



**UNIVERSIDAD TÉCNICA DE AMBATO**  
**FACULTAD DE INGENIERÍA EN SISTEMAS ELECTRÓNICA  
E INDUSTRIAL**  
**CARRERA DE INGENIERÍA EN SISTEMAS  
COMPUTACIONALES E INFORMÁTICOS**

**Tema:**

---

“TÉCNICAS SPAM PARA EL ENVÍO MASIVO DE INFORMACIÓN NO DESEADA A LAS CUENTAS DE CORREO ELECTRÓNICO DE LOS FUNCIONARIOS DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPALIDAD AMBATO”

---

**Trabajo de Graduación. Modalidad:** Seminario De Graduación “Seguridad Informática”, presentado previo la obtención del título de Ingeniero en Sistemas Computacionales e Informáticos.

**Subnivel de investigación:** Seguridad Informática

**AUTOR:** Verónica Jazmina Silva Mena

**PROFESOR REVISOR:** Ing. Luis Solís

Ambato – Ecuador

Abril-2013

## APROBACION DEL TUTOR

En mi calidad de tutor del trabajo de investigación sobre el tema **“TÉCNICAS SPAM PARA EL ENVÍO MASIVO DE INFORMACIÓN NO DESEADA A LAS CUENTAS DE CORREO ELECTRÓNICO DE LOS FUNCIONARIOS DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPALIDAD AMBATO”**, de la señorita Verónica Jazmina Silva Mena, estudiante de la Carrera de Ingeniería en Sistemas Computacionales e Informáticos, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial de la Universidad Técnica de Ambato , considero que el informe investigativo reúne los requisitos suficientes para que continúe con los tramites y consiguiente aprobación de conformidad el Art. 16 del Capítulo II, del Reglamento de Graduación para Obtener el Título Terminal de Tercer Nivel de la Universidad Técnica de Ambato.

Ambato,.....

EL TUTOR

-----

Ing. Luis Solís

## AUTORÍA

El presente trabajo de Investigación titulado **“TÉCNICAS SPAM PARA EL ENVÍO MASIVO DE INFORMACIÓN NO DESEADA A LAS CUENTAS DE CORREO ELECTRÓNICO DE LOS FUNCIONARIOS DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPALIDAD AMBATO”**. Es absolutamente original, autentico y personal, en tal virtud, el contenido, efectos legales y académicos que se desprenden del mismo son de exclusiva responsabilidad del autor.

Ambato, Abril 2013

-----

Verónica Jazmina Silva Mena

180276062-7

## **APROBACION DE LA COMISION CALIFICADORA**

La comisión calificadora del presente trabajo la conformada por los señores docentes Ing. Teresa Freire E Ing. Franklin Mayorga, Aprobó el informe Final Del trabajo de graduación Titulado **“TÉCNICAS SPAM PARA EL ENVÍO MASIVO DE INFORMACIÓN NO DESEADA A LAS CUENTAS DE CORREO ELECTRÓNICO DE LOS FUNCIONARIOS DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPALIDAD AMBATO”**, presentado por la señorita Verónica Jazmina Silva Mena de acuerdo al Art. 18 del Reglamento de Graduación para Obtener el Título Terminal de Tercer Nivel de la Universidad Técnica de Ambato.

Ing. Mg. Edison Homero Álvarez Mayorga

**PRESIDENTE DEL TRIBUNAL**

-----  
Ing. Teresa Freire

**DOCENTE CALIFICADOR**

-----  
Ing. Franklin Mayorga

**DOCENTE CALIFICADOR**

## DEDICATORIA

*A DIOS por su infinito amor, por guiarme siempre y nunca dejarme sola en cada instante de mi vida a mis queridos padres por esforzarse y ser quienes día a día velaron por mi bienestar brindándome el privilegio de estudiar gracias por apoyarme siempre para alcanzar mis metas.*

*A mi abuelito Jorge por brindarme siempre su dulzura, su ejemplo y sus consejos, por ser ese ser ejemplar a quien admiro y recordare siempre cuando ya no este.*

*A cada docente de mi querida facultad que contribuyo compartiendo sus conocimientos conmigo y mis compañeros, siempre dispuestos ayudarnos despejando cada inquietud.*

*A mis amigas/os quienes estuvieron apoyándome no solo en las alegrías sino en los momentos más difíciles siendo quienes jamás permitieron que desmaye, y hoy siguen en mi vida compartiendo el inmenso cariño que nos une.*

*Verónica Jazmina Silva Mena*

## AGRADECIMIENTO

*A ti padre amado, tu mi **Dios** generoso por brindarme la oportunidad de vivir y alcanzar este sueño tan anhelado, por guiar mis pasos en cada momento, por enseñarme a que una caída no es motivo para desmayar, pues tu siempre me has brindado tu mano para seguir adelante luchando hasta el final.*

*A ti madre querida que a pesar de que hoy no estás a mi lado, sé que en tu corazón estarás feliz al ver cumplir mis metas que en gran parte son gracias a ti por tus consejos, por enseñarme a que el estudio es la mejor herencia que en mi vida podías regalarme; a mi papito y mi hermana que son el apoyo más grande con el que cuento gracias por estar a mi lado y preocuparse siempre por mi bienestar y por mi formación profesional.*

*Agradezco también a toda mi familia por haberme dado su fuerza y apoyo en los momentos difíciles, gracias a sus consejos he seguido adelante.*

*A mi tutor de tesis Ing. LUIS SOLIS por su valioso tiempo y por compartir conmigo sus conocimientos, gracias por su apoyo.*

*Al GAD Municipalidad Ambato, por abrirme sus puertas y brindarme la oportunidad de desarrollar y aplicar el presente proyecto investigativo.*

*A mí misma porque tuve muchos obstáculos a lo largo de mi carrera, y sin embargo confíen en Dios y en mí para no perder el horizonte y seguir esforzándome día a día; por último a ese ser tan maravilloso que es una bendición, a quien amo y estoy segura que amare por el resto de mi vida.*

*Verónica Jazmina Silva Mena.*

## ÍNDICE

APROBACION DEL TUTOR.....	ii
AUTORIA.....	iii
APROBACION DE LA COMISION CALIFICADORA.....	iv
DEDICATORIA .....	v
AGRADECIMIENTO.....	vi
ÍNDICE .....	vii
RESUMEN EJECUTIVO .....	xiii
INTRODUCCIÓN .....	xv
CAPITULO I.....	1
1. PROBLEMA.....	1
1.1 TEMA: .....	1
1.2 PLANTEAMIENTO DEL PROBLEMA: .....	1
1.2.1 CONTEXTUALIZACIÓN .....	1
1.2.2 ÁRBOL DE PROBLEMAS .....	3
1.2.3 ANÁLISIS CRÍTICO .....	4
1.2.4 PROGNOSIS.....	4
1.2.5 FORMULACIÓN DEL PROBLEMA.....	5
1.2.6 DELIMITACIÓN .....	5
1.2.7 PREGUNTAS DIRECTRICES .....	5
1.3 JUSTIFICACIÓN.....	6
1.4 OBJETIVOS .....	7
1.4.1 OBJETIVO GENERAL .....	7
1.4.2 OBJETIVOS ESPECÍFICOS .....	7
CAPITULO II .....	8
2. MARCO TEÓRICO .....	8
2.1. ANTECEDENTES INVESTIGATIVOS: .....	8
2.2 FUNDAMENTACIÓN LEGAL: .....	9
2.3. FUNDAMENTACIÓN TEÓRICA .....	13
2.4 HIPÓTESIS: .....	32
2.5. SEÑALAMIENTO DE VARIABLES .....	32

CAPITULO III.....	33
3. MARCO METODOLÓGICO.....	33
3.1 ENFOQUE.....	33
3.2 MODALIDADES BÁSICAS DE LA INVESTIGACIÓN .....	33
3.3 TIPOS DE INVESTIGACIÓN.....	34
3.4 POBLACIÓN Y MUESTRA .....	35
3.5 OPERACIONALIZACIÓN DE VARIABLES .....	36
3.6 RECOLECCIÓN Y ANÁLISIS DE LA INFORMACIÓN .....	39
3.7 PROCESAMIENTO Y ANÁLISIS DE LA INFORMACIÓN.....	40
3.8 RECURSOS .....	41
3.8.1 INSTITUCIONALES.....	41
3.8.2 HUMANOS.....	41
3.8.3 MATERIALES.....	41
3.8.4 ECONÓMICAS .....	41
3.9 PRESUPUESTO .....	42
CAPITULO IV.....	43
4. ANÁLISIS E INTERPRETACIÓN DE LOS RESULTADOS.....	43
4.1 ANALISIS DE LA INFORMACIÓN .....	43
4.2. INTERPRETACIÓN DE LOS RESULTADOS.....	44
4.3. COMPROBACIÓN DE HIPÓTESIS.....	62
CAPITULO V .....	64
5. CONCLUSIONES Y RECOMENDACIONES .....	64
5.1. CONCLUSIONES .....	64
5.2. RECOMENDACIONES .....	65
CAPITULO VI.....	66
6. PROPUESTA.....	66
6.1. DATOS INFORMATIVOS .....	66
6.2. ANTECEDENTES DE LA PROPUESTA.....	67
6.3 JUSTIFICACIÓN .....	67
6.4. OBJETIVOS .....	69
6.4.1. OBJETIVO GENERAL .....	69
6.4.2. OBJETIVOS ESPECÍFICOS .....	69
6.5. ANÁLISIS DE FACTIBILIDAD.....	69



6.6. INFORME TECNICO.....	71
6.6.1. ANÁLISIS DE LAS TÉCNICAS SPAM .....	71
6.6.2. HERRAMIENTAS PARA ENVÍO DE SPAM .....	73
6.6.2.1. FILEZILA CLIENT .....	73
6.6.2.2. MOZILA THUNDERBIRD .....	75
6.6.2.3. OUTLOOK .....	79
6.6.2.4. CLAWS-MAIL .....	82
6.6.2.5. PHPLIST .....	87
6.6.3. PRUEBAS DE ENVÍO DE MENSAJES APLICANDO TÉCNICAS SPAM .....	92
6.6.3.1. PRUEBA CON LA HERRAMIENTA PHPLIST .....	93
6.6.3.2. PRUEBA CON LA HERRAMIENTA THUNDERBIRD.....	101
6.6.3.3. PRUEBA CON LA HERRAMIENTA CLAWS-MAIL.....	104
6.6.3.4. PRUEBA CON LA HERRAMIENTA OUTLOOK.....	104
6.6.4. ANÁLISIS COMPARATIVO DE LAS PRUEBAS SPAM.....	105
6.7.    DESARROLLO DEL MANUAL.....	109
6.8.    CONCLUSIONES Y RECOMENDACIONES.....	109
6.8.1.    CONCLUSIONES.....	109
6.8.2.    RECOMENDACIONES .....	110
ANEXO 1.....	116
ANEXO 2.....	119
ANEXO 3.....	122

## **INDICE DE GRÁFICAS**

Gráfico 1. 1 Análisis Crítico .....	3
Gráfico 1. 2 Variable Independiente .....	13
Gráfico 1. 3 Variable Dependiente .....	14
Gráfico 4. 1 Víctima de Spammer .....	44
Gráfico 4. 2 Infección de virus .....	46
Gráfico 4. 3 Listas de Correo spam.....	47

Gráfico 4. 4 Técnicas de protección del computador .....	49
Gráfico 4. 5 Tipo de información spam .....	51
Gráfico 4. 6 Servidor pop .....	53
Gráfico 4. 7 Remitentes desconocidos .....	54
Gráfico 4. 8 Servidor proxy inseguro.....	55
Gráfico 4. 9 Pérdida de Información.....	57
Gráfico 4. 10 Pérdida de Información.....	59
Gráfico 4. 11 Envío de mensajes con cadenas .....	61
Gráfico 6. 1 Inicio FileZila .....	74
Gráfico 6. 2 Conexión a servidor desde ftp.....	75
Gráfico 6. 3 Configuración de Mozilla Thunderbird.....	76
Gráfico 6. 4 Creación cuenta de correo en MT .....	76
Gráfico 6. 5 Bandeja de entrada de la cuenta en MT.....	77
Gráfico 6. 6 Redacción de mensajes en MT.....	78
Gráfico 6. 7 Creación de contactos en MT.....	78
Gráfico 6. 8 Inicio de Microsoft Outlook.....	79
Gráfico 6. 9 Pregunta de verificación de configuración Outlook .....	79
Gráfico 6. 10 Configuración de cuenta en Outlook.....	80
Gráfico 6. 11 Cuenta configurada correctamente.....	80
Gráfico 6. 12 Ventana de inicio de Outlook.....	81
Gráfico 6. 13 Redacción de mensajes en Outlook.....	81
Gráfico 6. 14 Inicio de Claws Mail.....	82
Gráfico 6. 15 Configuración de Claws Mail .....	83
Gráfico 6. 16 Configuración de POP3 en Claws Mail .....	83
Gráfico 6. 17 Configuración de servidor SMTP en Claws Mail .....	84
Gráfico 6. 18 Configuración Establecida .....	85
Gráfico 6. 19 Ventana de funciones de Claws mail .....	86
Gráfico 6. 20 Ventana de envío de mensajes .....	86
Gráfico 6. 21 Ventana PHPList iniciando.....	87
Gráfico 6. 22 Contenidos de PHPList.....	88
Gráfico 6. 23 Página principal de administración de PHPList .....	88
Gráfico 6. 24 Configuración de PHPList .....	89
Gráfico 6. 25 Configuración de Listas de Usuarios en PHPList .....	90
Gráfico 6. 26 Importación de e-mails de PHPList .....	91
Gráfico 6. 27 Acceso al dominio. Hosting .....	93
Gráfico 6. 28 Pagina systemjazz .....	93
Gráfico 6. 29 Conexión al servidor PHPList.....	94
Gráfico 6. 30 Levantamiento del cliente Filezila .....	95
Gráfico 6. 31 Verificación de lista de usuarios en PHPList .....	95
Gráfico 6. 32 Subir imágenes al Hosting .....	96
Gráfico 6. 33 Verificación en el cliente con la información del hosting .....	97
Gráfico 6. 34 Propiedades de imagen a adjuntar al mensaje .....	98

Gráfico 6. 35 Adjunto de imagen en el mensaje .....	98
Gráfico 6. 36 Guardar cambios en mensajes .....	99
Gráfico 6. 37 Procesamiento de sola de mensajes.....	99
Gráfico 6. 38 Verificación de envío de mensajes en cola.....	100
Gráfico 6. 39 Comprobación de recepción de mensaje .....	100
Gráfico 6. 40 Configuración para prueba de envío MT .....	101
Gráfico 6. 41 Especificación de Destinatarios .....	102
Gráfico 6. 42 Ventana de carga de mensaje MT .....	102
Gráfico 6. 43 Bandeja de salida MT .....	103
Gráfico 6. 44 Bandeja de entrada cuenta alternativa .....	103
Gráfico 6. 45 Envío de mensaje con Claws Mail .....	104
Gráfico 6. 46 Detección de cuenta en black list .....	105
Gráfico 6. 47 Comparación de herramientas de envío de mensajes .....	106
Gráfico 6. 48 Éxitos con PHPList.....	106
Gráfico 6. 49 Éxitos con MT .....	107
Gráfico 6. 50 Éxitos con Outlook .....	107
Gráfico 6. 51 Éxitos con Claws-Mail.....	108
Gráfico 6. 52 Comparación entre Herramientas aplicadas .....	109

## INDICE DE GAFICAS DE ANEXOS

-	
Gráfico A. 1 Reconocimiento de mensajes spam .....	126
Gráfico A. 2 Asusnto llamativo y en inglés.....	126
Gráfico A. 3 Mensajes spam asuntos y remitentes desconocidos .....	127
Gráfico A. 4 Contenido de mensajes Spam .....	129
Gráfico A. 5 Cadena de mensaje para reenviar.....	130
Gráfico A. 6 Envío de información de contactos .....	130
Grá Gráfico A. 7 Acceso al dominio. Hosting .....	132
Gráfico A. 8 Conexión al servidor PHPList .....	132
Gráfico A. 9 Levantamiento del cliente Filezila .....	133
Gráfico A. 10 Verificación de lista de usuarios en PHPList.....	133
Gráfico A. 11 . Subir imágenes al Hosting .....	134
Gráfico A. 12 Verificación en el cliente con la información del hosting .....	134
Gráfico A. 13. Propiedades de imagen a adjuntar al mensaje .....	135
Gráfico A. 14 Adjunto de imagen en el mensaje .....	135
Gráfico A. 15 Guardar cambios en mensajes.....	135
Gráfico A. 16 Procesamiento de sola de mensajes .....	136
Gráfico A. 17 . Verificación de envío de mensajes en cola .....	136
Gráfico A. 18 . Comprobación de recepción de mensaje .....	137
Gráfico A. 19 Configuración para prueba de envío MT .....	137
Gráfico A. 20 . Especificación de Destinatarios .....	138
Gráfico A. 21 Ventana de carga de mensaje MT .....	138

Gráfico A. 22 . Bandeja de salida MT .....	139
Gráfico A. 23 Bandeja de entrada cuenta alternativa.....	139
Gráfico A. 24 . Envío de mensaje con Claws Mail.....	140
Gráfico A. 25 Detección de cuenta en black list.....	140

## ÍNDICE DE TABLAS

Tabla 3. 1. Variable Independiente .....	37
Tabla 3. 2. Variable Dependiente .....	38
Tabla 4. 1. Frecuencia de la pregunta N° 1 .....	44
Tabla 4. 2 Frecuencia pregunta 2.....	46
Tabla 4. 3. Frecuencia pregunta 3 .....	47
Tabla 4. 4. Frecuencia pregunta 4.....	49
Tabla 4. 5 Frecuencia pregunta 5.....	51
Tabla 4. 6 Frecuencia pregunta 6a .....	53
Tabla 4. 7 Frecuencia pregunta 6b.....	53
Tabla 4. 8 Frecuencia pregunta 7.....	55
Tabla 4. 9 Frecuencia pregunta 8.....	57
Tabla 4. 10 Frecuencia pregunta 9 .....	59
Tabla 4. 11 Frecuencia pregunta 10.....	61

## INDICE DE TABLAS DE ANEXOS

Tabla A. 1 Consecuencias del spam .....	129
Tabla A. 2 Medidas de prevención en la recepción de spam .....	131

## **RESUMEN EJECUTIVO**

La investigación realiza un estudio profundo acerca del tipo de técnicas spam que inciden en la inundación de mensajes con contenido no deseado en las cuentas de correo de los funcionarios del GADMA, a pesar de tener algunas seguridades dentro de la institución.

Dentro del municipio de Ambato los funcionarios trabajan por departamentos, cada grupo de ellos, especializados en diferentes actividades, el área o departamento de sistemas en donde trabajan funcionarios con amplio conocimiento tecnológico ha puesto en consideración la facilidad de revisar el servidor donde se registran los correos de cada funcionario, para así poder conseguir información acerca del comportamiento de las técnicas de envío de SPAM.

Los departamentos requieren que los correos electrónicos de cada funcionario sean utilizados dentro de la empresa o fuera de ella con seguridad, sin exponerse a recibir mensajes de posibles spammers a quienes les favorece e interesa enviar su publicidad y su código malicioso, para apoderarse de información privada en caso de ser posible.

Se han suscitado algunos inconvenientes producto del excesivo spam que reciben los funcionarios en sus cuentas, como pérdidas de información enviada a través de sus correos, producto también de la falta de capacitación sobre el tema lo que provoca mayor vulnerabilidad al ataque masivo de spam.

Para disminuir los ataques se ha creado un manual que guíe a los funcionarios del GADMA en como disminuir el excesivo envío de información no deseada a sus cuentas de correo electrónico, y capacitar a cada uno a reducir su vulnerabilidad ante la exposición de su información personal y laboral, evitando así que sean ellos mismos quienes contribuyan a que el uso de técnicas spam crezca y se propague dentro de la municipalidad

## INTRODUCCIÓN

Al informe final de proyecto denominado “Técnicas spam para el envío masivo de información no deseada a las cuentas de correo electrónico de los funcionarios del Gobierno Autónomo Descentralizado Municipalidad Ambato” se pone en consideración:

En el **CAPÍTULO I** denominado “Problema” se presenta la identificación del problema a investigar, se plantea la justificación y los objetivos

En el **CAPÍTULO II** denominado “Marco Teórico” se presenta los antecedentes investigativos, la fundamentación legal, hipótesis y el señalamiento de las variables.

En el **CAPÍTULO III** denominado “Marco Metodológico” se muestra la metodología de investigación que se va a utilizar, el enfoque, la modalidad básica de la investigación, su tipo además de la población y muestra.

En el **CAPÍTULO IV** denominado “Análisis e Interpretación de los Resultados” se presenta el respectivo análisis e interpretación de resultados.

En el **CAPÍTULO V** denominado “Conclusiones y recomendaciones” se presenta las conclusiones y recomendaciones en base de los resultados obtenidos en la encuesta realizada a los funcionarios de departamento de sistemas.

En el **CAPÍTULO VI** denominado “Propuesta” se presenta el desarrollo de la propuesta planteada para el problema investigado.

**ANEXOS:** se presenta todos los documentos como encuestas, manuales de usuario o guías realizadas para esta investigación.

## **CAPITULO I**

### **1. PROBLEMA**

#### **1.1 Tema:**

Técnicas spam para el envío masivo de información no deseada a las cuentas de correo electrónico de los funcionarios del Gobierno Autónomo Descentralizado Municipalidad Ambato

#### **1.2 Planteamiento del Problema:**

##### **1.2.1 Contextualización**

En la actualidad no es desconocido para nadie que las bandejas de entrada de los correos electrónicos diariamente se llenan de mensajes publicitarios, imágenes, o simplemente información no importante, a este tipo de mensajes se los ha denominado Spam, el mismo que a nivel mundial ha venido creciendo y cuyo fin no es otro más que beneficiar a la empresas con una especie de marketing que se envía la mayor número de direcciones de correo o números de teléfono obtenidas al aplicar novedosas técnicas de spam creadas por los famosos spammer;

Además de las empresas que pagan por el servicio de spam también existen los hackers que enviando un mensaje spam con código malicioso oculto pueden no solo infectar a los ordenadores de las



víctimas sino que además de ello llegan hasta apoderarse y toman el control de los sistemas que posean los ordenadores que fueron víctimas.

En algunos países ya se han venido creando nuevos métodos para contrarrestar el spam, se han creado por ejemplo filtros detectores. O leyes que sancionen a los creadores de spam; Pero esto no ha sido suficiente ya que mientras más se crean filtros detectores, los spammers inventan una nueva técnica para burlar y pasar el control de filtrado.

En nuestro país también es muy común escuchar que los usuarios de chats, blogs o correo electrónico son constantemente atacados e invadidos de spam, es debido a la falta de seguridad que se pone en las cuentas de correo, además de la irresponsabilidad de dejar la dirección de correo en blogs o chats públicos de donde los spammers obtienen sus contactos, y si se conecta desde sitios públicos es recomendable saber si el servidor no se encuentra listado en una de las famosas listas negras que contienen innumerables direcciones de servidores que carecen de seguridad en los mismos.

En el Gobierno Autónomo Descentralizado Municipalidad Ambato, los funcionarios que a diario laboran y usan diversas tecnologías de comunicación como las cuentas de correo electrónico mismas que también se han convertido en víctimas de los spammers, ya que sus bandejas han sido llenadas de correos no deseados con anuncios publicitarios a los que nunca se habían suscrito, exponiendo así información personal y laboral..

## 1.2.2 Árbol de Problemas

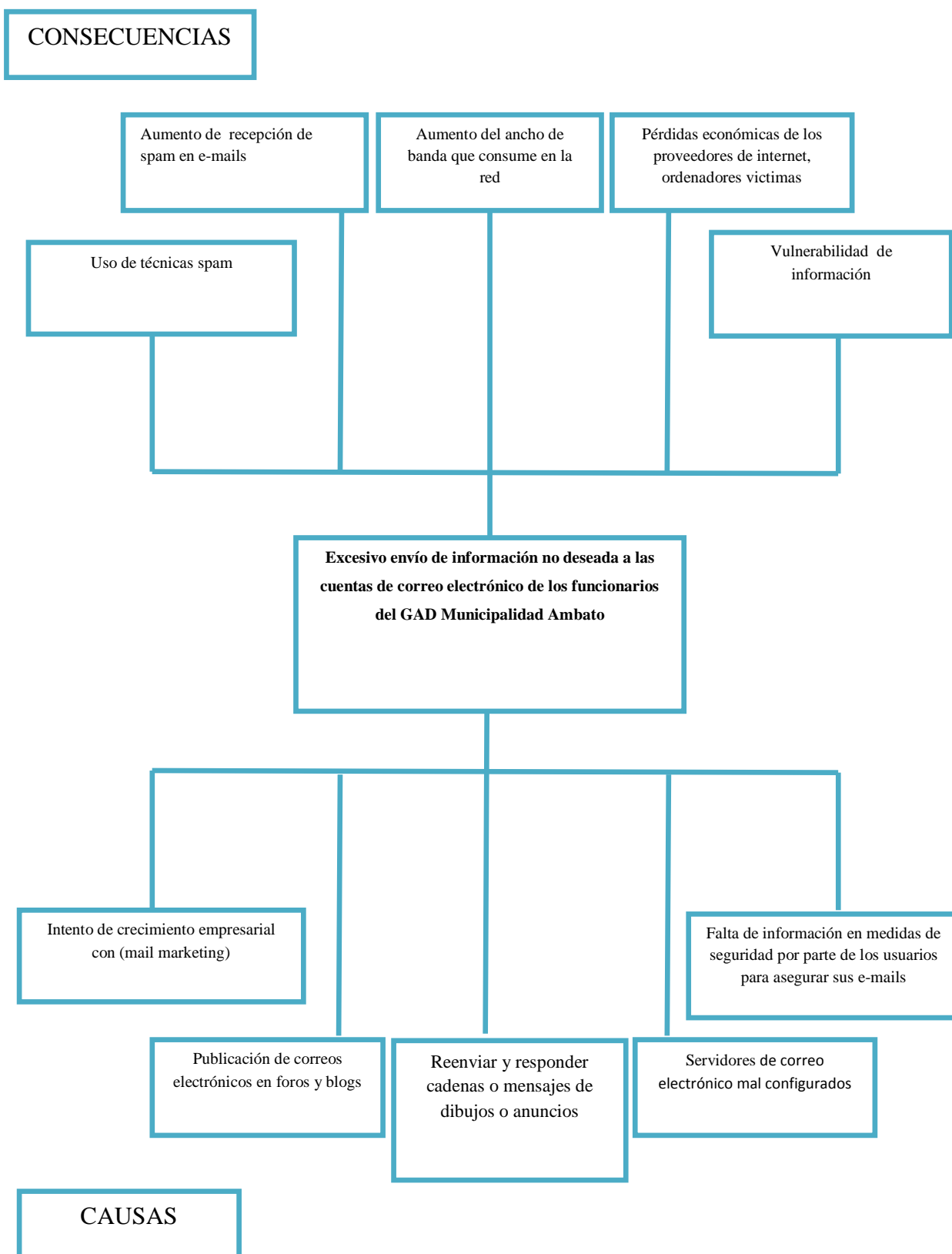


Gráfico 1. 1 Análisis Crítico

### **1.2.3 Análisis Crítico**

El intento de crecimiento empresarial a través del mail marketing crece día a día lo que provoca el uso de técnicas spam, para llegar a través de correos electrónicos a varios posibles clientes de un servicio o producto.

La constante publicación de correos electrónicos en foros y blogs por parte de miles de usuarios ocasiona también el aumento de spam.

Además los usuarios de correos electrónicos acostumbrar enviar, reenviar y responder mensajes concadenas, anuncios y dibujos sin saber que los mismos no son beneficiosos, por tal motivo se incrementa el consumo de banda ancha que tiene la red.

También la mala configuración que tienen algunos servidores de correo electrónico causa pérdidas económicas a proveedores de internet y a usuarios y propietarios de los ordenadores que han sido víctimas del spam.

Finalmente se sabe que la falta de precaución y desconocimiento de medidas de seguridad para proteger sus e-mails, por parte de los usuarios pone en riesgo no solo a su ordenador que podría ser infectado con algún código malicioso, sino también la información que tiene almacenada en su cuenta de correo electrónico, es decir existe vulnerabilidad en su información.

### **1.2.4 Prognosis**

En caso de no llegar a obtener los resultados esperados los funcionarios continuarían recibiendo información no solicitada con posible contenido malicioso o publicitario, lo que ocasionaría molestias, pérdida de tiempo y exposición de informacional de tipo laboral e institucional, esta exposición traería graves consecuencias

que afectarían directamente al GAD municipalidad Ambato el mismo que sufriría de inseguridad y desprestigio en el manejo de su información.

### **1.2.5 Formulación del Problema**

¿Cómo inciden las técnicas SPAM en el envío masivo de información no deseada a las cuentas de correo electrónico de los funcionarios del Gobierno Autónomo Descentralizado Municipalidad Ambato?

### **1.2.6 Delimitación**

Las investigación se realizó en el GAD de la ciudad Ambato, donde mediante un análisis se determinó cuáles son las técnicas más usadas para el envío de información no deseada a los usuarios de correos electrónicos.

El campo de esta investigación es científico basado en la Tecnología Informática.

Área: Seguridad Informática

Aspecto: Técnicas Spam

La información tomada para la presente investigación fue obtenida en el primer semestre del año 2012.

La presente investigación se llevó a cabo en la ciudad Ambato, en el Gobierno autónomo descentralizado Municipalidad Ambato.

### **1.2.7 Preguntas Directrices**

¿Cuáles son las técnicas spam que más afectan al GAD Municipalidad Ambato?

¿Qué tipo de información reciben los funcionarios del GADMA en sus cuentas de correo electrónico?

¿Cómo se proporcionaría seguridad para reducir el envío de información no deseada a las cuentas de correo electrónico de los funcionarios del GADMA?

### **1.3 Justificación**

El presente proyecto de investigación es de mucho interés para el investigador debido a que en la actualidad es un tema muy interesante y poco investigado dentro de nuestro país, el mismo que no ha sido la excepción al momento de recibir información basura o no solicitada por los usuarios; razón por la cual se pone a consideración el tema de este proyecto.

Para el desarrollo de la investigación se acudirá a fuentes científicas para realizar y detallar la teoría de la información obtenida; además con el fin de verificar la confiabilidad de las fuentes se realizarán prácticas con herramientas informáticas que apliquen técnicas spam en donde los destinatarios serán aquellos que consten en una amplia base de datos que conseguiremos en el desarrollo de esta práctica.

Las técnicas spam son muy utilizadas por los spammers, y llaman mucho la atención a todos aquellos que contribuyen al desarrollo de medios inteligentes que filtren o eliminen los mensajes spam, ya que mientras se crea una nueva técnica de filtrado aparece otra más novedosa para evitar los filtros y así lograr invadir las bandejas de entrada de los correos electrónicos.

A cada individuo que también usa su correo electrónico le interesa saber cómo es posible que le lleguen abundantes mensajes de contactos desconocidos, o con tanta publicidad, misma que nunca habían solicitado.

Y saber cuál es el método que usan estos atacantes de envío de spam es lo que se conseguirá al desarrollar esta investigación.

Mediante la presente investigación los lectores y beneficiarios podrán tomar medidas de prevención para evitar que sus cuentas de correo lleguen a manos de los spammers, o sean parte de largas listas de correo almacenadas en bases de datos vendidas a los mejores postores, también adquirirán información a través de un manual que estará basado en pruebas que les ayudara a conocer y comprender el proceso que tienen los mensajes basura para llegar hasta sus bandejas de entrada.

Desarrollar el tema propuesto es factible ya que se cuenta con los medios tecnológicos, humanos y económicos para llevarlo a cabo.

## **1.4 Objetivos**

### **1.4.1 Objetivo General**

Analizar las técnicas spam usadas para el excesivo envío de información no deseada a las cuentas de correo electrónico de los funcionarios del Gobierno Autónomo Descentralizado Municipalidad Ambato

### **1.4.2 Objetivos Específicos**

1. Analizar las técnicas spam que afectan las cuentas de correo electrónico de los funcionarios del GADMA.
2. Realizar un estudio del tipo de información que reciben en sus cuentas los funcionarios del GADMA.
3. Proponer un manual de seguridad que guie a los funcionarios del GADMA para disminuir el excesivo envío de información no deseada a sus cuentas de correo electrónico.

## CAPITULO II

### 2. MARCO TEÓRICO

#### 2.1. Antecedentes Investigativos:

La siguiente definición extraída de la tesis que reposa en la biblioteca virtual de universidades del Ecuador con acceso desde de la página de la “UNIVERSIDAD TECNICA DE AMBATO”.

GUZMÁN GARZÓN, Nancy, "Seguridad en el Perímetro de la Red Petroindustrial", Quito, junio 2005, con repositorio en <http://repositorio.iaen.edu.ec:9090/bitstream/123456789/351/1/IAEN-034-2005.pdf>

“**SPAM.-** El spam es el envío de mensajes electrónicos (habitualmente de tipo comercial) no solicitados y en cantidades masivas. Aunque se puede hacer por distintas vías, la más utilizada entre el público en general es la basada en el correo electrónico. El spam también puede tener como objetivo los teléfonos móviles (a través de mensajes de texto) y los sistemas de mensajería instantánea.”

En el repositorio de la tesis encontrada se ha extraído la información anterior ya que aporta de manera significativa en la definición de Spam, indicando sus características además de los términos que se involucran

directamente en la presente investigación, por ejemplo define el significado de spammer que son aquellos individuos que día a día usan técnicas de envío de información basura y así inundan las bandejas de entrada de varios usuarios de las actuales tecnologías de comunicación.

## **2.2 Fundamentación Legal:**

Constitución del estado

### **Sección tercera**

#### **Comunicación e Información**

**Art. 16.-** Todas las personas, en forma individual o colectiva, tienen derecho a:

1. Una comunicación libre, intercultural, incluyente, diversa y participativa, en todos los ámbitos de la interacción social, por cualquier medio y forma, en su propia lengua y con sus propios símbolos.
2. El acceso universal a las tecnologías de información y comunicación.
3. La creación de medios de comunicación social, y al acceso en igualdad de condiciones al uso de las frecuencias del espectro radioeléctrico para la gestión de estaciones de radio y televisión públicas, privadas y comunitarias, y a bandas libres para la explotación de redes inalámbricas.
4. El acceso y uso de todas las formas de comunicación visual, auditiva, sensorial y a otras que permitan la inclusión de personas con discapacidad.
5. Integrar los espacios de participación previstos en la Constitución en el campo de la comunicación.

