UNIVERSIDAD MAYOR DE SAN ANDRES

FACULTAD DE CIENCIAS PURAS Y NATURALES

CARRERA DE INFORMÀTICA

TESIS DE GRADO

TÉCNICAS ANTI SPAM EN EL CORREO ELECTRÓNICO EN BOLIVIA

PARA OPTAR AL TITULO DE LICENCIATURA EN INFORMÁTICA

MENCIÓN INGENIERÍA DE SISTEMAS

POSTULANTE: **Ludwing Gualberto Coca Jiménez**

TUTOR: **Lic. Roberto Vargas Blacutt**

REVISOR: **Lic. Hugo Javier Reyes Pacheco**

LA PAZ – BOLIVIA

2007

DEDICATORIA

A mi madre, por haberme inculcado principios éticos y morales enseñándome el valor de la vida, por darme la educación de la cual estoy orgulloso, por la comprensión que supo tenerme en los momentos mas difíciles y por todo el cariño que siempre me ha dado

AGRADECIMIENTO

La presente investigación carecería de valor si, a lo largo de su realización, yo mismo no hubiera sido capaz de aprender y mejorar el conocimiento construido en mis años de estudio. Son muchas las personas que me han apoyado a lo largo de mi formación académica, y es por ello que quiero, manifestarles mi agradecimiento:

En primer lugar, y de forma sincera, profunda y afectuosa, al Lic. Hugo Javier Reyes Pacheco por haber dirigido con paciencia mis vacilantes pasos y por su incondicional entrega a mi aprendizaje, profesional y personal. Igualmente, al Lic. Roberto Vargas Blacutt, mi tutor e impulsor de esta tesis, por su calidad de mentor, sus buenos consejos y su fe en mi trabajo. Espero que ambos me disculpen por cuantos errores haya cometido en el desarrollo de esta mi tarea y deseo que su colaboración, su apoyo y su amistad se mantengan, e incluso crezcan en el futuro.

A mis compañeros de Carrera, por la forma en que han avivado mis energías con sus palabras de aliento y con el interés transmitido hacia mi trabajo en todo momento, les quiero manifestar mi más sincera gratitud, especialmente, a mis amigos del área de Estadística y Derecho, cuyos consejos en el orden metodológico han sido una ayuda inestimable para llevar a buen término mi trabajo. A título personal, deseo recordar a todos mis docentes, cuyo trabajo ha sido para mí una auténtica brújula para recorrer mi camino. Finalmente, no puedo acabar sin recordar a todas aquellas personas de mi entorno más cercano, familiares y amigos, que me han dado todo su apoyo, su aliento, su paciencia y su cariño, aquellas personas que ocupan un lugar de honor en mi corazón, mis abuelos Patricio y María por supuesto, mis hermanas Brenda y Raquel, por quererme y comprenderme como soy y transmitirme su incondicional confianza durante la realización de este trabajo.... y siempre.

Ludwing_coca@hotmail.com

RESUMEN

El SPAM o Correo Electrónico no deseado, es un problema de las tecnologías de información y comunicación que afecta a Instituciones y personas naturales en lo económico y social, tomando como su principal medio de ataque al correo electrónico. Cuando se es victima de SPAM también se es susceptible a muchos tipos de daño desde virus hasta la perdida de datos personales muy valiosos o perdida económica; este tipo de ataques es generado por el Spammer quien es el que sustrae direcciones de correo electrónico y luego envía correos electrónicos generalmente publicitarios de forma masiva; el por qué del uso del correo electrónico como medio de difusión publicitaria y fraudulenta esta relacionado con los ínfimos costos que se tienen al usarlo, de un 100% de correos electrónicos que circulan a diario por internet aproximadamente un 70% es SPAM, es por eso que desde hace muchos años en países desarrollados se vienen implementando técnicas, estrategias y políticas anti SPAM ya que el impacto económico es muy grande; en la actualidad el SPAM a comenzado a distribuirse en países como Bolivia, y causa un daño económico imperceptible para el usuario de correo electrónico. En Bolivia no existe legislación que pueda coadyuvar a la solución de este problema es por esto que el presente trabajo plantea un estudio del impacto negativo que causa el SPAM en Bolivia en los usuarios finales y las instituciones públicas y privadas. Para afirmar lo expresado se entrevisto a profesionales en sistemas de diferentes instituciones estatales y privadas así como se realizo una encuesta a personas de diferentes edades y estratos sociales, utilizando para su análisis herramientas estadísticas. Por otro lado luego de haber realizado el estudio se identificaron las debilidades que tiene Bolivia como país en la lucha contra el SPAM haciendo un análisis detenido de la política legislativa existente en el Mundo se concluye que es necesaria una legislación expresa de lucha contra el SPAM, como también el uso de medios de difusión y educación para la concientización del usuario, el uso de filtros o

