REPÚBLICA DEL ECUADOR

POLICÍA NACIONAL DEL ECUADOR

INSTITUTO TECNOLÓGICO SUPERIOR
"POLICÍA NACIONAL"

ESPECIALIDAD DE VIGILANCIA SEGURIDAD
PÚBLICA Y PRIVADA

INPLEMENTACIÓN DE SEGURIDADES LÓGICAS INFORMÁTICA EN EL INSTITUTO TEGNOLÓGICO SUPERIOR DE LA POLICIA NACIONAL

Investigadores:
Edison Barrionuevo
Jairo Ñacata

Tutores:
Ing. Marco Herrera

Quito – Julio del 2006

APROBACIÓN DEL TUTOR

En mi calidad de tutor del trabajo de tesis, presentado por los señores Técnicos Superiores **EDISNO BARRIONUEVO y JAIRO ÑACATA**, para optar por el **TITULO DE TECNÓLOGO EN LA CARRERA DE VIGILANCIA Y SEGURIDAD PÚBLICA Y PRIVADA**, certifico que el trabajo:

"IMPLEMENTACIÓN DE SEGURIDADES LÓGICAS INFORMÁTICAS EN EL INSTITUTO TECNOLOGICO SUPERIOS DE LA POLICÍA NACIONAL", reúne los requisitos y méritos suficientes para ser sometido a la presentación pública y evaluación por parte del jurado examinador que se designe.

En la ciudad de Quito a los nueve días del mes de Julio del 2006.

Firma

.....

Ing. Marco Herrera

C.C. No.....

POLICÍA NACIONAL DEL ECUADOR

INSTITUTO TECNOLÓGICO SUPERIOR "POLICÍA NACIONAL"

REGISTRO INSTITUCIONAL No. 17-039P

IMPLEMENTACIÓN DE SEGURIDADES LÓGICAS INFORMÁTICAS EN EL INSTITUTO SUPERIOR DE LA POLICÍA NACIONAL

POR: EDISON BARRIONUEVO

JAIRO ÑACATA C

El presente grado de **TECNÓLOGO EN VIGILANCIA Y SEGURIDAD PÚBLICA Y PRIVADA**, luego de cumplir con todos los requisitos normativos, se aprueba, en nombre del Instituto Tecnológico Superior "Policía Nacional", en la ciudad de Quito a los 25 días del mes de Julio de 2006.

.....	.....
NOMBRE	NOMBRE
……	……
FIRMA	FIRMA
C.C.....	C.C.....

.....

NOMBRE

.....

FIRMA

C.C.....

INDICE GENERAL

Portada
Aprobación del tutor
Aprobación del grado

Contenido **Página**

Introducción I
Justificación II
Objetivos III
Planteamiento del problema IV
Hipótesis V
Variables VI

CAPITULO I

1. MARCO TEÓRICO

1.1 Historia de la seguridad……..……... 1
1.2. Historia, sobre seguridad informática…… ……..... 2
1.2.1. Qué es seguridad informática..... 3

1.4. LEGISLACIÓN INTERNACIONAL Y NACIONAL

1.4.1. Base legal Estados Unidos…….…… 6
1.4.2. Base Legal Alemania…….. 8
1.4.3. Base legal Austria…… 9
1.4.4. Base Legal Chilena…….. 9
1.4.5. Base Legal Ecuatoriana…….. 10
1.4.5.1 Reglamento General a la Ley de comercio
electrónico, firmas electrónicas y mensajes de datos. ……... 10

Contenido **Página**

1.5 SEGURIDAD LÓGICA

1.5.1. Controles de acceso…… 13
1.5.1.1 Identificación y autentificación……. 13
1.5.1.2 Transacciones…… 15
1.5.1.3 Limitaciones a los servicios…….. 15
1.5.1.4. Modalidad de acceso…… 16
1.5.1.5. Ubicación y horario……... 16

1.6. CONTROL DE ACCESO INTERNO

1.6.1. Palabras claves (PASSWORDS)…… 17
1.6.2. Encriptación…… 17
1.6.3. Listas de control de accesos…… 18
1.6.4. Limites sobre la interfase de usuario…….. 18

1.7. CONTROL DE ACCESO EXTERNO

1.7.1. Firewalls o puertas de seguridad……. 18
1.7.2. Acceso de personal contratado o consultores……. 19
1.7.3. Accesos públicos…… 19
1.7.4. Administración…… 19

1.8. ADMINISTRACIÓN DEL PERSONAL Y USUARIOS

1.8.1. Organización del personal…….. 20

Contenido **Página**

1.9. CREACIÓN Y DIFUSIÓN DE VIRUS

1.9.1. Virus informáticos vs. Virus biológicos……. 22
1.9.1.1. Virus Informático (VI)…… 22
1.9.1.2. Virus Biológico (VB)…….. 22
1.9.2. Tipos de virus……. 22
1.9.2.1. Virus de mail…… 23
1.9.2.2. Reproductores-gusanos……..... 23
1.9.2.3. Caballos de Troya…… 23
1.9.3. Modelo de virus informático…… 24
1.9.4. Tipos de daños ocasionados por los virus……..... 24

CAPITULO II

2. MARCO METODOLÓGICO

2.1. Diseño y tipo de investigación…….. 27
2.2. Población y muestra…….. 27
2.3. Instrumento de recolección de datos……. 28
2.4. Técnica de la recolección de datos…… 29
2.5. Recolección de Datos……. 29
2.6. Procedimiento de la investigación…… 30
2.7. Análisis de los resultados……... 30
2.8. Representación e interpretación de resultados……. 31

CAPITULO III

3. INPLIMENTACIÓN DE SEGURIDADES LÓGICAS INFORMATICA PARA EL INSTITUTO TECNOLÓGICO SUPERIOR DE LA POLICIA NACIONAL

Contenido **Página**

3.1 Introducción…… 56
3.2. Propósito……. 56
3.3. Responsabilidades……..... 57
3.4. Comité de informática…… 57

3.5. IMPLEMENTACIÓN DE SEGURIDADES INFORMÁTICAS

3.4.1. Comité de seguridad…… 58
3.4.2. Normas de Elección de Claves……. 58
3.4.3. Normas para Proteger una Clave…….. 59
3.4.4. Para los empleados del ITSPN……..... 60
3.4.5. Sobre el uso de Internet……..... 61
4.4.6. Políticas de seguridades para los computadores……..... 62
4.4.7. Sobre Antivirus…… 64
4.4.8. Seguridad de la información de los PC del ITSPN…….. 65
4.4.9. Sobre energía eléctrica……..... 66
4.4.10. Sobre iluminación……. 66
4.4.11. Sobre Mantenimientos a los equipos informáticos…….. 66

Conclusiones
Recomendaciones
Glosario
Bibliografía
Anexo de formatos

INTRODUCCIÓN

"Saber lo que soy, no es nada sin la Seguridad". Sin duda W. Shaquespeare (1564 – 1616), tenía un concepto más evolucionado de la seguridad que sus contemporáneos del siglo XV y quizás también que algunos de los nuestros".

La meta es ambiciosa. La seguridad como materia académica no existe, y es considerada por los "Estudiosos" como una herramienta dentro del ámbito en que se ha estudiado relaciones internacionales, nacionales, estudios de riesgo, prevención de crímenes y perdidas, etc. Muchos sostienen que es una teoría tan amplia, compleja y abstracta como la pobreza, la belleza o el amor; y ni siquiera arriesga su definición.

Ya desde la antigüedad el hombre tuvo la necesidad de proteger la información sin que otros hombres enemigos tuvieran la posibilidad de obtenerla, de esta necesidad de mantener los secretos surgió en el principio la **CRIPTOGRAFIA,** que no es otra cosa que el arte de ocultar la información.

En nuestro país las entidades privadas por el hecho de manejar un gran capital y brindar productos de alta calidad para el consumidor final se ve en la obligación de emplear un sistema o software de protección confiable porque cada vez utilizan más las redes de Internet para transmitir información.

Hoy en día se ha generado un hambre de información, el incremento de conexiones a Internet ha generado un incremento en las posibilidades de instrucción electrónica desde adentro y fuera de las empresas. El amplio desarrollo de las nuevas tecnologías informáticas esta ofreciendo un nuevo campo de acción a conductas antisociales y delictivas manifestadas en forma antes imposibles de imaginar, ofreciendo la posibilidad de cometer delitos tradicionales en formas no tradicionales.

El motivo de la presente tesis es desarrollar la implementación de procedimientos básicos sobre Seguridad Informática, que deben efectuarse en los equipos informáticos y empleados del Instituto Tecnológico Superior de la Policía Nacional, ya que se suele

manejar con el amarillismo por parte de personal ajeno a este centro con relación a las notas y antigüedades del alumnado que se prepara académicamente, dificultando esto su accionar y colocando en tema de juicio el arduo trabajo que se efectúa por parte de este Centro de Educación Superior.

También se intentará brindar al personal un básico plan de estrategias y metodologías, que si bien no brindan la solución total, podrá cubrir parte del “agujero” que hoy se presenta al hablar de Seguridad informática.

La mayoría del personal administrativo desconoce la magnitud del problema con el que se enfrenta y, generalmente no se invierte ni el capital humano ni económico necesario para prevenir, principalmente el daño y la pérdida de información que, en última instancia es el conocimiento con que se cuenta dentro de este Instituto educativo.

JUSTIFICACIÓN

El ITSPN, como instituto educativo requiere de un sistema informático, seguro, y confiable al igual de que personal, para de esta manera optimizar las funciones y labores diarias, es así; que a lo largo del tiempo se ha venido desarrollando diversos métodos para proteger la información ya en la actualidad al existir diversos mecanismos tecnológicos que con ayuda humana pueden lograr que la información no sea de fácil acceso impidiendo perdidas, alteraciones y hasta un caos financiero.

Al establecer dentro del personal del Instituto Tecnológico los conocimientos básicos y necesarios de las seguridades informáticas existentes, basándose en una implementación de seguridades lógicas se logrará adquirir un conocimiento científico y analizar los diferentes factores que pueden llegar a influir a individuos ajenos o inmersos a centro educativo a realizar estos ataques, con la finalidad de poner en tela de duda la ética profesional con la que se maneja la información.

Así mediante el desarrollo del pensamiento y conocimiento de la tecnología, se obtendrá una manera diferente de pensar y actuar ante estos eventos permitiendo evolucionar en forma técnica lo que dará como consecuencia un ambiente de tranquilidad para buscar un mejor entorno en el desarrollo científico, cultural y social de este centro de educación superior, evitando de esta manera retrasos y molestias en los trabajos que estos desarrollan.

OBJETIVOS

Objetivo General

- Aportar a la ejecución de procedimientos básicos de seguridad informática para que el personal del ITSPN, pueda manejar la información de manera óptima, eficiente y segura, ante posibles robos, contaminación de virus, alteración y pérdida de información.

Objetivos Específicos

- Recopilar información para implementar seguridades físicas y lógicas y de esta manera crear un ambiente seguro de trabajo.
- Desarrollar procedimientos básicos para proteger la información y evitar que al equipo puedan acceder con facilidad.
- Establecer conocimientos básicos y necesarios para saber de que manera proteger la información y que hacer en caso de que un virus ataque la máquina.

PLANTEAMIENTO DEL PROBLEMA

El Instituto Tecnológico Superior “Policía Nacional” ITSPN se creó mediante Acuerdo del Ministerio de Educación y Cultura N° 6617, del 15 de diciembre de 1993, quien autorizó su funcionamiento a partir del año lectivo 1994-1995.

Es así que el ITSPN realiza la adquisición del sistema informático para su funcionamiento en un número reducido, sin dejar de lado que sea el mejor sistema posible dentro del equilibrio que representa las necesidades y el presupuesto de la institución en los años 1994-1995.

Con el pasar de los años hasta llegar a la actualidad se debe tomar en consideración que el equipo informático adquirido años atrás por el ITSPN comienza a declinar, esto conlleva a que sea vulnerable a diferentes tipos de riesgos y que la información se encuentre expuesto tanto a peligros externos como internos.

La falta de implementación de seguridades informática en el medio para proteger la información, es uno de los problemas más trascendentales que confronta el ITSPN en la actualidad y conjuntamente se debe tomar en cuenta el engrandecimiento del la misma lo cual a demandado el ingreso a la institución educativa de un número de profesionales en área de administración, los mismos que traen como consecuencia la necesidad de adquirir equipo informático para cada uno de ellos, brindando de esta manera facilidad para que realicen sus trabajos otorgados.

Es así que la informática en los actuales años en la sociedad a provocado un cambio de tal magnitud que sobre pasa el mero hecho de una revolución tecnológica, por lo tanto es necesario que el ITSPN se comprometa a intentar estar actualizado en el campo de la informática, y de esta mantener se perfeccione la protección de la información.

La seguridad es esencialmente orientaciones e instrucciones que indican cómo manejar los asuntos de seguridad y forman la base de un plan maestro para la implantación efectiva que consiste en la aplicación de barreras y procedimientos que resguarden el acceso a los datos y solo se permita acceder a ellos a las personas autorizadas para hacerlo.

HIPOTESIS

La gran cantidad de personas que manejan la información de este Centro Educativo y que navegan en Internet sin utilizar las seguridades necesarias dan como resultado el robo, alteración de información y contaminación de virus en sus equipos.

VARIABLES

Variable Independiente

- El alto numero de personas que manejan información y navegan en Internet sin utilizar seguridades.

Variable Dependiente

- Perdida, alteración de información y contaminación de virus en equipos informáticos.

CAPITULO I

1. MARCO TEÓRICO

1.1. Historia de la seguridad

Ya desde la antigüedad el hombre tuvo la necesidad de transmitir información sin que otros hombres enemigos tuvieran la posibilidad de obtenerla. De esta necesidad de mantener secretos surgió la criptografía, el arte de ocultar la información (el nombre viene del griego criptos, ocultar, y grafos, escritura).

A lo largo de la historia se han ido desarrollando diversos métodos criptográficos. Los que se desarrollaron hasta la segunda guerra mundial aproximadamente son los conocidos como métodos clásicos.

Durante la Segunda Guerra Mundial se comenzaron a usar máquinas para encriptar mensajes que fueron los embriones de los computadores. Es aquí donde empieza la criptografía moderna.

A partir de este momento, la criptografía se desarrollará de modo paralelo a los ordenadores. Será esencial en la seguridad de los computadores y sus redes, al mismo tiempo que éstos permitirán una mayor capacidad de cálculo, y por tanto, mayor complejidad algorítmica. Este aumento de la complejidad servirá tanto para acabar con antiguos métodos como para crear nuevos.

La Humanidad ha entrado a la era de la Información y el conocimiento no queda excluido de esta realidad.

La informática es un nuevo campo que emerge para dar solución a problemas existentes.

Actualmente, la participación de la Informática extendido por todo el mundo pero principalmente al nivel de uso de sus herramientas tecnológicas más representativas, en lo que hemos denominado "tecnologías de la información".[1]

1.2. Historia, sobre seguridad informática

Conforme los actuales sistemas informáticos se han ido haciendo cada vez mas complejos han puesto de manifiesto una mayor cantidad de puntos vulnerables en cuanto a la seguridad de la información se refiere. Existe más elementos vulnerables a mayor facilitar para perpetrar en contra de ellos, existen dos razones fundamentales para que esto suceda:

El número de posibles atacantes al sistema y su imaginación crece rápidamente ante las posibilidades de obtención de, posiblemente, grandes beneficios. Se puede pensar en el posible beneficio de un posible ataque a una red bancaria la posibilidad de espionaje industrial, etc.

Los medios disponibles para poder vulnerar un sistema son tan sofisticados como el sistema mismo, puesto que tienen el mismo origen tecnológico.

En la actualidad, un sistema informático debe ser considerado como el conjunto de elementos Hardware software, datos y personal que permiten el almacenamiento, proceso y transmisión con el objetivo de realizar determinadas tareas.[2]

La seguridad y confidencialidad de los datos automatizados, contenidos en cualquier soporte legible por computadoras personales o no, no deben considerarse un lema puramente técnico.

