# UNIVERSIDAD AMAZONICA DE PANDO

## DIRECCIÓN DE POSTGRADO E INVESTIGACIÓN

**TESIS PARA OPTAR EL GRADO ACADEMICO DE**
**MAGISTER EN INGENIERIA INFORMÁTICA**

**"Modelo de Seguridad para Identificar Amenazas de los Correos Electrónicos Institucionales"**


**AUTOR: Lic. LOURDES FERNANDEZ**

**TUTOR: M.Sc. Lic. JUAN RAMIRO VILLA**



**POTOSÍ – BOLIVIA**
**2012**

## AGRADECIMIENTOS

**A Dios,** por todas sus bendiciones, su ayuda y protección durante toda mi vida.

**A mi madre,** con todo mi amor y admiración por darme su apoyo, fortaleza en todo momento y su fe en mí.

**A mi esposo,** por su amor, paciencia y apoyo incondicional.

**A mis docentes**, por haber contribuido en mi formación profesional, por ayudarme en la realización y corrección de la tesis al M.Sc. Lic. Juan Ramiro Villa, por ayudarme a perfeccionar este informe final al M.Sc. Lic. Roberto Pérez

**A mis amigos y familia**, es bueno saber que siempre están cerca.

Me hago responsable de todos los errores y agradecería mucho cualquier comentario acerca de este trabajo.

¡Gracias…!

# ÍNDICE

**RESUMEN**……..……

**INTRODUCCIÓN**……..…… 1

**CAPITULO I**

**DISEÑO TEÓRICO METODOLOGICO DE SEGURIDAD DE CORREOS ELECTRONICOS INSTITUCIONALES PARA LA IDENTIFICACION DE AMENAZAS**

1.1. Diseño Teórico…….……. 5

1.1.1. Planteamiento del problema…….……. 5

1.1.2. Problema…… 6

1.1.3. Objeto de estudio……..……. 7

1.1.4. Campo de acción…… 7

1.1.5. Idea a Defender…….……. 7

1.1.6. Tareas de investigación……..… 7

1.1.7. Justificación y aportes de la investigación……. 8

1.2. Diseño Metodológico……..……. 8

1.2.1. Tipo de investigación……. 9

1.2.2. Diseño de investigación……. 9

1.2.3. Métodos de investigación……. 9

**CAPITULO II**

**SUSTENTO TEÓRICO DE GESTION DE RIESGOS EN CORREOS ELECTRONICOS**

2.1. Correo electrónico…….…… 12

2.1.1. Concepto……... 12

2.1.2. Beneficios del correo electrónico……..…… 12

2.1.3. Desventajas del correo electrónico……... 13

2.2. Webmail……..…….. 13

2.3. Agentes de una comunicación de correo electrónico……... 14

2.3.1. Dirección de correo……... 15
2.3.2. Proveedor de correo…….. 15
2.3.3. Dominio de internet……... 16
2.3.4. DNS (Sistema de Nombres de Dominio)…… 17
2.3.5. Servidor de correo…… 17
2.3.5.1. SMTP (Simple Mail Transfer)…… 18
2.3.5.2. POP (Post Office Protocol)…… 19
2.3.5.3. POP 3…….. 20
2.3.5.4. IMAP(Internet Message Access Protocol)……. 20
2.3.5.5. Resumen…….. 21
2.3.5.6. AP (Lightweight Directory Access Protocol)……. 22
2.3.6. Cliente de servidor de correo electrónico…… 22
2.4. Seguridad Informática…… 23
2.4.1. Seguridad de la información……. 24
2.4.2. Estándar Internacional ISO/IEC 27002, Código de Práctica para la administración de la seguridad de la información……. 24
2.4.2.1. Directrices del Estándar ISO/IEC 27002…… 25
2.4.2.2. Certificación…… 26
2.4.3. Manejo de la información……. 27
2.4.4. Gestión de riesgo…… 27
2.4.5. Clasificación de la información…… 29
2.4.6. Tipos de información……. 29
2.5. Métodos y metodologías de gestión de riesgo utilizas…….. 30
2.6. Medidas y mecanismos de seguridad…… 31
2.6.1.1. Contraseñas…….. 31
2.6.1.2. Antiespias……. 32
2.6.1.3. Firewalls…… 33
2.6.1.4. Proxi……. 34
2.6.1.5. Antivirus…… 36
2.6.1.6. Antispam…….. 37
2.7. Amenazas de la información de los correos electrónicos…… 38
2.7.1.1. Espías……. 38

2.7.1.2. Spyware…….. 39
2.7.1.3. Sniffer…… 39
2.7.1.4. Hacker……..… 39
2.7.1.5. Craker ……..… 40
2.7.1.6. Lamer…….. 41
2.7.1.7. Pirata informático…… 41
2.7.2. Amenazas deliberadas a los correos electrónicos…….. 41
2.7.2.1. Interrupción……. 41
2.7.2.2. Interceptación…….. 42
2.7.2.3. Modificación…… 42
2.7.3. Ataques…….. 42
2.7.4. Virus…….……..…… 44
2.7.4.1. Clasificación…….. 44
2.7.5. Spam…….…… 45
2.7.5.1. Formas de enviar un spam…….. 46
2.7.5.2. Funcionamiento del spam…….……..…….. 47
2.7.6. Hoax/Joke…….…… 47
2.7.6.1. Tipos de hoax…….……. 48
2.8. Políticas de seguridad de la información…….. 48

## CAPITULO III

## MODELO DE SEGURIDAD PARA LA IDENTIFICACIÓN DE AMENAZAS DE LOS CORREOS ELECTRÓNICOS INSTITUCIONALES

3.1. Objetivos…….……... 50
3.1.1. Objetivo General…….. 50
3.1.2. Objetivos Específicos…….. 50

3.2. Modelo de seguridad de Correos electrónicos para identificación de Amenazas……..…… 51
3.2.1. Plan 1. Gestión de riesgos……..……..……. 53
3.2.1.1. Fase 1. Levantamiento de información……. 54

3.2.1.2. Fase 2. Identificación…….……..…… 55
3.2.1.3. Fase 3. Análisis de riesgos……... 58
3.2.1.4. Fase 4. Valoración de riesgos…….. 60
3.2.1.5. Fase5. Manejo de Riesgos……..……. 61
3.2.1.6. Fase 6. Informe, Plan de respuesta de riesgo……... 62
3.2.2. Plan 2. Reinstalación de la plataforma web…..……... 63
3.2.2.1. Descripción del SquirreIMail……... 63
3.2.2.2. Características o funcionalidades del SquirrelMail…….…… 64
3.2.2.3. Ventajas del SquirrelMail…… 65
3.2.2.4. Requerimientos del SquirrelMail para su instalación……... 66
3.2.3. Políticas de seguridad…….…. 68

**CAPITULO IV**

**RESULTADOS DE LA APLICACIÓN DEL MODELO PROPUESTO**

4.1. Aplicación del plan 1……. 72
4.1.1. Fase 1. Levantamiento de información……..…. 72
4.1.2. Fase 2. Identificación s de riesgos……..…… 77
4.1.3. Fase 3. Análisis de riesgos…….…. 83
4.1.4. Fase 4. Valoración de riesgos……. 84
4.1.5. Fase 5. Manejo de Riesgos…….. 85
4.1.6. Fase 6. Informe, plan de respuesta de riesgo……... 86
4.2. Viabilidad del modelo propuesto evaluado mediante criterio de expertos…… 98
4.2.1. Procesamiento de las encuestas a través del método Delphi……..…… 98
4.2.2.Análisis de los resultados obtenidos en la aplicación del método Delphi…… 98

Conclusiones……..…… 99
Recomendaciones……..……..…. 100

Bibliografía……..….. 101

**ANEXOS**

Anexo 1……. 104
Anexo 2…….. 106
Anexo 3…….…… 107
Anexo 4…….…… 109
Anexo 5……..…... 110
Anexo 6…….. 119
Anexo 7…….……. 121
Anexo 8.……..…… 124
Anexo 9……..…… 127

# ÍNDICE DE TABLAS

Tabla. 2.1. Comparación Pop3 vs. IMAP…….…… 22
Tabla 3.1. Riesgos de seguridad de correo electrónico……..…..... 57
Tabla 3.2 Clasificación de riesgos Existentes……..…. 57
Tabla 3.3 Resumen de Amenazas detectadas…….…….. 57
Tabla 3.4. Matriz de control de riesgo……..…… 58
Tabla 3.5. Valoración de los resultados (amenazas)…….……..…….. 59
Tabla 3.6. Valoracion de los resultados (objetos)…….……. 60
Tabla 3.7. Matriz de resultados con identificación de niveles de riesgo…… 61
Tabla 3.8. Establecer controles…….. 62

# ÍNDICE DE FIGURAS

Fig. 2.1. Agentes de comunicación de un correo electrónico…… 14
Fig. 2.2. Circulo de Deming……..…… 26
Fig. 3.1. Flujograma del modelo de seguridad propuesto…….. 52
Fig. 3.2. Etapas de la gestión de riesgo…….. 54

# RESUMEN

El presente trabajo muestra, la necesidad de proteger la información contenida en los correos electrónicos y se propone hacer que esta información sea confiable e integra, protegiéndola contra amenazas, como la pérdida, divulgación y manipulación. Para ello, el problema que se investigo fue ¿Como mejorar la gestión de riesgos de correos electrónicos institucionales para la identificación de amenazas?, el objetivo principal fue: diseñar un modelo de seguridad que coadyuve en la gestión de riesgos de la seguridad de correos electrónicos institucionales para la identificación de amenazas; la metodología utilizada fue la descriptiva, también se utilizo métodos tanto teóricos como empíricos con sus respectivos instrumentos, la principal conclusión fue que se cumplió con el objetivo principal.



Palabras Claves: Modelo, Seguridad, Correo electrónico

# INTRODUCCIÓN

El correo electrónico o e-mail es, sin duda, uno de los grandes hallazgos de Internet, tanto que se puede decir que ha revolucionado la forma de comunicarse con compañeros, amigos e, incluso, con la propia familia. Por lo que se ha convertido en uno de los servicios más utilizados de Internet.

Algunos lo señalan como la versión más "humilde" de la Red básicamente, su funcionamiento es muy similar al del correo postal: cada usuario de Internet tiene una dirección asociada que le es propia y que ningún otro usuario de la Red posee, lo cual permite comunicar a dos o más usuarios de una manera inequívoca.

Haciendo una analogía con el correo postal se puede decir que cuando es enviado un mensaje por correo electrónico, éste va pasando de red en red (las oficinas postales) por medio de "gateways" o compuertas (los camiones de correo) hasta que llega a su destino. Allí se dispone de una "casilla de correo electrónico" con el nombre correspondiente, y es recogido mediante un programa "cliente" de correo electrónico, y que hace las veces del tradicional cartero que entrega la correspondencia en el domicilio.

Las ventajas del correo electrónico son innumerables: es inmediato, se recibe a los pocos minutos de haber sido enviado; es cómodo, permite enviarlo desde casa (frente al correo tradicional); el costo no varía en función de la ubicación física del destinatario, resultando realmente económico; y es dinámico, ya que permite la posibilidad de recibir su correo aunque no esté en el lugar donde se usa habitualmente.

Lo que uno no se percata es del nivel significativo de ataques existentes derivados del uso del correo electrónico, como el acceso a información no personal, modificación o eliminación de esta información, es decir el mal uso del e-mail estriba en comprometer y/o divulgar el contenido del mensaje, o proporcionar información spammer acerca de uno.

En Bolivia los primeros correos electrónicos enviados y recibidos fueron en septiembre del año de 1990, con la conformación de un comité que llevo adelante el Proyecto para Desarrollar Servicios de Correo Electrónico, mismo que estaba conformado por ENTEL y la carrera de Ingeniería Electrónica de la UMSA, de esta forma comenzó la era del correo electrónico y sus múltiples derivaciones: acceso a bases de datos, listas electrónicas, etc., desde entonces este servicio se ha hecho indispensable tanto para las personas como para las instituciones por los diversos beneficios que esta proporciona.

A raíz de esto nace la necesidad del proteger al usuario de este servicio, es en este sentido que el 8 de agosto del 2011 se aprobó la Ley General de Telecomunicaciones, Tecnologías de Información y Comunicación, que en sus artículos 89, 90 y 91 tratan de regular y proteger la información contenida en los correos electrónicos.

Actualmente existen muchas formas de reprimir los diversos ataques que sufren los servidores de correos electrónicos institucionales, estos están dirigidos especialmente al nivel físico es decir existen firewalls, gateways que pueden detener muchos de los ataques exteriores, pero se debe tomar en cuenta que estos elementos físicos son costosos y muchas de las instituciones existentes en nuestro medio son pequeños para realizar semejantes inversiones, es por esto que muchas instituciones han optado por implementar diferentes políticas de seguridad, mismas que no son suficientes para afrontar estos ataques; es por esto que ve la necesidad de realizar un proceso de gestión de riesgos de los correos electrónicos, misma que ayude a identificar de forma puntual las diversas amenazas que se sufren, de esta manera poder solucionar las fallas existentes.

En consecuencia de lo mencionado se propone una gestión de riesgos existentes en los correos electrónicos, en un modelo de seguridad para identificar de forma puntual las amenazas existentes en los correos electrónicos, para atender de forma rápida y oportuna diferentes incidentes de seguridad con respecto a los mismos, de esta forma gestionar los riesgos, proveyendo de información sobre la utilización segura de la herramienta mediante políticas o normas que necesariamente deben existir o ser implementadas en una institución, el modelo de seguridad para correos electrónicos propuesto, puede ser usado en diferentes instituciones donde exista un servidor web ya que se adecua a las posibilidades de la mayoría de las

entidades de nuestro medio, puesto que son pocas las instituciones que toman medidas ante las amenazas existentes en la transmisión de datos mediante el correo electrónico.

Este modelo esta formado por diferentes planes que pueden ser usados según el tipo de servicio de correo electrónico con el que cuente la institución, en el que se implemente el modelo de seguridad de correos electrónicos, para esto se plantearon los siguientes aspectos que fueron el pilar de la presente investigación,

Problema: ¿Como coadyuvar en la gestión de riesgos de los correos electrónicos institucionales para la identificación de amenazas?.

Objetivo General: Diseñar un modelo de seguridad que coadyuve en la gestión de riesgos de la Seguridad de correos electrónicos institucionales para la identificación de amenazas.

Idea a defender: La aplicación de un modelo de seguridad para la identificación de amenazas permitirá una adecuada gestión de riesgos de los correos electrónicos institucionales

Alcance: La presente investigación pretende prevenir y contrarrestar las actividades ilegales como el acceso no autorizado o el bloqueo de los correos electrónicos desarrollando un modelo de seguridad, para dar solución a los problemas de seguridad que se presentan en los correos electrónicos, mismo que puede ser utilizado en diferentes instituciones ya sean publicas o privadas de nuestro medio.

La metodología que se puso en práctica fue la cualitativa, realizando un tipo de investigación descriptiva puesto que la presente investigación no utiliza el método experimental.

Los métodos teóricos utilizados son: Análisis-Síntesis, Inductivo-Deductivo, Histórico-Lógico, Abstracto-Concreto, Sistémico-Modélico; todos de gran utilidad en el momento de discernir la bibliografía consultada a diferentes autores.

Los Métodos Empíricos que se emplearon para la elaboración del modelo fueron: el método de la encuesta, con la técnica del cuestionario, la entrevista estructurada, la observación directa y la recopilación documental, así mismo se utilizó el método probabilístico y estadístico.

Teniendo como antecedente lo mencionado anteriormente se ha visto por conveniente realizar el siguiente orden de trabajo: el Primer Capítulo detalla el problema planteado, el objeto y campo de acción, la idea a defender, la metodología con la cual se llevo adelante toda la investigación, etc., además de reunir todas las características del sistema actual para luego realizar el modelo propuesto, el Segundo Capítulo recopila toda la información bibliográfica acerca de conceptos importantes de correos electrónicos, amenazas que existen en la información y seguridad de información, etc., los mismos que respaldarán el presente trabajo, el Tercer Capítulo está destinado a detallar el modelo propuesto mismo que podrá ser utilizado en cualquier institución, por ultimo el Capítulo Cuarto esta destinado a poner en práctica el modelo propuesto de seguridad de correos electrónicos que en el presente caso se lo aplico en Fundación ACLO.

# CAPITULO I
# DISEÑO TEÓRICO METODOLÓGICO DE SEGURIDAD PARA CORREOS ELECTRONICOS INSTITUCIONALES PARA LA IDENTIFICACION DE AMENAZAS

El presente capítulo cuenta con información como el problema, campo de acción, la metodología aplicada, así como el tipo y diseño de la investigación utilizada, esto de acuerdo a las particularidades del problema y a las técnicas aplicadas durante todo el proceso de investigación, en esta fase se llevó a cabo el levantamiento de información haciendo uso de las herramientas y técnicas que se utilizaron para la investigación, entre estos se tiene: entrevista estructurada, cuestionario, observación directa y revisión documental mismos que facilitaron la solución del problema.

## 1.1. Diseño Teórico.

### 1.1.1. Planteamiento del Problema.

El correo electrónico es una de las aplicaciones de internet más utilizadas para el intercambio de información, que ha ido evolucionando con el pasar de los años; en la actualidad es considerado como un recurso básico con un funcionamiento fácil y sencillo, es un servicio de mensajería electrónica que tiene por objeto la comunicación no interactiva de texto, datos, imágenes o mensajes de voz entre un "originador" y los destinatarios designados que se desarrollan en sistemas que utilizan equipos informáticos y enlaces de telecomunicaciones. El correo electrónico sobrepasa fronteras y soberanías de cada región, con una rapidez y facilidad asombrosa.

Precisamente por ser tan popular, actualmente el correo electrónico es uno de los servicios más afectados por los problemas de seguridad que proliferan en la red, ya que los criminales han encontrado en la tecnología nuevas formas de cometer delitos y aumentar los riesgos de los sistemas, puesto que el punto de entrada habitual a la red de una organización, es por correo

electrónico, tanto a través de servidores de correo inseguro o a través de los propios mensajes de correo electrónico.

Con el progreso constante del correo electrónico nace el derecho a la privacidad y la protección de los mensajes electrónicos de los usuarios, ya que estos constantemente se ven vulnerados por personas inescrupulosas con los conocimientos necesarios en informática.

El amplio desarrollo de las nuevas tecnologías está ofreciendo un nuevo campo de acción a conductas antisociales y delictivas manifestadas en formas difíciles de imaginar, ofreciendo la posibilidad de cometer delitos tradicionales en formas no tradicionales.

Hoy en día, la seguridad es un tema que preocupa y que está de actualidad en todas las instituciones y empresas en el mundo. Los sistemas de información sufren frecuentemente ataques de diversa naturaleza que traen gravísimas pérdidas económicas, de tiempo e información para las empresas que los utilizan.

Por lo mencionado, se definió como situación problemática:

Las instituciones que de alguna forma son victimas de diferentes ataques propiciados por programas o personas intrusas, tienen la necesidad de dar seguridad a los correos electrónicos institucionales identificando las amenazas existentes, de esta forma atender de forma rápida y oportuna cualquier incidente de seguridad con respecto a los mismos, como el acceso, modificación, destrucción y uso no autorizado de datos, para evitar perdidas económicas, información valiosa para la institución, o de tiempo tratando de resolver el problema.

### 1.1.2. Problema.

Por todos los motivos señalados anteriormente se ve la necesidad de dar atención al hecho de la seguridad en el envío y recibo de correos electrónicos institucionales, por esto se plantea el siguiente problema de investigación:

¿Como coadyuvar en la gestión de riesgos de los correos electrónicos institucionales para la identificación de amenazas?.

### 1.1.3. Objeto de Estudio.

La solución del problema gira en torno al siguiente objeto de estudio: Seguridad informática

### 1.1.4. Campo de Acción.

El campo de acción sobre el cual se desarrolló la investigación fue: Seguridad de correos electrónicos institucionales para la identificación de amenazas.

### 1.1.5. Idea a Defender.

Para dar solución al problema planteado se formulo la siguiente idea a defender:

La aplicación de un modelo de seguridad para la identificación de amenazas permitirá una adecuada gestión de riesgos de los correos electrónicos institucionales.

La operacionaliación de las variables identificadas para el desarrollo de la investigación se muestra en el Anexo 1.

### 1.1.6. Tareas de Investigación.

Las tareas de investigación que surgen en consecuencia son:

- Sistematizar los principales fundamentos teóricos relacionados con la seguridad informática para la gestión de riesgos de los correos electrónicos institucionales.
- Analizar métodos actuales de seguridad de correos electrónicos institucionales para la identificación de amenazas.

- Desarrollar componentes estructurales de un modelo de seguridad para la identificación de amenazas que permita una adecuada gestión de riesgos de los correos electrónicos institucionales
- Determinar el grado de viabilidad de la propuesta de un modelo de seguridad para identificar amenazas de los correos electrónicos institucionales

### 1.1.7. Justificación y Aportes de la Investigación

Esta investigación pretende prevenir y contrarrestar las actividades ilegales como el acceso no autorizado o el bloqueo de los correos electrónicos desarrollando un modelo de seguridad, para dar solución a los problemas de seguridad que se presentan en los correos electrónicos, en este sentido los aportes alcanzados con el desarrollo de la presente investigación están dados por:

El aporte social, los beneficiarios de esta investigación son todas las instituciones que cuentan con un servidor web ya que con este servicio sus dependientes pueden ingresar a una o más cuentas de correos electrónicos preservando la intimidad del usuario de este servicio, el uso del modelo de seguridad propuesto ayudará a prevenir el acceso, modificación, destrucción y uso no autorizado de datos que contengan los correos electrónicos institucionales.

El aporte teórico, se encuentra en el estudio de los conceptos y normas de seguridad informática que se aplicó a la seguridad de los correos electrónicos ya que se adquirió un mayor conocimiento acerca de las amenazas con las que cuentan los correos electrónicos, y como este conocimiento coadyuvó en el desarrollo del modelo para acrecentar la seguridad en el uso de los correos electrónicos, proveyendo información de su funcionamiento, así como la utilización segura de los mismos, los ataques basados en e-mails y la protección de la privacidad en línea.

La significación práctica, con la utilización del modelo de seguridad propuesto se pretende dar seguridad a los correos electrónicos, este hecho es importante para la sociedad puesto que los correos electrónicos manejan información tanto personal como laboral, en este sentido la pérdida o alteración de los mismos perjudica el diario vivir de las instituciones ya que el valor de la información manejada en los mismos es invaluable. Esta investigación esta enmarcada o

dirigida a cualquier institución que cuente con servidores web que sean administrados por la misma institución, ya que se debe contar con acceso constante al servidor para realizar los cambios que sean necesarios para dar seguridad a los correos electrónicos.

Utilidad Metodológica, Se propone una modelo de seguridad que en sus diferentes planes permite generar información a ser analizada y registrada en diferentes formularios, con la finalidad de encaminarse hacia la solución del problema de seguridad de los correos electrónicos.

## 1.2. Diseño Metodológico.

### 1.2.1. Tipo de investigación.

La metodología utilizada en el desarrollo de la presente investigación fue la cualitativa, dentro de la cual se realizo un tipo de investigación descriptiva, ya que durante la revisión bibliográfica se detectaron las variables sobre las cuales se fundamentó el trabajo, la investigación descriptiva va más allá de la toma y tabulación de datos; supone un elemento interpretativo del significado o importancia de lo que describe, combinando así el contraste, la interpretación y la evaluación de la misma, esto permitió describir las variables en un momento determinado, para su posterior análisis e interpretación de características homogéneas.

### 1.2.2. Diseño de la investigación.

El diseño de la investigación es no experimental ya que no se hizo una manipulación de las variables, y se presenta tal cual se dio en la realidad, la información recogida fue clara con respecto al problema planteado.

### 1.2.3. Métodos de investigación.

Para el diseño del modelo de seguridad propuesto se utilizaron diferentes métodos teóricos y empíricos, estos fueron seleccionados en función a la idea a defender, tareas científicas y el objetivo planteado.

Los métodos teóricos utilizados permitieron realizar el respectivo análisis y comparación de teorías así mismo permitió interpretar de forma teórica los datos empíricos que se fueron encontrando a lo largo de la investigación, estos métodos fueron:

- Análisis-Síntesis, se utilizó este método en toda la revisión bibliográfica que se realizó para diseñar un marco teórico que coadyuvó en la solución del problema, así mismo permitió contrastar varias posiciones teóricas para de esta forma contar con un punto de vista con respecto a cada concepto estudiado.

- Inductivo-Deductivo; se utilizó en la elección del tema de investigación, objetivo general y de los objetivos específicos así como en el desarrollo del marco teórico y el modelo propuesto.

- Abstracto-Concreto; que permitió el análisis del objeto de la investigación para descomponerlo en conceptos abstractos y llegar a un nuevo conocimiento concreto con la propuesta.

- Histórico Lógico; que permitió comprender el objeto de la investigación, sus antecedentes y desarrollo, como también permitió realizar una valoración crítica de la situación actual.

- Modelación; que permitió el estudio del objeto de investigación para lograr la solución integral del problema con el desarrollo y la aplicación del modelo de seguridad propuesto.

Los Métodos Empíricos empleados en la elaboración del modelo propuesto permitieron la recopilación de la información verídica misma que posteriormente fue analizada, esta información permitió comprobar de manera práctica la idea a defender, además de verificar el problema y contribuir en la validación del modelo propuesto, entre estos métodos se encuentran:

- La encuesta, con la técnica del cuestionario, se realizó tomando en cuenta los indicadores determinados en la operacionalización de variables, que se aplicó a las personas que

trabajan en la institución y que cuentan con uno o más correos electrónicos para tomar en cuenta su opinión con respecto al desarrollo del modelo propuesto, además de aplicar otro cuestionario al administrador de redes de la institución, y con esta información analizar la situación actual de la institución. (Ver Anexo 3)

- La entrevista estructurada; que se aplicó al administrador de la red permitió conocer la situación real de la institución con respecto al objeto de estudio. (Ver Anexo 4)

- La observación directa; que se aplicó a toda la población seleccionada, con el fin de conocer el comportamiento del objeto de estudio, sirviendo la información recolectada como base para conocer la situación de la institución al momento de iniciar el estudio y posterior aplicación del modelo de seguridad en la institución.

- La recopilación documental; con el fin de conocer los reglamentos con respecto a seguridad en la institución, así como la recopilación de información y documentación para el desarrollo de nuevas políticas de seguridad con respecto a correos electrónicos de la institución.

- Consulta a Expertos especialistas; con el fin de viabilizar la presente investigación con el fin de conocer la evaluación del modelo propuesto, mediante la evaluación del contenido del trabajo de investigación así como las recomendaciones que puedan surgir para el perfeccionamiento y la puesta en practica.

Los Métodos Matemáticos; permitieron la obtención del muestreo poblacional de la institución en la cual se puso en marcha el modelo de seguridad propuesto con el fin de procesar cuantitativamente los datos obtenidos, de la aplicación de la encuesta en función de enriquecer los criterios para las valoraciones cualitativas de los mismos tanto para la fase del diagnostico como para la fase validadora de la propuesta.

- Probabilístico y estadístico, permitió calcular la muestra de la población que cuenta con correos electrónicos en la institución, además de calcular los porcentajes y realizar las interpretación de los datos recolectados en los cuestionarios. (Ver anexos 5,6)

# CAPITULO II
# SUSTENTO TEÓRICO DE GESTION DE RIESGOS EN CORREOS ELECTRONICOS

En el presente capitulo se analizó, estudió, investigó e identifico vulnerabilidades y amenazas que pueden afectar a la información que circula por el sistema de correo electrónico, también se tomo en cuenta conceptos de correo electrónico, así como conceptos acerca de la seguridad de la información y específicamente conceptos relacionados con la seguridad en el servicio de correo electrónico, así mismo se realizo el estudio

## 2.1. Correo Electrónico.

### 2.1.1. Concepto.

Es un mensaje electrónico constituido por información binaria transmitida de un computador a otro, el mismo que puede transmitir mensajes personales o laborales, ya que puede llevar con el: archivos adjuntos como imágenes, documentos con formato, e incluso música y programas de computador; por tal razón cada vez más personas en el mundo lo utilizan.