software lógicos y tratados internacionales; considerando que la solución seria incompleta se plantea un proyecto de ley anti SPAM para Bolivia.

ABSTRACT

The SPAM or e- mail does not wished; it is a problem of the technologies of information and communication that it affects Institutions and natural people in the economic thing and the social thing, taking as its main means of attack to the electronic mail. When you are a victim of SPAM also you are susceptible to many types of damage from virus until the lost personal data very valuable, or economic lost; this type of attacks is generated by the Spammer who is the one that subtracts electronic mail addresses and then sends generally advertising electronic mail in a massive way; the why of the use of the electronic mail like means of advertising and fraudulent diffusion this related with the minimal costs that one has when using it, of 100% of electronic mail that circulate approximately to everyday for internet 70% is SPAM, it is for that reason that for many years in developed countries one comes implementing techniques, strategies and political against SPAM for the impact economic very big; at the present time the SPAM had begun to be distributed in countries like Bolivia, and it causes an imperceptible economic damage for the electronic mail user. In Bolivia any law against SPAM doesn't exist, neither a law project exists in roads of its approval that can cooperate to the solution of this problem. It is for this reason that the present work establishes a study of the negative impact that the SPAM causes in Bolivia in the final users and the public and private institutions. To affirm the previously expressed one interview professionals of different goverment and private institutions that work in this environment as well as people was carried out a survey to people of different ages and social strata, using for its analysis statistical tools. On the other hand after having did the study the weaknesses were identified that has Bolivia like country in the fight against the SPAM making the existent legislative politics's detained analysis in the World you concludes that it is necessary an expressed legislation of fight against the SPAM, also the use of diffusion

means and education for the user's awareness, the use of filters or logical software and international treaties considering that the solution would be incomplete thinks about a project of law against SPAM for Bolivia.

INDICE REFERENCIAL

INDICE DE TABLAS

INDICE DE FIGURAS

1. MARCO REFERENCIAL

1.1 Introducción

En los últimos años el uso del Internet se ha vuelto muy popular en todos los estratos sociales, de la misma forma nos hemos ido familiarizando con las distintas utilidades de esta herramienta, una de las actividades mas preferidas de los usuarios de Internet es el uso del correo electrónico, mediante este medio el usuario tiene muchas ventajas para poder tener una mejor comunicación, ya que además de comunicarnos el correo electrónico nos provee de una interfaz muy rica para poder intercambiar una variada cantidad de información. Así como el correo electrónico nos ofrece grandes ventajas también trae consigo algunos problemas, en particular uno y el mas conocido el SPAM o correo electrónico no deseado, este tipo de mensajes son del orden publicitario y en muchos casos fraudulentos, estos correos electrónicos llegan a la bandeja de entrada sin que el dueño de la cuenta lo haya autorizado, el SPAM es un problema tan grande que afecta a todo el mundo, y por esto existen muchas organizaciones que vienen luchando contra esta problemática, a esta lucha se adscribieron países desarrollados y en vías de desarrollo.

El SPAM generalmente es enviado de forma masiva por el Spammer, causando daño económico a las empresas que nos proveen el servicio de correo electrónico y también al usuario final, el objetivo que se persigue con estos mensajes generalmente es el de publicitar algún producto o servicio, para esto se utilizan estrategias de mercadotecnia entre ellas mensajes y cabeceras de mensajes con contenido muy atractivo para el receptor. En otros casos estos mensajes son fraudulentos y solo forman parte de una cadena de daño y fraude, entre las actividades fraudulentas detectadas están el Phishing o robo de información privada y valiosa, daño a los dispositivos computacionales por lo tanto daño económico.

