



**FACULTAD DE INGENIERÍA
ESCUELA ACADÉMICA PROFESIONAL
DE INGENIERÍA DE SISTEMAS E INFORMÁTICA**

Plan de seguridad informática en la Escuela Universitaria de Posgrado
de la Universidad Nacional Federico Villarreal

**TESIS PARA OPTAR AL TÍTULO PROFESIONAL
DE INGENIERO DE SISTEMAS E INFORMÁTICA**

Presentada por
Br. Liñán Salinas, Efraín

Asesor
Mg. Manuel Alcántara Ramírez

Lima-Perú
2008



DEDICATORIA

A Dios, por darme vida y salud.

A mis padres, por hacer de mí lo que soy, y ahora mi padre me reluce desde el cielo. Gracias, papá.

A mis hermanos, por confiar y creer en mí: gracias a ellos tengo ahora un horizonte diferente.

A Gisela, por su apoyo incondicional en este largo camino.

A mis amigos (los que estuvieron y los que están), por hacer, de lo que soy, algo mejor.

Efraín Liñán Salinas

ÍNDICE

I. Marco teórico	13
1.1. Seguridad informática	13
1.1.1. Antecedentes de seguridad informática	16
1.1.2. Debilidades de los sistemas informáticos	17
1.1.3. Vulnerabilidad de la información	20
1.2. Delitos informáticos	21
1.2.1. Legislación nacional sobre los delitos informáticos	22
1.2.2. Delincuentes informáticos	25
1.3. Plan de seguridad informática	27
1.3.1. Plan de contingencia	29
1.3.2. Políticas de seguridad informática	32
1.4. Auditoría de sistemas	38
1.4.1. Objetivos de la auditoría de sistemas	39
1.4.2. Controles de la auditoría	39
1.5. Estándares y normas de seguridad	41
II. Descripción de la metodología del desarrollo	48
2.1. El problema de la investigación	48
2.2. Objetivos de la investigación	49
2.3. Tipo y diseño de la investigación	49
2.4. Metodología de desarrollo de la investigación	50
2.5. Hipótesis de la investigación	50

2.6.	Variables de estudio	51
2.7.	Población y muestra	52
2.8.	Técnicas estadísticas	53
2.9.	Instrumentos utilizados	54
III.	Plan de seguridad informática en la EUPG-UNFV	57
3.1.	Análisis de situación actual de la seguridad informática	57
3.1.1.	Seguridad lógica	60
3.1.2.	Seguridad en las comunicaciones	64
3.1.3.	Seguridad en las aplicaciones	69
3.1.4.	Seguridad física	72
3.1.5.	Administración del centro de procesamiento de datos	75
3.1.6.	Auditorías y revisiones	80
3.1.7.	Plan de contingencia	82
3.2.	Plan de seguridad informática propuesto	86
3.2.1.	Seguridad lógica	89
3.2.2.	Seguridad en las comunicaciones	93
3.2.3.	Seguridad en las aplicaciones	97
3.2.4.	Seguridad física	102
3.2.5.	Administración del centro de procesamiento de datos	106
3.2.6.	Auditorías y revisiones	109
3.2.7.	Plan de contingencia	114
3.3.	Roles y responsabilidades en cuanto a seguridad informática	118
3.3.1.	Área de informática	118
3.3.2.	Custodio de la información	119
3.3.3.	Usuarios	120
3.3.4.	Propietarios de la información	120
3.3.5.	Auditoría interna	121
3.3.6.	Área de seguridad informática propuesto	121

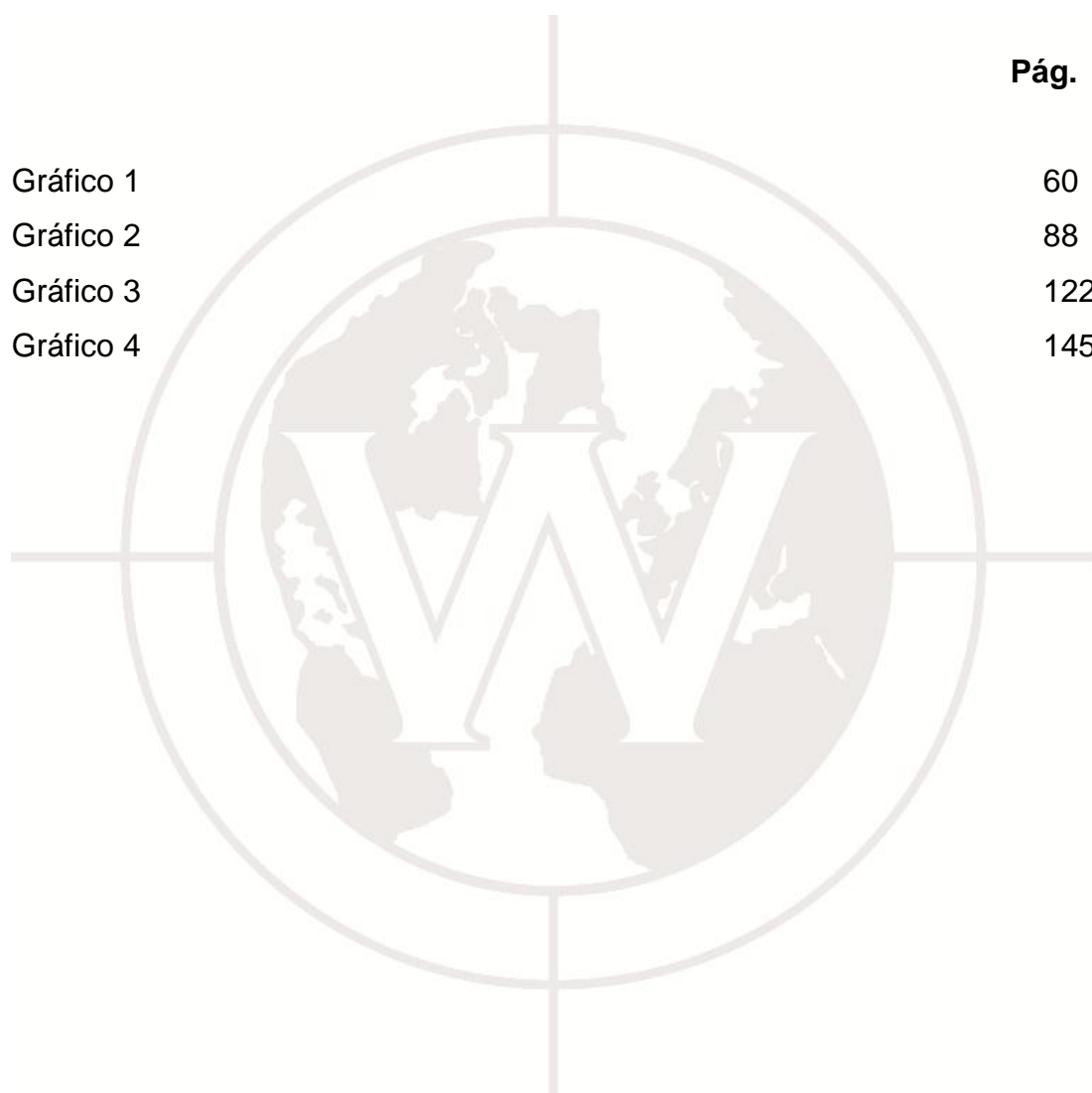
IV. Resultados de la investigación	
4.1. Diagnóstico de la seguridad informática antes de la formulación del plan	124
4.1.1. Evaluación de seguridad informática por factores	124
4.2. Análisis de la eficiencia del plan de seguridad informática propuesto	131
4.2.1. Evaluación del plan de seguridad informática por factores	131
4.3. Prueba sobre la eficiencia del plan de seguridad informática propuesto	141
4.3.1. Prueba o contraste de hipótesis	141
V. Discusión	146
VI. Conclusiones y recomendaciones	148
6.1. Conclusiones	148
6.2. Recomendaciones	149
Referencias bibliográficas	150
Anexos	154

ÍNDICE DE CUADROS

	Pág.
Cuadro 1	19
Cuadro 2	51
Cuadro 3	54
Cuadro 4	55
Cuadro 5	56
Cuadro 6	125
Cuadro 7	126
Cuadro 8	127
Cuadro 9	128
Cuadro 10	129
Cuadro 11	130
Cuadro 12	132
Cuadro 13	133
Cuadro 14	134
Cuadro 15	135
Cuadro 16	136
Cuadro 17	137
Cuadro 18	138
Cuadro 19	139
Cuadro 20	140
Cuadro 21	142
Cuadro 22	143
Cuadro 23	144

ÍNDICE DE GRÁFICOS

	Pág.
Gráfico 1	60
Gráfico 2	88
Gráfico 3	122
Gráfico 4	145



RESUMEN

La seguridad informática es un problema constante en todas las organizaciones públicas y privadas. Aunque algunas ya han tomado conciencia de esta problemática, muchas otras aún no participan de la cultura de la seguridad informática. Dentro de este segundo grupo de organizaciones se encuentra la Escuela Universitaria de Posgrado de la Universidad Nacional Federico Villarreal (EUPG-UNFV). Ello pone en serio peligro la información que gestiona y administra.

Es por este problema que se desarrolla la presente investigación, que contempla la formulación de un plan de seguridad informática que pruebe la eficiencia del mismo, mediante un estudio sobre la percepción de mejora en el tratamiento de seguridad de la información en la institución.

El desarrollo del trabajo se inicia con una encuesta, a modo de diagnóstico, acerca de la situación actual de la seguridad informática, mediante la cual se formula un plan, siguiendo los estándares de seguridad; luego de esta formulación, se aplica una segunda encuesta entre los expertos en informática, para probar la eficiencia del plan propuesto.

En base al análisis de la primera encuesta se logra diagnosticar la deficiencia de la seguridad informática existente en la EUPG-UNFV; y apoyándose en esta, se formula un plan, que comprende siete factores generales que se deben considerar para su estudio. Los resultados de la encuesta realizada a los expertos demuestran que el plan propuesto mejora la percepción en cuanto a la seguridad informática, y esta mejora evidencia la eficiencia del plan propuesto en la EUPG-UNFV.

Palabras claves: seguridad informática, amenazas informáticas, políticas de seguridad informática, plan de contingencia, vulnerabilidad de la información, eficiencia del plan.

ABSTRACT

Computer security is a constant problem in all public and private organizations, some have already become aware of this problem and many others still do not participate in the culture of computer security. Within this second type of organization is the University Graduate School of the National University Federico Villarreal (EUPG-UNFV), seriously endangering the information that manages constantly.

Motivated by this issue develops this investigation which includes the formulation of a plain of computer security that proves the efficiency of the same, through a study on the perceived improvement in the treatment of information security at the institution.

The development work began conducting a survey as a diagnosis about the current state of computer security, which formulates a plain to follow safety standards; after this formulation, applies a second survey among experts computer science, in order to test the efficiency of the proposed plain.

Based on the analysis of the first survey is done to diagnose the deficiency of computer security in the EUPG-UNFV, supported it, is formulated a plain that includes seven general factors to consider for study. The results of the survey show that the experts proposed plain improves the perception about computer security, and this improves the efficiency of evidence in the proposed plain EUPG-UNFV

Keywords: computer security, cyber threats, computer security policies, contingency plain, the vulnerability of information, efficiency of the plain.

INTRODUCCIÓN

Durante los últimos años, la era digital y las nuevas tecnologías de la información y comunicación dejan sentir su influencia en el medio peruano, a través del uso de Internet, del acceso a la supercarretera de la información, a la sofisticada tecnología de la computación, al comercio electrónico, a las transacciones bancarias y financieras, a la educación, a la multimedia. Se evidencia que para el Perú es importante el perfeccionamiento de las nuevas tecnologías de información.

Este crecimiento tecnológico implica gran debilidad de los sistemas informáticos, al volverse más complejos y sofisticados, apareciendo más elementos vulnerables relacionados con la seguridad de la información, lo que conlleva a la necesidad de una adecuada implementación de un plan de seguridad informática que permita a la institución proteger en forma correcta y oportuna su información.

En esta perspectiva, la Escuela de Posgrado de la Universidad Nacional Federico Villarreal ha ido creciendo a través del tiempo, disponiendo de recursos informáticos, una red local, acceso a Internet; por tanto, su información no deja de ser ajena a las amenazas informáticas, tanto externas como internas. He ahí la importancia y la trascendencia del estudio que motiva la presente tesis.

En la actualidad, dicha Escuela de Posgrado cuenta aproximadamente con 8000 estudiantes en diversas especialidades, que brindan los programas de maestría y doctorado. Definitivamente, desde un punto de vista informático, esto requiere de un celoso cuidado y de garantías de la información que se maneja.

Por lo expuesto, los responsables de la seguridad informática deben utilizar las herramientas adecuadas para diagnosticar los riesgos e identificar las amenazas informáticas a las cuales se ve expuesta la información de la EUPG-UNFV. En este contexto, se ve la necesidad de establecer un plan de seguridad informática que permita proteger y minimizar las vulnerabilidades de sus sistemas de información. Esta investigación se justifica por el crecimiento tecnológico que significa el aumento de la necesidad de salvaguardar, gestionar y controlar sus activos y todo aquello que le resulte clave para su desenvolvimiento eficiente.

La investigación se inicia realizando una encuesta a modo de diagnóstico acerca de la situación actual de la seguridad informática; se formula un plan de seguridad posible. Luego de esta formulación, se aplica una segunda encuesta entre los expertos en informática de la institución, mediante la que se prueba la eficiencia del plan propuesto.

La presente tesis se desarrolla en cuatro capítulos: el primero trata sobre el marco teórico, y contiene los fundamentos que sirven de base teórica al investigador para culminar con éxito la investigación.

El segundo capítulo expone propiamente la metodología de la investigación, y contiene la clasificación detallada de los componentes del estudio. Entre ellos se tiene el planteamiento del problema, los objetivos, el tipo de diseño, la metodología de desarrollo de la investigación, la hipótesis, las variables del estudio, la población y la muestra, las técnicas estadísticas y los instrumentos utilizados.

El tercer capítulo es la parte fundamental de la investigación. Allí se presenta de manera clara y detallada cada una de las fases del desarrollo de la investigación: el análisis de la situación actual a modo de diagnóstico, el plan de seguridad informática propuesto y la definición de los roles y responsabilidades que se deben cumplir.

El capítulo cuarto aborda el análisis y la interpretación de los resultados finales de la investigación, entre ellos, el resultado del diagnóstico de la seguridad informática actual. Se exponen los resultados de la evaluación del plan de seguridad informática propuesto. De la misma forma, se presenta la prueba de la eficiencia del plan propuesto. Asimismo, se muestran discusiones, conclusiones, recomendaciones, referencias bibliográficas y anexos.

Finalmente, se ofrece un cordial agradecimiento a las personas que participaron de una u otra forma en este trabajo de investigación, entre ellos, el asesor, magíster Manuel Alcántara Ramírez, por hacer legible esta investigación de manera permanente; la Universidad Norbert Wiener, por hacer realidad este sueño; y a los catedráticos, por compartir sus conocimientos.

I. MARCO TEÓRICO

*... el principio es lo más importante
en toda obra...*

Platón

*... sin causa y sin principio es imposible
que algo exista o se lleve a cabo.*

Aristóteles

1.1. Seguridad informática

Marcelo J. (1999) considera que la seguridad informática “[...] es un proceso continuo, no un producto”. Por lo tanto, es conjunto de sistemas, procedimientos, métodos y herramientas destinados a proteger la información.

Según Ribagorda M. (1994), la informática es una herramienta que implica “[...] riesgos cada vez más crecientes, a veces mal conocidos y poco combatidos”. Por ese motivo es preciso considerar el análisis de riesgo en las organizaciones, a fin de fortalecer la seguridad informática y garantizar la integridad, la confidencialidad y la disponibilidad de la información.

Por otro lado, la información es una fuente inagotable de cambios para una organización; como tal, la tecnología de la información viene transformando radicalmente la economía, la educación y la organización de las instituciones modernas.

Minguet J. (1997) sostiene que las nuevas tecnologías de la información “[...] aceleran el cambio en nuestras sociedades, fuerzan a la humanidad a adaptarse a nuevas relaciones en el espacio y en el tiempo. Tal radical cambio requiere un uso inteligente de los nuevos medios e instrumentos de la información. La red de redes se está convirtiendo en la base de una nueva economía, un nuevo comercio, una nueva educación, e influye fuertemente en los servicios financieros y administraciones públicas”.

El autor también manifiesta que el crecimiento tecnológico implica paralelamente una gran “[...] debilidad al hacerse más complejos e interconectados los sistemas informáticos, apareciendo más elementos vulnerables referente a la seguridad de la información”, lo que ocurre por dos razones básicas: los medios disponibles y el número de posibles manejadores o atacantes. Por otra parte, la extensión de la formación informática hace que se incremente el número de posibles atacantes con diversas motivaciones: reto personal, ideas políticas o sociales y posibilidad de beneficio económico, lo que implica definir políticas de seguridad informática para minimizar la vulnerabilidad de la información.

Según Joyanes L. (1997), “el impacto social de las tecnologías de la información y de la sociedad informatizada es vulnerable”.

Tomando como referencia lo que sostiene Joyanes, se puede afirmar que la seguridad informática nace con la aparición de los ataques a la información y de los activos informáticos por parte de los intrusos interesados en el contenido de esta. En este contexto, el objetivo de la seguridad de la información consiste en mantener la confidencialidad, la integridad y la disponibilidad.

Por su parte, Gonzales J. (2000) sostiene que la labor principal de la seguridad informática es el “[...] aislamiento de los actos no deseables y la prevención de aquellos que no se hayan considerado”, de forma que, si se producen estos, hagan el menor daño posible.

Por otro lado, Marcelo J. (1999) manifiesta que dentro del concepto de seguridad se debe “[...] distinguir la seguridad física y la seguridad lógica”.

a. La seguridad física. Comprende el aspecto del *hardware*, la manipulación del mismo y el ambiente en el cual se van a instalar los equipos. Para garantizar la seguridad se deben considerar los siguientes criterios:

- Uso del equipo por personal autorizado.
- Acceso al equipo del personal que tenga conocimientos mínimos sobre informática.
- Ambiente controlado.

b. La seguridad lógica. Comprende los sistemas tanto operativos como de información. Para garantizar la seguridad se deben considerar los siguientes criterios:

- Generación de contraseñas en diversos niveles del sistema, donde se permita solo el acceso a niveles de seguridad a usuarios con permiso.
- Generar un módulo del sistema para la emisión de reportes a cargo de un administrador, en donde se muestren las tablas de uso de los sistemas, los usuarios y los niveles de acceso.

1.1.1. Antecedentes de seguridad informática

A partir de los años 80, el uso del ordenador personal comienza a ser común, iniciándose la preocupación por la integridad de los datos. En la década de los 90 proliferan los ataques a sistemas informáticos, aparecen los virus y se toma conciencia del peligro que acecha a los usuarios de PC y a los equipos conectados a Internet; es decir, las amenazas se generalizan a finales de los 90. A partir del año 2000, los acontecimientos de la vulnerabilidad de la información fuerzan a que se tome en serio la seguridad informática.

Oppliger R. (1998) sostiene que el objetivo de la seguridad del ordenador es “[...] preservar los recursos de cómputo contra usos y abusos no autorizados, así como proteger los datos que representan y codifican la información de daños, revelaciones y modificaciones accidentales o deliberadas”.

Por su parte, Lardent A. (2001) manifiesta que el objetivo de la seguridad informática es mantener la “[...] integridad, la disponibilidad y la confidencialidad de la información”.

Cao J. (2005) sostiene que la seguridad es una “[...] cadena que siempre se rompe por el eslabón más débil”. En este contexto, la misión de cualquier responsable de seguridad informática es la gestión del riesgo sobre los sistemas de información que trata de proteger.

Según Steven B. (2001), las propiedades de la seguridad informática comprenden básicamente los siguientes aspectos:

- a. Confidencialidad.** Solo aquellos usuarios autorizados podrán acceder a los componentes del sistema.
- b. Integridad.** Los componentes del sistema solo pueden ser creados y modificados por los usuarios autorizados.

c. Disponibilidad. Los usuarios deben tener disponibles todos los componentes del sistema cuando así lo deseen.

Por su parte, Alcorcer C. (2000) afirma que existe una cuarta propiedad de la seguridad informática: “el no repudio de origen y destino”. Este término ha sido introducido en los últimos años como una característica más de los elementos que conforman la seguridad informática, la misma que cumple la aceptación de un protocolo de comunicación entre emisor y receptor (cliente y servidor), normalmente a través del intercambio de los respectivos certificados digitales de autenticación.

1.1.2. Debilidades de los sistemas informáticos

Con relación a las debilidades del sistema informático, se deben determinar los siguientes aspectos:

- a. Hardware.** Pueden producirse errores intermitentes, conexiones sueltas, desconexión de tarjetas, etc.
- b. Software.** Puede producirse sustracción de programas, ejecución errónea, modificación o defectos en llamadas al sistema.
- c. Datos.** Puede producirse alteración de contenidos, introducción de datos falsos o manipulación fraudulenta de datos.
- d. Memoria.** Puede producirse introducción de virus, mal uso de la gestión de memoria, bloqueo del sistema, etc.
- e. Usuarios.** Puede producirse suplantación de identidad, acceso no autorizado, visualización de datos confidenciales, etc.

Borghello C. (2001) define las amenazas informáticas como “[...] externas e internas”. Las amenazas externas se originan fuera de la organización y son los virus, los gusanos, los caballos de troya, los ataques de *hackers*, las represalias de exempleados o el espionaje. Por otro lado, las amenazas internas provienen del interior de la organización, lo cual es costoso, porque el infractor tiene mayor acceso y conocimiento de dónde reside la información sensible e importante.

Raya J. (2000) sostiene que las amenazas informáticas son básicamente de cuatro tipos diferentes: “interceptación, modificación, interrupción y generación”.

a. La interceptación. Ocurre cuando una persona no autorizada accede a una parte del sistema, haciendo uso de privilegios no adquiridos. Su detección es difícil, porque muchas veces no deja huella:

- Copias ilícitas de programas.
- Escucha en línea de datos.

b. La modificación. Trata de cambiar en todo o en parte el funcionamiento del sistema, con la finalidad de obtener beneficios personales. Su detección es difícil según las circunstancias:

- Modificación de base de datos.
- Modificación de elementos del *hardware*.

c. La interrupción. Se considera como temporal o permanente, lo cual puede ocasionar daño, pérdida o que deje de funcionar un punto del sistema. Su detección es inmediata:

- Destrucción del *hardware*.
- Borrado de programas o datos.
- Fallas en el sistema operativo.

d. La generación: Creación de nuevos objetos dentro del sistema. Su detección es difícil:

- Añadir transacciones en red.
- Añadir registros en base de datos.

Por su parte, Raya J. (2000) afirma que los datos de las redes informáticas son “[...] vulnerables a los desastres naturales (inundaciones, fuegos, pérdidas, averías), como a los daños provocados por gente maliciosa (competidores, gobiernos extranjeros, personas vengativas o solo curiosos)”.

Por lo expuesto, las amenazas informáticas son vistas como las condiciones del entorno del sistema de información (persona, máquina, suceso o idea). Podrían dar lugar a que se produzca una violación de la seguridad, perdiendo la confidencialidad, la integridad y la disponibilidad de la información. No obstante, un ataque informático no es más que la realización de una amenaza.

En esta perspectiva, Cariacedo J. (2004) afirma que las amenazas afectan principalmente al “[...] *hardware*, *software* y a los datos”, lo que está esquematizado en el siguiente cuadro:

Cuadro 1. Amenazas de los sistemas de información

Hardware	Software	Datos
<ul style="list-style-type: none"> ▪ Agua ▪ Fuego ▪ Electricidad ▪ Polvo ▪ Cigarrillos ▪ Comida 	<p>Además de algunos típicos del <i>hardware</i>.</p> <p>Borrados accidentales o intencionados.</p> <p>Fallas de programas.</p> <p>Bombas lógicas.</p> <p>Robo, copias ilegales, etc.</p>	<p>Tiene los mismos puntos débiles que el <i>software</i>, pero hay dos problemas añadidos: no tienen valor específico, pero sí su interpretación. Por otra parte, habrá datos de carácter personal y privado que podrían convertirse en datos de carácter público.</p>

Raya J. (2000) también menciona que los ataques al sistema de información se clasifican como “[...] ataques pasivos y activos”:

- a. Ataques pasivos.** Trata de recoger la información sin que nadie sepa que se está produciendo; por ejemplo, escucha, monitorea, para obtener información que está siendo transmitida. Sus objetivos son la interceptación de datos y el análisis del tráfico.
- b. Ataques activos.** Trata de cambiar los datos almacenados o transmitidos, e incluso puede provocar su borrado, su corrupción o el retraso de las transmisiones. Otra posibilidad de ataque activo es el embate de denegación de servicios, que impide el acceso a los usuarios autorizados a la red, congestionando el servidor con mensajes inservibles.

1.1.3. Vulnerabilidad de la información

La vulnerabilidad de la información es la posibilidad de ocurrencia de la materialización de una amenaza sobre un activo. En este contexto, Minguet J. (1997) manifiesta que también es la “[...] debilidad en los sistemas de información que pueda permitir a las amenazas causarles daños y producir pérdidas, que generalmente se producen por fallos en los sistemas lógicos, aunque también corresponden a defectos de ubicación e instalación”.

Para Ribagorda M. (1994), la administración de la seguridad informática consiste en “[...] autenticación, autorización, auditoría”:

- a. Autenticación.** Solo las personas autorizadas deben tener cuentas de acceso a dichos equipos, puesto que sería peligroso que alguna otra persona las tuviera. Se deben establecer algunas entidades que puedan tener acceso al universo de los recursos informáticos.
- b. Autorización.** Es el hecho de que las entidades autorizadas a tener acceso a los recursos de cómputo tengan, efectivamente, acceso únicamente a las áreas de trabajo que van a manejar.
- c. Auditoría.** Es la continua vigilancia de los servicios en producción, además de las políticas de uso y acceso a los recursos, así como los reglamentos que rijan la no divulgación de información confidencial.

1.2. Delitos informáticos

Los delitos informáticos son aquellas conductas ilícitas susceptibles de ser sancionadas por el derecho penal, en quienes hacen uso indebido de cualquier medio informático sin la autorización del autor.

El INEI (2001) resalta los delitos informáticos como “[...] actividades criminales que en un primer momento los países han tratado de encuadrar en figuras típicas de carácter tradicional, tales como robo, hurto, fraude, falsificaciones, estafa, sabotaje, etc.”.

Los delitos informáticos se desarrollan, según Borghello C. (2001), siempre con la “[...] complicidad de terceros, en forma física, y en determinadas eventualidades, y son realizadas totalmente a través de las computadoras”.

Entre ellos se podrían citar los siguientes aspectos:

- La propagación de virus informáticos.
- El envío masivo de correo no deseado o SPAM.
- El envío o ingreso subrepticio de archivos espías o *keyloggers*, etc.