El Correo Electrónico fue creado en 1971 por Ray Tomlinson, basado en la necesidad de un sistema de mensajería para que las computadoras conectadas en red puedan enviar y recibir mensajes a otras computadoras. Su funcionamiento es análogo al correo postal: ya que ambos sirven para enviar y recibir mensajes, además, los dos utilizan "buzones" intermedios (casilleros/servidores), en donde los mensajes se guardan temporalmente mientras se dirigen a su destino.

### 2.1.2. Beneficios del correo electrónico.

- Es una manera de mantenerse en contacto con familiares, amigos, colegas que trabajan o viven lejos.

- Ayuda ahorrar tiempo y dinero pues es rápido, fácil y mucho más barato que el correo postal.
- Es un servicio muy visitado y usado por las personas que manejan equipo informático.
- El correo electrónico es una manera de mantenerse en contacto sin acumular una enorme factura de teléfono.

### 2.1.3. Desventajas del correo electrónico.

Al ser un medio de comunicación masivo con grandes beneficios, no es de extrañarse que el correo electrónico también se haya convertido en el servicio más visitado por intrusos o curiosos. Un correo electrónico normal es como una tarjeta postal sin sobre, que puede leer todo aquel que tenga interés o por accidente llega a tener acceso al mismo. Por consiguiente, es necesario preservar la intimidad y la integridad en los mensajes de correo electrónico antes, durante y después de ser enviado. Entre los principales problemas y deficiencias que afectan a la seguridad y veracidad de éste medio de comunicación se tiene:

- Espías, sniffing.
- El spam y las cadenas de correo electrónico.
- Los virus.
- El phishing,

## 2.2. Webmail.

Es una manera alternativa de acceder al correo electrónico utilizando la web, mientras que el método tradicional consiste en conectarse con un programa local, o a un servidor remoto utilizando un protocolo ad-hoc (comunicaciones de tipo punto-a-punto) de transporte de correo, descargar los correos y almacenarlos localmente, el webmail permite listar, desplegar y borrar vía un navegador web los correos almacenados en el servidor remoto.

Casi todos los proveedores de correo dan el servicio de Correo Web (webmail) que permite enviar y recibir correos mediante una página web diseñada para ello, usando, por tanto, sólo un programa navegador web.

Como los correos no son descargados pueden ser consultados posteriormente desde otro computador conectado a la Internet que disponga de un browser. Existen empresas privadas que dan servicio de webmail sin costo, como: Yahoo, Hotmail, Gmail.

Sin embargo cualquier institución, empresa o grupo que posea conexión de red privada o dedicada a la Internet, puede construir un servicio de webmail para el uso de sus integrantes y de esta manera tener presencia en internet.

Como desventaja, es difícil de ampliar con otras funcionalidades, porque la página ofrece unos servicios concretos y no podemos cambiarlos. Además, suele ser más lento que un programa de correo, ya que hay que estar continuamente conectado a páginas web y leer los correos de uno en uno.

### 2.3. Agentes en una comunicación de correo electrónico

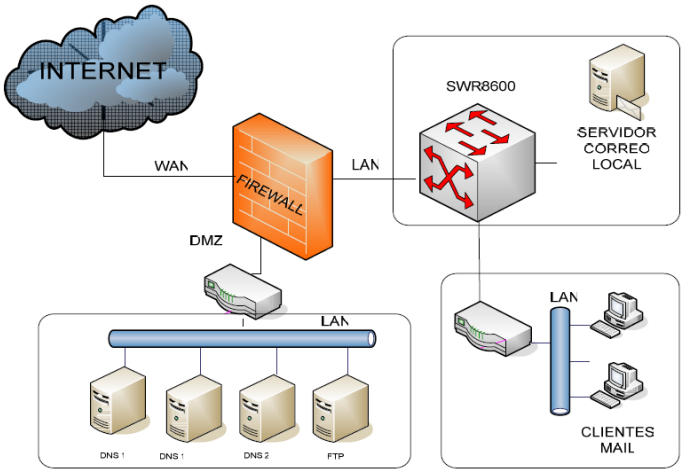



**Fig. 2.1. Agentes de comunicación de un correo electrónico**

**Fuente: Imágenes de google.**

Para que una persona pueda tener comunicación mediante correo electrónico y enviar un mensaje a otra, las dos personas deben tener una dirección de correo electrónico, estar conectados a un proveedor o servidor de correo que son quienes ofrecen el servicio de envío y recepción.

### 2.3.1 Dirección de correo.

Una dirección de correo electrónico es un conjunto de letras, números y signos que identifican a una persona para que pueda enviar y recibir correos electrónicos. Cada dirección es única y normalmente se eligen direcciones sencillas de memorizar para facilidad del propietario y de las personas que deseen escribirle; por cuanto, esta debe ser escrita de forma exacta, letra por letra, un solo error hará que no lleguen los mensajes de correo electrónico al destino.

Una dirección de correo electrónico (bmoreno@aclo.pts.bo), se divide en dos partes: a la izquierda del arroba (@) el nombre de usuario o alias (en este caso: bmoreno) que es un parámetro elegido por el usuario o el administrador del servicio de correo electrónico, a continuación el carácter arroba (@) que se lee o es análogo a decir "en", y finalmente a la derecha están los dominios al que pertenece está dirección de correo, los cuales no son modificables por el usuario (en este caso: aclo.pts.bo).

En resumen bmoreno@aclo.pts.bo identifica al buzón de correo electrónico del usuario cuyo alias es bmoreno que está en el servidor de dominio aclo.pts.bo, es decir que pertenece al servidor de correo electrónico de Fundación Aclo.

Una dirección de correo electrónico se diferencia de una página web porque siempre tiene la letra @, mientras que una dirección de sitio web se la distingue por las letras www, y está acompañada del tipo de información que contiene.

### 2.3.2. Proveedor de correo.

Son empresas que ofrecen servicio de correo electrónico, con lo cual permiten al usuario enviar y recibir correos electrónicos, generalmente hay que estar registrado en alguna de estas empresas. El registro en cualquiera de estas permite tener una dirección de correo personal única y duradera, a la que se puede acceder mediante un alias y una contraseña personal. Hay varios tipos de proveedores de correo, que se diferencian sobre todo por la calidad del servicio que ofrecen. Básicamente, se pueden dividir en dos tipos:

- **Correos gratuitos**: Son los más conocidos entre los usuarios, estos incluyen información publicitaria que algunos la llevan incrustada en cada mensaje y otros en la interfaz que se usa para leer el correo. Muchos sólo permiten ver el correo desde una página web propia del proveedor, para asegurarse de que los usuarios reciban la publicidad que se encuentra ahí. En cambio, otros permiten también usar un programa de correo configurado para que se descargue el correo de forma automática, los principales proveedores de servicios de correo electrónico gratuito son: Gmail: webmail, Hotmail: webmail, Yahoo!: webmail, etc.

- **De pago:** El dominio de tipo de proveedores (gratuito mail) @ xxxxxx.com, no es práctico para el uso de instituciones, para dar un aspecto más profesional a la organización, es necesaria la adquisición de un dominio propio institucional. Los correos de pago normalmente ofrecen todos los servicios disponibles, cuando se contrata la conexión con un proveedor de Internet, este puede proporcionar un correo como: xxxxxxx@aclo.pts.bo. También se puede considerar de pago el método de comprar un nombre de dominio e instalar un servidor de correo con los programas apropiados un MTA (Agente de Transporte de Correos), no se cancela cuotas por el correo, pero sí por el dominio. Los servicios de correo de pago los suelen dar las compañías de acceso a Internet o los registradores de dominios.

### 2.3.3. Dominio de Internet.

Es un sistema que permite reconocer e individualizar cada máquina que esté en conexión de red, es la parte de una URL (localizador uniforme de recurso) con la misma que se identifica al servidor en el que se aloja un sitio de Internet. Existen gran cantidad de dominios en la red y estos se clasifican por temas, según su terminación (o dominio raíz), de tal forma que los terminados en:

- .com Destinado a uso comercial,
- .org Organizaciones sin fin de lucro,
- .gov Páginas gubernamentales,
- .edu Instituciones educativas,
- .net Destinado a infraestructura de red, etc.

Cada país con conectividad a la red de redes tiene asignado un nombre de dominio de nivel superior CC TLD, (Country Code Top-Level Domain) los que cumplen la norma de dos letras con alguna rara excepción basados en sus códigos ISO de dos letras (ISO 3166), como .jp para Japón.

Las reglas en cuanto a quién tiene derecho a poseer dominios son desarrolladas por los administradores de DNS (Domain Name Service), quienes también son responsables de la operación del dominio. En algunos países cualquier persona puede adquirir un dominio en el NIC (Network Information Center); en otros casos, únicamente permiten a residentes del país o área dependiente tener un dominio en él.

El administrador de DNS es designado por ICANN (Internet Corporation for Assigned Names and Numbers) con el permiso del gobierno del país o área dependiente, como:

- .bo Para Bolivia,
- .ar Para Argentina,
- .int Internacional, para organizaciones como la ONU

Los dominios de nivel superior, que no son de países, se los registran a través de empresas conocidas como registradoras de dominios.

### 2.3.4. DNS, (Sistema de Nombres de Dominio)

El DNS (Sistema de Nombres de Dominio) es una gran base de datos descentralizada que asigna nombres de máquina (como www.aclo.org.bo) a direcciones IP (como 192.168.77.2). El DNS le dice al servidor de correo donde enviar el correo para un dominio dado.

### 2.3.5. Servidor de correo.

Es un ordenador de muy buenas características que tiene instalada una aplicación que permite enviar mensajes (correos) de unos usuarios a otros, con independencia de la red que dichos usuarios estén utilizando. Para lo cual se usan tecnologías con una serie de protocolos, cada uno con una finalidad concreta:

- SMTP
- POP3
- IMAP

#### 2.3.5.1. SMPT (Simple Mail Protocol Transfer)

El Protocolo Simple de Transferencia de Correo electrónico se utiliza para el envío de correo entre dos servidores de correo electrónico que intercambien mensajes. También es el más representativo de la filosofía cliente servidor dentro de la extensa familia de los protocolos TCP/IP. Ya que es un protocolo de red basado en texto muy utilizado para el intercambio de mensajes de correo electrónico entre computadoras o distintos dispositivos como PDA's, Celulares, etc.

**a) Funcionamiento SMTP,** El emisor y receptor intercambian mensajes y respuestas en un diálogo del tipo parada y espera. En respuesta a la solicitud de un cliente de correo electrónico a su mail-server, del envío de un mensaje, es entonces cuando el mail-server se transforma en un emisor SMTP el cual establece una conexión duplex integral con el receptor SMTP, el cual puede ser la dirección de destino o un host en el camino intermedio hacia éste.

El SMTP hace uso de los dominios para transferir los mensajes, pero para conocer la dirección de red de un dominio dado, usa los servicios de un DNS que como se indico anteriormente convierte un nombre de dominio dado, en una dirección de red IP. En cuanto a la aplicación TCP/IP, se utiliza el protocolo SMTP (Simple Mail Transfer Protocol) el cual se caracteriza por su eficiencia, sencillez y facilidad de depuración, gracias a los mensajes que acompañan a sus comandos. SMTP, sustenta el servicio de envió de correo electrónico utilizando por defecto el puerto TCP 25.

• **Establecimiento de la conexión,** Una vez abierto el canal de transmisión, los hosts conectados hacen un intercambio de información para asegurarse, que están hablando con quien ellos quieren, para esto el emisor envía un comando HELO seguido de su dominio.

• **Transferencia de Mail,** la transferencia de mail tiene tres pasos necesarios cada uno con un comando específico, y con respuestas afirmativas o negativas para cada uno de ellos. El primer paso es el envío del comando MAIL especificando el origen del mensaje con el "camino inverso", que se usará para reportar errores si los hubiera, el host receptor puede tanto aceptar el mensaje entrante, con una respuesta positiva, o rechazarlo con una respuesta negativa.

Este comando indica al receptor el inicio de la transacción de mail por lo que éste debe poner en cero sus tablas de estado, buffers, etc., este comando resetea al receptor. El camino inverso, es la ruta, lista de hosts, que ha seguido el mensaje hasta el host emisor, y tiene a éste al principio de la lista.

• **Liberación de la conexión,** Para finalizar la conexión simplemente el emisor envía el comando QUIT y se libera la conexión

**2.3.5.2 POP (Post Office Protocol).**

El Protocolo de Oficina de Correos es un protocolo que se utiliza para obtener los mensajes guardados en el servidor y pasárselos al computador del usuario; al contrario de otros protocolos creados con anterioridad como el SMTP el POP, no necesita una conexión permanente a Internet, puesto que en el momento de la conexión es cuando solicita al servidor el envío de la correspondencia almacenada en el servidor para dicho usuario.

Si se está permanentemente conectado a Internet, es recomendable configurar los programas cliente de correo de tal forma que la petición al servidor de correo se efectúe automáticamente cada cierto tiempo y de esta forma avise al usuario de que tiene correo pendiente de recibir.

La ventaja con otros protocolos es que entre servidor-cliente no se tienen que enviar tantas órdenes para la comunicación entre ellos. El protocolo POP también funciona adecuadamente si no se utiliza una conexión constante a Internet o a la red que contiene el servidor de correo.

#### 2.3.5.3 POP3.

Permite que los usuarios con conexiones intermitentes (tales como las conexiones dial up), descarguen su e-mail cuando se encuentren conectados de tal manera que puedan ver y manipular sus mensajes sin necesidad de permanecer conectados. Cabe mencionar que la mayoría de los clientes de correo incluyen la opción de dejar los mensajes en el servidor, de manera que, un cliente que utilice POP3 se conecta, obtiene todos los mensajes, los almacena en la computadora del usuario como mensajes nuevos, los elimina del servidor y finalmente se desconecta.

Los clientes que utilizan la opción dejar mensajes en el servidor por lo general utilizan la orden UIDL (Unique IDentification Listing). La mayoría de las órdenes de POP3 identifican los mensajes dependiendo su número ordinal del servidor de correo. Esto genera problemas al momento que un cliente pretende dejar los mensajes en el servidor, ya que los mensajes con número cambian de una conexión al servidor a otra. Cuando un cliente de correo compatible con POP3 se conecta al servidor utiliza la orden UIDL para obtener el mapeo del identificador de mensaje. De esta manera el cliente puede utilizar ese mapeo para determinar qué mensajes hay que descargar y cuales hay que guardar al momento de la descarga.

Al igual que otros viejos protocolos de internet, POP3 utilizaba un mecanismo de firmado sin cifrado. La transmisión de contraseñas de POP3 en texto plano aún se da en la actualidad POP3 y cuenta con diversos métodos de autenticación que ofrecen una diversa gama de niveles de protección contra los accesos ilegales al buzón de correo de los usuarios.

#### 2.3.5.4 IMAP (Internet Message Access Protocol)

El IMAP es el Protocolo de Red de Acceso a Mensajes Electrónicos almacenados en un servidor, su finalidad es la misma que la de POP, pero el funcionamiento y las funcionalidades que ofrecen son diferentes. Mediante el IMAP se puede tener acceso al correo electrónico desde cualquier equipo que tenga una conexión a Internet. Una vez configurada la cuenta IMAP, puede especificar las carpetas que desea mostrar y las que desean ocultar, esta característica lo hace diferente del protocolo POP.

IMAP fue diseñado como una moderna alternativa a POP pues fundamentalmente, los dos protocolos permiten a los clientes de correo acceder a los mensajes almacenados en un servidor de correo, y es utilizado frecuentemente en redes grandes, por ejemplo los sistemas de correo de un campus. IMAP permite a los usuarios acceder a los nuevos mensajes instantáneamente en sus computadoras, ya que el correo está almacenado en la red. Con el protocolo POP3 los usuarios tendrían que descargar el e-mail a sus computadoras o accesarlo vía Web.

Ambos métodos toman más tiempo de lo que le tomaría a IMAP, y se tiene que descargar el e-mail nuevo o refrescar la página para ver los nuevos mensajes.

#### 2.4.5.5 Resumen

Ya sea que se utilice POP3 o IMAP4 para obtener los mensajes, los clientes siempre utilizan SMTP para enviar mensajes. Los clientes de correo electrónico son comúnmente denominados clientes POP ó IMAP, pero en ambos casos se utiliza SMTP. Así pues, un servidor de correo consta en realidad de dos servidores: un servidor SMTP que será el encargado de enviar y recibir mensajes y un servidor POP/IMAP que será el que permita a los usuarios obtener sus mensajes.

En cualquier caso, los protocolos SMTP/POP/IMAP son inseguros en cuanto a que los mensajes viajan en claro por la red, es decir, es fácil obtener los mensajes y contraseñas. Para ello se suele añadir una capa SSL, es decir, un método de encriptación que puedan implementar tanto el servidor como el cliente.

| Comparación POP3 vs IMAP | | |
|---|---|---|
| **Característica** | **POP3** | **IMAP** |
| E-mail se almacena | PC | Servidor |
| E-mail se lee | Off-line | On-line |
| Tiempo de conexión | Bajo | Alto |
| Recursos empleados | Pocos | Muchos |
| Múltiples mailboxes | No | Sí |
| Adecuado usuarios móviles | No | Sí |
| Descarga parcial mensajes | No | Sí |
| Problema espacio servidor | No | Puede |
| Simplicidad implementación | Simple | Complejo |
| Uso generalizado | Sí | Medio |

**Tabla. 2.1. Comparación Pop3 vs. IMAP**

**Fuente: Pagina Wikipedia**

#### 2.3.5.6. AP (Lightweight Directory Access Protocol)

Es un protocolo de red de acceso unificado que permite el acceso a un servicio de directorio ordenado y distribuido para buscar diversa información en un entorno de red. LDAP puede considerarse una base de datos, aunque su sistema de almacenamiento puede ser diferente, habitualmente, se lo usa para almacenar información del usuario: Datos de contacto del usuario, ubicación de diversos recursos de la red, permisos incluso certificados, a los que se puede realizar consultas.

### 2.3.6. Cliente Servidor de Correo Electrónico

El cliente e-mail es un programa habitualmente llamado "mail" que permite la lectura de los ficheros buzón a cada usuario autorizado. También es capaz de manejar el "spool" de correo es decir, de enviar mensajes que serán leídos por el servidor e-mail para poder ser distribuidos a otros usuarios. El servicio encargado de proporcionar el intercambio de correo electrónico entre las máquinas se denomina servicio de e-mail, y puede ser ofrecido por distintos programas daemon, de los que el más extendido se llama "sendmail". El daemon sendmail es el servidor de correo electrónico más popular entre las máquinas de Internet. Según algunos estudios, constituye entre el setenta y el ochenta por ciento de las implementaciones existentes hoy en día.

Realiza su función manteniéndose a la escucha del socket 25, comunicándose con los daemons de otros sistemas para recibir el correo entrante y enviar el correo saliente. En cuanto a la aplicación TCP/IP, se utiliza el protocolo SMTP (Simple Mail Transfer Protocol), el cual se caracteriza por su eficiencia, sencillez y facilidad de depuración, gracias a los mensajes que acompañan a sus comandos.

Estos ¨mailer¨ son programas para gestionar los mensajes recibidos y poder escribir nuevos estos suelen incorporar muchas más funcionalidades que el correo web, ya que todo el control del correo pasa a estar en el ordenador del usuario.

El funcionamiento de un programa de correo es muy diferente al de un correo web, ya que un programa de correo descarga de una sola vez todos los mensajes que se tienen disponibles y luego pueden ser leídos sin estar conectados a Internet (además, se quedan grabados en el computador). En cambio, en una página web, se leen los mensajes de uno en uno, debiendo mantenerse activa la conexión a la red, algunos ejemplos de programas de correo son: Mozilla Thunderbird, Outlook Express y otros.

**2.4. Seguridad Informática.**

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

El concepto de seguridad de la información no debe ser confundido con el de seguridad informática, ya que este último sólo se encarga de la seguridad en el medio informático, pero la información puede encontrarse en diferentes medios o formas, y no solo en medios informáticos.

La seguridad informática es la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información seguro y confiable.

### 2.4.1. Seguridad de la Información.

Para llevar adelante la presente investigación se tomo en cuenta el estándar internacional ISO/IEC 27002 la misma que define a la seguridad de la información de la siguiente forma "La información es un recurso que, como el resto de los importantes activos comerciales, tiene valor para una organización y por consiguiente debe ser debidamente protegida".

Es decir es un proceso muy largo y complejo que comprende el uso de mecanismos y medidas, para impedir o dificultar la obtención de información por parte de entes no autorizados, desde los sistemas de comunicación. Puesto que los daños y perjuicios por la pérdida de información pueden llegar a poner en peligro el trabajo y el normal desempeño de la institución.

La confianza excesiva en cualquier sistema de comunicación o el uso de nuevas tecnologías conforme se confía el desempeño de tareas a los sistemas de comunicación electrónicos debilitan la seguridad de los mismos. Es por eso que la información debe ser protegida con todos los mecanismos y medidas de seguridad como sea posible.

### 2.4.2. Estándar Internacional ISO/Iec 27002, Código de Práctica para la administración de la seguridad de la información.

El presente trabajo de investigación se basa en esta norma Internacional ya que el mismo va orientado a la seguridad de la información en las empresas u organizaciones, de modo que las probabilidades de ser afectados por robo, daño o pérdida de información se minimicen al máximo.

ISO es el acrónimo de International Organization for Standardization, los fundadores decidieron que fuera ISO, derivado del griego "*isos"*, que significa "igual". Por lo tanto, en cualquier país o en cualquier idioma, el nombre de la institución es ISO. Se trata de una organización desarrolladora y publicadora de Estándares Internacionales más grande en el

mundo. ISO es una red de instituciones de estándares nacionales de 157 países, donde hay un miembro por país, con una Secretaría Central en Geneva, Suiza, que es la que coordina el sistema.

ISO es una organización no gubernamental que forma un puente entre los sectores públicos y privados. Nació con el objetivo de "facilitar la coordinación internacional y la unificación de los estándares industriales."

#### 2.4.2.1. Directrices del estándar ISO/IEC 27002.

El estándar internacional ISO/IEC 27002 esta basado en la ISO/IEC 17799 la misma proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información (GSI), a todos los interesados y responsables en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información.

La versión de 2005 del estándar incluye las siguientes once secciones principales:

1. Política de Seguridad de la Información.
2. Organización de la Seguridad de la Información.
3. Gestión de Activos de Información.
4. Seguridad de los Recursos Humanos.
5. Seguridad Física y Ambiental.
6. Gestión de las Comunicaciones y Operaciones.
7. Control de Accesos.
8. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información.
9. Gestión de Incidentes en la Seguridad de la Información.
10. Gestión de Continuidad del Negocio.
11. Cumplimiento.

Dentro de cada sección, se especifican los objetivos de los distintos controles para la seguridad de la información. Para cada uno de los controles se indica asimismo una guía para su implantación. El número total de controles suma 133 entre todas las secciones aunque cada

organización debe considerar previamente cuántos serán realmente los aplicables según sus propias necesidades.

### 2.5.1.2. Certificación.

La norma ISO/IEC 27002 especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI) según el famoso "Círculo de Deming": PDCA-acrónimo de **P**lan, **D**o, **C**heck, **A**ct (Planificar, Hacer, Verificar, Actuar), misma que fue elaborada con el propósito de poder certificar los Sistemas de Gestión de la Seguridad de la Información implantados en las distintas organizaciones por medio de un proceso formal de auditoría realizado por un tercero.




**Fig. 2.2.** Círculo de Deming
**Fuente**: Imágenes de internet

### 2.5.1. Preservación de la información.

Para la realización del presente trabajo de investigación se tomo en cuenta el estándar internacional ISO/IEC 27002 de acuerdo con esta norma, para proteger la información de los usuarios a través de redes de comunicación de datos, es necesario minimizar al máximo las probabilidades de pérdida de información, daño o robo dotando a la información de:

- **Integridad,** al hablar del término integridad de datos (cualquier documento o información almacenada digitalmente) se refiere a la veracidad, y completitud de los mismos que no han sido alterados (modificados, borrados) de una manera no autorizada

desde el momento en que fueron creados, guardados o mientras estos están siendo transmitidos.

- **Confidencialidad,** evita que se revelen, deliberada o accidentalmente, los datos de una comunicación. Las entidades no autorizadas no podrán tener acceso a la información protegida del sistema, además permite a un usuario enviar un mensaje asegurado con la garantía de que solamente su destinatario podrá leerlo

- **Disponibilidad**, garantiza que la información y la capacidad de su procesamiento manual y automático, sean resguardados y recuperados eventualmente cuando sea necesario.

### 2.4.3. Manejo de la Información

El correcto manejo de la información dentro de una institución requiere de políticas relacionadas al procesamiento de gestión del riesgo de cualquier tipo de información, sea que se produzca al interior de la institución o fuera de ella, esta gestión de riesgo engloba la obtención o generación de la información con un mínimo de riesgo, realizando la clasificación, envió-recepción y finalmente el archivo..

La información de un correo electrónico procesada clasificada y archivada correctamente ayudará a las instituciones a desempeñarse eficazmente, y a ser más rápidas en la toma de decisiones, haciendo la diferencia con las demás en todo momento. Esta información de acuerdo a su clasificación debe ser protegida, cuidándola de pérdidas, robos o alteraciones; pero a la vez se debe tratar que esta información sea accesible a las personas que deben hacer uso de ella en el momento apropiado.

### 2.4.4. Gestión de Riesgo

Antes de comenzar a describir en qué consiste el proceso de gestión de riesgos es importante saber diferenciar ciertos conceptos que son manejados en esta investigación tales como

amenaza, impacto, vulnerabilidad, etc. para definir y describir aspectos relacionados con los riesgos.

**Vulnerabilidad,** una vulnerabilidad es una debilidad que puede ser 'activada' de forma accidental o intencionadamente. Es un factor de riesgo interno de un elemento expuesto a una amenaza de ser susceptible a sufrir un daño y de encontrar dificultades en recuperarse posteriormente.

El análisis de la amenaza en una institución debe incluir un análisis de las vulnerabilidades asociadas al entorno del sistema. El objetivo es desarrollar una lista de vulnerabilidades que pueden transformarse en fuente potencial de amenazas.

**Amenaza,** una amenaza es la posibilidad de que se produzca una determinada vulnerabilidad de forma satisfactoria. Una fuente de amenazas no plantea un riesgo cuando no hay vulnerabilidades que puedan ser 'activadas'.

Al determinar la probabilidad de ocurrencia de una amenaza, se deben tener en cuenta las fuentes de las amenazas, las vulnerabilidades potenciales y los controles existentes, es decir, una amenaza es una circunstancia o evento con la capacidad de causar daño a un sistema, entendiendo como daño una forma de destrucción, revelación o modificación de datos.

**Impacto,** el impacto es la materialización de un riesgo; una medida del grado de daño, entendiendo como riesgo la probabilidad de que un evento desfavorable ocurra y que tendría un impacto negativo si se llegase a materializar.

**Riesgo,** es un evento o condición incierto que, si se produce, tendrá un efecto positivo o negativo sobre al menos un objetivo del proyecto, como tiempo, coste, alcance o calidad, las instituciones perciben los riesgos por su relación con las amenazas al éxito del proyecto.

Una vez conocidos los conceptos que serán manejados durante el proceso de investigación se pasa a definir lo que es gestión de riesgo.

Gestión de riesgo es un proceso iterativo y recurrente a lo largo de toda la vida del proyecto. El propósito de la gestión de riesgos es minimizar la probabilidad y consecuencias de los riesgos negativos (o amenazas) y maximizar la probabilidad y consecuencias de los riesgos positivos (u oportunidades) identificados para el proyecto de tal forma que los objetivos de los proyectos se cumplan.

Los objetivos de la gestión de los riesgos son aumentar la probabilidad y el impacto de los eventos positivos, y disminuir la probabilidad y el impacto de los eventos adversos. Las instituciones normalmente están en entornos de negocio con riesgo, ya que los proyectos tienen riesgos. Al gestionar los riesgos de forma proactiva, se conseguirá mejorar el beneficio de la institución.