El presente trabajo realizo un estudio del SPAM en Bolivia, el daño que causa a sus ciudadanos con acceso a internet y correo electrónico como también el daño que causa a instituciones publicas y privadas, para esto nos basamos en el análisis de documentos, el uso de encuestas y entrevistas, pruebas de filtros anti SPAM, esto con la finalidad de tener una mejor visión sobre el SPAM en Bolivia, posteriormente se evaluaron las medidas de lucha contra esta problemática en diferentes ámbitos como son el legislativo nacional e internacional, lógico y educativo. En el caso de las Instituciones y usuarios bolivianos de correo electrónico, se utilizaron encuestas y entrevistas para poder evaluar distintos parámetros a nivel social e institucional, y así verificar la hipótesis planteada en este trabajo. En el ámbito internacional se realizo un análisis de documentos sobre la legislación anti SPAM de países de la región y el mundo además de las organizaciones existentes que luchan contra el SPAM, de igual manera se hizo un análisis en el ámbito nacional acerca de toda la documentación relacionada a la legislación anti SPAM que se tiene en el país.

Para finalizar luego de haber evaluado la hipótesis y valorado los resultados se presentan los lineamientos técnicos informáticos base para la lucha anti SPAM en Bolivia, y en base a ellos se realizo un proyecto de ley anti SPAM para Bolivia.

1.2 Antecedentes

El concepto de SPAM nace alrededor de los años 80, cuando el uso del Internet no era tan masivo aun, sino mas bien se hacia uso de otros medios de comunicación como son el Fax y el Teléfono, las compañías que querían hacer publicidad de sus productos adquirían maquinaria que podían hacer llamadas de manera automática o el envió de faxes a personas desconocidas, esto con el fin de poder hacer una mejor difusión de sus productos y a costos mas bajos, posteriormente cuando el uso del Internet se fue haciendo mas común, este tipo de tele mercadeo se fue alterando y se oriento mas al correo electrónico, se empezaron a ver casos de saturamiento de cuentas electrónicas "se debe tomar en cuenta que en esos tiempos no se tenían las capacidades de almacenamiento actuales".

Debo agregar además que los conocimientos técnicos que tiene la población sobre esta problemática son casi nulos, casi todas las personas que tienen una cuenta de correo electrónico fueron victimas de SPAM, de una u otra forma, e incluso es posible que aun no lo sepan.

Actualmente el SPAM se convirtió en un problema mundial ya que se vieron casos de fraude, lavado de dinero, robo de identidades, infección de computadores he incluso algo que nunca se imaginó, violación física a personas citadas por medio de correos electrónicos, los más afectados niños(as) que son victimas de este delito.

A nivel internacional muchas organizaciones ya comenzaron a desarrollar estrategias Anti Spam, una de las más importantes la Unión Internacional de Telecomunicaciones que agrupa a países de los 5 continentes incluido Bolivia además de organizaciones, agencias, programas de las Naciones Unidas que desde el año 2003 vienen impulsando y

difundiendo estrategias Anti Spam que se ponen en practica en diferentes regiones del Mundo.

Otras compañías internacionales como Microsoft, IBM, Apple, Google, etc. Vienen haciendo investigaciones acerca del desarrollo de herramientas capaces de evitar que el Spam llegue a nuestros correos electrónicos, no es de sorprender que altos ejecutivos de las compañías mencionadas sufran del problema del SPAM, como Bill Gates que por ser una figura muy conocida en el mundo de la tecnología, es blanco de muchos Spammers y el SPAM; en un anuncio de la compañía el presidente de Microsoft Steve Ballmer dijo que Bill Gates recibe alrededor de 4 millones de correos electrónicos al día y que la mayoría son SPAM.