Nuñez J. (1999) afirma que los delitos informáticos son todas aquellas “[...] conductas ilícitas de quienes hacen uso indebido de cualquier medio informático para cometer sus actos ilícitos”. Por lo tanto, el delito informático resulta ser un buen negocio para quienes lucran con los recursos informáticos ajenos. Las características son las siguientes:

- Objetos pequeños (contenedores), donde la información es almacenada.
- Sin contacto físico: en la mayoría de los casos se asegura el anonimato y la integridad física del propio delincuente informático, ya que la información se puede sustraer a través de redes.
- Alto valor: el contenido (los datos) pueden valer mucho más que el soporte que los almacena (computador, disco, CD, USB, etc.).

1.2.1. Legislación nacional sobre los delitos informáticos

El 17 de julio del año 2000 se publicó en el diario oficial El Peruano la Ley N.º 27309, que incorporó al código penal peruano los delitos informáticos dentro de la figura genérica de los delitos contra el patrimonio, que a la letra, en el artículo 207, en los literales A, B y C, textualmente dice:

Artículo 207°-A. “El que utiliza o ingresa indebidamente a una base de datos, sistema o red de computadoras o cualquier parte de la misma para diseñar, ejecutar o alterar un esquema u otro similar, o para interferir, interceptar, acceder o copiar información en tránsito o contenida en una base de datos, será reprimido con pena privativa de libertad no mayor de

dos años o con prestación de servicios comunitarios de cincuenta y dos a ciento cuatro jornadas. Si el agente actuó con el fin de obtener un beneficio económico, será reprimido con pena privativa de libertad no mayor de tres años o con prestación de servicios comunitarios no menor de ciento cuatro jornadas”.

Artículo 207°-B. “El que utiliza, ingresa o interfiere indebidamente una base de datos, sistema, red o programa de computadoras o cualquier parte de la misma con el fin de alterarlos, dañarlos o destruirlos, será reprimido con pena privativa de libertad que no será menor de tres, ni mayor de cinco años, y con setenta a noventa días de multa”.

Artículo 207°-C. “En los casos de los artículos 207°-A y 207°- B, la pena privativa de libertad no menor de cinco ni mayor de siete años, cuando:

- El agente accede a una base de datos, sistema o red de computadora, haciendo use de información privilegiada, obtenida en función a su cargo.
- El agente pone en peligro la seguridad nacional”.

Igualmente, la Oficina Nacional de Gobierno Electrónico e Informático (2007), de acuerdo con el numeral 4.8 del artículo 4° y 49° del Reglamento de Organización y Funciones de la Presidencia del Consejo de Ministros (PCM), aprobado por el decreto supremo N.º 063-2007-PCM, que establece “normar, coordinar, integrar y promover el desarrollo de la actividad informática en la administración pública, impulsando y fomentando el uso de las nuevas tecnologías de la información para la modernización y desarrollo del estado, actúa como ente rector del sistema nacional de informática, y dirige y supervisa la política nacional de informática y gobierno electrónico.

- Mediante la resolución comisión de reglamentos técnicos y comerciales N.º 001-2007-INDECOPI-CRT del 5 de enero de 2007, se aprobó la Norma Técnica Peruana NTP-ISO/IEC 17799:2007 EDI. Tecnología de la información. Código de buenas prácticas para la gestión de la seguridad de la información.
- La Oficina Nacional de Gobierno Electrónico e Informático (ONGEI) de la PCM, en coordinación con el Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (Indecopi), ha recomendado la aplicación y uso obligatorio de la NTP antes mencionada en todas las entidades integrantes del sistema nacional de informática.
- De conformidad con lo dispuesto por el decreto legislativo N.º 560-Ley del Poder Ejecutivo, y el reglamento de organización y funciones de la PCM, aprobado por Decreto Supremo N.º 063-2007-PCM.

Se resuelve:

- Artículo 1º. Aprobar el uso obligatorio de la norma técnica Peruana NTP-ISO/IEC 17799:2007 EDI. Tecnología de la Información. “Código de buenas prácticas para la gestión de la seguridad de la información”, en todas las entidades integrantes del sistema nacional de informática, documento que será publicado en el portal de la PCM (www.pcm.gob.pe).
- Artículo 2º. La NTP señalada en el artículo precedente, se aplicará a partir del día siguiente de la publicación de la presente Resolución Ministerial N.º 246-2007-PCMI, debiendo las entidades antes mencionadas considerar las actividades necesarias en sus respectivos planes operativos informáticos, para su implantación.

En este contexto, la Norma Técnica Peruana, código de buenas prácticas para la gestión de seguridad de la información, señala recomendaciones para realizar la gestión de seguridad de la información. No obstante, es recomendable instalar en toda organización un proceso de gestión de seguridad informática para el desarrollo y mantenimiento de la continuidad de la tecnología de información.

1.2.2. Delincuentes informáticos

Borghello C. (2001) clasifica a los delincuentes informáticos, en su trabajo de investigación *Seguridad informática y sus implicancias e implementación*, como sigue:

“Los hackers son quienes interceptan dolosamente un sistema informático para dañar, apropiarse, interferir, desviar, difundir y/o destruir información que se encuentra almacenada en computadoras pertenecientes a entidades públicas o privadas. El término de “hackers” en castellano significa “cortador”. Los cuales son fanáticos de la informática, que tan solo con un computador personal, un *modem*, paciencia e imaginación son capaces de acceder, a través de una red pública de transmisión de datos, al sistema informático de una empresa o entidad pública, saltándose todas las medidas de seguridad y leer información, copiarla, modificarla, preparando las condiciones idóneas para llamar la atención sobre la vulnerabilidad de los sistemas informáticos, o satisfacer su propia vanidad”.

“Los crackers, en realidad, son hackers cuyas intenciones van más allá de la investigación. Es una persona que tiene fines maliciosos o de venganza, quiere demostrar sus habilidades pero de manera equivocada o simplemente personas que hacen daño solo por diversión”.

“Los phreakers son personas que ingresan al sistema telefónico, teniendo o no equipo de computación, con el propósito de apoderarse, interferir, dañar, destruir, conocer, difundir, hacer actos de sabotaje, o hacer uso de la información accediendo al sistema telefónico, provocando las adulteraciones que, en forma directa, conlleva este accionar, con su consecuente deterioro económico. Son personas con unos conocimientos de telefonía insuperables. Conocen a fondo los sistemas telefónicos, incluso más que los propios técnicos de las compañías telefónicas. Estas personas han sabido crear todo tipo de cajas de colores con una función determinada. Actualmente se preocupan más de las tarjetas de prepago que de las cajas, ya que suelen operar desde cabinas telefónicas o móviles. Un sistema de retos es capaz de captar los números de abonado en el aire. De esta forma es posible crear clones de tarjetas telefónicas a distancia”.

“Los carding-trashing son las personas que dedican sus esfuerzos a romper seguridad, como reto intelectual nació así:

- a. El *carding* es el uso ilegítimo de las tarjetas de crédito (o sus números) pertenecientes a otras personas con el fin de obtener bienes realizando fraude con ellas. Se relaciona mucho con el *hacking* y el *cracking*, mediante los cuales se consiguen los números de las tarjetas.
- b. El *trashing*, que consiste en rastrear en las papeleras en busca de información, contraseñas o directorios”.

“Los gurús son considerados los maestros y encargados de formar a los futuros hackers. Generalmente no están activos pero son identificados y reconocidos por la importancia de sus hurtos, de los cuales solo enseñan las técnicas básicas”.

“Los bucaneros son comerciantes que venden los productos sustraídos por otros. Generalmente comercian con tarjetas de crédito y de acceso y compran a los *copyhackers*. Son personas sin ningún (o escaso) conocimiento de informática y electrónica”.

“Los piratas informáticos son personajes generalmente confundidos con los hackers, son realmente peligrosos desde el punto de vista del copyright, ya que copian soportes audiovisuales (discos compactos, *cassettes*, DVD, etc.) y los venden ilegalmente”.

Nuñez J. (1999) también sostiene que los delincuentes informáticos son “[...] personas o grupos de personas que en forma asociada o individualmente realizan actividades ilegales haciendo uso de computadoras en agravio de terceros, en forma local o a través de internet”. Una de las prácticas más conocidas es la de interceptar compras en línea a través de Internet, haciendo uso del nombre, número de tarjeta de crédito y fecha de expiración, proporcionando la dirección de envío, diferente de la del titular del número de la tarjeta de crédito que usan en forma ilegal.

También son delincuentes informáticos los piratas que distribuyen *software* sin contar con las licencias de uso, proporcionadas por su autor o representantes, pues no solo atentan contra la propiedad intelectual, provocando la fuga de talentos informáticos, sino que se enriquecen ilícitamente, además de ser evasores de impuestos.

1.3. Plan de seguridad informática

El plan de seguridad informática es un documento que generan los responsables de la organización, en el que se establecen los principios y funciones de la seguridad, el cual es generado mediante el análisis de riesgo e identificación de las amenazas de los sistemas de información. No obstante, un plan de seguridad informática hace constar cuáles son los activos informáticos que deben protegerse.

En este contexto, el objetivo de un plan de seguridad es garantizar la continuidad y la privacidad de la información, tratando de minimizar la vulnerabilidad de los sistemas o de la información contenida en ellos, proteger las redes privadas y sus recursos, mientras se mantienen los beneficios de la conexión a una red pública o a una red privada.

Se coincide con lo que sostiene Maiwald E. (2003), quien manifiesta que la seguridad de la información son las “[...] medidas adoptadas para evitar el uso no autorizado, el mal uso, la modificación o la denegación del uso de conocimientos, hechos, datos o capacidades”. También menciona que la “[...] seguridad de la información es el nombre dado a los pasos preventivos que se toman para proteger la información”.

Para garantizar la seguridad informática en las instituciones, es preciso tomar en cuenta las siguientes medidas:

- a. Medidas administrativas y organizativas. Que son de competencia de la alta dirección de la entidad y de obligatorio cumplimiento por todo el personal. Comprenden la clasificación de la información, personal y responsabilidades.
- b. Medidas de seguridad físicas. Relacionadas con las áreas por proteger, especificando en cada caso que se consideran áreas vitales o reservadas, si se procesa información clasificada y sensible.
- c. Medidas de seguridad lógica. Se especifican las acciones por implementar en función del *software*, *hardware* o ambos. Se describe el mecanismo de identificación y autenticación de los usuarios con acceso a los sistemas de información, especificando cómo se implementa el nivel de sistema operativo y de aplicaciones, para evitar la modificación, destrucción y consistencia de los ficheros y datos.
- d. Medidas de seguridad en operaciones. Se relacionan los criterios adoptados para seleccionar los mecanismos de seguridad convenientes, así como para verificar sus niveles de efectividad y protección continua.

Incluyen las medidas que se establecen para garantizar que los mantenimientos de los equipos, soportes y datos se realicen en presencia y bajo la supervisión del personal responsable, y que, en caso del traslado del equipo fuera de la entidad, se garantice el control de la entrada y salida de las tecnologías de información (máquinas portátiles, soportes etc.), así como el uso para el que están destinadas.

e. Medidas educativas y de concientización. Se establecen campañas de educación para concientizar al personal que labora en la institución.

1.3.1. Plan de contingencia

Se define como una estrategia planificada con una serie de procedimientos que facilitan u orientan a una solución alternativa, que permiten restituir rápidamente los servicios de información. No obstante, un plan de contingencia es una herramienta que ayuda a que los procesos críticos de la institución u organización continúen funcionando a pesar de una falla en los sistemas computarizados. Es decir, un plan adecuadamente desarrollado permite a las organizaciones seguir operando, aunque sea al mínimo.

Para el INEI (2000), un plan de contingencia es “[...] una guía de acciones de emergencia que permite apoyar la continuidad de los procesos en una institución, ante la posibilidad que se produzcan imprevistos debido al problema informático. La aplicación del plan de contingencia permite atender fallas generadas en el funcionamiento interno, y además, previene fallas potenciales originadas en fuentes externos de la institución, las cuales pueden ser de orden financiero, tecnológico, de servicios públicos, insumos y productos, entre otros”.

Por lo expuesto, un plan de contingencia es el estudio y análisis pormenorizado de las áreas que componen la institución, y que sirve para establecer una política de recuperación ante un desastre. En este sentido, el plan de contingencia es un conjunto de datos estratégicos que la institución plasma en un documento, con el fin de protegerse ante eventualidades.

Objetivos del plan de contingencia

Garantizar la continuidad de los procesos y de los elementos considerados críticos. Define acciones y procedimientos por ejecutar en caso de fallas de los elementos que componen un sistema de información.

El INEI (1997) señala que el plan de contingencia “[...] permite a las instituciones mantener la continuidad de sus sistemas de información frente a eventos críticos de su entidad y minimizar el impacto negativo sobre la misma de sus empleados y usuarios”. No obstante, debe ser parte integral de la institución servir para evitar interrupciones y estar preparado para las fallas potenciales y orientaciones hacia una solución.

Desastres y medidas de prevención

Para prevenir las ocurrencias de los desastres es necesario definir medidas y procedimientos de seguridad informática, las mismas que sustentan los diversos desastres y medidas de prevención. Más de un estudioso, entre ellos Raya J. (2000), afirman que existen “[...] una serie de desastres [...]” que se deben tener en cuenta para proteger la información de manera adecuada.

- a. Desastres naturales: huracanes, tormentas, inundaciones, tornados, incendios, terremotos y otros, para lo cual se deben tomar las siguientes medidas de prevención:
- Emplazamientos adecuados.
 - Protección de fachadas, ventanas y puertas.
- b. Vandalismo informático: se considera al terrorismo, sabotaje, robo, virus, chantaje informático y programas malignos. Frente a estos ataques, considerar las siguientes medidas:
- Fortificación de entradas.
 - Guardianía.
 - Patrullas de seguridad.
 - Circuito cerrado de TV.
 - Control físico de accesos.
 - Protección de *software* y *hardware*.
 - Seguimiento de las políticas de seguridad en la institución.
- c. Amenazas de inundación. Se ha de considerar la inundación como un imprevisto sufrido por causa propia de la institución tanto como por causas ajenas y pequeños incidentes personales (derramar agua o café sobre el teclado). Igualmente, frente a estas amenazas se deben tener en cuenta las siguientes medidas:
- Revisar conductos de agua.
 - Instalar sistemas de drenaje de emergencia.

Amenazas del fuego. Se consideran como amenaza una mala instalación eléctrica o descuido personal de los trabajadores: Fumar en sala de ordenadores, papeleras mal ubicadas, vulnerabilidades del sistema ante el humo. Frente a este tipo de percances, se deben considerar las siguientes medidas de prevención:

- Colocar un detector de humo y calor.
- Almacén de papel separado de máquinas.
- Estado del pozo a tierra.
- Extintores revisados.

Cabe señalar que ante los desastres señalados la organización debe realizar campañas de capacitación para cada uno de sus empleados acerca la importancia de la seguridad informática, lo cual permitirá manipular los recursos informáticos adecuadamente.

1.3.2. Políticas de seguridad informática

Las políticas de seguridad informática son un conjunto de reglas aplicadas a todas las actividades relacionadas con el manejo de la información en una institución, y tienen como propósito proteger la información, los recursos informáticos y la reputación de la misma.

Según el INEI (1997), las políticas de seguridad son “[...] guías para asegurar la protección y la integridad de los datos dentro de los sistemas de aplicaciones, redes, instalaciones de cómputo y procedimientos manuales”.

Por su parte Lardent A. (2001) sostiene que la “[...] política de seguridad es un elemento clave para cumplir el éxito de la misma; por tanto, el propósito de seguridad es la formulación de una política que defina con claridad el marco de la seguridad y el establecimiento de responsabilidades”.

Estas políticas exigen los siguientes aspectos:

- Concientización formal de la importancia de la seguridad por parte de las autoridades o la alta gerencia.
- Percepción de la importancia por parte del personal en sus distintos niveles.

Es decir, una política de seguridad informática es una forma de comunicarse con los usuarios, con el fin de canalizar el uso adecuado de los recursos informáticos. La misma forma parte del sistema de información en toda institución u organización.

En esta perspectiva, la planificación de la seguridad informática es la etapa en la que se realiza la identificación de los requerimientos informáticos, los alcances que brindan servicios a los usuarios a nivel de aplicaciones, con lo cual se ejecuta una proyección en base al crecimiento de los servicios que se ofrecen.

Tomando en cuenta el punto de vista de Lardent A. (2001), quien sostiene que la identificación de los requerimientos son “[...] recursos para implementar y controlar el funcionamiento adecuado de los sistemas de información”:

- a. Demostrar que los costos de los recursos de seguridad están entendidos e incorporados explícitamente en las hojas de planificación del ciclo de vida total del sistema de una manera constante, con la dirección de presupuesto para la programación del capital.
- b. Incorporar un plan de seguridad que contenga lo siguiente:
 - Las reglas de utilización del sistema y las consecuencias al violar dichas reglas.
 - Los métodos para identificar y administrar los límites de las interconexiones con otros sistemas y los procedimientos específicos para vigilarlos.

- Procedimientos para el entrenamiento de los individuos que tienen acceso permitido al sistema.
- Procedimientos para el monitoreo de la eficacia de los controles de la seguridad.
- Procedimientos adecuados para reportar a las autoridades.

No obstante, los elementos de la tecnología de información (computadoras personales, servidores, tarjetas de red, cables, etc.) y los suministros (programas de computadora, *diskettes*, CD, DVD, USB, etc.), deben inventariarse, asegurarse apropiadamente y actualizarse de manera permanente.

Por otro lado, las instituciones que adquieren equipos físicos y programas de cómputo (computadoras personales, monitores, tarjetas de acceso a la red, etc.), deben anotar esos artículos en un banco de datos de control de activos, y verificarlos cuidadosamente para garantizar que son lo que se solicitó y que los artículos están configurados correctamente y funcionan apropiadamente.

Por lo expuesto, la administración del inventario es importante y se deben tomar en cuenta las siguientes acciones:

- a. En el momento en el que se recibe un equipo o componente electrónico, debe establecerse la configuración de cada pieza del equipo físico y programa.
- b. Describir detalladamente cada uno de los componentes del sistema, tanto el equipo físico como su ubicación en el ambiente destinado.
- c. Automatizar mediante el proceso de la administración del inventario.

Tomando el punto de vista de Gonzales J. (2000), quien considera el control de los riesgos como “constantes y se necesita contar con los mecanismos necesarios para analizarlos y aplicar las estrategias precisas frente a estos riesgos, y no esperar a que ocurran para plantear una solución”; por ello es necesario realizar las siguientes acciones:

- a. Establecer un método específico y entendible para evaluar continuamente los riesgos potenciales, con la finalidad de mantener la seguridad en un nivel aceptable, así como los procedimientos para asegurar un control eficaz con los tiempos de respuesta necesarios.
- b. Identificar los controles adicionales de seguridad informática para reducir al mínimo el riesgo potencial de pérdida de los sistemas al promover o permitir acceso público.

Según expresa Ituribe F. (2002), el concepto de los estándares de seguridad informática “[...] son recomendaciones técnicas que facilitan la administración y crecimiento de los recursos informáticos”. Tomando como referencia el punto de vista del autor, se deben tomar en cuenta los siguientes aspectos:

- a. Asegurar el uso de estándares, al implementar productos y herramientas informáticos.
- b. Usar productos de seguridad disponibles y probados en el mercado. Si los productos son nuevos, las metodologías usadas para probarlos pueden evaluar y examinar los resultados.

Para hacer cumplir las políticas de seguridad, según Alcorcer C. (2000), se deben “establecer métodos”; para ello, se considerarán los siguientes aspectos:

- a. Diseñar un sistema de seguridad basado en las necesidades del usuario, la naturaleza de las aplicaciones y la información que se debe asegurar.
- b. Aplicar las medidas de seguridad constantemente.

La capacitación en el uso del plan de seguridad informática, es, según Gómez A. (2006), la forma de “[...] asegurar la continuidad de la difusión de las políticas de seguridad en todos los niveles de la institución, desde los directivos hasta el personal que opera los sistemas.” Tomando en cuenta el punto de vista del autor, se deben considerar los siguientes aspectos:

- a. Crear procedimientos de capacitación de acuerdo con los niveles jerárquicos.
- b. Reforzar el adiestramiento mediante el examen y distribución de material relevante, por ejemplo, relatos relacionados con ataques cibernéticos o abusos de sistemas.

En sentido parecido, Marcelo J. (1999) define la segmentación de la información compartida como una “[...] política que tiene por finalidad proteger la información y los sistemas de acuerdo con su valor”:

- a. Los informes de inteligencia confidenciales deben estar protegidos mediante una seguridad elevada.

Siguiendo las líneas de la investigación, se expone también al respecto la documentación de la información relevante, como una política que consiste en documentar todos los procesos y configuraciones necesarias referidas a temas de seguridad de la información que se implementan en una institución; es decir, desde los manuales hasta los procedimientos de aplicación, pues una de las amenazas a la seguridad que se descuida con más frecuencia se relaciona con la documentación del sistema. A menudo, la documentación de cualquier tipo se trata con descuido y es posible encontrarla en oficinas que no son seguras. Por tanto, para mejorar la seguridad de la documentación se deben considerar los siguientes aspectos:

- a. La alta dirección de cada institución emitirá directivas internas referidas a la documentación de los procedimientos realizados, en beneficio de la seguridad de la información.
- b. Distribuir la documentación para que se tenga conocimiento.
- c. Controlar el acceso a la documentación y adiestrar a los usuarios acerca de cómo protegerla.

Gómez A. (2006) sostiene que una política de seguridad informática es una “[...] forma de comunicarse con los usuarios, ya que las mismas establecen un canal formal de actuación del personal, en relación con los recursos y servicios informáticos de la organización, pues una política de seguridad debe orientar las decisiones que se toman con relación a la seguridad. Se requiere la disposición de todos los miembros de la empresa para lograr una visión conjunta de lo que se considera importante”.

Con referencia al punto de vista del autor, las políticas de seguridad informática ofrecen explicaciones comprensibles sobre por qué deben tomarse ciertas decisiones y explicar la importancia de los recursos.

1.4. Auditoría de sistemas

Henríquez E. (2001) define la auditoría informática como una “[...] serie de exámenes que se realizan con carácter objetivo, crítico, sistemático y selectivo”, con el fin de evaluar la eficacia y la eficiencia del uso adecuado de los recursos informáticos, de la gestión informática y si estas han brindado el soporte adecuado a los objetivos y a las metas de la empresa o institución.

Lardent A. (2001) también define la auditoría informática “[...] como la revisión y la evaluación de los controles, sistemas, procedimientos de informática de los equipos de cómputo, su utilización, eficiencia y seguridad, de la organización que participa en el procesamiento de la información”.

En la misma línea de análisis se puede mencionar a Mugica O. (2006), quien afirma que la auditoría en informática no solo comprende la evaluación de los equipos de cómputo, de un sistema o procedimiento específico, “[...] sino que además evalúa los sistemas de información en general, desde sus entradas, procedimientos, controles, archivos”. Por otro lado, la auditoría evalúa y comprueba los controles y procedimientos informáticos más complejos, desarrollando y aplicando técnicas mecanizadas de auditoría, incluyendo el uso de *software*.

Es evidente que la auditoría en informática es de vital importancia para el buen desempeño de los sistemas de información, ya que proporciona los controles necesarios para que los sistemas sean confiables y posean un buen nivel de seguridad.

1.4.1. Objetivos de la auditoría de sistemas

- Buscar una mejor relación del costo-beneficio de los sistemas automáticos o computarizados.
- Incrementar la satisfacción de los usuarios de los sistemas computarizados.
- Asegurar mayor integridad, confidencialidad y disponibilidad de la información mediante la recomendación de seguridades y controles.
- Conocer la situación actual del área informática y las actividades y esfuerzos necesarios para lograr los objetivos propuestos de la organización.
- Seguridad de personal, datos, *hardware*, *software* e instalaciones.
- Minimizar existencias de riesgos en el uso de tecnología de información.
- Capacitación y educación sobre controles en los sistemas de información.

1.4.2. Controles de la auditoría

Conjunto de disposiciones metódicas, cuyo fin es vigilar las funciones y actitudes de las instituciones. Es necesario verificar si todo se realiza conforme programas adoptados, órdenes impartidas y principios admitidos.

Según Echenique J. (1999), la “clasificación de los controles” consiste en lo siguiente:

- a. Controles preventivos. Son aquellos que reducen la frecuencia con que ocurren las causas del riesgo, permitiendo cierto margen de violaciones. Como ejemplos, se tienen el letrero de "no fumar" para salvaguardar las instalaciones y los sistemas de claves de acceso.

- b. Controles detectivos. Son aquellos que no evitan que ocurran las causas del riesgo, sino que los detecta luego de ocurridos. En cierta forma sirven para evaluar la eficiencia de los controles preventivos. Como ejemplo se tienen los: archivos y procesos que sirven como pistas de auditoría.
- c. Controles correctivos. Ayudan corregir las causas del riesgo. La corrección adecuada puede resultar difícil e ineficiente, siendo necesaria la implantación de controles detectivos sobre los controles correctivos, debido a que la corrección de errores es en sí una actividad altamente propensa a errores.

Echenique J. (1999) también manifiesta que, para realizar “[...] una adecuada auditoría en informática, se deben seguir una serie de pasos previos que permitirán dimensionar el tamaño y características del área dentro del organismo a auditar”. En este contexto, en el caso de la auditoría informática, la planeación es fundamental, pues habrá que hacerla desde el punto de vista de dos objetivos:

- a. Evaluación de los sistemas y procedimientos.
- b. Evaluación de los equipos de cómputo.

Por otro lado, el autor manifiesta que, para realizar una planificación eficaz, lo primero que se requiere es obtener información en general sobre la organización y sobre la función informática por evaluar. Para ello se precisa la investigación preliminar y algunas entrevistas previas; en base a ello, se planificará el programa de trabajo, el cual debe incluir tiempo, costo, personal necesario y documentos auxiliares por solicitar o formular durante el desarrollo de la misma.

Por tanto, es importante realizar una investigación preliminar, lo que concuerda con lo señalado por Lardent A. (2001): “observar el estado general del área, su situación dentro de la organización, si existe la información solicitada, si es o no necesaria y la fecha de su última actualización”.

Por la exposición de los autores señalados, es necesario considerar una investigación preliminar solicitando y revisando la información de cada una de las áreas de una institución, la cual debe considerar los siguientes aspectos:

- Verificar que la estructura organizativa asegure una adecuada separación de funciones para cumplir con principios de control interno. Asegurar la protección de archivos (de datos y de programas) para mantener la continuidad de las operaciones bajo condiciones normales de procesamiento.
- Verificar que se mantenga un control eficaz en los niveles de autorización de datos y de procedimientos.
- Examinar la documentación existente y evaluar su contenido y nivel de actualización.

1.5. Estándares y normas de seguridad

Un estándar es una regla o norma ampliamente aceptada y aplicada; el concepto se utiliza generalmente como sinónimo de una norma técnica.

Una norma es una regla de validez universal publicada, decidida mediante un procedimiento de normalización y jurídicamente aceptada por todas las partes para la solución de un estado de cosas. No obstante, las normas internacionales de seguridad informática proporcionan un conjunto de buenas prácticas en gestión de seguridad de la información.

En este contexto, la norma ISO 27001/ISO17799:2005 define las exigencias relacionadas con los sistemas de gestión de la seguridad de la información. Para Yory J. (2006), el objetivo de la misma “[...] es permitir a las organizaciones identificar, tratar y limitar amenazas en los activos de la información”.

