobre las páginas accedidas por cada Puesto o Usuario?		

Web Site

Responda:

	Si	No
¿Dispone de Web Site empresarial?		
¿Se ha contratado el hosting a una empresa externa?		
¿Se realiza el mantenimiento por personal de la propia empresa?		
¿Está alojado en la red empresarial el Servidor de Web?		
¿Se ha contratado personal informático para que diseñe la protección?		
¿Dispone de firewall?		
¿Dispone de herramientas que auditen intentos de acceso externos?		

General

¿Alguno de los problemas presentados anteriormente ha ocasionado la interrupción de algún proceso de la empresa?

Si No

¿Durante cuánto tiempo?

Menos de 1 hora

Entre 2 y 9 horas

Entre 10 y 17 horas

Entre 18 y 24 horas

Un día

Una semana

Other

¿Cree Ud. que en el Ecuador, el Área de Seguridad Informática se ha fortalecido en los últimos años?

Si No

¿Qué cree Ud. que le hace falta con respecto a Seguridad?

_____

_____

_____

_____

ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

FACULTAD DE INGENIERIA EN ELECTRICIDAD Y COMPUTACIÓN

Encuesta:

Estudio sobre el Estado del Arte de la Seguridad Informática en el Ecuador, y sus necesidades reales

Estimado, A continuación se muestra un conjunto de preguntas, cuyas respuestas contribuirán con el Estudio del Estado del Arte de la Seguridad Informática en el Ecuador.

Importante: El contenido de éste documento será utilizado con fines académicos, los resultados se mostrarán en porcentajes.

1) Sexo

 Femenino

☐ Masculino

2) Edad
   - ☐ (0-17)
   - ☐ (18-30)
   - ☐ (31-50)
   - ☐ (51-más)
   - ☐ Anónimo

3) Ocupación:
   - ☐ Estudiante
   - ☐ Empleado
   - ☐ Profesional
   - ☐ Desempleado/a

4) Estudios cursando o completado:
   - ☐ Primario
   - ☐ Secundario
   - ☐ Universitario
   - ☐ Ninguno

5) ¿Te sientes preparado para realizar esta encuesta?
   - ☐ Si
   - ☐ No
   - ☐ No se

6) ¿Tienes contacto con la gente que está relacionada con la informática?
   - ☐ Si
   - ☐ No

7) ¿Tienes computadora en tu hogar o lugar de trabajo?
   - ☐ Si
   - ☐ No

8) ¿Te interesa lo relacionado con la informática?
   - ☐ Mucho
   - ☐ Normal
   - ☐ Poco
   - ☐ Nada

9) ¿Sabes cuánto impacto tiene la seguridad informática en el mercado laboral?

 Mucho

 Normal

 Poco

 Nada

10) ¿Sabes que la integridad, confidencialidad y autenticidad de datos es sólo una parte de la protección de datos?

 Si

 No

11) ¿Tus datos y tu información es privada?

 Si

 No

 No se

11) a) ¿La proteges sólo para que tú puedas verla?

 Si

 No

 No se

11) b) ¿Conoces o sabes lo que es un Cyber?

 Si

 No

11) c) ¿Sabías que existe la posibilidad de que el encargado de las computadoras de los Cybers puede afectarnos sin que lo sepamos?

 Si

 No

 No se

11) d) En caso de que hayas ido a un cyber alguna vez o vas, ¿haces operaciones de dinero o te conectas a páginas con cuentas que tengas que disponer de contraseñas?

 Si

 No

11) e) Ahora que sabes que existe la posibilidad de que el encargado de las PC pueda afectarnos sin que lo sepamos, ¿Sabías que existe la posibilidad de que este ente pueda recolectar las cuentas y contraseñas tuyas y la de los demás en las PC de ese Cyber?

 Si

 No

 No se

11) e) a) Seleccione los métodos que usa:

 Programas que registran las pulsaciones de teclado (Keyloggers)

 Programas para Control de la PC y monitoreo de la Misma

 Archivos de texto guardados en el disco (cookies)

 Cámaras ocultas

 Otro método

12) ¿Conoces las amenazas que rodea la inseguridad informática?