En Bolivia existen denuncias en ODECO y la Super Intendencia de Bancos, relacionadas a la llegada de E-mails (SPAM). En una entidad Bancaria nacional como es el Banco Nacional de Bolivia, el contenido de los mismos refiere a que se deben actualizar los datos de las cuentas personales que uno tiene en el mencionado "Banco" llenando un formulario que se ubica abriendo una URL indicada en el correo electrónico, detrás de este tipo de SPAM, están organizaciones delictivas que lo que quieren obtener, es códigos y contraseñas de tarjetas de crédito de ciudadanos bolivianos con el fin de obtener dinero de las mismas.

SITTEL (Súper Intendencia de Telecomunicaciones de Bolivia) presento una propuesta de "LEGISLATION AND SPAM CONTROL IN BOLIVIA" que viene a ser la Legislación y control del Spam en Bolivia desarrollada por la Dr. Gabriela Urquidi Morales, en ese momento Directora legal de SITTEL, esta propuesta se la presento el 8 de julio de 2004 en Génova en un congreso de la UNION INTERNACIONAL DE TELECOMUNICACIONES, el contenido de la propuesta hace referencia a convenios

internacionales para combatir el SPAM, Phishing, además de un proyecto de ley para el control del SPAM en BOLIVIA

El Honorable Senado de Bolivia presento un PROYECTO DE LEY DE DOCUMENTOS, FIRMAS Y COMERCIO ELECTRÓNICO, que en el contenido no hace referencia al concepto de SPAM en si, sino solo a el concepto de correos electrónicos de tipo personal, institucional, y laboral

1.3 Planteamiento del problema

El SPAM se genera por dos actividades:

1. La existencia de personas mal intencionadas que hacen mal uso de la tecnología del correo electrónico para cometer delitos como robo, fraude, etc.
2. La necesidad de las empresas de reducir costos en la publicidad de sus productos o servicios

Debemos tomar en cuenta que en primera instancia estas entidades hacen contacto con el Spammer que es la persona encargada de conseguir las direcciones electrónicas, éste debe de comprobar la información además de ser capaz de conseguir información adicional de las mismas cuentas electrónicas como son: datos personales de cada dirección electrónica, preferencias del usuario, códigos y contraseñas de tarjetas de crédito, amistades del usuario, etc. Para esto hace uso de diferentes técnicas como: **Spammers bots, Envió de e-mails de forma aleatoria, Hoaxes o emails en cadena, Phishing.** Todos ellos clasifican las direcciones de correo electrónico obtenidas según la información adicional que ellos tengan sobre cada cuenta de correo electrónico, estas técnicas son muy útiles en sociedades como la nuestra, que por la ingenuidad, poca experiencia y conocimiento que se tiene sobre el problema del SPAM no se toman las

precauciones necesarias, esto por que aun no se han implementado políticas de información y de sanción contra problemáticas como el SPAM.

Conociendo entonces la forma en que nuestros datos pueden ser obtenidos por el Spammer, y las actividades que el puede realizar con los mismos, podemos identificar el problema que nos interesa atacar.

El correo basura cuesta dinero, tanto por el tiempo que se pierde examinándolo, como por los recursos de hardware y software necesarios para manejarlo (ancho de banda, servidores de correo más potentes, software de filtrado, etc.), y la implicación económica que debe ser soportada por la institución en forma de inversión y horas de trabajo de sus empleados, para evitar que los correos se saturen a causa de la recepción de correo no deseado para la labor empresarial. Es claro que esto no sólo presenta perjuicios a nivel empresarial sino también para aquellos que hacen uso de una computadora personal en sus hogares, es poco agradable encontrar una bandeja de entrada llena de correos basura, además enterarse que mucha información que uno espera no puede ingresar a nuestras cuentas de correo electrónico por la saturación que el SPAM causo en los mismos

Por lo tanto el problema es:

"LA PRESENCIA DE SPAM EN EL CORREO ELECTRÓNICO DE USUARIOS BOLIVIANOS DE INTERNET"

1.4 OBJETIVOS

1.4.1 OBJETIVO GENERAL

Analizar el impacto social y económico que tiene el SPAM en Bolivia y a partir del mismo obtener las diferentes técnicas y estrategias anti SPAM aplicables en Bolivia