Los propietarios de la infamación y los directivos en general no pueden delegar en los informáticos, escuchándose en su propia ignorancia y deben aportar las líneas

[1] w.w.w, monografías. Com./trabajos11/trasnItrans/shtml/

[2] CETTICO, Enciclopedia de informática y computación

maestras a seguir para poder tener la garantía de que están cumpliendo sus requerimientos, tales como quien puede acceder a que, cuanto tiempo se esta guardando determinada información, que controles existen para garantizar la integridad de los datos mas críticos o la continuidad en el caso de incidentes.

1.2.1 ¿Qué es la seguridad Informática?

Técnicas desarrolladas para proteger los equipos informáticos individuales y conectados en una red frente a daños accidentales o intencionados. Estos daños incluyen el mal funcionamiento del hardware, la pérdida física de datos y el acceso a los datos por personas no autorizadas. Diversas técnicas sencillas pueden dificultar la delincuencia informática. Sin embargo, impedir los delitos informáticos exige también métodos más complejos.[3]

1.4. LEGISLACION INTERNACIONAL Y NACIONAL.

1.4.1. Base Legal de Estado Unidos.

El primer abuso de una computadora se registró en 1958 mientras que recién en 1966 se llevó adelante el primer proceso por la alteración de datos de un banco de Miniápolis. En la primera mitad de la década del 70, mientras los especialistas y criminólogos discutían si el delito informático era el resultado de una nueva tecnología o un tema específico, los ataques computacionales se hicieron más frecuentes. Para acelerar las comunicaciones, enlazar compañías, cernios de investigación y transferir daba, las redes deben ser accesibles, por eso el Pentágono, la OTAN, las universidades, la NASA, los laboratorios industriales y militares se convirtieron en el blanco de los intrusos.

[3] w.w.w. segu-info.com

Pero en 1976 dos hechos marcaron un punto de inflexión en el tratamiento policial de los casos: el FBI dictó un curso de entrenamiento para sus agentes acerca de delitos informáticos y el Comité de Asuntos del Gobierno de la Cámara presentó dos informes que dieron lugar a la Ley Federal de Protección de Sistemas de 1985.

Esta ley fue la base para que Florida. Michigan, Colorado, Rhode Island y Arizona se constituyeran en los primeros estados con legislación específica, anticipándose un año al dictado de la Computer Fraud y Abuse Art. de 1986.

Este se refiere en su mayor parte a delitos de abuso o fraude contra casas financieras, registros médicos, computadoras de instituciones financieras o involucradas en delitos interestatales. También especifica penas para el tráfico de claves con intención de cometer fraude y declara ilegal el uso de passwords ajenas o propias en forma inadecuada. Pero solo es aplicable en casos en los que se verifiquen daños cuyo valor supere el mínimo de mil dólares.

En 1994 se adopto el Acta Federal de Abuso Computacional (18 U.S.C. Sec 1030), modificando el Acta de 1986. Aquí se contempla la regulación del virus conceptual izándolos aunque no los limita a los comúnmente llamados virus o gusanos sino que contempla a otras instrucciones designadas a contaminar otros grupos de programas o bases de datos.

Modificar, destruir, copiar, transmitir datos o alterar la operación normal de las computadoras, los sistemas o las redes informáticas es considerado delito. Así, esta ley es un acercamiento real al problema, alejado de argumentos técnicos para dar cabida a una nueva era de ataques tecnológicos.

El FCIC (Federal Computers Investigation Commitee), es la organización más importante e influyente en lo referente a delitos computacionales: los investigadores estatales y locales. Los agentes federales, abogados, auditores financieros, programadores de seguridad y policías de la calle trabajan allí comunitariamente. El

FCIC es la entrenadora del resto de las fuerzas policiales en cuanto a delitos informáticos, y el primer organismo establecido en el nivel nacional.

1.4.2. Base legal de Alemania.

En Alemania, para hacer frente a la delincuencia relacionada con la informática, el 15 de mayo de 1986 se adoptó la Segunda Ley contra la Criminalidad Económica. Es la ley reforma el Código Penal (Art. 148 del 22 de diciembre de 1987) para contemplar los siguientes delitos:

- Espionaje de datos.
- Estafa informática.
- Falsificación de datos probatorios junto a modificaciones complementarias del resto de falsedades documentales como el engaño en el tráfico jurídico mediante la elaboración de datos, falsedad ideológica, uso de documentos falsos.
- Alteración de datos es ilícito cancelar, inutilizar o alterar datos e inclusive la tentativa es punible.
- Sabotaje informático.
- Destrucción de datos de especial significado por medio de deterioro, inutilización, eliminación o alteración de un sistema de datos. También es punible la tentativa.
- Utilización abusiva de cheques o tarjetas de crédito
- Por lo que se refiere a la estafa informática, el perjuicio patrimonial que se comete consiste en influir en el resultado de una elaboración de datos por medio de una realización incorrecta del programa, a través de la utilización de datos incorrectos o incompletos, mediante la utilización no autorizada de datos o a través de una intervención ilícita.

Esta solución fue también adoptada en los Países Escandinavos y en Austria.

1.4.3. Base Legal de Austria.

Según la Ley de reforma del Código Penal del 22 de diciembre de 1987, se contemplan los siguientes delitos:

- Destrucción de datos (Art. 126) no solo datos personales sino también los no personales y los programas.
- Estafa informática (Art. 148) se sanciona a aquellos que con dolo causen un perjuicio patrimonial a un tercero influyendo en el resultado de una elaboración de datos automática a través de la confección del programa, por la introducción, cancelación o alteración de datos o por actuar sobre el procesamiento de datos. Además contempla sanciones para quienes cometen este hecho utilizando su profesión.

1.4.4. Base Legal de Chile

Chile fue el primer país latinoamericano en sancionar una Ley contra Delitos informáticos. La ley 19223 publicada en el Diario Oficial (equivalente del BoletIn Oficial argentino) el 7 de junio de 1993 señala que la destrucción o inutilización de un sistema de tratamiento de información puede ser castigado con prisión de un año y medio a cinco.

Como no se estipula la condición de acceder a ese sistema, puede encuadrarse a los autores de virus. Si esa acción afectara los datos contenidos en el sistema. La prisión se establecerla entre los tres y los cinco años.

El hacking, definido como el ingreso en un sistema o su interferencia con el ánimo de apoderarse, usar o conocer de manera indebida la información contenida en éste, también es pasible de condenas de hasta cinco años de cárcel; pero ingresar en ese mismo sistema sin permiso y sin intenciones de ver su contenido no constituye delito.

Dar a conocer la información almacenada en un sistema puede ser castigado con prisión de hasta tres años, pero si el que lo hace es el responsable de dicho sistema puede aumentar a cinco años. [4]

1.4.5. Base Legal Ecuatoriana

Decreto Ejecutivo 3496. R.O. 735. Reglamento a la Ley de Comercio Electrónico de 31 de diciembre de 2002.

Considerando: Que mediante Ley número 67, publicada en el Registro Oficial Suplemento número 557 de 17 de abril del 2002 se expidió la Ley de Comercio Electrónico, Firmas y Mensajes de Datos;

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

- artículo 1º. Incorporación de archivos o mensajes adjuntos.
- Artículo 2º. Accesibilidad de la información.
- Artículo 3º. Información escrita.
- Artículo 4º. Información original y copias certificadas.
- Artículo 5º. Desmaterialización.
- Artículo 6º. Integridad de un mensaje de datos.
- Artículo 7º. Procedencia e identidad de un mensaje de datos.
- Artículo 8º. Responsabilidad por el contenido de los mensajes de datos.
- Artículo 9º. Prestación de servicios de conservación de mensajes de datos.
- Artículo 10º. Elementos de la infraestructura de firma electrónica.
- Artículo 11º. Duración del certificado de firma electrónica.
- Artículo 12º. Listas de revocación.
- Artículo 13º. Revocación del certificado de firma electrónica.

[4] www.seguridadcorporativa.org

- Artículo 14º. De la notificación por extinción, suspensión o revocación del certificado de firma electrónica.
- Artículo 15º. Publicación de la extinción, revocación y suspensión de los certificados de firma electrónica y digital.
- Artículo 16º. Reconocimiento internacional de certificados de firma electrónica.
- Artículo 17º. Régimen de acreditación de entidades de certificación de información
- Artículo 18º. Responsabilidades de las entidades de certificación de información.
- Artículo 19º. Obligaciones del titular de la firma electrónica.
- Artículo 20º. Información al usuario.
- Artículo 21º. De la seguridad en la prestación de servicios electrónicos.
- Artículo 22º. Envío de mensajes de datos no solicitados.
- Artículo 23º. Sellado de tiempo.
- Artículo Final. El presente reglamento entrará en vigencia a partir de su publicación en el Registro Oficial.

1.5. SEGURIDAD LÓGICA

Luego de ver como nuestro sistema puede verse afectado por la falta de Seguridad Física, es importante recalcar que la mayoría de los daños que puede sufrir un centro de cómputo no será sobre los medios físicos sino contra información por el almacenada y procesada.

Así, la Seguridad Física, solo es una parte del amplio espectro que se debe cubrir para no vivir con una sensación ficticia de seguridad. Como ya se ha mencionado, el activo más importante que se posee es la información, y por lo tanto

deben existir técnicas, más allá de la segundad física, que la aseguren. Estas técnicas las brinda la Seguridad Lógica.

Es decir que la Seguridad Lógica consiste en la aplicación de barreras y procedimientos que resguarden el acceso a los datos y solo se permita acceder a ellos a las personas autorizadas para hacerlo. Al respecto, el "National Institute for Standars and Technology (NIST)" ha resumido los siguientes estándares de seguridad que se refieren a los requisitos mínimos de seguridad en cualquier sistema:[5]

Los objetivos que se plantean serán:

- Restringir el acceso a los programas y archivos.
- Asegurar que los operadores puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no correspondan.
- Asegurar que se estén utilizados los datos, archivos y programas correctos.
- Que la información transmitida sea recibida solo por el destinatario al cual ha sido enviada *y* no a otro.
- Que la información recibida sea la misma que ha sido transmitida.

1.5.1. Controles de acceso

Estos controles pueden implementarse en el Sistema Operativo, sobre los sistemas de aplicación, en bases de datos, en un paquete específico de seguridad o en cualquier otro utilitario.

Es conveniente tener en cuenta otras consideraciones referidas a la seguridad lógica, como por ejemplo las relacionadas al procedimiento que se lleva a cabo para

[5] www.seguridadcorporativa.org

determinar si corresponde un permiso de acceso (solicitado por un usuario) a un determinado recurso. [6]

1.5.1.1 Identificación y autentificación

Es la primera línea de defensa para la mayoría de los sistemas computarizados, permitiendo prevenir el ingreso de personas no autorizadas. Es la base para la mayor parte de los controles de acceso y para el seguimiento de las actividades de los usuarios.

Se denomina Identificación al momento en que el usuario se da a conocer en el sistema: y Autenticación a la verificación que realiza el sistema sobre esta identificación.

Al igual que se considero para la seguridad física, y basada en ella existen cuatro tipos de técnicas que permiten realizar la autenticación de la identidad del usuario, las cuales pueden ser utilizadas individualmente o combinadas:

- Algo que solamente el individuo conoce: por ejemplo una clave secreta de acceso o password, una clave criptográfica, un número de identificación personal o PIN, etc.
- Algo que la persona posee: por ejemplo una tarjeta magnética.
- Algo que el individuo es y que le identifica unívocamente: por ejemplo las huellas digitales o la voz.
- Algo que el individuo es capaz de hacer: por ejemplo los patrones de escritura.

Para cada una de estas técnicas vale lo mencionado en el caso de la seguridad física en cuanto a sus ventajas y desventajas. Se destaca que en los dos primeros casos enunciados, es frecuente que las claves sean olvidadas o que las tarjetas o dispositivos se pierdan, mientras que por otro lado, los controles de autenticación biométricos

[6] www.seguridadcorporativa.org

serian los más apropiados y fáciles de administrar, resultando ser también los más costosos por lo dificultosos de su implementación eficiente.

La Seguridad Informática se basa, en gran medida, en la efectiva administración de los permisos de acceso a los recursos informáticos, basados en la identificación, autenticación y autorización de accesos. Esta administración abarca:

- Proceso de solicitud y de las cuentas de usuarios. Es necesario considerar que la solicitud de habilitación de un permiso de acceso para un usuario determinado debe provenir de su superior.

- Revisiones periódicas sobre la administración de las cuentas y los permisos de acceso establecidos los mismos que deben ser efectuados por personal de auditoria o por la gerencia propietaria del sistema, siempre sobre la base de que cada usuario disponga del mínimo permiso que requiera de acuerdo con sus funciones.

- Nuevas consideraciones relacionadas con cambios en la asignación de funciones del empleado. Para implementar la rotación de funciones, o en caso de reasignar funciones por ausencias temporales de algunos empleados, es necesario considerar la importancia de mantener actualizados los permisos de acceso.

- Procedimientos a tener en cuenta en caso de desvinculaciones de personal con la organización, llevadas a cabo en forma amistosa o no. Los despidos del personal de sistemas presentan altos riesgos ya que en general se trata de empleados con capacidad para modificar aplicaciones o la configuración del sistema, dejando “bombas lógicas” o destruyendo sistemas o recursos informáticos. No obstante, el personal de otras áreas usuarias de los sistemas también puede causar daños, por ejemplo, introduciendo información errónea a las aplicaciones intencionalmente.

Para evitar estas situaciones, es recomendable anular los permisos de acceso a las personas que se desvincularán de la organización, lo antes posible. En caso de despido, el permiso de acceso debería anularse previamente a la notificación de la persona sobre la situación.[7]

1.5.1.2 Transacciones

También pueden implementarse controles a través de las transacciones, por ejemplo solicitando una clave al requerir el procesamiento de una transacción determinada.[8]

1.5.1.3 Limitaciones a los servicios

Estos controles se refieren a las restricciones que dependen de parámetros propios de la utilización de la aplicación o preestablecidos por el administrador del sistema. Un ejemplo podrá ser que en la organización se disponga de licencias para la utilización simultánea de un determinado producto de software para cinco personas, en donde exista un control a nivel sistema que no permita la utilización del producto a un sexto usuario.[9]

1.5.1.4. Modalidad de acceso

Se refiere al modo de acceso que se permite al usuario sobre los recursos y a la información. Esta modalidad puede ser:

- **Lectura:** el usuario puede únicamente leer o visualizar la información pero no puede alterarla. Debe considerarse que la información puede ser copiada o impresa.

[7] w.w.w. segu-info.com
[8] www.seguridadcorporativa.org
[9] www.seguridadcorporativa.org

- **Escritura:** este tipo de acceso permite agregar datos, modificar o borrar información.

- **Ejecución:** este acceso otorga al usuario el privilegio de ejecutar programas.

- **Borrado:** permite al usuario eliminar recursos del sistema (como programas, campos de datos o archivos). El borrado es considerado una forma de modificación.

Además existen otras modalidades de acceso especiales, que generalmente se incluyen en los sistemas de aplicación:

- **Creación:** permite al usuario crear nuevos archivos, registros o campos.
- **Búsqueda:** permite listar los archivos de un directorio determinado.

1.5.1.4. Ubicación y horario

El acceso a determinados recursos del sistema puede estar basado en la ubicación física o lógica de los datos o personas. En cuanto a los horarios, este tipo de controles permite limitar el acceso de los usuarios a determinadas horas de día o a determinados días de la semana. De esta forma se mantiene un control más restringido de los usuarios y zonas de ingreso.