### 2.4.5. Clasificación de la información

Toda la información debe ser clasificada como restringida, confidencial, de uso interno o general. La clasificación de la información debe de ser documentada por el propietario, aprobada por el comandante responsable y distribuida a los custodios ya que la clasificación asignada a un tipo de información solo puede ser cambiada por el propietario de la información, luego de justificar formalmente el cambio en dicha clasificación.

La información que existe en más de un medio (documento, fuente, registro electrónico, reporte o red), debe tener la misma clasificación sin importar el formato. Frecuentemente la información deja de ser sensible o crítica después de un cierto periodo de tiempo, cuando la información se ha hecho pública.

### 2.4.6. Tipos de información

**Secretísima o Restringida:** Información con mayor grado de sensibilidad, el acceso a esta información debe ser autorizada, caso por caso.
**Secreta o Confidencial:** Información sensible que solo puede ser divulgada a aquellas personas que la necesiten para el cumplimiento de sus funciones.

Reservada o de uso Interno: Datos generados para facilitar las operaciones diarias, deben ser manejados de una manera discreta, pero no requiere de medidas elaboradas de seguridad.
**General:** Información que es generada específicamente para su divulgación a la población general de usuarios.

### 2.5. Métodos y metodologías de gestión de riesgo utilizadas.

Para el desarrollo de la propuesta se utilizo el método Delphi en la identificación de riesgos, que es una forma de llegar a un consenso de expertos. Es la búsqueda de consenso entre especialistas (expertos) sobre eventos futuros. Los expertos en riesgos de proyectos participan en esta técnica de forma anónima. Un facilitador emplea un cuestionario con definición clara de objetivos y resultados deseados, para solicitar ideas acerca de los riesgos importantes del proyecto. Las respuestas son resumidas y luego enviadas nuevamente a los expertos para que realicen comentarios adicionales. En pocas rondas de este proceso se puede lograr el consenso. El método Delphi ayuda a reducir sesgos en los datos y evita que cualquier persona ejerza influencias impropias en el resultado.

Para el análisis de los riesgos se utilizo la metodología Magerit, que es un método formal para investigar los riesgos que soportan los Sistemas de Información y para recomendar las medidas apropiadas que deberían adoptarse para controlar estos riesgos, esta metodología permite:

- Estudiar los riesgos que soporta un sistema de información y el entorno asociado a él. MAGERIT propone la realización de un análisis de los riesgos que implica la evaluación del impacto que una violación de la seguridad tiene en la institución; señala los riesgos existentes, identificando las amenazas que acechan al sistema de información, y determina la vulnerabilidad del sistema de prevención de dichas amenazas, obteniendo unos resultados.
- Los resultados del análisis de riesgos permiten a la gestión de riesgos recomendar las medidas apropiadas que deberían adoptarse para conocer, prevenir, impedir, reducir o controlar los riesgos identificados y así reducir al mínimo su potencialidad o sus posibles perjuicios.

## 2.6. Medidas y Mecanismos de Seguridad

Son elementos importantes dentro de la operación de un sistema de comunicaciones, ya que mediante el uso de estos se debe tratar de evitar que cualquier tipo de ataque afecte la integridad de recursos y datos que son manipulados. Un sistema de comunicaciones es seguro si cuenta con políticas y mecanismos que proporcionen protección y seguridad, de esta manera podemos establecer que para proteger un sistema de comunicaciones dependemos de la seguridad del mismo. La principal finalidad que se persiguen con estas medidas y mecanismos, son reducir las vulnerabilidades y deficiencias de los sistemas de comunicación. Dentro de las medidas y mecanismos más importantes tenemos los siguientes:

### 2.6.1.1 Contraseñas

Las palabras en español “contraseña” o “clave” que en inglés se las conoce como password (palabra de acceso) o, pass code (código de acceso), no son más que una forma de autenticación que utiliza información secreta del usuario para controlar el acceso hacia algún determinado recurso, no necesariamente involucran a una palabra familiar o un código numérico especifico, como normalmente se lo hace únicamente por razones de memorización y facilidad del usuario. También se las conoce con el nombre PIN (Personal Identification Number) por tratarse de códigos numéricos

- **Funcionamiento,** el uso de contraseñas es muy similar a la guardia militar que realizan los centinelas cuando custodian una dependencia, estos requerirán el santo y seña a la persona que desee ingresar y solamente le permitirán el acceso a aquella persona que conociera esta clave. En la actualidad, las contraseñas son usadas comúnmente para controlar el acceso a sistemas operativos de computadoras protegidas, teléfonos celulares, decodificadores de televisión por cable, cajeros automáticos, etc. Un computador puede hacer uso de contraseñas para diferentes propósitos, desde acceder al mismo computador, hasta realizar conexiones a cuentas de usuario de correo electrónico(e-mail), manejo de servidores, acceso a bases de datos, redes de comunicación, e incluso páginas web con servicios en línea.

- **Ventajas,** si algún recurso está protegido por una o más contraseñas, aunque esto signifique molestias para los usuarios, la seguridad se incrementa y reduce la vulnerabilidad.

- **Desventajas,** lamentablemente el proteger sistemas de comunicación mediante contraseñas no garantiza la total seguridad de estos. Una contraseña muy corta, quizás elegida por conveniencia del usuario, tanto para el buzón de correo electrónico como para su computadora y otros dispositivos es muy vulnerable, ya que en la actualidad las computadoras usando software (diccionarios) en los que se tienen almacenado pistas de las posibles contraseñas con las que se realiza comparaciones a grandes velocidades se intentan todas las combinaciones en orden alfabético, numérico y de caracteres especiales que tengan menos de 7 caracteres, de esta manera contraseñas débiles se pueden obtener fácilmente.

- **Recomendaciones de contraseñas,** enseñar al usuario a evitar usar contraseñas débiles así como dejar pistas de las mismas.

Por lo tanto serán necesarias contraseñas más robustas, esto se consigue realizando combinaciones de números, letras en carácter mayúscula y minúscula y mejor aún si se usan caracteres especiales como: @, €, #; pues el uso de caracteres ASCII en una contraseña la hace inquebrantable, además sistemas operativos como Windows permite usar espacios en blanco que no es muy recomendable pero de ser necesario y si el usuario está acostumbrado a usar complejos sistemas de contraseñas lo puede hacer.

#### 2.6.1.2. Antiespias

En todo momento se debe tener presente que el sniffing es un peligro real, que no necesita de grandes medios para su implementación y que además es indetectable en la mayor parte de casos, a pesar de que existen métodos para tratar de detectar sistemas con un interfaz en modo promiscuo, no suelen ser del todo efectivos, ya que el detectar una máquina en este estado no es una inmediata solución de seguridad total.

- **Funcionamiento,** para evitar que programas de tipo Snifig capturen información es recomendable implementar en el sistema de comunicación de datos: VPN (redes privadas virtuales), implantar protocolos SSL (https) o túneles seguros, que son más o menos efectivas, así como también sustituir los hubs de la red por switch, los que aíslan los dominios de colisión, con lo que se dificultan los ataques pero no se los imposibilitan.

- **Ventajas,** son técnicas sencillas que proporciona un incremento de seguridad abismal en el entorno de red al acceder sitios web seguros.

- **Desventajas,** implementar estos dispositivos quizás es algo costoso y que toma algo de tiempo, pero también en la mayoría de ocasiones es algo que se recomienda implementar a pesar de no ser una garantía de total seguridad.

- **Recomendaciones antiespías,** tener siempre al día las actualizaciones de seguridad del sistema operativo (parches), además se debe instalar un buen cortafuegos (firewall).

#### 2.6.1.3 Firewalls

Los Firewalls o cortafuegos son un tipo de seguridad muy efectiva en redes de comunicación de datos, que a menudo son instalados en el punto donde la red interna se conecta con Internet, para que todo el tráfico externo de Internet hacia la red interna pase a través del Firewall. De esta manera se puede determinar si dicho tráfico es aceptable e inofensivo de acuerdo a las políticas de seguridad de la administración, intentando así prevenir a los usuarios de la red interna de ataques externos.

- **Funcionamiento,** rara vez un Firewall es un simple objeto físico ya que generalmente es un conjunto de componentes de hardware y software combinaciones de routers, redes con software apropiado, computadoras y lógicamente un host que se encargan de proteger a la red interna de amenazas externas filtrando los paquetes de información que ingresan a la red.

El sistema de filtrado paquetes entre host internos y externos, de manera selectiva y permite bloquear cierto tipo de paquetes de acuerdo con las políticas de seguridad de la red. Casi todos los dispositivos actuales de filtrado de paquetes (enrutadores de selección o compuertas de filtro de paquetes) operan de la siguiente forma:

Cuando un paquete llega al puerto, los encabezados de los paquetes son analizados, la mayoría de los filtros analizan los campos sólo en los encabezados IP, TCP o UDP. Las reglas del filtrado de paquete se almacenan en un orden específico, cada regla se aplica al paquete en el mismo orden en que la regla del filtro de paquetes se almacenó. Si una regla permite la transmisión o recepción de un paquete, el paquete sigue su camino; si una regla bloquea la transmisión o recepción del paquete, el paquete no se acepta.

Si un paquete no satisface ninguna regla, es bloqueado; es decir no accede aquello que no esté expresamente permitido, es por eso que es muy importante colocar las reglas en el orden correcto.

- **Ventajas,** La principal aplicación del Firewall es el filtrado de paquetes pero también tiene otros usos y múltiples propósitos.

- **Desventajas,** un error común al configurar las reglas del filtro de paquetes es hacerlo en desorden. Si dichas reglas se colocan en un orden equivocado, podrían terminar denegando servicios válidos, mientras que permitirían los servicios que deseaba denegar.

- **Recomendaciones Firewall,** tener al día las actualizaciones de seguridad del sistema operativo (parches). El Firewall trabaja mejor si se complementa con una defensa interna y con otros mecanismos de seguridad.

#### 2.6.1.4. Proxi

Proxy es un sistema intermediario entre hosts internos de una red y los hosts de Internet de tal forma que reciba las peticiones de unos y se las pasen a los otros, previa la verificación de

accesos y privilegios. Este sistema puede correr en hosts "dual-homed" o hosts "bastion" los cuales son llamados Servidores Proxy.

Los sistemas Proxy son efectivos solo si se utilizan junto a métodos de restricción de tráfico IP entre clientes y servidores reales. De este modo, un cliente no podrá "bypasear" (desviar el trafico) el servidor Proxy para comunicarse con un servidor real utilizando este protocolo.

- **Funcionamiento,** El programa cliente usuario se comunica con el servidor proxy enviando pedido de conexión con un servidor real, el servidor proxy evalúa esta petición y decide si se permitirá la conexión, si el servidor Proxy permite la conexión, envía al servidor real la solicitud recibida desde el cliente.

  La comunicación entre el programa cliente y el servidor Proxy puede realizarse de dos formas distintas:

  - Custom Client Software.- Es un software cliente standard que ha sido modificado para que cumpla ciertos requerimientos. El cliente debe saber cómo opera el servidor Proxy, cómo contactarlo, cómo pasar la información al servidor real, etc.
  - Custom User Procedures.- El usuario utiliza un cliente standard para conectarse con un servidor Proxy y usa diferentes procedimientos (comandos del servidor Proxy) para pasar información acerca del servidor real al cual quiere conectarse, el servidor Proxy realiza la conexión con el servidor real.

- **Ventajas,** Permite a los usuarios acceder a los servicios de Internet ocultando totalmente la red interna, también permite un buen servicio de logs a nivel de cada aplicación, debido a que todo el tráfico pasa a través del servidor Proxy y se puede registrar gran cantidad de información con fines de auditoria y seguridad. El servidor Proxy de Circuito provee soporte para un conjunto grande de protocolos.

- **Desventajas,** A menudo se requiere la modificación del software cliente. Pero hay software que esta disponible solo para ciertas plataformas: Por Ej: GATEWAY es un package Proxy para FTP y TELNET de SUN que corre solo sobre SUN. La disponibilidad de estos tipos de paquetes a menudo no es inmediata.

Algunos servicios no son viables para trabajar con servidores Proxy, además el uso de servidores Proxy introduce algún retardo en las comunicaciones y finalmente los servidores Proxy de circuitos no brindan control específico sobre las aplicaciones.

#### 2.6.1.5. Antivirus

Los antivirus son programas de computadora cuyo propósito es detectar o encontrar la traza de los programas maliciosos mientras el sistema operativo está funcionando, con el fin de tener controlado el sistema, parando las vías conocidas de infección, combatiendo y eliminando virus informáticos y otros programas maliciosos, notificando, además, al usuario de posibles incidencias de seguridad mientras se está trabajando.

- **Funcionamiento,** el antivirus tiene un componente que se carga en memoria del computador y permanece en ella para verificar todos los archivos abiertos, creados, modificados y ejecutados en tiempo real; normalmente escanea cada archivo en la computadora e incluso archivos adjuntos de los correos electrónicos y compara el código de estos archivos con una base de datos de los códigos también llamados como firmas o vacunas de los virus conocidos hasta la ultima actualización, por lo que es muy importante actualizarla periódicamente a fin de evitar que un virus nuevo no sea detectado.

- **Ventajas,** el antivirus inspecciona los ficheros en busca de cadenas asociadas a virus y otros síntomas propios de la modalidad de virus que, permite su identificación. Si el antivirus tiene capacidad para ello, "desinfectará" el ordenador.

- **Desventajas,** como programa, que está continuamente funcionando, presentan ciertas desventajas, ya que al ser residentes consumen memoria RAM y pueden también resultar incompatibles con algunas aplicaciones.

  Por otro lado, pueden llegar a resultar bastante molestos, puesto que por lo general suelen interrumpir el trabajo habitual con la computadora alertándo de intentos de acceso a memoria o a disco que en muchos casos provienen de programas sanos.

- **Recomendaciones antivirus,** Tener siempre al día las actualizaciones de vacunas o firmas del antivirus. Instalar un buen cortafuegos (firewall) y tenerlos siempre activados. A la hora de comprar un buen antivirus el usuario debe saber con qué frecuencia el fabricante obtiene y publica actualizaciones de las tablas de virus y sus respectivos antivirus.

### 2.6.1.6. ANTISPAM

Es un software que sirve para evitar recibir correo electrónico no deseado y mailbombing, con el propósito de no hacer un mal uso de los recursos electrónicos o retardar el trabajo por la pérdida de tiempo de los usuarios.

- **Funcionamiento,** Este tipo de programas utilizan en general diversas técnicas, tales como enviar mensajes al postmaster del dominio del que procede el spam o borrar directamente los mensajes sospechosos del servidor de correo ya que suelen incluir sistemas de filtrado de mensajes que pueden ser útiles para evitar descargarlos.

- **Ventajas,** El disponer de software antispam es una buena medida de seguridad, aunque las actitudes a tomar por parte de los usuarios son las que verdaderamente ayudan a no ser victimas de este tipo de amenazas que tienen que ver más con la personalidad de quien recibe el mensaje.

- **Desventajas,** La lucha del antispam contra el spam es considerada como una guerra perdida ya que habiendo la probabilidad de que casi el 12% del correo no solicitado sea respondido, para los negocios es una razón factible para que se siga enviando correo no deseado aumentando el recibo de información no solicitada al buzón de correo electrónico.

- **Recomendaciones para evitar el spam,** Nunca se debe contestar un mensaje de spam ya que en muchos casos la dirección del remitente será falsa y al contestar este mensaje esto solamente servirá a la empresa de publicidad para saber que la dirección E-mail es correcta. Incluso cuando la empresa prometa dejar de enviar spam ya que a menudo ofrecen una forma de anular la suscripción a su boletín de mensajes (lo que en inglés llaman "opt-out", u optar por salir) que suele consistir en mandar un mensaje a una

dirección de tipo unsubscribe@dominio.com. Si se manda un mensaje a dicha dirección con la esperanza de dejar de recibir correo no solicitado, sólo se está confirmando que esa cuenta existe y está activa, por lo que el usuario acabará recibiendo más spam que antes.

Simplemente el usuario debe borrar el mensaje de su buzón y suponer que no lo recibió, muchos de estos son distinguibles a simple vista porque incluyen o el signo ($) dólar, o valores en el encabezado con palabras GRATIS o FREE.

## 2.7. Amenazas a la Información de los correos electrónicos.

Amenazas son condiciones que a diario rodean el entorno de un sistema de comunicación: personas, máquinas y sucesos; los mismos que aprovechan la mínima oportunidad para dar lugar a que se produzca una violación de la seguridad, confidencialidad, integridad, y disponibilidad, tales eventos que pueden causar un impacto adverso o no deseado, de orden menor o mayor.

La implementación de políticas de seguridad y el análisis de riesgos ayudan a identificar las amenazas que han de ser contrarrestadas, dependiendo del diseñador del sistema de seguridad que será el encargado de especificar los servicios y mecanismos de seguridad necesarios.

Las amenazas a la seguridad de la información puede estar presente en una fuente, como por ejemplo: un fichero, un disco duro o una región de la memoria principal, así mismo puede encontrarse en el transporte, como por ejemplo en la red y en su destino como en el buzón de correo del usuario. Un ataque sobre cualquiera de estos, no es más que la realización de una amenaza de las que podemos citar las siguientes:

#### 2.7.1.1. Espías

Son aquellos entes que, sin permiso o conciencia de sus actos por parte de un afectado, adquiere información privada de este para beneficio propio o de terceros. Estos espías pueden atacar desde Internet burlando la seguridad de la red, como también pueden infiltrarse físicamente dentro de la institución, aprovechando alguna vulnerabilidad. Se los considera

como delincuentes porque realizan ataques a un derecho de la humanidad como son la intimidad y la privacidad, sus prácticas son sancionadas por la ley pero sin embargo se la sigue realizando deliberadamente.

Dentro de esta clase de amenaza también se encuentran los espías internos que son personas que están dentro del entorno diario de trabajo y que gozan de total confianza por considerarlos inofensivos, los cuales pueden sobrepasar cualquier sistema de seguridad hasta los lugares donde reposa o circula la información y sin despertar la menor sospecha podrían realizar algún tipo de ataque en su beneficio o de terceros.

#### 2.7.1.2. Spyware

Es un Software de tipo espía, creado con la finalidad de recoger información del usuario, como por ejemplo saber qué tiene instalado en su computador. La manera como lo hacen es usando librerías que se instalan con muchos programas gratuitos o incluso en algunas cookies o banners que pincha o se descarga el usuario al visitar algunas páginas de Internet sin saber las intenciones ocultas que lleva consigo este software "gratuito" que se encarga de recoger la información sobre las páginas que son visitadas.

#### 2.7.1.3. Sniffer

Un programa sniffer tiene como utilidad la monitorización de la red (medir el ancho de banda utilizado y en que está siendo usado), también detecta fallos de seguridad en ella o en los sistemas. Dentro de los sniffers podríamos citar otras utilidades de control de programas del tipo KSA y SATAN, que, además de buscar las debilidades de un sistema, son empleados como Sniffers, esto es monitorización de la red y la unidad central. Una navegación lenta en Internet nos puede indicar que hay un sniffer en línea.

#### 2.7.1.4 Hacker

Se definen como hackers a los expertos en programación y que poseen conocimientos elevados sobre informática y electrónica que disfrutan explorando sistemas informáticos y probando sus

capacidades. Un Hacker no es un delincuente como los medios han difundido, más bien es un investigador antes que un destructor, este personaje ayuda a la comunidad de sistemas de información a analizar el código en los sistemas y programas que se utilizan a diario, y no son para nada, agentes destructivos que buscan dinero o reconocimiento, existen diferentes tipos de hacker entre estos se puede mencionar:

- **Hacker Ético (Profesional),** Profesional en seguridad empleando sus habilidades de hacking con propósitos defensivos.

- **Hacker (White Hat),** Analistas de seguridad, que utiliza sus conocimientos para proteger información de todo tipo además ayuda a las organizaciones a desarrollar sus defensas.

- **Hacker (Grey Hat),** Analistas de seguridad, que utiliza sus conocimientos para proteger información de todo tipo, sin embargo, sus intenciones y desarrollo de actividades se observan con recelo ya que en cierta medida pertenecen a grupos de trabajo Red Team (equipo de trabajo dedicado a desarrollar software) que ejercen ofensivas periódicas contra otros grupos en la red.

- **Hackers (Black Hat),** Hackers maliciosos, donde la mayoría de ellos tienen grandes habilidades computacionales.

- **Hackers (Formalmente Black Hat),** Pueden ser Crackers "reformados" tomando ventaja de haber estado en el lado oscuro de la ley (prisión), en muchos casos percibidos con mucha credibilidad por su experiencia.

#### 2.7.1.5. Craker

El Cracker diseña y fabrica tanto programas como hardware de guerra para reventar claves, software y servicios de comunicación como el teléfono, el correo electrónico o el control de otros computadores remotos, etc. Hay muchos Crackers que "cuelgan" páginas WEB por diversión o envían a la red su última creación de virus, también existen crackers que se dedican a crear Cracks para Software importante y negocian con ellos: Cracks para tarjetas, Shareware

y sistemas electrónicos como el DVD o las consolas Playstation entre otros, existen diferentes tipos de crackers estos son:

- **Cracker (Script Kiddie),** Hacker malicioso con un nivel de conocimiento limitado, motivado en muchos casos por venganza o desconocimiento.

- **Cracker (Packet Monkey),** Cracker muy parecido al script kiddie, pero que ejecuta mayormente ataques de denegación de servicios.

#### 2.7.1.6. Lamer

Es un aficionado en el tema y que ha visitado varias páginas web sobre Hacking y se ha bajado unos cuantos programas. Después hace uso de ellos indebidamente y sin conocimientos, de los mismos destruye su propio computador como otros de la red y cuando esto sucede se siente alguien superior a los demás. Este tipo de personajes es quien emplea los Back Orifice, Netbus o virus con el fin de fastidiar y lo realiza sin tener conocimientos de lo que realmente está haciendo.

#### 2.7.1.7. Pirata Informático

Un pirata informático es quien hace copias de Software en CD y comercializa con ellos. Posee conocimientos informáticos únicamente para duplicar discos y este es el grupo que más ensucia a la nueva sociedad de Hackers, después de los Lamers.

### 2.7.2. Amenazas Deliberadas a los correos electrónicos.

#### 2.7.2.1. Interrupción

Una interrupción del sistema de comunicación se da cuando todo el sistema o un recurso del mismo es destruido volviéndolo no disponible. Es por esto que también se lo puede considerar como un ataque contra la disponibilidad. Este tipo de interrupciones o ataques son la destrucción de un elemento hardware, como ser un disco duro, un servidor; cortar temporal o

indefinidamente una línea de alimentación de energía o de comunicación, también si accidental o maliciosamente se llegara a deshabilitar el sistema de gestión de archivos, ocasionando una indisponibilidad temporal o definitiva del sistema de comunicaciones.

#### 2.7.2.2. Interceptación

Es muy importante comprender que la interceptación de un sistema de comunicación es un ataque contra la confidencialidad de los usuarios del mismo. Ya que una entidad no autorizada (una persona, un ordenador o un programa) consigue tener acceso a determinado recurso de un sistema de comunicación realizando acciones de ataque, como puede ser pinchar una línea de comunicación, para que, con la intercepción de datos que circulen por la red, pueda elaborarse una copia ilícita de documentos, archivos o programas. También el interés puede ser la lectura de las cabeceras de paquetes para develar la identidad de uno o más de los usuarios implicados en la comunicación lo que desde luego es ilegal y se lo conoce como intercepción de identidad.

#### 2.7.2.3. Modificación

La modificación realizada por una entidad no autorizada, no sólo consigue acceder a un recurso, sino que además es capaz de manipularlo. Es por eso que es considerado como un ataque contra la integridad. Ejemplos de este ataque son: El cambio de valores en un archivo de datos, alterar un programa para que funcione de forma diferente o también el modificar o desviar el contenido de mensajes que están siendo transferidos por la red.

### 2.7.3. Ataques

Existen muchas formas de acceder a la información que viaja por una red y por cuestiones de seguridad esto no debe ser permitido, se tiene que contemplar esquemas de seguridad y protección que abarquen aquellos sitios donde la información pueda estar disponible para todos, pero cuidándonos de la presencia de los intrusos.

Cuando los elementos de red son abiertos o públicos no existen muchos medios de seguridad y es muy difícil proteger estos datos ya que están disponibles en todo momento de forma pública. Existen dos tipos de ataques que pueden hacerse sobre la información:

**a) Ataques pasivos, u**n ataque pasivo es aquel en el cual el intruso sin modificar la información solamente monitorea el tráfico de datos que están siendo transmitidos por la red para capturar contraseñas (passwords) u otra información para su uso posterior. Este intruso solo se limita a establecer patrones para observar los mensajes de las aplicaciones sin interferir con ellos, ya que sus objetivos son obtener información de la intercepción de datos y el análisis de tráfico, estos ataques pasivos son muy difíciles de detectar, ya que no provocan ninguna alteración de los datos.

**b) Ataques activos,** En un ataque activo, el intruso interfiere con el tráfico legítimo que fluye a través de la red, creando algún tipo de modificación sobre el flujo de los datos transmitidos o también puede crear un flujo falso de datos logrando interactuar de manera engañosa con el protocolo de comunicación. En este tipo de ataques se realizan una variedad de procesos en el flujo de los mensajes que nos pueden afectar directa o indirectamente. Se pueden destacar 4 categorías:

- **Modificación del mensaje,** Consiste en realizar modificaciones directamente sobre el contenido del mensaje (borrar, insertar, modificar). Una porción del mensaje legítimo es alterado o reordenado, para producir un efecto no autorizado.

- **Denegar entrega de mensaje,** Consiste en no permitir que el mensaje sea entregado a su destino a través de bloqueos o retenciones. Lo cual impide o inhibe el uso normal de la gestión de recursos informáticos y de comunicaciones.

- **Retardar o reactuar la entrega de mensajes,** Consiste en hacer que un mensaje, de manera deliberada, no llegue a su destinatario en el tiempo normal. O también que uno o varios mensajes legítimos sean capturados y repetidos con el objeto de producir un efecto no deseado, como por ejemplo ingresar determinados valores repetidas veces en una cuenta dada.

- **Enmascaramiento o suplantación de la identidad,** consiste en utilizar una falsa identidad a fin de que le sea entregado un determinado mensaje, ya que el intruso se hace pasar por una entidad diferente. Normalmente incluye alguna de las otras formas de ataque activo, por ejemplo, secuencias de autenticación pueden ser capturadas y repetidas, permitiendo a una entidad no autorizada acceder a una serie de recursos privilegiados suplantando a la entidad que posee esos privilegios.

### 2.7.4. Virus

Un virus es un "programa informático (sea en código ejecutable, objeto o fuente) capaz de autoproducir su código en otros programas informáticos o de computadoras de manera transparente al usuario y que luego de transcurrido el tiempo de incubación/propagación, interfiere con el normal funcionamiento de una computadora o red de computadoras".

Los efectos perniciosos que causan los virus son variados; entre éstos se encuentran el formateo completo del disco duro, eliminación de la tabla de partición, eliminación de archivos, disminución del rendimiento de la computadora hasta limites exagerados, enlaces de archivos destruidos, archivos de datos y de programas corruptos, mensajes o efectos extraños en la pantalla, emisión de música o sonidos, etc.

#### 2.7.4.1. Clasificación

Todos estos programas tienen en común la creación de efectos perniciosos; sin embargo, no todos pueden ser considerados como virus propiamente dichos. La clasificación de los virus informáticos es la siguiente:

- **Virus "Per sé",** un verdadero virus o virus "per sé", cumple con todas y cada una de las tres primeras fases del funcionamiento de un virus. Un virus "per sé" también debe modificar el código original del programa "huésped" o soporte objeto de la infección, para poder activarse durante la ejecución de dicho programa; al mismo tiempo, una vez activado, el virus suele quedar residente en memoria para poder infectar otros programas o medios de forma automática y sin la intervención del usuario.