1.4.2 OBJETIVOS ESPECIFICOS

- Realizar un estudio de las diferentes formas de SPAM presentes en el correo electrónico en Bolivia
- Investigar las diferentes técnicas de SPAM que se vienen utilizando en la actualidad, y especificar objetivos que se persiguen y a que tipo de sistemas atacan
- Identificar vulnerabilidades en los diferentes sistemas, que al proveernos de servicios de forma gratuita no nos proveen una seguridad contra SPAM
- Estudio de la legislación anti Spam en Bolivia
- Estudio de legislaciones Anti Spam de Países de la región
- Estudio de las diferentes herramientas desarrolladas para combatir SPAM y su forma de funcionamiento
- Estudio de filtros anti SPAM a nivel cliente y servidor
- Propuesta de un proyecto de ley Anti SPAM basado en los lineamientos técnico informáticos producto del presente estudio

1.5 HIPOTESIS

Un estudio técnico sobre la presencia de SPAM en el correo electrónico en Bolivia nos permitirá obtener los lineamientos técnicos informáticos base para la lucha anti SPAM en Bolivia

1.5.1 Operacionalización de variables

Identificación de variables : se identificaron 2 variables que son:

Variable Independiente (x): Estudio técnico sobre la presencia de SPAM en Bolivia
Variable Dependiente (y): Lineamientos técnico/informáticos base para la lucha contra el SPAM en Bolivia

Figura 1.5.1 Operacionalización de variables

1.6 Justificación

1.6.1 Justificación científica

El presente trabajo es oportuno por que apoya el desarrollo de nuevas investigaciones en relación a combatir el Spam en el correo electrónico en nuestro País, causando expectativas, análisis y discusión de mejores técnicas para combatir este problema ya que las que hasta ahora se tienen para combatir el problema del Spam en los correos electrónicos aun no son una solución global.

1.6.2 Justificación económica

El presente proyecto tiene una implicación a mejorar el uso de la tecnología, a permitir que el usuario final de correo electrónico en Bolivia pueda hacer el mejor uso del tiempo empleado en la revisión de su correspondencia electrónica, y ya que en cuestión de tecnología existe una relación en tiempo y dinero, se espera que el impacto económico sea de alto valor para, empresas, gobierno, y para cualquier otro usuario que haga uso de la tecnología del correo electrónico

1.6.3 Justificación social

Permitirá que los usuarios de correo electrónico en Bolivia tengan una mejor interacción con esta tecnología, facilitando el trabajo de depurar información no deseada, maliciosa, fraudulenta; Pudiendo confiar en el correo electrónico, ya que se tendrá una mejor calidad de servicio, seguridad y control.

1.7 Métodos y herramientas

El presente estudio tendrá dos fases, la fase explorativa y la fase explicativa.

1.7.1 Investigación Explorativa:

En una primera fase se hará una recopilación de datos de información relacionada con la actual presencia del SPAM en Bolivia, legislación, conocimiento que se tiene sobre esta problemática y daño que causo hasta la actualidad en Bolivia ya que es un tema de actualidad pero que no se tiene mucho conocimiento de el, para poder tener una mejor percepción acerca del impacto negativo que tiene el SPAM en el país se realizaron encuestas y entrevistas en la ciudad de La Paz y El Alto, además se hizo un análisis comparativo con otras sociedades de la región acerca de los logros que se tienen y se tuvieron en cuanto a la lucha contra esta problemática y las estrategias que se utilizaron

1.7.2 Investigación Explicativa:

Luego de tener y conocer información sobre el SPAM en Bolivia y en otros Países, se hará un análisis de todas las técnicas Anti SPAM conocidas, se evaluarán los filtros, antivirus, dispositivos físicos Anti Spam disponibles en Bolivia, además de todas las estrategias que se tienen en la actualidad para la lucha contra el SPAM como ser leyes de sociedades parecidas a la nuestra, tomando en cuenta costo/beneficio, disponibilidad, usabilidad. Esto con la finalidad de obtener información relevante para el estudio técnico sobre el SPAM en Bolivia