**Art. 17.-** El Estado fomentará la pluralidad y la diversidad en la comunicación, y al efecto:



1. Garantizará la asignación, a través de métodos transparentes y en igualdad de condiciones, de las frecuencias del espectro radioeléctrico, para la gestión de estaciones de radio y televisión públicas, privadas comunitarias, así como el acceso a bandas libres para la explotación de redes inalámbricas, y precautelaré que en su utilización prevalezca el interés colectivo.
2. Facilitará la creación y el fortalecimiento de medios de comunicación públicos, privados y comunitarios, así como el acceso universal a las tecnologías de información y comunicación en especial para las personas y colectividades que carezcan de dicho acceso o lo tengan de forma limitada.
3. No permitirá el oligopolio o monopolio, directo ni indirecto, de la propiedad de los medios de comunicación y del uso de las frecuencias.

**Art. 18.-** Todas las personas, en forma individual o colectiva, tienen derecho a:

1. Buscar, recibir, intercambiar, producir y difundir información veraz, verificada, oportuna, contextualizada, plural, sin censura previa acerca de los hechos, acontecimientos y procesos de interés general, y con responsabilidad ulterior.
2. Acceder libremente a la información generada en entidades públicas, o en las privadas que manejen fondos del Estado o realicen funciones públicas. No existirá reserva de información excepto en los casos expresamente establecidos en la ley. En caso de violación a los derechos humanos, ninguna entidad pública negará la información.

**Art. 19.-** La ley regulará la prevalencia de contenidos con fines informativos, educativos y culturales en la programación de los medios de comunicación, y fomentará la creación de espacios para la difusión de la producción nacional independiente. Se prohíbe la emisión de publicidad que induzca a la violencia, la discriminación, el racismo, la toxicomanía, el

sexismo, la intolerancia religiosa o política y toda aquella que atente contra los derechos.

**Art. 20.-** El Estado garantizará la cláusula de conciencia a toda persona, yal secreto profesional y la reserva de la fuente a quienes informen, emitan sus opiniones a través de los medios u otras formas de comunicación, o laboren en cualquier actividad de comunicación.

## **Capítulo octavo**

### **Derechos de protección**

**Art. 75.-** Toda persona tiene derecho al acceso gratuito a la justicia y a la tutela efectiva, imparcial y expedita de sus derechos e intereses, con sujeción a los principios de inmediación y celeridad; en ningún caso quedará en indefensión. El incumplimiento de las resoluciones judiciales será sancionado por la ley.

**Art. 82.-** El derecho a la seguridad jurídica se fundamenta en el respeto ala Constitución y en la existencia de normas jurídicas previas, claras, públicas y aplicadas por las autoridades competentes.

## **Sección octava**

### **Ciencia, tecnología, innovación y saberes ancestrales**

**Art. 385.-** El sistema nacional de ciencia, tecnología, innovación y saberes ancestrales, en el marco del respeto al ambiente, la naturaleza, la vida, las culturas y la soberanía, tendrá como finalidad:

1. Generar, adaptar y difundir conocimientos científicos y tecnológicos.
2. Recuperar, fortalecer y potenciar los saberes ancestrales.

3. Desarrollar tecnologías e innovaciones que impulsen la producción nacional, eleven la eficiencia y productividad, mejoren la calidad debida y contribuyan a la realización del buen vivir.<sup>174</sup>

**Art. 386.-** El sistema comprenderá programas, políticas, recursos, acciones, e incorporará a instituciones del Estado, universidades y escuelas politécnicas, institutos de investigación públicos y particulares, empresas públicas y privadas, organismos no gubernamentales y personas naturales o jurídicas, en tanto realizan actividades de investigación, desarrollo tecnológico, innovación y aquellas ligadas a los saberes ancestrales.

**Art. 387.-** Será responsabilidad del Estado:

1. Facilitar e impulsar la incorporación a la sociedad del conocimiento para alcanzar los objetivos del régimen de desarrollo.
2. Promover la generación y producción de conocimiento, fomentar la investigación científica y tecnológica, y potenciar los saberes ancestrales, para así contribuir a la realización del buen vivir, *alsumak kawsay*.
3. Asegurar la difusión y el acceso a los conocimientos científicos y tecnológicos, el usufructo de sus descubrimientos y hallazgos en el marco de lo establecido en la Constitución y la Ley.
4. Garantizar la libertad de creación e investigación en el marco del respeto a la ética, la naturaleza, el ambiente, y el rescate de los conocimientos ancestrales.
5. Reconocer la condición de investigador de acuerdo con la Ley.

**Art. 388.-** El Estado destinará los recursos necesarios para la investigación científica, el desarrollo tecnológico, la innovación, la formación científica, la recuperación y desarrollo de saberes ancestrales y la difusión del conocimiento. Un porcentaje de estos recursos se destinará financiar proyectos mediante fondos concursables. Las organizaciones que reciban fondos públicos estarán sujetas a la rendición de cuentas y al control estatal respectivo.

## 2.3. Fundamentación Teórica

### 2.3.1. Categorías Fundamentales

Variable Independiente

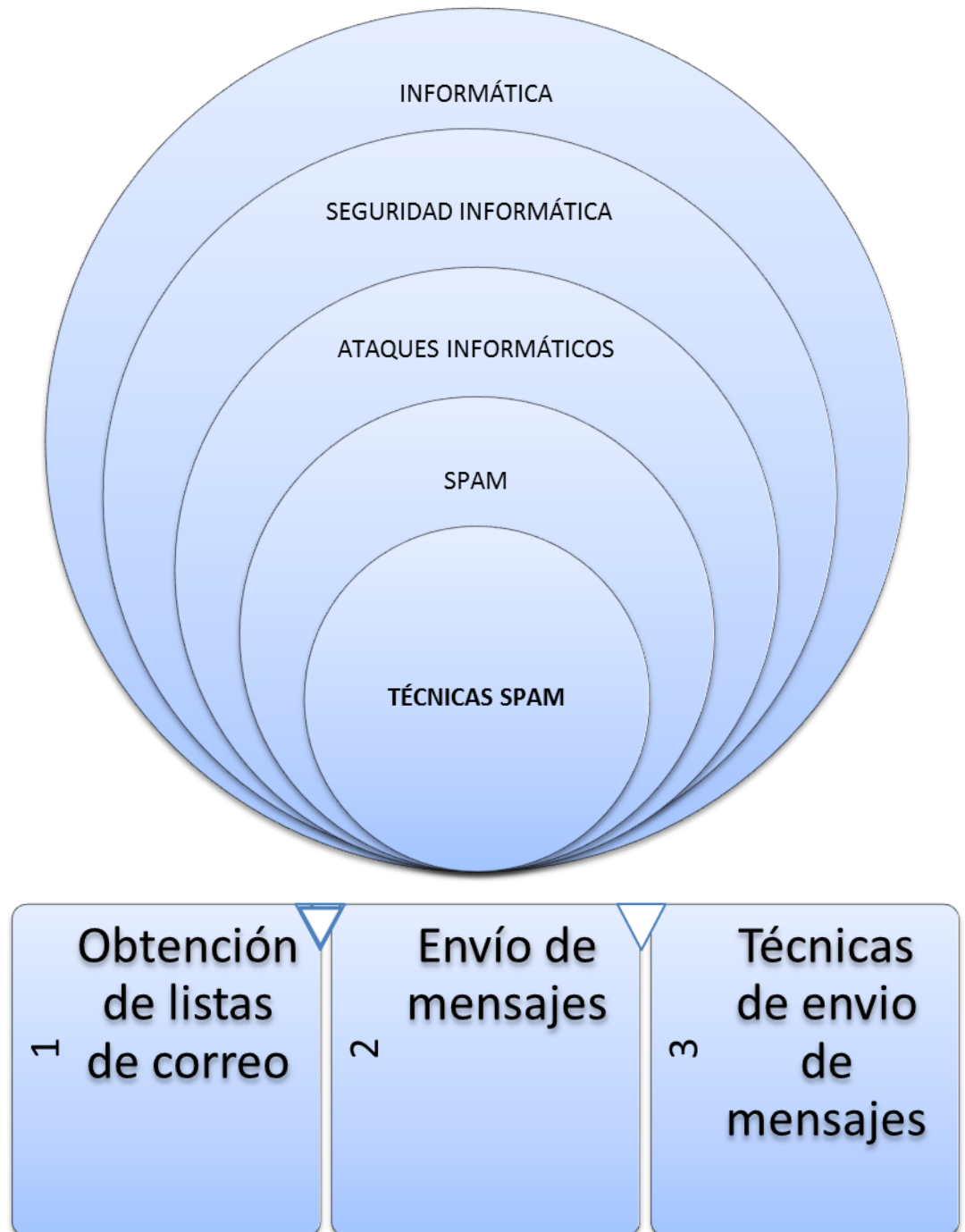


Gráfico 1. 2 Variable Independiente

Variable Dependiente

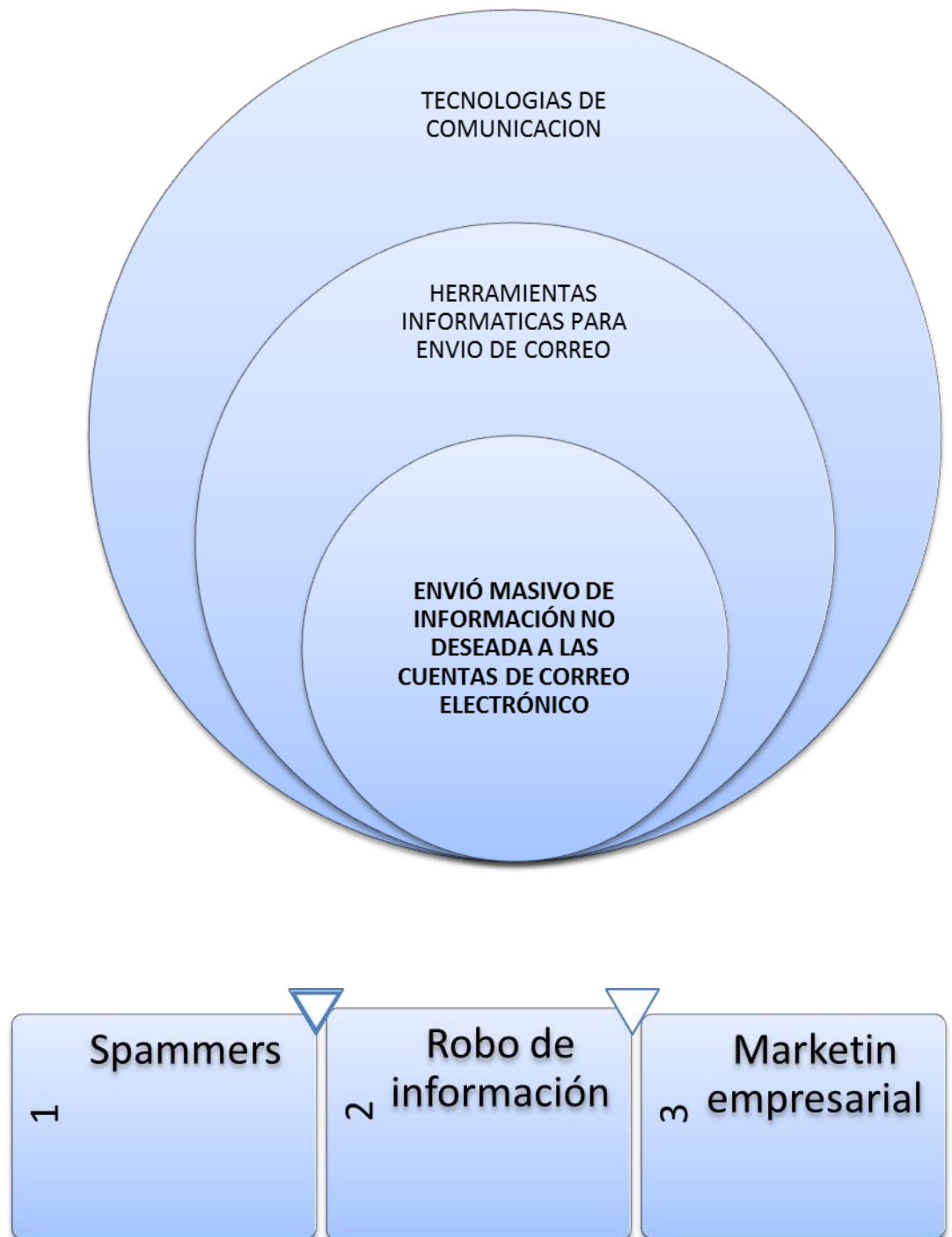


Gráfico 1. 3 Variable Dependiente

### **2.3.2. VARIABLE INDEPENDIENTE**

#### **Informática**

Según el artículo e internet publicado por su autora LANZILLOTTA, Analía(Internet; 12/02/2005,22/10/2011, 11:09) se define que:

“La informática es la ciencia que tiene como objetivo estudiar el tratamiento automático de la información a través de la computadora.

En cuanto al contenido de la Informática, se encarga de estudiar todo lo relacionado con las computadoras que incluye desde los aspectos de su arquitectura y fabricación hasta los aspectos referidos a la organización y almacenamiento de la información. Incluso contiene las cuestiones relacionadas con la robótica y la inteligencia artificial.”

Otra definición según CEJA VASQUEZ, José Raimundo, Introducción a la Informática (Internet; 22/10/2011, 12:04) dice que:

“La informática es la disciplina que estudia el tratamiento automático de la información utilizando dispositivos electrónicos y sistemas computacionales. También es definida como el procesamiento de la información en forma automática..”

Además otro autor llamado MEDINA, Antonio (Internet; 05/04/2004,22/10/2011, 11:25) redacta en su artículo lo siguiente:

La informática estudia lo que los programas pueden o no hacer (teoría de la computabilidad), de la eficiencia de los algoritmos que emplean (complejidad algorítmica, como han de organizar y almacenar los datos (estructuras/tipos de datos) y de la comunicación entre programas y humanos (interfaces de usuario y lenguajes de programación).

De las definiciones anteriores se puede resumir que la informática es la ciencia encargada de un estudio automático del procesamiento de la información, el mismo que debe ser rápido y eficaz, este puede realizarse mediante el uso de recursos tecnológicos como los ordenadores inteligentes; donde también la computación y programación van de la mano con la informática.

### **Seguridad Informática:**

Según una revista virtual de internet llamada Mastermagazine, Revista Virtual, Definición de Termino (Internet; 22/10/2011, 13:25) define que:

“Seguridad informática, técnicas desarrolladas para proteger los equipos informáticos individuales y conectados en una red frente a daños accidentales o intencionados. Estos daños incluyen el mal funcionamiento del hardware, la pérdida física de datos y el acceso a bases de datos por personas no autorizadas.”

El autor de un libro electrónico informático llamado AGUIRRE, Jorge, Universidad Politécnica de Madrid, Libro electrónico Informática (Internet; 28/02/2006,22/10/2011, 11:04) define lo siguiente:

“Un conjunto de métodos y herramientas destinados a proteger la información y por ende los sistemas informáticos ante cualquier amenaza, un proceso en el cual participan además personas. Concienciarlas de su importancia en el proceso será algo crítico”

Según la pagina web de Definición de término (Internet; 12/02/2005,01/11/2011, 15:34) se argumenta que:

“Seguridad Informática Seguridad informática, técnicas desarrolladas para proteger los equipos informáticos individuales y conectados en una red frente a daños accidentales o intencionados.”

Partiendo de las definiciones anteriormente citadas se define por Seguridad Informática a la estrategia o método denominado así debido a que se encarga mediante técnicas o procesos definidos previos a análisis ordenados y sistemáticos que tratan de proteger y resguardar la información y medios informáticos, para evitar que presenten daños o fallos ya sean físicos o lógicos.

### **Ataques informáticos:**

Se considera la definición extraída de la página web de WIKIPEDIA (Internet; 04/04/2011,02/11/2011, 10:34) donde se dice que:

“Un ataque informático es un método por el cual un individuo, mediante un sistema informático, intenta tomar el control, desestabilizar o dañar otro sistema informático (ordenador, red privada, etcétera).”

Por otra parte se toma como definición adicional la información de CARPETAANDRES10,Ataque Informático (Internet;15/02/2011, 02/11/2011, 12:34) publicación que dice:

“Un ataque informático consiste en aprovechar alguna debilidad o falla en el software, en el hardware, e incluso, en las personas que forman parte de un ambiente informático; para obtener un beneficio, por lo general de condición económica, causando un efecto negativo en la seguridad del sistema, que luego pasa directamente en los activos de la organización.”

También se presenta la definición encontrada en la página de información de WIKIPEDIA (Internet 04/04/2011, 11:03,02/11/2011, 15:45) donde se afirma que:



“Un ataque informático es un método por el cual un individuo, mediante un sistema informático, intenta tomar el control, desestabilizar o dañar otro sistema informático (ordenador, red privada, etcétera)”

Entonces se puede decir que los Ataques Informáticos son aquellos procesos o acciones que mediante el estudio de las vulnerabilidades de los ordenadores o medios que son víctimas, envían códigos o causan daños en los sistemas atacados, con el fin de apoderarse de ellos y tomar el control de los mismos; en la mayoría de los casos el dinero es el principal factor para que los atacantes informáticos sigan creando métodos sofisticados para obtener nuevas víctimas.

### **Spam**

Para el autor de la publicación encontrada en una página web MARCONE, Sandro, Que es el Spam (Internet, 28/11/2008, 06/11/11, 15:03) define que:

“El origen del término son las siglas de la frase en ingles, Simultaneously Posted Advertising Message, es decir, mensaje publicitario de publicación simultánea o masiva. En la vida cotidiana SPAM es el sinónimo de “correo basura”, “mensaje indeseado” o “correo no autorizado o no solicitado”.

Por otro lado la definición de SANZ DE LAS HERAS, Jesús, (Internet, 04/11/2011, 21:52) dice:

“El spam es un gran negocio que invade nuestros buzones. La mejora de los accesos a Internet ha incrementado el volumen del spam tanto por parte de los emisores como destinatarios. Los emisores porque disponen de más posibilidades de ancho de banda y uso de servidores propios. Los contenidos del spam son variados y difíciles de clasificar, pero es cierto que los hay de carácter fraudulento e ilegal y sobre todo molesto.”

Además otra definición de ESPECTADOR, Radio en vivo vía web, Contra el bombardeo electrónico (Internet, 03/11/2000, 06/11/11, 17:24) argumenta que:

"Spam es la denominación usada en Internet para el Correo Electrónico Comercial No Solicitado que está inundando la red. Él "spam" cuesta muy poco dinero a quien lo envía, porque la mayoría de los costos son pagados por los proveedores del sistema de Internet y los propios receptores del mensaje."

Para definir el término spam existen varias páginas, entre ellas está la definición de WIKIPEDIA, Spam(Internet 17/10/2011, 20:54,04/11/2011, 21:38) donde dice que:

“Se llama spam, correo basura o mensaje basura a los mensajes no solicitados, no deseados o de remitente no conocido, habitualmente de tipo publicitario, generalmente enviados en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptor.”

Partiendo de las definiciones anteriores se podría decir que el Simultaneously Posted Advertising Message, cuyas siglas forman el nombre SPAM llamado también correo no solicitado con información basura no es más que una estrategia comercial para las empresas que desean incrementar sus ingresos, así como también para los famosos spammers que desean enviar sus propios códigos maliciosos para apoderarse de los ordenadores de quienes lleguen a ser sus víctimas y así tomar el control y enviar más spam.

### **Técnicas Spam:**

Para el autor GIL, Manuel, Técnicas de Spam(Internet,13/08/2008, 04/11/2011, 21:12) las técnicas spam se resumen a:

“Las diferentes técnicas empleadas en la recolección de direcciones de correo validas.

E-Mail Address Harversting (Cosecha de direcciones de correo de publicaciones externas). Directory Harvest Attack (Ataques de diccionario sobre servidores de correo)

Originalmente, los spammers, enviaban el correo utilizando direcciones IP de origen conocidas, es decir; o bien sus propios sistemas; o bien, utilizaban servidores de correo de Internet, que no estaban bien configurados para prevenir su uso desde el exterior como relay's, es decir, aceptaban el relay.”

Para las empresas como para los spammers a quienes les favorece e interesa enviar su publicidad y su código malicioso, les beneficia la existencia de diversas técnicas de envío de spam, que son métodos o procesos para enviar spam, las mismas que tienen grandes ingenios para burlar los filtros de herramientas informáticas que tratan de suprimir o detectar el spam, dichas técnicas usan métodos como obtención de listas de correo, envío de mensajes, atacar a servidores proxy mal configurados, convertir ordenadores en zombis.

### **Obtención de listas de correo**

Se considera la definición de GIL, Manuel, Técnicas de Spam (Internet, 13/08/2008, 04/11/2011, 21 :12) donde argumenta que:

“E-Mail Address Harvesting es el proceso de obtener listas de direcciones de correo utilizando diversos métodos, para emplearlas en envío de correos masivos con un único fin, llenar nuestros buzones de SPAM.

La obtención de direcciones de correo a través de búsquedas realizadas en páginas WEB como pueden ser de Usenet, listas de archivos, foros,

artículos, etc... Utilizando un software conocido como "harvestingBots", "SPAMBots" o "Harvesters".

“Directory Harvest Attack Otra técnica utilizada recientemente para la obtención de direcciones de correo legítimas, son los ataques de diccionario sobre los servidores de correo, donde direcciones de correo válidas en dominios específicos son obtenidas por fuerza bruta, mediante el uso de nombres comunes en direcciones de correo dentro del dominio atacado y a través del estudio de la respuesta dada por el servidor, legitimar la dirección de correo o no.”

Por otra parte la definición de la página de WIKIPEDIA, Técnicas Spam (Internet, 03/10/2005, 07/11/2011, 00:12) dice que:

“Algunas de las principales fuentes de direcciones para luego enviar el spam son:

Las propias páginas web, que con frecuencia contienen la dirección de su creador, o de sus visitantes (en foros, weblogs, etc.).

Los grupos de noticias de usenet, cuyos mensajes suelen incluir la dirección del remitente.

Listas de correo: les basta con apuntarse e ir anotando las direcciones de sus usuarios., Correos electrónicos con chistes, cadenas, etc. que los usuarios de internet suelen reenviar sin ocultar las direcciones, y que pueden llegar a acumular docenas de direcciones en el cuerpo del mensaje. Páginas en las que se solicita tu dirección de para acceder a un determinado servicio o descarga.

Compra de bases de datos de direcciones de correo a empresas o particulares (ilegal en la mayor parte de los países).

Entrada ilegal en servidores. Por ensayo y error: se generan aleatoriamente direcciones, y se comprueba luego si han llegado los mensajes.”

Además se ha tomado en cuenta la definición de la pagina web de PANDA, Spam: mensajes de correo no solicitados (Internet, SF, 07/11/2011, 00:59) donde se define que:

“Los spammers tratan de conseguir el mayor número posible de direcciones de correo electrónico válidas, es decir, realmente utilizadas por usuarios. Con este objeto, utilizan distintas técnicas, algunas de ellas altamente sofisticadas:

Listas de correo, Compra de bases de datos de usuarios a particulares o empresas, Uso de robots (programas automáticos), que recorren Internet en busca de direcciones en páginas web, grupos de noticias, *weblogs*, etc. Técnicas de DHA (Directory Harvest Attack)”

Una vez entendidas las definiciones anteriores según sus respectivos autores la obtención de listas de correo es el proceso, método o técnica utilizados para adquirir o cosechar direcciones de correo electrónico validas usando fuentes como blogs, páginas web, cadenas de mensajes u ordenadores robots, también existe en el mercado la facilidad de comprar a supuestos proveedores de largas listas de correo almacenadas en bases de datos, todo esto con el fin de enviar spam.

### **Envío de mensajes**

Según la definición de GIL, Manuel, Técnicas de Spam (Internet, 13/08/2008, 04/11/2011, 21:12) dice:

“Los sistemas de correo abiertos, "Open Relay", es uno de los medios utilizados por los spammers para el envío de sus correos masivos. Para el propietario del servidor de relay abierto, las consecuencias son un uso excesivo del sistema atacado, consumo de recursos y ancho de banda, y para el resto de Internet, supone una fuente de correo no solicitado.

Directory Harvest Attack es utilizado por los spammers para el envío del spam y no solo para la recolección de direcciones válidas.

Otro método más lento, lo podemos encontrar en las típicas ofertas de un producto o servicio gratuito en una página WEB, que son ofrecidos simplemente con que el usuario escriba una dirección válida de correo electrónico”

Por otra parte se toma la definición de WIKIPEDIA, Técnicas Spam (Internet, 03/10/2005, 07/11/2011, 00:49) donde dice que:

“Una vez tienen una gran cantidad de direcciones de correo válidas (en el sentido de 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 internet, por consumirse gran parte del ancho de banda en mensajes basura.”

El envío de mensajes es la siguiente etapa de proceso de envío de spam, a partir de la obtención de correos, donde se utilizan herramientas de software que permiten dicho envío a las direcciones válidas obtenidas y aquellas ip detectadas previamente como vulnerables (open relay), este tipo de envío por su alta cantidad de mensajes consume un gran ancho de banda ocasionando pérdidas económicas tanto para los proveedores de internet como para los consumidores.

### **Técnicas de envío de mensajes**

La definición de FAJARDO, Javier (Internet, 02/04/2011, 16:59, 06/11/11 11:47) dice que:

“Para enviar y recibir correo electrónico, se precisa de un programa de gestión conocido como "cliente de correo electrónico", en el que se redacta el contenido y se indican las direcciones del o de los destinatarios, el mensaje de correo electrónico se envía a un servidor, que identifica el o los destinatarios y lo remite al propio servidor de correo de éstos, que es el encargado de almacenarlo hasta que el propio destinatario se conecte con

él y lo descargue en su terminal, utilizando también un software "cliente de correo electrónico; Los protocolos utilizados para el envío y recepción de correo electrónico varían según los servidores, los más comunes el SMTP (Simple Mail Transfer Protocol) para el envío y el POP3 (Post Office Protocol 3) o el IMAP (Internet Message Access Protocol) para la recepción.”

Además se toma la definición de RIVERA, Volkan, Seguridad (Internet, 01/03/2008, 07/11/11 01:47) que argumenta:

“El spammer crea cuentas de correo en los servicios de correo públicos y habilita el autoresponder y pone en el cuerpo del mismo la publicidad que quiere enviar. Luego enviar una serie de e-mails con el campo "Form" manipulado, en el cual pone la dirección e-mail de la víctima, y es la cuenta de correo legítima en el servidor público la que envía el spam de rebote.”

Se concluye que las técnicas de envío de mensajes son varias pero primero que nada se necesita tener acceso a las cuentas de correo para verificar que exista un emisor y un receptor, luego de ello se pueden aplicar técnicas tales como autoresponder a los mensajes que llegan a las bandejas de entrada enviando la publicidad o el malware que se vaya enviar, en la web existen un gran número de aplicaciones libres y pagadas disponibles para empresas y personas que deseen o necesiten enviar spam proveyéndola de listas de correo de posibles víctimas o en el caso empresas de futuros clientes.

### **2.3.3. VARIABLE DEPENDIENTE**

#### **Tecnologías de Comunicación**

La definición según el autor ROSARIO, Jimmy, "La Tecnología de la Información y la Comunicación (TIC)(Internet; 2005,04/11/2011, 20:38)

“Se denominan Tecnologías de la Información y las Comunicación al conjunto de tecnologías que permiten la adquisición, producción, almacenamiento, tratamiento, comunicación, registro y presentación de informaciones, en forma de voz, imágenes y datos contenidos en señales de naturaleza acústica, óptica o electromagnética. Las TICs incluyen la electrónica como tecnología base que soporta el desarrollo de las telecomunicaciones, la informática y el audiovisual.”

Por otro lado la definición de la página de WIKIPEDIA, Malware (Internet 03/11/2011, 07:08,04/11/2011, 20:48) argumenta que:

“Técnicas usadas para conseguir, recibir, adquirir, procesar, guardar y diseminar información numérica, textual, pictórica, audible, visible (multimedia) a través de accesorios o dispositivos basados en combinación de la microelectrónica, la computación y las telecomunicaciones.”

Además en el artículo de la pagina web de HISTLEROSE, Tecnologías De Comunicación e Historia del Mundo (Internet, 2005, 04/11/2011, 21:02) se dice que:

“Las tecnologías de comunicación crean una estructura dentro de la cual se expresen las culturas humanas. El modo de la comunicación influencia el tipo de expresión que ocurre en el "espacio" ese él ha creado.

La tecnología de comunicación permite a comunicador que puede ser separado físicamente de las audiencias para comunicarse con un número potencialmente ilimitado de personas”

Entonces se diría que las tecnologías de comunicación son todas aquellas invenciones actuales que han sido creadas con el propósito de ser intermedio de comunicación entre personas ya sea por medio de texto, imágenes o voz, sin importar las distancias en las que el emisor o receptor se encuentren; entre estas tecnologías se encuentran el internet a través de



correos electrónicos, foros, o blogs, la telefonía móvil con los diferentes celulares que permiten conexión a internet, las redes de comunicación, entre otros.

### **Herramientas Informáticas Para Envío De Correo**

Según la definición tomada de SendBlaster, Software envío spam (Internet, 2008, 07/11/11, 01:48) se dice que:

“La clave para un marketing por email ganadora es enviar emails a sus prospectos utilizando un software de correo masivo como programa de marketing por email: el software de envío de correo masivo gratis entregará automáticamente sus correos masivos personalizados a los usuarios suscriptos a sus listas de emails.”

Por otro lado según la definición de la página web de WIKIPEDIA, Email marketing (Internet, 02/11/2011, 15:27, 07/11/2011, 13:03) se define:

“El email marketing es una forma de marketing directo que utiliza el correo electrónico como un medio de comunicación de mensajes comerciales o de recaudación de fondos a una audiencia. En su sentido más amplio, cada correo electrónico enviado a un cliente potencial o actual puede ser considerado e-mail marketing

Añadir anuncios a los mensajes de correo electrónico enviados por otras compañías a sus clientes, y envío de mensajes de correo electrónico a través de la Internet, como correo electrónico y lo hace existir fuera de la Internet.”

Además la Comisión Federal de Comercio, Robots, Piratas y Spam (Internet, 06/2007, 07/11/11, 13:24) argumentan que:

“Loshackers y spammers invaden secretamente su computadora e instalan a escondidas un software que les permite acceder a su información, incluso a su programa de e-mail. Pueden espiar sus sesiones de navegación en Internet, robar su información personal y utilizar su computadora para enviar spam de contenido potencialmente ofensivo o ilegal a otras computadoras sin que su dueño se entere. Usualmente, un botnet, también llamado “ejército de zombis” (zombiearmy) está compuesto de decenas o cientos de miles de computadoras hogareñas que envían millones de mensajes electrónicos”

Luego de las definiciones anteriores se entiende que las herramientas informáticas para envío de correo son aquellas creadas con el fin de difundir a grandes escalas el spam, entre las herramientas existentes tenemos: listas de correo, software de envío de correo masivo llamado también mail marketing, ordenadores robots y servidores smtp, todas estas herramientas cuentan con opciones varias tales como envío de spam, obtención de listas de correo, y hacen posible tener control sobre sistemas u ordenadores de varias personas en el mundo, generalmente de usuarios normales que se conectan a internet a través de la web, sin que sepan que su sistema ahora sirve para aumentar la propagación de mensajes publicitarios generalmente con contenido pornográfico, medicinal y otro tipo de servicio o producto.

### **Envío masivo de información no deseada a las cuentas de correo electrónico.**

Según la definición de WIKIPEDIA, Correo Electrónico (Internet, 18/10/2011, 15:42, 07/11/11, 10:16) se dice que:

“Correo electrónico es un servicio de red que permite a los usuarios enviar y recibir mensajes y archivos rápidamente mediante sistemas de comunicación electrónicos. Principalmente se usa este nombre para

denominar al sistema que provee este servicio en Internet, mediante el protocolo SMTP. Por medio de mensajes de correo electrónico se puede enviar, no solamente texto, sino todo tipo de documentos digitales.”

En la página web de ALEGSA, Definición de cuenta de correo electrónico (Internet, 17/07/2010, 07/11/11, 10:37) se define que:

“Una cuenta de e-mail, Servicio online que provee un espacio para la recepción, envío y almacenamiento de mensajes de correo electrónico en internet. Una cuenta de e-mail se asocia a un único usuario, el cual puede acceder a su cuenta a través de un nombre de usuario y contraseña.”

Una vez determinado el concepto de información no deseada también llamada spam y de cuentas de correo electrónico se puede definir que el envío masivo de información no deseada a las cuentas de correo electrónico es el resultado de la implementación de herramientas de software que envían correo no deseado con contenido publicitario, además de posibles códigos malicioso los mismos que inciden en el aumento de spam en las cuentas de correo electrónico de usuarios que han creado sus cuentas para poder comunicarse con personas de todo el mundo a través de mensajes de texto, imágenes o voz sin importar que el destinatario esté disponible en el momento de envío.

### **Spammers**

Según el autor de la siguiente definición ALAVÉZ, Miguel (Internet, 16/06/2008,04/11/2011, 23:08) se argumenta que:

“Podemos definir a un spammer como aquella persona que roba o compra direcciones de correo electrónico y realiza el envío de correos no solicitados a estas direcciones. También, puede realizar el envío de spam a través de otras tecnologías.”

Por otro lado la definición de GONZALEZ, Raúl (Internet 28/05/2009, 04/11/2011, 23:16) dice que:

“Son individuos o empresas que envían spams y utilizan diversas técnicas para conseguir las largas listas de direcciones de correo que necesitan para su misión de propagar los correos basura.

Los spammers utilizan toda esta información personal para recopilar direcciones de e-mails y cuando envíen Spams, hacen que parezca que se envía desde los contactos directos”; lo que los convierte en un correo confiable y nos convertimos en víctimas.

El spammer también recoge información relativa a aficiones o intereses para crear mensajes con temas de interés para el usuario (se recibe desde un contacto), y esto aumenta las posibilidades de que el usuario abra ese correo malicioso y que el malware que contenga, se active.”

Entendiendo las definiciones citadas se puede concluir que aquellos individuos u organizaciones que se dedican al envío de spam son conocidos como spammers, quienes usan diversas técnicas para conseguir su objetivo que es enviar información no solicitada con contenido de tipo publicitario a varias direcciones de correo electrónico, y así propagar la información basura que en su mayoría evitan los filtros anti-spam, o apoderarse de ordenadores ajenos convirtiéndolos en zombis, para su objetivo hacen uso de herramientas informáticas diseñadas para el envío de spam.

### **Robo de Información**

Según la definición citada en la página de Strategy & Business, Tecnologías de Información (Internet, 01/09/2006, 06/11/11, 21:34), se argumenta que:

“El robo de información es una de las peores amenazas para las organizaciones; y, sin embargo, los ejecutivos le han delegado este problema a terceros.”