1.6. CONTROL DE ACCESO INTERNO

1.6.1. Palabras claves (PASSWORDS).

Generalmente se utilizan para realizar la autenticación del usuario y sirven para proteger los datos y aplicaciones. Los controles implementados a través de la utilización de palabras clave resultan de muy bajo costo. Sin embargo cuando el usuario se ve en la necesidad de utilizar varias palabras clave para acceder a diversos sistemas encuentra dificultoso recordarlas y probablemente las escriba o elija palabras fácilmente deducibles, con lo que se ve disminuida la utilidad de esta técnica.

Se podrá, por años, seguir creando sistemas altamente seguros, pero en última instancia cada uno de ellos se romperá por este eslabón: la elección de passwords débiles.

Caducidad y control: este mecanismo controla cuándo pueden y/o deben cambiar sus passwords los usuarios. Se define el período mínimo que debe pasar para que los usuarios puedan cambiar sus passwords, y un periodo máximo que puede transcurrir para que éstas caduquen.[10]

1.6.2. Encriptación

La información encriptada solamente puede ser desencriptada por quienes posean la clave apropiada. La encriptación puede proveer de una potente medida de control de acceso. [11]

---

[10] w.w.w.segu-info.com, www.seguridadcorporativa.org

[11] w.w.w.segu-info.com

1.6.3. Listas de control de accesos

Se refiere a un registro donde se encuentran los nombres de los usuarios que obtuvieron el permiso de acceso a un determinado recurso del sistema, así como la modalidad de acceso permitido. [12]

1.6.4. Limites sobre la interfase de usuario

Estos límites, generalmente, son utilizados en conjunto con las listas de control de accesos y restringen a los usuarios a funciones específicas. Básicamente pueden ser de tres tipos: menús, vistas sobre la base de datos y límites físicos sobre la interfase de usuario. Por ejemplo los cajeros automáticos donde el usuario solo puede ejecutar ciertas funciones presionando teclas especificas.[13]

1.7. CONTROL DE ACCESO EXTERNO

1.7.1. Firewalls o puertas de seguridad

Permiten bloquear o filtrar el acceso entre dos redes, usualmente una privada y otra externa (por ejemplo Internet). Los firewalls permiten que los usuarios internos se conecten a la red exterior al mismo tiempo que previenen la intromisión de atacantes o virus a los sistemas de la organización.[14]

---

[12] w.w.w.segu-info.com

[13] w.w.w.segu-info.com

[14] w.w.w.segu-info.com

1.7.2. Acceso de personal contratado o consultores

Debido a que este tipo de personal en general presta servicios temporarios debe ponerse especial consideración en la política y administración de sus perfiles de acceso.[15]

1.7.3. Accesos públicos

Para los sistemas de información consultados por el público en general, o los utilizados para distribuir o recibir información computarizada (mediante, por ejemplo, la distribución y recepción de formularios en soporte magnético, o la consulta y recepción de información a través del correo electrónico) deben tenerse en cuenta medidas especiales de seguridad, ya que se incrementa el riesgo y se dificulta su administración.

Debe considerarse para estos casos de sistemas públicos, que un ataque externo o interno puede acarrear un impacto negativo en la imagen de la organización.[16]

1.7.4. Administración

La política de seguridad que se desarrolle respecto a la seguridad lógica debe guiar a las decisiones referidas a la determinación de los controles de accesos y especificando las consideraciones necesarias para el establecimiento de perfiles de usuarios.

La definición de los permisos de acceso requiere determinar cual será el nivel de seguridad necesario sobre los dato, por lo que es imprescindible clasificar la información, determinando el riesgo que produciría una eventual exposición de la misma a usuarios no autorizados.

---

[15] w.w.w.segu-info.com
[16] w.w.w.segu-info.com

Así los diversos niveles de la información requerirán diferentes medidas y niveles de seguridad.

Para empezar la implementación, es conveniente comenzar definiendo las medidas de seguridad sobre la información más sensible o las aplicaciones más críticas, y avanzar de acuerdo a un orden de prioridad descendiente, establecido alrededor de las aplicaciones.

Una vez clasificados los datos, deberán establecerse las medidas de seguridad para cada uno de los niveles.

Debe existir una concientización por parte de la administración hacia el personal en donde se remarque la importancia de la información y las consecuencias posibles de su pérdida o apropiación de la misma por agentes extraños a la organización.[17]

1.8. ADMINISTRACION DEL PERSONAL Y USUARIOS

1.8.1. Organización del personal

Este proceso lleva generalmente cuatro pasos:

- **Definición de puestos:** debe contemplarse la máxima separación de funciones posibles y el otorgamiento del mínimo permiso de acceso requerido por cada puesto para la ejecución de las tareas asignadas.

- **Determinación de la sensibilidad del puesto:** para esto es necesario determinar si la función requiere permisos riesgosos que le permitan

[17] w.w.w.segu-info.com

alterar procesos, perpetrar fraudes o visualizar información confidencial.

- **Elección de la persona para cada puesto:** requiere considerar los requerimientos de experiencia y conocimientos técnicos necesarios para cada puesto.

- **Entrenamiento inicial y continuo del empleado:** cuando la persona seleccionada ingresa a la organización, además de sus responsabilidades individuales, deben comunicárseles las políticas organizacionales, haciendo hincapié en la política de seguridad. El individuo debe conocer las disposiciones organizacionales, su responsabilidad en cuánto a la seguridad informática y lo que se espera de él.

Esta capacitación debe orientarse a incrementar la conciencia de la necesidad de proteger los recursos informáticos y a entrenar a los usuarios en la utilización de los sistemas y equipos para que ellos puedan llevar a cabo sus funciones en forma segura, minimizando la ocurrencia de errores (principal riesgo relativo a la tecnología informática).

Solo cuando los usuarios están capacitados y tienen una conciencia formada respecto de la seguridad pueden asumir su responsabilidad individual.[18]

1.9. CREACIÓN Y DIFUSIÓN DE VIRUS

Quizás uno de los temas más famosos y sobre los que más mitos e historias fantásticas se corren en el ámbito informático sean los Virus.

[18] w.w.w.segu-info.com

Pero como siempre en esta obscura realidad existe una parte que es cierta y otra que no la es tanto. Para aclarar este enigma veamos porque se eligió la palabra Virus (del latín Veneno) que son realmente estos “parásitos”.

1.9.1. Virus informáticos vs. virus biológicos

Un análisis comparativo de analogías y diferencias entre las dos ‘especies”, muestra que las similitudes entre ambos es poco menos que asombrosas. Para notarlas ante todo debemos saber con exactitud que es un Virus Informático y que es un Virus Biológico.

1.9.1.1. Virus Informático (VI)

Pequeño programa, invisible para el usuario (no detectable por el sistema operativo) y de actuar especifico y subrepticio, cuyo código incluye información suficiente v necesaria para que, utilizando los mecanismos de ejecución que le ofrecen otros programas a través del microprocesador, puedan reproducirse formando replica de sí mismos (completas, en forma discreta, en un archivo, disco u computadora distinta a la que ocupa), susceptibles de mutar; Resultando de dicho proceso la modificación, alteración y/o destrucción de los programas, información y/o hardware afectados (en forma lógica).

1.9.1.2. Virus Biológico (VB)

Fragmentos de ADN o ARN cubiertos de una capa proteica. Se reproducen solo en el interior de células vivas, para lo cual toman el control de sus enzimas y metabolismo. Sin esto son tan inertes como cualquier otra macromolécula.

1.9.2. Tipos de virus

Un virus puede causar daño lógico (generalmente) o físico (bajo ciertas circunstancias y por repetición) de la computadora infectada y nadie en su sano juicio

deseará ejecutarlo. Para evitar la intervención del usuario los creadores de virus debieron inventar técnicas de las cuales valerse para que su programa pudiera ejecutarse. Estas son diversas y algunas de lo más ingeniosas:

1.9.2.1. Virus de mail

El ‘último grito de la tecnología” en cuestión de virus. Su modo de actuar, se basa en la confianza excesiva por parte del usuario: a este llega vía mail un mensaje con un archivo comprimido (ZIP por ejemplo), el usuario lo descomprime y al terminar esta acción, el contenido (virus ejecutable) del archivo se ejecuta y comienza el daño.

Este tipo de virus tomó relevancia estos últimos años con la explosión masiva de Internet y últimamente con el virus Melissa y I Love You. Generalmente estos virus sé auto envían a algunas de las direcciones de la libreta. Cada vez que uno de estos usuarios recibe el supuesto mensaje no sospecha y lo abre, ocurriendo el mismo reenvió y la posterior saturación de los servidores al existir millones de mensajes enviados.

1.9.2.2. Reproductores-gusanos

Son programas que se reproducen constantemente hasta agotar totalmente los recursos del sistema huésped y/o recopilar información relevante para enviarla a un equipo al cual su creador tiene acceso.

1.9.2.3. Caballos de Troya

De la misma forma que el antiguo caballo de Troya de la mitología griega escondía en su interior algo que los troyanos desconocían, y que tenia una función muy diferente a la que ellos podían imaginar; un Caballo de Troya es un programa que aparentemente realiza una función útil pero además realiza una operación que si el

usuario desconoce y que generalmente beneficia al autor del troyano o daña el sistema huésped.

Si bien este tipo de programas no cumple con la condición de auto-reproducción de los virus, encuadran perfectamente en la característica de programa dañino.

Consisten en introducir dentro de un programa una rutina o conjunto de instrucciones, no autorizadas y que la persona que lo ejecuta no conoce, para que dicho programa actúe de una forma diferente a como estaba previsto.

1.9.3. Modelo de virus informático

Un virus está compuesto por su propio entorno, dentro del cual pueden distinguirse tres módulos principales:

- **Módulo de Reproducción:** es el encargado de manejar las rutinas de parasitación de entidades ejecutables con el fin de que el virus pueda ejecutarse ocultotamente, permitiendo su transferencia a otras computadoras.

- **Módulo de Ataque:** Es el que maneja las rutinas de daño adicional al virus. Esta rutina puede existir o no y generalmente se activa cuando el sistema cumple alguna condición. Por ejemplo el virus Che móvil se activa cada vez que el reloj del sistema alcanza el 26 de cada mes.

- **Módulo de Defensa:** Este módulo, también optativo, tiene la misión de proteger al virus. Sus rutinas tienden a evitar acciones que faciliten o provoquen la detección o remoción del virus.

1.9.4. Tipos de daños ocasionados por los virus

Los virus informáticos no afectan (en su gran mayoría) directamente el hardware si no a través de los programas que lo controlan, en ocasiones no contienen código nocivo, o bien, únicamente causan daño al reproducirse y utilizar recursos escasos corno el espacio en el disco rígido, tiempo de procesamiento, memoria, etc. En general los daños que pueden causar los virus se refieren a que el sistema se detenga, el borrado de archivos, comportamiento erróneo de la pantalla, despliegue de mensajes, desorden en los datos del disco, aumento del tamaño de los archivos ejecutables o reducción de la memoria total.

Para realizar la siguiente clasificación se ha tenido en cuenta que el daño es una acción de la computadora, no deseada por el usuario:

- **Daño Implícito:** es el conjunto de todas las acciones dañinas para el sistema que el virus realiza para asegurar su accionar y propagación. Aquí se debe considerar el entorno en el que se desenvuelve el virus ya que el consumo de ciclos de reloj en un medio delicado (como un aparato biomédico) puede causar un gran daño.

- **Daño Explicito:** es el que produce la rutina de daño del virus. Con respecto al modo y cantidad de daño.

- **Daños triviales:** daños que no ocasionan ninguna pérdida grave de funcionalidad del sistema y que originan una pequeña molestia al usuario. Deshacerse del virus implica, generalmente, muy poco tiempo.

- **Daños Menores:** daños que ocasionan una pérdida de la funcionalidad de las aplicaciones que poseemos. En el peor de los casos se tendrá que reinstalar las aplicaciones afectadas.

- **Daños moderados:** los daños que el virus provoca son formatear el disco rígido o sobrescribir parte del mismo. Para solucionar esto se deberá utilizar la última copia de seguridad que se ha hecho y reinstalar el sistema operativo.

- **Daños mayores:** algunos virus pueden, dada su alta velocidad de infección y su alta capacidad de pasar desapercibidos, lograr que el día que se detecta su presencia tener las copias de seguridad también infectadas. Puede que se llegue a encontrar una copia de seguridad no infectada, pero será tan antigua que se haya perdido una gran cantidad de archivos que fueron creados con posterioridad.

- **Daños severos:** los daños severos son hechos cuando un virus realiza cambios mínimos, graduales y progresivos. No se sabe cuando los datos son correctos o han cambiado, pues no hay unos indicios claros de cuando se ha infectado el sistema.

- **Daños ilimitados:** el virus "abre puertas" del sistema a personas no autorizadas. El daño no lo ocasiona el virus, sino esa tercera persona que, gracias a él, puede entrar en el sistema.[19]

[19] w.w.w.segu-info.com

CAPITULOII

2. MARCO METODOLÓGICO

2.1. Diseño y tipo de investigación

El diseño de la investigación metodológica consiste en la planificación de los procedimientos que se llevaron a cabo para construir la información requerida en este estudio, de acuerdo con las características y objetivos planteados en la investigación.

La investigación “Implementación de Seguridades Lógicas Informáticas para el Instituto Tecnológico Superior de la Policía Nacional” corresponde a una investigación de campo de carácter descriptivo apoyada en una pesquisa documental característica fundamental de los estudios de campo.

Los contenidos que se indagaron en la investigación, constituyen características que han ocurrido y ocurren en El Instituto Tecnológico Superior de la Policía Nacional en el cantón Quito y que describen la propuesta de implementación de Seguridades Lógicas Informáticas, conjuntamente fue diagnosticar el problema y describirlo, para luego tomar acciones que promuevan soluciones.

2.2. Población y muestra

Para la presente investigación se considero como población de estudio a los miembros policiales que labora en el Instituto Tecnológico Superior de la Policía Nacional.

Población de los miembros policiales que laboran en el Instituto Tecnológicos Superior de la Policía Nacional.

Población	Frecuencia	Porcentaje
Jefes	1	5%
Oficiales	1	5%
Clases	8	42%
Policías	2	11%
Personal civil	7	37%
Total	19	100%

La **Muestra** constituye una parte de los elementos de la población, para el efecto se proceder al cálculo matemático para determinamos el tamaño de la muestra.

Formula para calcular la muestra:

$$n = \frac{PQ * N}{(N-1)\frac{E}{K} + PQ}$$

Finalmente se llega a concluir que la población es 19 y la muestra es de 11.

2.3. Instrumento de recolección de datos

Para dar cumplimiento a los objetivos y la hipótesis propuesta en la presente investigación, y como el estudio se sustentó en una investigación de campo de carácter descriptivo se elaboró un cuestionarios que permitan recabar la opinión de los encuestados.

El cuestionario está distribuido en cuatro partes:

1. Presentación.- Se expresa el motivo de la investigación.

2. Instrucciones.- Se expone la forma como llenar el cuestionario.
3. Información general.- Referida a la capacitación de los encuestados respecto al tema.

4. Información específica.- En la que se recabó la opinión de los miembros policiales del Instituto Tecnológico de la Policía Nacional.

2.4. Técnica de la recolección de datos

Para cumplir con los objetivos de la investigación, es necesaria la búsqueda de técnicas adecuadas que permitan la recopilación de la información.

2.5. Recolección de Datos

Para recabar la información y cumplir con los objetivos, se utilizó un cuestionario con escala dicotómica, para lo cual se le presentó al respondiente preguntas de manifestación y afirmaciones, para cada una de ellas se registró en una escala, su grado de frecuencia con el contenido del ítem. La escala que se utilizó es la siguiente:

Escala de evaluación del Instrumento de Campo

NIVELES DE RESPUESTA	**EQUIVALENCIA**
SI	Afirmativamente
NO	Negativamente

Las principales características del instrumento de campo son las siguientes:

- Considerando el tipo de respuesta el instrumento es estructurado, es decir, contiene preguntas cerradas.
- El número de ítems tiene correlación con los objetivos e interrogantes de la investigación.