1.8 Limites y alcances

El presente estudio busca hacer una exploración acerca de la preparación que tiene Bolivia para la lucha contra una problemática mundial como es el SPAM, se evaluaran tecnologías, y estrategias que se tienen en el mundo que estén al alcance y se necesiten en Bolivia, el estudio técnico acerca del SPAM en Bolivia tomara en cuenta todos los resultados obtenidos en la investigación, esto con el objetivo del desarrollo de Lineamientos Técnico/Informáticos que posibiliten un Marco de Ley Anti SPAM en Bolivia; en el estudio no se tomará en cuenta la parte legal del desarrollo de Marco de Ley Anti SPAM en Bolivia ni la Ejecución de la Ley en si, lo que se hará será un estudio de los lineamientos técnicos obtenidos a base del estudio técnico/informático del SPAM en Bolivia y se lo comparara con los lineamientos técnicos Anti Spam que se utilizaron en el desarrollo de leyes en otros países

La finalidad de la investigación es que los resultados del estudio se tomen como una base de marco de ley Anti SPAM en Bolivia que en la actualidad es muy necesaria, al final se espera tener conclusiones en materia legal y materia social, es el deseo de esta investigación que personas de escasos recursos pero con acceso a Internet dejen de pagar

cuentas elevadas por llamadas a otros lugares del mundo que nunca realizaron porque han sido victimas de este correo basura, problemas tan presentes en sociedades como la Boliviana como es el lavado de dinero, fraude y delito informático dejen de ocurrir.

2. MARCO TEORICO

Resumen

En este capitulo se da a conocer toda la teoría relacionada con el estudio de SPAM, el correo electrónico, la seguridad, las técnicas SPAM y el derecho informático, cada uno de estos puntos es desarrollado para poder dar mas claridad a los lineamientos técnicos informáticos

2.1 Derecho informático

2.1.1 El uso legítimo del correo electrónico

El e mail, correo electrónico o servicio de mensajería interpersonal, se ha convertido en una herramienta de comunicación eficaz dentro de las instituciones públicas y privadas y para el uso personal de los usuarios independientes. El correo electrónico ofrece una inmediatez en el envío de mensajes, sin necesidad de que el emisor y el receptor estén conectados simultáneamente. Las redes telemáticas permiten que mucha información que era previamente inaccesible y sin valor debido a que estaba en un lugar remoto, se convierta en útil y valiosa a través de la Red. Así el acceso a bases de datos remotas y la transmisión de datos, sonidos y imágenes en tiempo real a cualquier parte del planeta son ya hechos consumados. Del mismo modo personas con las cuales se podía mantener una relación a distancia pueden ser ahora compañeros de trabajo que interactúan de un modo eficaz."

Efectivamente, el correo electrónico ha permitido la desaparición de las fronteras para el desarrollo de relaciones humanas y ha impulsado el comercio internacional facilitando el acceso a productos e información puestos a disposición de quien lo desee. Incluso la Administración Pública basa sus proyectos más novedosos de E-government en esta herramienta de comunicación. Estos cambios que ha introducido la tecnología han reformado al mundo jurídico que ha entrado en una nueva etapa de desafíos, sobre todo cuando están en juego los derechos fundamentales de los usuarios. El ordenamiento jurídico debe hacer frente a esos cambios introducidos en la sociedad de la información para proteger los intereses y derechos de los ciudadanos que vean sus derechos constitucionales afectados. Hasta la fecha, el derecho se ha escrito para la regulación del mundo pre digital o analógico y ahora debe adecuarse a las nuevas tecnologías y su impacto en los derechos fundamentales con la llegada de la era de la digitalización.

El derecho a la intimidad como pilar fundamental de la protección a la individualidad de la persona se ha visto vulnerado por el uso indiscriminado de datos que sobrepasa las fronteras y la soberanía de cada región, con una rapidez y facilidad sorprendentes. Igualmente, este derecho es hoy objeto de estudio ante el uso del correo electrónico en él, tanto la interceptación de mensajes por ese medio puede significar una intromisión en la vida privada del usuario.