 Mucho

 Normal

 Poco

 Nada

13) ¿Sabías que la principal amenazas somos los seres humanos?

 Si

 No

14) ¿Sabes que es un Sistema Operativo?

 Si

 No

15) a) ¿Cuál de estos Sistemas Operativos usas?

 Windows

 Linux

 Google Chrome OS

 Mac

 Otro

16) b) ¿Eres consciente de que tu Sistema Operativo no es 100% seguro?

 Si

 No

17) c) ¿Sabías que esta inseguridad te puede causar graves daños?

 Si

 No

18) ¿Conoces los diferentes métodos de ser atacado por una amenaza?

- [ ] Si
- [ ] No

19) a) ¿Cuál de estos?

- [ ] Virus
- [ ] Mal uso
- [ ] Problemas con la electricidad
- [ ] Problemas con el proveedor de Internet
- [ ] Ingeniería Social, usando mensajes, páginas o enlaces falsos

20) ¿Sabes cómo actuar ante una posible amenaza?

- [ ] Si
- [ ] No

21) ¿Utilizas alguna técnica para proteger tus datos?

- [ ] Si
- [ ] No

22) a) Marcar formas:

- [ ] Uso Antivirus o programas
- [ ] Cambio las contraseñas cada 1 mes
- [ ] No dejo que nadie use la PC más que yo
- [ ] No abro cualquier página o no descargo casi nada
- [ ] No uso ninguna técnica
- [ ] En el caso de ir a un cyber a realizar operaciones de dinero me fijo si tiene instalado algún keylogger

23) ¿Sabes que es un Anti-Virus?

- [ ] Si
- [ ] No

24) a) ¿Para qué sirve? Marcar las opciones:

- [ ] Para Detectar virus en mi computadora, desinfectarlos y/o borrarlos
- [ ] Para que inhabilite el acceso a páginas maliciosas
- [ ] Para contraatacar contra los hackers o responsables de los virus
- [ ] Para nada. Solo para hacer plata

25) b) ¿Usas Anti-Virus?

 Si

 No

26) c) De ser afirmativa su respuesta, responda: ¿Cuál usas?

 ESET NOD32/Smart Security

 Avast

 Avira

 Kapersky

 Zone Alarm

 AVG

 Norton/Symantec

 Panda

 Mcafee

 Otro

27) d) ¿Actualizas tu Anti-Virus con frecuencia?

 Si

 No

 No Se

28) e) ¿Crees que las empresas que fabrican los antivirus son las mismas que fabrican algunos de esos virus?

 Si

 No

29) ¿Usas Internet adecuadamente?

 Mucho

 Normal

 Poco

 No se

30) Frecuentemente, ¿realizas descargas desde Internet?

 Si

 No

31) ¿Sabías que cuando navegas siempre dejas rastros?

 Si

 No

32) ¿Sabes donde se almacenan esos rastros y que tipos de archivos son?

- [ ] Si
- [ ] No

33) a) Marcar opciones:

- [ ] Se almacenan en nuestro disco rígido
- [ ] Se almacenan en las páginas web o servidores
- [ ] No sé donde se almacenan
- [ ] Los archivos se llaman cookies, que son datos de cada cosa que escribimos, almacenados en archivos de texto
- [ ] No se cuales son los tipos de archivos
- [ ] Creo que son archivos de texto pero no se su nombre

34) ¿Te actualizas con las noticias, cosas o programas que mas impacten en la seguridad informática?

- [ ] Mucho
- [ ] Normal
- [ ] Poco
- [ ] Nada

35) ¿Sabes si los programas que utilizas diariamente son originales o ilegales (piratas o truchos)?

- [ ] Si
- [ ] No

36) a) Caso afirmativo, ¿cuáles son estos programas? Marque los que sean así (no te preocupes no le diremos a nadie que usas esos programas, lo que tu respondas solo lo sabrás tú)

- [ ] Sistema Operativo con Licencia ilegal
- [ ] Antivirus con licencia ilegal
- [ ] Programas de oficina con licencias ilegales (Microsoft Office)
- [ ] Programas varios de uso hogareño
- [ ] No quiero decirlo, por miedo a que caigan los "azules" a mi casa

37) ¿Sabías que algunos de esos programas truchos pueden contener o atraer amenazas informáticas?