Por otro lado se ha tomado la definición de un Editor, Propiedad intelectual and Seguridad Informática (Internet, 29/03/2007, 06/11/2011, 23:15) donde se dice:

“Según la Business Software Alliance, organización dedicada a la promoción de un mundo digital seguro y legal, el robo de identidad y de números de tarjetas de créditos son los delitos más peligrosos que se cometen a través de Internet, lo cual califica al crecimiento del comercio y de la banca electrónicas como dos de las áreas más atractivas para los ciber-criminales, quienes pueden extraer la información financiera de una empresa o robar valiosa propiedad intelectual.”

Además para el autor ÁLVAREZ MARAÑÓN, Gonzalo, CSIC. (Internet, 1997, 07/11/11, 00:07) la definición que da es:

“En principio, todos los ordenadores contienen alguna información de interés para alguien. Es cierto que no siempre tendrá el mismo valor, pero siempre puede existir alguien interesado en conseguirla. Por consiguiente, uno de los ataques más comunes está dirigido a extraer información confidencial de un sistema”

Con las definiciones investigadas se definiría al robo de información que es considerado el delito informático más grande de la actualidad debido a que ataca a grandes y pequeñas organizaciones financieras, así como también a varios individuos que han tenido seguridades vulnerables en sus cuentas o archivos de información, y por lo mismo esta ha sido sustraída por personas dedicadas a este tipo de fraude informático, ocasionando grandes pérdidas económicas.

## **Marketing empresarial**

Según la definición encontrada en la página de SendBlaster, Software envío spam (Internet, 2008, 07/11/11, 01:16) se argumenta que:

“Marketing por email se refiere al uso del email cuyo objetivo es el de promocionar su negocio al enviar correos masivos y newsletters a personas incluidas en listas de correo masivo sobre bienes o servicios ofrecidos en su negocio.”

Por otro lado según la definición de la página de CantosConsultores,(Internet,SF,04/11/11 22:34) se dice que:

“El marketing es el conjunto de actividades que implican la organización y el intercambio de la comunicación entre la producción y el consumo. Ya no es estático, sino dinámico. Su función principal reside en orientar la empresa hacia el mercado, hacia el consumidor.”

Además la definición que da la pagina de WIKIPEDIA, Marketing (Internet 03/11/2011, 20:12,04/11/2011, 22:53) es:

“Según Philip Kotler es «el proceso social y administrativo por el que los grupos e individuos satisfacen sus necesidades al crear e intercambiar bienes y servicios. Es el arte o ciencia de satisfacer las necesidades de los clientes y obtener ganancias al mismo tiempo.”

En conclusión el marketing es la principal estrategia comercial que utilizan varias organizaciones que elaboran o desarrollan algún tipo de servicio o producto, las mismas que usan esta estrategia para ofrecer sus productos por medio de anuncios publicitarios también llamados propagandas usando diversos medios de comunicación, para así incrementar sus ingresos.

## **2.4 Hipótesis:**

El uso de técnicas spam influye en el excesivo envío de información no deseada a las cuentas de correo electrónico de los funcionarios de GAD Municipalidad Ambato.

## **2.5. Señalamiento de variables**

V. Independiente X = Técnicas Spam

V. Dependiente Y = Envío masivo de información no deseada a las cuentas de correo electrónico

## **CAPITULO III**

### **3. MARCO METODOLÓGICO**

#### **3.1 Enfoque**

El presente trabajo investigativo se enmarco con un enfoque Cualitativo - Cuantitativo por las siguientes consideraciones:

Se consideró siempre el entorno del trabajo en donde laboran cada uno de los funcionarios del gobierno autónomo descentralizado del Ilustre Municipio de Ambato además se respetan sus principios, culturas y opiniones que posee cada uno de ellos, existió un respeto mutuo entre los compañeros de trabajo sin forzarlos a realizar más trabajo de lo necesario siempre y cuando los funcionarios estén de acuerdo. La aplicación de la solución se realizó explícitamente dentro del Municipio de Ambato.

Con el estudio de técnicas spam usadas para él envió masivo de información no deseada a las cuentas de correo electrónico se definió una norma de seguridad y responsabilidad para seguirla.

#### **3.2 Modalidades básicas de la Investigación**

La presente investigación tiene las siguientes modalidades:



**Modalidad Bibliográfica o documentada:** Se ha considerado esta medidas ya que se han utilizado, diccionarios virtuales, libros, tesis de grado, internet, bibliotecas virtuales.

**Modalidad Experimental:** Se ha considerado la relación de la variable independiente técnicas spam y su influencia y relación en la variable dependiente envió masivo de información no deseada a las tecnologías de comunicación para considerar sus causas y sus efectos.

**Modalidad de Campo:** Se ha considerado esta modalidad ya que el investigador será quien recogerá la información primaria directamente de la fuente, que son los involucrados a través de una encuesta que será aplicada.

### **3.3 Tipos de Investigación**

Se ha realizado la investigación exploratoria, debido a que se permitió plantear el problema de la investigación “El uso de técnicas SPAM produce el envío masivo de información no deseada a las tecnologías de comunicación de los funcionarios del Gobierno Autónomo Descentralizado del Ilustre Municipio de Ambato”; Así mismo ésta investigación ayudó en el planteamiento de la hipótesis “La aplicación de herramientas informáticas para el envío de spam informará y prevendrá a funcionarios de Gobierno Autónomo Descentralizado del Ilustre Municipio de Ambato para evitar el envío masivo de información no deseada a sus tecnologías de comunicación”.

Se ha considerado la investigación descriptiva, ya que a través de ella se permite analizar el problema en sus partes, delimitando el tiempo y el espacio para construir el análisis crítico, la contextualización y los antecedentes investigativos de la presente investigación.

Por otro lado se ha tomado la Investigación correlacional, porque ha permitido medir la compatibilidad entre la variable dependiente envío masivo de información no deseada a las tecnologías de comunicación con la variable independiente técnicas spam.

### 3.4 Población y Muestra

En la presente investigación se estima que el número de funcionarios que laboran en el municipio de Ambato, es de 550, de ellos se tomara un grupo para aplicar las encuestas, aplicando la formula de la muestra.

#### Cálculo de la muestra:

$$N = \frac{PQN}{(N - 1)E^2/K^2 + PQ}$$

$$N = \frac{0,25(550)}{(550 - 1)0,1^2/2^2 + 0,25}$$

$$N = \frac{137}{(449)0,1^2/4 + 0,25}$$

$$N = \frac{137}{4,49/4 + 0,25}$$

$$N = \frac{137}{1.1225 + 0,25}$$

$$N = \frac{137}{1.3725}$$

$$N = 99.81$$

$$N = 100$$

### 3.5 Operacionalización de variables

Hipótesis El uso de técnicas spam influye en el excesivo envío de información no deseada a las cuentas de correo electrónico de los funcionarios de GAD Municipalidad Ambato.

Variable Independiente: técnicas Spam

Concepto	Categorías	Indicadores	Ítems	Técnicas e instrumentos
Son métodos que aplican procesos para enviar información no deseada, las técnicas usan herramientas informáticas con fines tales como obtención de listas de correo, envío de mensajes, atacar a servidores proxy mal configurados, convertir computadores en zombis.	Spammers	Ataque información	Ha sido Ud. víctima de un spammer? s/n	Encuesta a través de un cuestionario dirigido a los funcionarios del Gobierno Autónomo Descentralizado o Municipalidad Ambato
	Código malicioso	Virus Gusanos	Su sistema ha sido infectado por algún tipo de virus o gusano en los últimos meses, cuando?	
	Procesos	Obtención de listas de correo Envíos de mensajes	Cree que su cuenta es segura y no consta en listas de correos para envío de mensajes spam, porque?	
	Métodos	Técnicas	Qué tipo de técnica usa para proteger su computador?	
	Herramientas informáticas	Mail marketing	Le ha llegado a su correo alguna vez mensajes publicitarios ofreciéndole algún	

		Robots	producto o servicio?	
	correos	Pop Web	En su cuenta de correo de tipo pop o web, su bandeja electrónica se llena de mensajes de sus contactos o de remitentes desconocidos?	
	Servidores proxy	Open relays	Cuando se conecta desde lugares diferentes a su trabajo, sabe si los servidores proxy utilizados son seguros? s/n	

**Tabla 3. 1. Variable Independiente**

**Variable Dependiente:** Envió masivo de información no deseada a las cuentas de correo electrónico

Concepto	Categorías	Indicadores	Ítems	Técnicas e instrumentos
El envío masivo de información no deseada a las cuentas de correo electrónico es el resultado de la implementación de herramientas de software que envían correo no deseado con contenido publicitario, además de posibles códigos malicioso los mismos que inciden en el aumento de spam en las cuentas de correo electrónico de usuarios que han creado sus cuentas para poder comunicarse con personas de todo el mundo a través de mensajes de texto, imágenes o voz sin importar que el destinatario esté disponible en el momento de envió.	Información	Datos Imágenes Videos Mensajes Fotografías	¿El Municipio ha sufrido algún tipo de pérdida de información ya sea datos, imágenes, videos, mensajes, fotografías, etc.?	Encuesta a través de un cuestionario dirigido a los funcionarios del Gobierno Autónomo Descentralizado Municipalidad Ambato
	Herramientas de software	SMTP	¿Ah escuchado sobre alguna herramienta de software para el envío masivo de spam como el SMTP?	
	Mensajes de texto	Marketing	¿Ah recibido y reenviado alguna vez mensajes de texto con cadenas a sus contactos?	

Tabla 3. 2. Variable Dependiente

### 3.6 Recolección y análisis de la Información

<b>Secundaria</b>	<b>Primaria</b>
Se recolecta de estudios realizados anteriormente.	Se recolecta directamente del contacto con los usuarios de las tecnologías de comunicación del Gobierno Autónomo Descentralizado del Ilustre Municipio de Ambato.
Se encuentra registrada en documentos y material impreso: libros, revistas especializadas, informes técnicos, tesis de grado, bibliotecas virtuales, etc.	
Las fuentes de información son: bibliotecas de la facultad, internet, repositorios de tesis.	

#### Técnicas de Investigación

Bibliográficas	De Campo
El análisis de documentos (lectura científica)	
El fichaje	
Encuestas	La Encuesta

#### Recolección de la información

Preguntas	Explicación
1. ¿Preguntas?	Recolectar información primaria para comprobar y contrarrestar con la hipótesis, realizando y aplicando pruebas.
2. ¿A qué personas o sujeto?	La información será tomada de los funcionarios que laboran en el Gobierno Autónomo Descentralizado del Ilustre

	Municipio de Ambato.
3. ¿Sobre qué aspectos?	VI: Técnicas Spam VD: Envío masivo de información no deseada a las tecnologías de comunicación
4. ¿Quién?	La Investigadora
5. ¿Cuándo?	De acuerdo al cronograma establecido
6. ¿Lugar de recolección de información?	Gobierno Autónomo Descentralizado del Ilustre Municipio de Ambato.
7. ¿Cuántas veces?	Una sola vez
8. ¿Qué técnica de recolección?	Encuesta
9. ¿Con que?	Cuestionario
10. ¿En qué situación?	Situación normal y cotidiana

### **3.7 Procesamiento y Análisis de la Información**

#### **Revisión y codificación de la información**

Recolectar y organizar la información

#### **Categorización y tabulación de la información**

Tabulación a través de la herramienta Microsoft Excel.

#### **Análisis de los datos**

La interpretación de los datos se lo hará en gráficos y tablas para analizarlos e interpretarlos.

#### **Interpretación de los resultados**

Descripción de los resultados

Analizar la hipótesis en relación con los resultados obtenidos para verificarla o rechazarla.

Estudiar cada uno de los resultados por separado

Redactar una síntesis general de los resultados

## **3.8. MARCO ADMINISTRATIVO**

### **3.8 Recursos**

#### **3.8.1 Institucionales**

Gobierno Autónomo Descentralizado del Ilustre Municipio de Ambato.

#### **3.8.2 Humanos**

Investigador: Verónica Jazmina Silva Mena

Investigados: Funcionarios del Gobierno Autónomo Descentralizado Municipalidad Ambato.

Asesor: Dr. Msc. Mauricio Tamayo

Tutor: Ing. Luis Solís

#### **3.8.3 Materiales**

Ordenador

Útiles de escritorio (Papel bond, lápices, borrador, Flash memory, folders, impresiones)

##### **Tecnológicos:**

Dominio + hosting

Internet

Herramientas de software para envío de spam

##### **Indirectos:**

Transporte

Alimentación

#### **3.8.4 Económicas**

Estos serán financiados por el investigador y será el valor planteado en el presupuesto.



### 3.9 Presupuesto

A. RECURSOS MATERIALES				
N°.	DENOMINACION	TIEMPO	V UNITARIO	TOTAL
	Útiles de escritorio	6 meses	50,00	300,00
	Internet	6 meses	25,00	150,00
	Computador		880,00	880,00
	Herramientas Software	6 meses	20,00	120,00
	Dominio mas hosting		50,00	50,00
	Subtotal			1.500,00

B. OTROS				
N°.	DENOMINACION	TIEMPO	V UNITARIO	TOTAL
	Movilización	6 meses	30,00	180,00
	Alimentación	6 meses	30,00	180,00
	Subtotal			360,00
	TOTAL			1860,00

## **CAPITULO IV**

### **4. ANÁLISIS E INTERPRETACIÓN DE LOS RESULTADOS**

#### **4.1 ANALISIS DE LA INFORMACIÓN**

Lo que la institución necesita básicamente es tratar de evitar en lo posible la recepción de spam, adoptando medidas de prevención para ello, por lo que primero se desea saber qué tipo de información no importante es la que reciben continuamente, que tipo de errores cometen para incrementar la recepción de spam, que tan informados están acerca del tema, además de saber si su configuración de conexión es la más adecuada.

Para obtener todos estos datos se aplico una encuesta, misma que se encuentra como anexo en esta investigación.

Una vez obtenido los datos requeridos se procedió al análisis e interpretación de los resultados.

## 4.2. INTERPRETACIÓN DE LOS RESULTADOS

1. Ha sido Ud. víctima de un spammer?

N°	ITEMS	FRECUENCIA	%
1	SI	29	29
2	NO	71	71
Total		100	100

Tabla 4. 1. Frecuencia de la pregunta N° 1

Fuente: Estudio de Campo

Autor: Jazmina Silva

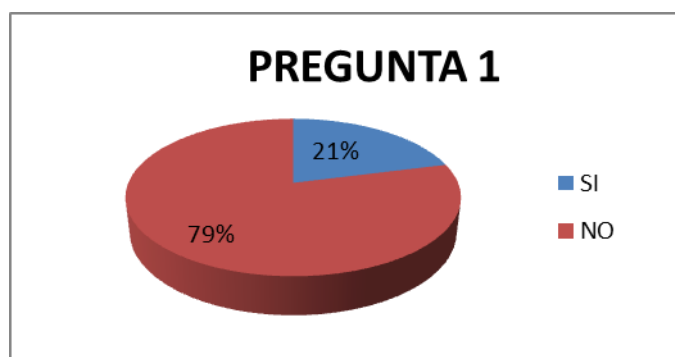


Gráfico 4. 1 Víctima de Spammer

Fuente: Estudio de Campo

Autor: Jazmina Silva

### INTERPRETACIÓN

Cuantitativo:

De los 100 encuestados el 21% que representa 29 personas indicó que ha sido víctima de un spammer; mientras que el 79% que representa 71 personas indicó no han sido víctimas de algún tipo de spammer.

Cualitativo:

Por lo tanto se considera lo que indica el autor Miguel Alvares, que un spammer roba o compra direcciones de correo electrónico y realiza el envío de correos no solicitados a estas direcciones.

#### CONCLUSIÓN

En el GAD municipalidad Ambato algunos correos electrónicos de los funcionarios han recibido spam.

#### RECOMENDACIÓN

Para seguridad de los funcionarios se debe mejorar la seguridad en sus correos electrónicos.

2. Su sistema ha sido infectado por algún tipo de virus o gusano en los últimos meses?

N°	ITEMS	FRECUENCIA	%
1	Virus	57	57
2	Gusano	15	15
	virus y gusano	14	14
	No	14	14
Total		100	100

Tabla 4. 2 Frecuencia pregunta 2

Fuente: Estudio de Campo

Autor: Jazmina Silva

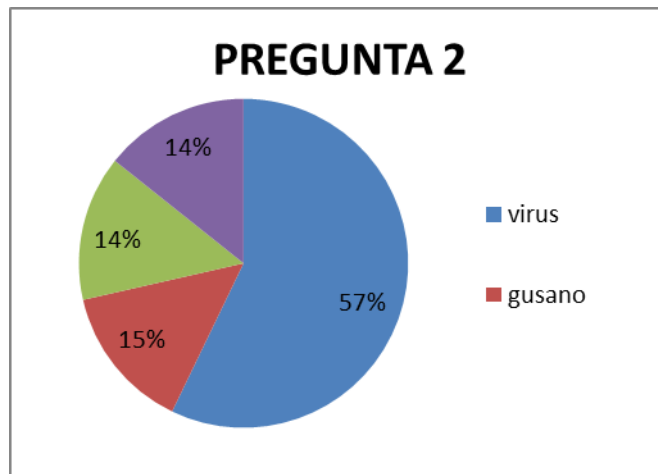


Gráfico 4. 2 Infección de virus

Fuente: Estudio de Campo

Autor: Jazmina Silva

## INTERPRETACIÓN

Cuantitativo:

De los 100 encuestados el 57% que representa 57 personas indicaron que ha sido infectado únicamente por virus; el 15% que representa 15 personas indicaron que ha sido infectado gusanos únicamente, mientras que 14 personas que equivale al 14% ha sido infectado por virus y gusanos, mientras que 14 personas indicaron que no han sido afectadas ni por virus ni por gusanos.

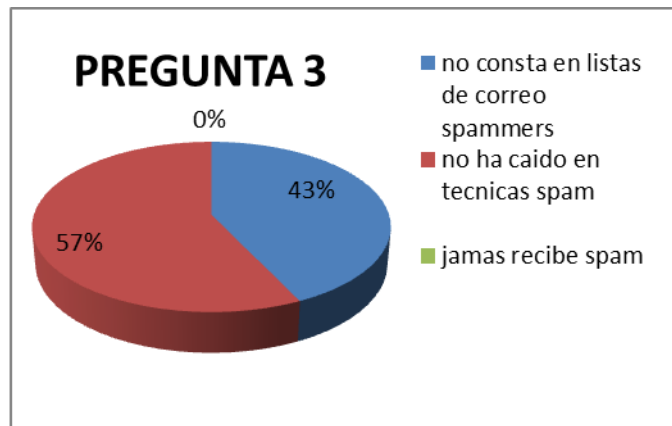
3. Cree que su cuenta es segura y no consta en listas de correos para envío de mensajes spam, porque?

N°	ITEMS	FRECUENCIA	%
1	no consta en listas de correo spammers	43	43
2	no ha caído en técnicas spam	57	57
3	jamás recibe spam	0	0
Total		100	100

**Tabla 4. 3.** Frecuencia pregunta 3

Fuente: Estudio de Campo

Autor: Jazmina Silva



**Gráfico 4. 3** Listas de Correo spam

Fuente: Estudio de Campo

Autor: Jazmina Silva

### INTERPRETACIÓN

Cuantitativo:

De los 100 encuestados el 43% que representa 43 personas indicó que su cuenta es segura porque no consta en listas de correo; mientras que el 57% que representa 57 personas indicó que su cuenta es segura porque no ha caído en técnicas spam.

Cualitativo:

Por lo tanto se considera lo que indica la pagina web de Panda, que los spammers tratan de conseguir el mayor número posible de direcciones de correo electrónico válidas, es decir, realmente utilizadas por usuarios.

#### CONCLUSIÓN

En el GAD municipalidad Ambato los funcionarios piensan que sus cuentas de correo electrónico están seguras porque usan algún tipo de método para saberlo.

#### RECOMENDACIÓN

Para seguridad de los funcionarios se debe verificar que su cuenta no consta en listas negras, existen algunas páginas que ayudan a saber si la cuenta de correo es segura.

4. Qué tipo de técnica usa para proteger su computador?

N°	ITEMS	FRECUENCIA	%
1	Antivirus	28	28
2	firewall activado	0	0
3	restricción a sitios web inseguros	0	0
4	antivirus y firewall	14	14
5	antivirus y restricciones	29	29
6	todos los anteriores	29	29
Total		100	100

Tabla 4. 4. Frecuencia pregunta 4

Fuente: Estudio de Campo

Autor: Jazmina Silva

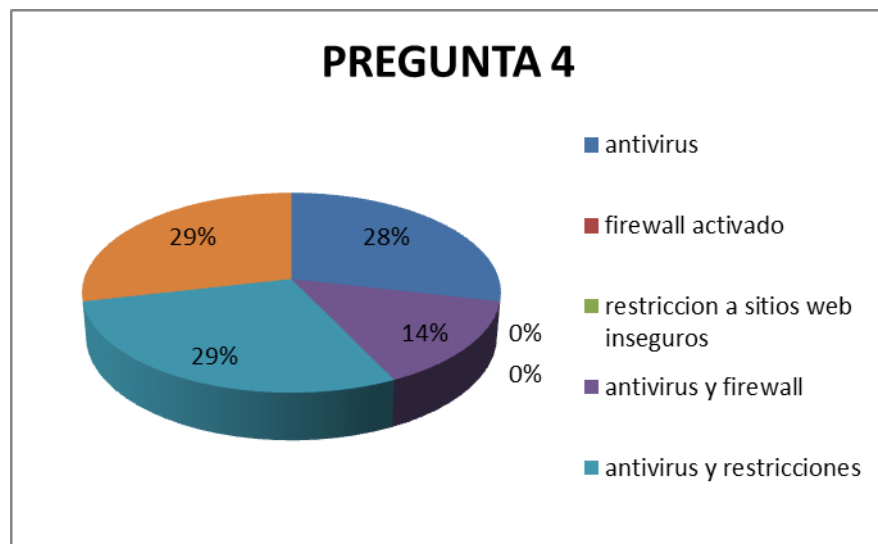


Gráfico 4. 4 Técnicas de protección del computador

Fuente: Estudio de Campo

Autor: Jazmina Silva



## INTERPRETACIÓN

### Cuantitativo:

De los 100 encuestados el 28% que representa 28 personas indicó que para proteger sus computadores utiliza únicamente un antivirus; mientras que el 14% que representa 14 persona indico que combina la protección de un antivirus más el firewall activado, otro 29% señalo que usa la protección de combinar el antivirus y restricciones a sitios web inseguros; mientras el 29% restante señalo que usa todas la opciones de seguridad anteriores.

## CONCLUSIÓN

En el GAD municipalidad Ambato los funcionarios usan en común para proteger su computador un antivirus, además de otros métodos conocidos.

## RECOMENDACIÓN

Para seguridad de los equipos con los que trabajan los funcionarios se debe mantener actualizado su antivirus y establecer normas de seguridad para brindar protección a cada equipo.

5. Le ha llegado a su correo alguna vez mensajes publicitarios ofreciéndole algún producto o servicio?

N°	ITEMS	FRECUENCIA	%
1	productos farmacéuticos	0	0
2	servicios de pornografía	0	0
3	servicios de viajes y turismo	0	0
4	tecnología	14	14
5	servicios de turismo y tecnología	43	43
6	productos farmacéuticos, turismo, tecnología	29	29
8	todos los anteriores	14	14
Total		100	100

Tabla 4. 5 Frecuencia pregunta 5

Fuente: Estudio de Campo

Autor: Jazmina Silva

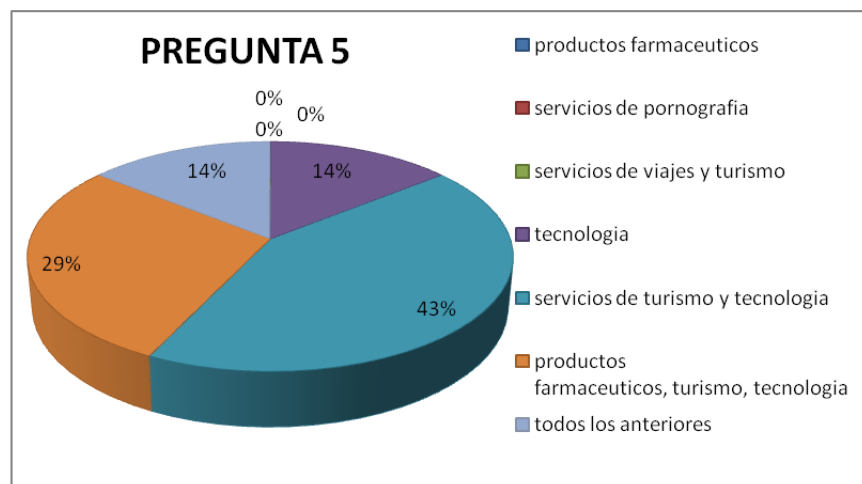


Gráfico 4. 5 Tipo de información spam

Fuente: Estudio de Campo

Autor: Jazmina Silva

## INTERPRETACIÓN

### Cuantitativo:

De los 100 encuestados el 14% que representa 14 personas indicó el tipo de información publicitaria que ha recibido es de tecnología; el 43% indicó que han recibido anuncios con contenido de tecnología y servicios de turismo y viajes, el 29% que equivale a 29 personas señaló que los anuncios que reciben contienen información de tecnología, turismo y medicina; mientras que el 14% señaló que ha recibido todo tipo de información publicitaria anteriormente mencionada.

## CONCLUSIÓN

En el GAD municipalidad Ambato los funcionarios han recibido varios anuncios con toda clase de información referente a turismo, pornografía, medicina y tecnología.

## RECOMENDACIÓN

Para evitar recibir información no solicitada se recomienda no abrir los mensajes de tipo spam, además de marcarlos como no deseados.

6. En su cuenta de correo de tipo pop o web, su bandeja electrónica se llena de mensajes de sus contactos o de remitentes desconocidos?

N°	ITEMS	FRECUENCIA	%
1	POP	0	0
2	WEB	100	100
Total		100	100

**Tabla 4. 6** Frecuencia pregunta 6a

Fuente: Estudio de Campo

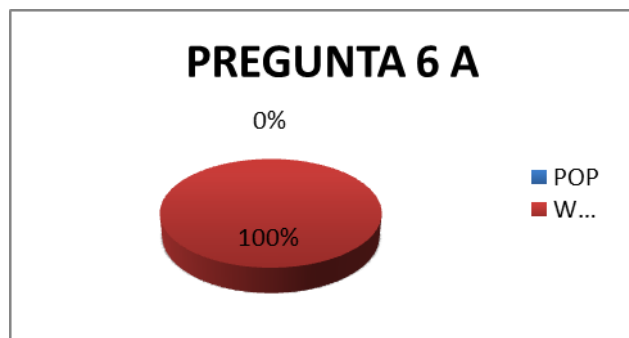
Autor: Jazmina Silva

N°	ITEMS	FRECUENCIA	%
3	remitentes desconocidos	71	71
4	remitentes conocidos	29	29
Total		100	100

**Tabla 4. 7** Frecuencia pregunta 6b

Fuente: Estudio de Campo

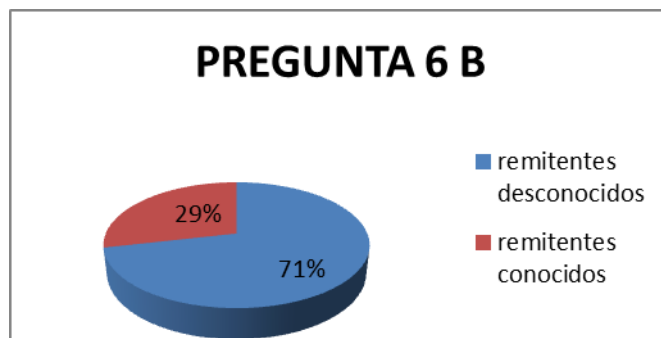
Autor: Jazmina Silva



**Gráfico 4. 6** Servidor pop

Fuente: Estudio de Campo

Autor: Jazmina Silva



**Gráfico 4. 7 Remitentes desconocidos**

Fuente: Estudio de Campo

Autor: Jazmina Silva

### INTERPRETACIÓN

Cuantitativo:

De los 100 encuestados el 100% que representa a todas las 100 personas indicó que su cuenta de correo es de tipo web;

Además se supo que el 71% que representa a 71 reciben mensajes que llenan su bandeja de entrada proveniente de remitentes desconocidos; mientras que el 29% indicó que han recibido mensajes de remitentes conocidos.

### CONCLUSIÓN

En el GAD municipalidad Ambato los funcionarios utilizan cuentas de correo electrónico de tipo pop, a pesar de ello más del 70% de ellos reportan que sus bandejas de entrada se llenan con mensajes de remitentes desconocidos.

### RECOMENDACIÓN

Para evitar que sus bandejas de entrada se llenen de información no deseada de remitentes desconocidos, se recomienda no suscribirse a cualquier tipo de anuncio en la web, y ser meticuloso al momento de compartir su dirección e-mail.

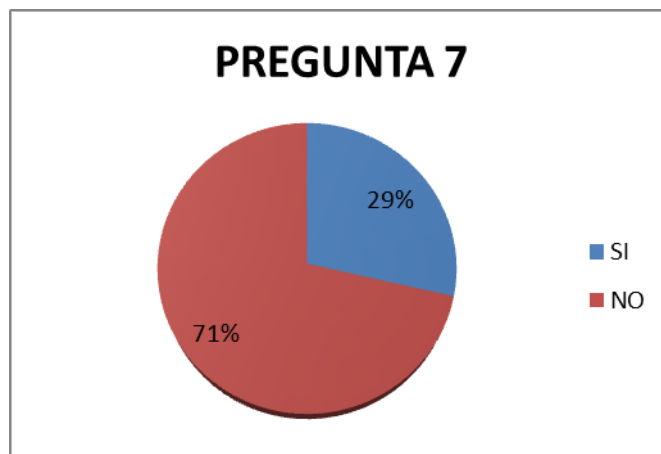
7. Cuando se conecta desde lugares diferentes a su trabajo, sabe si los servidores proxy utilizados son seguros?

N°	ITEMS	FRECUENCIA	%
1	SI	29	29
2	NO	71	71
Total		100	100

**Tabla 4. 8** Frecuencia pregunta 7

Fuente: Estudio de Campo

Autor: Jazmina Silva



**Gráfico 4. 8** Servidor proxy inseguro

Fuente: Estudio de Campo

Autor: Jazmina Silva

## INTERPRETACIÓN

### Cuantitativo:

De los 100 encuestados el 71% que representa a 71 personas indicaron que no saben si los servidores proxy desde donde se conectan son seguros o no; reciben mensajes que llenan su bandeja de entrada proveniente de remitentes desconocidos; mientras que el 29% indicó que han recibido mensajes de remitentes conocidos.

## CONCLUSIÓN

En el GAD municipalidad Ambato los funcionarios utilizan cuentas de correo electrónico de tipo pop, a pesar de ello más del 70% de ellos reportan que sus bandejas de entrada se llenan con mensajes de remitentes desconocidos.

## RECOMENDACIÓN

Para evitar que sus bandejas de entrada se llenen de información no deseada de remitentes desconocidos, se recomienda no suscribirse a cualquier tipo de anuncio en la web, y ser meticuloso al momento de compartir su dirección e-mail.

8. El Municipio ha sufrido algún tipo de pérdida de información?

N°	ITEMS	FRECUENCIA	%
1	Datos	15	15
2	Imágenes	0	0
3	Videos	0	0
4	mensajes vía mail	57	57
5	datos y mensajes vía mail	14	14
6	No	14	14
Total		100	100

Tabla 4. 9 Frecuencia pregunta 8

Fuente: Estudio de Campo

Autor: Jazmina Silva

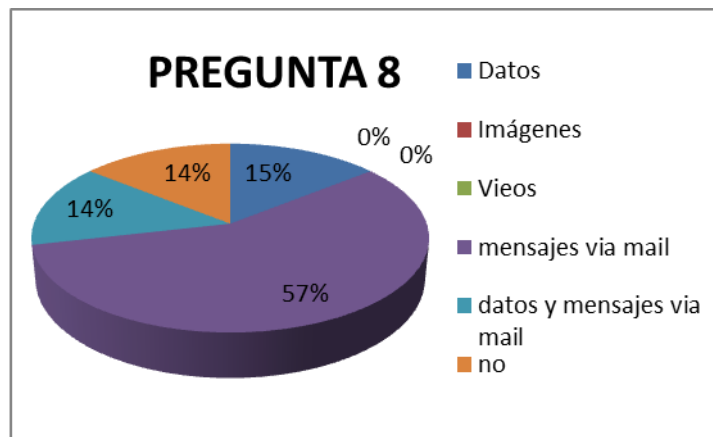


Gráfico 4. 9 Pérdida de Información

Fuente: Estudio de Campo

Autor: Jazmina Silva

## INTERPRETACIÓN

Cuantitativo:

De los 100 encuestados el 57% que representa a 57 personas indicaron que en su mayoría la información que ha perdido ha sido por mensajes vía mail; además el 14% que representa a 14 personas indicaron que la información que ha perdido se trata de datos que tenía



en su ordenador; mientras que otro 14% señalo que ha perdido datos y mensajes vía mail.

#### CONCLUSIÓN

En el GAD municipalidad Ambato cada funcionario ha reportado que ha sufrido pérdidas de información, siendo en su mayoría mensajes vía mail y datos de sus ordenadores.

#### RECOMENDACIÓN

Para evitar que los mensajes de correo electrónico que los funcionarios envíen se recomienda que verifiquen las direcciones a la que se desea que lleguen los mensajes.

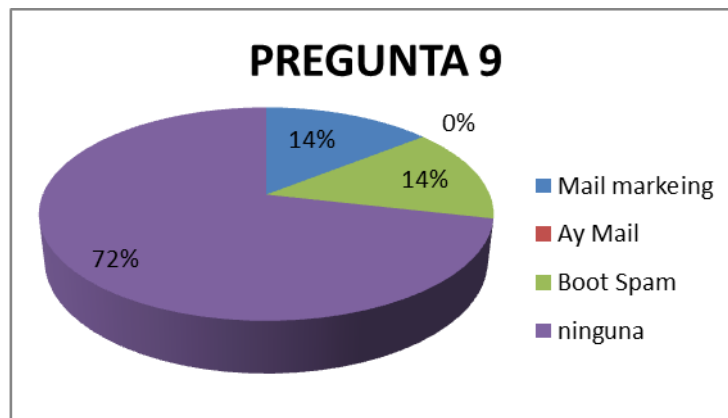
9. ¿Ah escuchado sobre alguna herramienta de software para el envío masivo de spam?