- Fue de aplicación directa e individual a los empleados que laboran en Instituto Tecnológico Superior de la Policía Nacional.

2.6. Procedimiento de la investigación

Para el logro de los objetivos del presente estudio, se cumplieron las siguientes etapas:

- Planteamiento del problema
- Revisión bibliográfica
- Definición y delimitación de la población
- Selección de la muestra
- Concreción del sistema de variables
- Diseño y elaboración de instrumentos
- Estudio de campo
- Procesamiento y análisis de la información
- Conclusiones y recomendaciones
- Formulación de la propuesta

2.7. Análisis de los resultados

A continuación se presentan de manera organizada y sistemática, el análisis e interpretación de los datos y resultados obtenidos a través de la aplicación del instrumento de investigación a los miembros policiales y personeros inmersos dentro del Instituto Tecnológico Superior de la Policía Nacional.

2.8. Representación e interpretación de resultados

Los resultados de la investigación de campo se presentan en las siguientes tablas de salida, para el análisis se transformó los datos originales en porcentajes con el fin de dar claridad a las opiniones de la población consultada.

Qué es para usted la seguridad informática.

Respuestas	**No. De Encuestados**	**Porcentaje**
Es una serie de protecciones al manejo de datos y archivos confidenciales	6	55%
Conjunto de normas, procedimientos y técnicas para asegurar la integridad de la información	3	27%
Es un sistema que permite a las instituciones guardar la información con reserva	1	9%
Desconoce	1	9%
TOTAL	**11**	**100%**

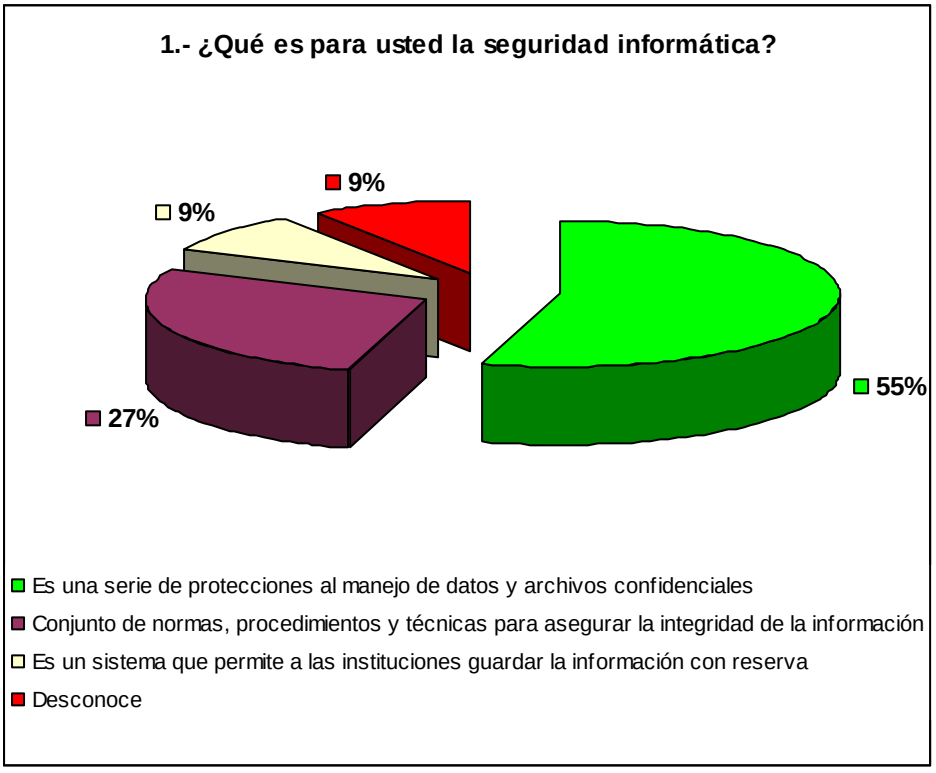
El 55% de las personas encuestadas del Instituto Tecnológico Superior de la Policía Nacional, afirma que la seguridad informática es una serie de protecciones al manejo de datos y archivos confidenciales.

El 27% de las personas encuestadas del Instituto Tecnológico Superior de la Policía Nacional, afirma que la seguridad informática es el conjunto de normas, procedimientos y técnicas para asegurar la integridad de la información.

El 9% de las personas encuestadas del Instituto Tecnológico Superior de la Policía Nacional afirma que la seguridad informática es un sistema que permite a las instituciones guardar la información con reserva.

El 9% de las personas encuestadas del Instituto Tecnológico Superior de la Policía Nacional, respondieron negativamente sobre la pregunta realizada en cuanto a seguridad informático.

Se concluye que el 82% de las personas encuestadas del Instituto Tecnológico Superior de la Policía Nacional, comprende que es la seguridad informática, mientras que, mientras que el 18% de las personas encuestadas respondieron negativamente a la pregunta efectuada.



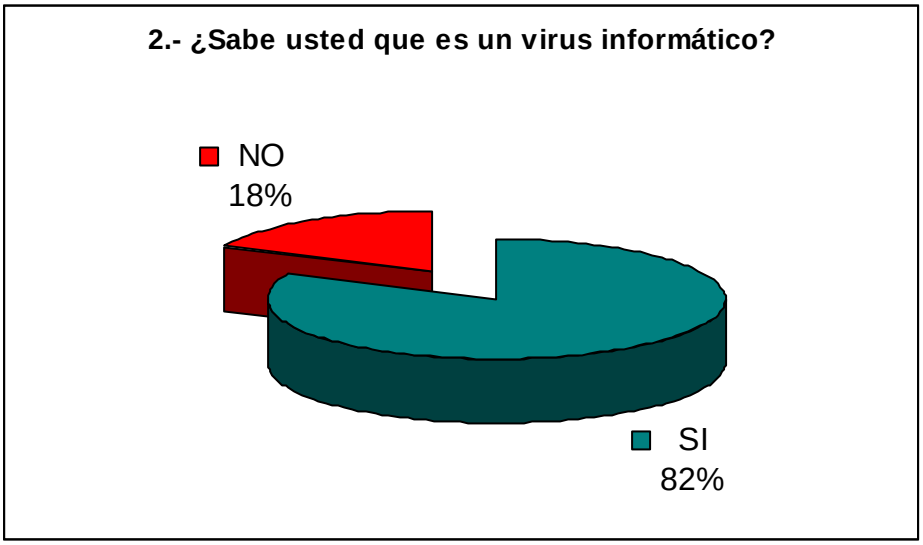
Sabe usted que es un virus informático

Respuestas	No. De Encuestados	Porcentaje
SI	9	82%
NO	2	18%
TOTAL	**11**	**100%**

El 88% de las personas encuestadas del Instituto Tecnológico Superior de la Policía Nacional, afirman conocer lo que es un virus informático.

El 18% de las personas encuestadas del Instituto Tecnológico Superior de la Policía Nacional, respondieron negativamente sobre la pregunta realizada en cuanto al conocimiento del virus informático.

Se concluye que el 88% de las personas encuestadas afirman saber que es un virus informático y que pueden combatirlos con programas antivirus, mientras que el 18% de las perdonas encuestadas responden negativamente sobre la pregunta efectuada y no saben de que manera combatir los virus informáticos.



Cuándo se encuentra ingresando información en su máquina usted la guarda.

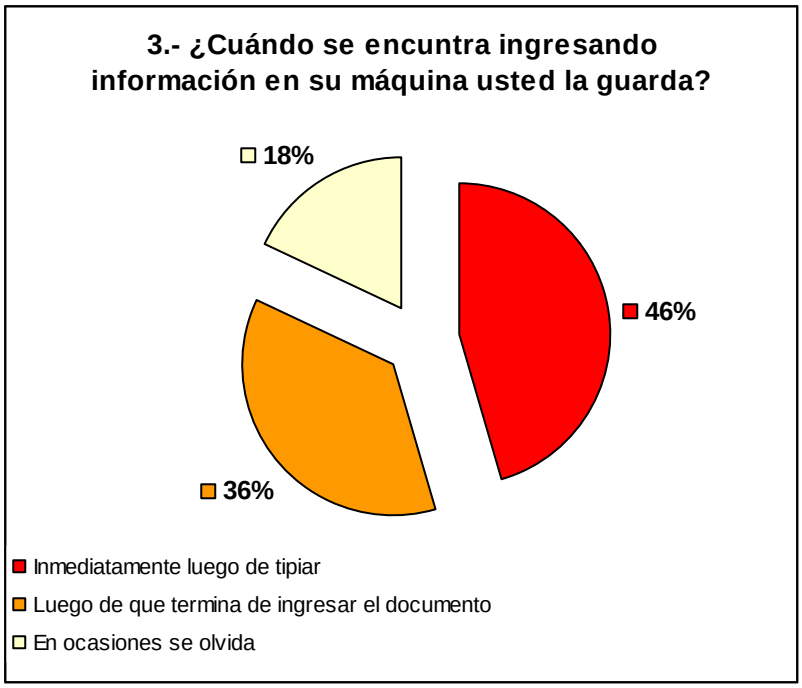
Respuesta	No. De encuestados	Porcentaje
Inmediatamente luego de tipiar	5	45%
Luego de que termina de ingresar el documento	4	36%
En ocasiones se olvida	2	18%
TOTAL	**11**	**100%**

El 45% de las personas encuestadas del Instituto Tecnológico Superior de la Policía Nacional, afirman guardar la información en su máquina inmediatamente luego de tipiar.

El 27% de las personas encuestadas del Instituto Tecnológico Superior de la Policía Nacional, afirman guardar la información en su máquina luego de que termina de ingresar el documento.

El 18% de las personas encuestadas del Instituto Tecnológico Superior de la Policía Nacional, afirman que en ocasiones se olvida de guardar la información en su máquina.

Se deduce que 81% de las personas encuestadas afirman guardar la información inmediatamente luego de tipiar y luego de terminar de ingresar el documento, mientras que el 18% de las personas encuestadas tienen el hábito de no acordarse de guardar la información.



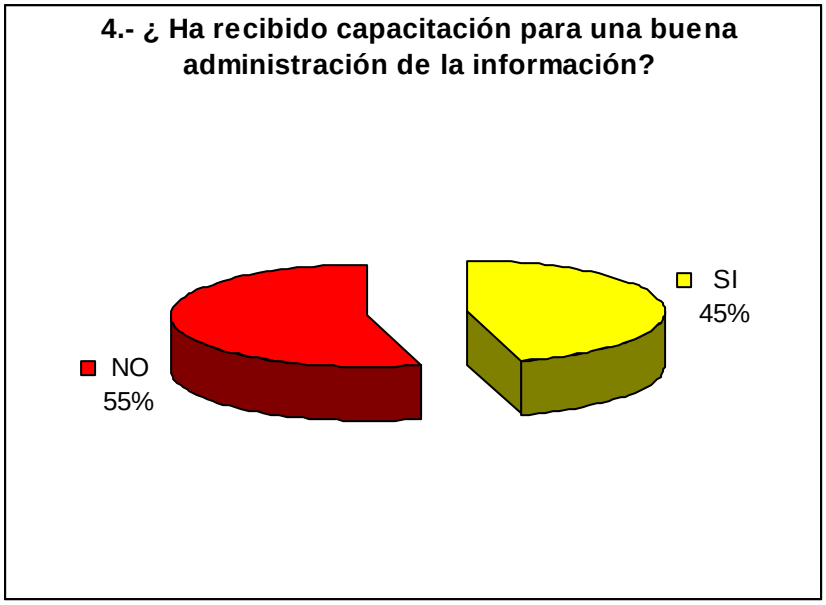
Ha recibido capacitación para una buena administración de la información.

Respuesta	No. De encuestados	Porcentaje
SI	5	45%
NO	6	55·%
TOTAL	**11**	**100%**

El 55% de las personas encuestadas del Instituto Tecnológico Superior de la Policía Nacional, afirman haber recibido capacitación para una buena administración de la información.

El 45% de las personas encuestadas del Instituto Tecnológico Superior de la Policía Nacional, respondieron negativamente sobre la pregunta realizada en cuanto si ha recibido capacitación para una buena administración de la información.

Se deduce que el 55% de las personas encuestadas afirman no haber recibido capacitación para una buena administración de la información, mientras que el 45% de las personas encuestadas han manifestado haber recibido capacitación para administrar la información.



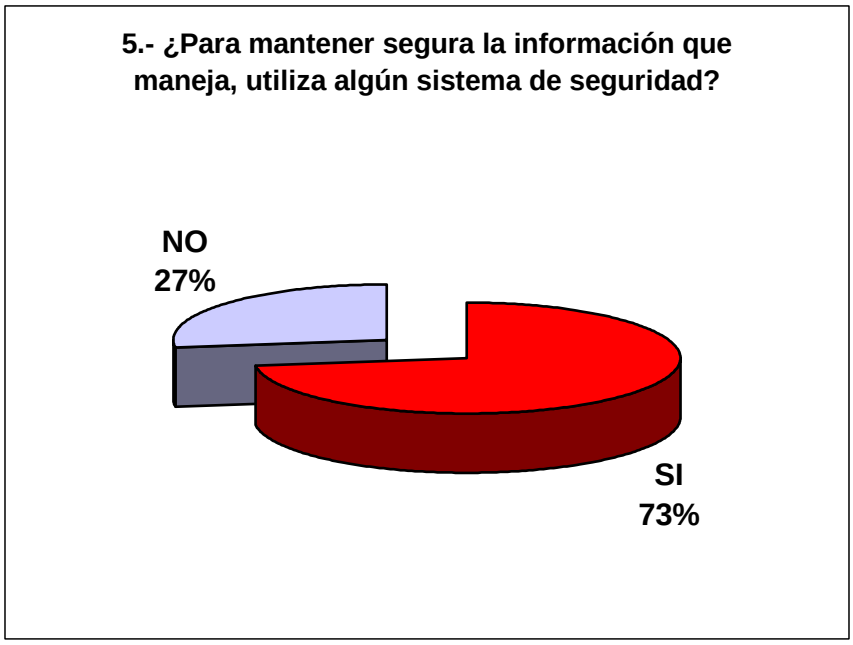
Para mantener segura la información que maneja, utiliza algún sistema de seguridad

Respuesta	No. De encuestados	Porcentaje
SI	8	73%
NO	3	27%
TOTAL	**11**	**100%**

El 73% de las personas encuestadas del Instituto Tecnológico Superior de la Policía Nacional, afirman utilizar algún sistema de seguridad para mantener segura la información.

El 27% de las personas encuestadas del Instituto Tecnológico Superior de la Policía Nacional, respondieron negativamente sobre la pregunta realizada en cuanto si utiliza algún sistema de seguridad para mantener segura la información.

Se concluye que el 73% de las personas encuestadas utiliza algún sistema de seguridad para mantener segura la información empleando claves personales, mientras que el 27% de las personas encuestadas respondieron negativamente utilizar algún sistema de seguridad.