- [ ] Si
- [ ] No

38) ¿Te sientes mas informado sobre la seguridad informática al haber realizado esta encuesta?

- [ ] Mucho
- [ ] Normal
- [ ] Poco
- [ ] Nada

39) ¿En qué ciudad trabaja o estudia? [ ]

REFERENCIAS BIBLIOGRÁFICAS

[1] Wikipedia, definición de Amenazas en Seguridad Informática, http://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica, fecha de consulta noviembre 2010

[2] Wikipedia, tipos de Amenazas en Seguridad Informática, http://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica, fecha de consulta noviembre 2010

[3] Wikipedia, tipos de Virus http://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica, fecha de consulta noviembre 2010

[4] Jbex,tipos de Virus, http://www.jbex.net/seguridad-informatica, fecha de consulta noviembre 2010

[5] Wikipedia, elementos de un análisis de riesgo, http://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica, fecha de consulta noviembre 2010

[6] Wikipedia, análisis de impacto al negocio, http://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica, fecha de consulta noviembre 2010

[7] Wikipedia, puesta en marcha de una política de seguridad, http://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica, fecha de consulta noviembre 2010

[8] Wikipedia, técnica para asegurar el sistema, http://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica, fecha de consulta noviembre 2010

[9] Redalyc, codificación de la Información, http://redalyc.uaemex.mx/pdf/903/90312176007.pdf, fecha de consulta noviembre 2010

[10] Wikipedia, codificación de la Información, http://es.wikipedia.org/wiki/Criptolog%C3%ADa, fecha de consulta noviembre 2010

[11] Wikipedia, definición de Zona Desmilitarizada, http://es.wikipedia.org/wiki/Zona_desmilitarizada_(inform%C3%A1tica), fecha de consulta noviembre 2010

[12] Wikipedia, definición de Cortafuegos, http://es.wikipedia.org/wiki/Cortafuegos_(inform%C3%A1tica), fecha de

consulta noviembre 2010

[13] Segu Info, tipos de Cortafuegos, http://www.segu-info.com.ar/firewall/firewall.htm, fecha de consulta noviembre 2010

[14] Wikipedia, sistemas de Detección de Intrusos, http://es.wikipedia.org/wiki/Sistema_de_detecci%C3%B3n_de_intrusos, fecha de consulta noviembre 2010

[15] Wikipedia, programa espía, http://es.wikipedia.org/wiki/Programa_esp%C3%ADa, fecha de consulta noviembre 2010

[16] Wikipedia, antivirus, http://es.wikipedia.org/wiki/Antivirus, fecha de consulta noviembre 2010

[17] Wikipedia, llaves para protección de software, http://es.wikipedia.org/wiki/Llaves_para_protecci%C3%B3n_de_software, fecha de consulta noviembre 2010

[18] Wikipedia, respaldo de Información, http://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica#Respaldo_de_Informaci.C3.B3n, fecha de consulta noviembre 2010

[19] Wikipedia, organismos Oficiales de Seguridad Informática, http://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica#Organismos_oficiales_de_seguridad_inform.C3.A1tica, fecha de consulta noviembre 2010

[20] Wikipedia, ley de comercio electrónico, firmas electrónicas y mensajes de datos, http://www.sinar.gov.ec/downloads/L_comercio.pdf, fecha de consulta noviembre 2010

[21] Wikipedia, estimación Estadística, http://es.wikipedia.org/wiki/Estimaci%C3%B3n_estad%C3%ADstica, fecha de consulta noviembre 2010

[22] Panda Security, Informe Trimestral PandaLabs, segundo trimestre 2010, http://www.pandasecurity.com/img/enc/Informe_Trimestral_PandaLabs_T2_2010.pdf, fecha de consulta Febrero 2011

[23] Panda Security, Caso Mariposa, http://www.pandasecurity.com/spain/enterprise/media/press-releases/viewnews?noticia=10084, fecha de consulta Marzo 2011

[24] Panda Security, Cloud Protection, http://cloudprotection.pandasecurity.com/index.php?lang=es, fecha de consulta Marzo 2011