- **Bomba Lógica,** se trata simplemente de un virus informático que permanece residente en su huésped y contaminando a otros programas o computadoras "sanos" y que solo se activa cuando se produce una acción concreta, predeterminada por su creador, por ejemplo cuando se llega a una fecha específica, cuando se ejecuta cierto programa o se produce determinado "suceso" o "evento" en la computadora huésped.

- **Gusano o Worm,** un gusano o Worm es un programa cuya única finalidad es la de ir consumiendo la memoria del sistema, mediante la realización de copias sucesivas de sí mismo, hasta desbordar la memoria RAM, siendo ésta su única acción maligna.

- **Virus de Macro,** un virus de macro es un programa pernicioso escrito en un lenguaje de alto nivel, que funciona en entornos muy específicos, tales como las aplicaciones de Microsoft Office, y su característica principal es que funcionan directamente en código fuente y este fuente puede facilitar el transportase en medios de alta difusión como son los documentos que pueden crearse con estos programas, cuando son leídos en una computadora "sana", se produce la infección de este sistema, y de ahí en adelante todos los documentos que se creen serán portadores de este virus.

- **Caballo de Troya,** es un programa maligno que se oculta en otro programa, que es una aplicación válida y de interés para el usuario y que produce sus efectos perniciosos al ejecutarse este último. En este caso, no es capaz de infectar otros archivos o soportes, pero sí es capaz de autoproducir su código en otras computadoras y sólo se ejecuta una vez, aunque es suficiente, en la mayoría de las ocasiones, para causar su efecto destructivo.

### 2.7.5. SPAM

Son mensajes no solicitados, habitualmente de tipo publicitario, enviados en cantidades masivas y por distintas vías, aunque la más utilizada entre el público en general es la basada en el correo electrónico, internet, grupos de noticias usenet, motores de búsqueda, wikis y blogs.

El correo no solicitado tomó el nombre de 'Spam' de un producto producido en 1926 Hormel's Spiced Ham la primera carne enlatada que no requería refrigeración, característica que hacia

que estuviera en todas partes, incluyendo en los ejércitos americanos y rusos de la segunda guerra mundial. Inicialmente internet no permitía su uso comercial, pero al ser comprobado que su uso comercial es el que sostiene su infraestructura hoy en día es permitido.

#### 2.7.5.1. Formas de enviar spam

- **Spam por correo electrónico,** el spam mediante el servicio de correo electrónico nació en 1994, cuando una firma de abogados de EE.UU, publica en Usenet un mensaje de anuncio de su firma legal, el cual en el primer día, luego de su publicación, facturó cerca de 10.000 dólares por casos de lectores y de sus amigos presentados por la red. Desde ese entonces, el marketing mediante correo electrónico ha crecido a niveles impensados desde su creación.

  Siendo el correo electrónico, el medio más común de spamming en internet involucra enviar mensajes idénticos o casi idénticos a un gran numero de direcciones. A diferencia de los correos electrónicos comerciales legítimos, el spam generalmente es enviado sin el permiso explícito de los receptores o por una ingenua subscripcion del usuario de la cuenta, y que frecuentemente contiene varios trucos para sortear los filtros de spam.

- **Spam por mensajería instantánea, e**l spam por mensajería instantánea, también conocido como spim, utiliza los sistemas de mensajería instantánea, tales como ICQ o MSN Messenger. Muchos sistemas de mensajería ofrecen un directorio de usuarios, incluyendo información demográfica tal como edad y sexo. Los publicistas pueden reunir esta información, conectarse al sistema, y enviar mensajes no solicitados. Para enviar mensajes instantáneos a millones de usuarios de la mayoría de los servicios de mensajería instantánea sólo se requiere software de scripting y los nombres de usuario de los receptores. Los spammers también apuntan hacia los canales IRC, utilizando bots IRC que se conectan a los canales y los bombardean con mensajes publicitarios.

- **Servidores de correo mal configuradas,** los servidores de correo mal configurados son aprovechados también por los spammers. En concreto los que están configurados como Open Relay. Estos no necesitan un usuario y contraseña para que sean utilizados para el envío de correos electrónicos.

#### 2.7.5.2. Funcionamiento del Spam

- **Envío de los mensajes,** una vez que tienen una gran cantidad de direcciones de correo válidas (que existen), los spammers utilizan programas que recorren la lista enviando el mismo mensaje a todas las direcciones. Esto supone un costo mínimo para ellos, pero perjudica al receptor (pérdidas económicas y de tiempo) y en general a la red interna, por consumirse gran parte del ancho de banda en mensajes basura.

- **Verificación de la recepción,** El spammer controla cuáles direcciones atacadas funcionan y cuáles no, por medio de spyware, web bugs o pequeñas imágenes o similares contenidas en el código html del mensaje. De esta forma, cada vez que alguien lee el mensaje, su ordenador solicita la imagen al servidor del spammer, que registra automáticamente el hecho. Otro sistema es el de prometer en los mensajes que se dejará de recibirlos, enviando un mail en el cual se notifica el no deseo de recibir ese tipo de información por parte del usuario, pero esto solamente es un truco para verificar la existencia y veracidad de la cuenta de correo electrónico del usuario ya que cuando alguien contesta, significa no sólo que lo ha abierto, sino que lo ha leído.

### 2.7.6. Hoax / Joke

Es un mensaje cuyo contenido está basado en mentiras, engaños o falsedades, es un montaje considerado como una broma repugnante y de pésimo gusto, pero muy ocurrente y bien desarrollada en ocasiones relativas a falsos virus, creado para su reenvío masivo que muchas personas la creen y difunden sin saber que dicho mensaje estaría creado bien para causar algún tipo de perjuicio o tal vez para diversión de los creadores del mismo.

En el ámbito del mundo antivirus, se considera a los Hoax como mensajes enviados por lo general mediante correo electrónico, aunque pueden aparecer muchas veces en papel fotocopiado en el ambiente institucional, en los cuales se avisa en tono alarmante de la existencia de nuevos y potentes virus, muy peligrosos y destructivos. Estos supuestos virus en realidad no existen, o son archivos inofensivos sobre los que recae la elección de los creadores del Hoax.

### 2.7.6.1. Tipos de Hoax

- **Catastrofistas,** suelen hacer referencia a nuevos virus o bacterias (Biológicos) escapes radiactivos, predicciones sobre el fin del mundo cuyos signos evidentes se encargan de hacernos ver, actos cometidos por maniacos terroristas a los que no se consigue apresar. Estos Hoax suelen citar fuentes "oficiales", es decir: gobiernos, cadenas de televisión o empresas de antivirus.

- **Sobre virus informáticos nuevos y muy peligrosos,** es el Hoax por excelencia estos avisan en tono exageradamente alarmante de nuevos virus que son capaces de infectarnos hasta el televisor. Este tono alarmista puede ser un síntoma de Hoax, aunque hagan referencia a una fuente fiable, como alguna casa de antivirus.

- **Cadenas de solidaridad,** se basan en peticiones de ayuda para un enfermo Terminal, también pueden pedir el reenvío de una imagen de algún niño o persona desaparecida o piden la difusión y colaboración con alguna causa que active la conciencia social.

## 2.8. Políticas de seguridad de la información

Una política de seguridad de la información es un conjunto de reglas aplicadas a todas las actividades relacionadas al manejo de la información de una entidad, con el propósito de proteger la información y los recursos de la misma.

El cumplimiento de las políticas de seguridad de la información debe ser obligatorio y debe ser considerado para el personal que trabaja en las diferentes instituciones y su incumplimiento deberá ser considerado como una falta.

# CAPITULO III

## MODELO DE SEGURIDAD PARA LA IDENTIFICACIÓN DE AMENAZAS DE LOS CORREOS ELECTRÓNICOS INSTITUCIONALES

Luego de haber realizado el estudio detallado de los conceptos necesarios acerca del correo electrónico y la seguridad de la información, en este capítulo se desarrollo de la propuesta para la cual se tomo en cuenta diferentes normas y metodologías de identificación y evaluación de riesgos como la norma ISO/IEC 27001 y 27002 y los métodos Delphi y Margerit que son metodologías que se aplican para evaluar los riesgos de seguridad en la información de los correos electrónicos, dando cumplimiento con los objetivos planteados.

### 3.1.Objetivos.

#### 3.1.1. Objetivo General.

El objetivo general de esta investigación fue: Diseñar un modelo de seguridad que coadyuve en la identificación de amenazas de la Seguridad de correos electrónicos institucionales para la gestión de riesgos.

#### 3.1.2. Objetivos Específicos

- Diseñar un modelo para identificar amenazas de los correos electrónicos institucionales que cumpla con la norma (ISO/IEC 27002) y las metodologías estudiadas (Magerit, Delphi).
- Determinar si un correo mantiene su información de forma integra, confidencial, confiable y disponible.
- Identificar las amenazas y problemas relativos a la seguridad de correos electrónicos institucionales.
- Garantizar la seguridad de la información que viaja por un correo electrónico institucional considerando los aspectos de confidencialidad, integridad y disponibilidad.
- Establecer políticas de seguridad de correo electrónico que deben aplicar los usuarios.

- Aplicar el modelo propuesto en una institución.

### 3.2. Modelo de seguridad de correos electrónicos para la identificación de amenazas.

El siguiente modelo de seguridad permite identificar amenazas de los correos electrónicos institucionales, una vez identificadas las amenazas permite una buena administración o gestión de riesgos es decir, identifica, analiza, valora y maneja las amenazas para presentar un informe final el cual cuente con un plan de manejo de riesgos.

**Sistema Fácil de usar**, el requisito más importante para la utilización de un sistema de correo electrónico seguro es la facilidad de uso, tanto para los usuarios que envían los correos, como para los que reciben. Si el envío de correo electrónico es moderadamente más complejo que el correo electrónico convencional, los usuarios no lo usarán. Además, tomando en cuenta la norma ISO/IEC 2002, las políticas de seguridad propuestas al final del informe cuentan con:

**Eficacia:** para garantizar que toda la información utilizada es necesaria y útil para el desarrollo de la seguridad de un correo electrónico.
**Eficiencia:** para asegurar que el procesamiento de la información se realice mediante una optima utilización de los recursos humanos y materiales.
**Confiabilidad,** para garantizar que los sistemas informáticos brinden correos electrónicos con información correcta para ser utilizada.
**Integridad**, para asegurar que todo sistema de correo electrónico seguro, procese toda la información necesaria y suficiente para el envió y recibo de los correos electrónicos en cada uno de los procesos.
**Exactitud,** para asegurar que toda la información se encuentre libre de errores y/o irregularidades de cualquier tipo.
**Transparencia Global**, un correo electrónico seguro debería ser transparente en su habilidad de comunicarse con usuarios de diferentes tipos, ya sea si son usuarios de un sistema de mensajería corporativo o usuarios externos.
**Disponibilidad,** para garantizar que la información y la capacidad de su procesamiento manual y automático son resguardados de manera tal que no se interrumpa significativamente

**Legalidad,** para asegurar que toda la información que sea procesada y transportada cumplan con las regulaciones legales vigentes.

**Confidencialidad,** para garantizar que toda la información sea protegida del uso no autorizado, revelaciones accidentales, violación de la privacidad y otras acciones similares de acceso de terceros no permitidos.

**Autorización;** para garantizar que todos los acceso a datos cumplan con los niveles de autorización correspondiente para su utilización y divulgación.

**Seguimiento Automático de Auditoría**, la habilidad de mantener huellas de Auditoria de cuándo los mensajes son recibidos se está volviendo muy importante debido a la regulación y otros requerimientos, y debería ser independiente de cualquier acción hecha por el destinatario.

**Control de Envío**, una extensión del mantenimiento de huella de auditoría es el control de envío del correo hasta el punto que el usuario destino abra el correo, En otras palabras, el usuario origen debería poder recobrar un mensaje antes de que sea leído, controlar cuando la entrega se debe llevar a cabo o destruir el correo electrónico antes de su entrega.

Tomando en cuenta que el modelo propuesto puede ser aplicado en diferentes instituciones se contempla diferentes planes que pueden ser empleados dependiendo del caso en el que se aplique.

Para que el modelo de seguridad propuesto pueda contemplar todos los aspectos mencionados anteriormente se propone el siguiente flujograma el cual contempla dos planes, los mismos que son procesos a desarrollar de manera independiente según las condiciones que ofrece la institución.

.

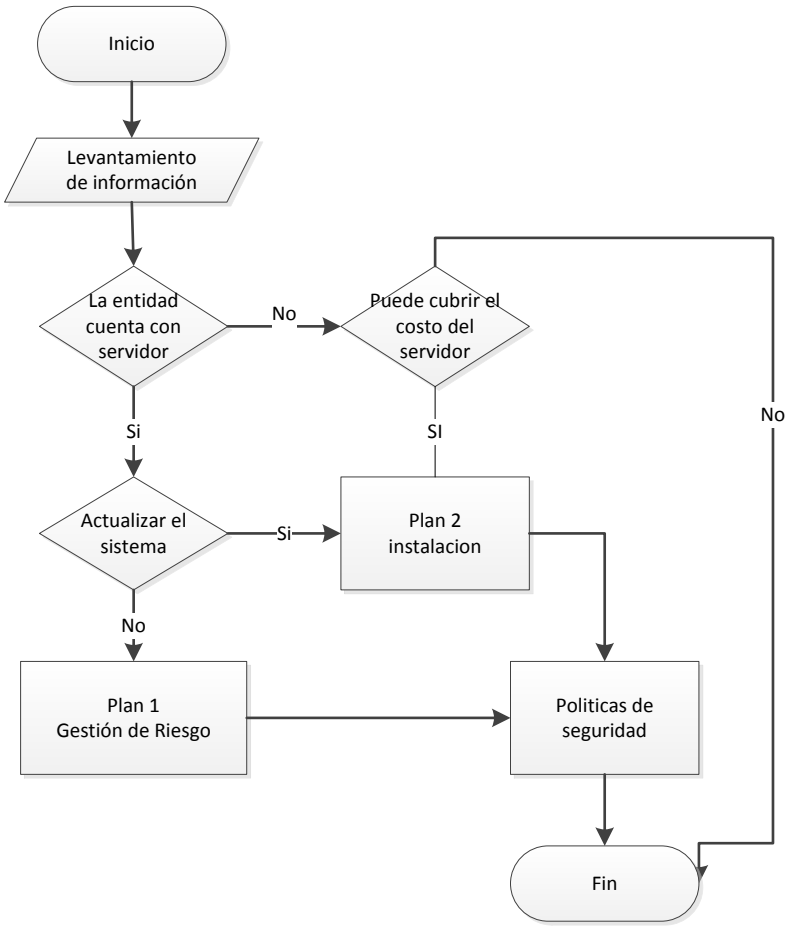



**Fig. 3.2. Flujograma del modelo de seguridad propuesto**
**Fuente: Propia**

### 3.2.1. PLAN 1. Gestión de Riesgos

Este plan se aplica a instituciones que cuenten con un servidor pero que no deseen la reinstalación de una nueva plataforma de correo electrónico, entonces se realiza el estudio de gestión de riesgos, el cual contempla de cuatro pasos importantes, para los cuales se tomaron en cuenta diferentes métodos de medición de riesgos como Delphi, que es un método que permitió la participación de expertos para la determinación y evaluación de los riesgos, así mismo, se tomó en cuenta también el método Magerit que permitió tener el conocimiento de cuanto de la información analizada esta en juego, este conocimiento coadyuva en la protección de la información.

Este proceso de gestión de riesgo cuenta con una serie de actividades que se deben llevar adelante para la identificación, análisis, planificación y control de riesgos, la mayoría de estas actividades se actualizan durante la ejecución del proyecto:

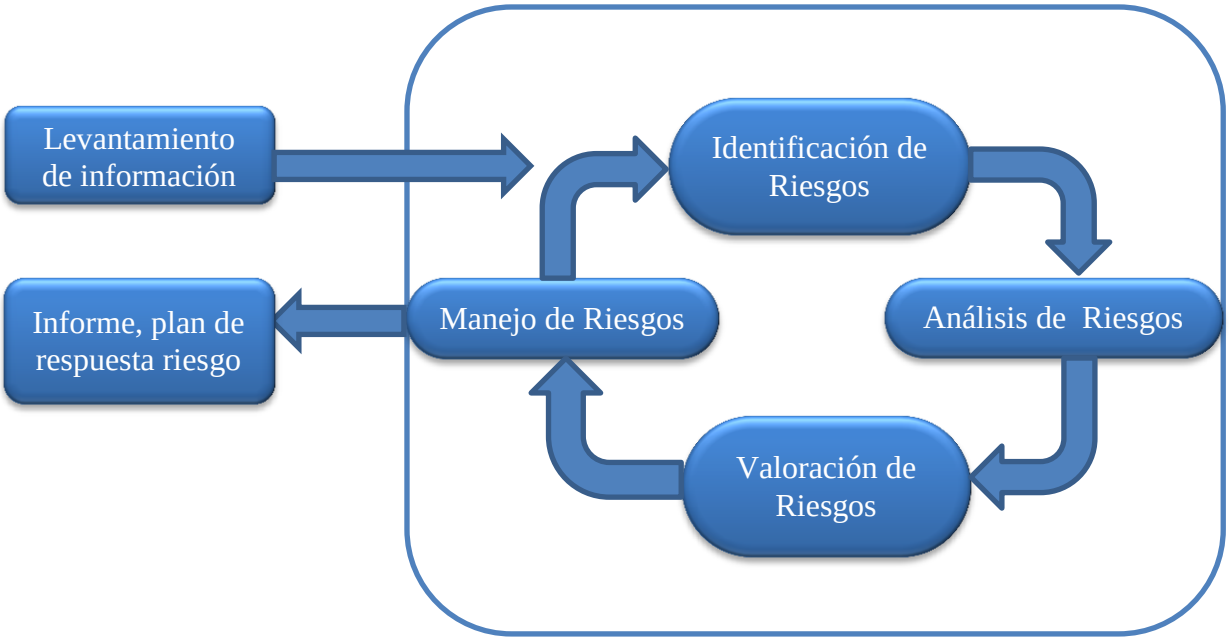



**Fig. 3.3. Etapas del proceso de gestión de riesgos**
**Fuente: Propia**

Como se puede observar estos procesos interactúan entre sí y también con los procesos de las demás áreas para evitar o minimizar los efectos negativos que puedan afectar los objetivos institucionales. Cada proceso puede implicar el esfuerzo de una o más personas o grupos de personas, dependiendo de las necesidades del proyecto. Cada actividad tiene lugar por lo menos una vez en cada proyecto y se realiza en una o más fases del proyecto.

#### 3.2.1.1. FASE 1. Levantamiento de información.

En esta fase se levanta información general de la institución en base a una serie de reuniones con el personal necesario, con el objetivo de tener el conocimiento acerca de la seguridad de correo electrónico con la que cuenta la institución y con esta información proporcionar recursos y tiempo suficientes para las actividades de gestión de riesgos, y para establecer una base para evaluar los riesgos. Esta fase debe completarse en las fases tempranas de la

planificación del proyecto, dado que es crucial para realizar con éxito los demás procesos, para esta tarea se toma en cuenta los siguientes puntos:

**1.- Descripción de la institución.-** En este punto se describirá de forma detallada a la institución en la cual se desea aplicar el modelo de seguridad propuesto, datos principales como:

- Objetivo de la institución
- Numero de trabajadores que posee
- Estructura orgánica de la institución

**2.- Descripción del entorno informático.** La institución cuenta con equipos informáticos que deben ser detallados de manera precisa para aplicar el modelo sobre datos concretos, en este punto se deben considerar condiciones como:

**a) Arquitectura informática**

- Red
- Equipos con los que se cuenta
- Características físicas del Servidor Linux
- Características físicas del Servidor Windows

**b) Software de sistemas y utilitarios**

- Sistema Operativo
- Lenguajes de programación
- Sistemas de aplicación
- Utilitarios

#### 3.2.1.2. FASE 2. Identificación de riesgos.

El objetivo de esta fase es identificar los riesgos potenciales que afectan a la seguridad del correo electrónico, para esto se desarrollo controles con el fin de minimizar y contrarrestar los riesgos encontrados, para evaluar de forma correcta este aspecto se debe tomar en cuenta los

siguientes puntos que también forman parte de los objetivos específicos señalados para la presente investigación.

**1.- Determinar la seguridad existente en el correo electrónico de la institución.** Para determinar la seguridad existente actualmente en la institución se aplicó una nueva entrevista (ver Anexo 7), en la cual se tomaron en cuenta algunos controles necesarios para asegurar la información contenida en los correos electrónicos, esta entrevista debe ser aplicada según la metodología Delphi solo a un grupo seleccionado de 3 o 4 personas expertas en el asunto, como la parte directiva, para la propuesta de este modelo de seguridad se tomo en cuenta los siguientes controles puntos críticos como:

- Seguridad de los equipos y control de accesos
- Claves de acceso,
- Cuentas de usuario,
- Políticas de seguridad
- Seguridad de la información

Esta información es necesaria para determinar si el correo de la entidad mantiene su información de forma confidencial, íntegra y disponible.

**2.- Identificar riesgos y problemas relativos a la seguridad de correo electrónico.** Este punto busca tener claramente identificados los riesgos potenciales de acuerdo a las respuestas obtenidas en la entrevista aplicada (Anexo 5), de acuerdo a este punto se debe establecer una agrupación o clasificación de riesgos existentes en la institución, para esto se realiza una matriz que propone el método Delphi para registrar una lluvia de ideas, la misma puede proporcionar todos los riesgos observados así como su impacto, para posteriormente poder clasificarlo.

Los puntos que se señalan a continuación son solo algunos ejemplos que pueden cambiar, dependiendo de las respuestas obtenidas en la entrevista aplicada (Anexo 5), y/o dependiendo de lo que los expertos consideren más importante para su institución:

| RIESGOS DE SEGURIDAD DE CORREO ELECTRONICO | |
|---|---|
| 1 | Las claves proporcionadas por el administrador de sistemas son sencillas y de fácil deducción |
| 2 | Falta de concientización sobre el uso del correo electrónico. |
| 3 | Ausencia de políticas de seguridad de correo electrónico. |

**Tabla 3.1. Lista de riesgos en la seguridad de correos electrónicos**
**Fuente: Elaboración propia**

**3.- Clasificar los riesgos referidos a la seguridad de la información.** Posteriormente se realiza la clasificación de los riesgos tomando en cuenta puntos de control (objeto), esto se deberá registrar en la tabla que se muestra, la misma que coadyuvara en la proposición de diferentes alternativas de control para poder minimizar los efectos de los riesgos.

**Clasificación de Riesgos Existentes**

| No. | OBJETOS | # RIESGO |
|---|---|---|
| 1 | **Usuarios y contraseñas.** | |
| | | |
| | | |
| 2 | **Servidor de correo.** | |
| | | |
| | | |
| 3 | **Cuentas de correo.** | |
| | | |
| | | |

**Tabla 3.2 Clasificación de riesgos Existentes**
**Fuente: elaboración propia**

Luego se deberá hacer un resumen de las amenazas detectadas para cada punto de control sugerido, tanto para la parte física como la lógica.

| No. | AMENAZAS | # AMENAZA |
|---|---|---|
| 1 | | 1 |
| 2 | | 2 |
| 3 | | 3 |

**Tabla 3.3 Resumen de Amenazas detectadas**
**Fuente: Elaboración propia**

### 3.2.1.3. FASE 3. Análisis de riesgos

El análisis de riesgos evalúa los riesgos identificados en la fase anterior para determinar el impacto y la probabilidad de que ocurran, estos hechos se ubican en una Matriz de Priorización.

**1.- Método matricial para el análisis de riesgos.** Este método consiste en utilizar una matriz que muestra gráficamente las amenazas a que está expuesto el correo electrónico y los objetos que intervienen para su uso. Los pasos que se tomaron en cuenta para el análisis de riesgo son:

- Identificar las amenazas (causas de riesgo) y los objetos del sistema.
- Categorizar los riesgos.

Luego de identificar las amenazas existentes en el servicio de correo electrónico, se determinan, los campos que formaran parte de la Matriz de Control de Riesgos (Amenazas y Objetos).

**Matriz de Control de Riesgo (Amenazas Y Objetos)**

| Amenazas / Objetos | | | | | |
|---|---|---|---|---|---|
| **Usuarios y Contraseñas.** | | | | | |
| **Servidor de correo.** | | | | | |
| **Cuentas de correo.** | | | | | |

**Tabla 3.4. Matriz de control de riesgo**
**Fuente: Elaboración Propia**

**2.- Categorización de riesgos**. Se categorizan las amenazas por niveles de riesgo, de mayor a menor, este hecho lo determina el grupo de expertos, que también realizan un proceso de votación, para determinar la valoración del riesgo (bajo, medio, alto), luego se procede a sumar primero los votos de las columnas y luego los votos de las filas; y finalmente para obtener la cifra total se suman los dos resultados antes obtenidos.

Los ítems que se muestran a continuación son ejemplos que pueden ser tomados en cuenta.

**Valoración de los Resultados (Amenazas)**

| | | | | | |
|---|---|---|---|---|---|
| Accesos no autorizados y/o mal uso de la información | Accesos no autorizados y/o mal uso de la información | $\sum_{n=1}^{n=5} Columnas$ $\sum_{n=1}^{n=5} filas =$ | Columnas+Filas | | |
| Perdidas monetarias | | Pérdidas monetarias | | | |
| Perdida de información y/o equipos | | | Perdida de información y/o equipos | | |
| Virus | | | | Virus | |
| Saturación del servidor | | | | | Saturación del servidor |

**Tabla 3.5. Valoración de los resultados**
**Fuente: Elaboración propia**

**Valoración del riesgo**

| Voto | Interpretación |
|---|---|
| I | Bajo |
| II | Medio |
| III | Alto |

**3.- Categorización de objetos.** Se procede de la misma forma como se categorizo las amenazas, es decir se categoriza los objetos según la sensibilidad utilizando como criterio de percepción el que tenga el grupo de trabajo al respeto.es decir, el grupo de votación decide cual de ellos es más sensible y según ese grado se va ordenando.

Posteriormente se procede a la votación del grupo de igual forma como se realizó con la categorización de las amenazas. Procediendo luego a sumar estos resultados, de la misma forma que se procedió con las amenazas.

**Valoración de los Resultados (Objetos)**

| | | | | | |
|---|---|---|---|---|---|
| Usuarios y contraseñas | Usuarios y contraseñas | | | | |
| Servidor de correo | | Servidor de correo | | | |
| Cuentas de correo | | | Cuentas de correo | | |
| Partes y/o piezas del computador | | | | Partes y/o piezas del computador | |
| Archivos | | | | | Archivos |

**Tabla 3.6. Valoracion de los resultados (objetos)**
**Fuente: Elaboracion propia**

### 3.2.1.4. FASE 4. Valoración de riesgos

Una vez realizada la categorización tanto de las amenazas como de los objetos se realiza una combinación de ambas categorías, elaborando una matriz de combinaciones, para esto se procede a colocar los totales en orden descendente (de izquierda a derecha y de arriba hacia abajo), en los dos casos.

Posteriormente se procede a realizar los cálculos correspondientes, multiplicando los valores de las amenazas y objetos para así poder obtener el nivel de riesgo / sensibilidad de las celdas. Al terminar este proceso si se presentan repeticiones, no deberán ser consideradas para determinar el nivel de riesgo de las celdas, luego se divide las celdas en regiones de mayor, mediano y menor riesgo.

Posteriormente se procede a dividir el número de celdas entre el número de expertos. La escala de valoración es Semicuantitativa ya que se asignan rangos numéricos a las características Alto, Medio y Bajo. Se toman las celdas con los productos más altos para determinarlas con

un nivel de riesgo alto, las siguientes celdas con los productos más bajos para determinarlas con un nivel de riesgo bajo; y las celdas restantes se las determina con un nivel de riesgo medio.