N°	ITEMS	FRECUENCIA	%
1	Mail marketing	14	14
2	Ay Mail	0	0
3	Boot Spam	14	14
4	Ninguna	72	72
Total		100	100

**Tabla 4. 10** Frecuencia pregunta 9

Fuente: Estudio de Campo

Autor: Jazmina Silva



**Gráfico 4. 10** Pérdida de Información

Fuente: Estudio de Campo

Autor: Jazmina Silva

### INTERPRETACIÓN

Cuantitativo:

De los 100 encuestados el 72% que representa a 72 personas indico que desconocen acerca de herramientas software que envíen mensajes spam, el 14% que representa 14 personas señalo que conoce del famoso mail marketing: mientras que otro 14% indico que solo ha escuchado acerca del boot spam.

## CONCLUSIÓN

En el GAD municipalidad Ambato la mayoría de los funcionarios desconocen acerca de herramientas de envío masivo de spam.

## RECOMENDACIÓN

Para evitar caer en técnica de envío de mensajes a través de herramientas software se recomienda informarse y capacitarse a cada funcionario, para aumentar el nivel de seguridad de su información.

10. ¿Ah recibido y reenviado alguna vez mensajes de texto con cadenas a sus contactos?

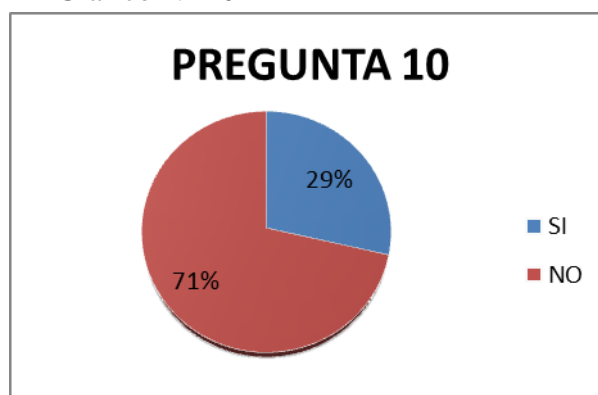
N°	ITEMS	FRECUENCIA	%
1	SI	71	71
2	NO	29	29
Total		100	100

**Tabla 4. 11** Frecuencia pregunta 10

Fuente: Estudio de Campo

Autor: Jazmina Silva

Grafico N° 10



**Gráfico 4. 11** Envío de mensajes con cadenas

Fuente: Estudio de Campo

Autor: Jazmina Silva

#### INTERPRETACIÓN

Cuantitativo:

De los 100 encuestados el 71% que representa a 71 personas indicó que si han enviado mensajes de cadenas de texto; mientras que el 29% indico que no lo ha hecho.

#### CONCLUSIÓN

En el GAD municipalidad Ambato la mayoría de funcionarios ha caído en la técnica de spam que se trata de enviar o reenviar mensajes con cadenas a sus contactos.

### RECOMENDACIÓN

Para evitar propagar el spam se recomienda evitar enviar o responder a mensajes con cadenas difundidas a través de mensajes vía mail.

### 4.3. Comprobación de Hipótesis

Se ha tomado en cuenta las preguntas discriminantes que nos llevaron a la comprobación de la hipótesis planteada, estas son:

Pregunta 5: Le ha llegado a su correo alguna vez mensajes publicitarios ofreciéndole algún producto o servicio?

N°	ITEMS	FRECUENCIA	%
1	productos farmacéuticos	0	0
2	servicios de pornografía	0	0
3	servicios de viajes y turismo	0	0
4	Tecnología	14	14
5	servicios de turismo y tecnología	43	43
6	productos farmacéuticos, turismo, tecnología	29	29
8	todos los anteriores	14	14
Total		100	100

Pregunta 6: En su cuenta de correo de tipo pop o web, su bandeja electrónica se llena de mensajes de sus contactos o de remitentes desconocidos?

N°	ITEMS	FRECUENCIA	%
1	POP	0	0
2	WEB	100	100
Total		100	100

N°	ITEMS	FRECUENCIA	%
3	remitentes desconocidos	71	71
4	remitentes conocidos	29	29
Total		100	100

Pregunta 8: El Municipio ha sufrido algún tipo de pérdida de información?

N°	ITEMS	FRECUENCIA	%
1	Datos	15	15
2	Imágenes	0	0
3	Videos	0	0
4	mensajes vía mail	57	57
5	datos y mensajes vía mail	14	14
6	No	14	14
Total		100	100

Entonces se tomo en cuenta tres preguntas discriminantes, la número 5, 6 y la número 10 de la encuesta aplicada, ya que de los resultados arrojados, se puede decir que la falta de seguridad y conocimiento en técnicas de seguridad para no caer en técnicas spam aumentan la recepción de spam en los correos electrónicos de los funcionarios del municipio, además de exponer la información y datos que se maneja dentro del GADMA.

## **CAPITULO V**

### **5. CONCLUSIONES Y RECOMENDACIONES**

El presente capítulo comprende las conclusiones y recomendaciones fundamentales en los resultados presentados y analizados conforme a los objetivos de estudio.

#### **5.1. CONCLUSIONES**

- Los funcionarios del gobierno autónomo descentralizado municipalidad Ambato reportan que el 100% de ellos ha recibido por lo menos un mensaje con anuncios de tipo spam, lo que muestra el alto índice de recepción de spam que las cuentas de correo electrónico poseen.
- Se supo que todos los funcionarios utilizan correos electrónicos de tipo web para comunicarse, los mismos que a pesar de tener seguridades por defecto, no son suficientes para contrarrestar las técnicas de spam que actualmente existen.
- Se ha determinado que más del 70% de los correos electrónicos que llenan las bandejas de entrada de los funcionarios, provienen de remitentes desconocidos, clara muestra de la elevada recepción de spam en sus mails.
- Mas del 50% de funcionarios han sufrido pérdidas de información enviándola vía mails, lo que afecta a la seguridad de la información con la que en el gobierno autónomo descentralizado trabaja.

- Al no contar con un manual de seguridad que guíe a los funcionarios, para asegurar sus cuentas de correo electrónico y evitar caer en técnicas spam, se pone en riesgo la información que se maneja dentro de la institución, teniendo alto índice de vulnerabilidad de información.

## **5.2. RECOMENDACIONES**

- En vista del alto índice de recepción de spam a través de mensajes electrónicos con anuncios que reciben los funcionarios, se recomienda no dejar publicadas sus cuentas de correo en páginas de acceso público como foros, blogs, etc. ya que esto aumenta la posibilidad de recepción de información no solicitada.
- Se recomienda incrementar el nivel de seguridad que traen por defecto las cuentas de correo electrónico, ya que esto ayudara a brindar mayor seguridad en las cuentas de cada funcionario.
- Además se recomienda que se marque como spam todo tipo de mensaje que provenga de un contacto desconocido, esto ayudara a filtrar los mensajes que se reciben y almacenan en las bandejas de entrada.
- Tomar las respectivas precauciones para evitar la pérdida de información vía mails, haciendo constantes monitoreos del funcionamiento de la red y del servidor de correos que se utilice en el GAD Municipalidad Ambato.
- Se recomienda contar con un manual para contrarrestar las técnicas spam para el envío masivo de información no deseada a las cuentas de correo electrónico de los funcionarios del gobierno autónomo descentralizado municipalidad Ambato.



## **CAPITULO VI**

### **6. PROPUESTA**

#### **6.1. DATOS INFORMATIVOS**

- Título  
Técnicas spam para el envío masivo de información no deseada a las cuentas de correo electrónico de los funcionarios del Gobierno Autónomo Descentralizado Municipalidad Ambato.
- Institución ejecutora  
Gobierno Autónomo Descentralizado Municipalidad Ambato
- Director de tesis  
Ing. Luis Solís
- Beneficiario  
Funcionarios del Gobierno Autónomo Descentralizado Municipalidad Ambato
- Ubicación  
Ambato calles Bolívar y Castillo
- Tiempo estimado para la ejecución
  - Fecha de inicio: Enero 2012
  - Fecha de finalización: Junio 2012
- Equipo técnico responsable
  - Jazmina Silva

## **6.2. ANTECEDENTES DE LA PROPUESTA**

En el último año dentro del Gobierno autónomo descentralizado Municipalidad Ambato se ha incrementado el porcentaje de recepción de información no solicitada, misma información que llena las bandejas de entrada de correos electrónicos de muchos de los funcionarios que laboran en esta municipalidad; Además de ello se ha reportado que más de la mitad de funcionarios ha sufrido pérdidas de información, sobre todo al enviarla por mails.

Para contrarrestar todo este tipo de inconvenientes que vienen afectando a los funcionarios se ha sugerido que los mismos no publiquen sus cuentas de correo en páginas de acceso público como foros, blogs, etc. además de incrementar el nivel de seguridad que traen por defecto sus cuentas de correo electrónico, tomando en cuenta que deberán marcar como spam todo tipo de mensaje que provenga de un contacto desconocido, y así evitar exponerse a técnicas spam, y posibles pérdidas de información; Ya que por el momento no cuentan con un manual de seguridad para evitar caer en técnicas spam de envío de información no solicitada a cuentas de correo electrónico.

## **6.3 JUSTIFICACIÓN**

El análisis de las técnicas spam usadas para el excesivo envío de información no deseada a las cuentas de correo electrónico es una investigación necesaria que ayudara a los funcionarios del Gobierno Autónomo Descentralizado Municipalidad Ambato y aportará en gran magnitud a brindar seguridad en la información que se maneja dentro del Municipio, para ello se contempla los siguientes aspectos:

- **Se dará a conocer nuevas técnicas de envío de spam**

Lo que se logrará es dar a conocer a los funcionarios cuales son las nuevas técnicas spam que existen, cómo funcionan y en qué medida afecta a los correos electrónicos, ya que este es el medio de comunicación más usado actualmente.

- **Evitará la introducción de spammers**

Con la información adquirida, los funcionarios tendrán más precaución al exponer su cuenta de correo, y adoptaran medidas de seguridad para evitar caer en el spam.

- **Brindará seguridad a la información manejada**

Se adoptarán medidas de prevención y corrección para garantizar la seguridad de la información que se reciba en las cuentas de correo electrónico; mismos métodos que serán implementados en el lugar y el tiempo que se considere pertinente.

- **Incrementará de seguridad en los correos electrónicos**

Se incrementaran las políticas de seguridad, reglas y normas internas de la municipalidad necesaria, misma que impedirán o trataran al máximo de minimizar la recepción excesiva de información no solicitada en las cuentas de correo electrónico de los funcionarios del municipio.

- **Minimizará los riesgos de recepción de spam**

Con la creación y desarrollo de un manual de seguridad que guíe a los funcionarios del GADMA para disminuir el excesivo envío de información no deseada a sus cuentas de correo electrónico, se evitará la recepción excesiva de spam.

## **6.4. Objetivos**

### **6.4.1. Objetivo General**

Desarrollar un manual que guie a los funcionarios del Gobierno Autónomo Descentralizado Municipalidad Ambato para disminuir el excesivo envío de información no deseada a sus cuentas de correo electrónico.

### **6.4.2. Objetivos específicos**

1. Analizar las herramientas de software que sirven para enviar correo electrónico con spam.
- 2- Realizar las pruebas de configuración y envío de spam con las herramientas investigadas.
- 3- Desarrollar un manual que guie a los funcionarios del GADMA en el manejo adecuado del envío y recepción de información a través de sus cuentas de correo electrónico para disminuir el spam.

## **6.5. ANÁLISIS DE FACTIBILIDAD**

- Política

Es política de la institución el permitir realizar cualquier mejora que traiga beneficios a la misma, siempre y cuando se encuentre supervisado por el personal autorizado, el cual brindara ayuda para la realización de cambios en caso de ser necesario.

- Socio cultural

Se dará un buen manejo de la información y además se garantiza que será usada de la mejor manera y con la discreción que se requiere, ya que solo se dará a conocer al personal autorizado.

- Tecnológico

La Municipalidad de Ambato brindará todos los recursos necesarios para el desarrollo de la tesis en cuanto a software y hardware, tomando en cuenta que el tema a desarrollarse no exige tantos recursos para su correcto desarrollo.

- Equidad de género

En este aspecto el desarrollo del proyecto de investigación no tendrá ninguna influencia ni preferencia hacia ningún género ya que será estrictamente profesional.

- Ambiental

La tesis a realizarse no afectará ni influirá en ningún aspecto en cuanto al medio ambiente se refiere.

- Económico-financiera

Para el desarrollo de la investigación no se requerirá de grandes inversiones ya que es estrictamente investigativo y bastará con los recursos con los que hasta el momento dispone la empresa.

- Legal.

Dentro de las leyes no existe ningún impedimento para la realización del proyecto de investigación por lo que el proyecto no tendría ningún inconveniente en cuanto a la ley se refiere.

## 6.6. INFORME TECNICO

### 6.6.1. Análisis de las Técnicas Spam

Existen varias técnicas para enviar spam, se sabe que lo principal es la obtención de direcciones de correo, seguido del uso de herramientas informáticas para el envío de mensajes electrónicos. A continuación se detallan los métodos comúnmente más usados por los spammers y por nosotros mismos como usuarios, sin tener conciencia que con lo que se hace es ayudar al spammer a que cumpla su objetivo y coseche varias direcciones de e-mail incluida quizá la nuestra.

De acuerdo al criterio de López, Diana. y Congote, Jhon (22/11/2012). Monografias.com. Recuperado desde (<http://www.monografias.com/trabajos39/spam-correo-electronico/spam-correo-electronico2.shtml>) se obtuvo la siguiente información:

- “Visitar muchos foros en Internet. En muchos de ellos para poder opinar y para que los demás usuarios contesten y dejen comentarios, se obliga a la persona a dejar su dirección de correo, la cual generalmente, queda a la disposición de cualquiera.
- Utilizar los grupos de noticias y dejar la dirección de correo en una gran lista de usuarios dispuestos para recibir cualquier tipo de correo.
- Una forma un poco más sofisticada, pero muy utilizada por los spammers es la creación de un pequeño programa, llamado "araña", el cual rastrea todas las páginas de Internet a la busca de cualquier dirección publicada en éstas. De esta forma cualquier dirección de correo publicada en una página personal, de trabajo o foro, se convierte en un blanco perfecto para las arañas. Para ello se recomienda utilizar algún tipo de código o

enmascarar la dirección Web para que estas arañas no las encuentren.

- Otro medio que utilizan los spammers es la compra de bases de datos a empresas o con miles de direcciones de correo electrónico.
- Reenviar correos electrónicos con chistes, cadenas, etc. sin ocultar las direcciones a las que ha sido enviado antes el mensaje, y que acumulan gran cantidad de direcciones en el cuerpo del mensaje.
- Acceder a páginas en las que se solicita la dirección de correo del visitante, o la de "sus amigos y contactos" para enviarles la página en un correo o para recomendársela, para acceder a un determinado servicio o descarga.
- Los spammers utilizan también una técnica conocida como "ensayo y error" que consiste en generar aleatoriamente direcciones, enviar los mensajes a esas direcciones, y posteriormente comprobar que sí han llegado los mensajes. Un método habitual en esta técnica es hacer una lista de dominios, y agregarles "prefijos" habituales.
- Otra práctica común en los spammers es el uso de troyanos y computadores zombis. La característica de los troyanos es que permiten acceso remoto a la maquina, así, los computadores de las víctimas son utilizados como "computadores zombis", que envían spam controlados por el spammers, pueden incluso rastrear los discos duros o libretas de direcciones en busca de más direcciones.”

Si cae en los errores comunes anteriormente detallados, los mismos causan perjuicios al usuario que ignora haber sido infectado, ya que pasa a ser identificado como spammer por los servidores a los que

envía spam sin saberlo y esto puede traer como consecuencia que no se le deje acceder a determinadas páginas o servicios.

Además facilita la propagación de spam cuando se cuenta con servidores de correo mal configurados “Open Relay”, ya que no necesitan un usuario y contraseña ni tienen ningún criterio para evitar que sean utilizados para el envío de correos electrónicos no autorizados.

### **6.6.2. Herramientas para envío de Spam**

En esta parte se explicara las herramientas que usan las técnicas spam detalladas anteriormente, para que más adelante podamos utilizar la más adecuada y eficaz en el envío de información no deseada a las cuentas de correo electrónico de los funcionarios del GAD Municipalidad Ambato.

Para el desarrollo de esta investigación se considero usar las herramientas conocidas como mozilla thunderbird, Outlook y claws-mail, además se utilizar un servidor de dominio llamado PHPList el mismo que permite también enviar mensajes de correo electrónico.

Para poder usar alguna de las herramientas mencionadas se necesita tener instalado un servidor FTP en este caso de tipo cliente, por facilidad y eficacia la herramienta a usar será FileZila Client.

Las configuraciones de cada herramienta de software a utilizar, no serán las comunes, pues para hacer uso de ellas incorporando el contenido spam, se configurara especificando el servidor a usar, y los servicios que se requieran en este caso los de correo electrónico.

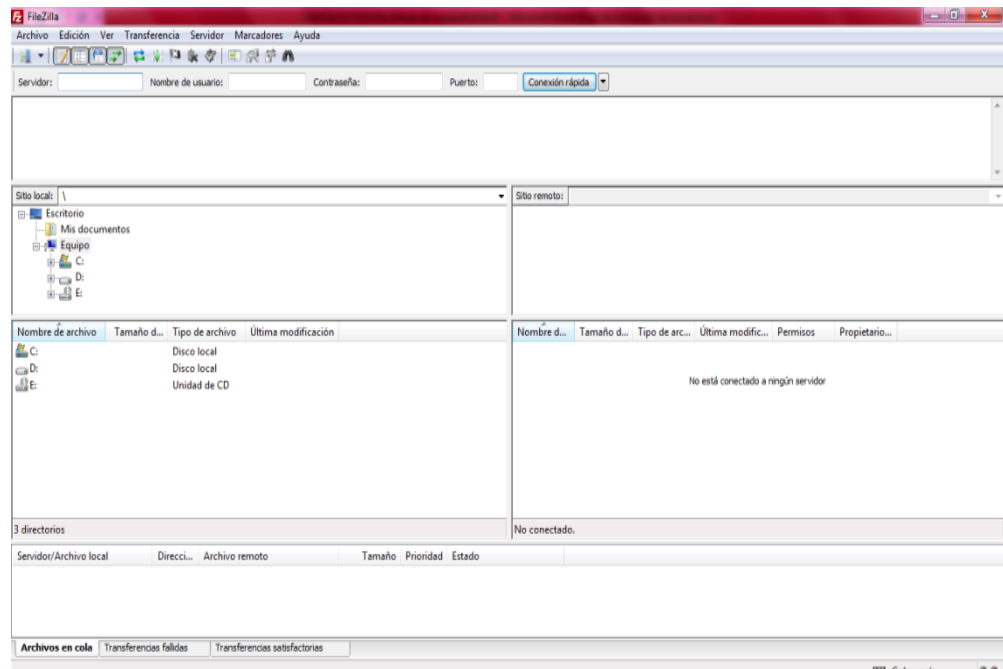
#### **6.6.2.1. FileZila Client**

Es un cliente FTP que tiene la característica de ser multiplataforma además puede soportar protocolos FTP, SFTP. Se necesita este cliente para usar el servicio de la cuenta del hosting con el que se está trabajando. Para



entender la próxima configuración se utilizara el dominio mentesinquietas.net.

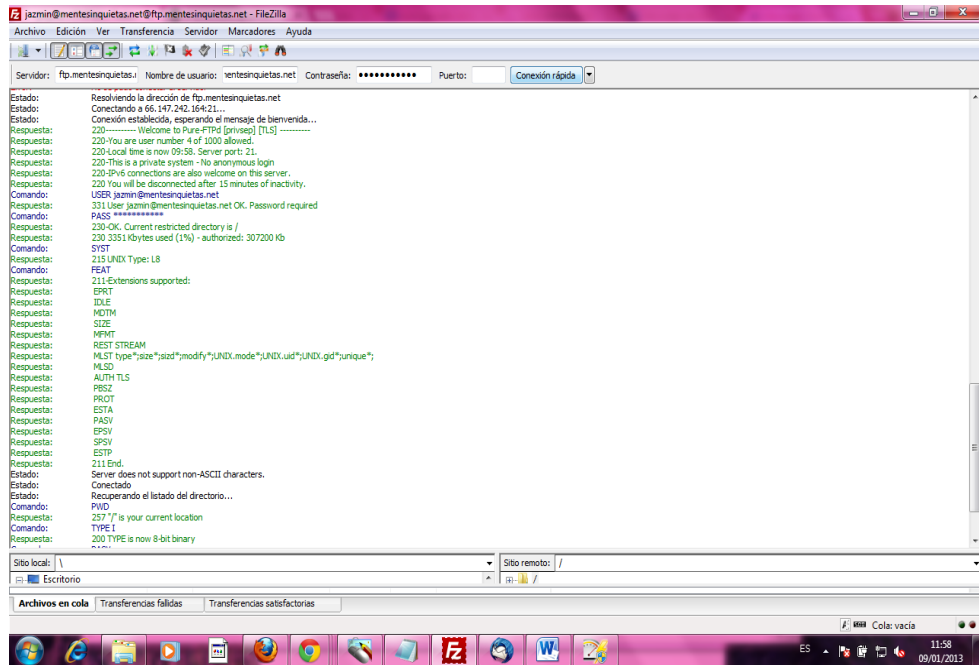
Esta herramienta es libre y puede ser descargada del internet e instalada fácilmente; una vez instalada aparecerá la ventana que se ve en la siguiente figura.



**Gráfico 6. 1** Inicio FileZila

Una vez que se puede visualizar la ventana de inicio del cliente FileZila se debe suministrar algunos datos para poder establecer conexión con el servidor. Los campos en blanco se llenaran con la siguiente información:

- FTP Username: jazmin@mentesinquietas.net
- FTP Server: ftp.mentesinquietas.net
- FTP Password: (la que se establezca)
- FTP Server Port: 21



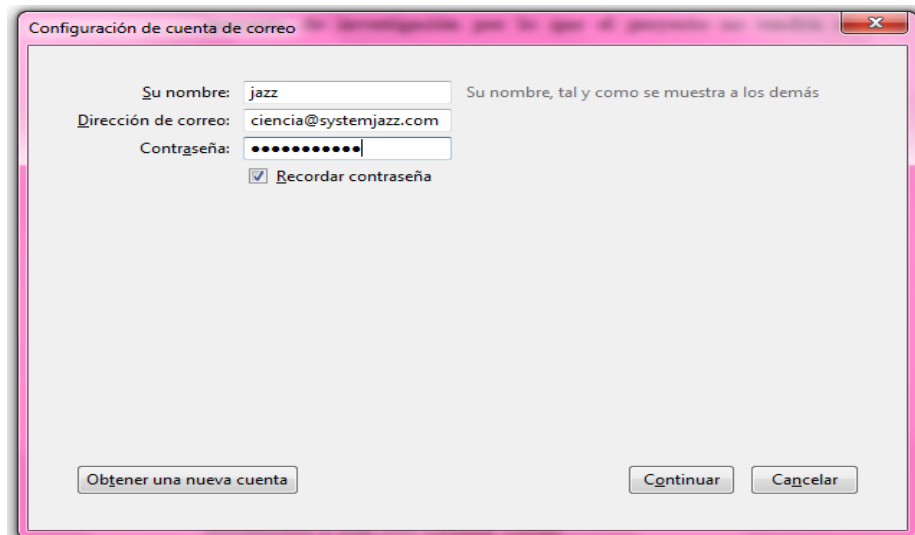
**Gráfico 6. 2** Conexión a servidor desde ftp

Al terminar de llenar los datos que se requieren se presionara el botón de conexión rápida y podrá observar cómo se levantan los servicios necesarios hasta lograr una conexión exitosa. Si se logra la conexión ya podrá hacer uso del servicio FTP.

### **6.6.2.2. Mozilla Thunderbird**

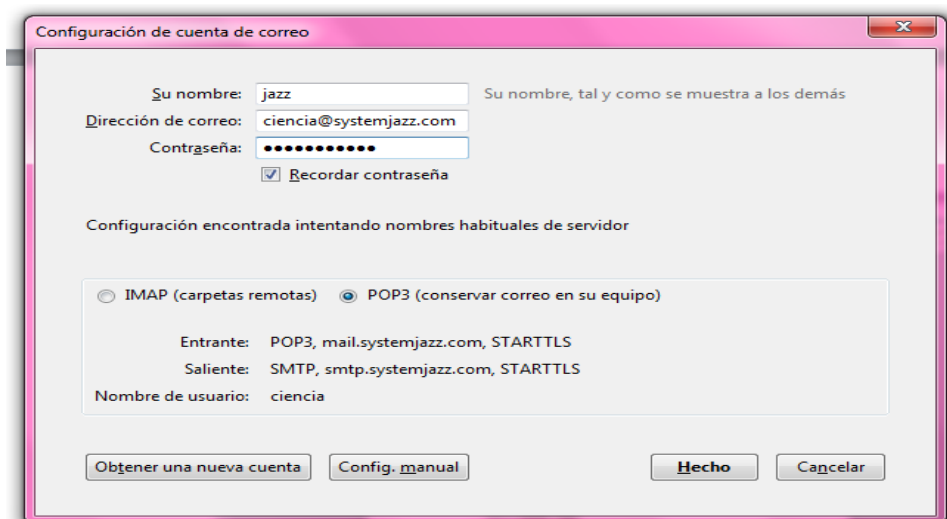
El programa Thunderbird es un cliente de correo electrónico muy bueno ya que es libre debido a que se lo puede descargar de la web e instalar fácilmente en nuestro pc, además su uso es muy sencillo y no presenta inestabilidades.

Una vez instalado en nuestra computadora, para poder usarlo correctamente debemos primero realizar una breve configuración donde crearemos paso a paso una cuenta de correo asociada a nuestro servidor para así lograr envíos y recepciones de correos exitosos.



**Gráfico 6. 3** Configuración de Mozilla Thunderbird

En la figura se muestra la creación de la cuenta de correo la que se asocia a la herramienta thunderbird, aquí se debe llenar los datos del nombre con el que se verá al enviar el mensaje, la dirección de correo asociada que en este caso será ciencia@systemjazz.com que es el dominio adquirido en este caso, y la contraseña respectiva, presionar continuar e ir al siguiente paso.

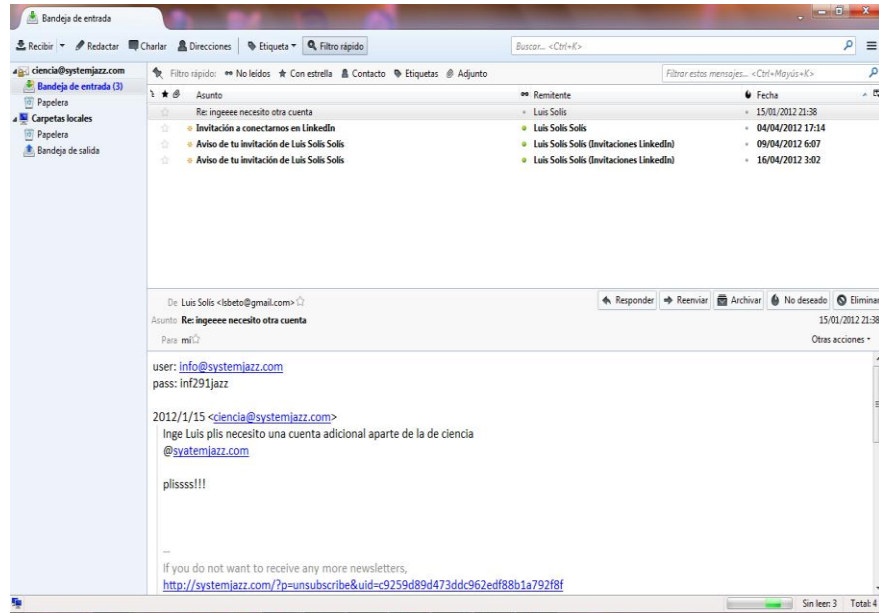


**Gráfico 6. 4** Creación cuenta de correo en MT

Una vez creada la cuenta se procede a configurar el servidor con el que va a trabajar para este caso POP3 y SMTP con la siguiente especificación:

- servidor smtp smtp.systemjazz.com
- servidor pop pop.systemjazz.com

Presionar el botón Hecho y esperar que se muestre la ventana donde se podrá empezar a utilizar las opciones de este cliente de correo.



**Gráfico 6. 5** Bandeja de entrada de la cuenta en MT

Al lograr establecer una conexión y creación exitosa de cuenta de correo se despliega los mensajes de bandeja de entrada que se ha recibido, como en todos los clientes de correo electrónico se tiene varias opciones para trabajar, esta herramienta no es la excepción pues posee varias funciones como: enviar mensaje, redactar borrar, responder, entre otros, por ahora las que en esta investigación nos interesa son las opciones de crear y redactar un nuevo mensaje el mismo que pueda tener contenido de tipo texto, imágenes o sonido, esto se podrá lograr también con la opción de adjuntar archivo.

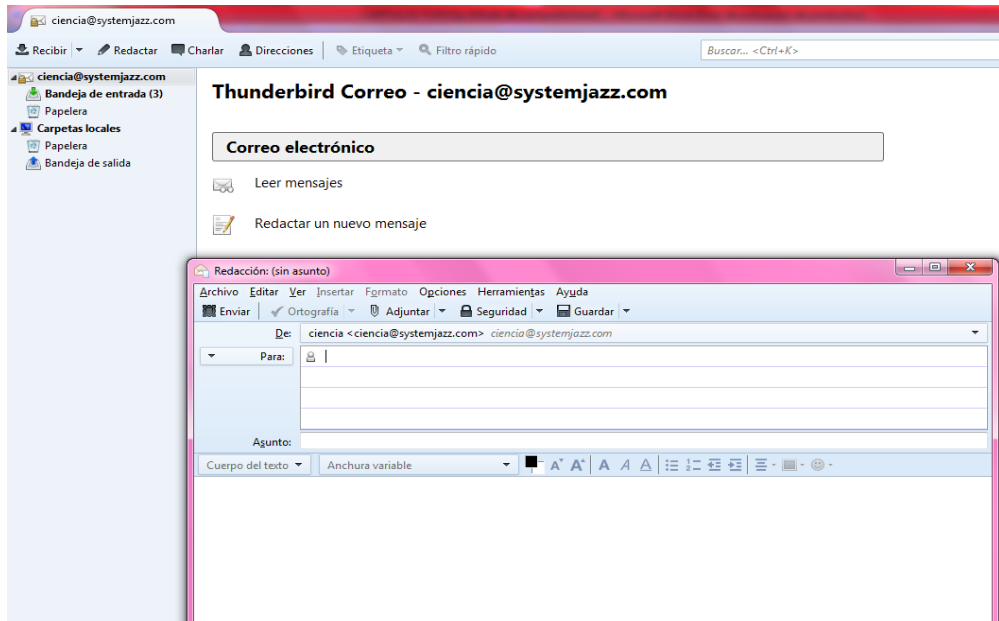


Gráfico 6. 6 Redacción de mensajes en MT

Para enviar la información que desee primero se deberá especificar el destinatario en la opción 'Para' además se puede escribir un 'asunto' el mismo que no necesariamente deberá ser llenado, además el texto que se puede escribir tiene la opción de ser arreglado con colores, tamaño y tipos de letras dando una mejor apariencia al mensaje que se enviara, el mismo que podría tener algún código cifrado u oculto al receptor.

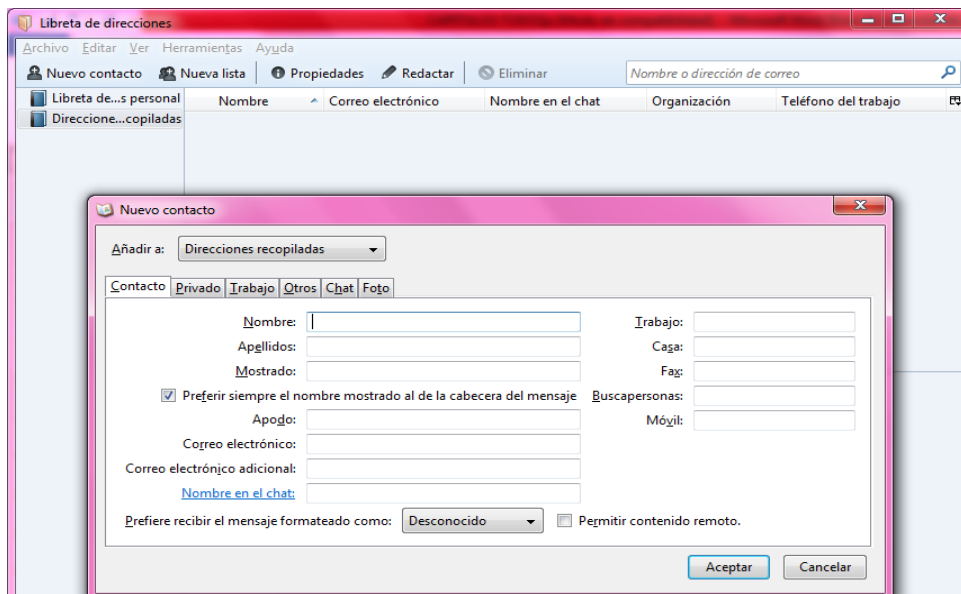


Gráfico 6. 7 Creación de contactos en MT

Otra opción que será de gran ayuda y brinda esta herramienta es la creación de contactos donde se especificarán nombres, apellidos, y todo tipo de información que se requiera, pero esto no es todo ya que también con los contactos creados se podrán crear listas y facilitar el envío masivo de mails, así como también importar contactos que tengamos recopilados.

### 6.6.2.3. Outlook

Esta herramienta es capaz de enviar, recibir y administrar el correo electrónico, también puede administrar el calendario y todo tipo de contactos ya sean sociales familiares o empresariales. Este software viene incluido en la instalación de “Office”, por lo que conseguirla es fácil; su uso es poco complejo. Al utilizarlo por primera vez se visualiza la siguiente ventana:

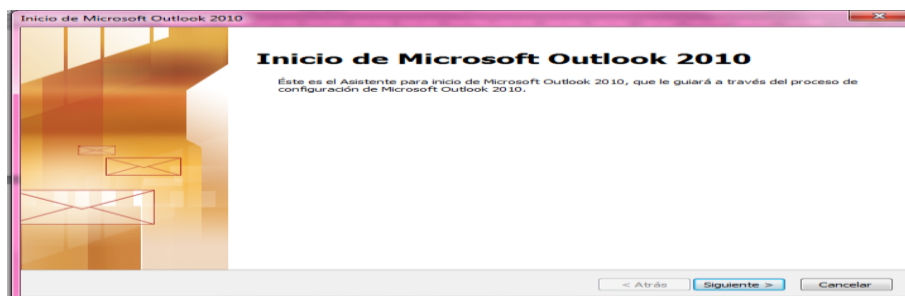


Gráfico 6. 8 Inicio de Microsoft Outlook

Para continuar presionar el botón resaltado ‘siguiete’ y aparecerá la ventana de cuentas de correo donde preguntará si deseamos configurar Outlook para conectar con un correo electrónico que poseamos.