Cabe mencionar que en la actualidad la norma internacional ISO 27001/ISO 17799:2005 es aplicable para la implantación de un sistema de gestión de la seguridad de la información. Esta norma proporciona una base común para la elaboración de las normas de seguridad de las organizaciones, un método de gestión eficaz de la seguridad, y establece informes de confianza en las transacciones y las relaciones entre las organizaciones. La misma ha sido publicada en dos partes:

- ISO/CEI 17799:2005. Código de buenas prácticas para la gestión de la seguridad de la información.
- ISO/CEI 27001:2005-BS 7799 Parte 2. Especificaciones relativas a la gestión de la seguridad de la información.

Se trata de dos estándares que están muy relacionados, pero que desempeñan papeles distintos. Así, mientras que la primera parte se aplica en la etapa de normalización, la segunda parte es aplicable en la etapa de certificación.

Por tanto, el ISO 17799:2005 es una guía que contiene consejos y recomendaciones, controles que permiten garantizar la seguridad de la información en una organización dentro de varios dominios de aplicación. Define una vía sistemática para manejar la información, que es apropiada para cualquier tipo de organización, pero no se trata de una norma certificable.

Es preciso mencionar que la norma ISO/CEI 17799:2005 fue inicialmente desarrollada por el organismo British Standards Institution (BSI) como BS 7799-1. En diciembre de 2000 fue adoptada según un "[...] procedimiento de vía rápida" por el Comité Técnico Mixto ISO/CEI JTC 1, Tecnologías de la Información, y publicado con las siglas ISO/CEI 17799:2000.

En junio de 2005, la norma ISO/CEI 17799:2000 fue revisada de forma sustancial, y se sustituyó con efecto inmediato por la norma ISO/CEI 17799:2005. En esta nueva norma se presentan 11 dominios de controles (uno más que en la versión anterior); algunos de los dominios han sido renombrados, se han introducido nuevos controles para gestionar una serie de temáticas no cubiertas y se han extendido otras áreas, tales como la finalización de contratos o la comunicación móvil distribuida. Destaca también que en cada control se ha incluido una breve guía de implantación. De modo que los 11 dominios de seguridad definidos en el estándar ISO/CEI 17799:2005 son los siguientes:

- Política de seguridad. Controles para proporcionar directivas y consejos de gestión para mejorar la seguridad de los datos.
- Organización de la seguridad de la información. Controles para facilitar la gestión de la seguridad de la información en el seno de la organización.
- Gestión de activos. Controles para catalogar los activos y protegerlos eficazmente.
- Seguridad de los recursos humanos. Controles para reducir los riesgos de error humano, robo, fraude y utilización abusiva de los equipamientos.
- Seguridad física y medioambiental. Controles para impedir la violación, el deterioro y la perturbación de las instalaciones y datos industriales.
- Gestión de las telecomunicaciones y operaciones. Controles para garantizar un funcionamiento seguro y adecuado de los dispositivos de tratamiento de la información.

- Control de accesos a los datos. Evitar accesos no autorizados a los sistemas de información.
- Adquisición, desarrollo y mantenimiento de los sistemas de información. Controles para garantizar que la seguridad esté incorporada a los sistemas de información.
- Gestión de incidencias. Controles para gestionar las incidencias que afectan la seguridad de la información.
- Gestión de la continuidad de las operaciones de la organización. Controles para reducir los efectos de las interrupciones de actividad y para proteger los procesos esenciales de la organización contra averías y siniestros mayores.
- Conformidad. Controles para prevenir los incumplimientos de las leyes penales o civiles de las obligaciones reglamentarias o contractuales y de las exigencias de seguridad.

Por otro lado, desde el 15 de octubre de 2005 las organizaciones que deseen certificar su sistema de gestión de la seguridad de la información pueden ser evaluadas con respecto a una nueva norma internacional ISO/CEI 27001:2005. Esta norma sustituye a la norma británica BS 7799-2:2002, que es la que ha sido mayormente utilizada hasta este momento.

No obstante, el estándar ISO/CEI 27001:2005 establece los requisitos para un sistema de gestión de la seguridad de la información (SGSI) y complementa el estándar ISO/CEI 17799:2005, código de buenas prácticas, asegurando la selección de controles de seguridad adecuados que protejan los activos de información y ofrezcan confianza a todas las partes interesadas.

En este contexto, la organización que obtiene la certificación es considerada que cumplimenta ISO 17799:2005, y que está certificada bajo ISO 27001:2005. Con la certificación, la organización demuestra a sus socios que su sistema cumple tanto con los estándares de la norma como con las exigencias de controles para la seguridad, que son establecidos según sus propias necesidades.

En la norma se presentan en detalle las etapas para el desarrollo del SGSI, para su implantación, así como aquellas para su mantenimiento. Incluye un método de evaluación, un proceso de documentación y un método de revisión que sigue el modelo PDCA (Planificar-Hacer-Verificar-Actuar).

Según Alberto G. (2006), el equipo de proyecto de la implantación “[...] debe estar formado por representantes de todas las áreas de la organización que se vean afectadas por el SGSI, liderado por la dirección y asesorado por consultores externos especializados en seguridad informática”.

También sostiene que la “[...] norma está orientada a establecer un sistema gerencial que permita minimizar el riesgo y proteger la información en las organizaciones de las amenazas externas e internas”. El argumento principal para adoptar un SGSI, según ISO 27001:2005, es que es un estándar basado en una metodología de proceso (PDCA), la misma que es capaz de proporcionar una situación continuada de seguridad en el tiempo. No obstante, este estándar se basa en la mejora continua que proporciona la metodología PDCA, la misma que se define de la siguiente forma:

Planificar

- Definir el alcance del SGSI y las políticas de seguridad.
- Seleccionar los objetivos de control y controles que ayudarán a manejar esos riesgos.
- Preparar el documento de la declaración de aplicabilidad.

Hacer

- Formular e implementar un plan de reducción de riesgos.
- Implementar los controles seleccionados a fin de cumplir con los objetivos de dichos controles.

Verificar

- Efectuar el control de los procedimientos.
- Proceder a exámenes periódicos para asegurar la eficacia del SGSI.
- Instaurar periódicamente auditorías internas para el SGSI.

Actuar

- Implementar las mejoras identificadas al SGSI.
- Realizar las acciones correctivas y preventivas.
- Mantener comunicaciones con todos los interesados.

Por lo expuesto, el modelo permite identificar y evaluar los riesgos sobre la información, desarrollar un plan que contenga las políticas y procedimientos para administrar y controlar estos riesgos, poner en ejecución y probar el plan y ajustarlo en forma continua.

Para sintetizar el plan propuesto en dicha investigación, se considera el modelo de diagrama “causa-efecto” o Ishikawa, también conocido como *espina de pescado*, o *árbol de causas*. Es una técnica gráfica ampliamente utilizada para apreciar con claridad las relaciones entre un tema o problema y sus posibles causas. Fue construido con la apariencia de una espina de pescado. Esta herramienta fue aplicada por primera vez en 1953 en Japón por el profesor de la Universidad de Tokio Kaoru Ishikawa, para sintetizar las opiniones de los ingenieros de una fábrica cuando discutían problemas relacionados con la calidad.

Este modelo es una representación gráfica de las relaciones lógicas que existen entre las causas que producen el efecto definido, lo que permite visualizar, en una sola figura, todas las causas asociadas y sus posibles relaciones.

El modelo también se utiliza entre otros motivos para establecer un proceso, aumentar la eficacia de los procesos, mejorar un bien o servicio, reducir o eliminar las deficiencias, modificar procedimientos o métodos de trabajo, identificar puntos débiles, guiar discusiones, dar soporte didáctico, etc.

Tomando como referencia el concepto del modelo causa-efecto, se presenta gráficamente el plan de seguridad informática propuesto en la EUPG-UNFV, lo que permite visualizar en una sola figura todas las causas asociadas con la seguridad y sus relaciones. No obstante, esta herramienta sirve de guía para cumplir con los objetivos propuestos y así fortalecer la seguridad informática, aumentando la eficacia y eficiencia en los servicios. Por tanto, el modelo esquematizado es explicado detalladamente en el tercer capítulo de la presente investigación, y permite visualizar gráficamente todas las causas sobre el efecto propuesto.

En términos generales, la aplicación del diagrama se orienta al proceso de mejoramiento de la seguridad informática, el cual se usa como una herramienta de educación y de entrenamiento para el personal involucrado (se presenta en el anexo 1 del presente trabajo de investigación).

II. DESCRIPCIÓN DE LA METODOLOGÍA DEL DESARROLLO

*El que nunca nada hace,
nunca se equivoca.*

Anónimo

2.1. El problema de la investigación

Actualmente, en la EUPG-UNFV no existe un sistema de seguridad informática que permita enfrentar el problema de seguridad de la información que se procesa en la institución. La falta de políticas, estrategias y acciones configuran uno de los problemas más graves que confronta la Escuela de Posgrado en lo que se refiere a la protección de su información frente a las amenazas externas e internas. Por tanto, se hace imperiosa la necesidad de formular un plan de seguridad informática que contemple todas las carencias antes expuestas, de manera sistemática. La presente investigación pretende resolver este problema.

Objetivos de la investigación

El objetivo general de la investigación es probar la eficiencia de un plan de seguridad informática propuesto para la EUPG-UNFV, el mismo que se logrará con los siguientes objetivos específicos:

- Hacer el diagnóstico del sistema de seguridad informática actual.
- Elaborar un plan de seguridad informática sobre la base del diagnóstico de la situación actual.
- Probar la eficiencia del plan de seguridad informática propuesto.

2.2. Tipo-diseño de la investigación

La presente investigación es de tipo transversal, en el sentido según el que se recogerá la información en un período y no a través del tiempo; es decir, en un momento único. Es de tipo descriptiva comparativa, porque los resultados de una primera fase serán comparados con los resultados de una segunda fase.

2.3. Metodología del desarrollo de la investigación

El estudio se ha desarrollado en dos fases: la primera está orientada a conocer el estado actual a modo de diagnóstico de la seguridad informática, mediante la aplicación de una encuesta a todos los empleados de la EUPG-UNFV involucrados en el tratamiento de la información. Después de este diagnóstico, y apoyado en estándares internacionales, se formula el plan de seguridad informática para la EUPG.

En la segunda fase, se somete el plan formulado a la opinión de los expertos en sistemas de información de la institución, y se recoge a través de una encuesta aplicada solamente a ellos su apreciación técnica. De esta manera se probará la eficiencia del plan propuesto.

2.4. Hipótesis de la investigación

Se logrará mejorar la seguridad informática en la EUPG-UNFV, mediante la formulación adecuada de un plan de seguridad informática.

2.5. Variables de estudio

En el cuadro 2 se listan las variables y los indicadores que permiten desarrollar y demostrar la hipótesis planteada de manera adecuada.

2.6. Variables de estudio

Cuadro 2. Variables e indicadores

Variable dependiente	Factores	Indicadores	Medida
Seguridad informática	> Recursos Tecnológicos	Hardware Software	Ordinal Likert > Excelente > Bueno > Regular > Mala > Muy mala
	> Sistemas de Información	Integridad Confidencialidad Disponibilidad Vulnerabilidad	
	> Amenazas Informáticas	Externas Internas	
	> Desastres	Naturales Inundación Fuego	
Variable independiente	Factores	Indicadores	Medida
Plan de seguridad informática propuesto.	> Lógica	Identificación de usuarios Autenticación Gestión de password Segregación de funciones	Ordinal Likert > Excelente. > Bueno > Regular. > Mala. > Muy mala.
	> Comunicaciones	Topología de red Conexiones externos Configuración lógica de la red Correo electrónico Antivirus Firewall Ataques de la red	
	> Aplicaciones	Software Seguridad de la base de dato Control de aplicaciones en las computadoras Control de datos en las aplicaciones Ciclo de vida de las aplicaciones	
	> Física	Equipamiento Control de acceso físico al área de Informática Control de acceso a equipos Dispositivos de soporte Estructura del edificio Cableado estructurado	
	> Administración del centro de procesamiento de datos	Administración del área de Informática Capacitación Backup Documentación	
	> Auditorías y revisiones	Revisión del sistema Responsabilidades de los encargados de seguridad Auditoría de control de acceso a los sistemas Auditoría de redes	
	> Plan de contingencia	Plan de administración de incidentes Backup de equipamiento Estrategias de recuperación de desastres	

2.7. Población y muestra

La población está conformada por todos los empleados usuarios que manipulan permanentemente los sistemas de información en la EUPG-UNFV: los expertos (20) y los no expertos (18) en informática. En total son 38 empleados.

Para la muestra no fue necesario realizar una estimación del tamaño de la misma, porque participaron todos los usuarios; de esta manera, el error por evaluación del tamaño del modelo es cero, dado que participan todos los usuarios. Sin embargo, es preciso detallar los criterios asumidos en cada una de las fases:

Fase 1. Para el diagnóstico del estado actual del sistema de seguridad informática participaron 38 usuarios. Todos trabajan de manera permanente con los sistemas de información de la EUPG-UNFV.

Fase 2. En esta fase de validación del plan participan 20 usuarios expertos y calificados en el uso y manejo de las tecnologías de información, cuyas características de inclusión fueron las siguientes:

- Personas vinculadas con el uso permanente en los sistemas de información.
- Con formación calificada en informática a nivel profesional.
- Que estén trabajando en la EUPG-UNFV por lo menos 5 años, de manera permanente.

2.8. Técnicas estadísticas

Se calculó el alpha de Cronbach, con la finalidad de obtener y ver los resultados de los indicadores de cada factor de las variables de la presente investigación. Este cálculo permite apreciar la fiabilidad y la validez de la escala de medición de las preguntas formuladas.

Se calculó la media aritmética de las respuestas de la encuesta aplicada, la cual permite apreciar el puntaje total de los resultados de cada indicador por cada factor de las variables de la presente investigación, lo que permite medir la eficiencia de los factores de las variables correspondientes.

De la misma forma se calculó la chi cuadrada de los resultados de la encuesta aplicada, la cual permite probar la hipótesis planteada y demostrar la eficiencia del plan propuesto.

Cabe mencionar que los cálculos se desarrollaron utilizando el *software* estadístico SPSS, lo que permite generar cuadros y gráficos de manera precisa y adecuada.

2.9. Instrumentos utilizados

Los instrumentos que se utilizaron en la investigación están relacionados con las técnicas que se detallan en el siguiente cuadro.

2.9. Instrumentos utilizados

Cuadro 3. Técnicas e instrumentos

Técnicas	Instrumentos
<ul style="list-style-type: none"> ▪ Análisis de contenido ▪ Análisis de la documentación 	<ul style="list-style-type: none"> ▪ Software de análisis (SPSS) ▪ Cuadros comparativos ▪ Gráficos
<ul style="list-style-type: none"> ▪ Encuesta 	<ul style="list-style-type: none"> ▪ Cuestionario para el diagnóstico del plan de seguridad actual. ▪ Cuestionario para evaluar la eficiencia del plan de seguridad propuesto

La encuesta se aplicó en dos etapas: la primera se utilizó para la etapa de diagnóstico y la segunda para probar la eficiencia del plan propuesto. Los ítems fueron de tipo cerrados y con preguntas alternativas filtros que impiden que los encuestados falseen sus respuestas o que quede alguna pregunta sin contestar. La misma se aprecia en los cuadros 4 y 5 de análisis de confiabilidad del instrumento de la encuesta, basadas en los ítems estandarizados.

Para demostrar la validez de la encuesta aplicada, se desarrolla la escala de confiabilidad. La misma es analizada en dos fases: la primera consiste en la fiabilidad de la etapa de diagnóstico de la seguridad informática actual. La segunda fase radica en análisis de la eficiencia del plan propuesto. Los resultados se presentan a continuación.

a. Escala de medición del diagnóstico. La escala estuvo compuesta por 15 preguntas, con cinco alternativas de respuestas cada una. Previa a la recopilación de la información se dio una breve información acerca de los temas que se estaban evaluando, para que posteriormente complementen la escala de manera individual; asimismo, esta escala tiene cuatro factores: recursos tecnológicos, sistemas de información, amenazas informáticas y desastres. Sus resultados se presentan en el siguiente cuadro.

Cuadro 4. Fiabilidad de la escala para la etapa de diagnóstico

Diagnóstico del sistema de seguridad informática actual	Ítems	Nº ítem	Fiabilidad Alpha
Recursos tecnológicos	1,3,8,10,11,15	6	0.879
Sistemas de información	2,4,7,9	4	0.876
Amenazas informáticas	5,12	2	0.854
Desastres	13,6,14	3	0.865
TOTAL		15	0.879

En general, se puede apreciar que la escala muestra una garantía en lo que respecta a la fiabilidad basada en la consistencia interna y evaluada con el coeficiente alpha de Cronbach. Los coeficientes para los factores, como la escala total, superan el $\alpha = 0,800$.

- b. Escala de medición del plan de seguridad informática propuesto. Siguiendo la metodología de Rensis Likert, se construyó una escala de medición global, que comprende 33 preguntas, cada una de ellas tiene alternativas de respuesta (excelente, bueno, regular, mala y muy mala); asimismo, esta escala tiene siete factores: seguridad lógica, en comunicaciones, aplicaciones, física, administración del centro de procesamiento de datos, auditorías y revisiones, plan de contingencias. Por otro lado, se ejecuta la fiabilidad de la escala de medición como soporte científico del instrumento (ver cuadro 5).

Cuadro 5. *Fiabilidad de la escala para la eficiencia del plan propuesto*

Plan de seguridad informática propuesto	Items	Nº Item	Fiabilidad Alpha
Seguridad lógica	1,5,9,14	4	0.879
Seguridad en las comunicaciones	2,6,12,17,21,25,30	7	0.779
Seguridad de las aplicaciones	7,11,16,20,24	5	0.901
Seguridad física	4,8,18,23,27,28	6	0.876
Administración del centro de procesamiento de datos	10,15,22,32	4	0.854
Auditorias y revisiones	13,19,26,33	4	0.765
Plan de contingencia	3,29,31	3	0.865
TOTAL		33	0.879

Como se puede observar, la escala global y el factor de seguridad muestran evidencias importantes de fiabilidad con el coeficiente alpha de Cronbach (todas superan el 0,755).

III. PLAN DE SEGURIDAD INFORMÁTICA EN LA EUPG-UNFV

Pide, y se te dará; busca, y lo hallarás.

Evangelio según San Mateo 7:7

Pondera la situación y luego actúa.

Sun Tzu (*El arte de la guerra*)

3.1. Análisis de situación actual de la seguridad informática

El análisis consiste en obtener información referente a la situación actual de la seguridad informática en la EUPG-UNFV, y tiene como finalidad identificar las vulnerabilidades de la seguridad, la misma que sirve como medio para definir adecuadamente un plan de seguridad informática en la institución mencionada.

En esta perspectiva Iturbie F. (2005) sostiene que para implementar un sistema general de seguridad informática se debe “[...] formular e implementar un plan de seguridad que identifique las acciones, responsabilidades y prioridades, capaces de detectar y dar respuesta a los incidentes de la seguridad informática”.

En este contexto, el desarrollo del análisis de la seguridad informática actual se agrupa en siete factores:

- Seguridad lógica.
- Seguridad en las comunicaciones.
- Seguridad de las aplicaciones.
- Seguridad física.
- Administración del centro de procesamiento de datos.
- Auditorías y revisiones.
- Plan de contingencia.

Para desarrollar apropiadamente el análisis de la seguridad informática actual, se establecieron los siguientes aspectos:

a. Metodología aplicada. La metodología de análisis de la seguridad informática actual se basa en el desarrollo de las siguientes aspectos:

- Análisis de fuentes de datos y recopilación de información.
- Generación de las encuestas.
- Recolección de documentos referentes a la seguridad informática.
- Reconocimiento del ambiente de trabajo.
- Análisis de los factores de riesgos.

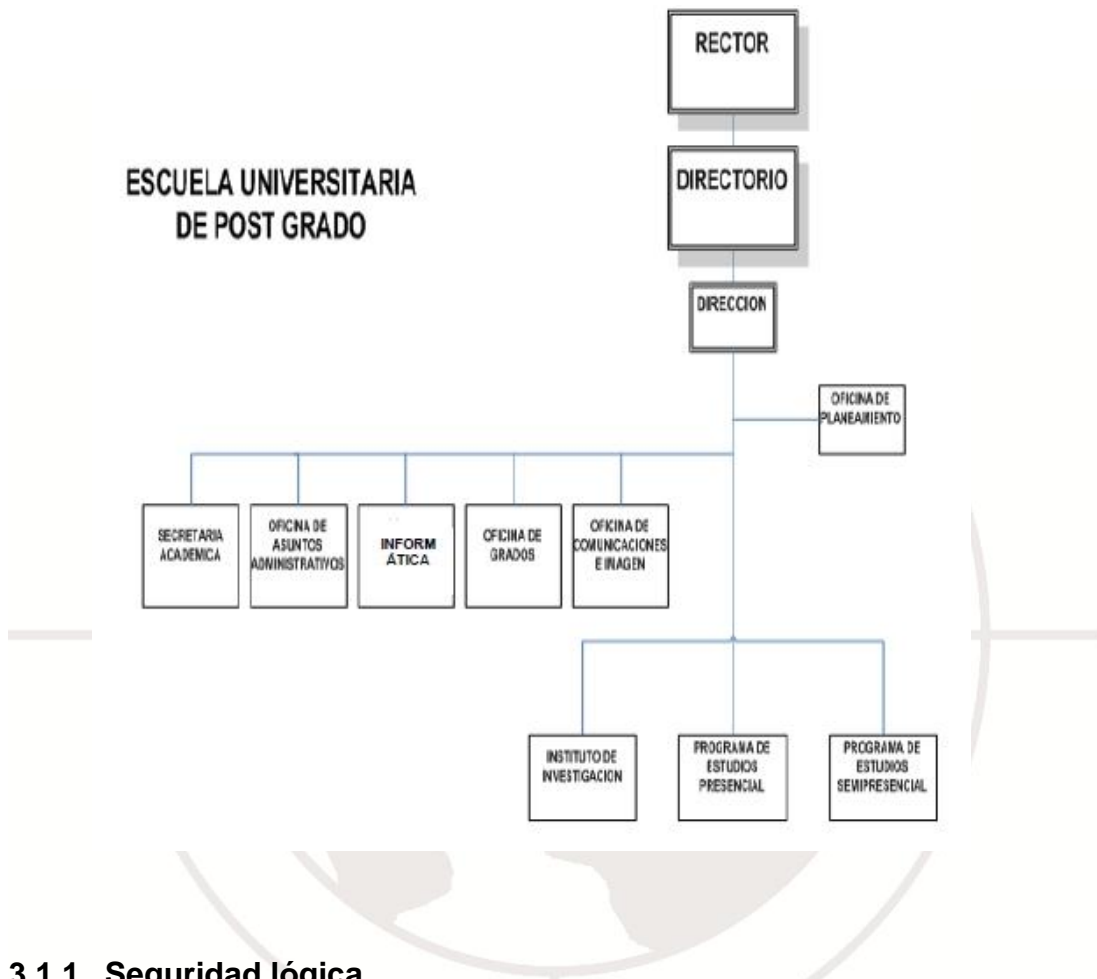
Normativas. Para ejecutar el análisis de manera adecuada se tomaron como referencia las siguientes normas de seguridad:

- ISO (International Standard Organization) “Estándar de Seguridad ISO 27001/ISO17799:2005” .
- Norma Técnica Peruana NTP-ISO/IEC 17799:2007 EDI. “Tecnología de la información. Código de buenas prácticas para la gestión de la seguridad de la información.”

b. Informe de relevamiento. La EUPG-UNFV está ubicada en Jr. Camaná 1014-Cercado de Lima, y promueve la formación de recursos humanos en estudios de maestría y doctorado en cinco áreas del conocimiento: ciencias de la salud, ciencias de la empresa, humanidades y ciencias sociales, derecho y ciencias políticas, ingeniería y ciencias básicas, las que se dividen en 64 especialidades de maestría y 17 especialidades de programas de doctorado; en consecuencia, alberga una población estudiantil de 8 mil alumnos, 402 docentes y 38 empleados.

En el siguiente gráfico se presenta la estructura orgánica de la Escuela Universitaria de Postgrado de la Universidad Nacional Federico Villarreal.

Gráfico N.º 1. Organigrama estructural



3.1.1. Seguridad lógica

La evaluación de la seguridad lógica consiste en analizar los controles de accesos de los usuarios a las plataformas de procesamiento informático y a los datos que gestionan frecuentemente, con el fin de identificar las vulnerabilidades que obstaculizan la confidencialidad, la integridad y la disponibilidad de la información. No obstante, la evaluación referente a la seguridad lógica consiste en los aspectos mencionados a continuación.

Identificación de usuarios

a. **Procedimiento para dar de alta a los usuarios:** cuando un usuario nuevo ingresa a la EUPG-UNFV, el área de Secretaria Administrativa toma sus datos, dando de alta su legajo; sin embargo, no existe un procedimiento formal para realizar estas tareas. Si este usuario requiere del sistema informático, se hace el pedido al área de Informática, la cual le asigna un equipo de cómputo con los accesos necesarios. Los datos que se ingresan en la cuenta de los usuarios son:

- ID de usuario.
- Password.
- Nombres y apellidos completos.
- Grupo al que pertenece, según al área de la EUPG-UNFV que fue asignada. Se observó que en algunos casos este campo permanece vacío, permitiendo que el usuario acceda a todos los menús del sistema.
- Fecha de expiración del *password*. Este campo no se completa, permitiendo que nunca se actualice la contraseña.
- No existe un contador de intentos fallidos. Por tanto, el usuario puede ingresar cuantas veces desea.
- Autorización de imprimir. No todos los usuarios pueden imprimir los datos del sistema.

b. **Procedimiento para dar de baja a los usuarios:** las cuentas de los usuarios no se eliminan del sistema ni se deshabilitan. De esta forma, los datos de los empleados dados de baja quedan almacenados, la misma puede ser usada por el ex empleado para vulnerar la información.

Procedimiento para dar mantenimiento a las cuentas de los usuarios:

no se lleva a cabo ninguna revisión periódica ni control sobre el buen funcionamiento de las cuentas de los usuarios ni sobre los permisos que tienen asignados.

c. **Procedimiento para dar permiso a los usuarios:** solo pueden interactuar con los datos de los módulos que tienen permiso. No existe en el sistema informático una lista de control de acceso que se utilice para identificar los tipos de permiso que tiene cada usuario con respecto a los datos. Al no existir esta lista de control, resulta complicado identificar qué datos pueden ser modificados por los usuarios. Tampoco se tiene en cuenta la restricción horaria del uso de los recursos tecnológicos. De la misma forma, no se considera restricción física sobre la máquina y la ubicación desde la que pueda ingresar un usuario a los sistemas de información.

d. **Procedimiento para identificar la inactividad del usuario:** si el usuario permanece un período de tiempo logeado sin actividad alguna, el sistema no ejecuta ninguna acción. Si las cuentas de usuarios permanecen varios días sin actividad, por licencias o por vacaciones, no pasan a un estado de suspensión; es decir, se mantienen activas.

e. **Cuentas de usuario:** los usuarios del área de Registros no son identificados en forma personal, sino que usan todos los mismos usuarios y contraseña para ingresar al servidor. Sin embargo, utilizan usuarios y contraseñas personales para acceder a los sistemas de información.