Riesgo Alto

Riesgo Medio

Riesgo Bajo

**Matriz de Resultados con Identificación de Niveles de Riesgo (Alto, Medio, Bajo)**

| Amenazas / Objetos | **Virus (5)** | **Pérdidas monetarias (4)** | **Accesos no autorizados (3)** | **Saturación de servidor (2)** | **Perdida de información y/o equipos (1)** |
|---|---|---|---|---|---|
| **Servido de correo. (5)** | | | | | |
| **Archivos. (4)** | | | | | |
| **Usuarios y contraseñas (3)** | | | | | |
| **Cuentas de correo (2)** | | | | | |
| **Partes y/o piezas del computador (1)** | | | | | |

**Tabla 3.7. Matriz de resultados con identificación de niveles de riesgo**
**Fuente: Elaboración propia**

### 3.2.1.5. FASE 5.- Manejo de Riesgos

Para finalizar, con los resultados obtenidos, apoyados en el método Delphi y en el modelo matricial Riesgo / Sensibilidad, se diseñan, analizan y documentan los controles a nivel: preventivo, detectivo y correctivo que sirve como referencia a la seguridad del correo electrónico.

**1.- Establecer controles y recomendaciones al gerente de la empresa para preservar la seguridad de correo electrónico,** después de realizar la evaluación a la seguridad del correo electrónico se debe informar al Directorio de la institución los resultados de la evaluación con sus respectivas recomendaciones, en este informe se incluirán los controles mínimos que deben existir.

A la Directiva se debe presentar una serie de controles preventivos, detectivos, correctivos y recomendaciones con la finalidad de minimizar los riesgos encontrados y así alcanzar los objetivos propuestos. Así mismo, se dará a conocer el orden en el cual los controles deben ser implementados, dependiendo exclusivamente de la institución considerarlos y ponerlos en práctica.

**Establecer controles (Método Magerit)**

| No. | Nombre | Nivel preventivo | Nivel detectivo | Nivel correctivo | Responsabilidad | Amenazas y/o objetos que cubren |
|---|---|---|---|---|---|---|
| 1 | | | | | | |
| 2 | | | | | | |
| 3 | | | | | | |
| 4 | | | | | | |
| 5 | | | | | | |

**Tabla 3.8. Establecer controles**
**Fuente: Elaboración Propia**

### 3.2.1.6. FASE 6. Informe, plan de respuesta de riesgo

Para resolver todas la vulnerabilidades encontradas durante el análisis de esta investigación se debe presentar a la Directiva los resultados del análisis de la evaluación de seguridad de correo electrónico de manera oportuna, el mismo debe ser presentado en un informe detallado mostrando los resultados de la evaluación, así la directiva de la institución podrá tomar las acciones necesarias para preservar la seguridad de su correo electrónico.

**1.- Resultados de la evaluación de riesgos.** Las debilidades encontradas, los efectos y una serie de recomendaciones y controles orientados a minimizar dichos riesgos detectados en el

uso de correo electrónico, deberán ser reflejados en un informe donde se debe detallar todos los aspectos que engloban la inseguridad de los correos electrónicos en la institución.

### 3.2.2. PLAN 2. Reinstalación de la plataforma web.

Sustitución del software gestor de correo electrónico (Sendmail) por un gestor de correo electrónico implementado en software libre**,** con opciones de seguridad más actualizadas, con la implementación de este plan ya se contaría con un servicio de correo electrónico seguro ya que en esta instalación se cuenta con la implementación de los servidores IMAP y en la parte del cliente para poder filtrar los correos con SPAM y realiza la transferencia segura de trafico, por tanto lo siguiente con lo que se debería contar con políticas de seguridad que se implementen en la institución para mantener la seguridad en los correos electrónicos.

Este plan de sustitución consiste en la migración del software del servicio de correo electrónico, existente actualmente, por una nueva plataforma que sea mas optima y se adapte mejor a los requerimientos de la institución. Se propone migrar a un software libre ya que el mismo permitirá adaptar los desarrollos de la institución a sus necesidades internas. Algunas de las razones para migrar a software libre son las siguientes:

- La copia es legal: es legal repartir software libre a otras personas. Usar un sistema libre evita en gran medida los problemas de la piratería. Si lo natural es compartir sus programas con otras personas.
- Abierto: Se puede usar el código de los programas y modificarlo.
- Colaborativo: El modelo de desarrollo de software libre es colaborativo y participativo.
- Ayuda: Existen innumerables grupos de usuarios que se ayudan entre sí a través de Internet.
- Auditable: El software libre se puede inspeccionar al disponer de su código fuente.
- Robusto frente a los virus: Existen muy pocos virus para GNU/Linux ya que el problema de los virus se debe al diseño del sistema operativo.
- Personalizable: Se puede personalizar toda la interfaz que el sistema presenta al usuario.

- Bajo costo: De estudios realizados para empresas e instituciones se han encontrado reducciones de hasta un 30% en TCO (Costo total de propiedad).
- Reutilización de equipos: GNU/Linux puede ejecutarse perfectamente en equipos que han sido desechados por las nuevas versiones de sistemas operativos propietarios.

Según la ultima ley 164 de telecomunicaciones se debe dar prioridad al software libre. Igualmente, en miras de una actualización tecnológica del servidor de correo en la institución y en búsqueda de factibilidades económicas operativas y técnicas, es necesario emigrar al uso de aplicaciones derivadas del Software Libre por su eficiencia, flexibilidad y seguridad para lograr este propósito.

Luego de un análisis comparativo entre varias aplicaciones en software libre como gestores de correo electrónico se selecciono la aplicación Squirrelmail. La opción planteada esta inclinada hacia uno de los sistemas GNU de servicio de correo electrónico más fuertes en el mercado. Se considera el SquirrelMail como la mejor alternativa, siendo este un Software Libre que cumple con las factibilidades económicas, técnicas y operativas que va de acuerdo con los requerimientos actuales de la Institución para añadir mejoras sustanciales en materia de seguridad al servicio de correo presente en la actualidad.

A continuación se presenta la descripción del SquirrelMail así como sus características y funcionalidades, ventajas y requerimientos necesarios para su instalación:

#### 3.2.2.1.Descripción del SquirrelMail

Es un programa de código abierto escrito en PHP4, que proporciona una interfaz para que los usuarios envíen, reciban y escriban correos electrónicos a través de un simple un navegador web. Todas las páginas de este programa tienen formato HTML 4.0 de tal forma que es compatible con la mayoría de los navegadores.

El SquirrelMail proporciona un sistema de correo electrónico totalmente funcional y de alto rendimiento que usa una completa gama de modernas tecnologías y protocolos que mejoran su

eficiencia, robustez, flexibilidad y seguridad. Asimismo, proporciona muchas facilidades de uso para los usuarios.

Debido a que este programa es un cliente de correo IMAP (Internet Message Access Protocol), los usuarios pueden tener varias carpetas de correos, también pueden filtrar sus mensajes a diferentes carpetas. Tienen filtros anti Spam, verificador de ortografía y un plugin para traducir mensajes de un idioma a otro. Por otra parte este software, soporta el despliegue de mensajes ordenados por tema o por fecha.

• SquirrelMail ofrece todas las posibilidades que se le puede pedir a un cliente de correo electrónico, incluyendo MIME (Multipurpose Internet Mail Extensión).

#### 3.2.2.2.Características o funcionalidades del SquirrelMail

• Gestión de carpetas.
• Internacionalización.
• Libro de direcciones personal y acceso a servicios de LDAP (Lighweight Directory Access Protocol).
• Búsqueda de direcciones
• Servicio de búsquedas en emails.
• Interfaz de usuario amigable y sencilla.
• Gestión de attachments.
• Configuración de las vistas de mensajes: numero de mensajes visibles en pantalla, campos visibles y orden.
• Comprobación de correos entrantes cada cierto intervalo de tiempo.

#### 3.2.2.3.Ventajas del SquirrelMail

- Independiza a los usuarios en el uso de las cuentas de correo electrónico.
- Combinar dominios virtuales con redirecciones a las cuentas del dominio principal.
- Autentica usuario a través de SASL (Simple Authentication and Security Layer), con métodos de texto plano o login.

- Realiza transferencia segura del tráfico mediante TLS (Transportation Layer Security).
- Permite accesar a los buzones de correo por IMAP sobre SSL (Secure Sockets Layer) y por webmail.
- Filtra correo electrónico en el servidor a través de Sieve.
- Filtra con antivirus y antispam.
- Utiliza como agente de transporte de correo el postfix, el cual no es un programa monolítico, sino una combinación de pequeños programas, cada uno de los cuales lleva a cabo una función especializada. El postfix además pretende ser rapido, flexible y seguro.
- A diferencia de muchas aplicaciones en PHP, Squirrelmail no requiere MYSQL (servidor de base de datos de Linux.), u otro tipo de base de datos.

### 3.2.2.4.Requerimientos del SquirrelMail para su instalación

1.- Sistema Operativo: Unix, Solaris, Linux o Windows.
El sistema operativo, recomendado para el caso en estudio es el LINUX, ya que este cae dentro de la categoría de software libre.

2.- Servidor IMAPrev1: entre los cuales estan w-imap, courier-imap,cyrus-imap, Comunigate, MS Exchange Server, MercuryMail 32.

Entre estos servidores se recomienda el Cyrus IMAP (Internet Message Access Protocolo) el cual es desarrollado y mantenido por el Andrew Systems Group de la Carnegie Mellon University.

A diferencia de otros servidores IMAP, Cyrus usa su propio método para almacenar el correo de los usuarios. Cada mensaje es almacenado en su propio fichero. El beneficio de usar ficheros separados es una mayor fiabilidad ya que sólo un mensaje se pierde en caso de error del sistema de ficheros. Los metadatos, tales como el estado de un mensaje (leído, etc.) se almacenan en una base de datos. Además, los mensajes son indexados para mejorar el rendimiento de Cyrus, especialmente con muchos usuarios y enormes cantidades de mensajes.

Otra característica muy importante es que no son necesarias cuentas locales de Linux para cada usuario. Todos los usuarios son autenticados por el servidor IMAP. Esto lo convierte en una magnífica solución cuando se tiene una gran cantidad de usuarios.

La administración es llevada a cabo mediante comandos especiales de IMAP (Internet Message Access Protocolo). Esto le permite usar tanto la interfaz de línea de comandos como los interfaces web.

3.- Servidor web (preferiblemente apache) y PHP4 instalado, el cual es un lenguaje de programación que se ejecuta en el servidor y se integra muy bien con el HTML y bases de datos MySQL.

El servidor Apache es un servidor HTTP de código abierto para plataformas Unix, GNU/Linux, Windows y otras, que implementa el protocolo HTTP/1.1 (RFC 2616) y la noción de sitio virtual. Apache presenta entre otras características mensajes de error altamente configurables, bases de datos de autenticación y negociado de contenido, lo cual proporciona seguridad.

4.- Perl (Practical Extraction and Report Language) instalado en el sistema, ya que para las configuraciones iniciales de correos es un buen asistente, sin embargo su instalación no es obligatoria ya que SquirrelMail funcionara sin problemas. Si no se tiene Perl se editara manualmente el archivo de configuración.

5.- OPENSSL instalado, por defecto, toda comunicación en Internet se hace sin ningún tipo de cifrado y sin una autenticación fiable. Esto significa que cualquiera con acceso físico a la línea de datos por la que viaja un paquete puede espiar dicha comunicación. Aún peor, es posible redirigir o alterar esa comunicación para que la información que se desea mandar se pierda y nadie se dé cuenta.

De cara a solventar estos problemas de seguridad, Netscape, introdujo el protocolo SSL (Secure Sockets Layer), que ha ido evolucionando en el protocolo estandarizado TLS (Transportation Layer Security). Ofrece tanto cifrado de la comunicación (frenando las

escuchas) como autenticación fuerte (asegurando que ambas partes de una comunicación son correctamente identificadas y que la comunicación no puede ser alterada). Postfix/TLS no implementa el protocolo TLS por sí mismo, sino que usa el paquete OpenSSL para esta tarea

6.- SIEVE instalado, es un lenguaje que puede usarse para crear filtros de correo electrónico en el momento de la entrega final del correo (en el lado del servidor). No está ligado a ningún sistema operativo o servidor de correo en particular.

Requiere el uso de la especificación de mensajes del RFC 822. El lenguaje es suficientemente potente para ser útil, pero está limitado de modo que permita la creación de sistemas de filtrado seguro en el lado del servidor. El objetivo es no permitir a los usuarios hacer nada más complejo (y peligroso) que escribir sencillos filtros de correo, además de facilitar editores basados en interfaces gráficas de usuario. Se supone que el uso del lenguaje tiene lugar al final de la entrega, cuando el mensaje se mueve a una cuenta accesible por el usuario. En aquellos sistemas donde el MTA (Mail Transport Agent) realiza la entrega final, es razonable clasificar cuando el MTA deposita el correo en la cuenta del usuario.

Sin embargo, los filtros Sieve pueden ser usados por varios "puntos finales de entrega" del sistema de correo, por el servidor SMTP, por un servidor IMAP o POP (Post Office Protocol), que archive una o más cuentas de usuario, o por un cliente de correo MUA (Mail User Agent) que actúe como gestor de las entregas (por ejemplo, un cliente POP o IMAP sin conexión).

7.- Con respecto al Hardware o plataforma física requerida para la instalación del SquirrelMail, las especificaciones con las que actualmente cuenta la institución para el servidor de correo, son suficientes.

### 3.2.3. POLITICAS DE SEGURIDAD

Las políticas de seguridad, son el pilar de cualquier institución, una buena Política de seguridad informática debe proporcionar la base a partir de la cual una institución diseñe su sistema de seguridad. Esto garantizará que la inversión que se realice sea adecuada, que los productos y soluciones adquiridos cumplan con los objetivos de la empresa y que éstos sean configurados

correctamente**.** A través de dichas políticas se informa a los usuarios de sus responsabilidades, con respecto a la institución.

Para finalizar el desarrollo del flujograma se propone un conjunto de políticas de seguridad en la que se incluyen los puntos que la norma ISO/27002 toma en cuenta como buenas practicas de seguridad, esta propuesta de políticas de seguridad pueden ser modificadas según los requerimientos de cada institución.

El Responsable de Seguridad Informática (si existe) junto al Responsable del Área Informática definen y documentan normas y procedimientos claros con respecto al uso del correo electrónico, que incluya al menos los siguientes aspectos:

**POLITICAS DE USO DE LAS CUENTAS DE CORREO ELECTRONICO**

a) Los Usuarios son completamente responsables de todas las actividades realizadas con sus cuentas de acceso y su buzón asociado a la Institución.

b) Es una falta grave facilitar y ofrecer su cuenta de correo electrónico (e-mail) a personas no autorizadas, su cuenta es personal e intransferible.

c) El correo electrónico es una herramienta para el intercambio de información entre personas, no es una herramienta de difusión de información.

d ) La violación de la seguridad de los sistemas de red, pueden incurrir en responsabilidades civiles y penales.

f) No es correcto enviar correo a personas que no desean recibirlo. Si la Institución recibe quejas, denuncias o reclamos por estas prácticas, se cancelara su cuenta.

f) Están completamente prohibidas las siguientes actividades:

1) Utilizar el Correo Electrónico para cualquier propósito comercial o financiero.

2) No se debe participar en la propagación de “cartas en cadenas”, ni en esquemas piramidales de índole político, religioso o temas similares.

3) Distribuir de forma masiva grandes cantidades de mensajes con contenidos inapropiados para la Institución.

g) Debido a que el espacio de las cuentas incide directamente sobre el espacio del servidor, se establece que :

1) Todos los Usuarios deben de revisar frecuentemente su Correo Electrónico para leer sus mensajes, de modo que los vayan borrando para no afectar el espacio de almacenamiento en e
2) Así mismo se agradece que vacíen frecuentemente las papeleras de su cuenta con el mismo fin de mantener el mayor espacio disponible en el servidor.

h) Toda información o contenido que sea transmitido por las cuentas de correo de este sitio, son responsabilidad únicamente del dueño de la cuenta, por lo que dichos contenidos no reflejan las preferencias o ideas de la institución.

i) Todos los correos pueden ser monitoreados.

j) El Servidor de Correos es depurado dos veces por año, en la primera quincena de Agosto y la primera quincena de Diciembre de cada año, por lo que se recomienda respaldar toda la información que considere importante para usted, antes de estas fechas.

**DATOS TÉCNICOS**

a) La dirección del correo electrónico de la institución esta compuesto de: nombre.apellidopaterno@dominio.extensiones, el password que se establece como valor inicial es su apellido paterno, se recomienda que lo cambie la primera vez que entre.

b) Tu nombre de Usuario es: apellidopaterno

c) Las cuentas de Correo Electrónico son manejadas por el administrador de red y por el director del departamento de Informática.

d) Se puede enviar a través de su cuenta todo tipo de datos adjuntos (attachments), siempre y cuando el tamaño total no exceda de 15MB.

e) Las cuentas permiten el acceso vía web, a través del sitio: nombre_institucion@dominio.extensiones.

f) Para pedir una clave de acceso (password) extraviada deberá ponerse en contacto con los administradores del sitio o el Administrador de Red.

**RESPONSABILIDADES Y GARANTÍAS**

a) La institución se compromete a prestar los Servicios Ofertados, no obstante, debido a la posibilidad de problemas propios de la red Internet y otras contingencias imprevisibles y de fuerza mayor, la institución garantiza al 99% la disponibilidad del servicio y por lo tanto no puede aceptar responsabilidades derivadas de pérdidas de datos.

b) Se realiza periódicamente copias de seguridad de los discos duros. En caso de que usted borre accidentalmente algún correo o carpeta de su cuenta de correo, la Institución no garantiza su reposición.

**SEGURIDAD**

a) Si por cualquier motivo sospecha que la seguridad de su cuenta se ve comprometida de cualquier forma debe notificarlo a la Dirección de Informática.

**CONFIDENCIALIDAD**

a) La institución se compromete a no ceder ni vender a terceros su información.

NOTA :

Se recomienda que cambie su password de acceso periódicamente, desde Internet, en el apartado de opciones. Se cuenta con un Manual de Usuario en línea, para Usuarios que revisan el correo desde Internet, en el apartado de Ayuda.

Luego de concluir con cualquiera de los planes se podrá contar con un sistema de correo electrónico seguro, confiable, integro y disponible para la entrega de documentos, archivos y mensajes electrónicos entre los usuarios de las instituciones que implementen el modelo propuesto, otorgando además, a través de los canales de Internet, garantía de privacidad y entrega sólo a los recipientes indicados, además de realizar un seguimiento de las entregas en todos los puntos durante el proceso. Gracias a este sistema, se tiene además del cumplimiento de los principios de confidencialidad, integridad, y disponibilidad.

# CAPITULO IV
# RESULTADOS DE LA APLICACIÓN DEL MODELO PROPUESTO

En este capitulo se puso en practica el modelo de seguridad de correos electrónicos institucionales diseñado en el capitulo anterior, para esto como se mencionó antes se tomo en cuenta a la institución, Fundación ACLO ya que la misma tiene muchas necesidades con respecto a seguridad en correos electrónicos, este hecho lleva a cumplir el último objetivo específico que lleva a demostrar los resultados de la investigación.

## 4.1. Aplicación del PLAN 1.

En el presente caso primero se obtuvo la muestra (Ver Anexo 2) a la cual se aplicó las herramientas de recolección de datos (Ver Anexos 3, 4), y tras el análisis (Ver Anexo 5,6) de esta información se pudo evidenciar que existe una urgente necesidad de tomar acciones con respecto a la seguridad de la información que se transmite mediante el correo electrónico. En este sentido y teniendo la información previa se sabe que la institución cuenta con un servidor y que por el momento no se desea cambiar ni actualizar la plataforma de software instalado en el, por esto, aplicando el modelo de seguridad se puede observar que es necesario aplicar el PLAN 1 propuesto en el modelo de seguridad, ya que es el que se adecua a las necesidades de la institución.

### 4.1.1. Fase 1. Levantamiento de información

**1.- Descripción de la Institución.**

**Diagnostico de la situación actual.**

En este punto se realizó el análisis general de la situación existente en la institución (Fundación ACLO) con el propósito de recolectar información referente a la seguridad en el servicio de correo electrónico y determinar la necesidad de diseñar un modelo de seguridad que garantice integridad, confiabilidad y disponibilidad del servicio.

La institución que se tomo en cuenta para coadyuvar con el diseño del Modelo de Seguridad de Correos Electrónicos es Fundación ACLO (Fundación Acción Cultural Loyola), esta institución tiene como principios:

- Ser una institución de inspiración cristiana liberadora, con voz propia, que contribuye a la construcción de una sociedad justa, incluyente, democrática, solidaria y un Estado Plurinacional con autonomías.
- Optar por los pueblos indígenas originarios campesinos y los sectores urbano-populares, como protagonistas de su propio cambio (emancipación) y el cambio estructural del país.
- Asumir la educación permanente e integral como elemento fundamental del cambio de la Sociedad y el Estado
- Practicar la igualdad y equidad de género y generacional en el marco de la interculturalidad.
- Valorar la diversidad cultural del país y promover relaciones interculturales respetuosas y horizontales.
- Promover y trabajar por un desarrollo sostenible en armonía con la naturaleza.
- Respetar las diferentes opciones religiosas, ideológicas y político partidarias.

La misión y visión de Fundación ACLO son:

**Visión.**

Buscar la construcción de una sociedad democrática, solidaria, justa, equitativa, intercultural y respetuosa del medio ambiente, con la participación activa de los pueblos indígenas originarios campesinos y sectores urbano-populares.

**Misión.**

Ser una institución de inspiración cristiana-ignaciana liberadora, con voz propia, que trabaja en el Sur de Bolivia en interacción con organizaciones de pueblos indígenas originarios campesinos y urbano-populares, para incidir con propuestas de políticas públicas que promuevan la construcción de una sociedad democrática, solidaria, justa, equitativa,

intercultural y respetuosa del medio ambiente, en el ámbito local, regional, departamental y nacional.

## Ámbito de Acción de Fundación ACLO

Fundación ACLO define como su ámbito de acción a los municipios, regiones y departamentos de Potosí, Tarija y Chuquisaca, que conforman el sur de Bolivia.

La estructura organizacional de Fundación ACLO esta conformado de la siguiente manera:

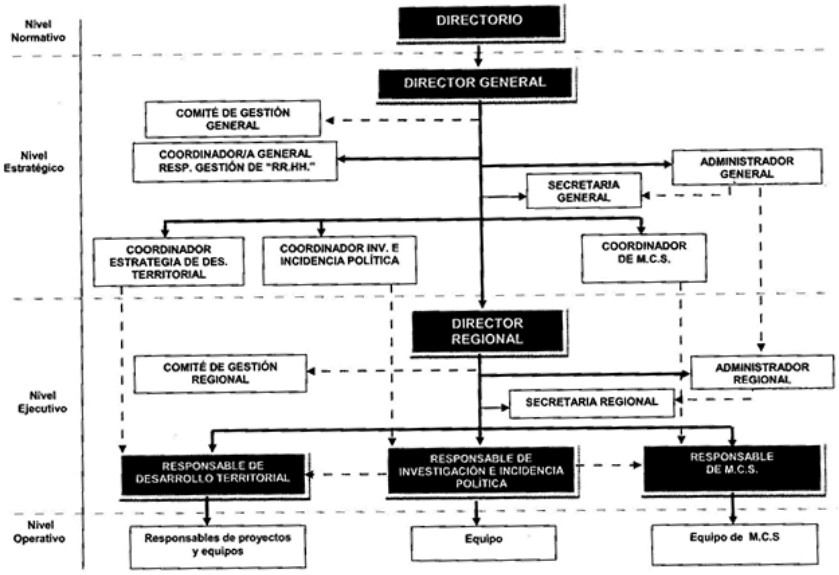



**Fig. 3.1. Estructura organizacional de Fundación ACLO**

**Fuente: Fundación ACLO**

Esta institución se encuentra ubicada en la ciudad de Potosí en Avenida Cívica # 765, el número total de personas que trabajan en esta entidad es 49, Fundación ACLO es una institución que trabaja con diversos tipos de proyectos como de: medio ambiente y cambio climático, economía y seguridad alimentaria, investigación e incidencia política, educación, comunicación, etc., debito a este tipo de trabajo su principal medio de comunicación tanto con las regionales como con las entidades financiadoras es el correo electrónico, ya que la información que se maneja es sumamente delicada puesto que la institución manda informes a los financiadores, hace contratos con otras entidades, etc., por esto la directiva considero importante la seguridad de la misma.

Actualmente la institución cuenta con un servicio de correo electrónico institucional que esta dado de la siguiente forma:

nombre_usuario@aclo.pts.bo

Según el cuestionario y la entrevista aplicados previamente se pudo observar que el servicio referido a correos electrónicos que ofrece la institución a sus empleados actualmente no funciona de forma adecuada ya que esta institución como muchas otras en la ciudad no cuentan con políticas de seguridad mínimas, es por esto que son victimas de muchas amenazas como: virus, correos electrónicos no deseados, spam, etc., que requieren ser atendidas.

Resumiendo la información obtenida se tiene:

- Objetivo de la institución: Trabaja con diferentes tipos de proyectos en el área rural del departamento de Potosí.
- Numero de trabajadores que posee: 49
- Estructura orgánica de la institución: Ver Fig. 4.1

**2.- Descripción del entorno informático.**

**a) Arquitectura informática**

- Red, la institución cuenta con una red que tiene un servidor con sistema operativo Windows 2000 server.
- Equipos con los que se cuenta, Fundación ACLO cuenta con 52 equipos de computación incluidos los servidores que están interconectadas entre si mediante una red, todas tienen acceso al servicio de correo electrónico. Es necesario señalar que la mayoría de los equipos cuentan con las mismas características de hardware exceptuando los equipos que se maneja en el sector de la radio ya que deben ser equipos con gran capacidad de disco duro y memoria ram para almacenar música y propagandas que se hacen en la misma radio y los servidores
- Servidor Linux, sus características son:
    - Pentium Core 2 Duo 3.0

- Disco duro 120 Gb
- 1 Gb. ram de memoria
- 1 unidad de CD rom
- 4 Puertos USB
- 2 tarjetas de red

- Servidor Windows
  - Pentium Core 2 Duo  3.0
  - Disco duro 120 Gb
  - 1 Gb. ram de memoria
  - 1 unidad de CD rom
  - 4 Puertos USB
  - 1 tarjetas de red

**b) Software de sistemas y utilitarios**

- Sistema Operativo: Actualmente el sistema operativo que se utiliza en la institución es Windows 7 en el servidor de Windows y en el otro servidor Linux
- Lenguajes de programación: la institución no utiliza lenguajes de programación
- Sistemas de aplicación: la institución cuenta son sistemas para llenar el POA y otras aplicaciones similares.
- Utilitarios: Los mas usados por la institución son: Microsoft Office, Internet Explorer, Programas para realizar jingles, reproducir música, etc.

### 4.1.2. Fase 2. Identificación de riesgos.

**1.- Determinar la seguridad existente en el correo electrónico de la institución**

**Entrevista para la evaluación de controles y seguridad del correo electrónico**

**Institución:** Fundación ACLO

**Departamento:** Sistemas

**Persona entrevistada:** Encargado de Sistemas

**Fecha:** 12 de diciembre de 2011

1. ¿Posee correo electrónico la organización?

   Si [X] No [ ]

2. ¿Cuál es el sistema de correo electrónico que usa?

   Internet Explorer.

3. ¿Cuál es su proveedor de Internet y por qué?

   Entel es el proveedor Internet, ya que se cuenta con internet las 24 horas al día, y los 7 días de la semana, es decir los 365 días al año.

**Seguridad de los equipos y control de accesos**

4. ¿Poseen seguro de equipos?

   Si [ ] No [X]

5. ¿Con cuantos equipos cuenta la institución para uso de correo electrónico y como están distribuidos los equipos?

   Tenemos un total de cuarenta equipos con acceso a correo electrónico y dos servidores de correo uno en Linux y el otro en Windows.

6. ¿Dónde se encuentran ubicados los servidores de correo?

   No se encuentran en un departamento específico pero si se encuentran en una oficina aislada.

7. ¿Quienes tienen acceso al departamento de sistemas?

   Cualquier persona de la institución ya que por el momento no se cuenta con un área específica dedicada a sistemas.

8. ¿Quiénes tienen acceso al servidor de correo?
   El administrador de sistemas.

**Claves de acceso**

9. ¿Poseen claves de acceso los servidores de correo y como están compuestas?
   Sí, están compuestas de por solo letras minúsculas las cuales son asignadas y cambiadas únicamente por el administrador de sistemas.