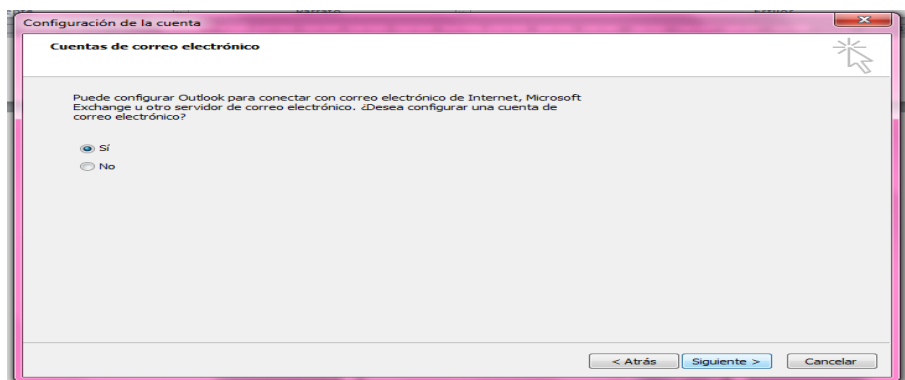


Gráfico 6. 9 Pregunta de verificación de configuración Outlook

Seleccionar la opción 'sí' y dar clic en siguiente para saltar a otro paso.

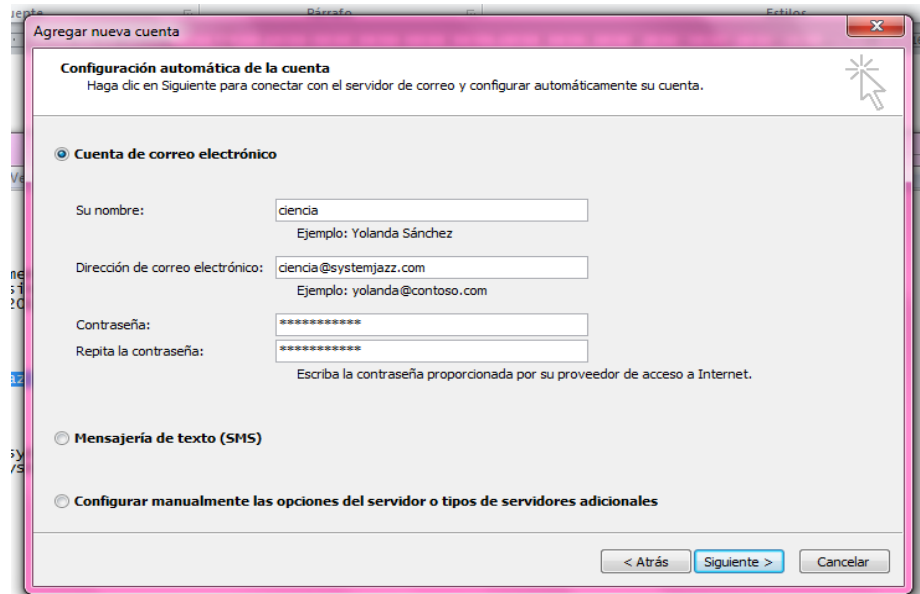


Gráfico 6. 10 Configuración de cuenta en Outlook

Al igual que en los otros servidores de correo electrónico en este también debe configurar una nueva cuenta con su respectiva contraseña, la misma que se verifica repitiéndola e ingresándola correctamente, se seguirá usando la cuenta de ciencia@systemjazz.com y seguir al próximo paso que será la búsqueda de la configuración del servidor en línea.

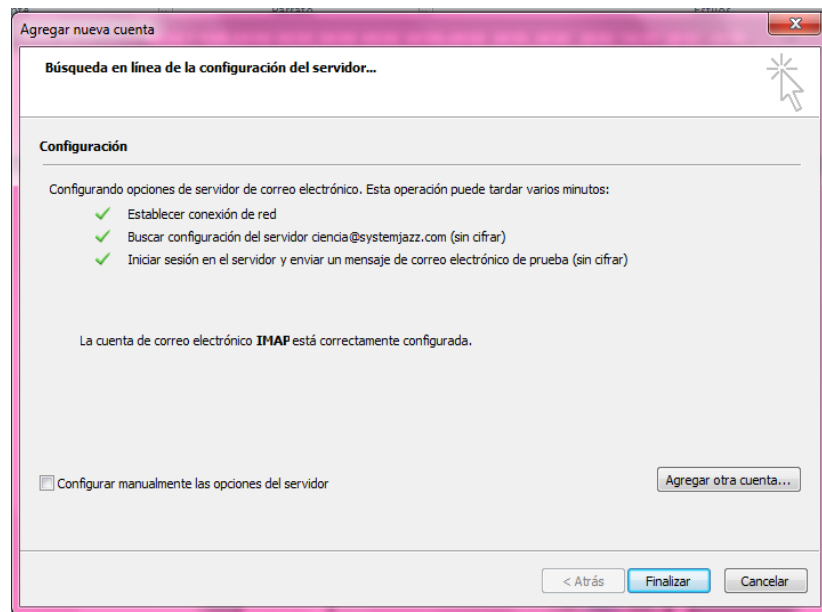


Gráfico 6. 11 Cuenta configurada correctamente

Si pasan las pruebas de conexión, configuración del servidor de la cuenta además de verificar el envío y recepción de un mensaje a modo de prueba con el servidor se podrá finalizar correctamente la configuración y se visualizara una ventana de Outlook cargando sus complementos, al finalizar se podrá hacer uso de todas las ventajas esta herramienta.

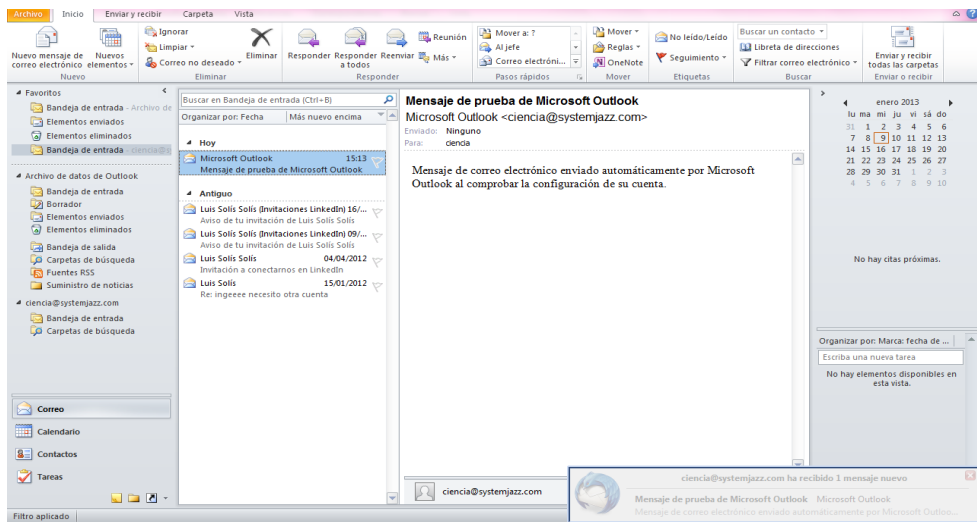


Gráfico 6. 12 Ventana de inicio de Outlook

Como todos los pasos fueron correctamente configurados ya se puede tener acceso a la información de la cuenta de correo y también empezar hacer uso de sus opciones de envío de mensajes. Las opciones de calendario no son de mucha importancia en esta investigación.

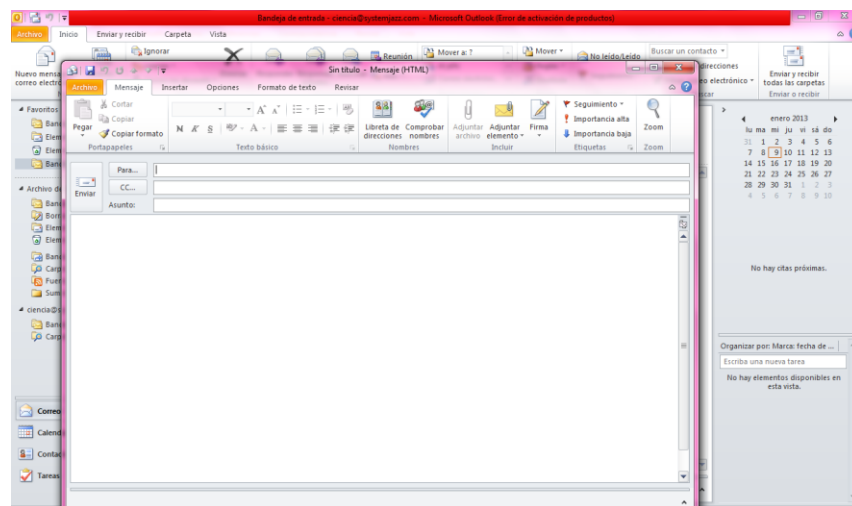


Gráfico 6. 13 Redacción de mensajes en Outlook



La utilización de esta herramienta se centrara en el envío de mensajes a varias cuentas de correo las mismas que se ingresarán a la agenda de contactos de esta herramienta, luego de seleccionar el destinatario especificar el asunto o motivo del mensaje y complementar el contenido del mensaje, también se puede adjuntar todo tipo de archivo.

#### 6.6.2.4. Claws-mail

A diferencia de Outlook claws mail no es un gestor de información personal completo, y no permite escribir y enviar correos HTML; pero a pesar de ello también es un cliente de correo electrónico que se caracteriza por orientarse a ser rápido fácil y potente permite la recuperación de correo POP3, IMAP4, también soporta algunos métodos de autenticación además se puede utilizar en cualquier tipo de ordenador pues se acopla fácilmente sin consumir mucha memoria, para conseguirlo solamente puede buscarlo en la web y descargarlo a manera de prueba.



Gráfico 6. 14 Inicio de Claws Mail

Una vez que descargue esta herramienta, de preferencia desde su propio Sitio web: [www.claws-mail.org](http://www.claws-mail.org) la instala y la ventana que se mostrara será la de la figura anterior (Inicio de Claws Mail), donde además se solicita que responda algunas preguntas con el fin de obtener información para

configurar la cuenta, dichas preguntas son sencillas y fáciles de responder, esto no llevará mucho tiempo.



Gráfico 6. 15 Configuración de Claws Mail

Lo primero será que llene su nombre junto a la dirección de correo y la organización a la que pertenece, después de llenar estos datos se podrá pasar a la siguiente pagina.

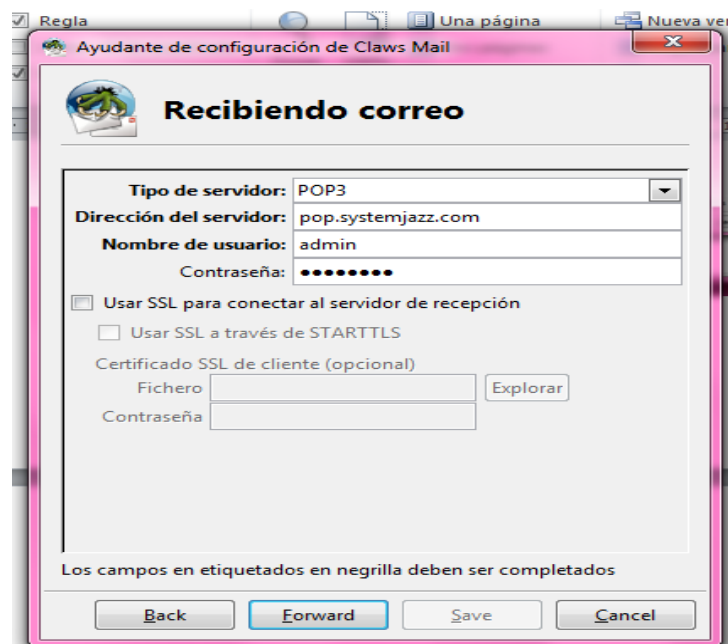
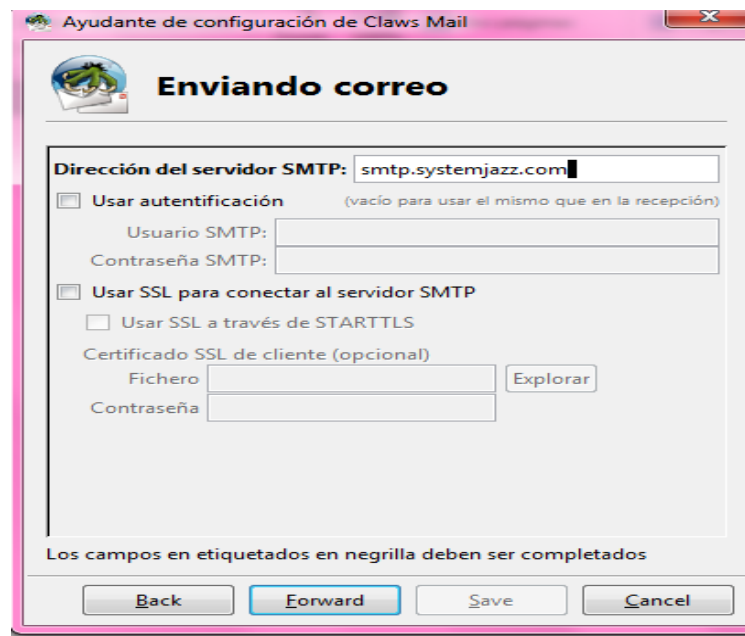


Gráfico 6. 16 Configuración de POP3 en Claws Mail

En esta página de Configuración de POP3 se permite especificar los detalles o la información que permita recuperar el correo electrónico al elegir POP3, se debe ingresar los datos del servidor, el nombre de usuario con el que se trabajará y la contraseña, si no se ingresa la contraseña, esta será solicitada las veces que sean necesarias posteriormente. Al terminar esta configuración se pasará a la página de configuración del servidor SMTP.



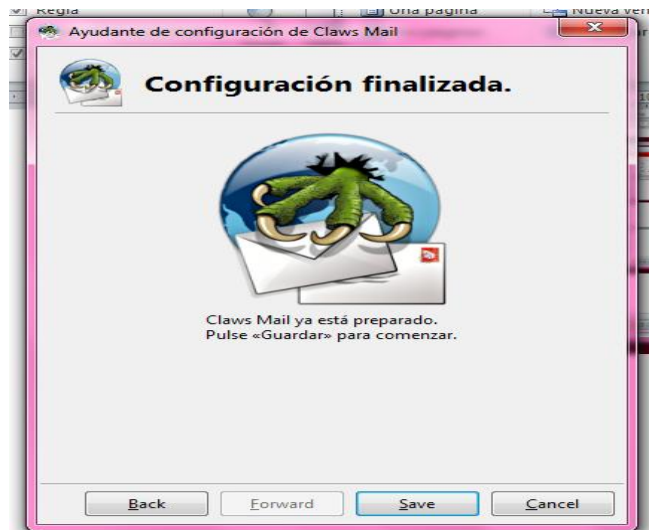
The image shows a screenshot of the Claws Mail configuration window titled "Ayudante de configuración de Claws Mail" and "Enviando correo". The window contains the following fields and options:

- Dirección del servidor SMTP:** smtp.systemjazz.com
- Usar autenticación** (vacío para usar el mismo que en la recepción)
  - Usuario SMTP: [Empty field]
  - Contraseña SMTP: [Empty field]
- Usar SSL para conectar al servidor SMTP**
  - Usar SSL a través de STARTTLS
  - Certificado SSL de cliente (opcional)
    - Fichero: [Empty field] **Explorar**
    - Contraseña: [Empty field]

At the bottom, there is a note: "Los campos en etiquetados en negrilla deben ser completados". Below the note are four buttons: "Back", "Forward", "Save", and "Cancel".

**Gráfico 6. 17** Configuración de servidor SMTP en Claws Mail

También se conoce como servidor saliente al servidor SMTP, se especifica el nombre del servidor smtp.systemjazz.com, existen las opciones para autenticación al enviar un correo, esta opción no es necesaria así que no la señalaremos.



**Gráfico 6. 18** Configuración Establecida

Finalizar la configuración de esta cuenta y guardar los cambios efectuados; luego de esto podrá visualizar la pagina de Claws Mail con todas sus múltiples opciones como redactar, enviar correo o crear contactos; Al igual que en las herramientas usadas anteriormente esta también servirá para enviar correo a varios contactos, pues el mayor objetivo es lograr enviar la mayor cantidad de Spam, sin que sea detectado por los filtros que trae cada herramienta

Por lo general se empieza a usar esta herramienta con la opción de recuperación de correo, los mensajes recuperados se mostraran dentro de la carpeta de Entrada. También podemos visualizar el panel con la lista de los mensajes recibidos ya sean leídos o por leer, en adición se puede seleccionar uno de ellos, mismo que mostrara automáticamente su contenido.

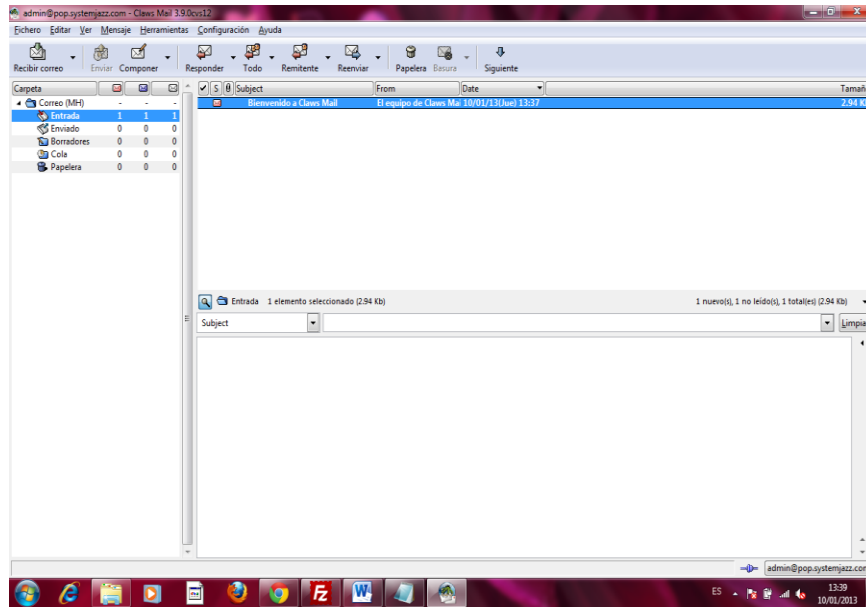


Gráfico 6. 19 Ventana de funciones de Claws mail

Como ya se menciona el objetivo es enviar mensajes para ello deberá seleccionar la opción Correo que se encuentra en la barra de herramientas y podrá visualizar una ventana para Componer Mensaje, en ella se muestran varios campos entre los mas importante y los que se usará será la especificación de el o los destinatarios en el botón “Para”, indicará el asunto de su mensaje y luego se concentrará en escribir o especificar el contenido, además se puede adjuntar algún archivo como imágenes, documentos de texto, archivos pdf, etc.

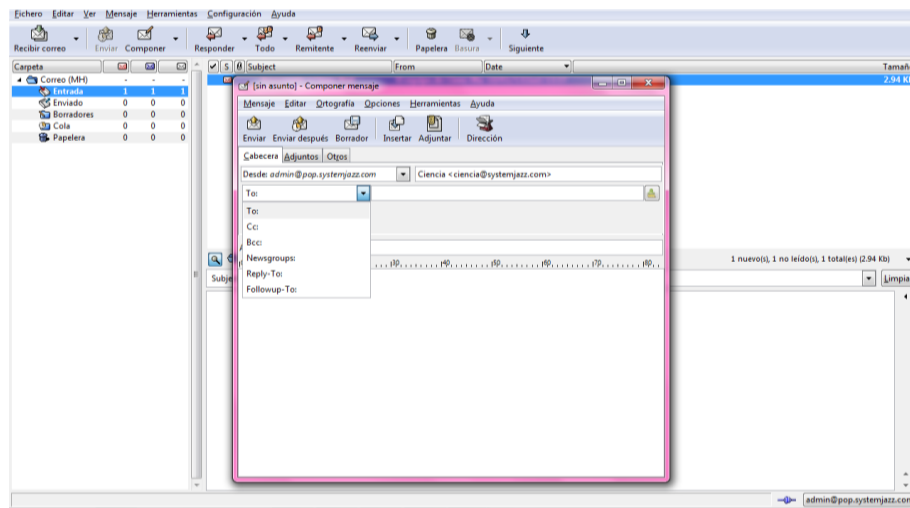


Gráfico 6. 20 Ventana de envío de mensajes

Cuando se finalice con la escritura o especificación del contenido del mensaje pulsar el botón “enviar” y el mensaje será enviado inmediatamente, automáticamente al verificar el envío la ventana de componer mensaje se cerrara sola, en caso de existir algún tipo de error esta permanecerá abierta. El o los mensajes enviados se almacenaran en la carpeta “Enviado”.

En conclusión este servidor de correo es muy útil y sencillo al usarlo, ofrece muchas utilidades, que nos han servido de ayuda en nuestra investigación

#### 6.6.2.5. PhpList

Esta herramienta software está basada en código abierto usado para gestionar listas de correo electrónico, usada generalmente para difundir publicidad, noticias novedosas entre otro tipo de información a los suscriptores miembros de sus listas; Además administra una base de datos en línea usada para enviar varios correos a sus múltiples suscriptores.

Una vez instalado PHPLIST se muestra la siguiente ventana:

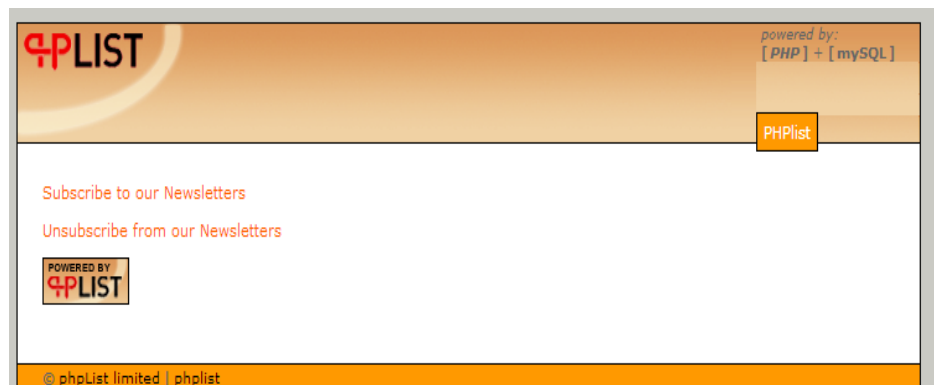


Gráfico 6. 21 Ventana PHPList iniciando

Para obtener mayor información de esta herramienta el usuario o administrador puede ingresar a la opción “Acerca de” donde encontrara datos útiles acerca de su uso y funcionamiento, pues trae incorporado varios link que redirigen a páginas con contenido interesante y útil para la correcta utilización y configuración de este software.

En la figura que se muestra a continuación se puede ver la ventana antes mencionada:

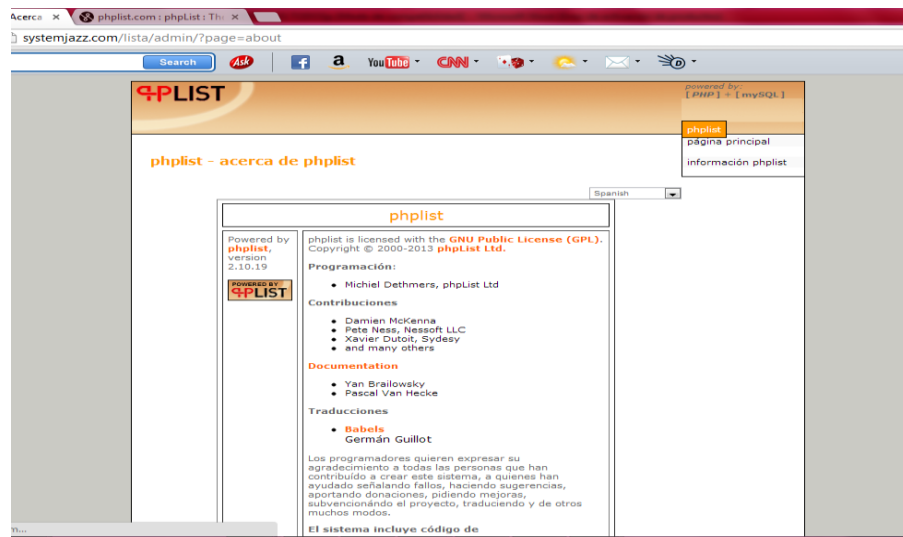


Gráfico 6. 22 Contenidos de PHPList

Este software posee una gran variedad de funciones, las mismas que son de gran utilidad al momento de especificar los requerimientos que tiene el administrador de la página, Para configuraciones del administrador esta disponible la pagina principal de administración donde se configuraran sus funciones, entre ellas se tiene: funciones de sistema, funciones de configuración, de listas y usuarios, funciones de administrador, funciones de mensajes, entre otras también muy útiles.



Gráfico 6. 23 Página principal de administración de PHPList

Es necesario realizar una configuración que responda a las necesidades del administrador, en la página de configuración se permite configurar elementos que para el sistema son básicos y esenciales, como el nombre del dominio de nuestro sitio web, la dirección mail del sistema, además de mensajes enviados por defecto a usuarios que cancelen su suscripción, o realicen modificaciones en el tipo de información que desean recibir. Las configuraciones que se harán serán:

Para la dirección Web se usó el dominio siguiente (www.systemjazz.com), la herramienta PHPLIST usa este tipo de configuración para realizar referencias internas. Para configurar el dominio del servidor que será usado en cuentas de correo se utilizará systemjazz.com. Especificar además a quien estará encargado del manejo del sistema en este caso se pondrá la dirección de correo de un super-administrador o del webmaster, entonces será (webmaster@systemjazz.com) a esta dirección ingresada llegarán todas las notificaciones como suscripciones, confirmaciones, cambios de preferencias de los usuarios.



Gráfico 6. 24 Configuración de PHPList

Existe también la opción de atributos del sistema, que permite añadir atributos como nombres apellidos, país de origen, dirección, fecha de



nacimiento entre otras; así no se tendrá una dirección de correo simple sino con detalles; por lo que se comprueba que PHPList funciona también como una base de datos.

La página de listas de los usuarios muestra los usuarios existentes dentro de una lista, pero primero hay que saber que para PHPList un usuario es una dirección de correo electrónico que está registrado en su base de datos, además por cada dirección de correo es también válido obtener más información en base a los atributos especificados anteriormente por el administrador.

Además en la página de usuarios se puede elegir el orden de los mismos, tiene opciones de búsquedas rápidas especificando algún tipo de atributo o por defecto el correo electrónico que consta en la BDD. A los usuarios creados se puede suscribirlos a listas creadas también por aquel que tomae el papel de administrador.

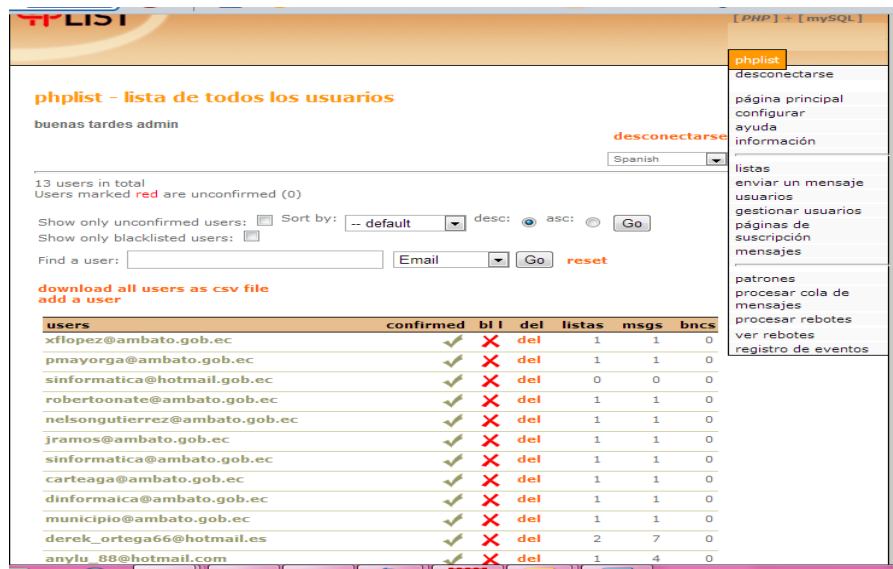


Gráfico 6. 25 Configuración de Listas de Usuarios en PHPList

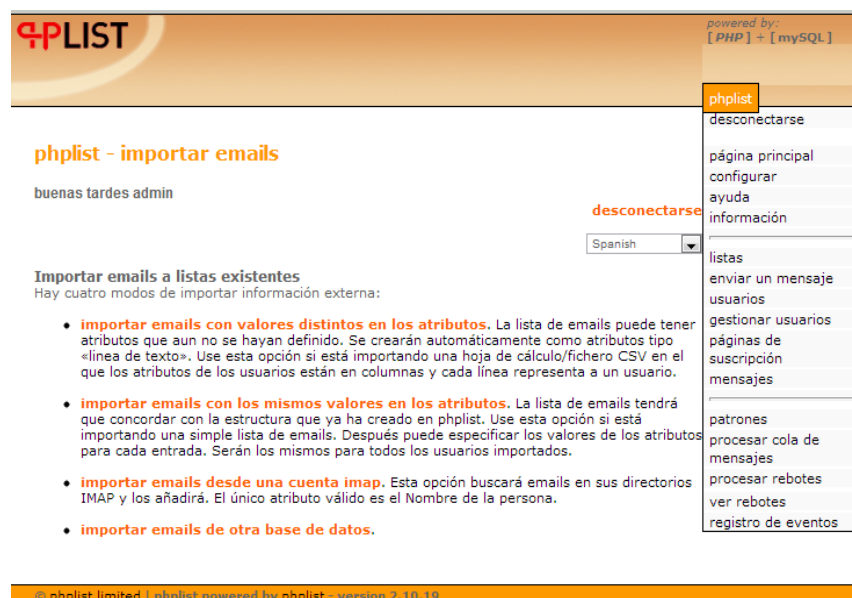
En el caso de existir varios usuarios se puede visualizar por defecto únicamente los 50 primeros, se crean ventanas de navegación internas para poder seguir viendo el resto de usuarios, los mismos que estarán en varias columnas. Para obtener información acerca del usuario y sus suscripción deberá fijarse si ya han confirmado su suscripción, si no lo hicieron los

mensajes que se envíen a una lista no llegaran a los que no se hayan suscrito correctamente.

En PHPList solo los administradores pueden manejar listas, así como también enviar mensajes a las listas que deseen, pues esta herramienta no permite las listas sean usadas para intercambio entre usuarios, es decir que las listas son solo usadas para enviar mensajes en sentido único;

Existe la posibilidad de tener más de un administrador dentro de esta herramienta y cada uno de ellos puede crear varias listas, por consiguiente cada administrador puede poseer varias listas, pero no podrá enviar mensajes a listas de otro administrador.

Otra de las páginas además de suma utilidad es la de importación de emails que a continuación se muestra:



**Gráfico 6. 26** Importación de e-mails de PHPList

Se puede importar cualquier cantidad de direcciones de correo siempre y cuando estas estén almacenadas en una base de datos o una hoja de cálculo con extensión (.csv), las direcciones por preferencia deberán estar separadas por un “Tab”, las mismas que pueden tener atributos como nombres apellidos además de la dirección de correo. El archivo a importar no deberá ser mayor a 1Mb.

Para proceder a la importación seleccionar la opción “administrar usuarios” que se encuentra en la página de administración (Grafica 36. Página principal de administración de PHPList), después presionar el botón de “Importar usuarios” y seleccionar una de las cuatro formas de importar información, ya que se lo puede hacer para emails con diferentes valores para los atributos, para emails con valores iguales para sus atributos, importación desde una cuenta IMAP, o seleccionar otro tipo de base de datos.

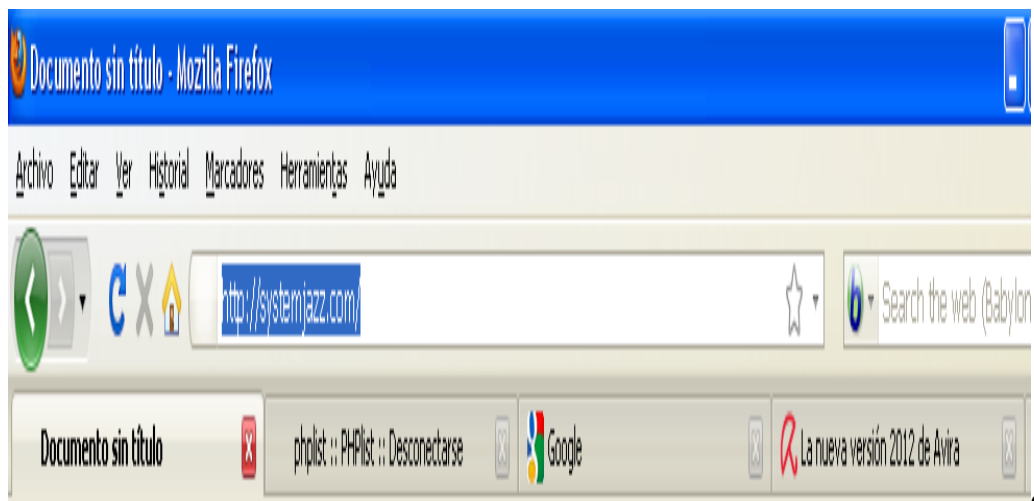
Al seleccionar la opción que necesita, deberá tener en cuenta que se puede sobrescribir la información existente por lo que antes se debe asegurar de no duplicar la información de las cuentas de correo electrónico.

### **6.6.3. Pruebas de Envío de Mensajes Aplicando Técnicas Spam**

Para la realización de la presente investigación y propuesta se han realizado varias pruebas donde se pone en práctica la información adquirida y aprendida en el marco teórico.

Con las pruebas mencionadas se puede saber y detectar el tipo de vulnerabilidad que pueden tener las cuentas de correo electrónico de los funcionarios, además de definir las técnicas spam más usadas, con esto se puede crear y desarrollar el manual de guía con varios consejos y normas útiles que con toda seguridad ayudaran a que el nivel de seguridad de su información aumente, además de evitar el riesgo de recibir tanto spam.

Para analizar las técnicas spam, y poder probar el proceso de obtención de direcciones, creación de mensaje y envío del mismo ha sido necesario contar con un dominio y hosting adecuado, ya que por los filtros de spam que existen no se puede utilizar un hosting gratuito.