Los módulos del sistema solo permiten hacer consultas a la base de datos (listado de los docentes, alumnos, historial de notas, historial de pagos, etc.). Los usuarios del sistema pueden tener abiertos al mismo tiempo todos los menús a los que están autorizados y varias sesiones del mismo menú.

No se hacen restricciones en cuanto a la cantidad de sesiones que los usuarios pueden utilizar simultáneamente.

En la EUPG-UNFV existen dos personas con perfil de administrador. Cada una de ellas tiene su cuenta con un *password* personal, pero, para fines prácticos, los dos conocen todos los *password* de las demás cuentas, ya que no hay una clara definición de tareas.

Autenticación

En la pantalla de ingreso del sistema de información se muestran y se ingresan los siguientes datos:

- Nombre de usuario.
- *Password*.

Cuando un usuario ingresa su *password* al sistema, aparecen asteriscos en lugar de mostrar el dato que está siendo ingresado. Una vez que algún usuario ha logrado ingresar al sistema de información, aparecen en la pantalla las iniciales del usuario y la fecha de ingreso. En cuanto al control de acceso a los sistemas BIOS de los equipos de cómputo, no existe, de manera que al momento del encendido cualquier otra persona podría modificar las opciones de la configuración.

Gestión del *password*

En cuanto a la gestión del *password* se realizan los siguientes aspectos:

- a. **Generación:** los *password* son generados en forma manual, sin procedimientos automáticos. Como restricción se considera una longitud máximo de 10 caracteres, numéricos o alfanuméricos.

b. **Cambios:** los realiza el responsable en forma manual desde la tabla de usuarios de la base de datos, aunque generalmente los *password* no son actualizados, permaneciendo iguales por largos períodos.

Segregación de funciones

No existe ningún régimen de separación de tareas para evitar que un solo empleado realice la totalidad de una operación. Tampoco se lleva a cabo ninguna rotación del personal, solo se varían las tareas cuando un empleado toma sus vacaciones o cuando sale de licencia.

3.1.2. Seguridad en las comunicaciones

La evaluación de la seguridad en las comunicaciones consiste en datos transmitidos, dispositivos usados durante la transmisión y documentación necesaria para la realización eficiente e ininterrumpida de la comunicación. No obstante, la evaluación consiste en los siguientes aspectos:

Topología de la red

La topología de la red en la EUPG-UNFV es de tipo estrella, lo que permite a las estaciones de trabajo conectarse directamente a un punto central. Está diseñada por las siguientes razones:

- Porque es fácil para implementar y ampliar, incluso en grandes redes.
- Adecuada para redes temporales (instalación rápida).
- No tiene problemas con colisiones de datos, ya que cada estación tiene su propio cable al *switch* central.

a. **Componentes de la red:** la red informática se compone de los siguientes equipamientos:

- 50 PC distribuidas en todas las oficinas.
- 1 servidor IBM xSeries 236, para aplicaciones y bases de datos.
- Cables UTP categoría 6.
- Telefonía IP.
- Patchera conectada al *switch* central de 64 entradas para PC.
- 1 *switch* CISCO 1900 de 64 entradas.
- 2 *hubs* de 1000 MB.
- Canaletas para tendido de cableado.

b. Descripción de la red

- UTP en conexiones internas: el cableado está realizado con UTP categoría 6.
- Canaletas: el cableado ha sido realizado por medio de canaletas; esto permite proteger los cables de red de cualquier contingencia.

Conexiones externas

Para la conexión a Internet se utiliza un proxy Wingate, el cual está configurado de manera estricta, de forma que solo tiene conexión al exterior un rango de direcciones IP definido por el responsable. No existe documento alguno que señale qué equipos de cómputo tienen permiso de salida al exterior. La ausencia de este documento puede repercutir en la seguridad informática de la EUPG-UNFV.

Configuración lógica de la red

Todas las máquinas están conectadas a la red: desde cualquiera de ellas se puede acceder a los recursos de las otras.

Recursos compartidos. El entorno de red de cada uno de los usuarios está configurado para que los usuarios no vean toda la red, sino solo una parte de la misma, pero no hay ninguna medida tomada para que un usuario no comparta sus datos con otro. Las carpetas compartidas del servidor se pueden visualizar, debido a que están en el área compartida del disco, sin restricción alguna.

En el servidor de aplicaciones se comparte una carpeta a la que los usuarios de registros tienen acceso, porque utilizan una carpeta compartida que contiene el sistema de gestión académico desarrollado en FoxPro para DOS. También el responsable que realiza la copia de seguridad tiene acceso, porque cuenta con una carpeta donde realiza en forma diaria una copia del sistema transaccional, para luego transferirla a un equipo adicional.

Correo electrónico

En la EUPG solo existen tres cuentas de correo, ya que muchos de los empleados no necesitan de este servicio. Las mismas son utilizadas para recibir información de los pagos realizados por los alumnos en el Banco de Comercio, una cuenta para el proceso de admisión y otra para el uso personal del director de la EUPG.

a. Alta de usuarios de correo electrónico: si un usuario requiere de una cuenta de correo electrónico, la solicita a Dirección, que gestiona al Centro de Cómputo Central de la UNFV.

b. Opciones de configuración: se ejecutan los siguientes aspectos:

- Antivirus: no se encuentra configurado para chequear el *mail*, inspeccionando todos los mensajes entrantes y salientes.
- Prioridades: no se implementa un sistema de prioridades de los mensajes.

Cabe mencionar que las opciones de configuración del correo electrónico se realizan a las cuentas generadas por la UNFV, debido a que cumplen para los intereses de la EUPG, mas no a las cuentas personales de cada usuario.

Antivirus

En la EUPG-UNFV existen problemas por contagio de virus en las PC, infectadas por los mismos usuarios utilizando discos magnéticos, los cuales se erradican con el uso del antivirus NOD32.

- a. Herramientas: en la EUPG-UNFV disponen del NOD32 para las PC. Para el servidor hay una versión del NOD32 que está ejecutándose continuamente. Es importante mencionar que el antivirus utilizado es el demo (o prueba del producto) NOD32, que se obtiene en forma gratuita de Internet y que vence cada 30 días.
- b. Actualización: se realiza por medio de carpeta compartida. Los usuarios son los responsables de actualizar sus propios antivirus, pero no se hacen chequeos ocasionales para ver si se han actualizado correctamente.
- c. Escaneo de virus: no se hacen escaneos periódicos buscando virus en los servidores ni en las PC. No hay ninguna frecuencia para realizar este procedimiento, ni se denominó a ningún responsable.

Firewall

El firewall se encuentra instalado y actúa a modo de filtro, bloqueando o permitiendo determinadas conexiones y transmisiones de datos desde o hacia Internet; es decir, actúa como una barrera entre la red y las computadoras de las estaciones de trabajo. Cabe mencionar, que el *software* es del producto del McAfee Personal Firewall Plus.

La configuración de la misma es realizada de manera que prohíbe los servicios que no son necesarios, habilitando lo necesario, esto en base a una política que discrimina tres clases de paquetes de la red:

- Los paquetes entrantes a la red.
- Los paquetes salientes de la red.
- Los paquetes en tránsito.

Cabe mencionar que nunca se hicieron pruebas de escaneos ni intentos de intrusión o de escucha. Tampoco se hace un testeo periódico de puertos o de los servicios que están habilitados.

Ataques a la red

La EUPG-UNFV no dispone de herramientas destinadas exclusivamente para prevenir los ataques a la red, debido a que no se han presentado grandes problemas hasta el momento.

- a. Sistema de detección de intrusos: en la EUPG-UNFV no se han registrado intrusiones, solo por medios magnéticos por parte de los usuarios.

Sniffing: En la EUPG-UNFV la red se encuentra segmentada a través de un *switch*, que, efectivamente, reduce la posibilidad de *sniffing*, ya que direcciona los paquetes de red de acuerdo al destino que tienen. Así se evita que el paquete viaje a través de toda la red o por destinos innecesarios.

3.1.3. Seguridad en las aplicaciones

La evaluación de la seguridad en las aplicaciones consiste en analizar la entrada y la salida de la información, la integridad de las bases de datos y la existencia y el uso de la documentación necesaria para su funcionamiento adecuado. No obstante, la evaluación en las aplicaciones consiste en los siguientes aspectos:

Software

En la EUPG-UNFV hay un servidor con sistema operativo Windows Server 2003, el 95 % de los equipos de cómputo usa Windows XP Profesional, y el 5 % usa el sistema operativo Windows 98. Las aplicaciones estaban desarrolladas en FoxPro para DOS. Actualmente se están migrando a Visual Basic. Hasta el momento, esta migración se encuentra en el 90 %, los módulos del sistema se encuentran funcionando desde hace dos años.

Seguridad de la base de datos

Como base de datos se utiliza el lenguaje SQL Server 2000, el cual permite administrar datos de manera adecuada. Cuenta con un control que restringe el acceso a ciertos datos críticos en las aplicaciones propias de la EUPG-UNFV, pero no existe una clasificación formal.

Tampoco se realizan controles de acceso lógico a las carpetas donde se almacenan los archivos indexados, ya que estos archivos están en una carpeta del servidor no compartida para el resto de la red, a lo que se agregan los controles de seguridad física del servidor. Cabe señalar que los recursos del servidor están en uso en un 30 %, el resto se encuentra libre. El porcentaje es alto debido a que no se hace el uso adecuado del servidor.

Control de aplicaciones en las computadoras

No existen estándares definidos ni procedimientos, tampoco documentación respecto a la instalación y actualización de la configuración de las PC; solo hay una instalación básica de alguna versión del Windows, Internet Explorer y NOD32. En el caso de que una PC presente errores en su configuración, se formatea según el caso y requerimiento del usuario, pero no se deja constancia de la operación ni fecha de la modificación.

Tampoco se realizan actualizaciones de los programas instalados, como el Internet Explorer y el Microsoft Office, Service Packs, ni se buscan nuevas versiones.

Solamente el responsable asignado por el jefe del área de Informática tiene acceso para realizar instalaciones en las PC, aunque para los usuarios no existen restricciones con respecto a la instalación de programas, pues pueden bajar de la web cualquier aplicación e instalarla en su PC sin ningún control sobre las licencias ni autorización previa. Esto se debe a que, para controlar problemas de licencias, virus o programas no permitidos, no hay ninguna herramienta en uso, ni mucho menos se realiza auditoría interna.

Cuando se hace un cambio en la configuración del servidor, se guardan copias de la configuración anterior y posterior al cambio, pero no se documentan los cambios que se realizan ni la fecha de las modificaciones.

Control de datos en las aplicaciones

En las aplicaciones no se controlan los datos de entrada ni de salida, lo cual hace vulnerable la integridad, la confidencialidad y la disponibilidad de la información que manejan diariamente los usuarios.

Ciclo de vida de las aplicaciones

La EUPG-UNFV cuenta con aplicaciones propias desarrolladas para cada uno de los procesos, las cuales no siguen una metodología estandarizada. Durante el ciclo de vida no se priorizan los requisitos de seguridad del sistema, debido a la urgencia de cada proceso.

- a. Análisis: no se realizó un relevamiento formal para el desarrollo de los sistemas de información. Los programadores tenían noción de los requerimientos y necesidades de los usuarios por el conocimiento del sistema anterior.
- b. Desarrollo: la implementación del sistema de información se ha desarrollado en Visual Basic.
- c. Prueba: para el testeado del sistema se generaron casos de pruebas donde se definen tablas con valores de entrada al sistema, realizándose pruebas de integración de los módulos. Los resultados obtenidos en las pruebas no son documentados.
- d. Instalación y modificaciones: una vez hecha la instalación, las únicas modificaciones se realizaron según la necesidad de cada proceso, pero no se llevó a cabo ningún control de versiones ni gestión de configuración de las modificaciones.
- e. Documentación: no se cuenta con diagramas ni documentación de los sistemas; es decir, no existen manuales técnicos de usuario.

3.1.4. Seguridad física

La evaluación de la seguridad física consiste en analizar los equipos de cómputo, dispositivos, medios de almacenamientos y las personas que conforman el sistema informático. No obstante, la evaluación consiste en los siguientes aspectos:

Equipamiento

a. Característica del servidor: en la EUPG-UNFV existe un servidor IBM Serie 236 comprado en el año 2005, con las siguientes características:

- Dos procesadores Intel Xeon de 3.0 GHz de velocidad.
- Dos fuentes (redundantes).
- Dos tarjetas de red.
- Memoria 1 GB de RAM.
- Dos discos con tecnología SCSI-HOT-SWAP con 80 GB de capacidad cada uno.

b. Características de las PC: la EUPG-UNFV en su totalidad posee alrededor de 130 PC, de las cuales 80 se encuentran en el laboratorio de cómputo y 50 en las oficinas administrativas. El 75 % de las PC es de marca DELL, el 20 % es de marca IBM, y el 5 % son compatibles.

Las de marca DELL y las IBM funcionan con sistema operativo Windows XP Professional, y tienen un disco duro de 80 GB y 512 MB de RAM. Las compatibles están con sistema operativo Windows 98 y tienen un disco duro de 20 GB y 64 MB de RAM.

Control de acceso físico al área de Informática

En el momento de la instalación del área de Informática no se efectuó un análisis de costo-beneficio para determinar qué controles de acceso físico sería necesario implementar.

La EUPG-UNFV cuenta con guardias de seguridad las 24 horas del día, los que están ubicados en el interior y exterior de la misma; sin embargo, no existen tarjetas magnéticas de entrada ni llaves cifradas en ningún sector del edificio.

Control de acceso a equipos

Todas las máquinas disponen de disqueteras y lectoras de CD, aunque el 90 % de los usuarios no las necesitan. Solo se utilizan para realizar alguna instalación del *software*. Muchas veces los usuarios solo las utilizan para escuchar música.

Estos dispositivos están habilitados y no hay ningún control sobre ellos. No se hacen controles automáticos de virus ni se prohíbe el booteo desde estos dispositivos. Nunca hubo robo de datos usando medios externos, solo fue necesario hacer bloqueos de las impresoras para restringir los datos de salida del sistema, previniendo posibles robos electrónicos.

El gabinete donde se ubica el *switch* central, por medida de precaución, está cerrado con llave, para evitar que el personal de limpieza o cualquier otra persona desconecte los cables de la red o lo conecte a otros puertos libres que hay en estos dispositivos. No se realizan controles periódicos sobre los dispositivos de *hardware* instalados en las PC, de manera que alguien podría sacar o poner otros. Una vez que se ha completado la instalación de algún equipo, el responsable no realiza chequeos rutinarios o periódicos, solo revisa cuando un equipo no funciona adecuadamente, o por un problema reportado por el usuario.

Dispositivos de soporte

La EUPG-UNFV dispone de los siguientes dispositivos para soporte del equipamiento informático:

- Aire acondicionado: la temperatura se mantiene en 20 °C. Existe un equipo adicional de aire acondicionado solo para el área de Informática, con el fin de mantener esta temperatura en verano.
- Generador de energía: la EUPG-UNFV cuenta con un generador de energía.
- UPS (Uninterruptible Power Supply): en el área de Informática existe un UPS en serie que mantiene al servidor funcionando por una hora.
- Pozo a tierra: existe uno; sin embargo, no está operativo.

Estructura del edificio

Cuando se construyó el edificio no se tomó en cuenta el diseño del área de Informática, que se encuentra ubicada en el segundo piso del edificio, que se instaló sin pensar en su futuro crecimiento. Actualmente sus instalaciones se encuentran relativamente incómodas para desarrollar sus funciones adecuadamente.

Cableado estructurado

La instalación del cableado fue realizada por la empresa Telefónica, y se implementó un cableado estructurado de tipo estrella, brindándole a la EUPG-UNFV una garantía para su desarrollo.

En todo el trayecto del cableado se tuvo en cuenta la distancia mínima necesaria entre cables para no provocar interferencias, daños o cortes. Además, no hay distancias grandes recorridas con cables UTP.

Para evitar grandes recorridos del cableado, se utilizan dos *hub* en las áreas de Contabilidad y en la oficina de Investigación.

En el *switch* central hay un puerto dedicado para cada máquina, y puertos que están libres para una posible ampliación de la red. Además, hay dos *hub* que llegan al *switch*, los cuales conectan 5 y 7 máquinas, respectivamente. Para que no haya interferencias se utilizó cableado UTP categoría 6. Los cables en la patchera están numerados, de manera que se los puede identificar fácilmente. En la parte posterior se encuentran instalados los siguientes conectores, que no todos son utilizados:

- Un tomadato.
- Un tomadato de teléfono.

Todas estas líneas no producen interferencias debido a la calidad de los cables de red.

3.1.5. Administración del Centro de Procesamiento de Datos

La evaluación del Centro de Procesamiento de Datos consiste en analizar la existencia de los recursos físicos, lógicos y humanos necesarios para el desarrollo apropiado de la institución. No obstante, la evaluación consiste en los siguientes aspectos:

Administración del área de Informática

Se evaluó la correcta organización y administración del área de Informática, así como la asignación de tareas y responsabilidades del personal que la conforma, a fin de que esta brinde condiciones óptimas de operación que posibiliten un ambiente adecuado de control y permitan mejorar la disponibilidad de sus servicios, de acuerdo con las normas existentes que regulan esta actividad.

- a. Responsabilidad del equipo de sistemas: no hay responsabilidades puntuales asignadas a cada empleado, tampoco hay un encargado de la seguridad. Existe un jefe del área de Informática: él es el que planifica y delega las tareas a los empleados del área. Existe un empleado que realiza el mantenimiento de la página web y de los equipos de cómputo, y que también realiza copias de seguridad, pero no genera documento alguno sobre el cambio realizado.
- b. Mantenimiento: cada vez que los usuarios necesitan asesoramiento o servicios del área de Informática, se comunican directamente con el personal responsable, pero no queda ninguna constancia de las tareas desarrolladas por los empleados del área ni de las solicitudes de los usuarios.
- c. Mantenimiento preventivo: en este momento en el área de Informática no se desarrolla ningún mantenimiento preventivo, al no contar con una persona que se dedique a esto.
- d. Clasificación de datos y *hardware*: los equipos no han sido clasificados formalmente según su prioridad, aunque se puede identificar que las máquinas que están en el sector de atención al público tienen mayor prioridad que el resto.

Rótulos: no hay procesos para rotular, manipular y dar de baja un equipo, sus periféricos o los medios de almacenamiento, solo las licencias de *software* están registradas. Las máquinas y dispositivos no se identifican entre ellas, aunque hay un inventario de la cantidad de máquinas que existen, pero no tiene detalles suficientes.

e. Instaladores: los instaladores de las aplicaciones utilizadas en la EUPG-UNFV se encuentran en sus CD originales, y no disponen de instaladores en disquetes. Los instaladores de uso más frecuente, como los NOD32, se actualizan mensualmente obteniendo el demo desde la web en forma gratuita, y la instalación se realiza por medio de carpeta compartida. Otros igualmente utilizados, como las distintas versiones de Windows, se ejecutan desde copias de los CD originales, para evitar posibles daños en los discos originales.

f. Licencias: como ya se ha mencionado, en el área de Informática se mantiene un registro de los números de licencia de las aplicaciones instaladas en las PC y en el servidor. Los programas de los que se dispone licencias son los siguientes:

- Windows 98 y XP Professional en las PC.
- Microsoft Office 2003 en las PC.

El resto de las aplicaciones son propias, por lo que no necesitan de licencias, o son *freeware*, como el Acrobat Reader, el Winrar, etc.

Capacitación

No se realizan campañas de capacitación a los usuarios. Cuando ingresa un empleado nuevo a la EUPG-UNFV, se le enseña el uso del sistema, más no se le capacita sobre la importancia de la seguridad informática. Mucho menos se le capacita sobre las nuevas tecnologías que existe en el mercado.

Backup

Se realizan copias de datos, de tal forma que ellas permitan restaurar la información, pero no existe procedimiento alguno para realizarlas. Los aspectos que se realizan son los siguientes:

a. Backup de datos del servidor: cuando se hace un cambio en la configuración del servidor, se guardan copias de las configuraciones anteriores, pero no se documentan los cambios que se realizan ni la fecha de estas modificaciones. Las copias de las configuraciones se almacenan en un equipo adicional en la misma área de Informática, pero no existe ningún procedimiento formal para la realización ni la recuperación de los *backup*. Además, no se realizan chequeos para comprobar que el funcionamiento sea el correcto.

Por otro lado, la copia de seguridad se hace diariamente al inicio del día. La hora es relativa pues puede ser entre 7:40 a. m. y 8:15 a. m. Esta frecuencia de ejecución se realiza por precaución, debido a que no existen políticas de seguridad. Cabe mencionar que la copia de seguridad solo se realiza a la base de datos de Gestión Académica en forma manual. Una vez generada esta copia, el responsable realiza la transferencia a una máquina adicional en la misma área de Informática.

Es importante manifestar que no existe un responsable designado para realizar los *backup*, aunque generalmente los hace solo una persona, pero no hay políticas de recuperación ni chequeos periódicos de este proceso.

b. Backup de datos en las PC: los usuarios realizan sus propios *backup* de los datos almacenados en sus máquinas, ya que estos datos son propiedad de ellos. Usualmente no los realizan debido al desconocimiento sobre la importancia de la información. Los usuarios han sido instruidos para almacenar la información generada en una carpeta de la unidad “D” de la máquina que utilizan, pero no realizan revisión alguna para comprobar la integridad de los datos.

c. Backup de la página web: el responsable realiza un *backup* de la página web completa en una PC del área de Informática, pero sin una frecuencia preestablecida.

d. Protección de los *backup*: las copias de seguridad no están protegidas con ningún control de acceso. Esta situación puede resultar peligrosa ante cualquier incidente o extravío de las mismas, ya que contienen las bases de datos de la EUPG-UNFV.

e. Documentación del *backup*: no hay documentación escrita sobre las copias de seguridad, dónde se realizan estas, ni datos históricos referidos a la restauración de las mismas.

Documentación

a. En el área de Informática existe documentación referente a lo siguiente:

- Licencias del *software*, y en qué máquinas está instalado.
- Números de IP de las máquinas, *switch* de las impresoras.
- Inventario de insumos, no actualizados.

b. Manuales

- No existe manuales de usuario y técnico de los sistemas.
- No existe plano de la red Lan.

c. Planes

- No existe ningún plan de contingencia.
- No existe plan de continuidad de negocio.
- No existe un plan de seguridad ni procedimientos desarrollados formalmente.

3.1.6. Auditorías y revisiones

La evaluación consiste en auditoría interna y revisiones, con el fin de encontrar debilidades y proponer mejoras en base a las normativas existentes. La evaluación de la auditoría y las revisiones consisten en los siguientes aspectos:

Revisión del sistema

No se realiza ningún chequeo en forma periódica a los sistemas, porque no existe un responsable asignado para realizar esta actividad.

a. Herramientas de generación y administración de logs: en la EUPG-UNFV, las siguientes aplicaciones o sistemas generan logs de auditoría:

- El sistema operativo del servidor (Windows Server 2003).
- El Proxy del Internet.

Por otro lado, no realizan chequeos de logs, debido a que no existe una aplicación de administración de logs que genere reportes, ni hay alarmas en el sistema que alerten al responsable de la ocurrencia de un evento en particular.

b. Log del servidor: el sistema operativo Windows Server 2003 genera los siguientes logs:

- Servicios de la red.
- Reinicio del servidor.

c. Auditoría interna: en la EUPG-UNFV no se realizan auditorías programadas ni rutinas de chequeos de logs, debido a que no existe una política de seguridad informática definida.

Auditorías de control de acceso a los sistemas

a. Control de acceso a logs: se almacenan en el servidor de aplicaciones, pero no hay ningún control de acceso lógico y físico a las carpetas donde están almacenados. Estas pueden ser accedidas desde cualquier máquina conectada a la red.

b. Modificación de datos: el sistema de gestión académica genera logs, indicando la hora y qué persona realizó el cambio, pero no son analizados, solo se almacenan.

c. Cambio de *password*: No se generan logs cuando un usuario modifica su *password*, tampoco se guardan las contraseñas anteriores (para evitar la repetición). No se determina qué aplicación se ha usado para realizar el cambio. En caso de que el cambio resulte fallido, tampoco se genera el logs sobre el motivo del fallo.

d. Perfil de usuario: con los logs que generan los diferentes aplicativos sería posible generar perfiles de los requerimientos de cada usuario, pero no realizan estas tareas.

Reportes de correo

Los logs del correo electrónico no sacan líneas de base ni se grafican, pues el encargado los revisa con la autorización del propietario de la cuenta. Esta operación se realiza cuando ocurre una falla en el servicio o cuando el usuario no puede abrir un archivo adjunto, pero no se genera un documento sobre el motivo de la falla.

- a. Estadísticas de red: no existen gráficos sobre el tráfico en la red.
- b. El proxy Wingate: genera logs detallados con datos sobre las páginas visitadas y los horarios de entrada y de salida, aunque no se generan reportes con datos relativos a los archivos descargados desde Internet. Tampoco existen reportes sobre las aplicaciones utilizadas por cada usuario, ni las prioridades de estas aplicaciones, con el fin de discriminar qué cantidad de tráfico genera cada aplicación.

3.1.7. Plan de contingencia

La evaluación consiste en determinar qué activos informáticos tienen mayor prioridad en cada proceso y las más vulnerables, con el fin de orientar y proponer el desarrollo de un plan de contingencia y de continuidad de servicios críticos, teniendo en cuenta los riesgos más probables y considerando las distintas soluciones posibles.

La evaluación consiste en los siguientes aspectos:

Plan de administración de incidentes

En la EUPG-UNFV no existen planes formales para la administración de incidentes, como planes de contingencia, de recuperación de desastres o de reducción de riesgos. Actualmente las emergencias son administradas por el responsable del área de Informática, aunque no existen roles o responsabilidades formales asignadas a ningún empleado.

Backup de equipamiento

- a. Equipamiento de los servidores: el servidor cuenta con dos discos duros, cada uno con una capacidad de 80 GB. Son discos de tipo SCSI-HOT-SWAP; es decir, se puede trasladar e instalar a otro equipo sin apagar el equipo de cómputo. Con esta metodología pueden caerse hasta dos o más discos simultáneamente sin inconvenientes para el funcionamiento del sistema, y, al reponer el disco que falta, el servidor actualiza los datos automáticamente.
- b. Equipamiento de red: no existe *backup* de *hardware*, debido a que no hay un responsable que se dedique específicamente a esta actividad.
- c. Centro de procesamiento de datos alternativo: los datos de la EUPG-UNFV y el servidor se encuentran en la misma infraestructura, ya que no hay ningún centro de procesamiento de datos alternativo.

Estrategias de recuperación de desastres

Debe cubrir toda la gama, desde lo más sencillo hasta lo más complejo, dependiendo de las necesidades y de las amenazas potenciales.