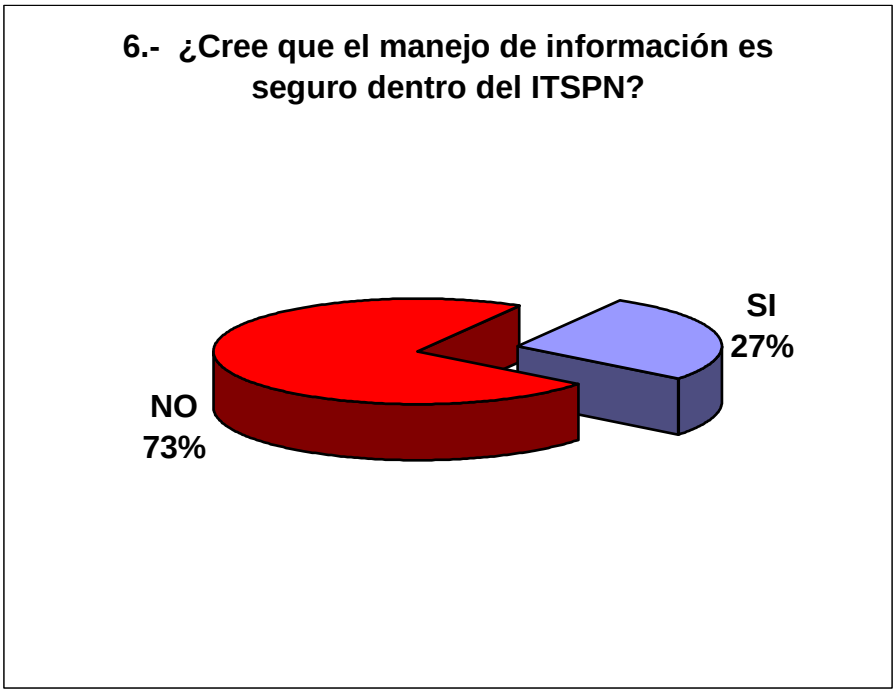
Cree que el manejo de información es seguro dentro del ITSPN

Respuesta	No. De encuestados	Porcentaje
SI	3	27%
NO	8	73%
TOTAL	**11**	**100%**

El 27% de las personas encuestadas del Instituto Tecnológico Superior de la Policía Nacional, afirman conocer que es seguro el manejo de la información dentro del ITSPN.

El 73% de las personas encuestadas del Instituto Tecnológico Superior de la Policía Nacional, respondieron negativamente sobre la pregunta realizada en cuanto si es seguro el manejo de la información dentro del ITSPN.

Se deduce que el 73% de las personas encuestadas manifiesta conocer que el manejo de la información no es seguro en el ITSPN debido a que se comparten los equipos, claves y no existen normas en cuanto al uso de los mismo, mientras que el 27% de las personas encuestadas afirman conocer que si es seguro el manejo de la información en el ITSPN



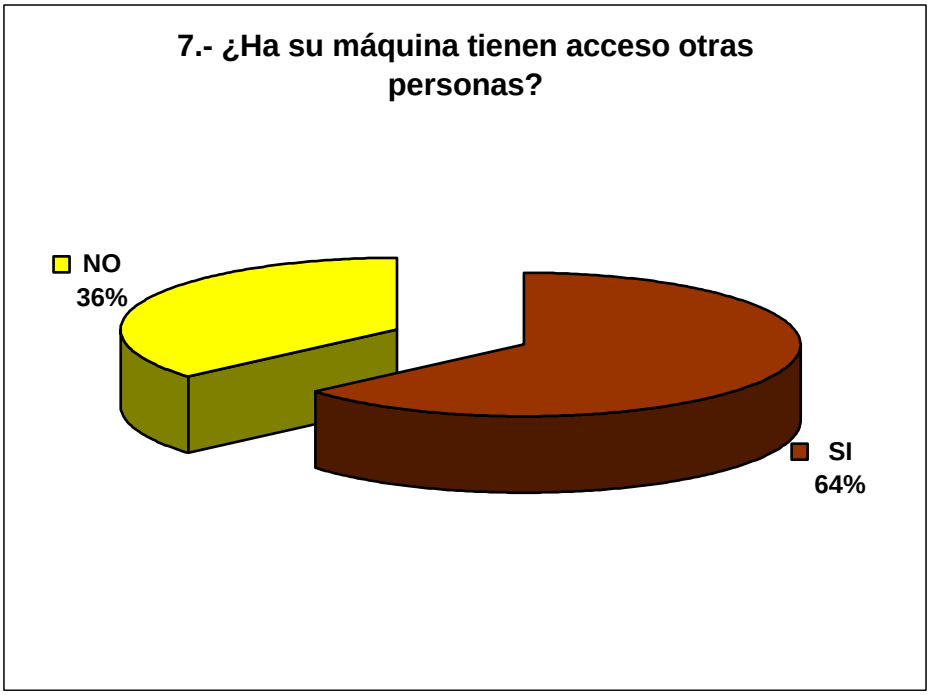
Ha su máquina tiene acceso otra persona.

Respuesta	No. De encuestados	Porcentaje
SI	7	64%
NO	4	36%
TOTAL	**11**	**100%**

El 64% de las personas encuestadas del Instituto Tecnológico Superior de la Policía Nacional, afirman conocer que si tienen acceso otras personas ha su máquina.

El 36% de las personas encuestadas del Instituto Tecnológico Superior de la Policía Nacional, respondieron negativamente sobre la pregunta realizada en cuanto desconocen si tienen acceso otras personas ha su máquina.

Se concluye que 64% de las personas encuestadas afirman conocer que si tiene acceso a su equipo otras personas, mientras que así mismo el 36% de las personas encuestadas desconocen si a su maquina tienen acceso otras personas.



Ha sufrido perdida de información a causa de.

Respuesta	No. De opciones	Porcentaje
Virus	5	31%
Apagón	6	38%
Robo de Información	0	0%
Fallas Mecánicas	1	6%
Fallas humanas	3	19%
Nunca	1	6%
TOTAL	**16**	**100%**

El 31% de las personas encuestadas del Instituto Tecnológico Superior de la Policía Nacional, afirman haber sufrido perdida de información a causa de virus.

El 38% de las personas encuestadas del Instituto Tecnológico Superior de la Policía Nacional, afirman haber sufrido perdida de información a causa de apagones.

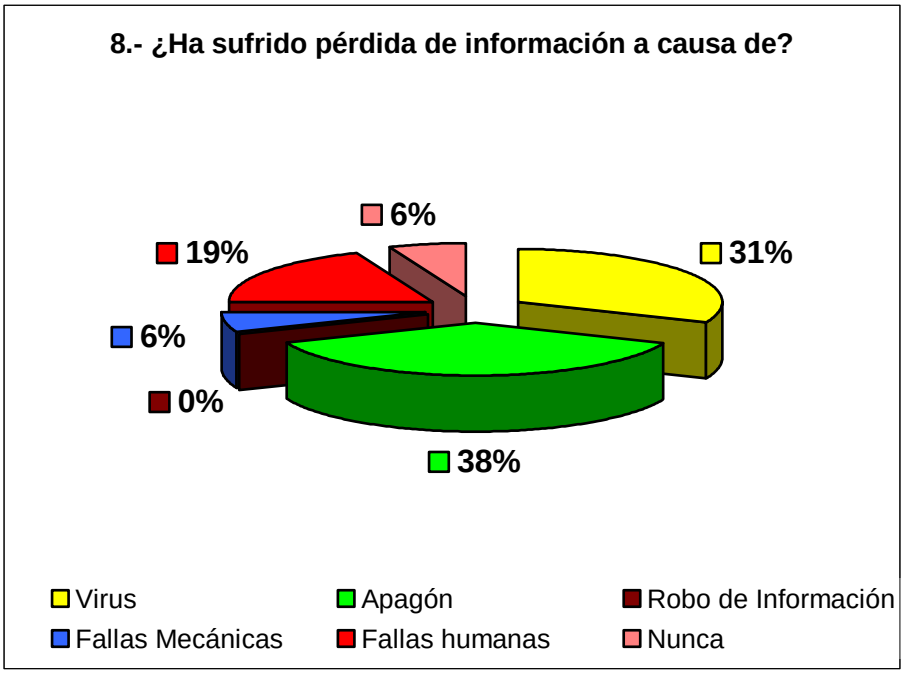
El 0% de las personas encuestadas del Instituto Tecnológico Superior de la Policía Nacional, no ha sufrido perdida de información a causa de robo de información.

El 6% de las personas encuestadas del Instituto Tecnológico Superior de la Policía Nacional, afirman haber sufrido perdida de información a causa de fallas mecánicas.

El 3% de las personas encuestadas del Instituto Tecnológico Superior de la Policía Nacional, afirman haber sufrido perdida de información a causa de fallas humanas.

El 6% de las personas encuestadas del Instituto Tecnológico Superior de la Policía Nacional, afirman nunca a sufrido pérdida de información.

Se deduce que existe una mayor perdida de información con una suma total del 88% a causa de apagones 38%, por virus con un 31% y por fallas humanas con un 19%, mientras que un 6% de las personas encuestadas han perdido su información a causa de fallas mecánicas y otro 6% de las personas encuestadas nunca han perdido su información de ningún modo, además predomina un 0% por robo de información.



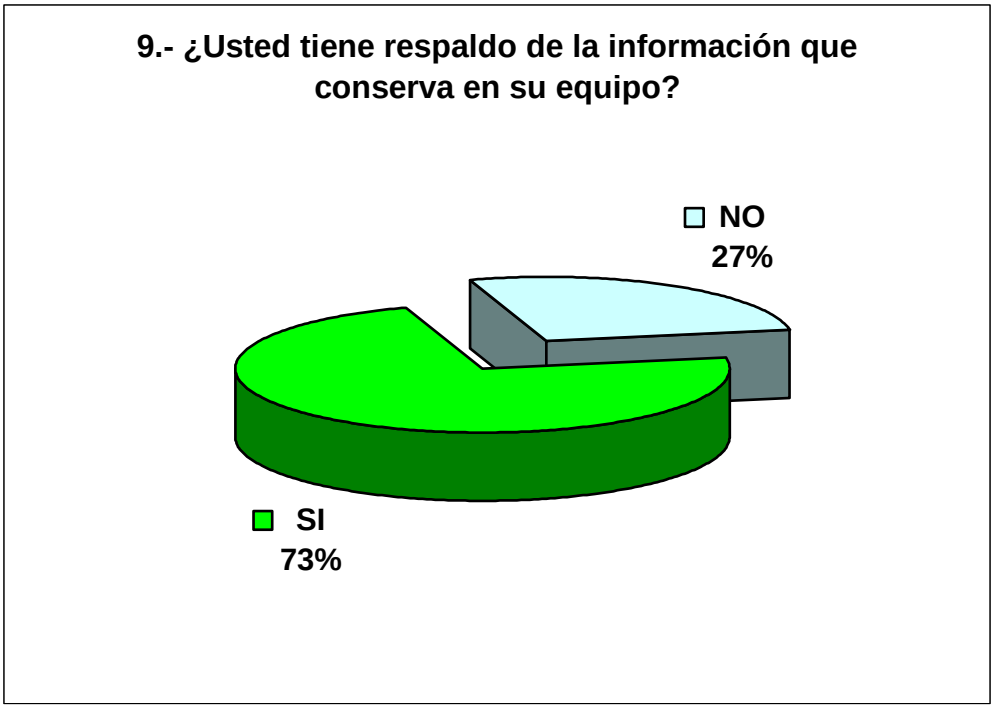
Usted tiene respaldo de la información que conserva en su equipo.

Respuesta	No. De encuestados	Porcentaje
SI	8	73%
NO	3	27%
TOTAL	**11**	**100%**

El 73% de las personas encuestadas del Instituto Tecnológico Superior de la Policía Nacional, afirman que si tienen respaldo de la información que conserva en su equipo.

El 36% de las personas encuestadas del Instituto Tecnológico Superior de la Policía Nacional, respondieron negativamente sobre la pregunta realizada en cuanto si tienen respaldo de la información que conserva en su equipo.

Se determina que el 73% de las personas encuestadas afirman tener respaldo de la información que conservan el su equipo en: CD, Disketts, correo electrónico, fhas memory y archivos manuales, mientras que el 27% de las personas encuestadas no poseen respaldo de la información que conservan el su equipo.



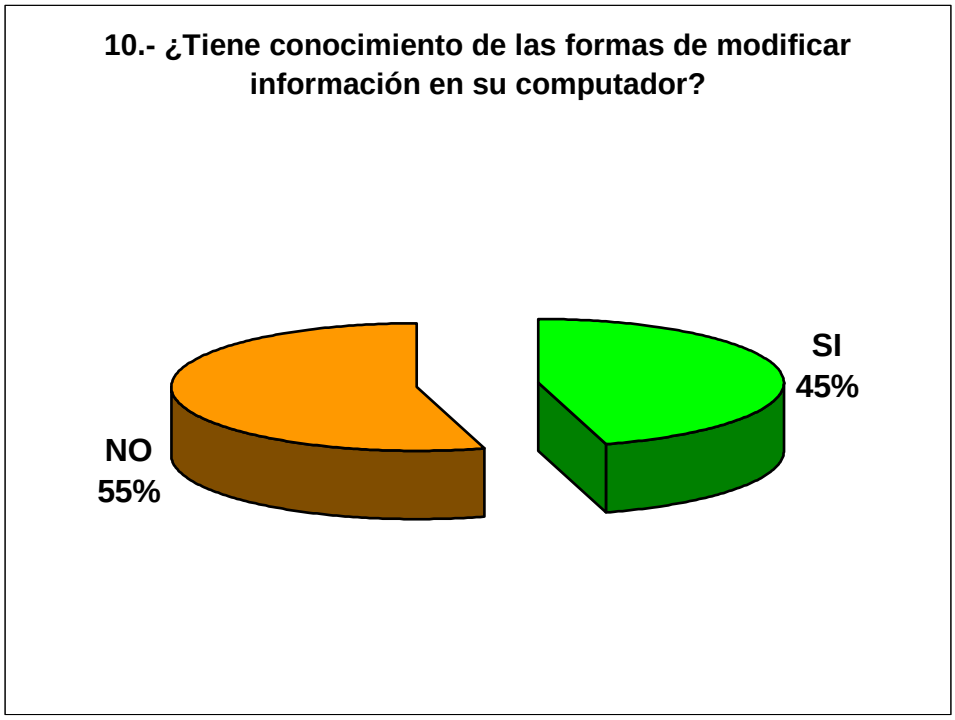
Tiene conocimientos de las formas de modificar información en su computador.

Respuesta	No. De encuestados	Porcentaje
SI	5	45%
NO	6	55%
TOTAL	**11**	**100%**

El 45% de las personas encuestadas del Instituto Tecnológico Superior de la Policía Nacional, afirman que si tienen conocimientos de las formas de modificar información en su computador.

El 55% de las personas encuestadas del Instituto Tecnológico Superior de la Policía Nacional respondieron negativamente sobre la pregunta realizada en cuanto considera conocer las formas de modificar información en su computador.

Se deduce que el 45% de las personas encuestadas afirman conocer las formas de modificar la información, mientras que el 55% desconoce de las formas de modificar la información en un computador.



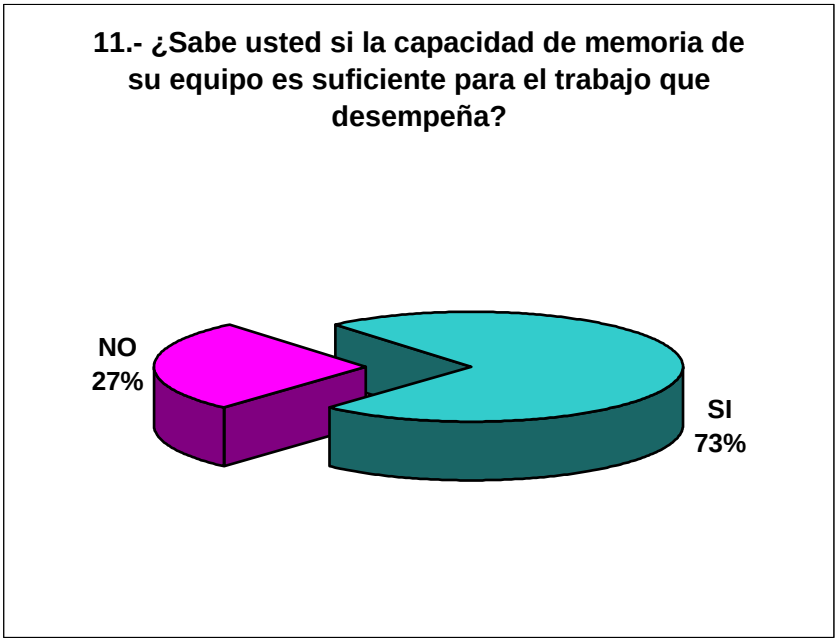
Sabe usted si la capacidad de memoria de su equipo es suficiente para el trabajo que desempeña.