Grá

Gráfico 6. 27 Acceso al dominio. Hosting

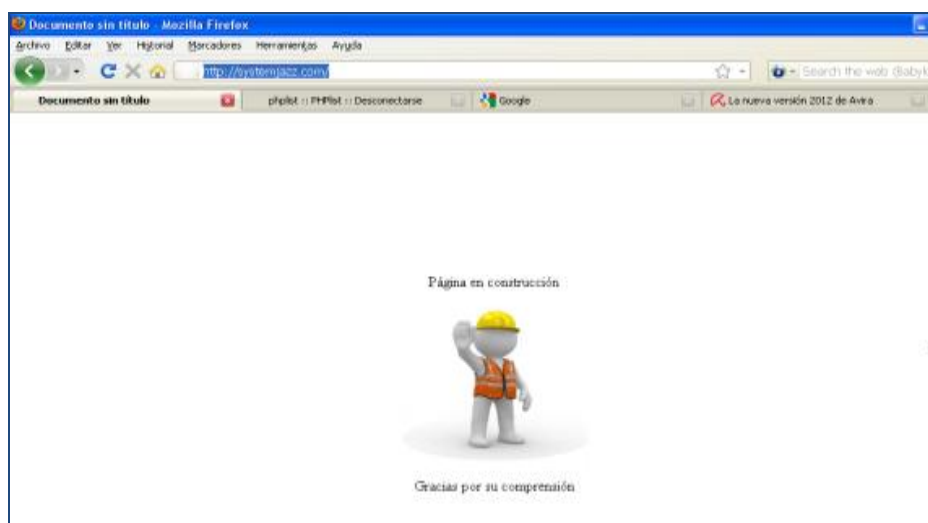


Gráfico 6. 28 Pagina systemjazz

### 6.6.3.1. Prueba con la herramienta PHPLIST

El hosting y dominio adquirido será el que servirá para el envío de mensajes a los destinatarios que desee, para lograr este objetivo previamente se ha añadido la herramienta phplist a la pagina; en la siguiente figura se podrá observar el acceso a la configuración de nuestro hosting y dominio, llamado systemjazz.com



**Gráfico 6. 29** Conexión al servidor PHPLIST

Dentro de la configuración de phplist se tiene varias opciones útiles, entre ellas la posibilidad de crear listas de correo así se puede clasificar a cada usuario que se cree. PhpList no es la única herramienta con la que se puede enviar el correo deseado, existe también varias opciones entre ellas Mozilla Thunderbird, Outlook, Claws-Mail, entre otros.

Se necesita configurar los servicios de ftp y de smtp, además de pop3, para ello se requiere usar las herramientas anteriormente mencionadas, y para ftp se usará la herramienta fileZila client, se recomienda usar la versión más actual que exista.

Luego de su instalación se debe configurar la cuenta FTP Username: usuario@sudominio.net, FTP Server: ftp.mentesinquietas.net FTP Password: suclave FTP Server Port: 21. La ventana de configuración deberá ser similar a la siguiente:

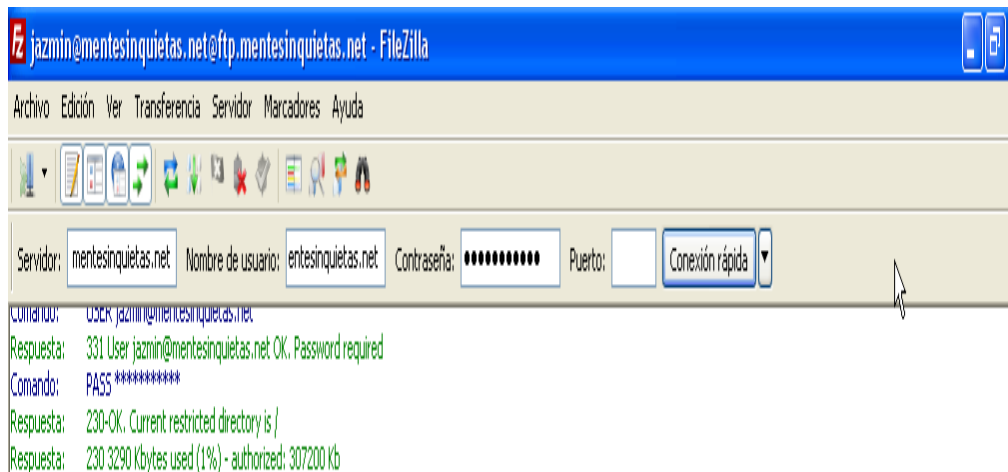


Gráfico 6. 30 Levantamiento del cliente Filezilla

Una vez establecida la conexión se puede añadir todo tipo de archivo a las carpetas del hosting. Además se pueden crear directorios dentro del mismo.

En esta herramienta se puede crear usuarios e irlos añadiendo uno a uno, una de las técnicas spam conocidas es recopilar cuentas de correo electrónico validas, para la prueba se han utilizado cuentas que han sido facilitadas por el encargado de sistemas de la entidad donde a futuro se realizaran el 100% de las pruebas.

Para añadir usuarios a una lista el proceso es crear la lista y añadir el usuario a la misma, así evita la pérdida de tiempo al añadir uno a uno el destinatario.



Gráfico 6. 31 Verificación de lista de usuarios en PHPList

La primera prueba de envío de mensaje se ha realizado con phplist, para poder añadir imágenes u otro tipo de animación o archivo es necesario que todo este subido en nuestro hosting así que lo que se realiza es fácil; Al establecer conexión desde filezilla se tiene acceso a las carpetas y elegimos la que deseamos para añadir el contenido que necesitamos así:

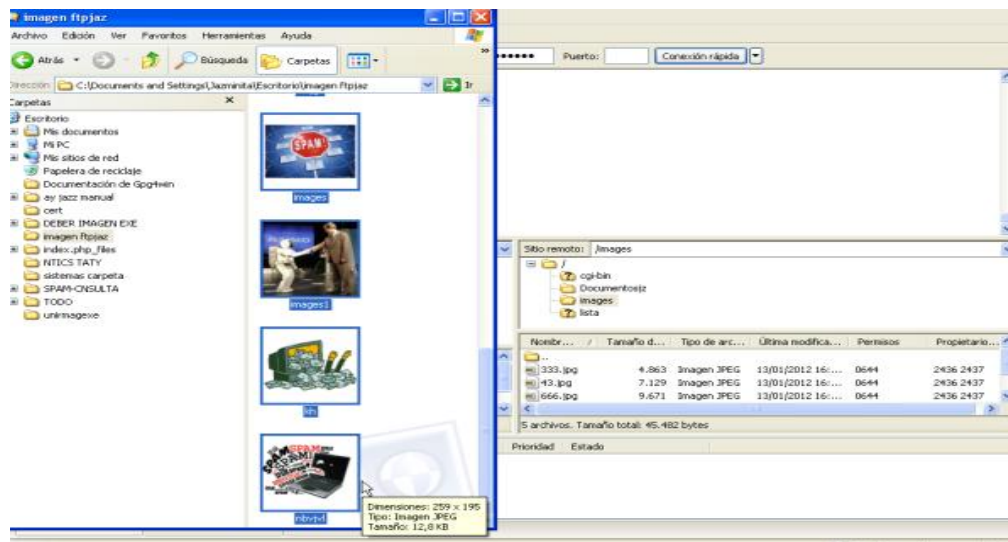
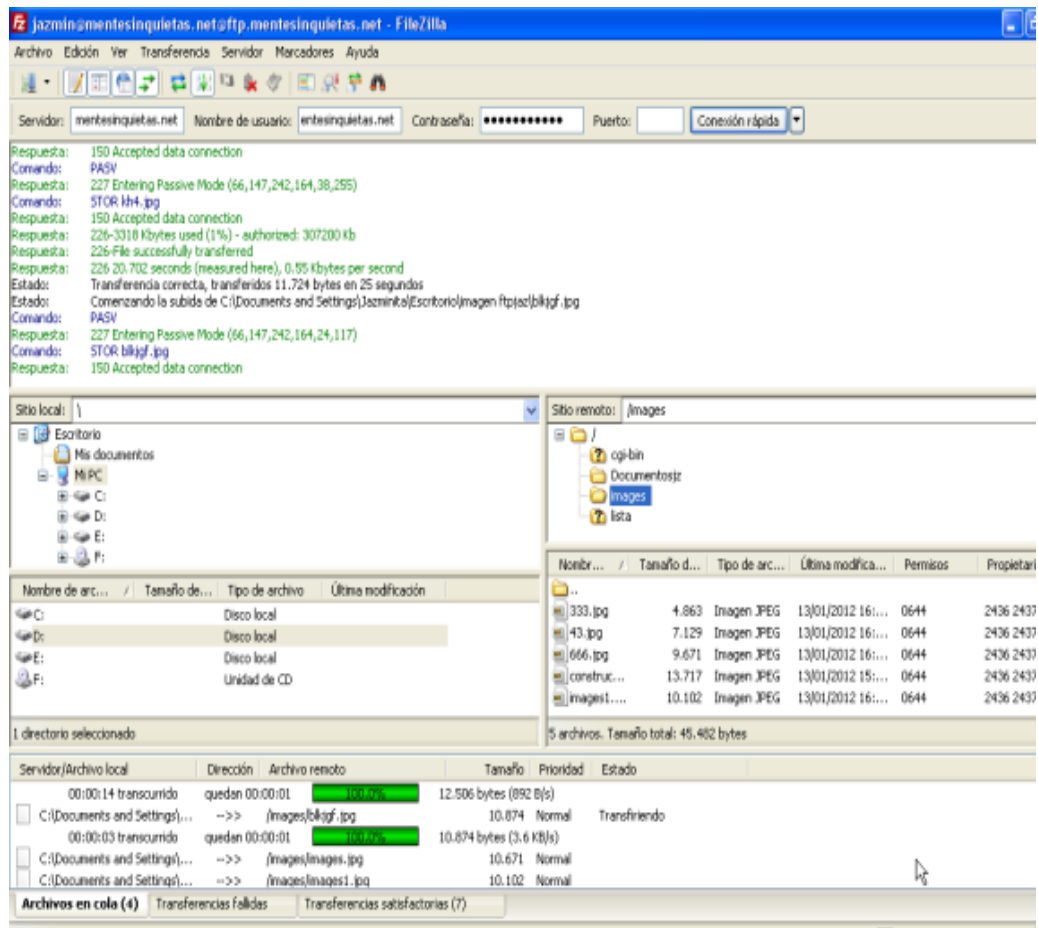


Gráfico 6. 32 Subir imágenes al Hosting

Ahora ya cuando se han seleccionado los elementos que se van a añadir se mostrara la carga de cada uno de ellos luego de unos momentos ya al finalizar dicha carga se podrá comprobar el éxito o fracaso de la misma desde el hosting accediendo al directorio en donde lo almacena a través de la barra de direcciones.



**Gráfico 6. 33** Verificación en el cliente con la información del hosting

Así podrá utilizarlos en el cuerpo del mensaje que vamos a enviar, al crear un mensaje se despliegan algunas opciones entre ellas una imagen donde se añade una figura, en este caso el formato es el mismo claro que con la diferencia que se debe especificar la dirección que tiene la imagen dentro del hosting.



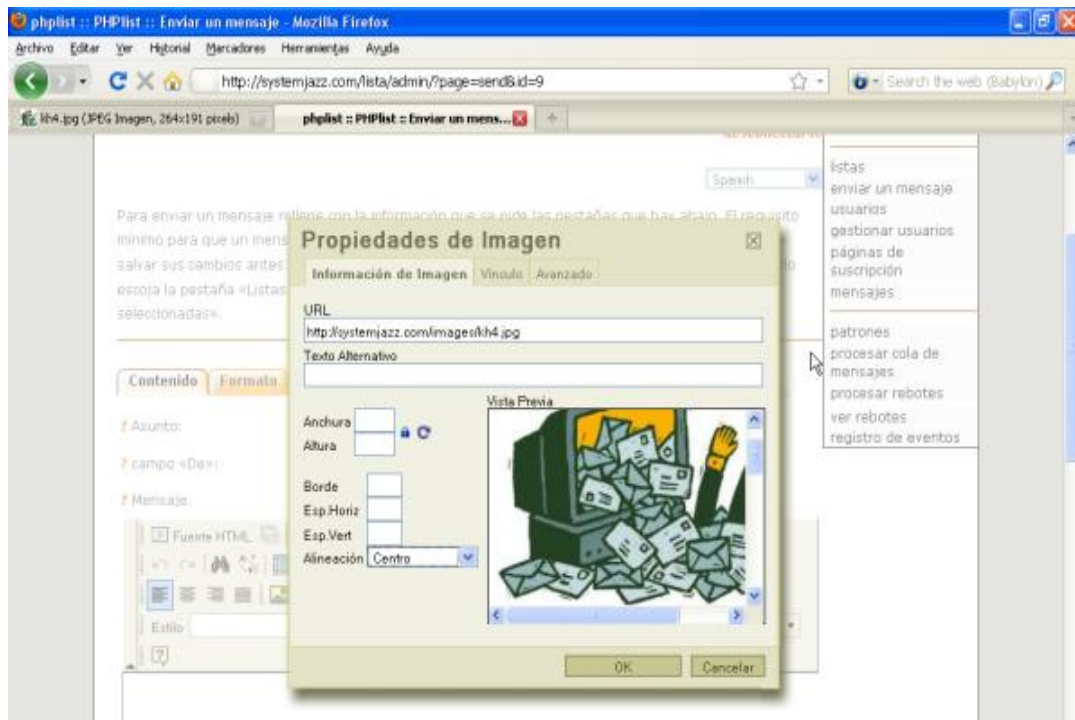


Gráfico 6. 34 Propiedades de imagen a adjuntar al mensaje

En la ventana que aparece la opción para añadir una imagen se puede configurar sus propiedades como su alineación y tamaño, al finalizar la imagen será adjuntada en el cuerpo del mensaje.

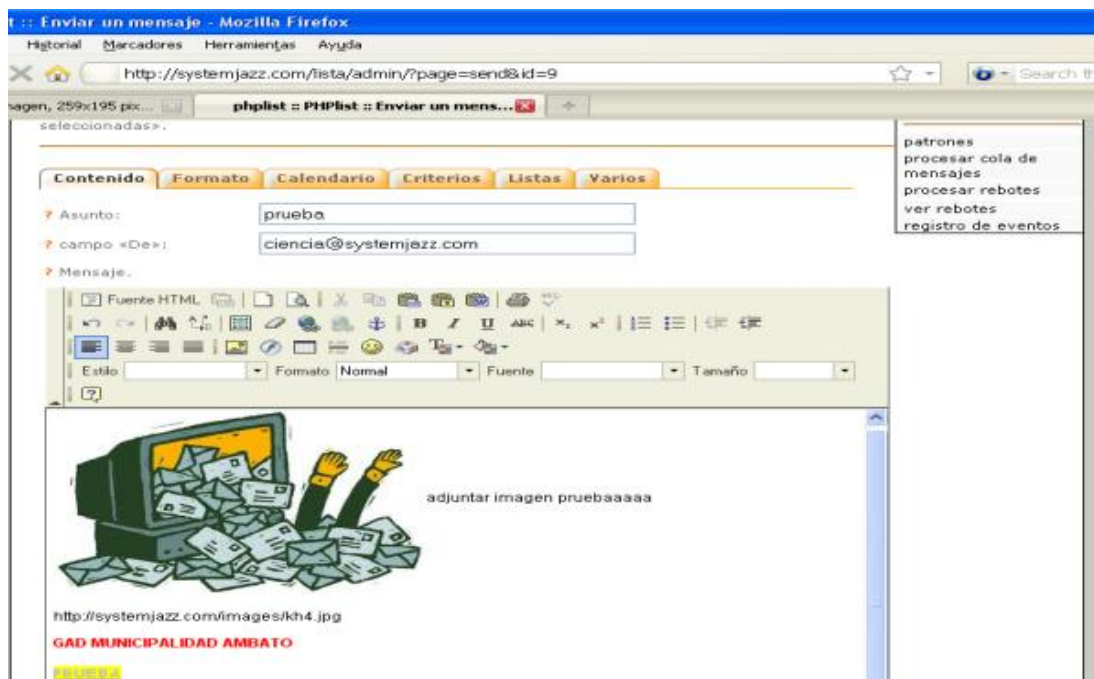


Gráfico 6. 35 Adjunto de imagen en el mensaje

Ahora para guardar todos los cambios efectuados se presiona el botón salvar cambios.

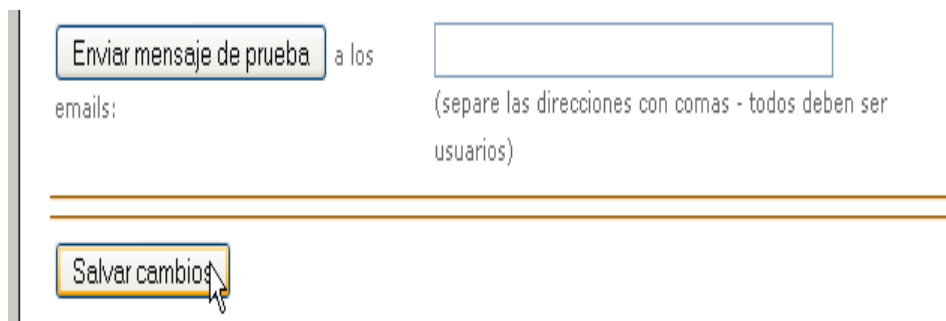


Gráfico 6. 36 Guardar cambios en mensajes

Para especificar los destinatarios se tiene la opción de seleccionar la lista de contactos a los que queremos que llegue el mensaje. Guarde los cambios y envíe el mensaje; pero para que el o los mensajes sean enviados deberá procesar la cola de los mensajes.

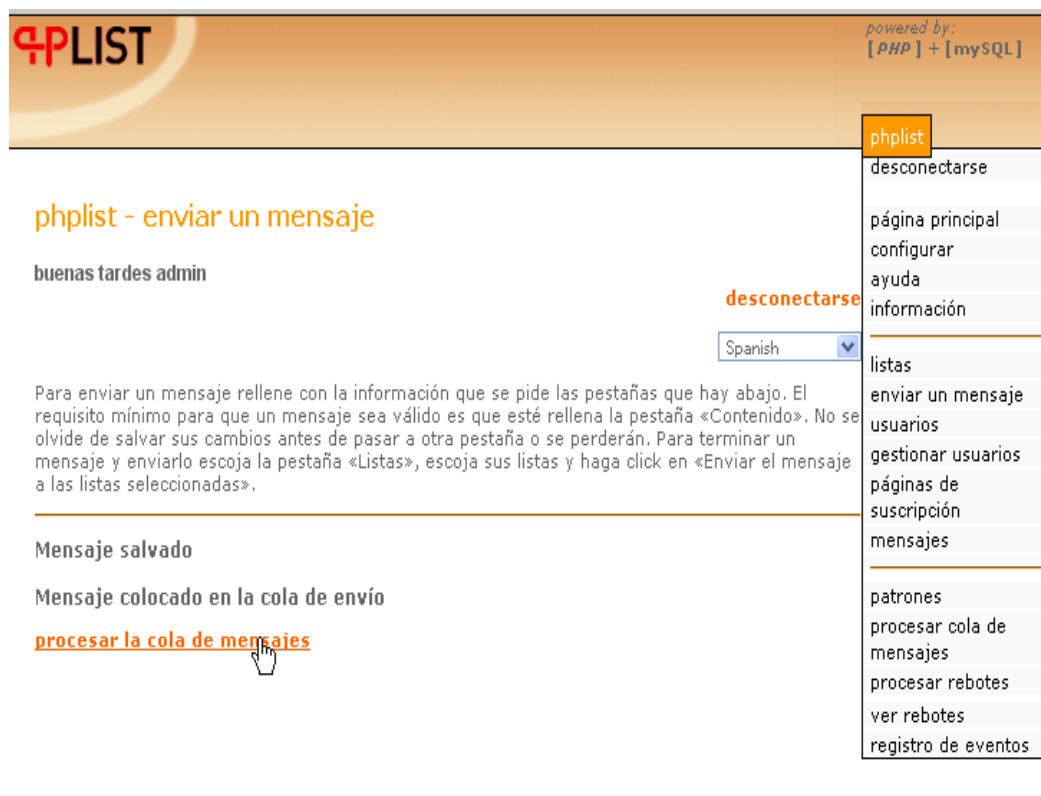


Gráfico 6. 37 Procesamiento de sola de mensajes

Al dar clic en esta opción aparecerá una ventana donde se ve el proceso de envío de mensajes, y notifica cuantos mensajes han sido enviados satisfactoriamente.

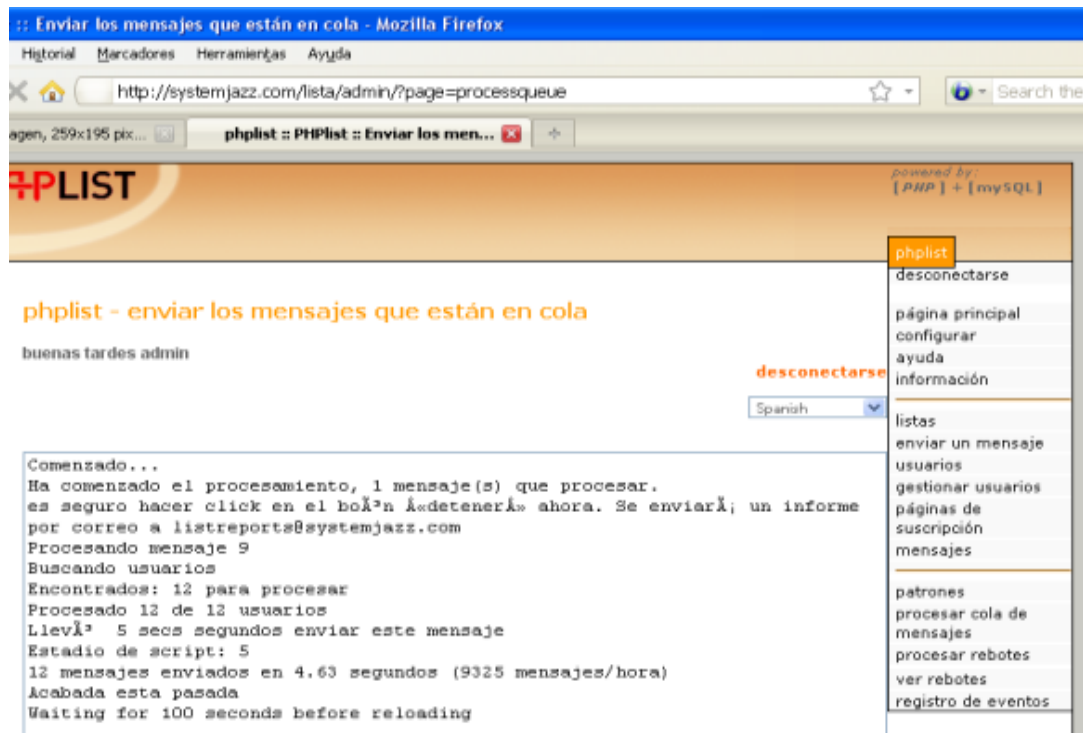


Gráfico 6. 38 Verificación de envío de mensajes en cola

Para verificar que el envío ha sido exitoso se ha creado una cuenta alternativa donde se han recibido los mensajes enviados a manera de prueba.



Gráfico 6. 39 Comprobación de recepción de mensaje

Así queda comprobado que el spam usa métodos diversos que le permiten llegar a las bandejas de usuario de millones de personas en el mundo, en este caso a cada funcionario del GADMA.

Con estas pruebas se puede decir que es muy simple añadir contenido como imágenes o contenido ejecutable al unirlo o incrustarlo una imagen u archivo, el mismo que en varios casos se trata de código malicioso que trata de apoderarse de los ordenadores de los destinatarios;

Para las pruebas se usan archivos ejecutables que no causen daños a los ordenadores que abran el mensaje.

### 6.6.3.2. Prueba con la herramienta Thunderbird

Thunderbird es otra herramienta que como ya se explico anteriormente permite enviar fácilmente correos electrónicos, para usarlo debe configurar primero la cuenta y tipo de servidor de correos al que se va a conectar, a ello se refiere la configuración de la cuenta donde añade el nombre del emisor con el que se desea enviar el mensaje, y especificar el servidor del protocolo smtp y servidor de correos pop3.

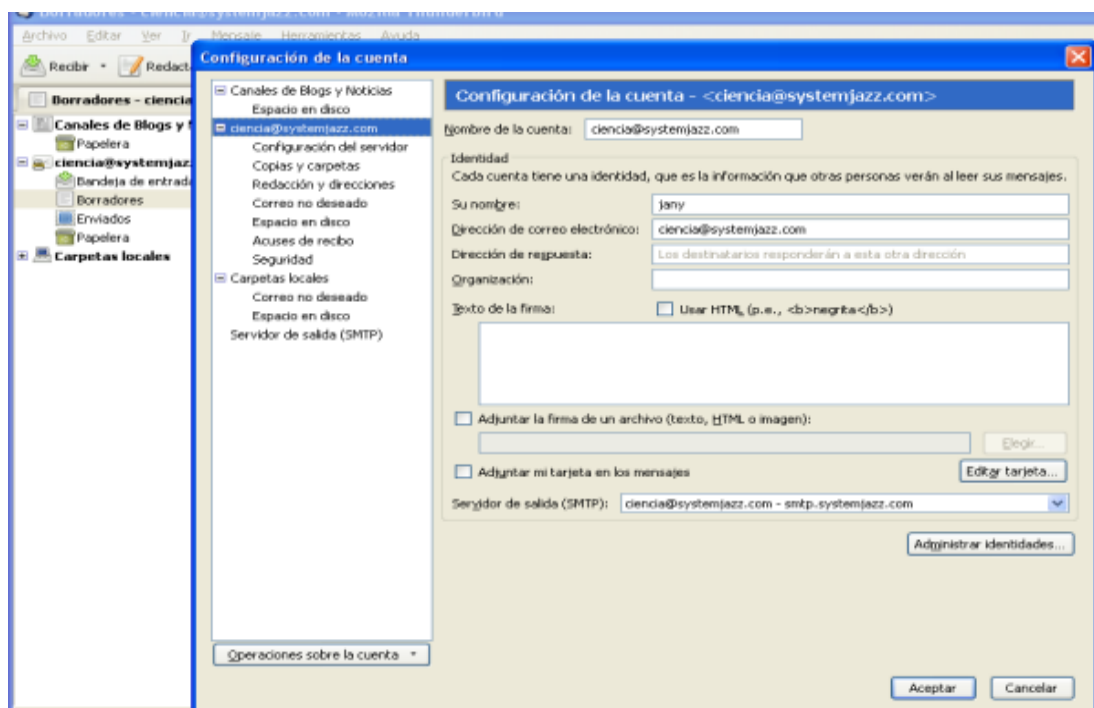


Gráfico 6. 40 Configuración para prueba de envío MT

Una vez configurado el servidor de correos, la manera de enviar mensaje es sencilla y muy parecida a varios servicios de correo electrónico, para enviar un mensaje se especifica el asunto, el destinatario y se añade al cuerpo de mensaje el contenido deseado, además tendrá la opción de añadir todo tipo de contenido, para probar se puede adjuntar una imagen con un ejecutable incrustado.

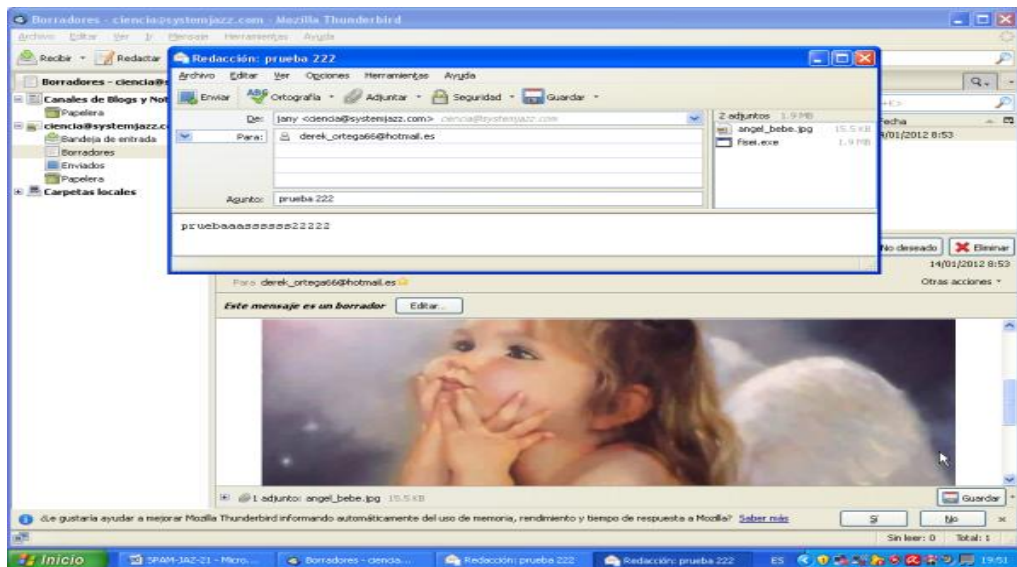


Gráfico 6. 41 Especificación de Destinatarios

Al terminar de escribir este mensaje, lo enviara a los destinatarios elegidos.

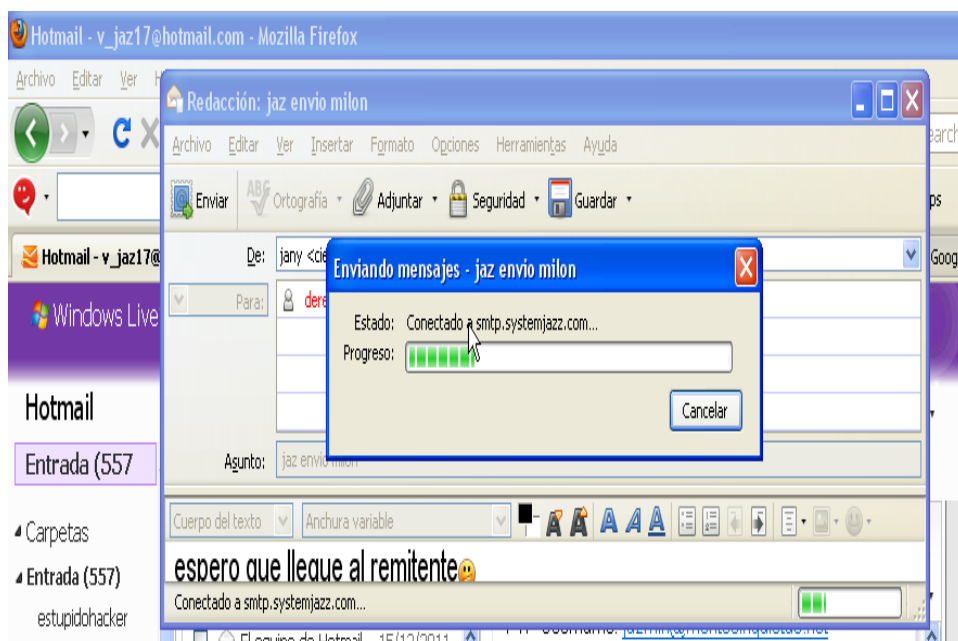


Gráfico 6. 42 Ventana de carga de mensaje MT

Como se sigue trabajando con cuentas a prueba se puede verificar que el mensaje llego a su destino:

Una de las maneras es comprobar que el mensaje este en la bandeja de salida de mozilla thunderbird:

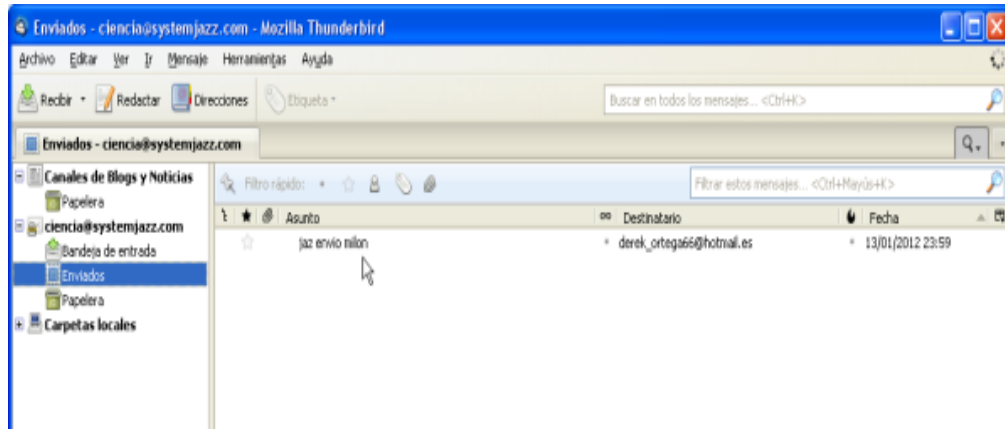


Gráfico 6. 43 Bandeja de salida MT

Y la otra opción, además más segura es verificar por si mismos el mensaje recibido en la cuenta que ya se tenía para verificar las recepciones.

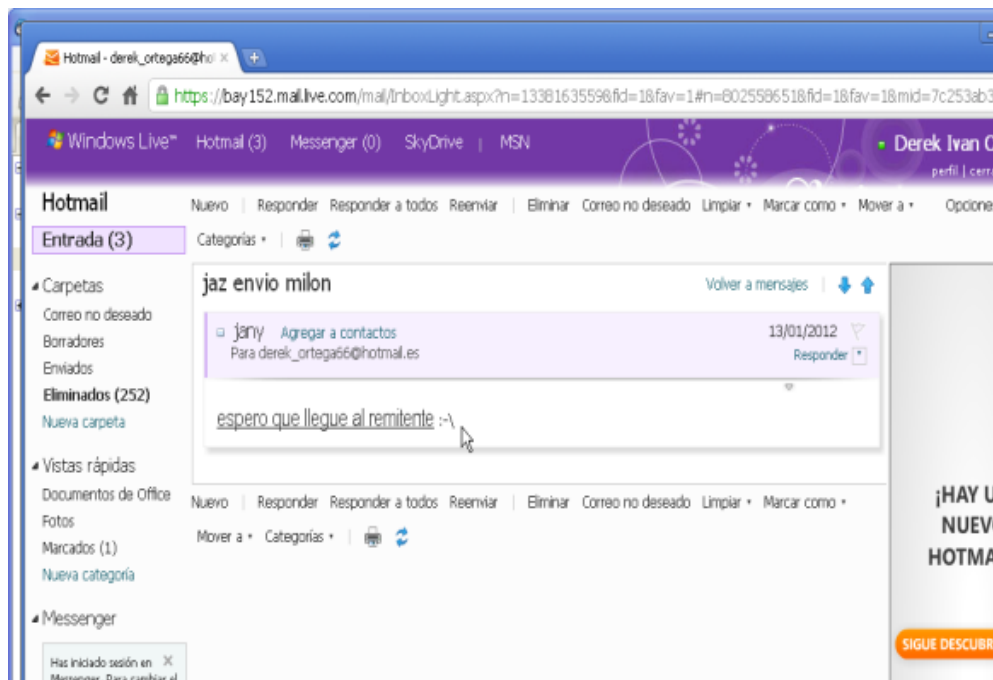


Gráfico 6. 44 Bandeja de entrada cuenta alternativa

Así se muestra que los famosos spammers ahorran mucho dinero utilizando pocos recursos, e incrementan sus ingresos con el éxito que da la publicidad o contenido recibido por sus víctimas.