Para ello se analizan los siguientes aspectos:

a. **Estrategia preactiva**

- Constitución del grupo de desarrollo del plan: en el caso de que se genere un plan de emergencia, el responsable del desarrollo e implementación del plan debería ser el jefe del área de Informática.
- Sistemas de información: el usuario es responsable directo de la información que utiliza diariamente, pero no existe documento alguno sobre esta responsabilidad. Tampoco están identificados todos los sistemas de información a modo de inventario, contemplando sus características principales, de manera que no es posible asignarles prioridades y así determinar qué sistema es más importante a la hora de recuperar la operatividad luego de un desastre.
- Equipos de cómputo: no hay inventario de los equipos de *hardware* ni de *software*, ni documentación con respecto a los equipos de la red física, de manera que no se les asigna un orden de importancia.
- Establecimiento del plan de acción: en caso de una emergencia, sería necesario desarrollar un plan de acción en el cual el servidor de aplicaciones y de la base de datos sería el activo con mayor importancia al momento de continuar con las tareas, debido a que en él se encuentran los sistemas propios de la EUPG-UNFV y sus datos.

Los activos más críticos a proteger consiste en lo siguiente:

- Datos: bases de datos, datos compartidos, documentación del área de Informática, de Sistemas, datos de todas las oficinas.
Programas fuentes y ejecutables del sistema.

- *Hardware:*
Servidor, *switch*, hub, equipos de cómputo.
Redes.
Soporte físico de *backup*.

- b. Estrategia de acción: no hay funciones claras que debe realizar el personal durante una contingencia, ya que no hay responsabilidades asignadas.

- c. Estrategia reactiva:
 - Evaluación de daños: una vez que ha ocurrido una contingencia, los encargados de evaluar los daños son los responsables de cada una de las oficinas, encabezados por el director de la EUPG, reportando al responsable, el cual evalúa los resultados para aplicar una solución apropiada.
 - Ejecución de actividades: una vez ocurrido el siniestro, el responsable del área de Informática la pone en marcha, realizando las actividades de recuperación sin respaldarse de un plan o manual formal de procedimientos.
 - Retroalimentación del plan de acción: no hay un plan de acción, tampoco se toman acciones correctivas ante una emergencia. Cuando ocurren desastres, no se genera documentación con respecto de las modificaciones realizadas, ni sobre las acciones correctivas que se llevaron a cabo; tampoco se realiza un inventario de lo ocurrido.

3.2. Plan de seguridad informática propuesto

Producto de la evaluación de seguridad informática actual, y tomando como referencia la Norma Internacional de Seguridad de la Información (International Organization for Standardization ISO 27001/ ISO17799:2005), se formula un plan de seguridad informática que promueva el uso adecuado de la tecnología de la información, estableciendo una cultura de seguridad. Asimismo, el análisis obliga a redactar los roles y responsabilidades para cada uno de los propietarios de la información.

Para definir apropiadamente las políticas de seguridad informática, se ejecutaron los siguientes aspectos en el plan propuesto:

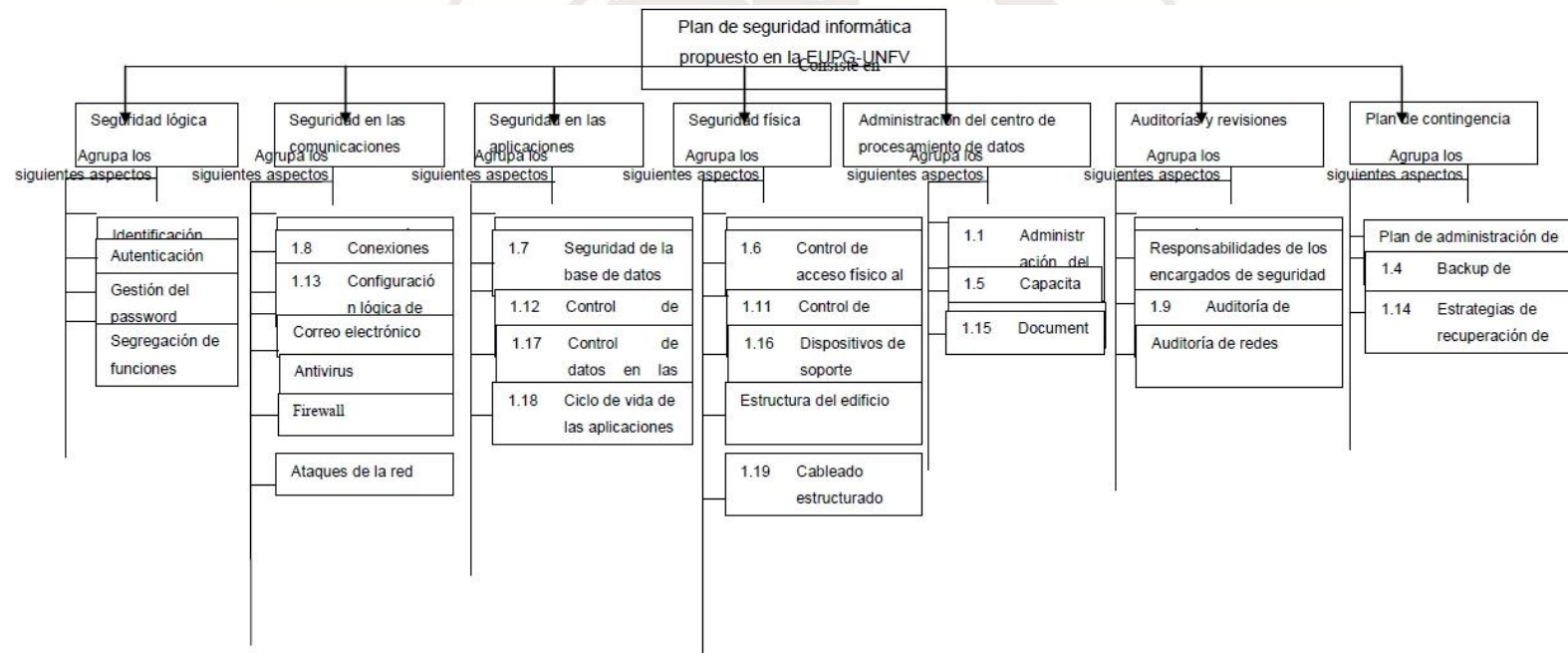
- a. Antecedentes: los resultados del análisis evidencian la no existencia de un sistema de seguridad informática en la EUPG-UNFV, estando expuesta la información a amenazas informáticas, tanto externas como internas.
- b. Legislación: para el desarrollo del plan de seguridad se tomó como referencia la Ley N.º 27309, que incorporó al Código Penal peruano los delitos informáticos dentro de la figura genérica de los delitos contra el patrimonio, a la letra en el artículo 207, literales A, B y C.
- c. Propósito: las políticas de seguridad informática formuladas en el plan propuesto tienen como propósito proteger la información, consiguiendo la confidencialidad, la integridad y la disponibilidad de la información, la misma que surge como una herramienta para concientizar a cada uno de sus empleados acerca de la importancia y la sensibilidad de la información, de tal forma que permitan a la EUPG-UNFV cumplir con su misión y objetivos propuestos.

La definición de las políticas de seguridad informática, como todo proceso técnico-administrativo, debe abarcar todas las áreas de la EUPG-UNFV, apoyados por la alta dirección. Por tanto, el plan propuesto se agrupa en siete factores:

- Seguridad lógica.
- Seguridad en las comunicaciones.
- Seguridad de las aplicaciones.
- Seguridad física.
- Administración del centro de procesamiento de datos.
- Auditorías y revisiones.
- Plan de contingencia.

De la misma forma, el plan propuesto se esquematiza en el gráfico 2 de la presente investigación, donde se puede apreciar de manera detallada cada una de las políticas que conforman el plan de seguridad informática propuesto en la Escuela Universitaria de Postgrado de la Universidad Nacional Federico Villarreal.

Gráfico 2. Mapa conceptual del plan de seguridad informática propuesto



Para sintetizar el plan propuesto, se esquematizó en modelo de causa efecto o Isikawa, llamado también *espina de pescado* y *árbol de causas*, lo que permite visualizar todas las causas con todas sus relaciones sobre el efecto de un plan de seguridad informática en la EUPG-UNFV (anexo 1).

No obstante, estas políticas y medidas de seguridad informática propuestas deben ser revisadas periódicamente, analizando la necesidad de cambios, mejoradas o adaptadas para cubrir los riesgos existentes y auditando su cumplimiento.

De la misma forma, se señalan los procedimientos que pautan las actividades relacionadas con la seguridad informática para cada uno de los aspectos que comprenden las políticas de seguridad informática del plan propuesto.

3.2.1. Seguridad lógica

La información manejada por los sistemas de información y las redes asociadas debe estar protegida adecuadamente contra las modificaciones no autorizadas, su divulgación o su destrucción. El plan propuesto referente a la seguridad lógica consiste en los siguientes aspectos:

Identificación de usuarios

a. Para la administración y el control de acceso a los datos debe existir una política formal de “control de acceso del usuario”, donde se detalle como mínimo lo siguiente:

- Confidencialidad de los datos que se ingresan al momento de acceder a los sistemas de información:
 - Usuario.
 - *Password*.

- Procedimientos de otorgamiento de claves de usuarios para el ingreso a los sistemas de información.
 - Estándares fijados para la identificación y la autenticación de usuarios.
- b. Para dar de alta a un usuario: establecer el procedimiento formal que regule y exija el ingreso de los siguientes datos:
- Identificación del usuario, único e irrepitible.
 - *Password* personal e ingresado por el usuario.
 - Nombres y apellidos completos.
 - Grupo de usuarios al que pertenece, que debe estar organizado por áreas u oficinas.
 - Fecha de expiración del *password*.
 - Fecha de anulación de la cuenta.
 - Autorización para imprimir.
- c. Asignar permisos mínimos y necesarios para que cada usuario desempeñe su tarea adecuadamente.
- d. Control de acceso al sistema (auditar), ingreso del usuario, modificación de datos, permisos para ejecutar.
- e. Restringir el acceso al sistema o la utilización de recursos en un rango de horario definido, teniendo en cuenta lo siguiente:
- Los usuarios no deben acceder al sistema en horarios no laborales de acuerdo con el grupo al que pertenezcan.
 - Desactivar las cuentas de los usuarios durante las vacaciones o licencias.

- Desactivar las cuentas de los empleados en días feriados. Realizar chequeo mensual de las cuentas de cada usuario, asegurando que los permisos sean correctos.

- f. El área de Secretaría Administrativa comunicará al administrador del sistema los cambios del personal de la EUPG-UNFV.

- g. Para dar de baja a un usuario del sistema debe existir un procedimiento formal por escrito. Los datos no se eliminarán, se actualizará la fecha de anulación de su cuenta, quedando estos datos registrados en el histórico.

- h. Llevar a cabo una política de desvinculación o cancelación del trabajador, bloqueando permisos de acceso.

- i. Las PC deben tener instalado un protector de pantalla con contraseña, con la finalidad de evitar el acceso no autorizado.

- j. Controlar la existencia de perfiles genéricos de los usuarios en todos los sistemas operativos y sistemas de información de la EUPG-UNFV.

- k. Minimizar la generación y el uso de perfiles de usuario con máximos privilegios.

- l. Si se realiza mantenimiento externo, crear una cuenta con los permisos mínimos; una vez finalizado el mantenimiento, el administrador del sistema deberá modificar la contraseña de esa cuenta.

Autenticación

a. La pantalla de acceso al sistema deberá mostrar los siguientes datos:

- Nombre de usuario.
- *Password*.
- Opción para cambiar la clave.

b. Mientras el usuario esté ingresando su contraseña, esta no debe ser mostrada por pantalla.

c. Cuando el usuario ingrese al sistema, deberán mostrarse los siguientes datos:

- Nombre de usuario.
- Fecha y hora de la última conexión.

d. La aplicación para administrar los datos de usuarios solo deberá ejecutarse en máquinas designadas por el responsable del área de Informática.

Gestión del *password*

a. Los *password* deberán tener las siguientes características:

- Conjunto de caracteres alfanuméricos.
- Longitud mínima de 6 y máxima de 10 caracteres.

b. El *password* deberá tener una fecha de caducidad, para obligar el cambio.

La fecha de expiración del password deberá ser de cuatro meses. El sistema exigirá automáticamente el cambio, una vez cumplido el plazo.

- c. El *password* no deberá contener el nombre de la institución, el nombre del usuario ni palabras reservadas.
- d. Bloquear el perfil de todo usuario que haya intentado acceder al sistema en forma errada por más de tres veces consecutivas.
- e. El usuario debe poder modificar su *password* cuantas veces considere necesario, sin seguir procedimiento formal de aviso.

Segregación de funciones

- a. Existirá una adecuada y documentada separación de funciones.
- b. El área de Informática deberá figurar en organigrama de la EUPG-UNFV (ver 1).
- c. Realizar rotación en las tareas del personal del área de Informática para evaluar su desempeño durante cierto período. Asimismo, establecer un proceso de capacitación adecuado y permanente.

3.2.2. Seguridad en las comunicaciones

La administración de las comunicaciones en la EUPG-UNFV es esencial para mantener la continuidad de los sistemas de información y de los servicios. Los requerimientos de seguridad deben ser desarrolladas adecuadamente, por lo que todas las comunicaciones e intercambios de información deben ser asegurados y monitorizados apropiadamente. El plan referente a la seguridad en las comunicaciones consiste diversos aspectos, que se mencionan a continuación.

Topología de la red

- a. Asegurar la integridad, disponibilidad y confidencialidad de los datos transmitidos a través de los dispositivos *hardware*, de los protocolos de transmisión o de los controles aplicativos.
- b. Documentar detalladamente sobre los diagramas topológicos de las redes.
- c. Que existan medios alternativos de transmisión en caso de que alguna contingencia afecte al medio primario de comunicación.

Conexiones externos

- a. La conectividad a Internet será autorizada por el director de la EUPG-UNFV. Los usuarios no autorizados deberán estar imposibilitados de conectarse al exterior.
- b. Los usuarios de la EUPG-UNFV que utilicen Internet deben recibir capacitación específica respecto de su funcionalidad y de los riesgos y medidas de seguridad pertinentes.
- c. Asegurar que la totalidad del tráfico entrante y saliente de la red interna sea filtrada y controlada por un *firewall*, prohibiendo el pasaje de todo el tráfico que no se encuentre expresamente autorizado.
- d. Las conexiones a Internet de la EUPG-UNFV deben traspasar por un *firewall* y luego por un servidor proxy.
- e. El uso de Internet debe ser monitoreado periódicamente.

Configuración lógica de la red

- a. El riesgo aumenta con el número de conexiones a redes externas; por tanto, la conectividad al exterior debe ser la mínima y necesaria.

- b. Asegurar que la dirección IP de la EUPG-UNFV sea un número variable.
- c. Los recursos lógicos o físicos de los distintos puestos de trabajo no deben ser visibles en el resto de la red informática. Los recursos de los servidores serán visibles solo en los casos necesarios y con las medidas de seguridad correspondientes.
- d. Tomar recaudos necesarios para restringir todo tipo de aplicaciones que no ayuden al cumplimiento de los objetivos de la EUPG-UNFV, tales como las herramientas de chateo, etc.

Correo electrónico

- a. La dirección de la EUPG-UNFV determinará qué empleados deben contar con una cuenta de correo electrónico generado por la UNFV, según lo amerite su tarea.
- b. Existirá un procedimiento formal para dar de alta y de baja las cuentas de correo electrónico en el sistema informático.
- c. El correo electrónico no debe ser utilizado para enviar correos no deseados.
- d. Los mensajes de correo electrónico deben ser considerados como documentos formales y deben respetar todos los lineamientos referentes al uso inapropiado del lenguaje.
- e. El correo electrónico no debe ser utilizado para enviar cadenas de mensajes. No debe relacionarse con actividades ilegales y no éticas o para mensajes no relacionados con los propósitos de la EUPG-UNFV.

Antivirus

- a. En todos los equipos de la EUPG-UNFV debe existir una herramienta antivirus ejecutándose permanentemente y en continua actualización.

- b. La actualización de los antivirus de todos los equipos de la EUPG-UNFV deberá realizarse a través de un procedimiento formal y, si es posible, automático, y por medio de una consola.
- c. Programar escaneos periódicos de virus en todos los equipos de cómputo.
- d. Deberá existir un procedimiento formal en caso de que se detecte un virus en algún equipo de cómputo.

Firewall

- a. El *firewall* de la EUPG-UNFV presentará una política de negación preestablecida, configurado de manera que se prohíban todos los protocolos y servicios, habilitando los necesarios.
- b. Habilitar los servicios o protocolos que solo sean necesarios. Aquellos que sean considerados riesgosos, habilitarse bajo estrictas limitaciones de uso, considerando el equipo desde el que se utilizará, hacia qué destino, las fechas y los horarios para dichas conexiones. A modo de ejemplo, esto puede aplicarse a la utilización del protocolo FTP para la comunicación con las otras facultades de la UNFV.
- c. El responsable debe controlar periódicamente la configuración del *firewall* y los servicios de la red, documentando los resultados de dichas pruebas.

Ataques de la red

- a. Existir procedimientos formalmente documentados destinados a prevenir los ataques de la red más frecuentes.
- b. Usar algún sistema de detección de intrusos, tolerantes al fallo, utilizando los mínimos recursos posibles.

- c. Utilizar una herramienta que monitoree la red, con el fin de evitar el ataque de negación de servicio.

3.2.3. Seguridad en las aplicaciones

Las aplicaciones de los sistemas de información y del usuario final deben soportar los requerimientos generales de la seguridad informática documentados en la política del plan propuesto. La protección de la misma debe ser adecuada y consistente. El plan propuesto referente a la seguridad en las aplicaciones consiste en los siguientes aspectos:

Software

- a. El sistema operativo del servidor deberá presentar las siguientes características:

- Alta confidencialidad en el acceso de los usuarios.
- Compatibilidad e interoperatividad con los sistemas operativos de las PC y demás sistemas usados en la EUPG-UNFV.
- Disponibilidad de *software* de aplicación y actualizaciones.
- Disponibilidad de documentación.

- b. Además, deberá presentar las siguientes características en lo relativo a la seguridad:

- Identificación y autenticación de los usuarios.
- Control de acceso de los usuarios.
- Seguridad en la transmisión de los datos.
- Requerimientos sobre privacidad de datos.

Seguridad de la base de datos

- a. Control de acceso, de forma tal que la única persona que pueda tener acceso a los recursos de la base de datos sea el responsable del área de Informática.
- b. Que exista una aplicación que registre las siguientes ocurrencias:
 - Tiempo y duración de los usuarios en el sistema.
 - Número de conexiones a las bases de datos.
 - Número de intentos fallidos de conexiones a las bases de datos.
 - Estadísticas de entrada/salida para cada usuario.
 - Modificación de datos.
- c. Hacer chequeo regular de la seguridad de la base de datos, en los que se deberá verificar lo siguiente:
 - Si son efectivos los *backup* y los mecanismos de seguridad.
 - La no existencia de usuarios de la base de datos que no tengan asignada una contraseña.
 - Que se revisen los perfiles de los usuarios que no han usado la base de datos por un período largo.
 - Además del responsable de datos, ninguna otra persona debe acceder a los archivos del *software* de la base de datos.
 - Solo el responsable de la base de datos debe tener acceso de lectura y escritura.
- d. Debe existir una clasificación de los datos en base a su sensibilidad para definirlos como críticos y así determinar controles específicos, para lo cual se definen tres niveles de información.

Crítica

- La no disponibilidad de esta información ocasiona daño en los activos de la EUPG-UNFV.
- Se considera recurso crítico a aquel recurso interno que debe estar disponible solamente para un conjunto determinado de personas. Debe ponerse cuidado especial en la información que por ley o por políticas de la EUPG-UNFV deben permanecer en estado confidencial; la clasificación de un recurso como crítico deberá incluir los criterios. De ser necesaria su transmisión por redes externas o su almacenamiento en sistemas de la red perímetro, deberán tomarse medidas de seguridad extremas.

Confidencial

- La información en poder de personas no autorizadas compromete los intereses de la EUPG-UNFV.
- Todo aquel recurso que no haya sido explícitamente clasificado como disponible al público por la EUPG-UNFV.

Pública

- Información de libre circulación.
- Aquel que no requiere permanecer como de uso interno y que explícitamente se ha clasificado como un recurso público. Esta clasificación deberá ser documentada e informada a todo el personal de la EUPG-UNFV, y deberá evaluarse y actualizarse periódicamente.
- Debe existir un responsable en cada área de la EUPG-UNFV, que responda por la información que se maneja en dicho sector.
- Definir la clasificación de los datos y los controles de acceso que son necesarios.

Control de aplicaciones en las computadoras

- a. Deben existir estándares de configuración de los puestos de trabajo, servidores y demás equipos de la red informática.
- b. Generar procedimientos donde se especifique qué aplicaciones deben instalarse de acuerdo al perfil de cada usuario, y con qué frecuencia se harán las actualizaciones de dichas aplicaciones.
- c. Las aplicaciones solo se actualizarán debido al reporte de algún mal funcionamiento o a un nuevo requerimiento por parte de los usuarios o del personal del área de Informática.
- d. Antes de hacer un cambio en la configuración del servidor, se deberá hacer un *backup* de la configuración existente.
- e. Establecer un procedimiento de emergencia para dejar sin efecto los cambios efectuados y poder recuperar las versiones autorizadas anteriores en el caso de generarse problemas.
- f. Documentar no solo el procedimiento de instalación y reparación de equipos, sino además cada uno de los mantenimientos que se realicen. Generar historiales para calcular datos estadísticos de los cambios realizados y de los errores reportados.
- g. En el momento en el que un nuevo usuario ingrese a la EUPG-UNFV, notificar y aceptar que tiene prohibida la instalación de cualquier producto de *software* innecesario en los equipos.
- g. Realizar chequeos periódicos en PC, servidor y demás equipos, en búsqueda de aplicaciones instaladas no autorizadas o innecesarias.

Control de datos en las aplicaciones

- a. Los datos de entrada y de salida del sistema deberán poseer controles en los que se verifique la integridad, la confidencialidad y la disponibilidad de la información.
- b. Los datos de salida del sistema de la EUPG-UNFV deben restringir con controles lógicos, de acuerdo con los permisos de acceso.
- c. Proteger con controles de acceso a las carpetas que almacenen los archivos de las aplicaciones. Solo el administrador de sistemas tendrá acceso a ellas.

Ciclo de vida de las aplicaciones

- a. Antes de realizar alguna modificación en el sistema, realizar un análisis del impacto de este cambio.
- b. Implementar una gestión de configuración y documentar los cambios desarrollados en las aplicaciones.
- c. Existir un documento formal de solicitud de cambios donde quede reflejado el motivo y la solicitud del cambio; la documentación de los cambios debe incluir:
 - Sistema que afecta.
 - Fecha de modificación.
 - Desarrollador que realizó el cambio.
 - Empleado que solicitó el cambio.
 - Descripción global de la modificación.
- d. El formulario anterior se utilizará para actualizar la documentación del desarrollo y de los distintos manuales generados.

e. Todo nuevo desarrollo o modificación deber estar probado y aprobado por los usuarios del mismo antes de su instalación en el ambiente de trabajo. Se informará por escrito la importancia de la seguridad de la información a todo el personal.

3.2.4. Seguridad física

Se asocia a la protección del sistema ante amenazas físicas, incendios, inundaciones, edificios, cables, control de accesos de personas, etc. Las medidas de protección deben ser consistentes y adecuadas, para mantener la continuidad de la información en la EUPG-UNFV. Por tanto, el plan propuesto referente a la seguridad física consiste en los siguientes aspectos:

Equipamiento

Existirá una adecuada protección física y un mantenimiento permanente de los equipos e instalaciones que conforman los activos de la EUPG-UNFV.

Control de acceso físico al área de Informática

- a. Restringir el acceso físico de las áreas críticas a toda persona no autorizada, para reducir el riesgo de accidentes y actividades fraudulentas.
- b. Utilizar sistemas de monitoreo automáticos o manuales, que controlen el ingreso al área de informática.
- c. El área de informática donde se encuentran los servidores, el *switch* central y demás equipamiento crítico solo debe tener permitido el acceso a los responsables.

- d. El personal del centro de procesamiento, así como el personal contratado, solo podrá permanecer en las instalaciones de la EUPG-UNFV durante el horario autorizado. Se debe establecer un procedimiento de autorización para el personal que pueda permanecer fuera de su horario habitual de trabajo.
- e. Realizar un adecuado mantenimiento y prueba de los procedimientos para la restricción de acceso físico, así como de los dispositivos de seguridad para prevención, detección y extinción del fuego.

Control de acceso a equipos

- a. Las disqueteras y lectoras de CD deberán deshabilitarse en aquellas máquinas en que no se necesiten.
- b. El responsable del sistema deberá gestionar un *password* de administrador en el BIOS de cada equipo de cómputo.
- c. El servidor deberá tener una llave de bloqueo de *hardware*.
- d. Cualquier dispositivo externo que no se encuentre en uso deberá permanecer guardado bajo llave en el área de Informática.
- e. El gabinete donde se ubican los *switch* de la EUPG-UNFV deberá permanecer guardado bajo llave y fuera del alcance del personal no autorizado.
- f. El responsable deberá realizar chequeos periódicos para comprobar lo siguiente:
- La correcta instalación de los dispositivos de los equipos.
 - Su buen funcionamiento.
 - Que sus números de serie correspondan con los datos registrados por el responsable al momento de la instalación.

- El servidor deberá apagarse automáticamente una vez que han cerrado todas las oficinas de la EUPG-UNFV.

Dispositivos de soporte

a. Deberán existir los siguientes dispositivos de soporte en la EUPG-UNFV:

- Aire acondicionado: en el área de Informática la temperatura debe mantenerse entre los 16 °C y los 18 °C.
- Extintor: deberán ser dispositivos químicos y manuales que cumplan las especificaciones para apagar incendios en equipos de cómputo y otros, los mismos que deberán ser instalados en lugares estratégicos de la EUPG-UNFV. El área de Informática deberá contar con uno propio.
- Alarmas contra intrusos: que se active en horarios no hábiles. Deberá activarse manualmente en horarios laborales ante una emergencia.
- Generador de energía: que se pondrá en marcha cada vez que haya problemas con el suministro de energía eléctrica o avisos de cortes de luz.
- UPS: (Uninterruptible power supply): deberá existir al menos un UPS en el área de Informática, que atienda al servidor con tiempo suficiente para que se apaguen de forma segura.
- Luz de emergencia: que se active automáticamente ante una contingencia.
- Pozo a tierra: deberán existir métodos de descarga a tierra para el edificio y otra independiente para el área de Informática.

b. Todos estos dispositivos deberán ser evaluados periódicamente.

c. Existirá una llave de corte de energía general en la salida de emergencias.

d. Existirán procedimientos detallados para el personal en caso de emergencia, indicando responsables, quienes deben estar adecuadamente capacitados.

Estructura del edificio

- a. El área de Informática deberá ubicarse en un piso superior del edificio, y tendrá protecciones contra ruidos e interferencias electromagnéticas y visuales.
- b. Todas las salidas hacia el exterior del área de Informática deberán estar protegidas con rejas y métodos que impidan la visión.
- c. En el diseño del área de Informática deberá tenerse en cuenta el futuro crecimiento de la EUPG-UNFV, permitiendo la expansión del mismo y predisponiéndolo a reinstalaciones.