Respuesta	No. De encuestados	Porcentaje
SI	8	73%
NO	3	27%
TOTAL	**11**	**100%**

El 73% de las personas encuestadas del Instituto Tecnológico Superior de la Policía Nacional, afirma conocer que saben la capacidad de memoria de su equipo es suficiente para el trabajo que desempeña.

El 27% de las personas encuestadas del Instituto Tecnológico Superior de la Policía Nacional, respondieron negativamente sobre la pregunta realizada en cuanto si la capacidad de memoria de su equipo es suficiente para el trabajo que desempeña

Se concluye que el 73% de las personas encuestadas afirman conocer que su equipo tiene suficiente capacidad para el trabajo que desempeñan por que han revisado en del disco duro y se han molestado en preguntar a una persona que sepa, mientras que el 27% de las personas encuestados desconocen si su equipo tiene suficiente capacidad debido a que desconocen como verifica si la capacidad es suficiente.



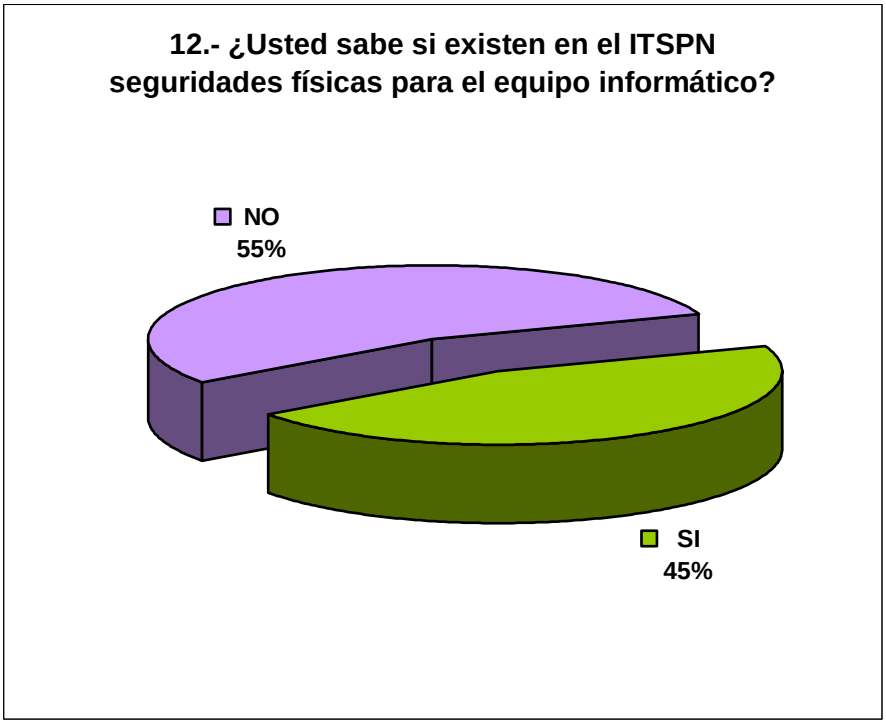
Usted sabe si existen en el ITSPN seguridades físicas para el equipo informático

Respuesta	No. De encuestados	Porcentaje
SI	5	45%
NO	6	55%
TOTAL	**11**	**100%**

El 45% de las personas encuestadas del Instituto Tecnológico Superior de la Policía Nacional, afirman conocer que existen seguridades físicas para el equipo informático.

El 55% de las personas encuestadas del Instituto Tecnológico Superior de la Policía Nacional, respondieron negativamente sobre la pregunta realizada en cuanto no existen seguridades físicas para el equipo informático.

Se deduce que el 55% de las personas encuestadas afirman conocer que no existen seguridades físicas para el equipo informático debido a que no existen seguridades en las puertas y cerramientos del establecimiento, mientras que el 45% de las personas encuestadas afirman conocer que si existen seguridades físicas para los equipos informáticos.



Conoce si el equipo a su cargo posee sus dispositivos en buen estado

Respuestas	SI	NO	No. De encuestados	Porcentaje SI	Porcentaje NO	TOTAL
CDRom	9	2	11	82%	18%	100%
Diskettera	8	3	11	73%	27%	100%
Impresora	6	5	11	55%	45%	100%
Scanner	1	10	11	9%	91%	100%
Protector de pantalla	7	4	11	64%	36%	100%

El 82% de personas encuestadas del Instituto Tecnológico Superior de la Policía Nacional, afirman conocer que los CDRom se encuentran en buen estado, mientras que el 18% de las personas encuestas del Instituto Tecnológico Superior de la Policía Nacional, manifiestan conocer que el CDRon se encuentra en mal estado

El 73% de las personas encuestadas del Instituto Tecnológico Superior de la Policía Nacional, afirman conocer que las Disketteras se encuentran en buen estado, mientras que el 27% de las personas encuestas del Instituto Tecnológico Superior de la Policía Nacional, manifiestan conocer que las Disketteras están en mal estado.

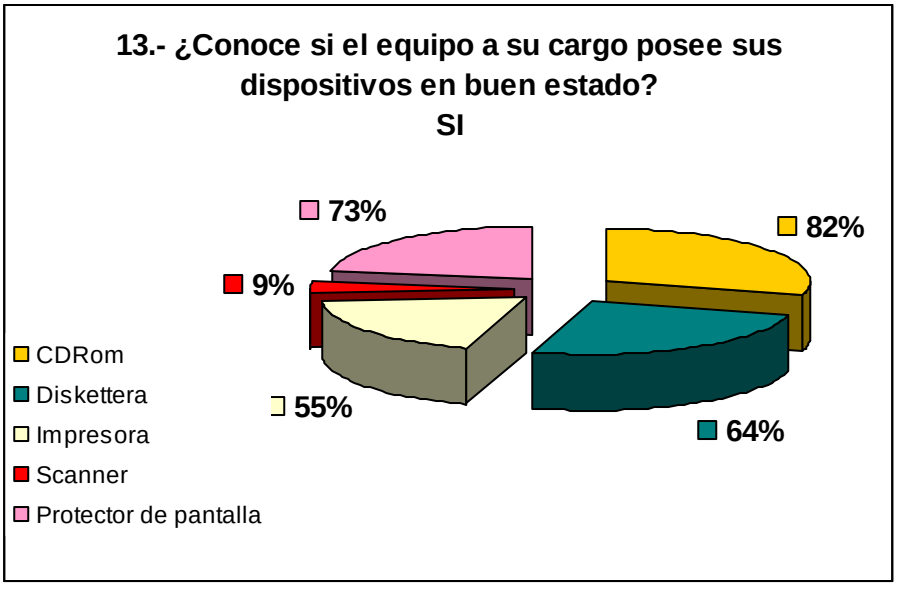
El 55% de personas encuestadas del Instituto Tecnológico Superior de la Policía Nacional, afirman conocer que las impresoras se encuentran en buen estado, mientras que el 45% de las personas encuestadas del Instituto Tecnológico Superior de la Policía Nacional, manifiestan conocer que las impresoras se encuentran en mal estado.

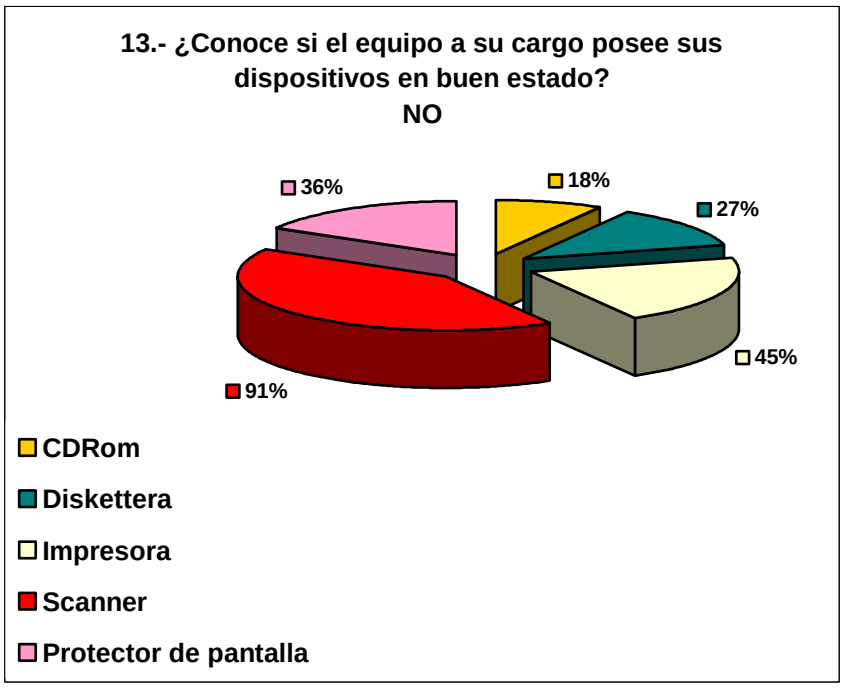
El 9% de personas encuestadas del Instituto Tecnológico Superior de la Policía Nacional, afirman conocer que los Scanner se encuentran en buen estado, mientras

que el 91% de las personas encuestadas del Instituto Tecnológico Superior de la Policía Nacional, manifiestan conocer que lo Scanner se encuentran en mal estado

El 64% de personas encuestadas del Instituto Tecnológico Superior de la Policía Nacional, afirman conocer que los protectores de pantalla se encuentran en buen estado, mientras que 36% de las personas encuestadas del Instituto Tecnológico Superior de la Policía Nacional, manifiestan conocer que los protectores de pantalla se encuentran en mal estado.

Se determina que existe un mayor porcentaje que advierte que los dispositivos de los computadores se encuentran en buen estado como son: CDRom 82%, Disketteras 73%, impresoras 55%, protector de pantalla 64%, mientras que los dispositivos de los computadores que no se encuentran en buen estado son los Scanner con un 9%.





Existe una persona a cargo del mantenimiento del sistema informático

Respuesta	No. De encuestados	Porcentaje
SI	5	45%
NO	6	55%
TOTAL	**11**	**100%**

El 45% de las personas encuestadas del Instituto Tecnológico Superior de la Policía Nacional, afirman conocer que existe una persona cargo del mantenimiento del sistema informático.

El 55% de las personas encuestadas del Instituto Tecnológico Superior de la Policía Nacional, respondieron negativamente sobre la pregunta realizada en cuanto al conocimiento de que existe una persona cargo del mantenimiento del sistema informático.

Se deduce que el 55% de las personas encuestadas manifiesta conocer que no existe una persona encargada del mantenimiento del sistema informático, mientras que el 45% de las personas encuestadas a firman conocer que si existe una persona encargada de dar mantenimiento al sistema informático que el Sr. Policía Robinsón Calle.

Los equipos cada que tiempo reciben mantenimiento

Respuesta	No. De encuestados	Porcentaje
Trimestralmente	0	0%
Semestralmente	3	27%
Anualmente	2	18%
Nunca	**6**	55%
TOTAL	**11**	**100%**

El 0% de las personas encuestadas del Instituto Tecnológico Superior de la Policía Nacional, respondieron negativamente sobre la pregunta realizada en cuanto al conocimiento que si trimestralmente reciben mantenimiento los equipos informáticos.

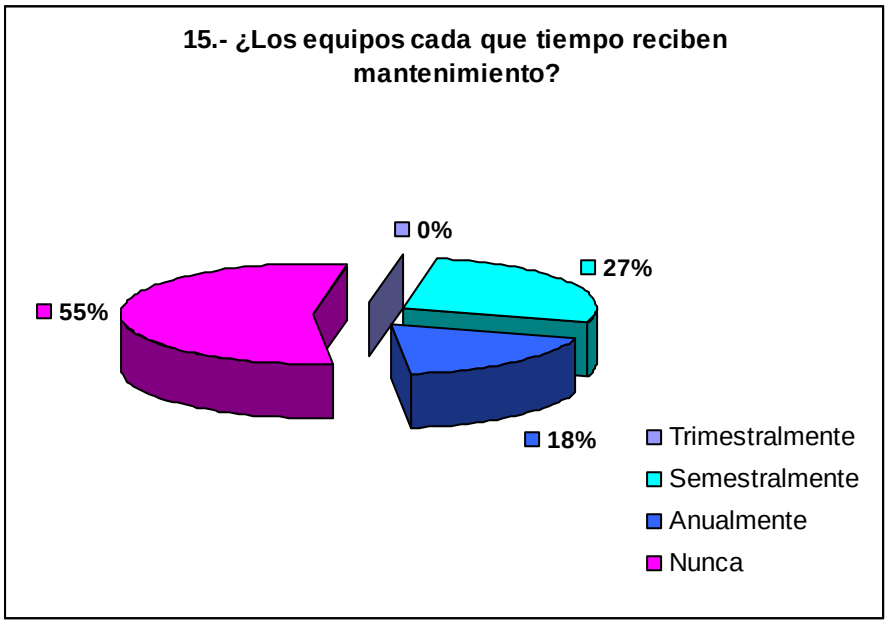
El 27% de las personas encuestadas del Instituto Tecnológico Superior de la Policía Nacional, afirman conocer que semestralmente reciben mantenimiento los equipos informáticos.

.

El 18% de las personas encuestadas del Instituto Tecnológico Superior de la Policía Nacional, afirman conocer que anualmente reciben mantenimiento los equipos informáticos.

El 55% de las personas encuestadas del Instituto Tecnológico Superior de la Policía Nacional, afirman conocer que nunca reciben mantenimiento los equipos informáticos.

Se concluye que el 55% de las personas encuestadas indican conocer que los equipos informáticos nunca han reciben mantenimiento, mientras que el 18% y 27% de las personas encuestadas afirman conocer que los equipos informáticos si reciben mantenimiento anualmente y semestralmente, además sobresale un 0% por Trimestralmente.



Usted presenta informes del trabajo que efectúa

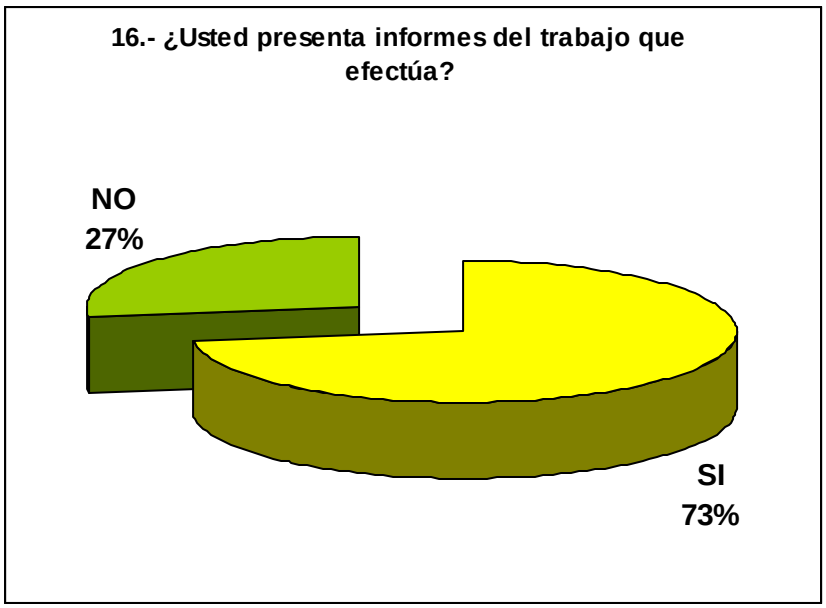
Respuesta	No. De encuestados	Porcentaje
SI	8	73%
NO	3	27%
TOTAL	**11**	**100%**

El 73% de las personas encuestadas del Instituto Tecnológico Superior de la Policía Nacional, afirman que presentan informes del trabajo que efectúan.

El 27% de las personas encuestadas del Instituto Tecnológico Superior de la Policía Nacional, respondieron negativamente sobre la pregunta realizada en cuanto si presentan informes del trabajo que efectúan.