### 6.6.3.3. Prueba con la herramienta Claws-Mail

Con la herramienta Claws-Mail el proceso es similar, se configura una cuenta especificando el servidor de correo y a continuación se podrá iniciar con la creación, recepción y envío de mensajes a correos electrónicos.

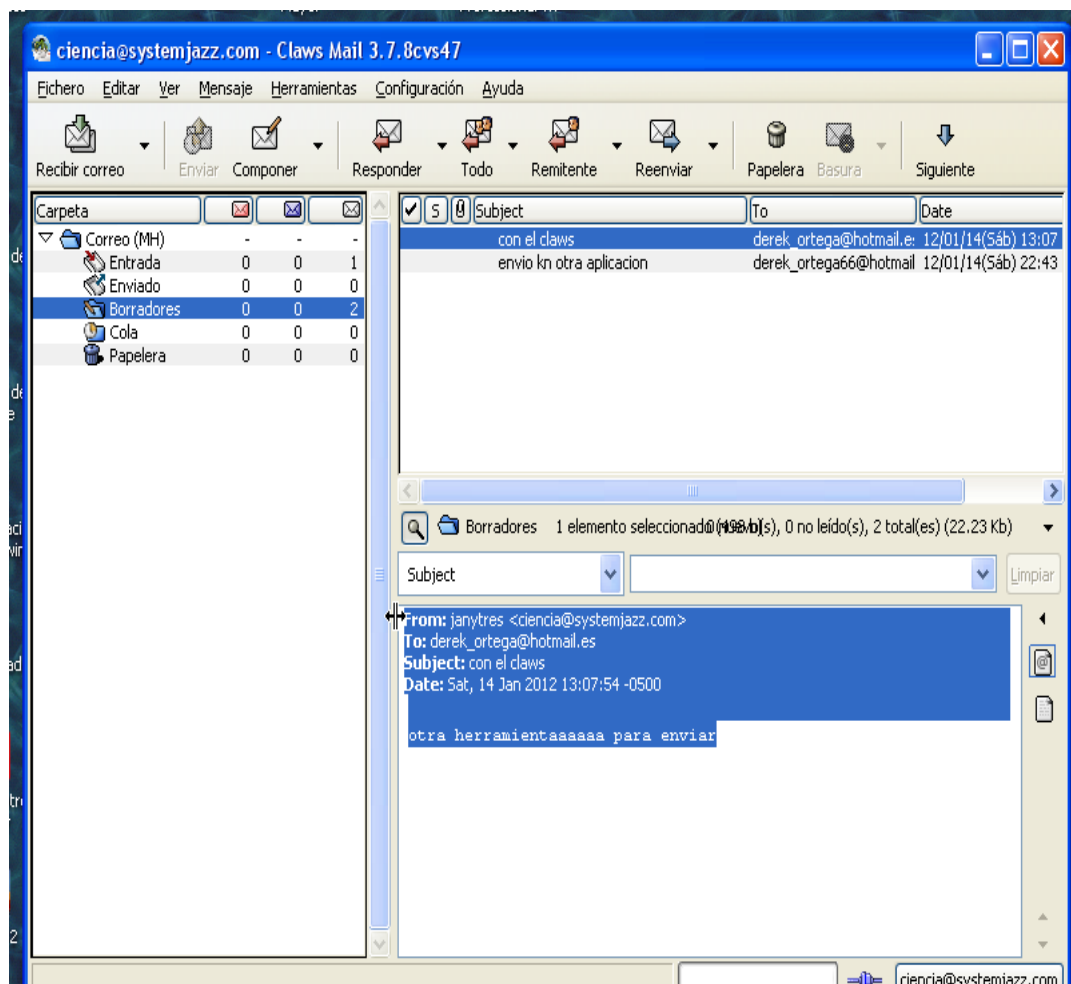


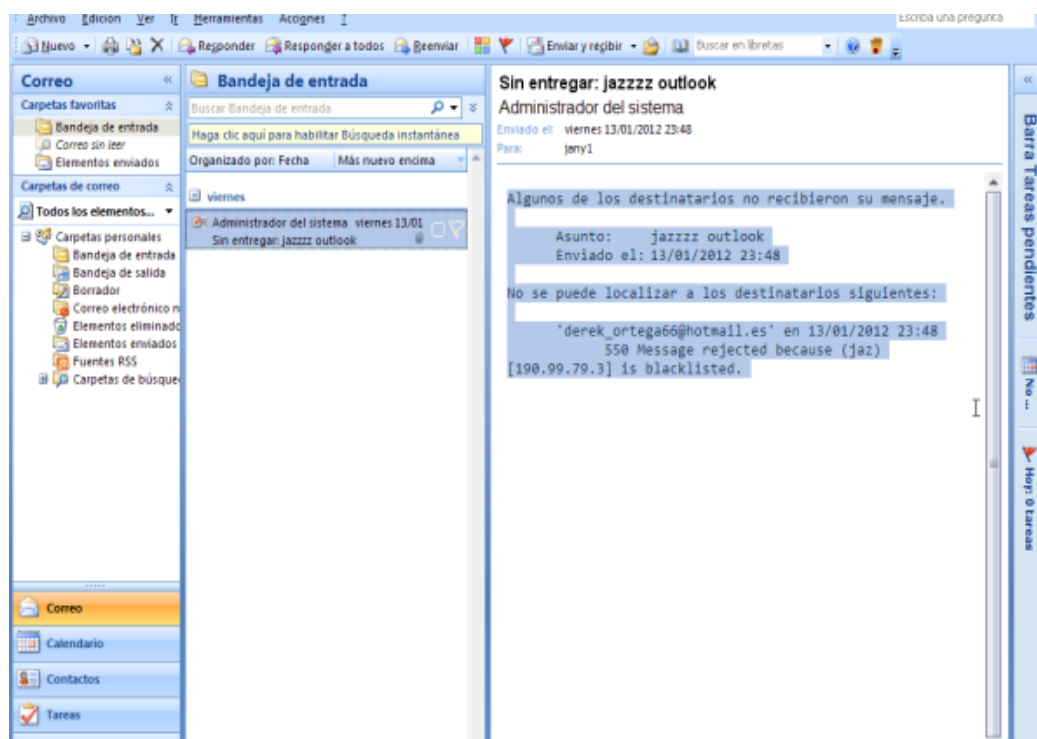
Gráfico 6. 45 Envío de mensaje con Claws Mail

### 6.6.3.4. Prueba con la herramienta Outlook.

Con Outlook se realiza también la prueba de envío de mensaje, en este se configuro también una cuenta para el servidor de correos, pero al momento de



enviar los mensajes estos no pudieron llegar ya que la dirección que emitía el mensaje fue detectada como miembro de una lista negra. Con ello se confirma que dependiendo del tipo de cuenta que se tenga existen varios filtros para detectar el spam.



**Gráfico 6. 46** Detección de cuenta en black list

En la figura anterior se muestra el mensaje de error recibido para notificar que la dirección reposa en una blacklist, que es una lista negra en donde reposan o se archivan las direcciones desde las que se ha difundido mensajes calificados como spam.

Con la obtención de varias cuentas de correo electrónico adicionales a las de los funcionarios se realizaron estas pruebas comprobando que las técnicas de propagación de spam, funcionan satisfactoriamente.

#### **6.6.4. Análisis comparativo de las pruebas Spam.**

Al finalizar las distintas pruebas de envío de mensajes, es necesario saber un valor aproximado del número de éxitos y fracasos que tuvieron las diferentes



herramientas que se han utilizado, además de diferenciar cuales son los servidores de correo electrónico que tienen mejores detectores y filtros de spam.

Para hacer las primeras pruebas se tomó únicamente una parte del total, aplicando la formula de obtención de muestra el valor sobre el cual se trabajará será 100, pero en estas prueba se estimaron 250 cuentas.

Para ello se ha elaborado un grafico comparativo donde se especifica la herramienta utilizada para enviar mails, además del número de éxitos y fracasos que se obtuvieron.

herramienta	# cuentas	# exitos	# fallos
php list	25	23	2
moxila thunderbird	25	25	0
Outlook	25	10	15
Claws-Mail	25	15	10

Gráfico 6. 47 Comparación de herramientas de envío de mensajes

Se puede observar que no todos los envíos tuvieron éxito, esto dependió del tipo de mensaje y del tipo de filtro antispam que poseen los proveedores de las cuentas de correo electrónico de los destinatarios.

Por cada herramienta utilizada se presentan los gráficos donde muestra su éxito y fracaso por envíos.

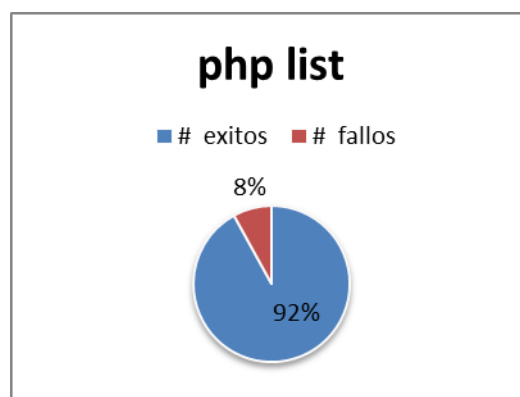


Gráfico 6. 48 Éxitos con PHPList

Utilizando phplist se ha obtenido un 92% de éxitos, lo que significa que es una buena herramienta que se puede utilizar para enviar este tipo de información.

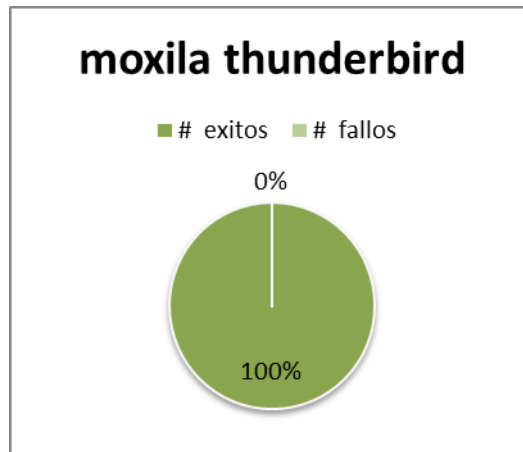


Gráfico 6. 49 Éxitos con MT

En el caso de Moxila Thunderbird es evidente el éxito alcanzado ya que permite enviar información y añadir todo tipo de archivo, incluso una imagen con un .exe incrustado.

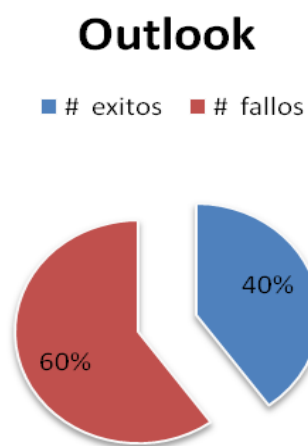
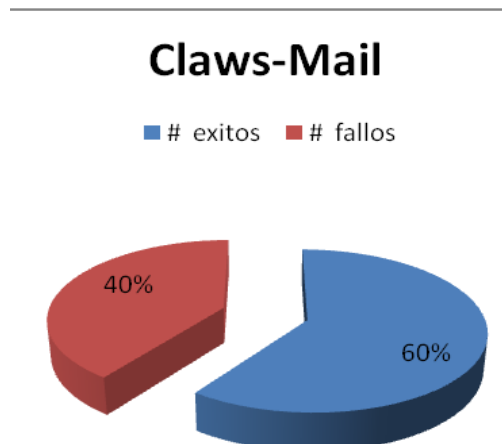


Gráfico 6. 50 Éxitos con Outlook

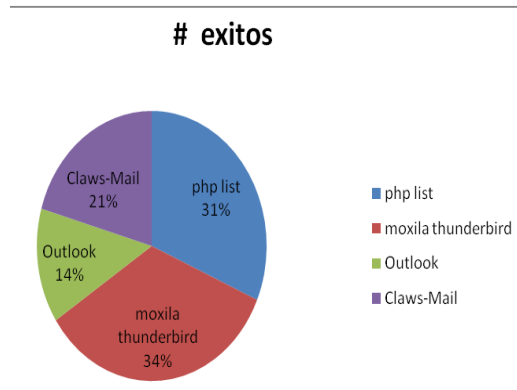
Para Outlook las pruebas dieron a conocer que no todos los mensajes enviados fueron recibidos, pues detecta con mayor rigor el contenido adjuntado e incrustado en el cuerpo del mensaje.



**Gráfico 6. 51** Éxitos con Claws-Mail

Claws-Mail también es una herramienta diseñada para el envío masivo de información no deseada a cuentas de correo electrónico, pero presenta un alto porcentaje de error, pues 4 de cada 10 mensajes enviados han sido rebotados, además dependiendo del servidor de correo electrónico desde el que se envíe la información, este puede o no procesar el envío de mensajes.

Al culminar se dio como resultado general que cada herramienta es buena, pero mozilla thunderbird presento mejores resultados que las demás, obteniendo el mayor número de éxitos; mientras Outlook y claws-mail por su configuración misma no permitió que todos los mensajes lleguen a su destino. Reportando al final la dirección de envío como una parte de una lista negra.



**Gráfico 6.52** Comparación entre Herramientas aplicadas

Con todo esto se podrá culminar el presente trabajo con normas y tips útiles y eficaces para reducir el spam, llamado también correo no deseado.

## **6.7. DESARROLLO DEL MANUAL**

Al termino de estas pruebas para cumplir con los objetivos de la investigación se procedió a realizar un manual con una guía teórica y práctica acerca de las técnicas spam, el contenido del mismo está basado en definiciones de términos para que los usuarios se familiaricen con el tema, además de especificar los aspectos básicos del spam, como reconocerlo, como evitar ser víctimas de él y medidas que deberán tomar para evitar propagarlo y recibirlo.

Todo esto se podrá observar en el anexo 3 de esta investigación.

## **6.8. CONCLUSIONES Y RECOMENDACIONES**

### **6.8.1. CONCLUSIONES**

La técnica de envío de mensajes en cadena por medio de los propios usuarios es la más común, al pasar desapercibida para el usuario.

Las herramientas de servidor de correo electrónico son fundamentales para la propagación de mensajes spam, cuando estas tienen una configuración especial para admitir el spam.

Mozilla Thunderbird presento mejores resultados, obteniendo el mayor número de éxitos al enviar spam.

Con Claws- mail no todos los mensajes pudieron ser entregados debido a sus configuraciones internas, propias de la herramienta.

Al utilizar Phplist se obtuvo un 92% de éxitos, demostrando ser una buena herramienta para enviar y propagar spam.

No todos los envíos tuvieron éxito, cada entrega satisfactoria dependió del tipo de mensaje incrustado y el tipo de filtro antispam que poseen los proveedores de las cuentas de correo electrónico de los destinatarios.

A pesar de los fracasos de envío el porcentaje de éxitos con las herramientas utilizadas fue bastante alto, logrando así enviar la mayora cantidad posible de spam.

#### **6.8.2. RECOMENDACIONES**

Como se ha podido observar en la mayoría de casos son los usuarios de cuenta de correo los que ayudan a propagar el spam por lo que se recomienda que al recibir un mensaje fijarse en los siguientes aspectos que indicarían la recepción de un mensaje spam:

- Si el Asunto es llamativo
- Idioma del asunto que generalmente es inglés
- Si el cuerpo del mensaje suele ser publicidad agresiva prometiendo milagros sobre algo.
- Al ser un mensaje de Remitente desconocido.
- No tener una dirección de respuesta.

Por otro lado se sabe que evitar en un 100% el spam resulta ser casi imposible pero se puede evitar en un gran porcentaje ser víctimas de él, siguiendo las siguientes sugerencias:

- Cuidado con los mails en cadena: suele ser una táctica de los spammers para lograr que cuando un usuario va reenviando el email “secuestrar” todas las direcciones.
- Usar la copia oculta: al enviar un email a muchas personas se debe usar la opción Copia Oculta (CCO) para evitar que nadie tenga acceso a las direcciones de email de nuestros contactos.
- Su email en internet: no debe publicar su dirección en webs de libre acceso ya que usan robots para “coger” las direcciones que hay escritas en páginas webs.
- Segunda cuenta de correo: cree una cuenta de correo alternativa y gratuita para los sitios que pidan una cuenta de email para darse de alta, así nuestra su cuenta personal estará a salvo.
- No responder al spam: jamás se debe contestar a un mensaje de spam porque si lo hace, estará confirmando que la cuenta es buena y operativa

## **BIBLIOGRAFIA**

### **Libros**

JORGE Ramiro Aguirre, Libro Electrónico de Seguridad Informática y Criptografía, año de publicación 2006. Versión 4.1

AGUILERA, Purificación. Seguridad Informática. Editorial Editex, Madrid- España.

### **Tesis**

GUZMÁN GARZÓN, Nancy, “Seguridad en el Perímetro de la Red Petroindustrial”, Quito, junio 2005, con repositorio en <http://repositorio.iaen.edu.ec:9090/bitstream/123456789/351/1/IAEN-034-2005.pdf>

### **Internet**

Definición de Informática. MASTERMAGAZINE. Extraído el 22 de noviembre de 2011 desde <http://www.mastermagazine.info/termino/5368.php>

Definición de Seguridad Informática. MASTERMAGAZINE. Extraído el 22 de noviembre der 2011 desde <http://www.mastermagazine.info/termino/6638.php>

Libro Electrónico de Seguridad Informática y Criptografía. Jorge Ramiro Aguirre. Extraído el 22 de noviembre de 2011 desde [http://www.criptored.upm.es/guiateoria/gt\\_m001a.htm](http://www.criptored.upm.es/guiateoria/gt_m001a.htm)

Ataque Informático. Wikipedia. Extraído el 22 de noviembre de 2011 desde [http://es.wikipedia.org/wiki/Ataque\\_inform%C3%A1tico](http://es.wikipedia.org/wiki/Ataque_inform%C3%A1tico)

Ataques Informáticos. Carpetaandres10. Extraído el 22 de noviembre de 2011 desde

<http://carpetaandres10.blogspot.es/1297729440/>

Que es el Spam. Sandro Marcone. Extraído el 22 de noviembre de 2011 desde

<http://sandromarcone.blogspot.com/2008/11/qu-es-el-spam.html>

Evaluación de alternativas para reducir el spam. Jesús Sanz. Extraído el 22 de noviembre de 2011 desde

<http://www.rediris.es/mail/abuso/doc/MedidasAntiSPam.pdf>

Contra el bombardeo electrónico. El Espectador. Extraído el 22 de noviembre de 2011 desde

<http://www.espectador.com/spam/spam.htm>

Técnicas de SPAM I. Manuel Gil Barrio. Extraído el 22 de noviembre de 2011 desde

[http://blogs.oracle.com/mgil/entry/font\\_id\\_z\\_dd\\_size](http://blogs.oracle.com/mgil/entry/font_id_z_dd_size)

Spam-Técnicas de spam. Wikilearning. Extraído el 22 de noviembre de 2011 desde

<http://www.wikilearning.com/monografia/spam/5515-3>

Internet, Correo electrónico y Outlook. Javier Fajardo. Extraído el 22 de noviembre de 2011 desde

<http://www.monografias.com/trabajos21/internet-correo-outlook/internet-correo-outlook.shtml>

Nueva forma de enviar spam usando el autoresponder. Volkan Rivera. Extraído el 22 de noviembre de 2011 desde

<http://www.volkanrivera.com/esp/?p=260>



La Tecnología de la Información y la Comunicación (TIC). Su uso como Herramienta para el Fortalecimiento y el Desarrollo de la Educación Virtual. Jimmy Rosario. Extraído el 22 de noviembre de 2011 desde <http://www.cibersociedad.net/archivo/articulo.php?art=218>

Envío de spam: tecnologías modernas. Viruslist. Extraído el 22 de noviembre de 2011 desde <http://www.viruslist.com/sp/spam/info?chapter=153350528>

Correo Spam. Sergio Alavéz Miguel. Extraído el 22 de noviembre de 2011 desde <http://www.seguridad.unam.mx/descarga.dsc?arch=1227>

Según la BSA el robo de información y descarga de software ilegal son los mayores peligros en Internet. Extraído el 22 de noviembre de 2011 desde <http://www.delitosinformaticos.com/03/2007/propiedad-intelectual/segun-la-bsa-el-robo-de-informacion-y-descarga-de-software-ilegal-son-los-mayores-peligros-en-internet>

# ANEXOS

## Anexo 1

### Encuesta

UNIVERSIDAD TÉCNICA DE AMBATO



FACULTAD DE INGENIERÍA EN SISTEMAS



CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES E  
INFORMÁTICOS

LUGAR A ENCUESTAR: Gobierno Autónomo Descentralizado Del Ilustre  
Municipio De Ambato

OBJETIVO DE LA ENCUESTA: En la presente encuesta el objetivo es realizar  
un estudio de las técnicas de envío de spam, saber si el funcionario ha sido  
víctima de spam y cuáles fueron las posibles causas.

INDICACIONES: Señores, su veracidad en las respuestas permitirá al grupo  
investigador desarrollar un trabajo real y efectivo.

Agradecemos su colaboración y garantizamos absoluta reserva de su  
información.

### CUESTIONARIO

1. Ha sido Ud. víctima de un spammer?

Si  No

2. Su sistema ha sido infectado por algún tipo de virus o gusano en los  
últimos meses?

Virus  Gusano

3. Cree que su cuenta es segura y no consta en listas de correos para envío de mensajes spam, porque?

Su cuenta no consta en listas de correo de spammers

No ha caído en técnicas de spam

Jamás recibe spam en su correo electrónico

4. Qué tipo de técnica usa para proteger su computador?

Antivirus

Firewall Activado

Restricción a sitios web inseguros

5. Le ha llegado a su correo alguna vez mensajes publicitarios ofreciéndole algún producto o servicio?

Productos farmacéuticos

Servicios de pornografía

Servicios de viajes y turismo

Tecnología

6. En su cuenta de correo de tipo pop o web, su bandeja electrónica se llena de mensajes de sus contactos o de remitentes desconocidos?

Pop

Web

Remitentes:

Desconocidos

Conocidos

7. Cuando se conecta desde lugares diferentes a su trabajo, sabe si los servidores proxy utilizados son seguros?

Si

No

8. El Municipio ha sufrido algún tipo de pérdida de información?

Datos,

Imágenes,

Videos,

Mensajes vía mail

9. ¿Ah escuchado sobre alguna herramienta de software para el envío masivo de spam?

Mail marketing

Ay Mail

Boot spam

10. ¿Ah recibido y reenviado alguna vez mensajes de texto con cadenas a sus contactos?

Si

No

## Anexo 2

### Glosario de Términos

En el siguiente glosario se presentan los términos usados frecuentemente en el entorno de uso de técnicas spam para envío masivo de información no deseada a cuentas de correo electrónico.

**Ataque Informático:** Es la acción o método que una persona a través de un sistema informático trata de tomar el control de un computador de otro usuario o una red para desestabilizar o dañar otro sistema

**Blog:** Pagina web constituida por textos o entradas, ordenados cronológicamente, en donde una nueva entrada o anotación aparece en la parte superior de la página tiene facilidad de actualización de contenidos y presentación visual.

**Directorio:** Llamado así a la carpeta o conjunto de carpetas que poseen varios archivos o datos almacenados dentro.

**Ejecutable:** Es el tipo de archivo que tiene la opción de correr o ser cargado automática o manualmente.

**Foro:** Se llama así al grupo de usuarios que tienen un espacio donde poder compartir constantemente todo tipo desinformación, opiniones, archivos además puede hacer preguntas y respuestas acerca de uno o un conjunto de temas.

**Hosting:** Es el alojamiento web, lo que significa poner una página web en un servidor de Internet para que la misma se pueda ver en cualquier lugar del mundo que tenga acceso al Internet.

**Malicioso:** Creado para causar daño o molestias en los ordenadores.

**Protocolo:** Lenguaje conformado por un conjunto de reglas que sirven para comunicar computadoras entre sí a través de la red local o de internet.

**Servidor:** Computador remoto encargado de proveer datos solicitados por parte de los navegadores de otros computadores, además en ellos se almacena gran cantidad de información en forma de páginas web y a través de protocolos de internet.

**Software:** Herramienta o programa informático creado por un conjunto de reglas, sentencias y códigos en base a cumplir una o varias funciones, tomando en cuenta las necesidades del usuario o entidad interesada.

**Spam:** Se llama así a todo tipo de información no solicitada, también llamada correo basura, mensajes que no han sido pedidos y cuyo remitente es desconocido, los mismos que son difundidos por medio del internet en la mayoría de los casos, en e-mail, redes sociales, foros, o mensajes a celulares.

**Spammer:** Aquel individuo que se encarga de propagar la mayor cantidad posible de spam mediante varias técnicas, con el fin de propagar publicidad o contagiar de virus o programas maliciosos a computadores de usuarios desconocidos.

**Virus:** Programa creado para infectar un computador, o medio electrónico como flash memory, se propaga en el con el propósito de dañar o robar información, además de causar varias molestias, la mayoría de veces intenta pasar desapercibido ante el usuario.

**Web:** Significa red informática, se llama web al internet o a todo tipo de página de internet.

**Zombis:** Computador que ha sido atacado, y cuyo atacante se ha apoderado de sus sistema, el mismo que cumple funciones ordenadas por su atacante, pasando desapercibido por su legitimo administrador o propietario.



Anexo 3

**Resumen ejecutivo Informe Técnico-Manual de seguridad**



**UNIVERSIDAD TÉCNICA DE AMBATO**



**FACULTAD DE INGENIERÍA EN SISTEMAS ELECTRÓNICA  
E INDUSTRIAL**

**CARRERA DE INGENIERÍA EN SISTEMAS  
COMPUTACIONALES E INFORMÁTICOS**

**Tema:**

**MANUAL QUE GUIE A LOS FUNCIONARIOS  
DEL GOBIERNO AUTÓNOMO  
DESCENTRALIZADO MUNICIPALIDAD  
AMBATO PARA DISMINUIR EL EXCESIVO  
ENVÍO DE INFORMACIÓN NO DESEADA A  
SUS CUENTAS DE CORREO ELECTRÓNICO.**

## **1. Introducción**

La siguiente guía se presenta con el fin de ayudar a cada uno de los funcionarios del GADMA, para incrementar sus conocimientos acerca del SPAM y sobre todo para informar acerca de las medidas para prevenir ser víctima de un spammer, o convertirse en su víctima sin saberlo.

Tanto para las empresas como para los spammers a quienes les favorece e interesa enviar su publicidad y su código malicioso, les beneficia la existencia de diversas técnicas de envío de spam, las mismas que tienen grandes ingenios para burlar los filtros de herramientas informáticas que tratan de suprimir o detectar el spam, que está en los correos electrónicos, además de los foros, blogs o redes sociales.

El dinero es el motor de la propagación de mensajes basura en las cuentas de correo de usuarios de todo el mundo, ya que si al menos el 1% de todos los mensajes es enviado, para las empresas eso significa posibles y futuras ganancias.

Por lo tanto, todos los usuarios que poseen el servicio de cuentas de correo electrónico corren el riesgo de ser víctimas de estos intentos de ataques; y para ello se debe adoptar medidas de prevención para no exponer su información personal en sitios públicos, y dejar de caer en las famosas cadenas típicas de la actualidad.

## **2. Definiciones**

Primero se debe tener claro a cerca de lo que tratará esta guía, para ello se describe a continuación el significado más acertado para los términos o variables de la investigación realizada.

- 1) Spam.- Es aquella actividad que consiste en enviar correo no deseado en forma masiva y sin control, burlando filtros de seguridad, es común usar técnicas spam y poseer correos electrónicos o usar las redes sociales para enviar mensajes masivamente a distintas personas desconocidas; su objetivo generalmente es hacer publicidad, aunque también se pueden enviar virus con el spam, incluyendo principalmente spywares también llamados programas espías que atacan al computador de la victima sin que esta se de cuenta enseguida.
- 2) Spamer.- Se llama así a quién está detrás de los mensajes spam es decir quién los crea o los envía para beneficio propio o de la empresa a la que brinda sus servicio, un spammers consigue las direcciones de correo de forma fraudulenta o comprando listas de emails a terceros y así difundir su información, la publicidad que llega suele ser de productos dudosos e ilícitos; Usan llamativos títulos para intentar captar la atención del lector.
- 3) Correo Electrónico.- Es una aplicación que permite mandar un mensaje desde un computador a otro, esto se hace mediante una cuenta de correo, el dueño de dicha cuenta puede enviar o recibir mensajes sin importar que la otra persona no se encuentre en ese momento, ya que los computadores seguirán intentando comunicarse hasta conseguir la entrega del mensaje. Esto se realiza siempre y cuando se tenga conexión a la red (Internet).
- 4) Software.- Se llama así a todo programa o aplicación desarrollada para realizar tareas específicas. Un ejemplo de software son los programas que generalmente usamos en nuestros computadores, sin ellos solamente tendríamos el equipo físico y nada más.

- 5) POP3.-Es un protocolo que sirve para recibir mensajes e-mail conocido como Post Office Protocol 3 o Protocolo 3 de correo, su uso se ve cuando los e-mails enviados a un servidor, son almacenados por el servidor pop y si el usuario se conecta al mismo siempre y cuando conozca la dirección POP3, el nombre de usuario y la contraseña, podrá hacer la descargar los ficheros.
  
- 6) SMTP.- sus siglas quieren decir Simple Mail Transfer Protocol, que no es más que un protocolo de comunicaciones que utiliza un servidor de correo para enviar los mensajes hacia otro servidor de correo, para recibir los mensajes, el cliente de correo del receptor se comunica con su servidor de correo utilizando los protocolos POP o IMAP.

Ahora que sabe de qué trata cada término visto, hay que enfocarse en el problema que comúnmente se presenta en las cuentas de correo electrónico que posee cada funcionario, sea esta personal o laboral. Es decir la acumulación de mensajes en sus bandejas de entrada, los mismos que en su mayoría pertenecen a remitentes o contactos desconocidos, que no saben cómo obtienen sus cuentas de correo, además el contenido de dichos mensajes por lo general es publicitario, incitando a quien lo lee a comprar un producto, esto en el mejor de los casos, pues la pornografía y la propagación de malware o virus también representa una gran amenaza al propagarse este tipo de mensajes basura o spam.

Parecería increíble que con un simple mensaje de correo se pueda causar tantos daños o molestias a los lectores, pero si es posible, en la actualidad varias empresas usan técnicas spam para difundir información acerca de sus productos o servicios ya sean lícitos o no, por otro lado los famosos spammers también usan técnicas spam para enviar virus a través de códigos ocultos en los mensajes, estos pueden ser en imágenes, videos, links, o archivos adjuntos, cuyo fin sea infectar o apoderarse del computador que recibe el mensaje, si esto

ocurre nuestro computador podría pasar a ser un zombi, manejado y administrado por una máquina que puede encontrarse en cualquier parte del mundo administrada por un spammer o hacker.

### 3. Aspectos básicos de un mensaje spam

Es preciso saber cuáles son los mensajes con contenido spam para ello le daremos algunos aspectos que permitirán al usuario saberlo:

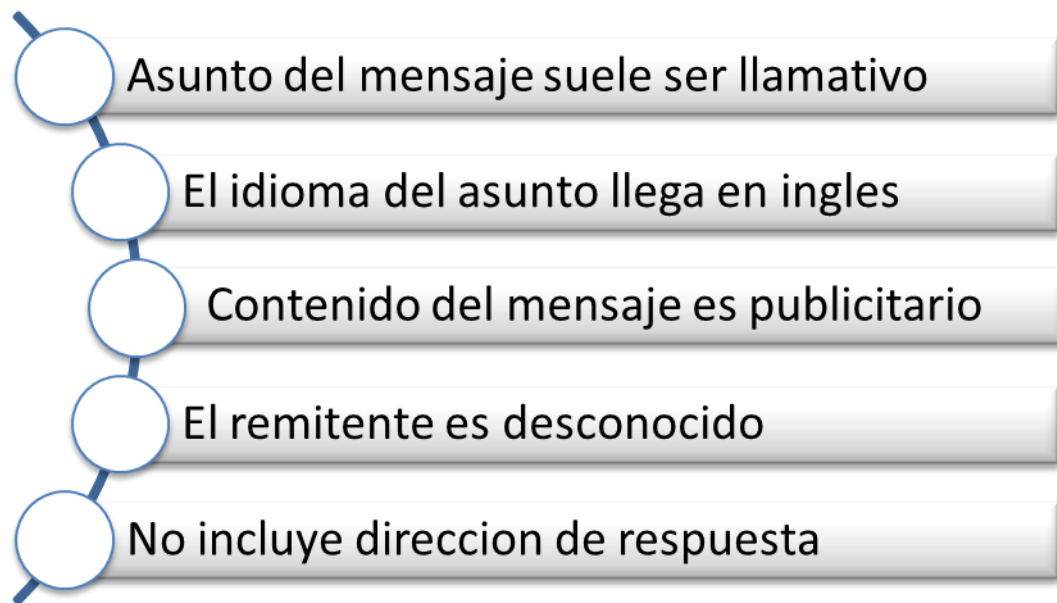


Gráfico A. 1 Reconocimiento de mensajes spam

En las siguientes figuras se podrá observar algunos de los aspectos mencionados para reconocer un mensaje spam.



Gráfico A. 2 Asusnto llamativo y en inglés

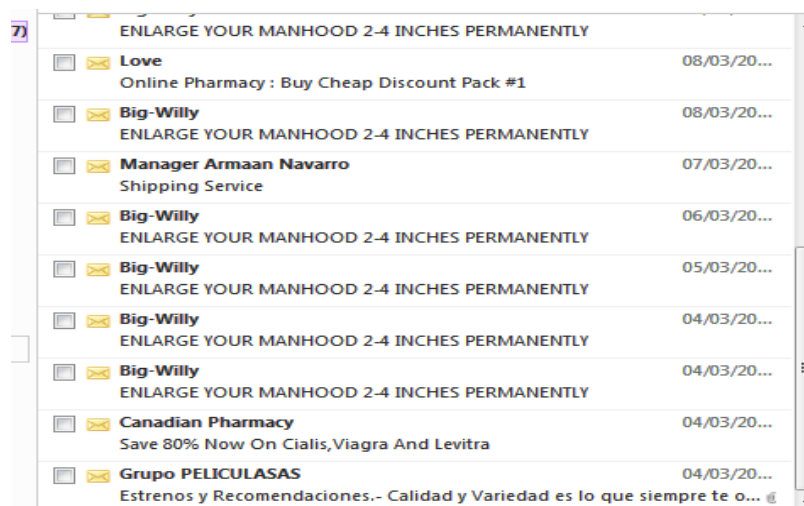


Gráfico A. 3 Mensajes spam asuntos y remitentes desconocidos

#### 4. ¿Qué causa el Spam?

La recepción de mensajes spam trae algunas complejidades entre ellas tenemos las siguientes:

Inunda los buzones de correo, saturando la capacidad máxima de los mismos y por lo tanto, provocando la pérdida de correo deseado y útil.