Cableado estructurado

- a. Debe seguir las normas del cableado estructurado, que garantizan el funcionamiento eficiente de la red.
- b. Documentar en planos los canales de tendidos de cables y la toma datos de la red existentes.
- c. Existirá tendido de cableado redundante para futuros puestos de trabajo.
- d. habrá un procedimiento manual de respaldo para realizar las tareas cotidianas.
- e. Ante un corte del suministro de energía eléctrica, deberán apagarse los equipos de cómputo en forma segura, como medida de prevención.

3.2.5. Administración del centro de procesamiento de datos

La administración del centro de procesamiento de datos debe ser organizada y administrada con los mismo métodos que han demostrado su efectividad en otros segmentos de la EUPG-UNFV. Debe existir un plan de organización y una clara asignación de responsabilidades. Para la administración adecuada, debe existir documentación de los procedimientos y normas previstas con los cuales se podrán comparar los resultados, a fin de que este brinde condiciones óptimas de operaciones, facilitando un ambiente adecuado de control y mejorando la disponibilidad de sus servicios. Por tanto, el plan propuesto referente a la administración del centro de procesamiento de datos consiste en los siguientes aspectos:

Administración del área de Informática

- a. Asegurar la correcta organización y administración del área de Informática, a fin de que esta brinde condiciones generales de operación que posibiliten un ambiente adecuado de control.
- b. Designar en la dirección del área un profesional que acredite experiencia en el manejo de los recursos informáticos y comprenda los riesgos y los problemas relativos a la tecnología y sistemas de información. Es su obligación y responsabilidad el mantener seguros los sistemas que operan diariamente.
- c. Designar un encargado de la seguridad del sistema, que coordine las tareas correspondientes, haciendo cumplir las políticas de seguridad en toda la EUPG-UNFV.
- d. Existirá una planificación formalizada y completa de las actividades que se desarrollan normalmente. Designar responsabilidades claras y documentadas.

- e. El equipo de sistemas debe hacer hincapié en la concientización de todos los usuarios, generando una cultura de la seguridad, haciéndolos partícipes de las medidas de seguridad, tanto los usuarios actuales como los que se incorporen en el futuro. El proceso de concientización debe ser renovado y transmitido a los usuarios en forma anual.
- f. Implementar un buzón de sugerencias donde los usuarios recomienden mejoras o realicen comentarios, expresando sus inquietudes.
- g. Existirá un procedimiento para realizar la publicidad de políticas, planes o normas de la EUPG-UNFV y sus modificaciones.
- h. Habrá un encargado de llevar a cabo el mantenimiento preventivo y el equipamiento informático de la EUPG-UNFV, monitorizando, chequeando y auditando las PC y demás dispositivos que conforman la red.
- i. Los administradores deberán informar el tiempo de suspensiones del servicio necesario para el mantenimiento, especificando fecha, hora y duración.
- j. Generar un inventario detallado donde se describan los sistemas de información y de los equipos de cómputo utilizados en la EUPG-UNFV. Deberá asignarse un responsable de mantenerlo actualizado y de realizar controles periódicos.
- k. Existirá un procedimiento para controlar que en la EUPG-UNFV solamente se utilicen productos de *software* adquiridos por vías oficiales.

Capacitación

- a. El personal del área de Informática debe mantenerse capacitado respecto de las nuevas tecnologías.
- b. Impartir capacitación a los usuarios, a efectos de que puedan operar adecuadamente los recursos informáticos.

- c. El personal debe ser capacitado para el cumplimiento de lo especificado en la política de seguridad informática. Se debe entregar una copia de la misma a cada empleado.
- d. Obtener un compromiso firmado por parte del personal respecto del cumplimiento de las medidas de seguridad definidas en la política de seguridad informática, destacando específicamente el mantenimiento de la confidencialidad de las claves de acceso, la no divulgación de información de la EUPG-UNFV, el cuidado de los recursos, la utilización de *software* sin licencia y el reporte de situaciones anormales. Debe confirmar este compromiso anualmente o cada vez que se produzcan cambios en las funciones asignadas al personal.
- e. Asegurar que los empleados reciban capacitación continua para desarrollar y mantener sus conocimientos competencia, habilidades y concienciación en materia de seguridad informática dentro del nivel requerido, a fin de lograr un desempeño eficaz.

Backup

- a. Asegurar la existencia de un procedimiento aprobado para la generación de copias de resguardo sobre toda la información necesaria para las operaciones de la organización, donde se especifique la periodicidad y el lugar físico donde se deben mantener las copias generadas.
- b. La periodicidad de la generación de los resguardos debe ser acorde a la criticidad de la información y la frecuencia de cambios.
- c. La ubicación de los *backup* debe contar con adecuadas medidas de seguridad, sin estar expuestos a las mismas contingencias que el área de Informática; es decir, deberán almacenarse en el exterior de la EUPG-UNFV.

- d. Los archivos de *backup* en cintas o en otros dispositivos deben tener un control de acceso lógico de acuerdo con la sensibilidad de sus datos, además de contar con protección física.
- e. Realizar chequeos para comprobar el funcionamiento correcto de los medios externos donde se realizan las copias de respaldo. Además, debe existir una política de reemplazo de medios externos de almacenamiento de *backup*.
- f. Existirá una política de documentación de copias de respaldo, donde se registren todos los datos necesarios para la gestión del procedimiento de *backup*. Se deberá llevar un inventario actualizado de las copias de respaldo.
- g. Generar una copia de respaldo de toda la documentación del área de Informática, incluyendo *hardware*, *software* y plan de contingencia.

Documentación

- a. Generar un soporte de documentación, con información correcta, consistente y actualizada, sobre políticas, procedimientos y manuales. Deberá asignarse un responsable a cargo de la gestión de la documentación en el área de Informática.
- b. Existirá una documentación y un registro de las actividades del área de Informática (procesos normales, eventuales que se desarrollan diariamente), que incluya como mínimo el detalle de los procesos realizados.
- c. Habrá un registro de eventos, errores y problemas del *hardware* y el *software* utilizados en las operaciones de procesamiento de datos.

3.2.6. Auditorías y revisiones

La auditoría informática consiste en la metodología de control y revisiones que se lleven a cabo en forma periódica y permanentemente sobre todas las herramientas, programas, aplicaciones, documentación y papeles de

trabajo, con el fin de encontrar debilidades y proponer mejoras y recomendaciones. Por tanto, el plan propuesto, referente a auditoría y revisiones, consiste en los siguientes aspectos:

Revisión del sistema

a. La EUPG-UNFV debe asegurar que los sistemas provean las herramientas necesarias para garantizar un correcto control y auditabilidad; de la misma forma, asegurará la integridad, la confidencialidad y la disponibilidad de la información. Para ello debe existir lo siguiente:

- Herramientas que registren todos los eventos relacionados con la seguridad de la información procesada en área de Informática.
- Herramientas para analizar los registros generando reportes, estadísticas, gráficos con relación a los datos recogidos, con distintas frecuencias (diarios, semanales, mensuales y anuales). Deberá tener la capacidad de generar alarmas teniendo en cuenta la severidad de los eventos acontecidos.
- Procedimientos de revisión de los eventos registrados a cargo de un empleado designado por la alta gerencia, con finalidad de detectar anomalías y tomar las acciones correctivas necesarias.

b. Registrar, mediante logs de auditoría, aquellos eventos relacionados con la seguridad de la información. Dichos registros deberán contener como mínimo lo siguiente:

- Fecha y hora del evento.
- Fuente (el componente que disparó el evento).
- Id del evento (número único que identifica el evento).
- Equipo (máquina donde se generó el evento).

- Usuario involucrado (que usuario).
 - Descripción (acción).
- c. Registrar como mínimo los siguientes eventos respecto de los servidores:
- Servicios de red.
 - Configuración del servidor.
 - Reinicio del servidor.
- d. Actualizar continuamente las herramientas de análisis de logs, asignándole la responsabilidad de esta tarea a una persona en particular.
- e. Generar líneas de base que contengan información sobre PC, servidor y sistema informático en su totalidad, con datos históricos obtenidos de los registros de auditoría, reportes diarios, semanales, mensuales y anuales.
- f. Programar auditorías periódicas y chequeos aleatorios, para controlar las áreas o funciones críticas con respecto de la seguridad de los datos de la EUPG-UNFV, documentando la ejecución y los resultados de dichas pruebas.
- g. Analizar periódicamente los siguientes eventos específicos como mínimo:
- Controles de acceso y permisos de los usuarios.
 - Uso de recursos informáticos.
 - Operaciones de borrado o modificación de objetos críticos.
 - Intentos de ingreso al sistema fallidos.
- h. Documentar las revisiones y controles efectuados, y comunicar las excepciones encontradas a los responsables involucrados y al propietario de los datos afectados por las anomalías, los que deberán determinar

la severidad del incidente y las acciones que sean necesarias para la protección y control de los datos.

Responsabilidades de los encargados de seguridad

a. El administrador del sistema o un encargado de auditoría deberá realizar las siguientes operaciones:

- Determinar qué logs se generarán en forma constante.
- Determinar qué eventos de seguridad se auditarán.
- Determinar qué datos se recogerán de estas auditorías.
- Administrar, desarrollar e implementar los procedimientos de auditoría.
- Chequear aleatoriamente para verificar el cumplimiento de los requerimientos y procedimientos de seguridad.
- Revisar los reportes de auditorías cuando se advierten anomalías.

Auditoría de control de acceso a los sistemas

- a. Los logs deben almacenarse en una carpeta del servidor protegida con contraseña. Esta contraseña debe ser desconocida para todos los usuarios del sistema, incluso para el administrador, por lo que debe conservarla un miembro del directorio.
- b. Generar logs referidos a la modificación de datos, identificando los datos modificados por cada usuario y el valor anterior de dicho dato.
- c. Generar logs cuando un usuario modifica su contraseña, con datos sobre la aplicación desde la que se realizó el cambio y, en caso de que el cambio resulte fallido, el motivo del fallo.
- d. Generar logs cuando hubo un fallo en el logeo de un usuario, indicando el motivo del fallo.

e. Generar perfiles de los usuarios en base a algunos de los siguientes datos:

- Uso de internet.
- Tráfico de red que genera cada usuario o sector de la EUPG
- Terminales utilizadas.
- La hora de acceso.

Auditoría de redes

a. Generar un plan de monitorización de red utilizando algún escáner de seguridad integral (*overall security scanner*).

b. Con respecto de las conexiones a Internet, deben almacenarse datos sobre lo siguiente:

- Número IP de la máquina conectada.
- Dirección de las páginas visitadas.
- *Cookies* guardadas.
- Archivos descargados.
- Aplicaciones utilizadas.

c. Con respecto de la utilización del correo electrónico, deben almacenarse datos sobre lo siguiente:

- Correo entrante y saliente.
- Hora de envío.
- Contenido del *mail*.
- Asunto del *mail*.
- Archivos adjuntos.
- Reporte de virus de cada parte del mail.

- Direcciones de máquina destino y fuente.
- Tamaño del mensaje.

Cabe mencionar, al respecto del almacenamiento de las características del correo electrónico, que tiene como finalidad evitar algún robo de la información de la EUPG-UNFV por parte de los usuarios o exempleados con fines ajenos a la institución mencionada.

d. Con respecto de la utilización de la red informática, deben almacenarse datos sobre lo siguiente:

- Ancho de banda utilizado y cuellos de botella en el tráfico de red.
- Tráfico generado por las aplicaciones.
- El estado de cada aplicación (en cola, ejecutándose, esperando una respuesta).
- Intentos de intrusión.
- Uso de los protocolos.
- Solicitudes de impresión de datos.

3.2.7. Plan de contingencia

Es una estrategia planificada que contiene una serie de procedimientos que permiten la continuidad de servicios críticos, teniendo en cuenta los riesgos más probables y considerando las distintas soluciones posibles. Por tanto, el plan propuesto referente al plan de contingencia consiste en los siguientes aspectos.

Plan de administración de incidentes

a. Asegurar la continuidad de la recolección de datos y su procesamiento ante cualquier contingencia que afecte a los centros de procesamiento. Para ello se deberá realizar lo siguiente:

- Generar procedimientos manuales de respaldo para cada una de las actividades desarrolladas.
- Preparar, probar y mantener actualizado un plan de contingencia, coordinando el mismo con los procedimientos de copias de respaldo y almacenamiento externo.
- Definir y asignar claramente las responsabilidades de las tareas detalladas en el plan.
- Prever un programa de entrenamiento para el personal involucrado en el plan de contingencia.

b. Almacenar una copia del plan de contingencia en el exterior de la EUPG-UNFV, protegiéndola contra su divulgación y actualizándola permanentemente.

Backup de equipamiento

a. El equipamiento informático de la EUPG-UNFV debe contar con dispositivos de respaldo ante cualquier tipo de incidente.

b. Los mecanismos de recuperación de los dispositivos de respaldo deben ser probados periódicamente, comprobando su buen funcionamiento.

c. El sistema informático no deberá verse afectado ante una contingencia en el área de Informática, por lo que el equipamiento informático debe distribuirse en lugares físicos diferentes.

d. En el caso de que ocurra alguna contingencia con el servidor de aplicaciones, el servidor web se utilizará como servidor de aplicaciones.

Estrategias de recuperación de desastres

- a. Conformar un grupo de desarrollo encargado de concebir, probar e implementar el plan de contingencia. Este debe estar a cargo del jefe del área de Informática e integrado por los responsables de cada área de la EUPG-UNFV.
- b. Asignar un orden de importancia a los sistemas de información y a los equipos de la red informática, de acuerdo al análisis de riesgo y al impacto que representaría para la EUPG-UNFV su ausencia.
- c. Los equipos deberán estar señalizados o etiquetados de acuerdo a la importancia de su contenido, para ser priorizados en caso de evacuación.
- d. Definir las funciones o servicios críticos de la EUPG-UNFV, junto con los recursos mínimos necesarios para su funcionamiento, asignándoles una prioridad en el plan de contingencia.
- e. Identificar las contingencias que podrían ocurrir para cada nivel de servicio crítico definido.
- f. Conformar un plan de emergencias, determinando los procedimientos a llevar a cabo para cada contingencia identificada, considerando los distintos escenarios posibles. Cada procedimiento deberá estar claramente definido, y tener asignado un responsable para su ejecución.
- g. Para el desarrollo del plan de contingencia deben contemplarse las siguientes pautas:
 - Estar documentado y testeado antes de su puesta en práctica.
 - Basarse en un análisis de riesgo, determinando qué acciones merecen estar incluidas.
 - Abarcar la totalidad de la EUPG-UNFV.
 - Mantenerse actualizado, de acuerdo a nuevos puestos de trabajos y funciones.
 - Ser probado frecuentemente.

- Contener la siguiente información:
 - Objetivo del plan.
 - Modo de ejecución.
 - Tiempo de duración.
 - Costes estimados.
 - Recursos necesarios.

- h. Definir cuánto tiempo se aceptará estar en condición de emergencia.
- i. Documentar la realización de las siguientes actividades después de un incidente:
 - Determinar la causa del daño.
 - Evaluar la magnitud del daño que se ha producido.
 - Qué sistemas se han afectado.
 - Qué modificaciones de emergencia se han realizado.
 - Qué equipos han quedado no operativos.
 - Cuáles se pueden recuperar y en cuanto tiempo.

Cada una estas actividades deberán ser reportadas por los líderes de cada área al responsable de la seguridad.

- j. Asignar a un responsable que se encargue de las operaciones necesarias para que el sistema funcione correctamente después de la emergencia. Deberá retroalimentarse el plan luego de una contingencia, ajustando las directivas en consecuencia.
- k. Establecer planes de prueba periódicos que incluyan simulacros de siniestros para evaluar la eficiencia y eficacia del plan.

3.3.

Roles y responsabilidades en cuanto a seguridad informática

La redacción de roles y responsabilidades tiene como objetivo establecer lineamientos que permitan fortalecer la seguridad, haciendo cumplir el plan propuesto en dicho documento, promoviendo una cultura en torno a la seguridad informática. En este contexto, la definición abarca para cada uno de los propietarios de la información.

El área de Informática debe soportar los objetivos de seguridad de la información. Dentro de sus responsabilidades se encuentran la gestión y la coordinación con cada uno de los empleados, siendo estos los últimos responsables de la información que utilizan. Los propietarios de los datos deben verificar la integridad de su información y velar por la disponibilidad y la confidencialidad de la misma. Los roles y las responsabilidades relacionadas con la administración de seguridad de la información abarca lo siguiente:

3.3.1. Área de informática

Encargada de administrar la seguridad de la información, tiene como responsabilidad la de establecer y documentar la responsabilidad de la EUPG en cuanto a la seguridad de la información.

- Identificar objetivos de seguridad de la EUPG–UNFV (prevención de virus, uso de herramientas de monitoreo, etc.).
- Definir procesos relacionados con la seguridad de la información.
- Comunicar aspectos básicos de seguridad de la información a los empleados.
- Monitorear el cumplimiento de la política de seguridad.
- Controlar e investigar incidentes o violaciones de seguridad.

- Realizar una evaluación periódica de vulnerabilidad de los sistemas que conforman la red de datos.
- Verificar que cada activo de información de la EUPG-UNFV haya sido asignado a un responsable, el cual debe definir requerimientos de seguridad como políticas de protección, perfiles de acceso y respuestas ante incidentes.
- Coordinar las funciones relacionadas a seguridad, como seguridad física, personal y de la información almacenada en medios no electrónicos.

3.3.2. Custodio de la información

Responsable de la administración diaria de la seguridad en los sistemas de información y el monitoreo del cumplimiento de las políticas de seguridad en los sistemas que se encuentran bajo su dirección. Sus responsabilidades son las siguientes:

- Administrar acceso en red (sistemas operativos).
- Administración accesos en base de datos.
- Administrar los accesos a archivos físicos de información almacenada en medios magnéticos (diskettes, cintas, CD, USB, etc.) o impresos.
- Monitorear el cumplimiento de la política y procedimientos de seguridad en los activos de la información que custodia.
- Administrar los procedimientos de *backup*, recuperación y plan de continuidad de los sistemas.

3.3.3. Usuarios

La responsabilidad de los usuarios, es decir, de aquellas personas que utilizan información como parte de su trabajo diario, son las siguientes:

- Mantener la confidencialidad de las contraseñas en los sistemas de información.
- Reportar supuestas violaciones de la seguridad de la información.
- Asegurar el ingreso de la información adecuada a los sistemas.
- Adecuarse a las políticas de seguridad y utilizar la información únicamente para los propósitos autorizados.

3.3.4. Propietarios de la información

Los propietarios de la información son los jefes de las oficinas, responsables de la información que se genera y que se utiliza en las operaciones de su oficina. Entre sus responsabilidades están las siguientes:

- Asignar los niveles iniciales de clasificación de información.
- Revisión periódica de la clasificación de la información con el propósito de verificar que cumpla con los requerimientos.
- Asegurar que los controles de seguridad aplicados sean consistentes con la clasificación realizada.
- Determinar los criterios y niveles de acceso a la información.
- Revisar periódicamente los niveles de acceso a los sistemas a su cargo.
- Determinar los requerimientos de copias de respaldo para la información que les pertenece.
- Verificar periódicamente la integridad y la coherencia de la información producto de los procesos de su área.

3.3.5. Auditoría interna

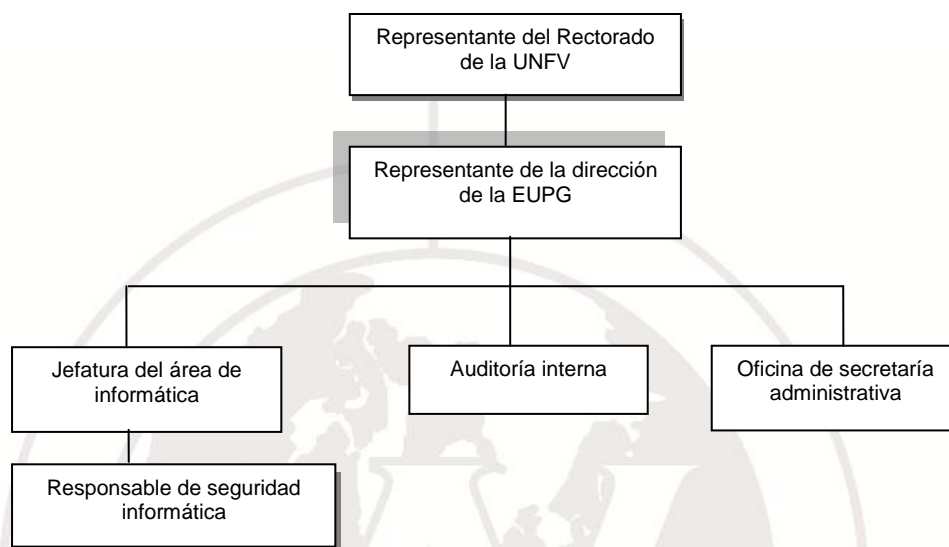
El personal de auditoría es responsable de monitorear el cumplimiento de los estándares y de las guías definidas en las políticas.

3.3.6. Área de seguridad informática propuesto

Dado el volumen de operaciones y la criticidad que presenta la información para los propósitos de la EUPG-UNFV, y tomando como referencia las mejores prácticas, es necesaria la existencia de un área organizacional que administre la seguridad informática. Considerando la falta de una estructura organizacional de seguridad informática en la EUPG-UNFV, se propone que el comité de coordinación esté conformado por las siguientes áreas:

- Representante del rectorado de la UNFV.
- Representante de la dirección de la EUPG-UNFV.
- Responsable de seguridad informática.
- Jefatura del área de Informática.
- Auditoría interna.
- Oficina de secretaría administrativa.

Gráfico N° 3. Comité organizacional propuesto



Este comité determinará el progresivo traslado de la responsabilidad de seguridad al área de Seguridad Informática, y monitoreará las labores realizadas por el área.

IV. RESULTADOS DE LA INVESTIGACIÓN

*Si buscas resultados distintos,
no hagas siempre lo mismo.*

Albert Einstein

*¿Podemos permitirnos el lujo
de jugar sobre seguro?*

Charles Chaplin

En el siguiente capítulo se presentan los resultados obtenidos al tratar de alcanzar los objetivos específicos. En primer lugar, se muestran los resultados del diagnóstico del sistema de seguridad informática que existía antes de formular el plan de seguridad. En segundo lugar, los resultados estadísticos que prueban la eficiencia del plan de seguridad informática propuesto; asimismo, se presenta el contraste de la hipótesis planteada en la presente investigación.

4.1. Diagnóstico de la seguridad informática antes de la formulación del plan

La etapa diagnóstico implica una exploración sobre cuánto conocen los empleados en la EUPG-UNFV acerca de los temas relacionados con los sistemas de información que se emplean con mayor frecuencia, sobre todo los riesgos a los que pudieran estar expuestos los sistemas de información. A pesar de que son personas calificadas, los niveles de evaluación muestran una diferencial en los variados dominios de la tecnología de información.

Como punto de partida, se exploran los conocimientos sobre la exposición al riesgo de los sistemas de información cuando esto no está previamente planificado o adecuadamente protegido. Por tanto, se consideran cuatro factores de exposición al riesgo: recursos tecnológicos, sistemas de información, amenazas informáticas y desastres.

4.1.1. Evaluación de seguridad informática por factores

Se pasa a evaluar en forma detallada los resultados obtenidos en el diagnóstico del sistema de seguridad informática, antes de la formulación del plan.

En el siguiente cuadro se presentan los resultados obtenidos respecto del factor “recursos tecnológicos”, en donde se consideran *hardware* y *software*.

Cuadro 6. Factor de recursos tecnológicos

Recursos tecnológicos	Respuestas				
	Muy mala	Mala	Regular	Buena	Excelente
<i>Hardware</i>	9	10	50	19	12
<i>Software</i>	9	45	35	7	4
Media aritmética	9	27,5	42,5	14	7

De manera específica se exploró acerca de los riesgos o amenazas en lo relacionado con *software* y *hardware*. Los resultados fueron claros: solo el 21 % de los usuarios consideran que la protección ante las amenazas informáticas en *software* y *hardware* son buenos y excelentes; en cambio, la diferencia considera entre regular (42,5 %), mala (27,7 %) y muy mala (9 %), lo que implica que la vulnerabilidad en los recursos tecnológicos es significativa.

Con una metodología similar a la anterior se evaluó la protección para los riesgos con respecto del factor “sistemas de información”, en la que se consideran integridad, confidencialidad, disponibilidad y vulnerabilidad. Los resultados se presentan en forma detallada en el siguiente cuadro.

Cuadro 7. Factor de sistema de información

Sistemas de información	Respuestas				
	Muy mala	Mala	Regular	Buena	Excelente
Integridad	5	40	30	14	11
Confidencialidad	3	45	35	9	8
Disponibilidad	5	55	30	7	3
Vulnerabilidad	6	65	29	0	0
Media aritmética	4,75	51,25	31	7,5	5,5

Según el cuadro 7, el 56 % de los usuarios considera que la protección para los sistemas de información es deficiente, el 31 % considera que es regular, el 7,5 % califica la protección como buena, y, por último, el 5,5 % menciona que es excelente.

En lo que respecta al factor “amenazas informáticas”, se consideran las externas y las internas. Los resultados obtenidos sobre la forma de protección de los factores señalados son presentados en el siguiente cuadro:

Cuadro 8. Factor de amenazas informáticas

Amenazas informáticas	Respuestas				
	Muy mala	Mala	Regular	Buena	Excelente
Externas	3	60	32	3	2
Internas	5	55	32	3	5
Media aritmética	4	57,5	32	3	3,5

En el cuadro 8 se visualizan resultados de los que se desprende que solo el 6,5 % considera que la protección para las amenazas externas e internas es buena y excelente, el 32 % la considera regular y más del 61.5 % la considera mala o muy mala.

Finalmente, en cuanto a la protección para el factor desastres, las medidas preventivas con las que cuenta la EUPG-UNFV, en opinión de los usuarios, tampoco son alentadoras. Los resultados se presentan en el siguiente cuadro:

Cuadro N° 9. Factor de desastre

Desastres	Respuestas				
	Muy mala	Mala	Regular	Buena	Excelente
Naturales	6	36	25	25	8
Inundaciones	4	52	32	12	0
Fuego	9	43	35	9	4
Media aritmética	6,33	43,67	30,67	15,33	4,00

Según el cuadro 9, los resultados evidencian que el 19,33 % la considera que buena o excelente, el 30,67 % considera que es regular y el 50 % de los encuestados consideran que es mala o muy mala.