10. ¿Cada cuánto tiempo son cambiadas éstas claves?
    Las claves de acceso no son cambiadas desde el momento en que fueron creados.

11. ¿Las contraseñas de usuario asignadas inicialmente bajo qué parámetros fueron establecidas?
    El parámetro de asignación de claves es el Carnet de Identidad. Ejemplo:
    Usuario: jgarcia
    Contraseña: 4002060

12. ¿Cada cuánto tiempo los usuarios cambian sus contraseñas y bajo qué parámetros?
    No pueden cambiar sus contraseñas de forma personal, si se desea el cambio de una contraseña esto debe ser realizado por el administrador de sistemas. Y no se cuenta con un parámetro establecido de cómo deben estar compuestas las contraseñas. En algunos casos las contraseñas que asignan los usuarios son sus fechas de cumpleaños o la de sus hijos o sus nombres. Algunos de los usuarios conservan las contraseñas iniciales igual al nombre de usuario creado.

**Cuentas de usuario**

13. ¿Quién es el encargado de la creación y eliminación de cuentas de correo electrónico?
    El administrador de Sistemas es la persona encargada de crear o eliminar las cuentas a los usuarios y asignarles una contraseña.

14. ¿La solicitud de creación de una cuenta de usuario se la realiza de forma verbal o escrita?

    En el momento que una persona forma parte de la institución se le crea una cuenta de correo electrónico, que debe ser autorizado por el director general de la regional.

15. ¿Posee respaldo de las cuentas de usuario?

    Si [ ] No [X]

16. ¿Posee un registro o bitácora de control de las cuentas de usuario?

    Si [ ] No [X]

17. ¿Posee un registro actualizado de la creación y eliminación de cuentas de correo?

    Si [ ] No [X]

18. ¿Cuántas cuentas de usuario de se encuentran activas al momento?

    En este momento tenemos 56 cuentas de usuario.

19. De las cuentas de usuario antes mencionadas, ¿Todas pertenecen a trabajadores actuales?

    No, sólo 49 son de trabajadores actuales. Lo que sucede es que las otras cuentas son de trabajadores que fueron despedidos y no han sido eliminadas por falta de tiempo.

20. ¿Cuál es la capacidad de almacenamiento de cada cuenta de usuario?

    Su capacidad es ilimitada.

**Políticas de Seguridad**

21. ¿Se cuenta con un manual de políticas de seguridad de correo electrónico?

    Si [ ] No [X]

22. ¿Al momento de crear una cuenta de correo se le indica al usuario las responsabilidades que está adquiriendo así como el uso que le debe dar?

    No, se asume que ellos ya las conocen.

23. ¿Los usuarios utilizan el correo para actividades ajenas a la empresa?

    Algunos usuarios utilizan la cuenta de correo institucional para recibir y/o enviar mensajes personales. Esto depende de cada usuario.

**Seguridad de Información**

24. ¿Por cuánto tiempo puede permanecer abierto un correo sin ser usado?

    El correo puede quedar abierto por tiempo indefinido aunque no se esté usando.

25. ¿Qué posibilidad existe de que los equipos se infecten por algún mensaje que contenga virus?

    En el momento que llega un correo infectado, el servidor automáticamente lo intenta desinfectar, pero si no puede hacerlo borra el mensaje automáticamente y al destinatario le llega un mensaje indicándole de que un correo ha sido eliminado de su cuenta por contener virus.

26. ¿Cuál es la capacidad de archivos adjuntos que puede recibir y enviar en un mail?

    La capacidad de archivos adjuntos que pueden recibir es ilimitada mientras que la de enviar es de 2 GB.

27. ¿Posee Firma electrónica?

    Si [ ] No [X]

28. ¿Posee certificado digital?

    Si [ ] No [X]

29. ¿Se tiene conciencia de la seguridad que debe poseer el correo electrónico de la empresa?

    Si, pero todo cambio lleva tiempo.

30. Cuáles son los problemas mas comunes que se han presentado en el uso del correo electrónico?

Uno de los problemas que se ha presentado es que los usuarios utilizan su cuenta de correo electrónico para almacenar y enviar información personal, es decir ajena a la institución aumentando la posibilidad de que el servidor se sature o que los equipos se infecten de virus.

31. ¿A la presente fecha se ha realizado una auditoria informática en la institución?

A nivel informático nunca.

**2.- Identificar riesgos y problemas relativos a la seguridad de correo electrónico**

| **RIESGOS DE SEGURIDAD DEL CORREO ELECTRONICO** | |
|---|---|
| 1 | Las claves proporcionadas por el administrador de sistemas son sencillas ya que basta con prestarse el CI. de alguien para conocer su contraseña. |
| 2 | Falta de concientización sobre el uso del correo electrónico. |
| 3 | Ausencia de políticas de seguridad de correo electrónico. |
| 4 | Carencia de bitácora de control sobre las cuentas de usuario creadas, eliminadas y los perfiles. |
| 5 | No existe respaldo de información. |
| 6 | Accesos no autorizados a las cuentas de correo (divulgación y manipulación de información). |
| 7 | Ausencia de medidas de seguridad en los equipos. |
| 8 | Virus en los equipos. |
| 9 | Carencia de firma electrónica. |
| 10 | Fácil acceso al servidor de correo por personas no autorizadas. |
| 11 | Saturación de servidor por SPAMS adjuntos a los mensajes. |
| 12 | Falta de disponibilidad de información (perdida de información). |
| 13 | Suplantación de identidad. |
| 14 | Intercepción de mensajes. |

**3.- Clasificar los riesgos referidos a la seguridad de la información**

**Clasificación de riesgos existentes**

| No. | OBJETOS | # RIESGO |
|---|---|---|
| 1 | **Usuarios y contraseñas.** | |
| | Las claves proporcionadas son sencillas y de fácil deducción. | 1 |
| | Falta de concientización de los usuarios acerca del uso del correo electrónico de la organización. | 2 |
| 2 | **Servidor de correo.** | |
| | Las cuentas de usuario poseen capacidad ilimitada de almacenamiento provocando saturación del servidor. | 11 |
| | El servidor de correo se encuentra en un lugar de fácil acceso a las personas. (sabotajes, daños, errores) | 10 |
| 3 | **Cuentas de correo.** | |
| | Las cuentas de los usuarios de correo electrónico pueden quedar abiertas durante tiempo indefinido aunque no se las esté usando. | 13 |
| | Accesos no autorizados. | 6 |
| | No hay respaldo de las cuentas de usuario (backups). | 5-12 |
| | Inexistencia de un manual de política de seguridad de correo electrónico. | 3 |
| | Ausencia de bitácora de control de las cuentas de usuario. | 4 |
| 4 | **Partes y/o piezas del computador.** | |
| | Ausencia de medidas de seguridad en los equipos. | 7 |
| 5 | **Archivos** | |
| | Recibir mensajes infectados. | 8 |
| | Carencia de firma electrónica. | 9 - 14 |

Las amenazas detectadas y que afectan tanto a la parte física como a la parte lógica son:

| No. | AMENAZAS | # AMENAZA |
|---|---|---|
| 1 | Accesos no autorizados a las cuentas de correo y/o uso inadecuado del correo y de la información. | 1 |
| 2 | Pérdidas monetarias. | 2 |
| 3 | Pérdida de información y/o equipos. | 3 |
| 4 | Infectar las máquinas con virus. | 4 |
| 5 | Saturación del servidor. | 5 |

### 4.1.3. Fase 3. Análisis de riesgo.

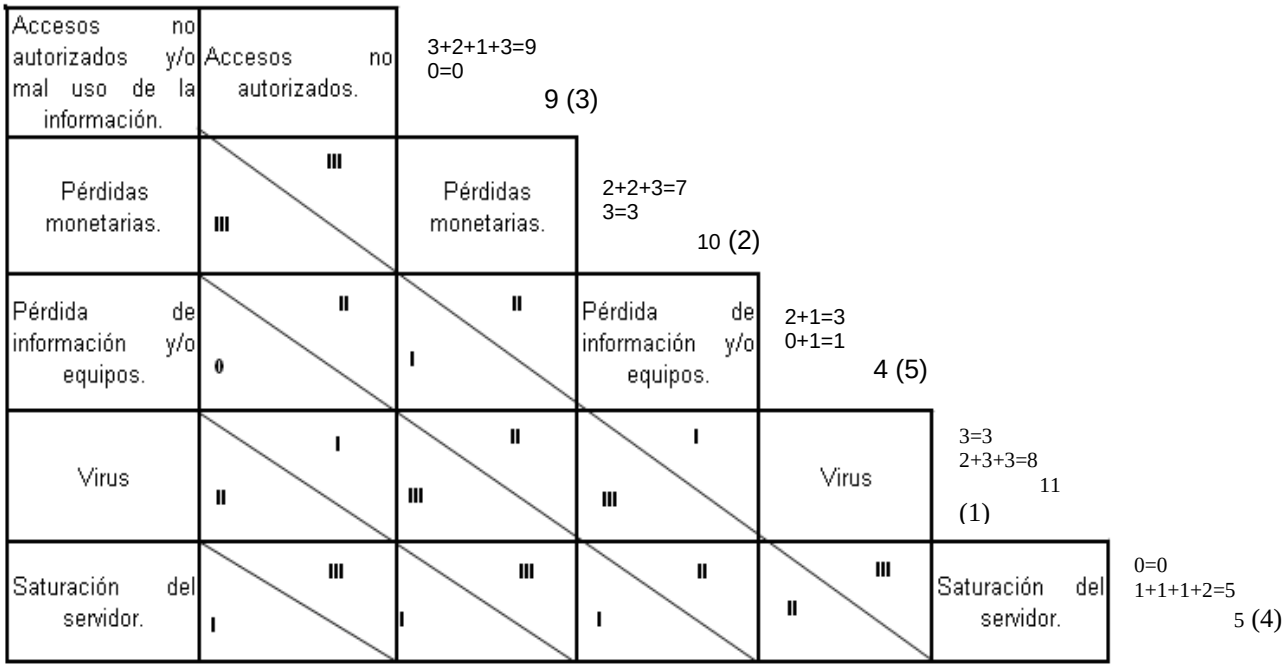
## 1.- Método matricial para el análisis de riesgos

**Matriz de Control de Riesgo (Amenazas y Objetos)**

| Amenazas / Objetos | Accesos no autorizados y/o mal uso de la información | Pérdidas monetarias | Pérdida de información y/o equipos | Virus | Saturación del servidor |
|---|---|---|---|---|---|
| **Usuarios y Contraseñas.** | | | | | |
| **Servidor de correo.** | | | | | |
| **Cuentas de correo.** | | | | | |
| **Partes y/o piezas del computador.** | | | | | |
| **Archivos** | | | | | |

## 2.- Categorización de riesgos

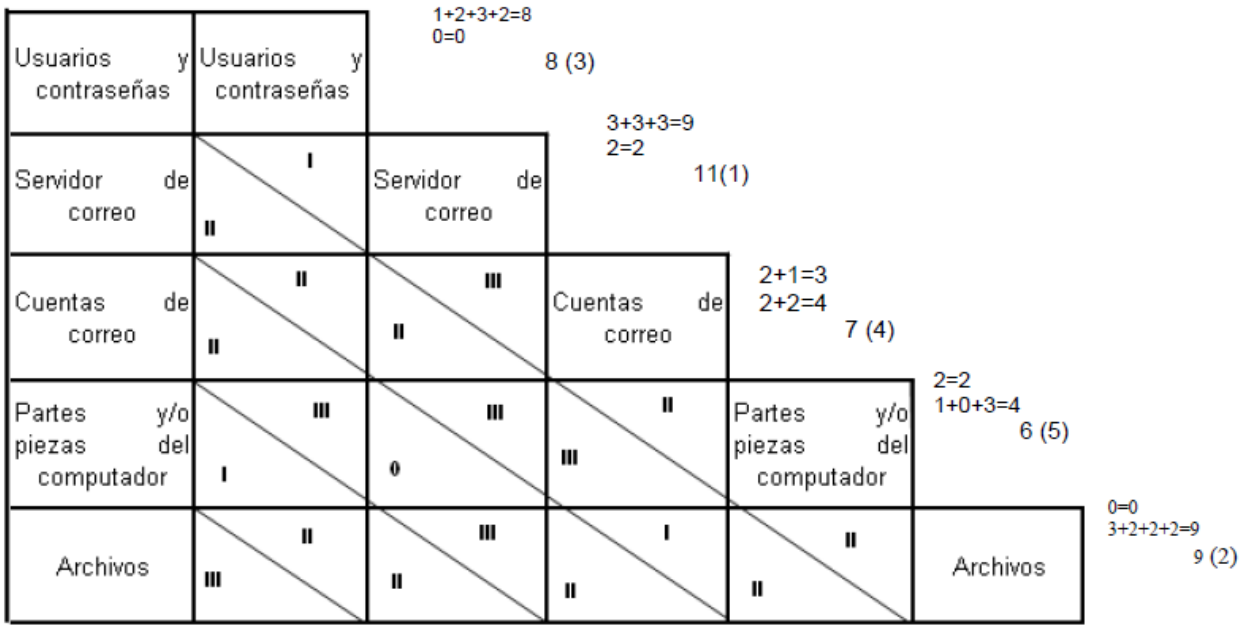
**Suma De Los Resultados (Amenazas)**




**Valoración del riesgo**

| Voto | Interpretación |
|---|---|
| 0 | Ninguno |
| I | Bajo |
| II | Medio |
| III | Alto |

### 3.- Categorizacion de objetos




### 4.1.4. Fase 4. Valoración de riesgos.

**Matriz de resultados de Identificación de Niveles de Riesgo (Alto, Medio, Bajo)**

| Amenaza / Objetos | Virus (11) | | Pérdidas monetarias (10) | | Accesos no autorizados (9) | | Saturación de servidor (5) | | Perdida de información y/o equipos (4) | |
|---|---|---|---|---|---|---|---|---|---|---|
| **Servidor de correo (11)** | **121** | **1** | **110** | **2** | **99** | **3** | **55** | **14** | **44** | **17** |
| **Archivos (9)** | **99** | **3** | **90** | **4** | **81** | **6** | **45** | **16** | **36** | **19** |
| **Usuarios y contraseñas (8)** | **88** | **5** | **80** | **7** | **72** | **9** | **40** | **18** | **32** | **21** |
| **Cuentas de correo (7)** | **77** | **8** | **70** | **10** | **63** | **12** | **35** | **20** | **28** | **23** |
| **Partes y/o piezas del computador (6)** | **66** | **11** | **60** | **13** | **54** | **15** | **30** | **22** | **24** | **24** |

### 4.1.5. Fase 5. Manejo de Riesgos.

### 1.- Establecer controles y recomendaciones al gerente de la empresa para preservar la seguridad de correo electrónico

**Controles Establecidos (Método Magerit)**

| No. | Nombre | Nivel preventivo | Nivel detectivo | Nivel correctivo | Responsabilidad | Amenazas y/o objetos que cubren |
|---|---|---|---|---|---|---|
| 1 | Claves de acceso | Asignar claves con un mínimo de 8 caracteres combinados entre números y letras mayúsculas y minúsculas | Revisar si las contraseñas establecidas por los usuarios cumplen con el mínimo de caracteres establecido | informar a los usuarios que todas las contraseñas que no cumplan con los requerimientos deben ser cambiados | Administrador de sistemas | Amenazas: Acceso no autorizado, violación a la privacidad. Objetos: Usuarios y contraseñas, cuentas de correo, texto, imágenes y archivo |
| 2 | Administración de contraseñas | Informar a los usuarios que las contraseñas proporcionadas por el administrador de sistemas debe ser cambiadas | Revisar si las contraseñas asignadas por el administrador de sistemas ha sido cambiado | Configurar las cuentas de correo para que el usuario pueda cambiar su contraseña | Administrador de sistemas | Amenazas: Acceso no autorizado, violación a la privacidad. Objetos: Usuarios y contraseñas, cuentas de correo, texto, imágenes y archivo |
| 3 | Seguridad en la entidad | Restringir la entrada a la oficina donde se encuentra el servidor, manteniendo la puerta cerrada y colocando un aviso de área restringida | Mediante monitoreo y observación se puede detectar e identificar el ingreso de personal no autorizado a la oficina de sistemas | Comunicar a todos los empleados de la institución acerca de la restricción del acceso a la oficina de sistemas | Directorio y administrador de sistemas | Amenazas: Acceso no autorizado, robo o perdida de información, violación a la privacidad, fraude y/o sabotaje. Objetos: Servidor de correo, partes y/o piezas del computador |
| 4 | Respaldo de las cuentas de usuario | Se necesita respaldar las cuentas de usuarios periódicamente | Revisar si se han respaldado las cuentas de correo para así evitar futuros inconvenientes | Respaldar las cuentas de correo con una frecuencia semanal o aun mejor diaria | Administrador de sistemas | Amenazas: Robo y/o perdida, Objeto: Cuentas de correo, texto, imágenes y archivos. |
| 5 | Tiempo de espera | Comunicar a los usuarios que las cuentas de correo se cierran automáticamente después de 10 minutos de presentar inactividad | configurar el cierre de sesión | Corregir errores de configuración | Administrador de sistemas | Amenazas: Acceso no autorizado, robo o perdida de información, violación a la privacidad, fraude y/o sabotaje. Objetos: usuarios y/o contraseñas, cuentas de correo, texto, imágenes y archivos |

| | | | | | | |
|---|---|---|---|---|---|---|
| 6 | Evaluar uso del correo electrónico | Informar a los usuarios que el correo institucional es para fines laborales, estableciendo políticas de uso del mismo | Tener identificados quienes son los usuarios que no cumplen con la política establecida | Capacitar a los usuarios sobre el uso optimo que deben darle a su cuenta de correo, recordando que su uso es exclusivamente laboral | Directorio y administrador de sistemas | Amenazas: correo no deseados y/o infectados, Objetos: servidor de correo, texto, imágenes y archivos |

### 4.1.6. Fase 6. Informe, plan de respuesta de riesgo.

**1.- Resultados de la evaluación de riesgos**

## INFORME DE GESTION DE RIESGOS

El modelo de seguridad de correo electrónico fue aplicado a Fundación ACLO institución que requiere dar seguridad al servicio de correo electrónico que ofrece a sus dependientes, para esto resta presentar el informe de acuerdo a los datos obtenidos de la aplicación del modelo de seguridad de correo electrónico propuesto.

## INFORME

**A: MSC. Lic. Vincent Nicolas**
**Director General Fundación ACLO**

Después de haber aplicado el modelo de seguridad de correo electrónico en este documento se presenta el resultado detallado por unidad de análisis, es decir se realiza la evaluación según los tipos de control que se plantearon durante la implementación del modelo.

**Evaluación de controles y seguridad del correo electrónico.**

Luego de haber aplicado el cuestionario con expertos para identificar los puntos más comunes de riesgo, en la que se basaron los datos analizados, se presentan los siguientes resultados

*1. Correo electrónico.*

1. **Manual de políticas de seguridad de correo electrónico, no existe actualmente en la institución.**

**Situación Actual:**

Durante la aplicación del modelo se pudo observar que: no se cuenta con una política de seguridad de correo electrónico.

**Efectos:**

- Existe mal uso de las cuentas de correo.
- Falta de seguridad por parte de los nuevos usuarios al tratar de utilizar sus cuentas de correo electrónico.
- Se ignoren las responsabilidades que se están adquiriendo.

**Recomendaciones:**

Desarrollar a la brevedad posible políticas de seguridad de correo electrónico en la que se describa las responsabilidades que adquiere el usuario al momento de la creación de su cuenta. De igual manera se debe señalar que el correo de la empresa sólo será usado para fines laborales.

**Indicadores:**

Proporción de usuarios que conocen la política de seguridad de correo electrónico de la institución. Las personas que tienen algún conocimiento de políticas de seguridad en la institución son pocas por esto es indispensable la aplicación de normas y políticas de seguridad.

2. **Las cuentas de los usuarios de correo pueden quedar abiertas y activas durante tiempo indefinido aunque no se las esté usando.**

Las cuentas de correo electrónico no deben mantenerse abiertas si no se las esta usando ya que esta puede ser una invitación a algún curioso que pueda dañar su cuenta.

**Efectos:**

Este tipo de errores puede causar:

- Acceso a información confidencial.
- Divulgación de información confidencial.
- Personas no autorizadas hagan uso de una cuenta.
- Se reste privacidad a los mensajes.
- Manipulación de información.

**Recomendación:**

El Gerente de Sistemas debe configurar de manera general las cuentas de todos los usuarios para que después de cinco minutos de inactividad se cierre la sesión. Se debe tener en cuenta que el tiempo de espera no debe ser muy extenso (mínimo 5 minutos y máximo 10).

Las cuentas de trabajadores que no desempeñan sus funciones en la organización deben ser dadas de baja.

**3. Acceso no autorizado a las cuentas de correo**

**Situación actual**

Mediante cuestionario y observación se pudo constatar que la empresa no cuenta con medidas de seguridad para evitar el acceso de personas no autorizadas a las cuentas de correo.

**Efecto:**

- Divulgación no autorizada de información.
- Pérdidas monetarias en el negocio.
- Acceso a información reservada.
- Adulteración de información.
- Falta de privacidad.

**Recomendación:**

Capacitar a los usuarios sobre las responsabilidades y precauciones con que debe usar sus cuentas de correo.

**4. No hay respaldo de las cuentas de usuario (Backups)**

**Situación actual:**

Mediante confirmación, cuestionario y observación (Anexo 4) pudimos constatar que la empresa no cuenta con respaldo de las cuentas de usuario.

**Efecto:**

- Se pierda el usuario.
- Se pierda el Password.
- Se pierdan los mail guardados del usuario (pérdida de información)
- Pérdida de tiempo.
- En caso de fallas no se puede recuperar estos datos.

**Recomendaciones:**

Respaldar las cuenta de usuario semanalmente para así evitar pérdida de información.

Hacer backups de las cuentas.

**5. No existe bitácora de control de las cuentas de usuario.**

**Situación Actual:**

Producto del análisis se pudo constatar que el administrador de Sistemas no posee un documento donde se registre en forma ordenada y actualizada todas las cuentas de usuario creadas con sus características.

**Efecto:**

Esta situación puede originar que:

- No se tenga un control de las cuenta de usuario creadas.

- No se posea las características principales de cada cuenta de usuario.

**Recomendación:**

Elaborar una bitácora de control donde se registre la creación y eliminación de las cuentas de usuario así como una descripción detallada de todas las características del usuario de la cuenta.

***2. Usuarios y contraseñas***

**6. Se pudo observar que las claves proporcionadas por el Jefe de Sistemas son sencillas y de fácil deducción.**

**Situación Actual:**

Producto de la revisión conocimos que las contraseñas proporcionadas por el Jefe de Sistemas a los usuarios son sencillas y por ende fáciles de deducir.

**Efecto:**

Este tipo de situaciones puede causar:

- Se reste confidencialidad y seguridad al correo ya que las claves son fáciles de deducir y por ende de copiar.
- Se produzca accesos no autorizados a la cuenta de un usuario produciendo una violación a la privacidad.

**Recomendaciones:**

Es aconsejable utilizar claves con un mínimo de ocho caracteres con una combinación de letras y números. Para esto es recomendable implementar un software que cumpla con los parámetros antes establecidos. Así mismo no es adecuado utilizar paswords de: nombres, fechas, entre otros que son de fácil deducción.

De igual manera se debe recordar al usuario cambiar sus contraseñas cada tres meses como máximo y como mínimo de forma mensual. Debemos tener en mente que toda protección que tomemos para salvaguardar la seguridad de nuestro correo no esta de más.

El Jefe de Sistemas deberá revisar si las contraseñas establecidas cumplen con los parámetros señalados así mismo debe mantener un registro de las contraseñas previas del usuario; por ejemplo, de los 12 meses anteriores, y evitar la reutilización de las mismas.

Finalmente informar a los usuarios que todas las contraseñas que no cumplan con los parámetros establecidos deben ser cambiadas inmediatamente.

**7. Falta de concientización de los usuarios acerca del uso del correo electrónico de la institución.**

**Situación Actual:**
Durante el análisis conocimos que los usuarios hacen uso de su cuenta de correo no solamente para fines laborales sino también personales.

**Efecto:**
Esta situación permite que:

- Al utilizar el correo de la organización para otros fines aumenta las probabilidades de que las máquinas se infecten de virus.
- Posible saturación del servidor de correo.
- Elevar costos de la empresa.
- Baja productividad.

**Recomendaciones:**
Al momento que el Administrador de Sistemas crea una nueva cuenta de correo estará en la obligación de indicarle a cada usuario las responsabilidades y obligaciones que adquiere en su uso así como de enseñarles a gestionar con efectividad sus correos electrónicos garantizando que guarden y borren mensajes cuando sea necesario. De igual manera se le debe indicar a cada usuario que dicha cuenta ha sido creada exclusivamente para fines laborales. Establecer una política de correo en la cual se indique:

1. No se debe utilizar la cuenta de correo de la empresa para recibir horóscopo, chistes, entre otros ya que algunos de estos mensajes podrían tener virus.

2. No abrir mensajes de personas desconocidas o con asuntos inusuales como por ejemplo: “Eres millonario”.
3. Las claves proporcionadas por el administrador de sistemas deben ser personalizadas por los usuarios.

El administrador de sistemas debe tener identificado quienes son los usuarios que no están cumpliendo con la política establecida.

**8. Las cuentas de usuario poseen capacidad ilimitada de almacenamiento.**

**Situación Actual:**

Mediante entrevista realizada al administrador de sistemas se pudo conocer que las cuentas de usuario poseen capacidad ilimitada de almacenamiento.

**Efecto:**

Esta situación puede afectar en:

- Saturación del servidor de correo.
- Falta de disponibilidad del servicio.

**Recomendaciones:**

El Administrador de Sistemas debe asignar capacidad de almacenamiento a cada cuenta de usuario de acuerdo a las necesidades del cargo y/o función que desempeñe en la institución o también puede asignarlas de manera general, es decir, a todos los usuarios asignarles por igual una cantidad mínima de almacenamiento.

**9. El servidor de correo se encuentra en un lugar de fácil acceso a las personas. (Sabotajes, daños, errores)**

**Situación Actual:**

Durante la revisión se pudo observar que el lugar donde se encuentra el servidor de Correo Electrónico es de fácil acceso a las personas, cualquiera que desee puede tener contacto a poca distancia.

**Efectos:**

Esta situación implica que:

- Que cualquier persona que posea conocimientos superiores de informática acceda al Server para cometer un sabotaje, una travesura, entre otras y por ende la pérdida total o parcial de la información del servidor.
- El servidor se encuentra vulnerable a fallas de seguridad físicas como un daño parcial o total del equipo ya sea voluntaria o involuntariamente, robo, destrucción, entre otros.
- Puede ocurrir que alguien por descuido o imprudencia tropiece con el equipo provocando daños.

**Recomendaciones:**

Resguardar en un lugar seguro y restringido el servidor de tal manera que la probabilidad de que exista un incidente contra el computador sea mínima al igual que la probabilidad de que exista manipulación del equipo por cualquier persona no autorizada. Esto ayudará a resguardar las aplicaciones en términos de confidencialidad, integridad y disponibilidad.

Se deben colocar letreros prohibiendo el ingreso al área de sistemas de parte de personal no autorizado y mantener la puerta siempre cerrada.

Así también mediante el monitoreo se puede detectar e identificar el ingreso de personal no autorizado a dicha área.

Dar a conocer a todos los empleados de Fundación ACLO sobre la restricción del acceso a dicha oficina.

***Partes y/o piezas del computador***

**10. Ausencia de medidas de seguridad en los equipos.**

**Situación actual:**

Mediante cuestionario y observación se constató que los equipos servidores (Linux y Windows) carecen de seguridad física.

**Efecto:**

- Pérdida parcial o total de los equipos, sus partes y/o piezas.
- Perdida de dinero.
- Perdida de información

**Recomendación:**

Establecer un área restringida para ubicar los servidores.

Prohibir el ingreso de personas no autorizadas al departamento de sistemas.