Reduce la efectividad del correo al ser molesto u ofensivo para el receptor.

Afecta los recursos de los servidores ya que procesar *spam* hace lento el procesamiento del correo normal y otros procesos.

Afecta al ancho de banda congestionando las infraestructuras de comunicaciones utilizadas para el servicio del correo electrónico y la conexión a Internet en general.

Afecta el tiempo empleado por los usuarios en leer, borrar, denunciar, filtrar etc. Y también el tiempo de los responsables de la gestión de los servidores de correo.

Afecta la imagen de la Empresa que distribuye el spam.

Son los afectados y las víctimas los que en últimas terminan pagando los costos y recibiendo todo el impacto negativo del spam.

Causa pérdida de confianza en el servicio de correo electrónico.

Amenaza la viabilidad del Internet como un medio efectivo de comunicación, comercio electrónico y productividad para las empresas.

Puede dañar la imagen de terceros, pues puede ser utilizado para el envío de spam con direcciones falsificadas y éste no estarse dando cuenta.

Puede llegar a dañar la infraestructura informática, por un uso inútil de la banda ancha, la denegación de servicio por saturación o la transmisión de virus y gusanos.

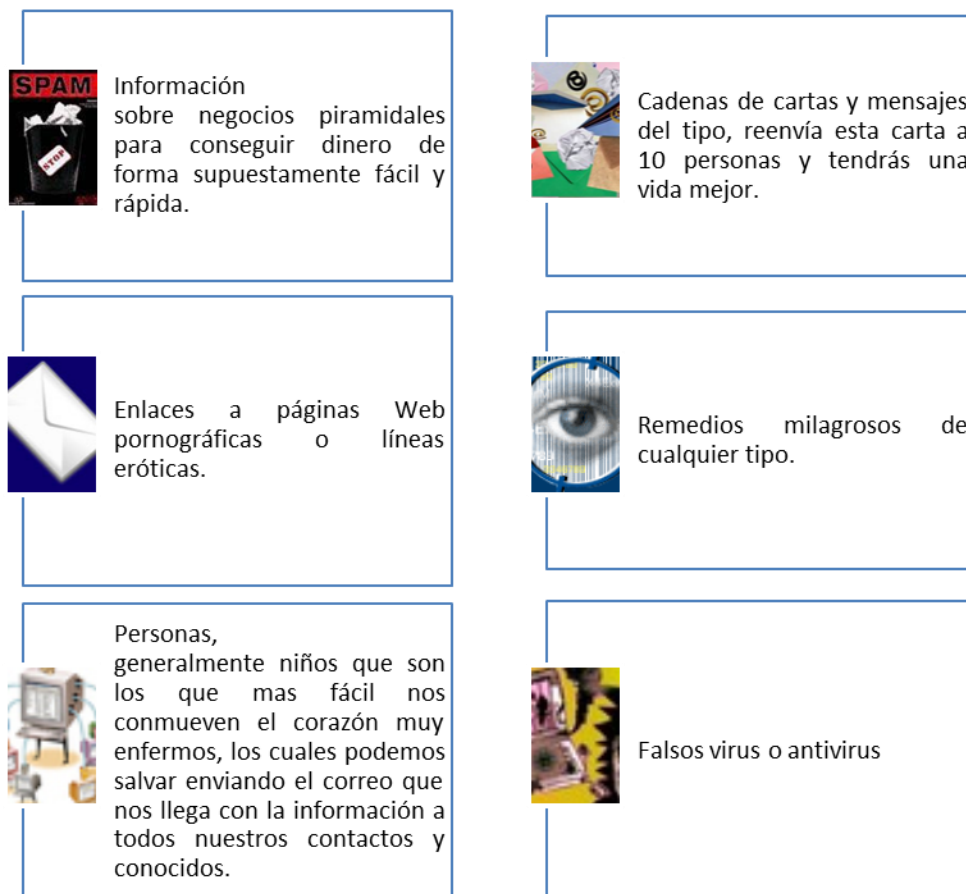
Afecta la productividad empresarial.

Genera importantes costos a las empresas e ISPs.
Se ha transformado en un medio para la comisión de delitos tales como el fraude, la pornografía infantil, entre otros.
Incremento de la propagación de virus informáticos

**Tabla A. 1** Consecuencias del spam

## 5. Contenido de los mensajes Spam

En la mayoría de correos no deseados se presenta la siguiente información:



**Gráfico A. 4** Contenido de mensajes Spam



## Ejemplos de mensajes con contenido spam

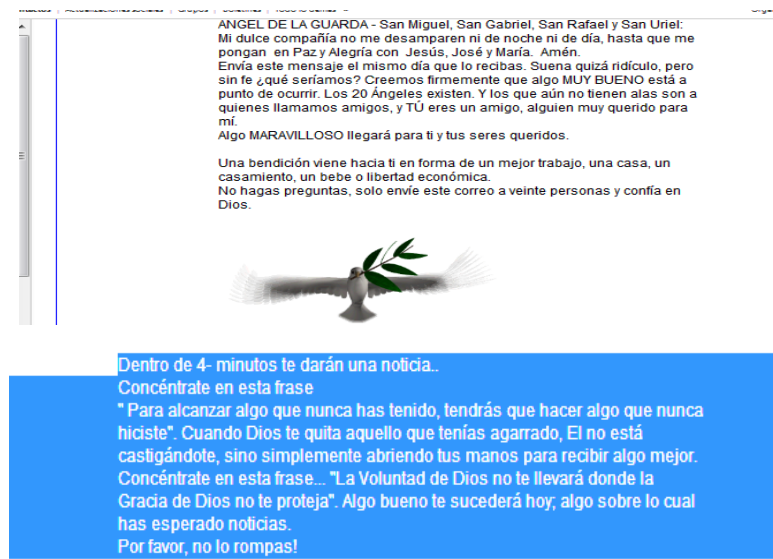


Gráfico A. 5 Cadena de mensaje para reenviar

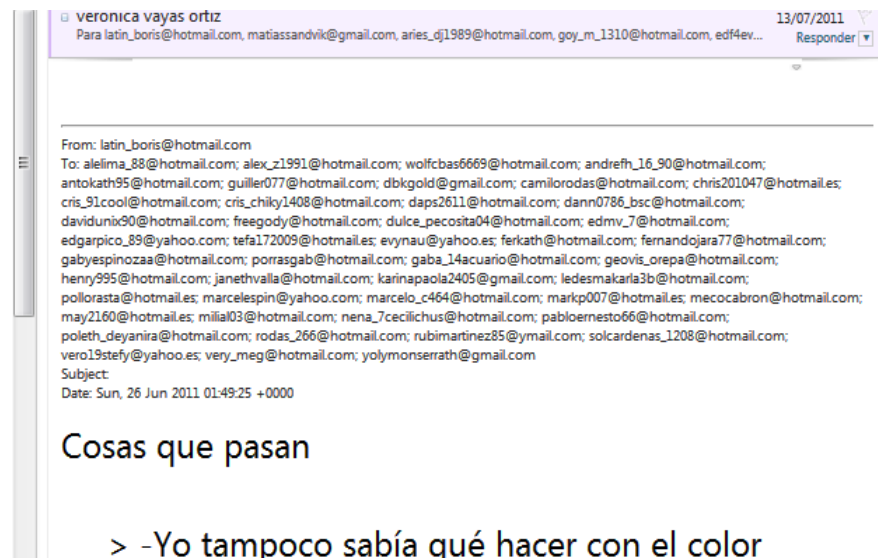


Gráfico A. 6 Envío de información de contactos

## 6. Medidas de seguridad para evitar recibir spam

Las medidas a tomar para reducir el número de mensaje spam que invade la bandeja de entrada de nuestras cuentas de correo electrónico son las siguientes:

Cuidado con los mails en cadena: suele ser una táctica de los spammers para lograr que cuando un usuario va reenviando el email "secuestrar"

todas las direcciones.
Usar la copia oculta: al enviar un email a muchas personas se debe usar la opción Copia Oculta (CCO) para evitar que nadie tenga acceso a las direcciones de email de nuestros contactos.
Su email en internet: no debe publicar su dirección en webs de libre acceso ya que usan robots para “coger” las direcciones que hay escritas en páginas webs.
Segunda cuenta de correo: puede crearse una cuenta de correo alternativa y gratuita para los sitios que pidan una cuenta de email para darse de alta, así su cuenta personal estará a salvo
No responder al spam: nunca se debe contestar a un mensaje de spam porque con ello les están confirmando que la cuenta es buena y operativa.

**Tabla A. 2** Medidas de prevención en la recepción de spam

Una vez que se ha puesto a disposición este manual de seguridad queda a consideración de los lectores adoptar las medidas de prevención para detectar y controlar el correo no deseado que invade de forma masiva la bandeja de entrada de sus cuentas de correo.

Para entender como ocurren los envíos de spam, sin que el usuario de correo sepa, se presenta una breve práctica paso a paso de la aplicación de técnicas spam para enviar correos electrónicos en forma masiva, en el anexo adjunto a este manual.

# Anexos del manual

## Aplicación de técnicas spam para envío masivo de información no deseada

Para analizar las técnicas spam, y poder probar el proceso de obtención de direcciones, creación de mensaje y envío del mismo ha sido necesario contar con un dominio y hosting adecuado, ya que por los filtros de spam que existen no se puede utilizar un hosting gratuito.

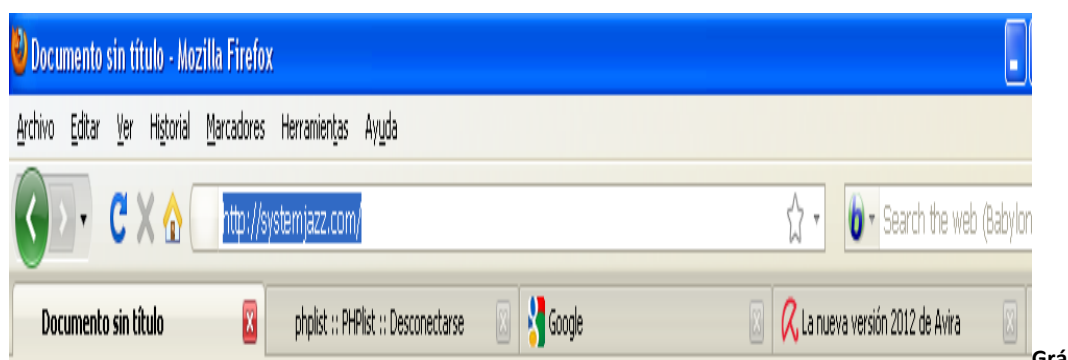


Gráfico A. 7 Acceso al dominio. Hosting

El hosting y dominio adquirido será el que sirva para el envío de mensajes a los destinatarios que se desee, para lograr este objetivo previamente se ha añadido la herramienta phplist a la pagina; en la siguiente figura se podrá observar el acceso a la configuración del hosting y dominio, llamado systemjaz.com

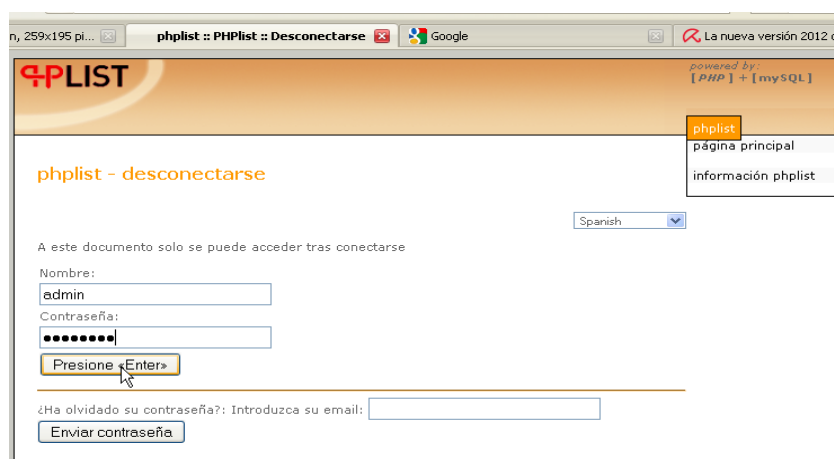


Gráfico A. 8 Conexión al servidor PHPList

Dentro de la configuración de phplist se tiene varias opciones útiles, entre ellas la posibilidad de crear listas de correo así se puede clasificar a cada usuario que se cree.

Se necesita configurar los servicios de ftp y de smtp, además de pop3, para ello se requiere usar las herramientas anteriormente mencionadas, y para ftp se uso la herramienta fileZilla client, se recomienda usar la versión más actual que exista.

Luego de su instalación se debe configurar la cuenta FTP Username: usuario@sudominio.net, FTP Server: ftp.mentesinquietas.net FTP Password: suclave FTP Server Port: 21. La ventana de configuración deberá ser similar a la siguiente:

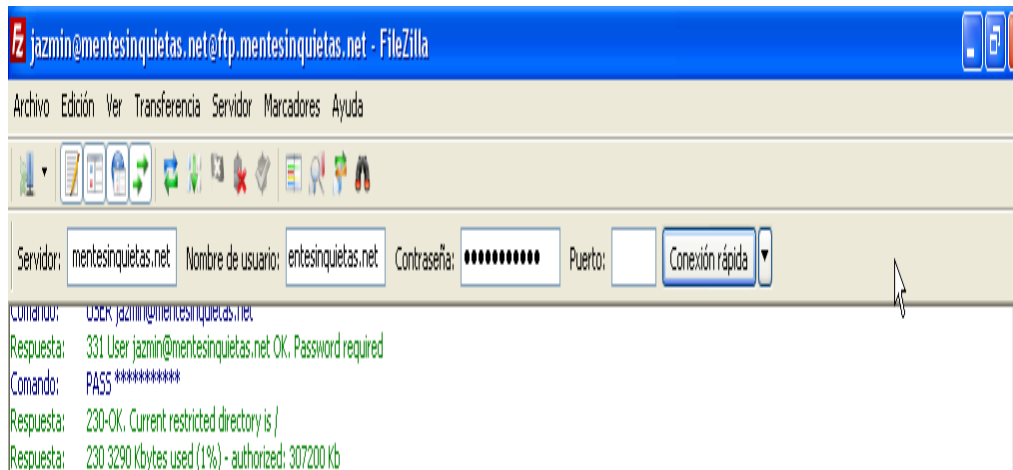


Gráfico A. 9 Levantamiento del cliente Filezilla

Una vez establecida la conexión se puede añadir todo tipo de archivo a las carpetas del hosting. Además se pueden crear directorios dentro del mismo.

Para añadir usuarios a una lista el proceso es crear la lista y añadir el usuario a la misma, así se evito la pérdida de tiempo al añadir uno a uno el destinatario.



Gráfico A. 10 Verificación de lista de usuarios en PHPList

La primera prueba de envío de mensaje se ha realizado con phplist, para poder añadir imágenes u otro tipo de animación o archivo es necesario que todo este subido en el hosting así que lo que se realiza es fácil; Al establecer conexión desde filezilla se tiene acceso a las carpetas y se elige la que desea para añadir el contenido que necesita así:

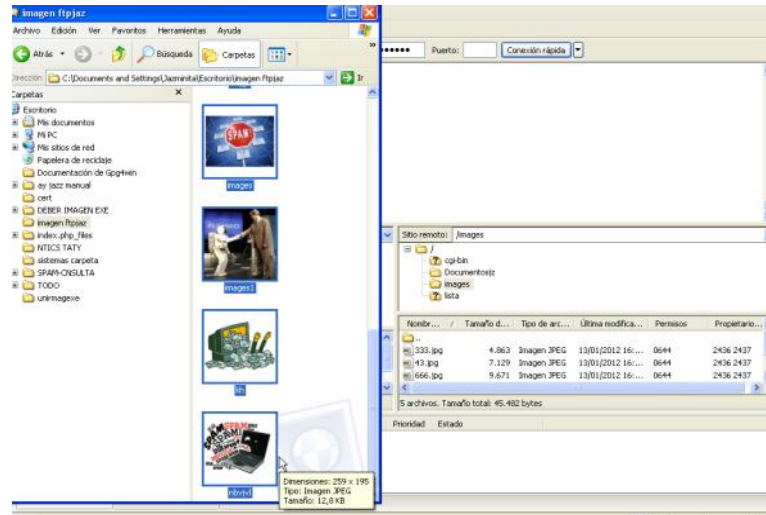


Gráfico A. 11 . Subir imágenes al Hosting

Ahora ya cuando se han seleccionado los elementos que se van a añadir se mostrara la carga de cada uno de ellos luego de unos momentos ya al finalizar dicha carga se podrá comprobar el éxito o fracaso de la misma desde el hosting accediendo al directorio en donde se lo almacenó a través de la barra de direcciones.

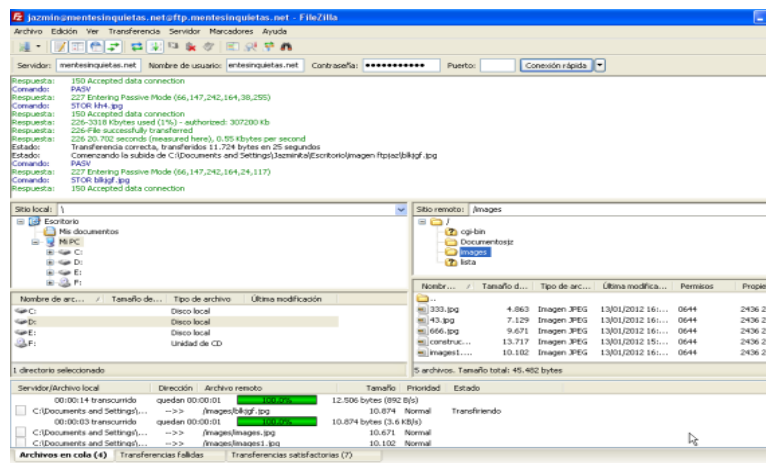


Gráfico A. 12 Verificación en el cliente con la información del hosting

Así podrá utilizarlos en el cuerpo del mensaje que va a enviar, al crear un mensaje se despliega algunas opciones entre ellas una imagen donde se añade una figura, en este caso el formato es el mismo claro que con la diferencia que

se debe especificar la dirección que tiene la imagen dentro del hosting. La imagen añadida puede contener código maliciosos oculto o código ejecutable.

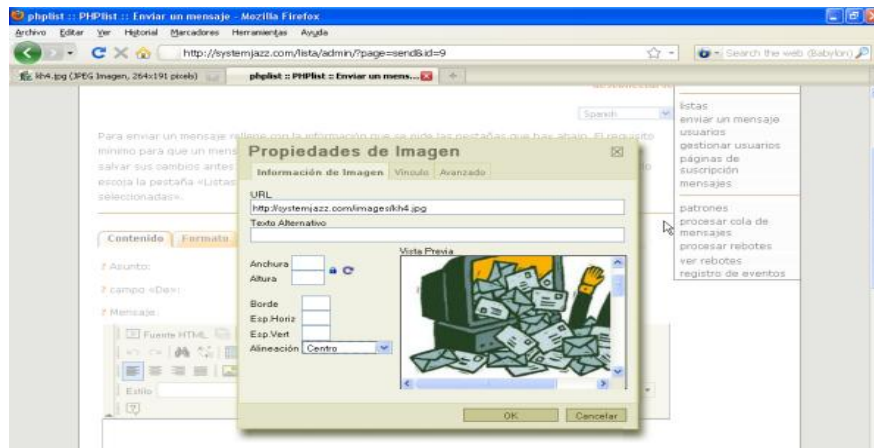


Gráfico A. 13. Propiedades de imagen a adjuntar al mensaje

En la ventana que aparece la opción para añadir una imagen se puede configurar sus propiedades como su alineación y tamaño, al finalizar la imagen será adjuntada en el cuerpo del mensaje.

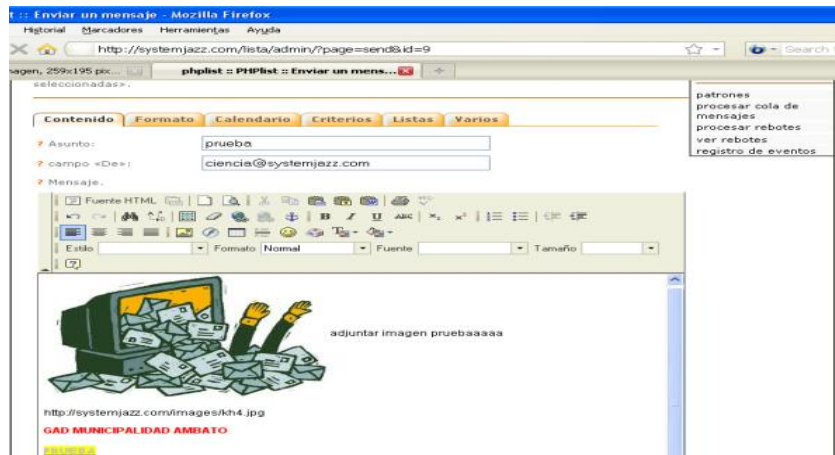


Gráfico A. 14 Adjunto de imagen en el mensaje

Ahora para guardar todos los cambios efectuados presionar el botón salvar cambios.

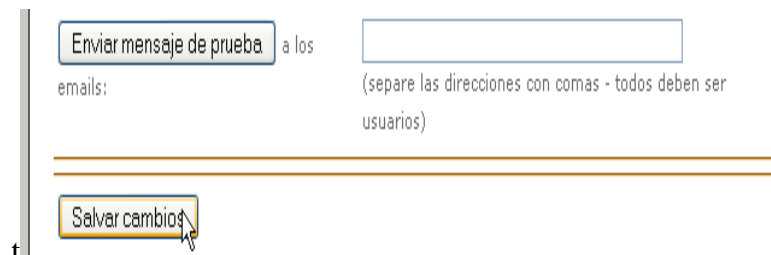


Gráfico A. 15 Guardar cambios en mensajes

Para especificar los destinatarios se tiene la opción de seleccionar la lista de contactos a los que quiere que llegue el mensaje. Guardar los cambios y enviar el mensaje; pero para que el o los mensajes sean enviados deberá procesar la cola de mensajes.



Gráfico A. 16 Procesamiento de sola de mensajes

Al dar clic en esta opción aparecerá una ventana donde se ve el proceso de envío de mensajes, y notifica cuantos mensajes han sido enviados satisfactoriamente.



Gráfico A. 17. Verificación de envío de mensajes en cola

Para verificar que el envío ha sido exitoso se ha creado una cuenta alternativa donde se han recibido los mensajes enviados a manera de prueba.



Gráfico A. 18 . Comprobación de recepción de mensaje

El spam usa métodos diversos que le permiten llegar a las bandejas de usuario de millones de personas en el mundo, en este caso a cada funcionario del GADMA.

Para las pruebas se usaron archivos ejecutables que no causen daños a los ordenadores que abran el mensaje.

Thunderbird es otra herramienta permite enviar fácilmente correos electrónicos, para usarlo debe configurar primero la cuenta y tipo de servidor de correos al se va a conectar, esto se refiere la configuración de la cuenta donde añade el nombre del emisor con el que desea enviar el mensaje, y especificar el servidor del protocolo smtp y servidor de correos pop3.

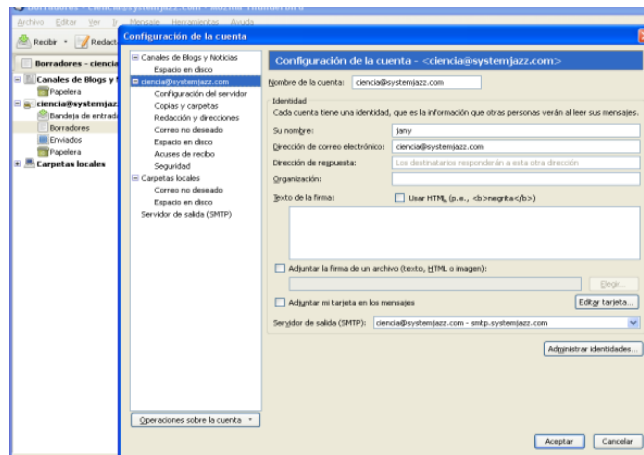
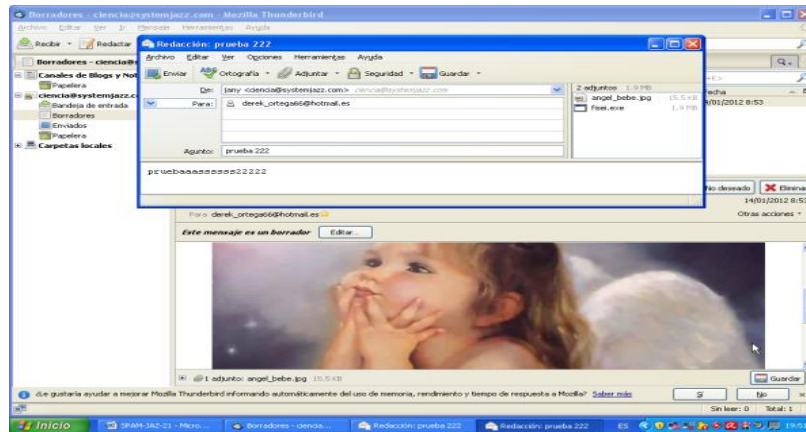


Gráfico A. 19 Configuración para prueba de envío MT

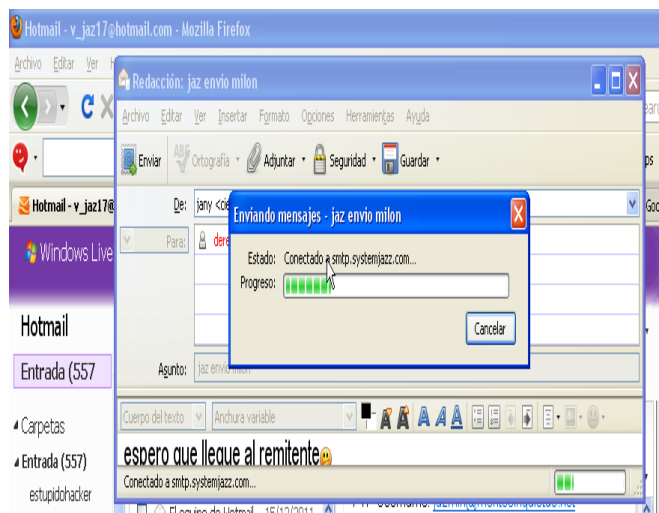
Una vez configurado el servidor de correos, la manera de enviar mensaje es sencilla y muy parecida a varios servicios de correo electrónico, para enviar un mensaje especifica el asunto, el destinatario y añade al cuerpo de mensaje el contenido deseado, además tiene la opción de añadir todo tipo de contenido.





**Gráfico A. 20 . Especificación de Destinatarios**

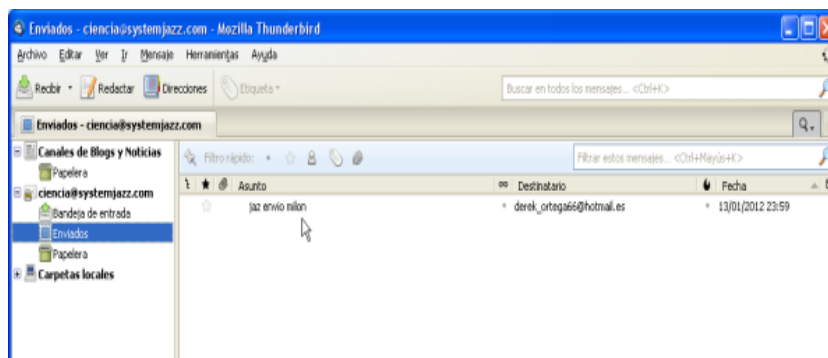
Al terminar de escribir el mensaje, lo enviará a los destinatarios elegidos.



**Gráfico A. 21 Ventana de carga de mensaje MT**

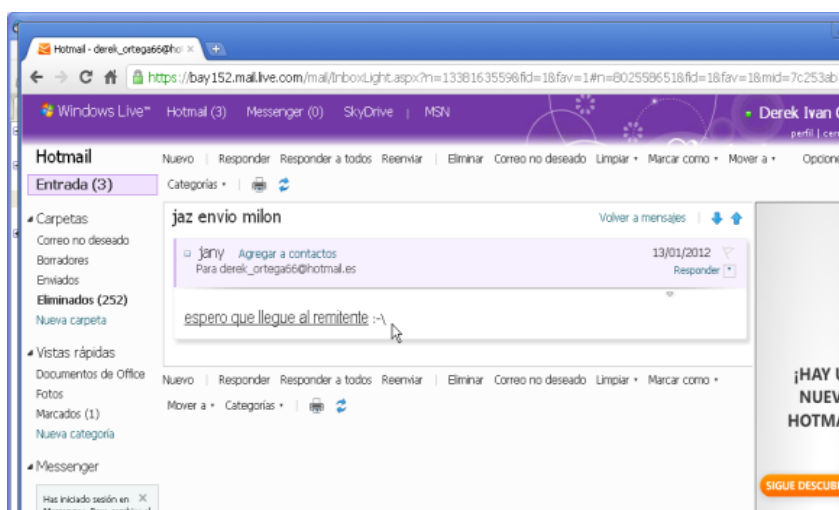
Como se estuvo trabajando con cuentas a prueba se puede verificar que el mensaje lleve a su destino:

Una de las maneras es comprobar que el mensaje este en la bandeja de salida de mozilla thunderbird:



**Gráfico A. 22 . Bandeja de salida MT**

Y la otra opción, además más segura es verificar por sí mismo el mensaje recibido en la cuenta que ya se menciona se tiene para verificar las recepciones.



**Gráfico A. 23 Bandeja de entrada cuenta alternativa**

Así se muestra que los famosos spammers ahorran mucho dinero utilizando pocos recursos, e incrementan sus ingresos con el éxito que da la publicidad o contenido recibido por sus víctimas.

Con la herramienta Claws-Mail el proceso es similar, se configura una cuenta especificando el servidor de correo y a continuación se podrá iniciar con la creación, recepción y envío de mensajes a correos electrónicos.

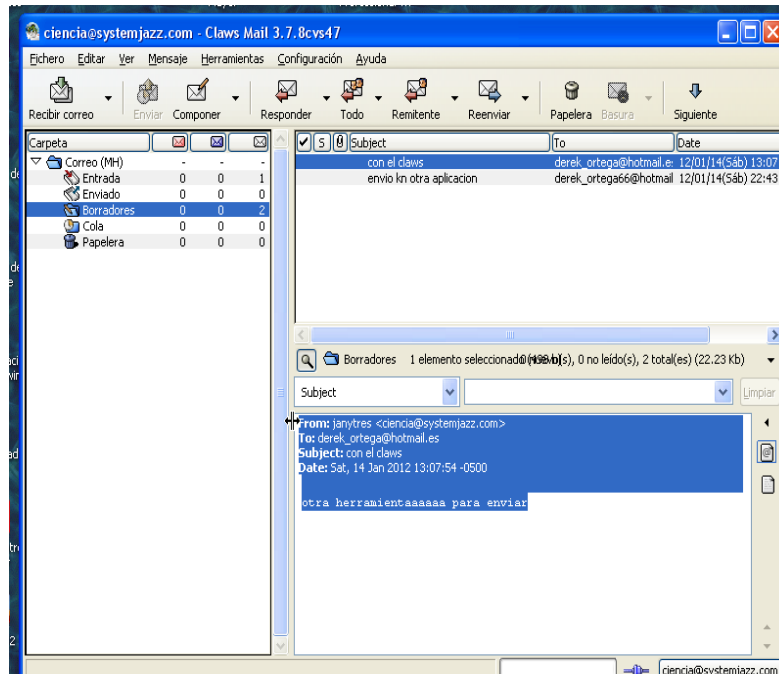


Gráfico A. 24 . Envío de mensaje con Claws Mail

Con Outlook se realizó también la prueba de envío de mensaje, en este se configuro una cuenta para el servidor de correos, pero al momento de enviar los mensajes estos no pudieron llegar ya que la dirección que emitía el mensaje fue detectada como miembro de una lista negra. Con ello se confirma que dependiendo del tipo de cuenta que se tenga existen varios filtros para detectar el spam.

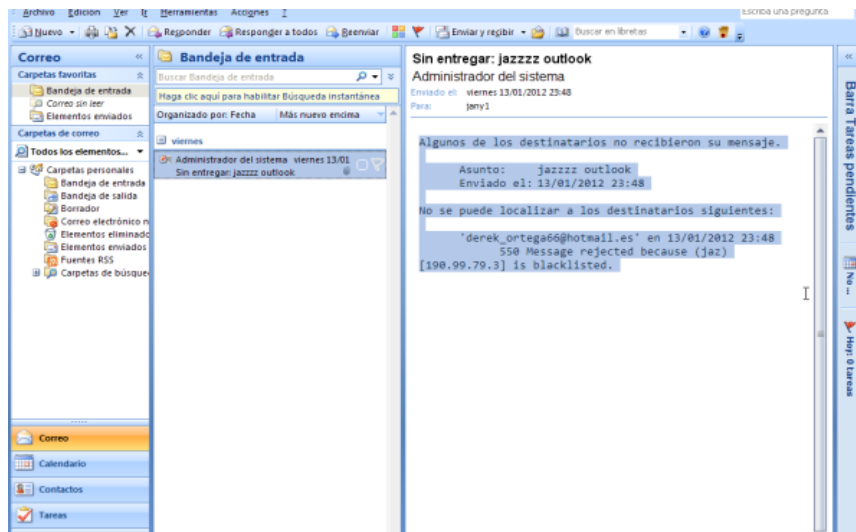


Gráfico A. 25 Detección de cuenta en black list

En la figura anterior se muestra el mensaje de error recibido para notificar que la dirección reposa en una blacklist.

Luego de la aplicación de la herramientas vistas se ha observado como se puede propagar el spam, además para las pruebas no solo se usaron cuentas de correo obtenidas de los funcionarios, sino aquellas que miles de personas olvidaron o dejaron en foros que se visito, además de las cadenas en donde envían también la información de sus contactos.