Producto de la evaluación de los cuatro factores (recursos tecnológicos, sistemas de información, amenazas informáticas y desastre), se analizaron los resultados globales, lo que implica conocer cuánto cree el usuario que los sistemas informáticos están protegidos. En este contexto, estos resultados muestran una tendencia muy similar a la evaluada por factores, y son presentados en el siguiente cuadro:

Cuadro 10. Promedio global de los resultados por factores de la seguridad informática actual

Resultados	Respuestas				
	Muy mala	Mala	Regular	Buena	Excelente
	6,0	45,0	34,0	10,0	5,0

En el cuadro 10 apreciamos que solo el 15 % de los usuarios considera que la seguridad informática en la EUPG–UNFV es buena o excelente, la tercera parte cree que la seguridad actual es regular y más de la mitad cree que es mala o muy mala, lo cual evidencia la falta de un plan de seguridad informática que permita minimizar la vulnerabilidad de los recursos informáticos. Según los resultados obtenidos en el diagnóstico del sistema de seguridad informática actual, y considerando las categorías de las variables que son de medida ordinal tipo Likert, se realizaron algunas operaciones estadísticas, con las que se obtuvieron las puntuaciones directas. Sobre esta base se evaluaron los resultados con los coeficientes de las medidas de tendencia central y de dispersión. Los resultados se presentan en el siguiente cuadro:

Cuadro 11. Resultados descriptivos de las puntuaciones totales del diagnóstico de seguridad informática

Estadísticos	Coefficientes
Media	37.41
Mediana	36,00
Moda	35.00
Desviación típica	12,86
Asimetría	,349
Mínimo	19,00
Máximo	62,00

En el cuadro 11 se aprecia que los valores de media, mediana y moda se encuentran entre las categorías de regular y mala, lo que indica que los usuarios son conscientes de que los mecanismos de seguridad informática con los que cuenta la EUPG-UNFV no son precisamente los más adecuados para evitar las posibles amenazas informáticas. Estos resultados se corroboran con la información de la asimetría, que, al ser positiva, indica que las valoraciones tienden a agruparse en la posición de las menores puntuaciones.

4.2. Análisis de la eficiencia del plan de seguridad informática propuesto

Una vez elaborado el plan de seguridad informática con previsiones teóricas y previo análisis exhaustivo, es preciso probar el funcionamiento de este plan. Para ello se recurrió a una prueba de eficiencia del plan propuesto, desde el punto de vista de las opiniones de los expertos en informática, quienes están involucrados directa e indirectamente de manera permanente con los sistemas de información. Es así que el plan propuesto se agrupa en siete factores básicos: seguridad lógica, comunicaciones, aplicaciones físicas, administración del centro de procesamiento de datos, auditorías y revisiones y plan de contingencia.

4.2.1. Evaluación del plan de seguridad informática por factores

Se pasará a evaluar de forma detallada los resultados obtenidos por factores sobre la percepción de la eficiencia del plan propuesto en la EUPG-UNFV.

En el siguiente cuadro se muestran los resultados con respecto de la seguridad lógica.

Cuadro 12. Seguridad lógica

Seguridad lógica	Respuestas				
	Excelente	Buena	Regular	Mala	Muy mala
Identificación de usuarios	30	70	0	0	0
Autenticación	50	50	0	0	0
Gestión del <i>password</i>	70	30	0	0	0
Segregación de funciones	35	60	5	0	0
Media aritmética	46.25	52.5	1.25	0	0

En el cuadro 12 se aprecia que el 98,75 % de los usuarios considera que la aplicación del presente plan sería entre buena y excelente, solo el 1,25 % considera que sería regular.

Con una metodología similar a la anterior se evaluaron los resultados del factor “seguridad en las comunicaciones”. Se esquematizó en el siguiente cuadro:

Cuadro 13. Seguridad en las comunicaciones

Seguridad en las comunicaciones	Respuestas				
	Excelente	Buena	Regular	Mala	Muy mala
Topología de la red	10	90	0	0	0
Conexiones externos	45	40	15	0	0
Configuración lógica de la red	25	65	10	0	0
Correo electrónico	15	60	25	0	0
Antivirus	90	10	0	0	0
Firewall	40	45	15	0	0
Ataques de la red	50	40	10	0	0
Media aritmética	39,29	50,00	10,71	0	0

Según el cuadro 13, el 89,29 % de los usuarios considera que el plan, de aplicarse, sería entre bueno y excelente; solo el 10,71 % considera que sería regular, y ninguno considera que sería malo o perjudicial.

Al respecto del factor seguridad en las aplicaciones, los resultados obtenidos se esquematizan en el siguiente cuadro:

Cuadro 14. Seguridad en las aplicaciones

Seguridad en las aplicaciones	Respuestas				
	Excelente	Buena	Regular	Mala	Muy mala
<i>Software</i>	10	90	0	0	0
Seguridad de la base de dato	20	65	15	0	0
Control de aplicaciones en computadoras	10	65	25	0	0
Control de datos en las aplicaciones	5	60	35	0	0
Ciclo de vida de las aplicaciones	0	25	50	25	0
Media aritmética	9,00	61,00	25,00	5,00	0

Según el cuadro 14, los resultados con respecto a la seguridad en las aplicaciones son los siguientes: el 70 % considera la entre buena y excelente; el 25 %, regular; y el 5 % considera que no sería beneficiosa.

Con una metodología similar a la anterior se evaluaron los resultados obtenidos al respecto del factor “seguridad física”, lo que se esquematiza en el siguiente cuadro:

Cuadro 15. Seguridad física

Seguridad física	Respuesta				
	Excelente	Buena	Regular	Mala	Muy mala
Equipamiento	20	80	0	0	0
Control de acceso físico al área de informática	15	60	25	0	0
Control de acceso a equipos	0	55	35	10	0
Dispositivos de soporte	5	95	0	0	0
Estructura del edificio	10	55	20	15	0
Cableado estructurado	0	75	25	0	0
Media aritmética	8,33	70,00	17,50	4,17	0

Según el cuadro 15, los usuarios consideran que lo previsto en el plan para la seguridad física oscila entre bueno y excelente (78,33 %). El 17 % lo considera regular; y el 4,17 %, será mala o desfavorable.

Con respecto del factor seguridad en la administración del centro de procesamiento de datos, los resultados obtenidos se esquematizan en forma detallada en el siguiente cuadro:

Cuadro 16. Administración del centro de procesamiento de datos

Administración del centro de procesamiento de datos	Respuesta				
	Excelente	Buena	Regular	Mala	Muy mala
Administración del área de					
Informática	65	30	5	0	0
Capacitación	30	70	0	0	0
<i>Backup</i>	65	35	0	0	0
Documentación	30	45	25	0	0
Media aritmética	47,5	45,00	7,5	0	0

Según el cuadro 16, en los resultados con respecto del plan de seguridad contemplado para la administración del centro de procesamiento de datos, el 92,5 % lo considera entre bueno y excelente; el 7,5 %, regular; y ninguno considera que sea desfavorable. Por lo tanto, el plan propuesto es favorable y contundente para las necesidades de la EUPG-UNFV.

Con una metodología similar a la anterior se evaluaron los resultados obtenidos al respecto del factor de auditorías y revisiones, lo que se esquematiza en el siguiente cuadro:

Cuadro 17. Auditorías y revisiones

Auditorías y revisiones	Respuesta				
	Excelente	Buena	Regular	Mala	Muy mala
Revisión del sistema	45	50	5	0	0
Responsabilidades de los encargados de seguridad	10	80	10	0	0
Auditoría de control de acceso a los sistemas	75	25	0	0	0
Auditoría de redes	85	15	0	0	0
Media aritmética	53.75	42.5	3.75	0	0

En el cuadro 17 se muestran los resultados con respecto a auditorías y revisiones: el 96,25 % las considera entre buenas y excelentes; el 3,75 %, regular; y ninguno considera que fueran desfavorables, lo que evidencia la eficiencia del plan propuesto.

Con respecto al factor plan de contingencia, los resultados obtenidos se esquematizan en forma detallada en el siguiente cuadro.

Cuadro 18. Plan de contingencia

Plan de contingencia	Respuesta				
	Excelente	Buena	Regular	Mala	Muy mala
Plan de administración de incidentes	20	60	19	0	1
Backup de equipamiento	15	85	0	0	0
Estrategias de Recuperación de desastres	5	54	40	0	1
Media aritmética	13,33	66,33	19,63	0	0,67

Según el cuadro 18, en cuanto a los resultados relacionados con el plan de contingencia, el 79,67 % de los usuarios considera que lo previsto en el plan de seguridad sería bueno o excelente; el 19,63 % cree que sería regular; por último, el 0,67% menciona que no sería eficiente. Por tanto, el plan propuesto es adecuado para las necesidades de la EUPG-UNFV.

Producto de la evaluación de los siete factores del plan propuesto, se analizan los resultados globales, lo que implica conocer la eficiencia del plan, en opinión de los usuarios expertos en informática, lo que se esquematiza en forma detallada en el siguiente cuadro:

Cuadro 19. Promedio global de los resultados por factores del plan propuesto

Resultados	Excelente	Buena	Regular	Mala	Muy mala
	31,06	55,33	12,20	1,00	1,00

Según el cuadro 19, los resultados obtenidos por cada factor del plan de seguridad informática propuesto son contundentes y se relacionan con los resultados globales: el 86,40 % considera que el plan, de aplicarse, estaría considerado entre bueno y excelente; el 12,20 % de los usuarios considera que el plan sería regular si se aplicase; y solo el 2 % considera que el plan sería desfavorable.

— No obstante, el soporte de estos resultados guarda relación con el criterio de los usuarios expertos en informática, puesto que son personas que están directamente vinculadas con el uso permanente de los sistemas de información.

En el siguiente cuadro se presentan detalladamente los resultados estadísticos obtenidos, que evidencian la eficiencia del plan propuesto en la presente investigación.

Cuadro 20. Resultados descriptivos de las puntuaciones totales-eficiencia del plan de seguridad informática

Estadísticos	Coefficientes
Media	136,8500
Mediana	138,0000
Moda	109,00(a)
Desviación típica	14,86173
Asimetría	-,249
Mínimo	109,00
Máximo	162,00

Después de desarrollar algunas operaciones aritméticas con los datos de los diversos ítems, se determina la puntuación total de la evaluación sobre seguridad informática. Los valores de las puntuaciones totales oscilan entre 33 y 165. Atendiendo a cuatro cortes teóricos, con sus categorías evaluativas respectivas, quedarían de la siguiente forma: puntuaciones menores e iguales a 66, se considera que el plan no sería eficiente en absoluto; entre 67 a 99, con regular eficiencia; de 100 a 132, el plan sería bueno; finalmente, de 133 a más, el plan sería excelente.

Como se puede apreciar en el cuadro 20, se tiene que en las dos medidas de tendencia central (media y mediana) los coeficientes de 136,85 y de 138.00, respectivamente, se ubican en el rango de excelente; además, se aprecia de manera contundente que la distribución se presenta con sesgo negativo o hacia la izquierda, lo que indica que las puntuaciones se concentran en el intervalo de la categoría de excelente. El plan de seguridad sería excelente en opinión de los usuarios expertos en informática.

4.3. Prueba sobre la eficiencia del plan de seguridad informática propuesto

Se comparan los resultados obtenidos sobre la percepción de los usuarios respecto de la protección o plan de seguridad informática en la EUPG–UNFV antes de la implementación del plan, al que se ha denominado “diagnóstico”, con los resultados de la percepción después de la formulación del plan de seguridad informática. A esto último se denominó “eficiencia probada de la implementación del plan de seguridad informática propuesto”.

Para demostrar la eficiencia del plan propuesto es necesario contrastar las hipótesis planteadas. A continuación se presenta la demostración de las mismas.

4.3.1. Prueba o contraste de hipótesis

Las respuestas sobre la seguridad informática dependen de si se implementa o no el plan propuesto.

Ho: Independencia de las variables.

H1: Dependencia de las variables.

Si $P \leq 0,05$ rechazo Ho.

Con la finalidad de conocer si existe dependencia o no entre las categorías de las variables, antes y después, se somete a las pruebas no paramétricas chi cuadrado y coeficiente de Pearson, cuyos resultados se presentan a continuación:

Cuadro 21. Prueba de la eficiencia del plan de seguridad informática propuesto

Momento evaluación		Respuestas					Total	
		Muy mala	Mala	Regular	Bueno	Excelente		
Antes	Recuento	6	45	34	10	5	100	
	Frecuencia esperada	3,5	23	23	32,5	18	100	
	Residuo	2,5	22	11	-22,5	-13		
	Residuos tipificados	1,3	4,6	2,3	-3,9	-3,1		
	Después	Recuento	1	1	12	55	31	100
Después	Frecuencia esperada	3,5	23	23	32,5	18	100	
	Residuo	-2,5	-22	-11	22,5	13		
	Residuos tipificados	-1,3	-4,6	-2,3	3,9	3,1		
	Total	Recuento	7	46	46	65	36	200
	Frecuencia Esperado	7	46	46	65	36	200	

En el cuadro 21, denominado “cuadro de contingencia”, se presentan las respuestas en porcentajes de los usuarios antes de la formulación del plan versus las respuestas después de la prueba de la eficiencia del plan propuesto. Se incorporan los residuos tipificados para conocer la relación entre las categorías.

En los siguientes cuadros se presentan la prueba chi cuadrado y las medidas simétricas respectivamente.

Cuadro 22. Prueba chi cuadrado

	Valor	gl	Sig. asintótica (bilateral)
Chi-cuadrado de Pearson	106,112 (a)	4	,000
Razón de verosimilitud	124,253	4	,000
Asociación lineal por lineal	89,546	1	,000
N.º de casos válidos	200		

a. 2 casillas (20,0 %) tienen una frecuencia esperada inferior a 5. La frecuencia mínima esperada es 3,50.

Con un valor chi cuadrado de 106,112, 4 grados de libertad y una probabilidad de 0.00, se rechaza la hipótesis nula y se afirma que sí hay dependencia; es decir, difieren las respuestas de antes y las de después. Las dependencias están fuertemente asociadas (0,728), y significativa (P = 000), esto último ha sido evaluado con el coeficiente V de Cramer (ver cuadro de medidas simétricas).

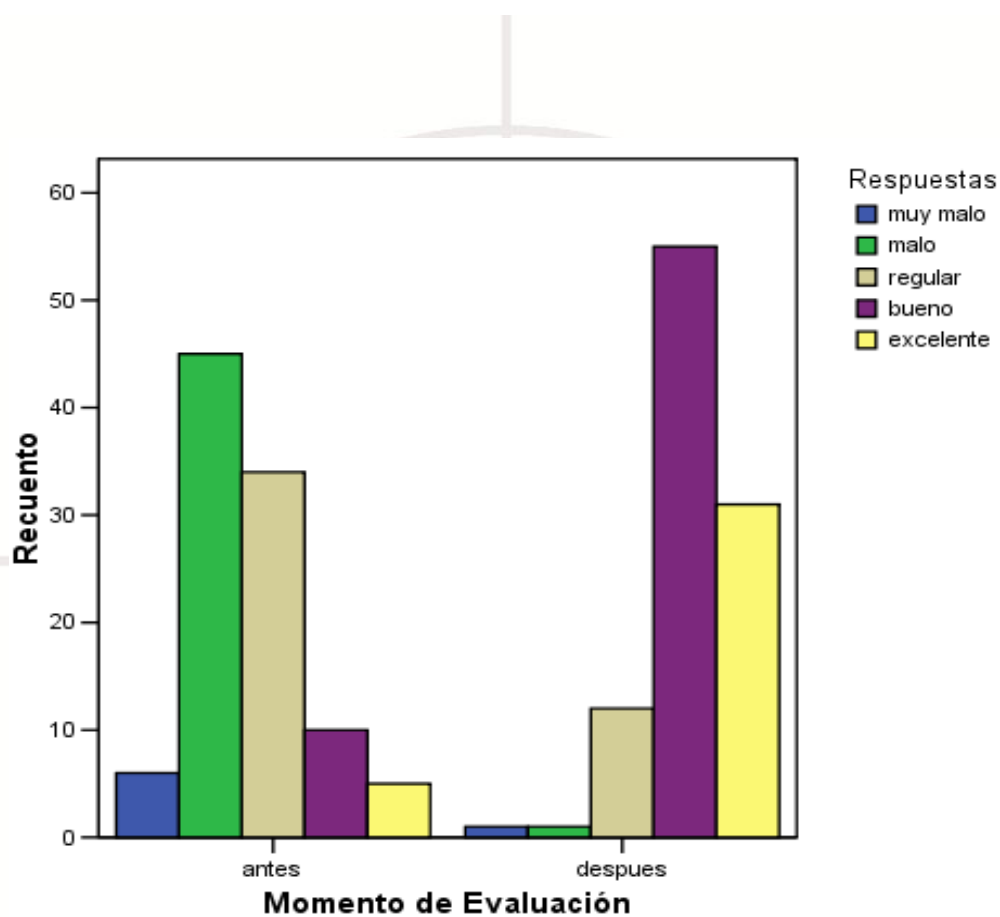
Cuadro 23. Medidas simétricas

		Valor	Sig. aproximada
Nominal por nominal	Phi	,728	,000
	V de Cramer	,728	,000
N de casos válidos		200	

a Asumiendo la hipótesis alternativa.
b Empleando el error típico asintótico basado en la hipótesis nula.

Con los resultados de los residuos tipificados, se tiene que las respuestas respecto de la protección con que cuenta la información de la EUPG–UNFV en la fase de diagnóstico se encuentran entre “regular”, “mala” y “muy mala” (2,3, 4,6 y 1.3), respectivamente; en cambio; las respuestas sobre la formulación del plan de seguridad informática propuesto se encuentran entre “bueno” y “excelente” (3,9 y 3,1), respectivamente. De manera visual, estos resultados se aprecian también en el gráfico 4. En definitiva, el plan propuesto se muestra eficiente.

Gráfico 4. Eficiencia del plan de seguridad informática propuesto



V. DISCUSIÓN

El propósito general de esta investigación está centrado en probar la eficiencia del plan de seguridad informática propuesto, a fin de prevenir y salvaguardar la información. El plan no hubiera sido posible sin previa evaluación del estado actual en el que se encuentra la seguridad informática de la EUPG–UNFV, a lo que se ha denominado “etapa diagnóstico”. Sobre esa base, se elaboró un plan acorde con las necesidades de la institución.

Por un lado, está claro que los participantes en este estudio deberían ser todos aquellos que de alguna forma están involucrados directamente con el manejo de los sistemas de información.

En la primera etapa participaron 38 empleados y la escala de recopilación de información constó de 15 ítems tipo Likert, con una fiabilidad total de $\alpha = 0,879$ (ver cuadro 4). En la segunda etapa se puso a prueba la eficiencia del plan propuesto, bajo un criterio de comprobación. En esta oportunidad participaron 20 empleados, con el criterio de mayor dominio y especialización técnica en el manejo de los sistemas de información. Los resultados de la primera parte, en general, fueron claros y contundentes: los empleados ponen de manifiesto la seria exposición de riesgos y de amenazas informáticas en la que se encuentra la información de la EUPG–UNFV. Las respuestas cualitativas la catalogan entre “regular”, “mala” y “muy mala”, que concentra el 85 % de las respuestas (ver cuadro 10). Esto se corrobora con la distribución de asimetría hacia la derecha en las puntuaciones directas (ver cuadro 11). En definitiva, esto no hace más que

corroborar que el estado actual de seguridad informática no es el más apropiado para el desarrollo adecuado de la institución. Se evalúan también de manera detallada los factores en la etapa diagnóstico: recursos tecnológicos, sistemas de información, amenazas informáticas y desastres. Las respuestas de los participantes se concentraron en las categorías de “regular”, “mala” y “muy mala”; así, para el factor de recursos tecnológicos (79 %), factor de sistemas de información (87 %), amenazas informáticas (93,5 %) y desastre (80,67 %). Se recomienda revisar los cuadros 6, 7, 8 y 9. El análisis exhaustivo de la teoría, complementado con las opiniones de expertos por consenso, fueron el punto de partida para formular el plan propuesto, al que fue necesario someter a una evaluación para probar su eficiencia, desde luego, en condiciones a modo de prueba; en esta oportunidad participó un grupo selecto con mayor dominio y profesionalización, escogido entre los que habían participado anteriormente. Los resultados fueron analizados de manera global y por factores tales como seguridad lógica, seguridad en las comunicaciones, seguridad en las aplicaciones, seguridad física, administración del centro de procesamiento de datos, auditorías y revisiones y plan de contingencia.

Con una distribución de asimetría a la izquierda y una media de 136,85 (ver cuadro 20), estos resultados se ubican cualitativamente en un rango de bueno y excelente. Los indicadores se muestran algo similar por factores: descienden los porcentajes en la categoría de regular y prácticamente desaparecen en las categorías de mala y muy mala (ver los cuadros 12, 13, 14, 15 16, 17 y 18). Estas valoraciones cualitativas fueron probadas a través de un contraste de hipótesis. El objetivo central era probar el cambio significativo de la percepción de la seguridad informática actual con la percepción del plan propuesto. La aplicación de chi cuadrado permitió corroborarlo, afirmando que el cambio es significativo (ver los cuadros 21, 22 y 23), lo que da fe de la eficiencia del plan en condiciones de prueba.

VI. CONCLUSIONES Y RECOMENDACIONES

6.1 Conclusiones

Luego de recopilar, analizar y contrastar la información, se llegó a las siguientes conclusiones:

1. Sin la aplicación del plan de seguridad informática, se demostró que el estado actual de la seguridad informática en la EUPG–UNFV es deficiente para las necesidades del complejo de información que maneja.
2. Luego de someter el plan propuesto al juicio de los expertos en informática de la EUPG-UNFV, se apreció una mejora sustancial en la seguridad informática.
3. La mejora en la percepción de la seguridad informática demuestra la eficiencia del plan propuesto en la EUPG-UNFV.

6.2. Recomendaciones

1. Muchas de las amenazas informáticas están relacionadas por factores externas e internas; por otro lado, derivan por el mal uso de las tecnologías de la información, por lo que se sugiere realizar campañas de capacitación a todo el personal, las mismas que tendrían que estar orientadas bajo los conceptos básicos de seguridad, y a grupos específicos con temas correspondientes a sus responsabilidades.
2. Sería interesante realizar un análisis del costo y del tiempo como consecuencias de la falta de prevención de los sistemas de información. Esto puede concientizar a la institución a analizar la probabilidad de que ocurran ciertos sucesos, para lo cual la alta gerencia debe determinar las consecuencias que traerían el costo y productividad por la pérdida de información, clientes, confianza de los usuarios y costos asociados con las soluciones de seguridad informática.
3. Finalmente, se recomienda considerar las sugerencias del plan propuesto, para minimizar las amenazas tanto externas como internas, a fin de proteger la información de valía para la EUPG–UNFV.

REFERENCIAS BIBLIOGRÁFICAS

Libros

- Alcórcer C. (2000). *Seguridad de redes de computadoras*. 2.^a ed. Lima: Inforlink; 440 pp.
- Ávila, R. (2001). *Metodología de la investigación*. Lima: Ra-Ma.
- Campbell, P. (1998). *Redes para la pequeña y mediana empresa*. Buenos Aires: Hasa; 317 pp.
- Cariacedo J. (2004). *Seguridad en redes telemáticas*. Madrid: McGraw-Hill Interamericana; 548 pp.
- Echenique J. (1999). *Auditoría en informática*. Argentina: Mc. Graw Hill Interamericana; 456 pp.
- Gómez A. (2006). *Enciclopedia de la seguridad informática*. España: Ra-Ma; 690 pp.
- Gonzales J. (2000). *Seguridad profesional en Windows NT*. México: Alfa Omega; 307 pp.
- Joyanes L. (1997). *Cibersociedad: los retos sociales ante un nuevo mundo digital*. Madrid: McGraw-Hill Interamericana; 533 pp.
- Henríquez E. (2001). *Auditoría en informática*. Colombia: Ceca; 128 pp.
- Hernández R. (2006). *Metodología de la investigación*. México: McGraw Hill Interamericana; 250 pp.
- Lardent A. (2001). *Sistemas de información para la gestión empresarial-procedimientos, seguridad y auditoría*. Buenos Aires: Pearson Educación; 443 pp.
- Maiwald E. (2003). *Fundamentos de seguridad de redes*. México: McGraw-Hill Interamericana; 475 pp.
- Marcelo J. (1999). *Riesgo y seguridad de los sistemas de información*. España: Universidad Politécnica de Valencia; 423 pp.

- Oppliger R. (1998). *Sistemas de autenticación para seguridad en redes*. Santa Fe, Bogotá: Alfa Omega; 187 pp.
- Raya J. (2000). *La seguridad de una red con Netware 5*. México: Alfa Omega; 178 pp.
- Ribagorda M. (1994). *Seguridad y protección de la información*. España: Ramón Areces.
- Steven B. (2001). *Implementación de redes privadas virtuales (RPV)*. México: McGraw-Hill Interamericana; 395 pp.

Revistas

- Muller H. (2002). "Los delitos informáticos en el Código Penal". *Revista Policial N.º 81*; 39 pp.
- Núñez J. (1999). "Los delitos informáticos". *Revista de Derecho* [8 páginas]. [Consultado el 10 de setiembre de 2007]. Disponible en <http://www.alfa-redi.org/rdi-articulos.htm l?x=343>


Tesis

- Borghello C. (2001). *Seguridad informática sus implicancias e implementación*. (Tesis de licenciatura en Sistemas). Argentina: Universidad Tecnológica Nacional; 365 pp.
- Mugica O. (2006). *La gestión del conocimiento aplicada a la auditoría de sistemas de información empresarial*. (Tesis doctoral en Ingeniería). Lima: UNFV-EUPG; 239 pp.
- Murillo S. (2001). *Diseño y aplicación de un sistema integral de seguridad informática para la UDLA*. (Tesis de maestría en Ciencias, con especialidad en Ingeniería en Sistemas Computacionales). México: Universidad de las Américas; 310 pp.