Se determina que el 73% de las personas encuestadas señalan que si presentan informes del trabajo que efectúan semanalmente, mensualmente, trimestralmente o depende de cuando se terminen los trabajos encomendados, mientras que el 27% de

las personas encuestadas manifestaron que no presentan informes del trabajo que efectúan.



Existe ventilación en los lugares donde se encuentran los equipos informáticos

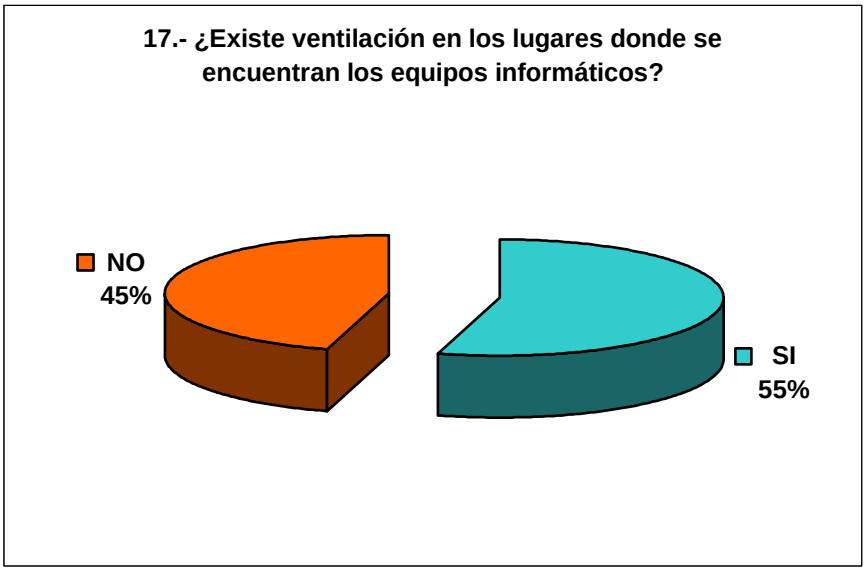
Respuesta	No. De encuestados	Porcentaje
SI	6	55%
NO	5	45%
TOTAL	**11**	**100%**

El 55% de las personas encuestadas del Instituto Tecnológico Superior de la Policía Nacional, afirman conocer que existe ventilación en los lugares donde se encuentran los equipos informáticos.

El 45% de las personas encuestadas del Instituto Tecnológico Superior de la Policía Nacional, respondieron negativamente sobre la pregunta realizada en cuanto al

conocimiento de que existe ventilación en los lugares donde se encuentran los equipos informáticos.

Se deduce que el 55% de las personas encuestadas sostienen conocer que si existe ventilación en los lugares donde se encuentran los equipos informáticos, mientras que el 45% de las personas encuestadas manifiestan conocer que no existe ventilación en los lugares donde se encuentran los equipos informáticos.



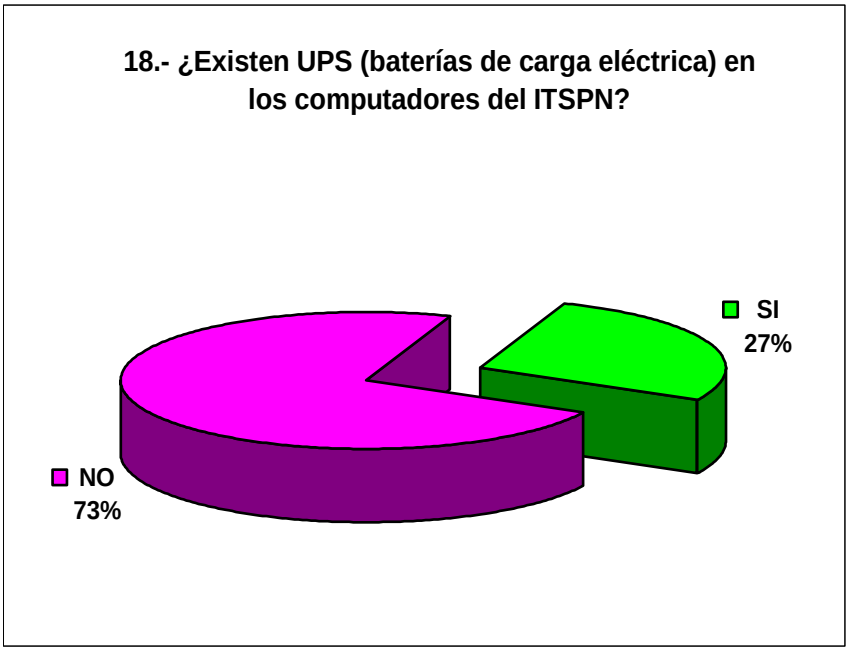
Existen UPS (baterías de carga eléctrica) en los computadores del ITSPN

Respuesta	No. De encuestados	Porcentaje
SI	3	27%
NO	8	73%
TOTAL	**11**	**100%**

El 27% de las personas encuestadas del Instituto Tecnológico Superior de la Policía Nacional, afirman conocer que existen UPS en los computadores del ITSPN.

El 73% de las personas encuestadas del Instituto Tecnológico Superior de la Policía Nacional, respondieron negativamente sobre la pregunta realizada en cuanto al conocimiento de que existen UPS en los computadores del ITSPN

Se determina que el 73% de las personas encuestadas testifican conocer que no existe UPS (baterías de carga eléctrica) en los computadores del ITSPN, mientras que un 27% de las personas encuestadas afirman conocer que si existe UPS en los computadores ITSPN.



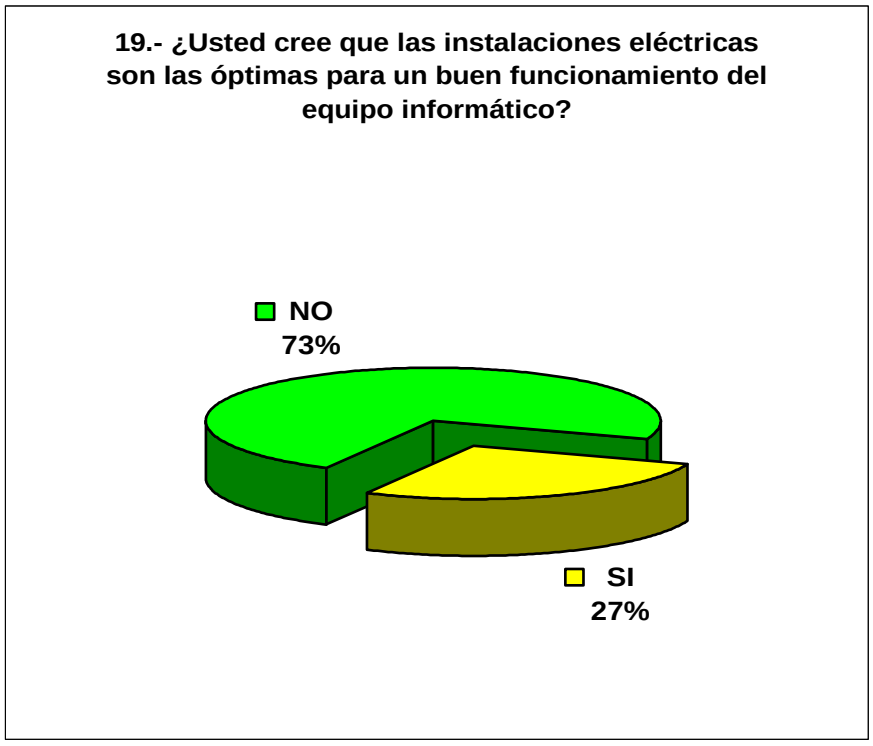
Usted cree que las instalaciones eléctricas son las óptimas para un buen funcionamiento del equipo informático

Respuesta	No. De encuestados	Porcentaje
SI	3	27%
NO	8	73%
TOTAL	**11**	**100%**

El 27% de las personas encuestadas del Instituto Tecnológico Superior de la Policía Nacional, afirman conocer que las instalaciones eléctricas son óptimas para un buen funcionamiento del equipo informático.

El 73% de las personas encuestadas del Instituto Tecnológico Superior de la Policía Nacional, respondieron negativamente sobre la pregunta realizada en cuanto al conocimiento que las instalaciones eléctricas son óptimas para un buen funcionamiento del equipo informático.

Se concluye que el 73% de las personas encuestadas afirman conocer que las instalaciones eléctricas del ITSPN no son óptimas para un buen funcionamiento de los equipos informáticos, mientras que un 27% de las personas encuestadas manifiestan conocer que las instalaciones eléctricas si son óptimas para el funcionamiento de los equipos informáticos.



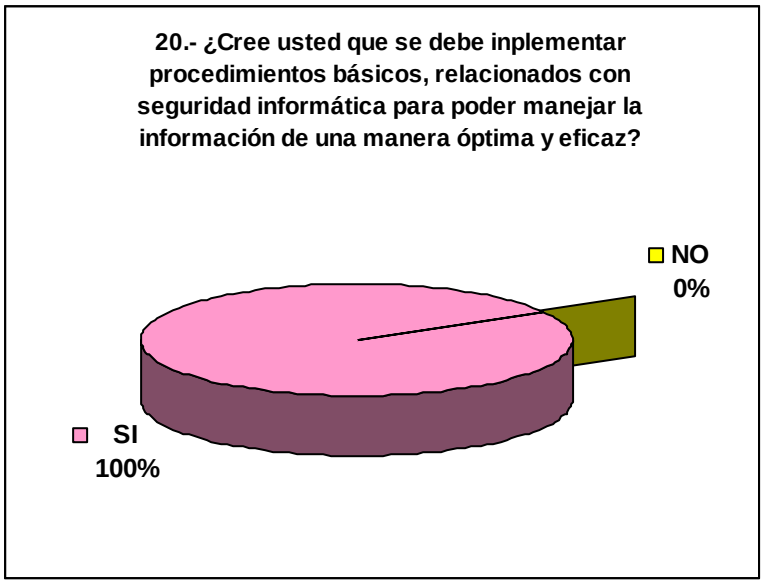
Cree usted que se debe implementar procedimientos básicos, relacionados con seguridad informática para poder manejar la información de una manera óptima y eficaz

Respuesta	No. De encuestados	Porcentaje
SI	11	100%
NO	0	0%
TOTAL	**11**	**100%**

El 100% de las personas encuestadas del Instituto Tecnológico Superior de la Policía Nacional, afirman que se debe implementar procedimientos básicos, relacionados con seguridad informática para poder manejar la información de una manera óptima y eficaz.

El 0% de las personas encuestadas del Instituto Tecnológico Superior de la Policía Nacional, respondieron negativamente sobre la pregunta realizada.

Se deduce que el 100% de los encuestados concuerda a favor de la implementación de procedimientos básicos, relacionados con seguridad informática, para de esta forma manejar la información de una manera óptima y eficaz



CAPITULO III

IMPLEMENTACIÓN DE SEGURIDAD LÓGICAS INFORMÁTICA PARA EL INSTITUTO TECNOLÓGICO SUPERIOR DE LA POLICÍA NACIONAL “ITSPN”

3.1 Introducción

Con la confianza de resolver los problemas de seguridad Informáticas, rápidamente en muchas Instituciones simplemente se compran uno o más productos de seguridad. En estos casos, a menudo se piensa que nuevos productos (ya sea en hardware, software, o servicios), es todo lo que se necesita. Luego que se instalan los productos, sin embargo, se genera una gran desilusión al darse cuenta que los resultados esperados no se han materializado. En un número grande de casos, esta situación puede atribuirse al hecho que no se ha creado una infraestructura organizativa adecuada para la seguridad informática.

3.2. Propósito

Los presentes fundamentos técnicos tienen como propósito fundamental determinar políticas y procedimientos para la seguridad informática de los equipos informáticos del ITSPN, a fin de que al ponerse en práctica estas políticas, se eviten riesgos innecesarios dentro del trabajo diario del ITSPN.

3.3. Responsabilidades

La seguridad Informática es responsabilidad de todos quienes conforman el ITSPN, el laboratorio de cómputo y todos los equipos informáticos de las diferentes

oficinas dependen completamente que cada empleado reconozca actos y condiciones que brinden poca seguridad.

Para este fin, se han delineado responsabilidades específicas para el comité de informática y/o encargado del equipo informático y los jefes de áreas y el resto de los empleados.

3.4. Comité de informática.

El Modelo del Comité de Seguridad Informática deberá estar compuesto por los representantes del ITSPN, un ejemplo seria por el Gerente de Informática, el Gerente de Telecomunicaciones (cuando exista), y el abogado o representante legal del ITSPN.

El comité de Informática es responsable de implantar y velar por el cumplimento de las políticas, normas, pautas, y procedimientos de seguridad en el ITSPN, También es responsable de evaluar, adquirir e implantar productos de seguridad informática, y realizar las demás actividades necesarias para garantizar un ambiente informático seguro. Además debe ocuparse de proporcionar apoyo técnico y administrativo en todos los asuntos relacionados con la seguridad, y en particular en los casos de infección de virus, penetración de hackers, fraudes y otros percances.

3.5. IMPLEMENTACIÓN DE SEGURIDADES INFORMÁTICAS

La implementación de seguridades informáticas en ITSPN son esencialmente orientaciones e instrucciones que indican cómo manejar los asuntos de seguridad y forman la base de un plan maestro para la implantación efectiva de medidas de protección tales como: identificación y control de acceso, respaldo de datos, planes de contingencia y detección de intrusos.

3.5.1. Comité de seguridad

- El comité de seguridad es el encargado de la seguridad informática es responsable de dirigir las investigaciones sobre incidentes y problemas relacionados con la seguridad, así como recomendar las medidas pertinentes.

3.5.2. Normas de Elección de Claves

Se debe tener en cuenta los siguientes consejos:

- No utilizar contraseñas que sean palabras (aunque sean extranjeras), o nombres (el del usuario, personajes de ficción, miembros de la familia, mascotas, marcas, ciudades, lugares, u otro relacionado).

- No usar contraseñas completamente numéricas con algún significado (teléfono, fecha de nacimiento, patente del automóvil, etc.).

- Elegir una contraseña que mezcle caracteres alfabéticos (mayúsculas y minúsculas) y numéricos.

- Deben ser largas, de 8 caracteres o más.

- Tener contraseñas diferentes en máquinas diferentes. Es posible usar una contraseña base y ciertas variaciones lógicas de la misma para distintas máquinas.

- Deben ser fáciles de recordar para no verse obligado a escribirlas. Algunos ejemplos son: Combinar palabras cortas con algún número o carácter de puntuación: (soy2_yo3),

- Usar un acrónimo de alguna frase fácil de recordar: (A r io R evuelto G anancia d e P escadores -> ArRGdP).

- Añadir un número al acrónimo para mayor seguridad: (A9r7R5G3d1P).

- Mejor incluso si la frase no es conocida: (H a sta A h ora n o h e O l vidado m i C o ntraseña -> aHoelIo)

- Elegir una palabra sin sentido, aunque pronunciable: (taChunda72, AtajulH, Wen2Mar).

- Realizar reemplazos de letras por signos o números: (E n S eguridad M ás V ale P revenir q ue C urar -> 35M\/Pq<)

3.5.3. Normas para Proteger una Clave

- Un password debe ser como un cepillo de dientes. Úsalo cada día; cámbialo regularmente; y NO lo compartas con tus amigos

Algunos consejos a seguir:

- No permitir ninguna cuenta sin contraseña. Si se es administrador del sistema, repasar este hecho periódicamente.

- Nunca compartir con nadie la contraseña. Si se lo hace, cambiarla inmediatamente.

- No escribir la contraseña en ningún sitio. Si se escribe, no debe identificarse como tal y no debe identificarse al propietario en el mismo lugar.

- No teclear la contraseña si hay alguien mirando. Es una norma tácita de buen usuario no mirar el teclado mientras alguien teclea su contraseña.