Dar mantenimiento a la red y a los equipos cada vez que se crea necesario.

***Archivos (imágenes y texto)***

**11. Recibir mensajes infectados.**

**Situación actual:**

Mediante reuniones y entrevistas realizadas se pudo comprobar que a las cuentas de correo llegan mensajes con imágenes y texto infectados por algún virus.

**Efecto:**

- Pérdida de información.
- Dañar las máquinas.
- Infectar toda la red.
- Pérdidas económicas para el negocio.

**Recomendación**

Implantar filtros de spam para controlar la cantidad de mensajes no deseados que reciben los usuarios.

Levantar un firewall para de esta forma proteger la red contra intentos de accesos no autorizados.

Advertir a los usuarios de nunca abrir archivos enviados por desconocidos ni de extensiones desconocidas.

Analizar los archivos adjuntos con el antivirus antes de abrirlos.

El jefe de sistemas debe actualizar el antivirus y realizar monitoreos a la red periódicamente.

Al momento de considerar un analizador de virus para servidor de correo se deben tener en cuenta ciertos puntos como: poder analizar archivos comprimidos, actualización automática, simpleza en la administración.

**12. Carencia de una firma electrónica.**

**Situación Actual:**

Durante la revisión se pudo observar que la empresa no posee firma digital, aunque no descartan la idea de implantarla con el tiempo.

**Efecto:**

Estas situaciones permiten que:

- Personas con los conocimientos necesarios y no autorizadas accedan a la información de la empresa y hagan uso de ella.
- Violación a la privacidad de los mensajes.
- Violación a la integridad de los mensajes.
- Falta de confidencialidad de información.
- Mal uso de información.
- Divulgación no autorizada de información.

**Recomendaciones:**

La pronta implantación de una firma digital que permita al receptor verificar la integridad de los mensajes. Posteriormente obtener un certificado digital para garantizar la autenticidad de la firma digital.

- Desconocimiento de la directiva acerca de la seguridad de correo electrónico que debe poseer la organización.

- Interés del director por alcanzar los más óptimos niveles de seguridad, garantizando la integridad de la información que viaja por la red.

- Preocupación de parte de los directivos de que la información que se transmite sea obtenida por la competencia.

- Deseo de la Directiva de evaluar la seguridad de la información que viaja por la red para así incrementar o fortalecer dichos niveles de seguridad.

Estos justificativos son detallados a continuación:

**Desconocimiento de la Directiva acerca de la seguridad de correo electrónico que debe poseer la organización.**

La Directiva desconoce los niveles de seguridad que existen y deben implementarse en la organización dentro del correo electrónico.

Para la Directiva de Fundación ACLO esto constituye un justificativo para la realización del trabajo de investigación.

**Interés del Director por alcanzar los más óptimos niveles de seguridad garantizando la integridad de la información que viaja por la red**

Existe preocupación e interés por parte de la Alta Directiva por salvaguardar la integridad de la información que viaja por la red pues ésta es muy sensible y confidencial. Partiendo de que los riesgos no son eliminados sino más bien controlados.

Los controles y las seguridades cada vez se vuelven más indispensables para salvaguardar la información del correo de ACLO.

**Preocupación de parte de los directivos de que la información que se transmite sea obtenida por la competencia**

Debido a que la empresa intercambia información respecto a innovaciones y productos especiales con filiales de otros países es necesario preservar la privacidad de la misma. Las tablas de valores de tasas de descuento, el costo de la mercadería, el precio de venta al por mayor, entre otros; constituye la información que se debe preservar.

**Deseo de los directivos de evaluar la seguridad de su información que viaja por la red para así incrementar o fortalecer dichos niveles**

Debido a los riesgos que puede sufrir la información que es transmitida por correo electrónico se ve la necesidad de evaluar la seguridad de información permitiendo obtener los controles mínimos a implementar en materia de seguridad. La información que viaja por correo electrónico es de vital importancia para Fundación ACLO de allí la necesidad de fortalecer los esquemas de seguridad.

En el informe que se presenta se pretende englobar los puntos mas vulnerables de la institución con respecto al correo electrónico, para esto se tomo la situación actual de cada punto, los efectos que la causan y las recomendaciones a ser tomadas en cuenta por toda directiva de la institución.

## 4.2. Viabilidad del modelo propuesto evaluado mediante criterio de expertos.

Para validar la presente investigación “Modelo de seguridad para identificar amenazas de los correos electrónicos” fue necesaria la determinación del grado de viabilidad del modelo a través del criterio de especialistas, mismos que fueron seleccionados por su experiencia profesional y sobre todo por su conocimiento acerca del tema que se presenta en esta investigación. Fueron seleccionados 5 especialistas tomando en cuenta el método estadístico no probabilista “muestreo de selección experta”.

### 4.2.1. Procesamiento de las encuestas a través del método Delphi.

La valoración se realizo en función de especialistas, para lo cual se utilizaron instrumentos de recolección de datos como el cuestionario mostrado en Anexo 8, posteriormente se aplicó la consulta de opiniones al mismo grupo, con el fin de valorar su coeficiente de competencia y someter a su criterio el modelo propuesto y de esta forma obtener su aprobación o desaprobación.

### 4.2.2. Análisis de los resultados obtenidos en la aplicación del método Delphi.

Con la aplicación del método de expertos Delphi se pudo realizar varias correcciones necesarias para que la presente investigación quede apta para su presentación, en los resultados obtenidos en el Anexo 9 se puede evidenciar que los capítulos II y III fueron calificados como bastante adecuados y el capítulo IV fue calificado como adecuado, por tanto se tiene la aprobación de los especialistas y se considera que el modelo de seguridad propuesto elaborado esta en función de satisfacer las necesidades de las instituciones que apliquen el modelo propuesto y de esta forma mejorar la seguridad en los correos electrónicos, dando así solución al problema planteado y cumplimiento al objetivo propuesto.

# CONCLUSIONES

1. El modelo propuesto cumple con el objetivo general planteado en la presente investigación, de esta forma se plasma la idea a defender.

2. El estudio de todos los conceptos y teorías relacionadas con correo electrónico y seguridad de la información, coadyuvaron en el diseño de la propuesta presentada.

3. La implementación del primer plan del modelo de seguridad propuesto muestra todo un análisis del servicio de correo electrónico de una institución aplicando metodologías de identificación de riesgos como Delphi y análisis de riesgos como Magerit cumpliendo de esta forma con todos los objetivos específicos planteados.

4. El segundo plan del modelo consiste en la sustitución de la plataforma de software de correo electrónico existente actualmente en la institución, la cual puede ser factible a través de un software libre y seguro, proporcionando una mayor seguridad al servicio de correo electrónico, esto condujo a investigar las posibles opciones existentes en el mercado y seleccionar la que se adaptara a los requerimientos y necesidades de la mayoría de las instituciones, en este sentido se propone la aplicación Squirrelmail.

5. En este modelo también se propone algunas políticas de seguridad generales mismas que pueden ser adecuadas a la institución en la que se implemente el modelo de seguridad según sus necesidades.

6. Para lograr el éxito en la implantación del modelo de seguridad propuesto es necesario que los usuarios de los correos electrónicos institucionales se comprometan y cumplan con las políticas de seguridad que sean planteados por la institución, para garantizar el funcionamiento exitoso de los correos electrónicos.

# RECOMENDACIONES

1. Implementar técnicas de encriptación de mensajes o firma digital para el intercambio seguro de la información mediante el correo electrónico.

2. Durante el desarrollo del presente trabajo se vio que seria interesante la implementación de un Sistema de Correo Electrónico Seguro, empleando certificados y firmas digitales, para las diferentes Instituciones tanto estatales como privadas, esto una vez que se cuenten con Autoridades Certificadoras

3. Para evitar que el sistema se colapse, se podría implementar un control de flujo que llevara a cabo un control de los clientes presentes en el sistema y supervisara los intervalos de transmisión de los mensajes

4. Llevar a cabo un sistema de respaldo mayor al que se realiza actualmente, para poder garantizar la seguridad de los datos de los usuarios ante eventuales e inevitables fallas de seguridad en el servicio de correo electrónico.

# BIBLIOGRAFÍA


**Libros impresos**

HERNÁNDEZ, R; FERNÁNDEZ, C. y BAPTISTA, P. Metodología de la Investigación. 2ª ed. México: McGraw Hill,1998.

PRESSMAN, R., Ingeniería del Software. 5ª ed. España: McGraw Hill,2001

**Libros Electrónicos**

AGUIRRE, J. y MIRET, J. Seguridad Informática y Criptografía, 6ª ed. [en línea]. España: Universidad Politécnica de Madrid, 2006

BISOGNO, M. Metodología para el aseguramiento de entornos informatizados- MAEI [en línea]. Argentina: Universidad de Buenos Aires, 2004

INOSTROZA, JC. Postfix: Guía de Configuración [en línea]. Chile: 2002.

LOPEZ, D. y CONGORTE, J. Spam en el Correo Electrónico [en línea]. España: Universidad EAFIT Departamento de Informática y Sistemas Medellin, 2006.

**Revista electrónica**

Administración de riesgos – Metodología de administración de riesgos en la Universidad Tecnológica de Pereira. [Fecha de consulta: 12 de diciembre 2011]. Disponible en http://www.cybercursos.net.

Correo electrónico y comunicación [Fecha de consulta: 08 de noviembre 2011]. Disponible en www.us-cert.gov/cas/tips

Cronología de la historia del Internet en Bolivia [Fecha de consulta: 9 de agosto 2012] disponible en http://www.lostiempos.com/media_pdf/2012/05/23/362733_pdf.pdf

Estandar internacional ISO/IEC 17799 - [Fecha de consulta: 9 de agosto 2012] disponible en http://mmujica.files.wordpress.com/2007/07/iso-17799-2005-castellano.pdf

Instalación de un Servidor de Correo Send Mail [Fecha de consulta: 11 noviembre 2011]. Disponible en http://www.cybercursos.net.

Metodología de análisis de riesgos informáticos - [Fecha de consulta: 14 Noviembre 2011]. Disponible en http://sgsi-iso27001.blogspot.com/2011/07/las-dificultades-del-ser-humano-para-la.html

MAGERIT - Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información - [fecha de consulta: 14 Noviembre 2011]. Disponible en http://www.csi.map.es/csi/pg5m20.htm

Método Delphi - [Fecha de consulta: 9 de Agosto 2012]. Disponible en http://es.wikipedia.org/wiki/M%C3%A9todo_Delphi

Metodologia Magerit - [Fecha de consulta: 9 de Agosto 2012]. Disponible en http://es.wikipedia.org/wiki/Magerit_(metodolog%C3%ADa)

OCTAVE, - [Fecha de consulta: 14 de Noviembre 2011]. Disponible en http://www.utpl.edu.ec/eccblog/wp-content/uploads/2007/04/articulo-tecnico-evaluacion-de-amenazas-y-vulnerabilidades-de-recursos-criticos-operacionalesoctave-a-nivel-de-usuario-final-para-la-utpl.pdf

Seguridades para Internet y Correo Electrónico 2006, Products and Services, - [Fecha de consulta: 20 de julio 2011]. Disponible en http://www.microsistemas.net

Tecnología de Información y la Comunicación – Correo Electrónico [fecha de consulta: 13 diciembre 2011]. Disponible en http://es.wikipedia.org/wiki/Tecnolog%C3%ADas_de_la_informaci%C3%B3n_y_la_comunicaci%C3%B3n

Todo sobre Correo Electrónico Seguro - [Fecha de consulta: 20 de julio 2011]. Disponible en www.emagister.com/

Zimbra como Solución Libre a un Servidor de Correo [fecha de consulta: 09 Noviembre 2011]. Disponible en http://amperis.blogspot.com

**Congresos o conferencias**

FIGUEIRA, C. En: Criptografía y Seguridad de datos seguridad en el Correo Electrónico. Conferencia Internacional. Universidad Simón Bolívar, 2002.

PONS, M. En: Seguridad en Correo Electrónico. Memoria del I Foro Internacional Escuela Universitaria de Mataró, 2000.

# ANEXO 1

**Identificación de Variables**

Se identifico como elementos de la idea a defender:

Unidad de análisis: Correos electrónicos
Variable independiente: Modelo de seguridad
Variable dependiente: Gestión de riesgo
Enlace lógico: Permitirá

**Definición de Variables**

A continuación se presentan los cuadros de las variables a considerar:

**a) Definición Conceptual**

| IDEA A DEFENDER | VARIABLES | DEFINICION CONCEPTUAL |
|---|---|---|
| La aplicación de un modelo de seguridad para la identificación de amenazas permitirá una adecuada gestión de riesgos de los correos electrónicos institucionales | Modelo de Seguridad | Representación de un sistema de seguridad que se enfoca en el control y la protección de la integridad y privacidad de la información. |
| | Gestión de riesgo | Conjunto de operaciones que se realizan para dirigir y administrar la proximidad de una amenaza. |

**b) Definición Operacional procedimiento**

| VARIABLES | DEFINICION CONCEPTUAL | DIMEN-SIONES | INDICADORES | ITEMS | APLI-CADO |
|---|---|---|---|---|---|
| Modelo de seguridad | Representación de un sistema de seguridad que se enfoca en el control y la protección de la integridad y privacidad de la información. | Seguridad | Políticas | 1,2 | Administrador |
| | | | Difusión de políticas | 3,4 | |
| | | | Física | 5 | |
| | | | Lógica | 6 | |
| | | Control | Causas | 7 | |
| | | | Estrategias aplicadas | 8 | |
| | | | Respuesta ante incidentes | 9,10 | |
| Gestión de riesgos | Conjunto de operaciones que se realizan para dirigir y administrar la proximidad de una amenaza. | Amenaza | Frecuencia de uso del correo electrónico | 1 | Usuarios |
| | | | Mensajes enviados | 2 | |
| | | | Privacidad | 3 | |
| | | | Identificación del remitente | 4 | |
| | | | Fidelidad del contenido | 5 | |
| | | | Notificación de entregado | 6 | |
| | | | Manejo de Spam | 7 | |
| | | | Interferencia entre usuarios | 8 | |
| | | | Claves de acceso | 9 | |
| | | | Virus | 10 | |
| | | | Uso de filtros | 11 | |
| | | | Políticas | 12 | |

# ANEXO 2

**Población y muestra.**

Se puede decir que la población es el conjunto de todas las unidades (personas o cosas) que concuerden con una serie de descripciones. La población compone el objetivo de la investigación, ya que es el centro de la misma y de ella se extrae la información requerida para el estudio de la investigación. En este sentido fue necesario determinar la institución en la cual se aplicó el modelo de seguridad propuesto.

Fundación ACLO que es la institución en la cual se implemento el diseño del modelo propuesto cuenta con 49 empleados y todos ellos son los que se tomaron en cuenta para aplicar las herramientas de investigación, ya que ellos son los directos interesados en que el servicio de correo electrónico que brinda la institución sea la mas adecuada, por esto la población tomada en cuenta para este estudio es 49 empleados y el administrador de sistemas, este estudio no tiene una muestra ya que como se indico se tomo en cuenta a toda la población, este tipo de muestreo responde al tipo de “muestreo convencional”

# ANEXO 3

**(Dirigido al personal que conforma la institución)**

A fin de optimizar un modelo de seguridad en la prestación del servicio de Correo Electrónico que ofrece Fundación ACLO, la Universidad Privada Domingo Savio conjuntamente con una participante del Postgrado de Ingeniería Informática, se desea conocer su opinión y apreciación en cuanto a estos procesos a fin de determinar con precisión, la situación en cuanto a debilidades, fortalezas, puntos críticos y mecanismos que son de fundamental importancia para los usuarios de este servicio.

**ITEM 1:** ¿Hace uso del correo electrónico en la institución?

| | | | |
|---|---|---|---|
| Siempre | ☐ | Casi nunca | ☐ |
| Casi siempre | ☐ | Nunca | ☐ |
| Algunas veces | ☐ | No responde | ☐ |

**ITEM 2:** ¿Cuándo utiliza el correo electrónico confía en la entrega de todos los mensajes enviados?

| | | | |
|---|---|---|---|
| Siempre | ☐ | Casi nunca | ☐ |
| Casi siempre | ☐ | Nunca | ☐ |
| Algunas veces | ☐ | No responde | ☐ |

**ITEM 3:** ¿Confía Ud. en la privacidad de sus correos electrónicos?

| | | | |
|---|---|---|---|
| Siempre | ☐ | Casi nunca | ☐ |
| Casi siempre | ☐ | Nunca | ☐ |
| Algunas veces | ☐ | No responde | ☐ |

**ITEM 4:** ¿Logra identificar en forma inequívoca al emisor de algún correo antes de abrirlo?

| | | | |
|---|---|---|---|
| Siempre | ☐ | Casi nunca | ☐ |
| Casi siempre | ☐ | Nunca | ☐ |
| Algunas veces | ☐ | No responde | ☐ |

**ITEM 5*:*** ¿Puede confiar que el contenido de sus mensajes no ha sido alterado en ningún momento?

| | | | |
|---|---|---|---|
| Siempre | ☐ | Casi nunca | ☐ |
| Casi siempre | ☐ | Nunca | ☐ |
| Algunas veces | ☐ | No responde | ☐ |

**ITEM 6:** ¿Cuándo envía un correo dispone de algún mecanismo para confirmar que el mismo fue entregado al destinatario?

| | | | |
|---|---|---|---|
| Siempre | ☐ | Casi nunca | ☐ |
| Casi siempre | ☐ | Nunca | ☐ |
| Algunas veces | ☐ | No responde | ☐ |

**ITEM 7:** ¿Cuándo revisa su correo está disponible una opción para controlar el correo Spam (correo masivo indeseado)?

| | | | |
|---|---|---|---|
| Siempre | ☐ | Casi nunca | ☐ |

| | | | |
|---|---|---|---|
| Casi siempre | ☐ | Nunca | ☐ |
| Algunas veces | ☐ | No responde | ☐ |

**ITEM 8:** ¿Existe seguridad de que otros usuarios no interfieran en su cuenta de correo electrónico?

| | | | |
|---|---|---|---|
| Siempre | ☐ | Casi nunca | ☐ |
| Casi siempre | ☐ | Nunca | ☐ |
| Algunas veces | ☐ | No responde | ☐ |

**ITEM 9:** ¿La institución le ofrece la posibilidad de cambiar su Passwords en cualquier momento?

| | | | |
|---|---|---|---|
| Siempre | ☐ | Casi nunca | ☐ |
| Casi siempre | ☐ | Nunca | ☐ |
| Algunas veces | ☐ | No responde | ☐ |

**ITEM 10:** ¿Su computadora cuenta con antivirus actualizado que le permita detectar virus en los archivos adjuntos a los correos recibidos?

| | | | |
|---|---|---|---|
| Siempre | ☐ | Casi nunca | ☐ |
| Casi siempre | ☐ | Nunca | ☐ |
| Algunas veces | ☐ | No responde | ☐ |

**ITEM 11:** ¿Utiliza algún sistema para filtrar los correos entrantes (por cabecera, listas, contenidos u otra referencia) usando el servicio de correo electrónico?

| | | | |
|---|---|---|---|
| Siempre | ☐ | Casi nunca | ☐ |
| Casi siempre | ☐ | Nunca | ☐ |
| Algunas veces | ☐ | No responde | ☐ |

**ITEM 12:** ¿Conoce si existen políticas de seguridad para protegerlo como usuario del servicio de correo electrónico?

| | | | |
|---|---|---|---|
| Si | ☐ | No | ☐ |

# ANEXO 4
## (Dirigido al administrador de red de la institución)

A fin de optimizar un modelo de seguridad en la prestación del servicio de Correo Electrónico que ofrece Fundación ACLO, la Universidad Privada Domingo Savio conjuntamente con una participante del Postgrado de Ingeniería Informática, se desea conocer su opinión y apreciación en cuanto a estos procesos a fin de determinar con precisión, la situación en cuanto a debilidades, fortalezas, puntos críticos y mecanismos que son de fundamental importancia para los usuarios de este servicio.

**ITEM 1:** ¿Qué servicios o mecanismos de seguridad contempla la institución para el servicio de correo electrónico?

**ITEM 2:** ¿Con que políticas de seguridad cuenta la institución para el uso del servicio de correo electrónico?

**ITEM 3:** ¿Dan a conocer las políticas de seguridad a los usuarios de correo electrónico?

**ITEM 4:** ¿Cómo dan a conocer sus políticas de seguridad?

**ITEM 5: ¿**Cuales son los dispositivos de seguridad con que cuenta la institución, mencione las características principales en cada uno de ellos?

**ITEM 6**: ¿Cuál es la plataforma de software para el servicio de correo electrónico de la institución?

**ITEM 7:** ¿Cuáles son las causas de las fallas mas frecuentes en el servicio de correo electrónico?

**ITEM 8**: ¿Qué estrategias se usan para la prevención de ataques al correo electrónico?

**ITEM 9:** ¿Qué estrategias o medidas se utilizan para la detección de intrusos?

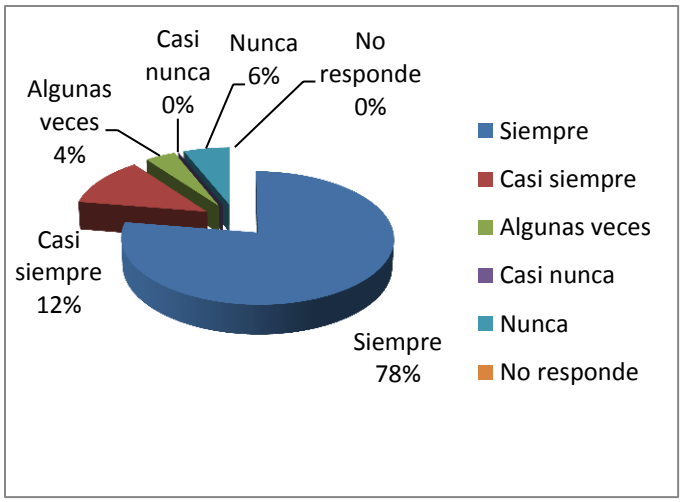
**ITEM 10:** ¿Cuáles son las respuestas o medidas tomadas ante incidentes por fallas en la seguridad del servicio de correo electrónico?

# ANEXO 5

**Resumen de cuestionario aplicado a los funcionarios involucrados con el servicio de correo electrónico.**

**ITEM 1:** ¿Hace uso del correo electrónico en la institución?

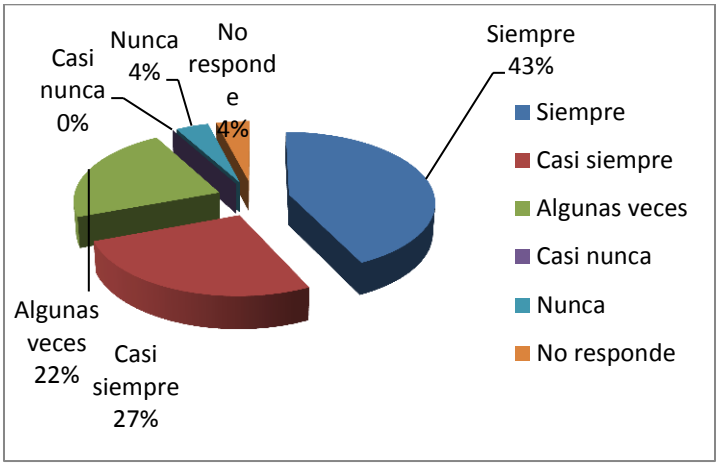
| **Utilización del correo electrónico** | **Nro.** | **%** |
|---|---|---|
| Siempre | 38 | 77,55 |
| Casi siempre | 6 | 12,24 |
| Algunas veces | 2 | 4,08 |
| Casi nunca | 0 | 0,00 |
| Nunca | 3 | 6,12 |
| No responde | 0 | 0,00 |
| **Total** | **49** | **100** |




En el cuadro se detecta que un alto número de usuarios de la institución hacen uso del servicio de correo electrónico, ya que el 90% de la población manifestó que "Siempre" o "Casi siempre" aplica esta herramienta ya que a ella llegan los mensajes tanto personales como de trabajo.

**ITEM 2:** ¿Cuándo utiliza el correo electrónico confía en la entrega de todos los mensajes enviados?

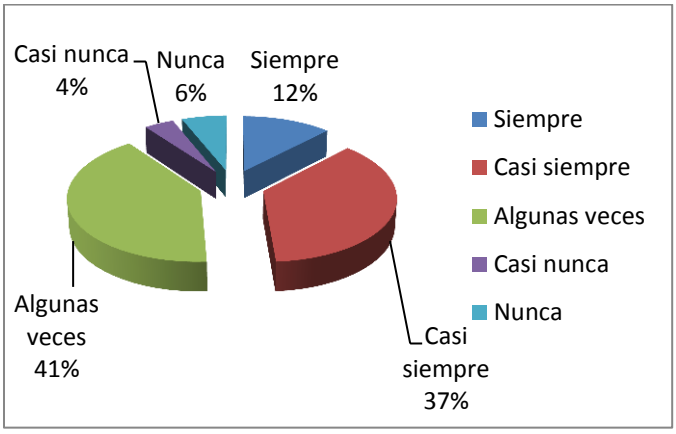
| Confía en la entrega de sus mensajes | Nro. | % |
|---|---|---|
| Siempre | 21 | 42,86 |
| Casi siempre | 13 | 26,53 |
| Algunas veces | 11 | 22,45 |
| Casi nunca | 0 | 0,00 |
| Nunca | 2 | 4,08 |
| No responde | 2 | 4,08 |
| **Total** | **49** | **100** |




Los resultados indican que aproximadamente el 70% de los usuarios de la institución confían plenamente en que sus mensajes enviados a través del servicio de correo electrónico logran ser entregados. Mientras que un 24% mantienen sus reservas, lo que indica que existen algunas fallas de control y seguridad en la red que impide que la globalidad de lo que circula por los paquetes de mensajería llegue a su destino.

**ITEM 3:** ¿Confía Ud. en la privacidad de sus correos electrónicos?

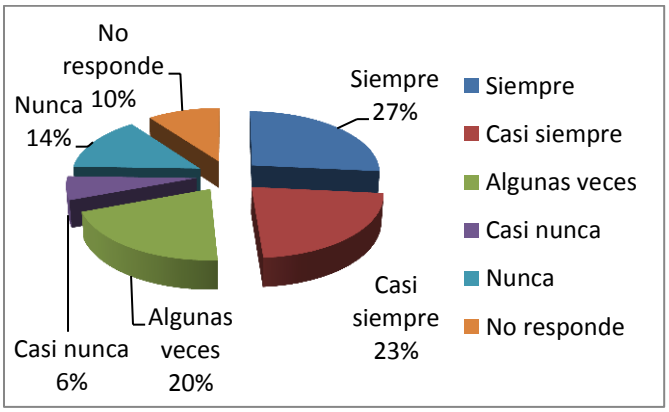
| Confía en la privacidad | Nro. | % |
|---|---|---|
| Siempre | 6 | 12,24 |
| Casi siempre | 18 | 36,73 |
| Algunas veces | 20 | 40,82 |
| Casi nunca | 2 | 4,08 |
| Nunca | 3 | 6,12 |
| **Total** | **49** | **100** |




Se aprecia que solo el 49% de los encuestados ("siempre" y "casi siempre") dan plena confianza al aspecto de la privacidad de los correos electrónicos, indicando de esta manera que han existido fallas en algún momento en cuanto al manejo de la seguridad en la información o pocas medidas y restricciones para el acceso a las cuentas de correo institucional.