Páginas web

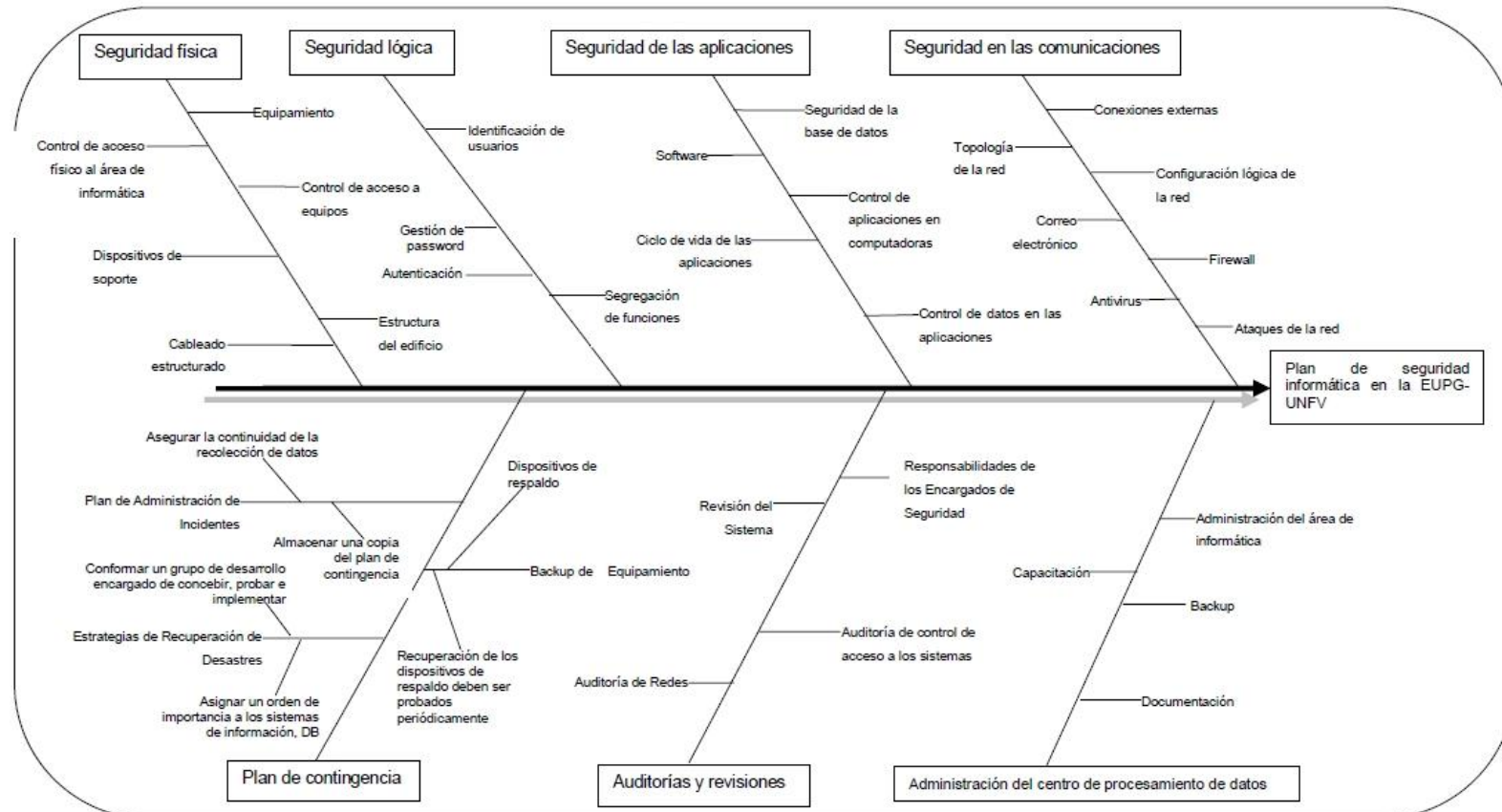
- Alberto G. (2006). *Implantación del ISO-2700:2005 “Sistema de gestión de seguridad de información”*; 36 pp. [Consultado el 10 de junio de 2007]. Disponible en http://www.centrum.pucp.edu.pe/excelencia/ensayos/Implantacion_del_ISO_27001_2005.pdf
- Cao J. (2005). *Análisis y gestión de riesgos de la seguridad de los sistemas de la información*; 14 pp. [Consultado el 11 de mayo de 2007]. Disponible en http://www.cii-murcia.es/informas/abr05/articulos/Analisis_gestion_riesgos_seguridad_sistemas_informacion.php
- Instituto Nacional de Estadística e Informática (INEI). (1997). *Plan de contingencia y seguridad de la información*; 117 pp. [Consultado el 20 de junio de 2007]. Disponible en <http://www.inei.gob.pe/biblioinei.asp>
- Instituto Nacional de Estadística e Informática (INEI). (2000). *Resumen de la guía metodológica: elaboración del plan de contingencias*; 35 pp. [Consultado el 25 de junio de 2007]. Disponible en <http://www.inei.gob.pe/biblioinei.asp>
- Instituto Nacional de Estadística e Informática. (INEI). (2001). *Delitos informáticos*; 72 pp. [Consultado el 28 de junio de 2007]. Disponible en <http://www.inei.gob.pe/biblioinei.asp>
- Ituribe F. (2002). *British Standard 7799-2:2002*; 4 pp. [Consultado el 4 de junio de 2007]. Disponible en <http://www.cybsec.com/upload/Cybsec-Norma-BS7799-2.pdf>
- Minguet J. (1997). *Introducción a la seguridad informática*; 35 pp. [Consultado el 10 de abril de 2007]. Disponible en <http://www.uned.es/413042/material/IntroSegInformática.doc>

- Naciones Unidas (NU). (1998). *Tipos de delitos informáticos*; 45 pp. [Consultado el 25 de junio de 2007]. Disponible en <http://www.delitosinformaticos.com/delitos/elitosinformaticos2.html>
- Oficina Nacional de Gobiernos Electrónicos e Informáticas (ONGEI). (2007). *Tecnología de la información. Código de buenas prácticas para la gestión de la seguridad de la información*; 180 pp. [Consultado el 3 de junio de 2007]. Disponible en <http://www.ongei.gob.pe/normativas/>
- Yory J. (2006). *Mejores prácticas de seguridad de información ISO 17799:2005*; 30 pp. [Consultado el 9 de agosto de 2007]. Disponible en http://www.Mvausa.Com/Colombia/Presentaciones/INTRODUCCION_ISO17799.pdf
- Temas relacionados con investigación, desarrollo, informes y documentos.* Disponible en <http://www.criptored.upm.es/paginas/investigacion.htm>
- Implantación de un sistema de gestión de seguridad de la información.* Disponible en http://www.csi.map.es/csi/tecniemap/tecniemap_2006/tema_01.htm
- Guía de planeamiento de la seguridad de las cuentas de administrador.* Disponible en <http://www.microsoft.com/latam/technet/seguridad/default.aspx>
- Buenas prácticas en la administración de la evidencia digital.* Disponible en <http://www.virusprot.com/Articulo.html>
- Términos relacionados con la seguridad informática. Disponible en http://es.wikipedia.org/wiki/Seguridad_inform%C3%A1tica
- Gestión de seguridad de la información ISO 27001.* Disponible en <http://iso9001-iso27001-gestion.blogspot.com/2006/09/itil-y-la-norma-isoiec-20000.html>



	ANEXOS	
Anexo 1		155
Anexo 2		156
Anexo 3		159
Anexo 4		165
Anexo 5		166
Anexo 6		169

Anexo 1. Modelo de Ishikawa del plan de seguridad informática propuesto



Anexo 2. Evaluación de los factores de riesgo de seguridad informática

La evaluación de los factores de riesgo de la seguridad informática en la EUPG-UNFV ha sido desarrollada con el propósito de determinar qué activos tienen mayor vulnerabilidad ante las amenazas informáticas, tanto externas como internas, y que pueden afectarla considerablemente. Se desarrollaron los siguientes aspectos:

- a. **Listado de los recursos informáticos.** Se evaluaron los distintos activos físicos y de *software*, generando un inventario de aquellos que son considerados como vitales para el desarrollo adecuado de la EUPG-UNFV.
- b. **Definición de factores de riesgo.** Se listaron los factores de riesgo que realmente pueden verse sometidos a cada uno de los activos informáticos mencionados.

Activos y factores de riesgos

Los distintos activos informáticos reconocidos en la EUPG-UNFV como vulnerables, así como los factores de riesgo que pueden afectar a dichos activos, son los siguientes:

Nº	Activos a proteger
1	Servidor
2	Base de dato
3	Software de aplicación, programas fuente, sistemas operativos
4	Backup
5	Cableado, switch, hubs.
6	Red de datos
7	Documentación de programas, hardware, sistemas, procedimientos administrativos locales, manuales, etc.
8	Hardware (teclado, monitor, unidades de discos)
9	Insumos (cintas, cartuchos de tinta, toner, papel, formularios, etc.)
10	Datos de los usuarios

N°	Factores de riesgo
1	Acceso no autorizado a datos (borrado, modificación, etc.)
2	Administración impropia del sistema de tecnología de información
3	Almacenamiento negligente de passwords
4	Configuración inadecuada de los componentes de la red
5	Copia no autorizada de un medio de datos
6	Corte de luz, UPS descargado o variaciones de voltaje.
7	Descripción de archivos inadecuado
8	Documentación insuficiente o faltante
9	Errores de software
10	Factores ambientales
11	Falla de base de datos
12	Falla del sistema
13	Falta de auditorías
14	Falta de espacio de almacenamiento
15	Límite de vida útil - Máquinas obsoletas
16	Longitud de los cables de red
11	Mal uso de derechos de administrador
18	Medios de datos no están disponibles cuando son necesarios
19	Modificación no autorizada de datos
20	Pérdida de backups
21	Perdida de confidencialidad en datos privados y de sistema
22	Portapapeles, impresoras o directorios compartidos
23	Riesgo por el personal de limpieza o personal externo
24	Robo de información
25	Seguridad de base de datos deficiente
26	Software desactualizado
27	Virus, gusanos y caballos de Troya

Anexo 3. Glosario

Activo: Recurso del sistema de información o relacionado con este, necesario para que la organización funcione correctamente y alcance los objetivos propuestos.

Amenaza: Cualquier evento que pueda provocar daño en los sistemas de información, produciendo a la empresa pérdidas materiales, financieras o de otro tipo.

Ataque: Acción intencional e injustificada (desde el punto de vista del atacado). Intento por romper la seguridad de un sistema o de un componente del sistema.

Datos: En general, se considera como datos tanto los estructurados como los no estructurados, las imágenes, los sonidos, etc.

Datos encriptados: Es la información que ha sido convertida de texto simple a texto cifrado.

Datos personales: Véase información personal identificable.

Decriptación: Es el proceso de convertir los datos encriptados de regreso a su forma original.

Eficiencia: Es la capacidad de disponer de alguien o de algo para conseguir un efecto determinado.

Elección: Es la habilidad de un individuo para determinar cómo la información personal identificable reunida de él o ella puede ser utilizada, especialmente para propósitos más allá de aquellos para los cuales se proporcionó la información originalmente.

Elevación de privilegios: Proceso mediante el cual el usuario engaña al sistema para que le otorgue derechos no autorizados, usualmente con el propósito de comprometer o destruir el sistema.

Encriptación: Se refiere al proceso de convertir datos en texto cifrado para evitar que terceras personas lo puedan ver o acceder.

Filtro: Patrón o máscara a través del cual la información es pasada para separar elementos específicos. Por ejemplo, un filtro utilizado en correo electrónico o al recobrar mensajes de un grupo de noticias puede permitir a los usuarios descartar automáticamente mensajes que vienen de usuarios específicos.

FTP: (File Transfer Protocol). Protocolo parte de la arquitectura TCP/IP utilizado para la transferencia de archivos.

Firewall: Es un dispositivo que se utiliza para proteger una computadora o una red interna de intentos de acceso no autorizados desde Internet, denegando las transmisiones y vigilando todos los puertos de red. Su uso más común es situarlo entre una red local y la red de Internet, evitando que los intrusos puedan atacar o acceder la red de computadoras local.

Firma digital: Es la información incluida con un mensaje o transmitida separadamente que se utiliza para identificar y autenticar al emisor y la información del mensaje. Una firma digital también puede confirmar que el mensaje no haya sido alterado.

HUB: En castellano, *concentrador*. Es un dispositivo electrónico que permite centralizar el cableado de una red.

HTTP: (protocolo de transferencia de hipertexto-HyperText Transfer Protocol). Es el protocolo usado en cada transacción de la web (www). El hipertexto es el contenido de las páginas web, y el protocolo de transferencia es el sistema mediante el cual se envían las peticiones de acceso a una página y la respuesta con el contenido. También sirve el protocolo para enviar información adicional en ambos sentidos, como formularios con campos de texto.

IEC: Comisión Electrotécnica Internacional (International Electrotechnical Commission).

Incidente de seguridad: Cualquier evento que tenga o pueda tener como resultado la interrupción de los servicios suministrados por un sistema de Información y/o pérdidas físicas, de activos o financieras. En otras palabras, la materialización de una amenaza, pues, como no existe el riesgo cero, siempre es posible que una amenaza deje de ser tal para convertirse en una realidad.

Información: Es conjunto de datos significativos y pertinentes que describen sucesos o entidades.

Impacto: Es la medición y valoración del daño que podría producir a la organización un incidente de seguridad. La valoración global se obtendrá sumando el coste de reposición de los daños tangibles y la estimación, siempre subjetiva, de daños intangibles tales como la calidad del servicio y la imagen de la organización.

IP: Dirección de 32 bits definida por el protocolo de Internet.

LAN: Surgieron a partir de la revolución de la PC. Las LAN permitieron que varios usuarios ubicados en un área geográfica relativamente pequeña pudieran intercambiar mensajes y archivos.

Log: Registro de actividad de un sistema, que generalmente se guarda en un fichero de texto, al que se le van añadiendo líneas a medida que se realizan acciones sobre el sistema. A través de los logs se puede encontrar información para detectar posibles problemas en caso de que no funcione algún sistema como debiera o de que se haya producido una incidencia de seguridad.

Proxy: El proxy es un servidor que, conectado normalmente al servidor de acceso a la www de un proveedor de acceso, va almacenando toda la información que los usuarios reciben de la web; por tanto, si otro usuario accede a través del proxy a un sitio previamente visitado, recibirá la información del servidor proxy en lugar del servidor real.

Usuarios: Individuos que utilizan la estructura tecnológica y de comunicaciones que manejan la información.

SPAM¹: Correo no deseado o mensajes no solicitados, habitualmente de tipo publicitario, enviados en cantidades masivas que perjudican de una u otra manera al receptor.

SMTP: (Simple Mail Transfer Protocol). Protocolo simple de transferencia de correo electrónico. Protocolo de red basado en texto utilizado para el intercambio de mensajes de correo electrónico entre computadoras o distintos dispositivos.

TI: Tecnología de la información.

Recurso de recuperación: Recurso necesario para la recuperación de las operaciones en caso de desastre, como las cintas magnéticas de salvaguarda o los equipos de respaldo.

Riesgo: Es la probabilidad de que una amenaza se materialice sobre una vulnerabilidad del sistema informático, causando un impacto en la empresa. Evidentemente, el riesgo es característico para cada amenaza y cada sistema, pudiéndose disminuir tomando las medidas adecuadas.

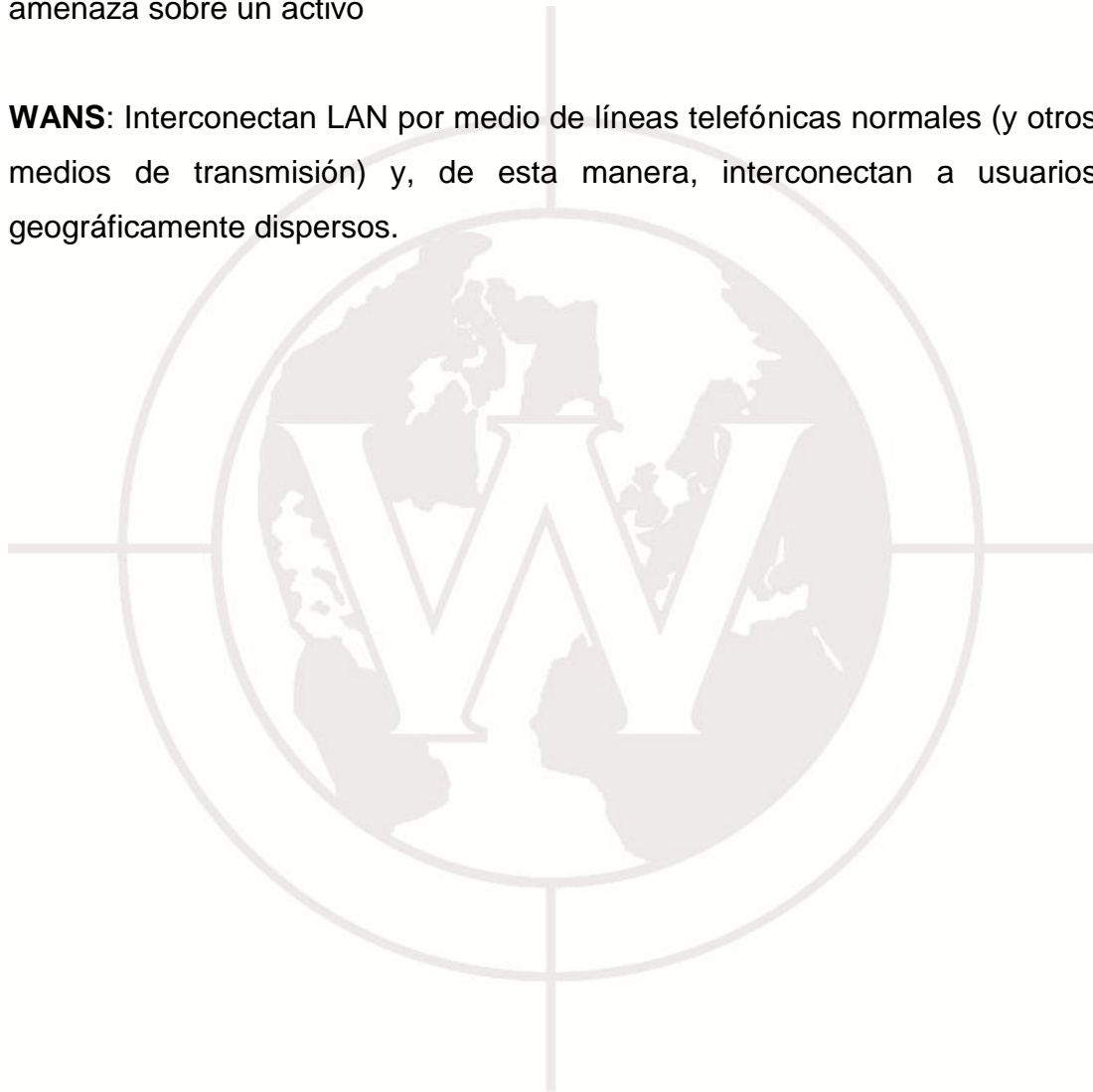
Redes: Interconectan computadoras con distintos sistemas operativos, ya sea dentro de una empresa u organización (LAN) o por todo el mundo (WAN, Internet).

¹ Mediante Ley N.º 28493 se aprobó la Ley que regula el uso del correo electrónico comercial no solicitado (SPAM). El objetivo de la Ley objeto es la regulación del envío de comunicaciones comerciales publicitarias o promocionales no solicitadas, realizadas por correo electrónico; el artículo 10º de la citada Ley establece que el Poder Ejecutivo, mediante decreto supremo refrendado por el Ministro de Transportes y Comunicaciones, la reglamentará.

Tecnología: Conjunto de saberes, destrezas y medios necesarios para llegar a un fin predeterminado (como el *software* y el *hardware*; los sistemas operativos; los sistemas de gestión de base de datos).

Vulnerabilidad: Posibilidad de ocurrencia de la materialización de una amenaza sobre un activo

WANS: Interconectan LAN por medio de líneas telefónicas normales (y otros medios de transmisión) y, de esta manera, interconectan a usuarios geográficamente dispersos.



Anexo 4. Encuesta acerca de la situación actual de seguridad informática en la EUPG-UNFV

La siguiente encuesta tiene como finalidad de analizar la situación actual de la seguridad informática a modo de diagnóstico. Por tanto, sírvase rellenar con un aspa en los casilleros correspondientes, según a su percepción del tema motivo de la investigación:

Valoración de las respuestas

(5) Excelente	(4) Buena	(3) Regular	(2) Mala	(1) Muy mala
---------------	-----------	-------------	----------	--------------

Nº	Cuestionario	Valoración				
		1	2	3	4	5
1	¿A su criterio como considera la seguridad relacionado al hardware?					
2	¿A su criterio en qué medida evalúa la integridad de los sistemas de información?					
3	¿De qué manera se realiza la revisión periódica de los sistemas de información?					
4	¿La confidencialidad de los sistemas de información, a su criterio en qué forma se encuentra?					
5	¿A su criterio las amenazas externas, en qué forma están identificadas?					
6	¿A su criterio, en qué forma están protegidos los sistemas de información, al respecto de las amenazas naturales?					
7	¿La disponibilidad de los sistemas de información, a su criterio en qué forma se encuentra?					
8	¿La Seguridad al respecto de software, en qué forma está protegida?					
9	¿En qué manera, la vulnerabilidad de los sistemas de información está identificada y minimizada?					
10	¿La información que usted utiliza, de qué manera está protegida?					
11	¿En qué manera está usted, capacitado en seguridad informática?					
12	¿En que medida están identificadas las amenazas internas, existe alguna medida para minimizarlas?					
13	¿A su criterio, los desastres de inundación, en qué medida se encuentran?					
14	¿Los desastres relacionados con el fuego, a su criterio en qué forma están identificados?					
15	¿De qué manera está definido el nivel de acceso a los recursos informáticos?					

Sobre la eficiencia del plan seguridad informática propuesto

El objetivo de la encuesta es conocer la percepción de los expertos en sistemas de información sobre el plan de seguridad informática propuesto. La misma consiste en saber la percepción de la eficiencia del plan de seguridad informática propuesto. Tiene por objetivo poner en prueba el plan formulado, según la percepción de los expertos. Por tanto, sírvase rellenar con un aspa en los casilleros correspondientes, según su conocimiento.

Anexo 5. Encuesta acerca de la eficiencia del plan de seguridad informática propuesto

Valoración de las respuestas									
(5) Excelente		(4) Buena		(3) Regular		(2) Mala		(1) Muy mala	

Nº	Preguntas	Valoración				
		1	2	3	4	5
1	¿La identificación de los usuarios, según el plan propuesto, permitirá mejorar la administración de forma?					
2	¿El plan propuesto al respecto a la topología de red, de qué manera permitirá fortalecer la seguridad informática?					
3	¿Según el plan propuesto la administración de incidentes, de qué manera permitirá mejorar la continuidad de la información?					
4	¿Mediante el plan propuesto el equipamiento del sistema de información, de qué manera mejorara?					
5	¿El plan propuesto al respecto de la autenticación de los usuarios, de qué manera permitirá mejorar la seguridad informática?					
6	¿Las conexiones externas, de que manera mejoraran con el plan propuesto?					

Nº	Preguntas	Valoración				
		1	2	3	4	5

7	¿La seguridad de la base de datos, de qué manera mejorara con el plan propuesto?						
8	¿El control de acceso físico al Centro de Cómputo, de qué manera mejorara con el plan propuesto?						
9	¿El plan propuesto referente al password, mejorara el acceso al sistema de información de forma?						
10	¿La administración del Centro de procesamiento de datos, de qué manera mejorara con el plan propuesto?						
11	¿El plan propuesto referente al software que se utiliza en la EUPG, de qué manera permitirá mejorar la seguridad informática?						
12	¿La configuración lógica de la red, mediante el plan propuesto de qué forma permitirá mejorar la seguridad?						
13	¿La revisión de los sistemas de información, de qué manera mejorara con el plan propuesto?						
14	¿La segregación de funciones, permitirá mejorar las responsabilidades en el uso adecuado de la información en forma?						
15	¿La capacitación al personal referente al uso adecuado de la tecnología de información, de qué manera permitirá mejorar la seguridad?						
16	¿El control de aplicaciones en las PC'S, de qué manera mejorara mediante el plan propuesto?						
17	¿El plan propuesto al respecto del uso de correo electrónico, de qué manera permitirá mejorar el uso de la misma?						
18	¿El control de acceso a equipos, de qué forma mejorara con el plan propuesto?						
19	¿Las responsabilidades de los encargados de seguridad informática, mediante el plan propuesto, de qué manera permitirán mejorar la seguridad?						
20	¿El control de datos en las aplicaciones, de qué manera mejorara, con el plan propuesto?						
Nº	Preguntas	Valoración					
		1	2	3	4	5	

21	¿La implementación del antivirus adecuado, de qué manera permitirá fortalecer la seguridad informática?							
22	¿La generación de los backup, adecuadamente documentada, de qué manera permitirá mejorar la continuidad de la información?							
23	¿Los dispositivos de soporte, propuesto en dicho plan de qué manera mejorara la continuidad de la información?							
24	¿El control del ciclo de vida de las aplicaciones, de qué manera mejorara con el plan propuesto?							
25	¿Según el plan propuesto el firewall, de qué manera mejorara, para la continuidad de la información?							
26	¿La auditoría de control de acceso a los sistemas de información, permitirá fortalecer la seguridad de forma?							
27	¿El plan propuesto respecto a la estructura del edificio, de qué manera permitirá mejorar la seguridad de la información?							
28	¿El cableado estructurado, de qué manera mejorar con el plan propuesto?							
29	¿Las estrategias de recuperación de desastres, mediante el plan propuesto, de qué manera permitirá mejorar la continuidad de la información?							
30	¿El plan propuesto respecto al ataque de la red, de qué manera permitirá mejorar la seguridad?							
31	¿El backp de equipamiento, de qué manera mejorara con el plan propuesto?							
32	¿El plan referente a la documentación, de qué manera permitirá mejorar la seguridad?							
33	¿La implementación de auditoría de redes, de qué manera permitirá mejorar la continuidad de la comunicación?							

Anexo 6. Matriz de consistencia. Plan de seguridad informática en la Escuela Universitaria de Postgrado de la Universidad Nacional Federico Villarreal

PROBLEMA	OBJETIVOS	HIPÓTESIS	VARIABLES	TIPO DE ESTUDIO	DISEÑO	METODO	RESULTADOS	CONCLUSIONES
<p>No existe sistema de seguridad informática en la EUPG-UNFV.</p>	<p><u>Objetivo principal</u></p> <p>Probar la eficiencia de un plan de seguridad Informática propuesto en la EUPG-UNFV.</p> <p><u>Objetivos específicos</u></p> <p>Hacer el diagnóstico del sistema de seguridad Informática actual de la EUPG-UNFV</p> <p>Elaborar un plan de seguridad Informática sobre la base del diagnóstico de la situación actual.</p> <p>Probar la eficiencia del plan propuesto.</p>	<p>Se logrará mejorar la seguridad informática en la EUPG-UNFV, mediante la formulación adecuada de un plan de seguridad Informática.</p>	<p><u>Variable independiente</u></p> <p>Plan de seguridad Informática propuesto.</p> <p><u>Variable dependiente</u></p> <p>Seguridad Informática</p>	<p><u>Descriptiva comparativa</u></p> <p>Porque los resultados de una primera fase, serán comparados con los resultados de una segunda fase</p>	<p><u>Transversal</u></p> <p>Recolectaremos los datos en un momento dado por única vez.</p> <p><u>No Experimental</u></p> <p>Porque implica la observación de las situaciones en su condición natural sin intervención de los investigadores.</p>	<p><u>Cuantitativo</u></p> <p>Recogemos datos numéricos que se cuantificaron y se sometieron a un análisis estadístico para determinar los resultados obtenidos.</p> <p><u>Cualitativo</u></p> <p>Se recogió datos descriptivos con los cuales damos explicaciones para las situaciones específicas y así profundizar la investigación sobre factores concretos.</p>	<p>Se realizó el diagnóstico de la seguridad Informática actual en la EUPG-UNFV</p> <p>Se elaboró un plan seguridad Informática para EUPG-UNFV</p> <p>Se probó la eficiencia del plan de seguridad Informática elaborado</p>	<p>Sin la aplicación del plan de seguridad Informática, se demostró que el estado actual de la seguridad Informática en la EUPG-UNFV, es deficiente para las necesidades del complejo de información que maneja.</p> <p>Luego de someter el plan propuesto al juicio de los expertos en informática de la EUPG-UNFV, se aprecia una mejora sustancial en la seguridad Informática</p> <p>La mejora en la percepción de la seguridad Informática, demuestra la eficiencia del plan propuesto en la EUPG-UNFV.</p>