- No enviar la contraseña por correo electrónico ni mencionarla en una conversación. Si se debe mencionar no hacerlo explícitamente diciendo: "mi clave es...".

- No mantener una contraseña indefinidamente. Cambiarla regularmente. Disponer de una lista de contraseñas que puedan usarse cíclicamente (por lo menos 5).

- Muchos sistemas incorporan ya algunas medidas de gestión y protección de las contraseñas. Entre ellas podemos citar las siguientes: Número de intentos limitado. Tras un número de intentos fallidos, pueden tomarse distintas medidas: Obligar a rescribir el nombre de usuario (lo más común). Bloquear el acceso durante un tiempo. Enviar un mensaje al administrador y/o mantener un registro especial. Longitud mínima. Las contraseñas deben tener un número mínimo de caracteres (se recomienda 7 u 8 como mínimo).

- Restricciones de formato. Las contraseñas deben combinar un mínimo de letras y números, no pueden contener el nombre del usuario ni ser un blanco.

- Envejecimiento y expiración de contraseñas. Cada cierto tiempo se fuerza a cambiar la contraseña. Se obliga a no repetir cierta cantidad de la anterior. Se mantiene un periodo forzoso entre cambios, para evitar que se vuelva a cambiar inmediatamente y se repita la anterior.

- Ataque preventivo. Muchos administradores utilizan crackeadores para intentar atacar las contraseñas de su propio sistema en busca de debilidades.

3.5.4. Para los Empleados del ITSPN

- Se comprometerán a estar atentos a las condiciones de seguridad Informática del los equipos, centro o laboratorio de cómputo.

- Reportaran todos los accidentes, incidentes, actos y condiciones poco seguras a su jefe inmediato o comité de informática.

- Deberán cumplir con las reglas y procedimientos de seguridad establecidos para este fin.

- Los empleados del ITSPN son responsables de cumplir con todas las políticas de la instituto relativas a la seguridad informática y en particular:

- Conocer y aplicar las seguridades y procedimientos apropiados en relación al manejo de la información y de los sistemas informáticos.

- No divulgar información confidencial del ITSPN a personas no autorizadas.

- No permitir y no facilitar el uso de los sistemas informáticos del ISTPN a personas no autorizadas.

- No utilizar los recursos informáticos (hardware, software o datos) y de telecomunicaciones (teléfono, fax) para otras actividades que no estén directamente relacionadas con el trabajo ITSPN.

- Proteger meticulosamente su contraseña y evitar que sea vista por otros en forma inadvertida.

- Seleccionar una contraseña robusta que no tenga relación obvia con el usuario, sus familiares, el grupo de trabajo, y otras asociaciones parecidas.

- Reportar inmediatamente al comité de Seguridad Informática cualquier evento que pueda comprometer la seguridad del ITSPN y sus recursos informáticos, como por ejemplo contagio de virus, intrusos, modificación o pérdida de datos y otras actividades poco usuales.

- Los empleados del ITSPN no deberán Introducir alimentos, bebidas o fumar dentro del laboratorio de cómputo.

- No deben instalar programas y/o archivos ajenos al ITSPN sin autorización.

3.5.5. Sobre el Uso de Internet.

- El uso de Internet estará a disposición de los empleados del ITSPN de los Laboratorios de Cómputo; con los lineamientos definidos en las políticas de la institución.

- El servicio de Internet que se presta en el ITSPN es estrictamente académico u oficial, por lo se debería prohibirse con fines comerciales, lucrativos y entretenimiento.

4.5.6. Políticas de seguridades para los computadores

- Los computadores del ITSPN sólo deben usarse en un ambiente seguro. Se considera que un ambiente es seguro cuando se han implantado las medidas de control apropiadas para proteger el software, el hardware y los datos. Esas medidas deben estar acordes a la importancia de los datos y la naturaleza de riesgos previsibles.

- Los equipos del ITSPN sólo deben usarse para actividades de trabajo y no para otros fines, tales como juegos y pasatiempos.

- Debe respetarse y no modificar la configuración de hardware y software establecida por el Departamento de Informática.

- No se permite fumar, comer o beber mientras se está usando un PC.

- No se permite que el lugar de trabajo se encuentre en desorden.

- Deben protegerse los equipos de riesgos del medioambiente (por ejemplo, polvo, incendio y agua).

- Deben usarse protectores contra transitorios de energía eléctrica y en los servidores deben usarse fuentes de poder interrumpibles (UPS).

- Cualquier falla en los computadores o en la red debe reportarse inmediatamente ya que podría causar problemas serios como pérdida de la información o indisponibilidad de los servicios.

- Deben protegerse los equipos para disminuir el riesgo de robo, destrucción, y mal uso. (Las medidas que se recomiendan incluyen el uso de vigilancia y cerradura con llave).

- Los equipos deben marcarse para su identificación y control de inventario. Los registros de inventario deben mantenerse actualizados.

- No pueden moverse los equipos o reubicarlos sin permiso. Para llevar un equipo fuera del ITSPN se debe requerir una autorización escrita.

- La pérdida o robo de cualquier componente de hardware o programa de software debe ser reportada inmediatamente.

- Para prevenir el acceso no autorizado, los usuarios deben usar un sistema de contraseñas robusto.

- Deben configurar el protector de pantalla para que se active al cabo de 15 minutos de inactividad y que requiera una contraseña al reasumir la actividad. Además el usuario debe activar el protector de pantalla manualmente cada vez que se ausente de su oficina.

- Si un PC tiene acceso a datos confidenciales, debe poseer un mecanismo de control de acceso especial, preferiblemente por hardware.

- Los datos confidenciales que aparezcan en la pantalla deben protegerse de ser vistos por otras personas mediante disposición apropiada del mobiliario de la oficina y protector de pantalla. Cuando ya no se necesiten o no sean de utilidad, los datos confidenciales se deben borrar.

- Debe implantarse un sistema de autorización y control de acceso con el fin de restringir la posibilidad de los usuarios para leer, escribir, modificar, crear, o borrar datos importantes. Estos privilegios deben definirse de una manera consistente con las funciones que desempeña cada usuario.

- No se deberá permitir llevar al ITSPN computadores portátiles (laptops) a los empleados que desempeñan funciones administrativas y en caso de ser necesario se requiere solicitar la autorización correspondiente.

- Los empleados no deben copiar a un medio removible (como un diskette, memory, CD), el software o los datos residentes en las computadoras del ITSPN, sin la aprobación previa del encargado.

- No pueden del ITSPN extraerse datos sin la aprobación previa de la gerencia del instituto.

4.4.7. Sobre Antivirus

- Debe instalarse y activarse una herramienta antivirus, la cual debe mantenerse actualizada. Si se detecta la presencia de un virus u otro agente potencialmente peligroso, se debe notificar inmediatamente al Jefe de Seguridad Informática y poner la PC en cuarentena hasta que el problema sea resuelto.

- No deben usarse diskettes u otros medios de almacenamiento en cualquier computadora del ITSPN a menos que se haya previamente verificado que están libres de virus u otros agentes dañinos

- Para ayudar a restaurar los programas originales no dañados o infectados, deben hacerse copias de todo software nuevo antes de su uso, y deben guardarse tales copias en un lugar seguro, como son: entidades bancarias si la información fuese demasiada importante o en un lugar apartado de las instalaciones del ITSPN que se han seguras.

4.4.8. Seguridad de la información de los PC del ITSPN

- Periódicamente debe hacerse el respaldo de los datos guardados en PC y servidores del ITSPN y las copias de respaldo deben guardarse en un lugar seguro, a prueba de hurto, incendio e inundaciones. Los programas y datos vitales para la operación del ITSPN deben guardarse en otra sede, lejos del edificio.

- Los usuarios de PC son responsables de proteger los programas y datos contra pérdida o daño. El Administrador de cada uno de esos sistemas es responsable de hacer copias de respaldo periódicas. Los gerentes de los distintos departamentos son responsables de definir qué información debe respaldarse, así como la frecuencia del respaldo (por ejemplo: diario, semanal) y el método de respaldo (por ejemplo: incremental, total).

- La información del ITSPN clasificada como confidencial o de uso restringido, debe guardarse y transmitirse en forma cifrada, utilizando herramientas de encriptado robustas y que hayan sido aprobadas por la Gerencia de Informática.

- No debe borrarse la información original no cifrada hasta que se haya comprobado que se puede recuperar desde los archivos encriptados mediante el proceso de descifrado.

- El acceso a las claves utilizadas para el cifrado y descifrado debe limitarse estrictamente a las personas autorizadas y en ningún caso deben revelarse a consultores, contratistas y personal temporal.

4.4.9. Sobre energía eléctrica

- Se deberán utilizar canaletas en caso de que existieren cables sueltos en las instalaciones del ITSPN para un buen orden de los mismos.

- Se deben asegurar que los cables eléctricos y las cajas de empalme estén levantados del piso.

- Los cables eléctricos, cajas de empalme, switches, toma de energía eléctrica y paneles estén localizados fuera del alcance de derrames potenciales de líquidos.

- Se debe asegurar que todos los circuitos estén conectados a una tierra común y de que haya suficientes circuitos para que ninguno se sobrecargue.

- Se deberá procurar que las cajas de interruptores de energía eléctrica estén accesibles fácilmente e instalados cerca de la entrada al centro o laboratorio de computo o salidas del edificio.

4.4.10. Sobre iluminación

- Se aseguraran que haya iluminación adecuada para prevenir esfuerzo innecesario de la vista de los empleados del ITSPN,

4.4.11. Mantenimientos a los equipos informáticos

- Se deberá dar al equipo informático mantenimiento preventivo y correctivo para un buen funcionamiento de los mismos.

- El comité de seguridad informática deberá definir el tiempo correspondiente para el mantenimiento a los equipos informáticos.

- Los empleados que tenga a su cargo un equipo de informática estarán en la obligación de comunicar al comité de informática o encargado, de cualquier imperfección o fallo en su equipo inmediatamente.

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES (página sola sin numeración)

Del presente trabajo de investigación presentamos las siguientes conclusiones:

1 De las encuestas realizadas se llegó a determinar que la mayor parte del personal que labora en el Instituto Tecnológico Superior de la Policía Nacional de Quito, manifiesta que el manejo de la información es inestable.

2 Los empleados que laboran en Instituto Tecnológico Superior de la Policía Nacional no han recibido capacitación para un buen manejo de la información.

3 Un alto porcentaje del personal que labora en el área administrativa del Instituto Tecnológico Superior de la Policía Nacional tienen acceso a los computadores de las distintas oficinas.

4 Existe en el Instituto Tecnológico Superior de la Policía Nacional un alto porcentaje de perdida de información a causa de apagones y virus informáticos.

5 No existen en las instalaciones del Instituto Tecnológico Superior de la Policía Nacional seguridades físicas para los equipos informáticos.

6 En el Instituto Tecnológico Superior de la Policía Nacional, no existe una persona encargada de dar mantenimiento al sistema informático.

7 Existe carencia en el Instituto Tecnológico Superior de la Policía Nacional de UPS (baterías de carga eléctrica) para los equipos informáticos y las instalaciones eléctricas no son óptimas para el funcionamiento.

8 El Instituto Tecnológico Superior de la Policía Nacional, carece de procedimientos básicos relacionados con seguridad informática, para el manejo de la información.

RECOMENDACIONES

En base a experiencias profesionales propias y las conclusiones establecidas en el presente trabajo recomendamos las siguientes acciones a realizar:

1 Se recomienda la implantación de procedimientos, políticas de seguridad informática para cuidar de la información, existente en el equipo informático del Instituto Tecnológico Superior de la Policía Nacional.

2 Se recomienda que se cree en el Instituto Tecnológico Superior de la Policía Nacional un Comité de seguridad informática.

3 Se sugiere una permanente capacitación a los empleados del Instituto Tecnología Superior de la Policía Nacional en cuanto al manejo de la información y seguridades informáticas.

4 Se aconseja solicitar a quien corresponda la contratación de un profesional en informática, para que se encuentre pendiente de los equipos informático y planifique un mantenimiento continuo de las mismas.

5 Se sugiere que se realice las adquisiciones de UPS (baterías de carga eléctrica) para todos los computadores del Instituto Tecnológico Superior de la Policía Nacional

6 Se recomienda que se realicen correcciones y mantenimientos periódicos del sistema eléctrico del Instituto Tecnológico Superior de la Policía Nacional

7 Se aconseja mejorar las seguridades físicas, de los sitios donde se encuentren los equipos informáticos, dentro del Instituto Tecnológico Superior de la Policía Nacional

GLOSARIO (sin numeración de página)

EQUIPO INFORMÁTICO.- Es una máquina capaz de realizar cualquier trabajo que necesite manejar gran cantidad de datos a altas velocidades y con absoluta precisión.

SEGURIDAD INFORMÁTICA.-Son técnicas desarrolladas para proteger los equipos informáticos individuales y conectados en una red frente a daños accidentales o intencionales, estos daños incluyen el mal funcionamiento del hardware, la perdida física de datos y el acceso a los datos por personas autorizadas.

CRIPTOGRAFIA.- La palabra Criptografía proviene etimológicamente del griego Kruiptoz (Kriptos-Oculto) y Grajein (Grafo-Escritura) y significa "arte de escribir con clave secreta o de un modo enigmático" (**).

ENCRIPTADO.-Término en Ingles: Encryption, Es un proceso de cifrado de las con unificaciones que tiene como finalidad que no puedan ser interceptadas. Las personas pueden desencriptar y leer el mensaje solo si poseen la clave adecuada.

FIRWALL.- Es un sistema capaz de separar el habitáculo de nuestra red, o sea, el área interna de la misma, del posible incendio de crakers.

ARCHIVO.- Nombre que se le da a la información en el computador.

HARDWARE.- Son todos los componentes físicos y tangibles (la computadora)

SOFTWARE.-Son todos los componentes lógicos e intangibles (los programas)

FCIC.- fuerzas policiales en cuanto a delitos informáticos, y el primer organismo establecido en el nivel nacional.

SEGURIDAD FÍSICA.- Se puede decir que la seguridad física surge como respuesta a los problemas físicos de la seguridad informática y se refiere a cualquier peligro que

puede ser causado por agentes externos al sistema (fuego, inundación, sobre cargar eléctrica)

SEGURIDAD LÓGICA.- Surge como respuesta a los problemas lógicos que conllevan una serie de aspectos mas amplios, por su complejidad e identificación. Estos pueden ir desde la recuperación del sistema tras un problema hasta proteger el acceso al sistema frente aun usuario no deseado.

SISTEMAS INFORMATICOS.- Es el conjunto de medios informáticos destinados a asegurar la ejecución de operaciones administrativas o científicas o ambas.

IDENTIFICACIÓN.- Se denomina identificación al momento en el que el usuario se da a conocer el sistema.

AUTENTICACIÓN.-Se de nomina a la verificación que realiza el sistema sobre esta identificación.

PASSWORDS.- Clave de acceso o contraseña necesaria para acceder a un determinado sistema.

VIRUS INFORMÁTICO.- Un virus es un programa creado por un programador informático.

ANTIVIRUS.- Son programas que están diseñados para actuar contra un grupo especifico de virus.

PROGRAMACIÓN.- Es un lenguaje de informático de alto nivel (como pascal).

PERIFERICOS.- Son dispositivos que complementan las funciones de una con pujadora son: impresora, cámara, jostick. Etc.

CARPETA.-Término en Ingles: Fólder. Es un área donde UD. almacena materiales similares para ubicarlos luego más fácilmente.

UPS.-Baterías de carga eléctrica.

SUBREPTICIO.- oculto

BIBLIOGRAFÍA

http:www.monografias.com/trabajos11/tranas/trans/shtm/
http:www.segu-info.com.ar/delitos/información y delitos.
http:www.segu-info.com
http:www.egu-info.com.ar/tiposdelitos.htm
http:www.ilustraddos.com/publicaciones
http:www.colpos.mx/comino/nsegurid.exe
CETTICO, Enciclopedia de informática y computación.