**ITEM 4:** ¿Logra identificar en forma inequívoca al emisor de algún correo antes de abrirlo?

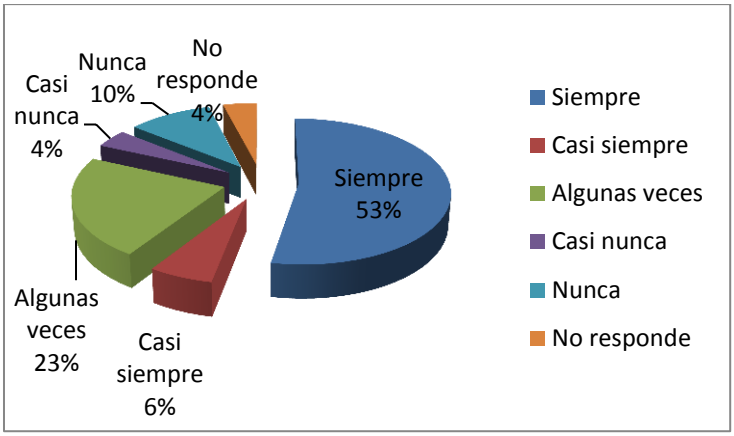
| **Logra identificar al emisor** | **Nro.** | **%** |
|---|---|---|
| Siempre | 13 | 26,53 |
| Casi siempre | 11 | 22,45 |
| Algunas veces | 10 | 20,41 |
| Casi nunca | 3 | 6,12 |
| Nunca | 7 | 14,29 |
| No responde | 5 | 10,20 |




Igual que en el ítem anterior, solo el 49% logra identificar en forma inequívoca al remitente de los correos, indicando con ello un deficiente monitoreo del correo Spam dentro del servicio de correo electrónico. Esto señala un alto índice de riesgo, porque los usuarios pueden abrir correo con contenidos de virus y otras formas de enlaces que pueden causar inestabilidad en la calidad del servicio

**ITEM 5:** ¿Puede confiar que el contenido de sus mensajes no ha sido alterado en ningún momento?

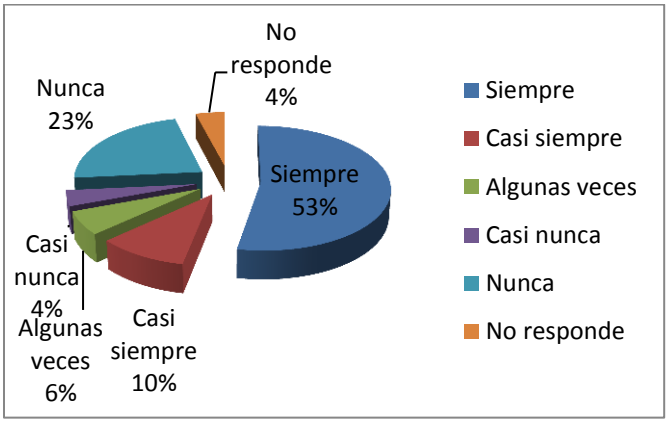
| Confía en la no alteración | Nro. | % |
|---|---|---|
| Siempre | 26 | 53,06 |
| Casi siempre | 3 | 6,12 |
| Algunas veces | 11 | 22,45 |
| Casi nunca | 2 | 4,08 |
| Nunca | 5 | 10,20 |
| No responde | 2 | 4,08 |
| **Total** | **49** | **100** |




Se detecta que cerca del 60% de los usuarios confían (Siempre y casi siempre)
en que el contenido de sus mensajes no es alterado, por lo que la seguridad en cuanto a posibilidad de modificar la información transmitida por este medio es bastante aceptable, pues solo un 13,33% desconfían de este aspecto, posiblemente, por lo indicado en los ítems anteriores en cuanto a la privacidad y entrega de los mensajes.

**ITEM 6:** ¿Cuándo envía un correo dispone de algún mecanismo para confirmar que el mismo fue entregado al destinatario?

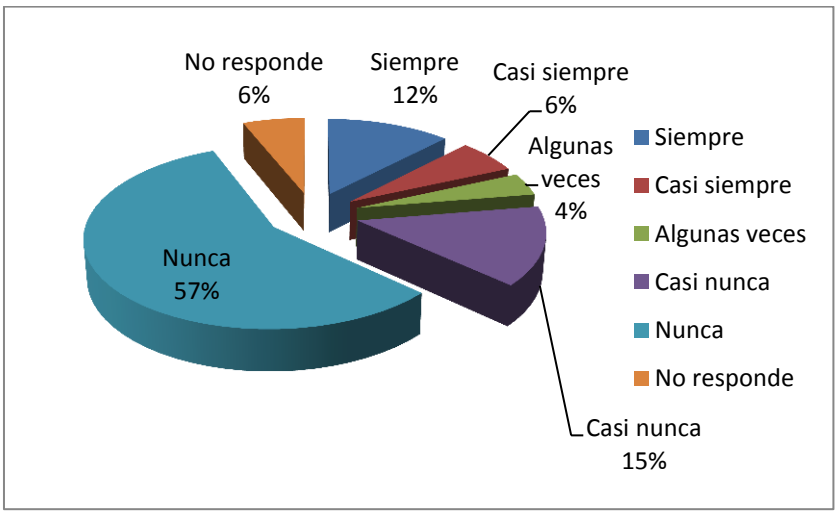
| Uso de alguna herramienta para confirmar | Nro. | % |
|---|---|---|
| Siempre | 26 | 53,06 |
| Casi siempre | 5 | 10,20 |
| Algunas veces | 3 | 6,12 |
| Casi nunca | 2 | 4,08 |
| Nunca | 11 | 22,45 |
| No responde | 2 | 4,08 |
| **Total** | **49** | **100** |




Existe un grupo de la muestra casi el 70% que verifica que el correo ha sido entregado, los que respondieron en contra 26% es porque desconocen las utilidades que presenta el servicio en cuanto a la opción "Notificar al ser leído" o en su defecto la opción "Notificar al ser entregado", aspecto importante en cuanto a la eficiencia de la calidad del servicio en los aspectos de seguridad y control en la circulación del correo entre las diferentes estaciones de trabajo.

**ITEM 7:** ¿Cuándo revisa su correo está disponible una opción para controlar el correo Spam (correo masivo indeseado)?

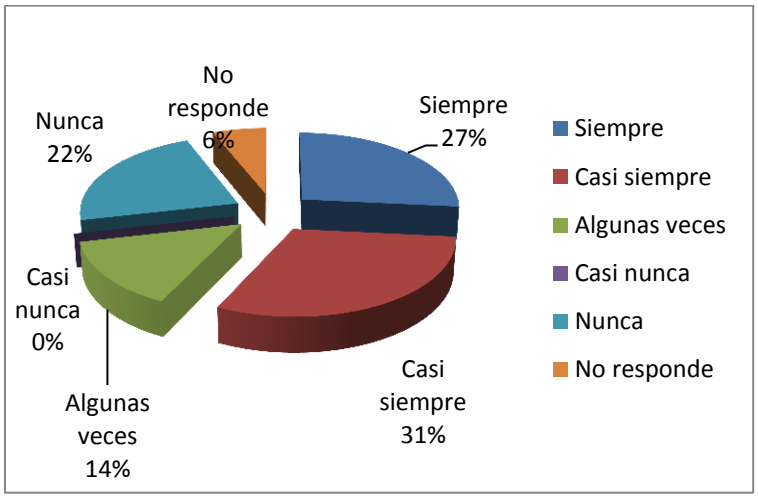
| **Usa la opcion para controlar el Spam** | **Nro.** | **%** |
|---|---|---|
| Siempre | 6 | 12,24 |
| Casi siempre | 3 | 6,12 |
| Algunas veces | 2 | 4,08 |
| Casi nunca | 7 | 14,29 |
| Nunca | 28 | 57,14 |
| No responde | 3 | 6,12 |
| **Total** | **49** | **100** |



Los bajos resultados indican que muy pocos usuarios logran detectar la opción spam al igual que otras opciones o en todo caso, no tienen destreza o conocimiento para usarlas. Lo cual hace ver que no toman las debidas precauciones para evitar la saturación en su buzón del correo indeseado. El hecho que el 57% de los usuarios "nunca" lo utilizan es un aspecto que debe ser tomado en cuenta, en el sentido que el mismo se configure como opción por defecto.

**ITEM 8:** ¿Existe seguridad de que otros usuarios no interfieran en su cuenta de correo electrónico?

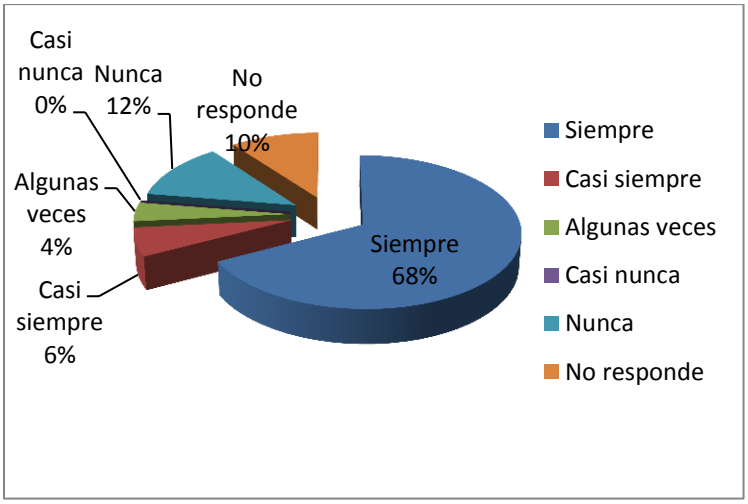
| **No hay interferencia** | **Nro.** | **%** |
|---|---|---|
| Siempre | 13 | 26,53 |
| Casi siempre | 15 | 30,61 |
| Algunas veces | 7 | 14,29 |
| Casi nunca | 0 | 0,00 |
| Nunca | 11 | 22,45 |
| No responde | 3 | 6,12 |
| **Total** | **49** | **100** |




En general solo el 57% confían "Siempre o Casi siempre" en la seguridad del servicio, es decir que confían en que otros usuarios no interfieren en la cuenta de su correo electrónico, situación que puede considerarse crítica, por cuanto una vez abierta una cuenta de correo, no debe haber posibilidad de que otros usuarios logren modificar los parámetros o se visualicen los mismos; ya que en todo caso el administrador es el que puede plantear cambios en cuanto aspectos de capacidad o restricciones en el tipo de correo que recibe, en particular el spam o al volumen de archivos.

**ITEM 9:** ¿La institución le ofrece la posibilidad de cambiar su Passwords en cualquier momento?

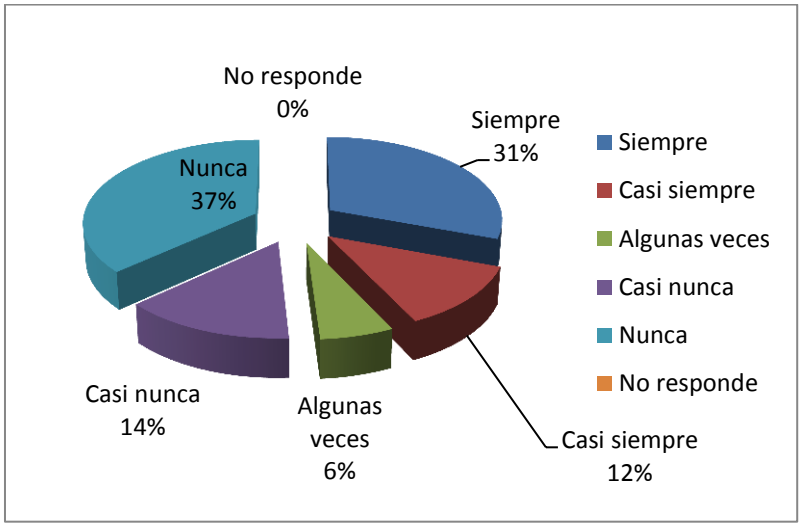
| Posibilidad cambiar password | Nro. | % |
|---|---|---|
| Siempre | 33 | 67,35 |
| Casi siempre | 3 | 6,12 |
| Algunas veces | 2 | 4,08 |
| Casi nunca | 0 | 0,00 |
| Nunca | 6 | 12,24 |
| No responde | 5 | 10,20 |
| **Total** | **49** | **100** |




En general un alto porcentaje 73% conoce que tienen disponible la opción de cambiar el passwords para tener acceso a su cuenta de correo electrónico. Medida muy efectiva para controlar la seguridad, ya que evita en cierta medida que otros usuarios por alguna circunstancia logre identificar su clave, por lo que debería incorporarse la opción de que el passwords deba cambiarse cada cierto tiempo.

**ITEM 10:** ¿Su computadora cuenta con antivirus actualizado que le permita detectar virus en los archivos adjuntos a los correos recibidos?

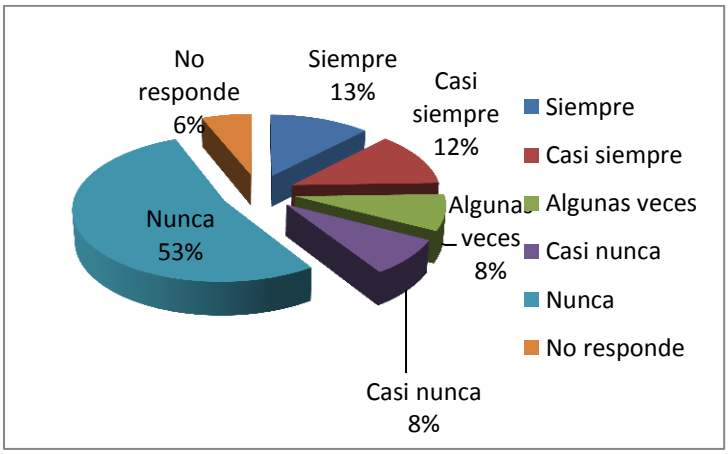
| Uso de opción antivirus | Nro. | % |
|---|---|---|
| Siempre | 15 | 30,61 |
| Casi siempre | 6 | 12,24 |
| Algunas veces | 3 | 6,12 |
| Casi nunca | 7 | 14,29 |
| Nunca | 18 | 36,73 |
| No responde | 0 | 0,00 |
| **Total** | **49** | **100** |




Manteniendo la tendencia de la muestra, muchos de los usuarios del servicio de correo electrónico no conocen o no logran identificar en que parte de la pantalla de visualización del correo está la opción que permite chequear el análisis de los archivos recibidos como archivos adjuntos que pueden contener algún virus. Hecho que se evidencia cuando el 36% señala que su computadora no cuenta con un antivirus actualizado.

**ITEM 11:** ¿Utiliza algún sistema para filtrar los correos entrantes (por cabecera, listas, contenidos u otra referencia) usando el servicio de correo electronico?

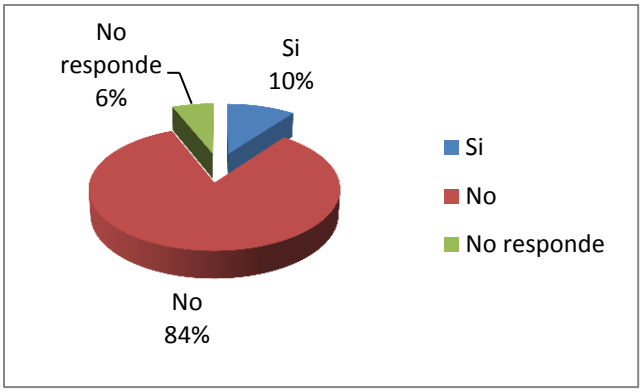
| **Uso de sistema de filtro** | **Nro.** | **%** |
|---|---|---|
| Siempre | 6 | 12,24 |
| Casi siempre | 6 | 12,24 |
| Algunas veces | 4 | 8,16 |
| Casi nunca | 4 | 8,16 |
| Nunca | 26 | 53,06 |
| No responde | 3 | 6,12 |
| **Total** | **49** | **100** |



Indudablemente la generalidad de la muestra no logra utilizar los mecanismos anti-spam para el correo entrante no deseado, se comprueba en este ítem, que una mayor proporción de ellos ni siquiera utilizan algún sistema para filtrar el volumen de correo entrante y poder clasificarlo para separar el correo no deseado, o tipificarlos para no perder tiempo leyendo correo no relevante o de utilidad para el usuario.

**ITEM 12:** ¿Conoce si existen políticas de seguridad para protegerlo como usuario del servicio de correo electrónico?

| **Existen politicas de seguridad** | **Nro.** | **%** |
|---|---|---|
| Si | 5 | 10,20 |
| No | 41 | 83,67 |
| No responde | 3 | 6,12 |
| **Total** | **49** | **100** |




Un alto porcentaje 83% de los usuarios del servicio de correo electrónico desconoce la existencia y vigencia de políticas de seguridad para el manejo del correo electrónico, por lo que la falta de información atenta contra las posibles fallas que pueden deberse al desconocimientos de las medidas preventivas que debe tomar y/o acatar el usuario en el manejo de su cuenta de correo institucional o privada.

# ANEXO 6

**Resumen de cuestionario aplicado al administrador de sistemas involucrado con el servicio de correo electrónico.**

**ITEM 1:** ¿Qué servicios o mecanismos de seguridad contempla la institución para el servicio de correo electrónico?

El administrador contesto, que los servicios que contempla Fundación ACLO para la prestación de servicio de correo electrónico son: confidencialidad, autenticación, integridad y control de acceso.

**ITEM 2:** ¿Con que políticas de seguridad cuenta la institución para el uso del servicio de correo electrónico?

El administrador manifestó no contar con ningún tipo de políticas y que se confía en que los empleados de la institución usen este servicio y el e internet en general con responsabilidad.

**ITEM 3:** ¿Dan a conocer las políticas de seguridad a los usuarios de correo electrónico?

El administrador manifestó, que si dan a conocer a los usuarios algunas recomendaciones de seguridad para el uso del servicio de correo electrónico.

**ITEM 4:** ¿Cómo dan a conocer sus políticas de seguridad?

El administrador contesto, que el medio mediante el cual dan a conocer las políticas de seguridad es solo a través de recomendaciones verbales en el caso de que algún usuario haya tenido algún incidente**.**

**ITEM 5: ¿**Cuales son los dispositivos de seguridad con que cuenta la institución, mencione las características principales en cada uno de ellos?

Los dispositivos de seguridad con que cuenta la Fundación ACLO son: firewall por hardware el cual tiene como característica que contempla: antivirus, anti spam, filtraje de tráfico y sistema detector de intrusos para el servicio de correo electrónico. Para la parte de antivirus cuenta con una base de datos de 4000 antivirus aproximadamente, para realizar, el anti spam se realiza permanentemente un monitoreo de todo el tráfico de la red haciendo un filtraje de archivos POP, HTTP, SMTP, IMAP y FTP, también se hace un filtraje de archivos por paquete y por extensiones de archivos, todo este filtraje se realiza a través de la opción spam filters.

**ITEM 6**: ¿Cuál es la plataforma de software para el servicio de correo electrónico de la institución?

El administrador manifestó que la plataforma de software utilizada para el servicio de correo electrónico es SENDMAIL, y que el sistema operativo bajo el cual se encuentra instalada la plataforma es Solaris Versión 8. Por otra parte, añadió que las especificaciones técnicas del

hardware donde se encuentra instalado el software de correo electrónico son: memoria ram de 1024 GB, 2 procesadores Pentium y un Disco duro de 150 GB.

**ITEM 7:** ¿Cuáles son las causas de las fallas mas frecuentes en el servicio de correo electrónico?

El administrador manifestó, que la causa de las fallas mas frecuentes en el servicio de correo electrónico esta relacionada con problemas en los buzones de correo electrónico ya que los usuarios no están pendiente de descargar o vaciar los mismos y el administrador no puede asumir dicha función debido a que el no esta al tanto de saber que debe y no borrar, por lo tanto los buzones de correos están permanentemente saturados de correos y en muchos casos estos correos son spam.

**ITEM 8**: ¿Qué estrategias se usan para la prevención de ataques al correo electrónico?

El administrador contesto, confiar en que el usuario maneje los datos de forma prudente, además que físicamente se utiliza un anti spam y un firewall.

**ITEM 9:** ¿Qué estrategias o medidas se utilizan para la detección de intrusos?

El administrador contesto, que se utiliza un sistema detector de intrusos a través del firewall, el cual contempla un monitoreo permanente y hace filtraje de archivos con extensiones POP, HTTP, SMPTP, IMAP y FTP, además realiza filtraje por archivos de paquetes y por extensiones de archivos.

**ITEM 10:** ¿Cuáles son las respuestas o medidas tomadas ante incidentes por fallas en la seguridad del servicio de correo electrónico?

El administrador respondió, que las medidas tomadas son: registro del incidente, recuperación de la falla y respaldo de la data acotando que dicho respaldo debe ser mayor pues las fallas son eventuales e inevitables.

# ANEXO 7

## ENTREVISTA

### Evaluación con expertos de controles y seguridad del correo electrónico

**Institución:**
**Departamento:**
**Persona entrevistada:**
**Fecha:**

2. ¿Posee correo electrónico la organización?

Si ☐ No ☐

2. ¿Cuál es el sistema de correo electrónico que usa?

27. ¿Cuál es su proveedor de Internet y por qué?

**Seguridad de los equipos y control de accesos**

28. ¿Poseen seguro de equipos?

Si ☐ No ☐

29. ¿Con cuantos equipos cuenta la institución para uso de correo electrónico y como están distribuidos los equipos?

30. ¿Dónde se encuentran ubicados los servidores de correo?

31. ¿Quienes tienen acceso al departamento de sistemas?

32. ¿Quiénes tienen acceso al servidor de correo?

**Claves de acceso**

33. ¿Poseen claves de acceso los servidores de correo y como están compuestas?

34. ¿Cada cuánto tiempo son cambiadas éstas claves?

35. ¿Las contraseñas de usuario asignadas inicialmente bajo qué parámetros fueron establecidas?

36. ¿Cada cuánto tiempo los usuarios cambian sus contraseñas y bajo qué parámetros?

**Cuentas de usuario**

37. ¿Quién es el encargado de la creación y eliminación de cuentas de correo electrónico?

38. ¿La solicitud de creación de una cuenta de usuario se la realiza de forma verbal o escrita?

39. ¿Posee respaldo de las cuentas de usuario?

Si ☐ No ☐

40. ¿Posee un registro o bitácora de control de las cuentas de usuario?

Si ☐ No ☐

41. ¿Posee un registro actualizado de la creación y eliminación de cuentas de correo?

Si ☐ No ☐

42. ¿Cuántas cuentas de usuario de se encuentran activas al momento?

43. De las cuentas de usuario antes mencionadas, ¿Todas pertenecen a trabajadores actuales?

44. ¿Cuál es la capacidad de almacenamiento de cada cuenta de usuario?

**Políticas de Seguridad**

45. ¿Se cuenta con un manual de políticas de seguridad de correo electrónico?

Si ☐ No ☐

46. ¿Al momento de crear una cuenta de correo se le indica al usuario las responsabilidades que está adquiriendo así como el uso que le debe dar?

47. ¿Los usuarios utilizan el correo para actividades ajenas a la empresa?

**Seguridad de Información**

48. ¿Por cuánto tiempo puede permanecer abierto un correo sin ser usado?

49. ¿Qué posibilidad existe de que los equipos se infecten por algún mensaje que contenga virus?

50. ¿Cuál es la capacidad de archivos adjuntos que puede recibir y enviar en un mail?

27. ¿Posee Firma electrónica?

Si ☐ No ☐

28. ¿Posee certificado digital?

Si ☐ No ☐

29. ¿Se tiene conciencia de la seguridad que debe poseer el correo electrónico de la empresa?

31. Cuáles son los problemas mas comunes que se han presentado en el uso del correo electrónico?

32. ¿A la presente fecha se ha realizado una auditoria informática en la institución?

# ANEXO 8

**UNIVERSIDAD AMAZONICA DE PANDO**
**DIRECCION DE POSTGRADO – PROGRAMA DE MAESTRIA EN INGENIERIA INFORMÁTICA**

**Consulta a especialistas en la aplicación de un Modelo de Seguridad para Identificar Amenazas de los Correos Electrónicos Institucionales**

Distinguido directivo o docente, el presente cuestionario tiene como propósito conocer su opinión acerca de la aplicación de un Modelo de Seguridad para Identificar Amenazas de los Correos Electrónicos Institucionales, con este fin solicito afectuosamente su colaboración. Teniendo en cuenta que su opinión será de gran valor en este trabajo de investigación para validar o rectificar la propuesta, por tanto insinúo su colaboración en el análisis y la valoración de las siguientes preguntas de acuerdo a las referencias que se presentan. De antemano, agradezco su valiosa contribución.

I.- Por favor complete la siguiente información

Nombre:

Institución donde trabaja:

Cargo que ocupa:

Años de experiencia en su desempeño profesional:

Nivel de profesionalización y/o trabajos de investigación recientes:

II.- Según su criterio marque con una X**,** en una escala creciente del 1 al 10, el grado de conocimiento que usted tiene sobre el tema de estudio.

| **ESCALA** | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|
| **EXPERTO** | | | | | | | | | | |

III.- Marque con una X, según su opinión, respecto a los aspectos siguientes relativos al modelo de seguridad propuesto atendiendo a las siguientes categorías:

- (MA) Muy adecuado
- (BA) Bastante adecuado
- (A) Adecuado
- (PA) Poco adecuado
- (I) Inadecuado

| No. | ASPECTOS A VALORAR | MA | BA | A | PA | I |
|---|---|---|---|---|---|---|
| 1 | ¿Considera usted que el **sustento teórico** que respalda la investigación, permite llegar a una conceptualización clara y comprensible sobre la gestión de riesgos, controles que se deben aplicar y amenazas que sufren los correos electrónicos? | | | | | |
| 2 | ¿Considera usted que la **sistematización de la propuesta,** ofrece una orientación adecuada para identificar amenazas y realizar una adecuada gestión de riesgos? | | | | | |
| 3 | ¿Considera usted que los **objetivos** planteados son los mas adecuados y tienen relación con el contenido de la investigación? | | | | | |
| 4 | ¿Considera usted que el modelo propuesto de permitirá la una **eficiente identificación de amenazas y por tanto una adecuada gestión de riesgos** en los correos electrónicos? | | | | | |
| 5 | ¿Considera usted que incluir en la propuesta del modelo de seguridad un **proceso detallado de gestión de riesgos con sus fases de identificación, análisis, valoración y manejo de los riesgos**, permite la identificación adecuada de las amenazas existentes en los correos electrónicos? | | | | | |
| 6 | ¿Considera usted que los **resultados de la aplicación del modelo de seguridad propuesto** cumplen con el objetivo propuesto? | | | | | |

VI.- Considerando los números correspondientes en que aparecen los diferentes aspectos de la propuesta del Modelo de Seguridad para Identificar Amenazas de los Correos Electrónicos

Institucionales, diga qué modificaría, que incluiría y que eliminaría en cada uno de ellos considerando su experiencia profesional.

| Nº | ASPECTOS A VALORAR | QUE MODIFICAR | QUE INCLUIR | QUE ELIMINAR |
|---|---|---|---|---|
| 1 | Sustento teórico. | | | |
| 2 | Sistematización de la propuesta. | | | |
| 3 | Objetivo general de la propuesta. | | | |
| 4 | Proceso de identificación de amenazas. | | | |
| 5 | Proceso de proceso detallado de gestión de riesgos | | | |
| 6 | Resultados de la aplicación del modelo propuesto. | | | |

GRACIAS POR SU COLABORACIÓN!!!!

.

# ANEXO 9

## RESUMEN DE LA VALORACION DEL CUESTIONARIO

| Nro. Experto | Grado de Conocimiento | Preg. 1 | Preg. 2 | Preg. 3 | Preg. 4 | Preg. 5 | Preg. 6 |
|---|---|---|---|---|---|---|---|
| 1 | 7 | 4 | 3 | 3 | 5 | 4 | 3 |
| 2 | 9 | 3 | 4 | 4 | 4 | 4 | 5 |
| 3 | 6 | 5 | 5 | 5 | 5 | 3 | 4 |
| 4 | 5 | 4 | 4 | 4 | 3 | 5 | 4 |
| 5 | 8 | 5 | 4 | 4 | 4 | 5 | 3 |
| **PROMEDIO** | | 4,2 | 4 | 4 | 4,2 | 4,2 | 3,8 |
| **PORCENTAJE** | | 84 | 80 | 80 | 84 | 84 | 76 |

Según la escala:

| | |
|---|---|
| Muy adecuado (MA) | 5 |
| Bastante adecuado (BA) | 4 |
| Adecuado (A) | 3 |
| Poco adecuado (PA) | 2 |
| Inadecuado (I) | 1 |