El Internet introdujo una modalidad de tratamiento invisible de los datos que se ha acentuado a través del comercio electrónico. Todos los días miles de ciudadanos proporcionan sus datos personales (identificación personal y hasta datos de tarjeta de crédito) de forma expresa o tácita a empresas públicas y privadas a través de Internet, generalmente utilizando su dirección de correo electrónico. Eso provoca que pese a la seguridad imperante las empresas realicen ciertos tratamientos de datos que no son perceptibles al usuario, ya sea porque se presentan en principio como intrascendentes o bien porque se obtienen sin el consentimiento del usuario o a expensas de omisiones ilegítimas de información que afectan su autodeterminación informativa.

En este estudio se analiza la vulnerabilidad los de derechos de la persona ante el uso del correo electrónico y aspectos entre los que se incluyen la intimidad en las comunicaciones privadas y la naturaleza pública o privada de este medio de comunicación, con el fin de proponer un acercamiento hacia un derecho que regule estas nuevas fronteras de la información en beneficio de la protección de los derechos fundamentales de los usuarios de Internet.

2.1.2 Naturaleza jurídica del correo electrónico

Como se dijo antes, el correo electrónico es un nuevo medio de comunicación que permite la transmisión de datos, el flujo o distribución de material de todo tipo, incluso protegido por el derecho de autor, transacciones económicas y correspondencia en general. Este servicio de Internet lo define Corripio diciendo que: "El correo electrónico constituye un servicio de mensajería electrónica que tiene por objeto la comunicación no interactiva de texto, datos, imágenes o mensajes de voz entre un «originador» y los destinatarios designados y que se desarrolla en sistemas que utilizan equipos informáticos y enlaces de telecomunicaciones."

2.1.3 Formas del correo electrónico según la visión jurídica

2.1.3.1 Como correspondencia o comunicación

El correo electrónico posee una idéntica naturaleza a la del correo tradicional, con la diferencia de que las comunicaciones (equivalentes del correo ordinario) se transmiten a través de la Red mediante tecnología digital.

Por ello en principio y como norma básica, el correo electrónico también es inviolable y no puede ser interceptado, abierto, manipulado, retenido o violentado de cualquier forma sin autorización judicial o con el consentimiento expreso del usuario de la cuenta. Si coincidimos en que la naturaleza del email es una comunicación, también debe de ser protegida como se protege al correo postal.

La información que consta en torno al correo electrónico pertenece a la vida privada tanto si nos referimos al contenido de los mensajes como a la dirección IP que queda evidenciada en una transmisión y a la misma dirección electrónica (elemento identificatorio como el ID del correo electrónico así como el elemento que determina el servidor que proporciona el servicio) todo lo cual va a constar como datos personales del usuario, según lo veremos más adelante. ***Por tanto, tanto los datos recibidos como los***

datos enviados desde la cuenta de correo, constituyen elementos protegidos bajo el principio de inviolabilidad de las comunicaciones.

2.1.3.2 Como conjunto de datos

El correo electrónico es un conjunto de datos personales del usuario y como tal su manipulación se encuentra supeditada a las normas relativas a la protección de datos personales.

Con los datos obtenidos a través de una cuenta de correo se puede constituir el perfil de un usuario, quedando vulnerada con ello su intimidad, su vida privada. Por ejemplo, a simple vista una dirección puede evidenciar el nombre y apellidos del usuario, el lugar geográfico de origen, su lugar de trabajo e incluso aspectos más delicados como su inclinación política, religiosa o sexual, dependiendo del servidor que proporcione la dirección de correo. En el caso que el usuario haya proporcionado más datos de su vida privada en el momento de adquirir la cuenta, también desde su perfil se pueden determinar números de teléfono, dirección domiciliaria, gustos o incluso su profesión.

Dentro del conjunto de datos también la transmisión de mensajes electrónicos hace posible que pueda averiguarse la dirección IP del usuario (protocolo de Internet) que es en sí misma un dato personal, pues si se llega a descifrar la misma, se puede identificar la terminal del usuario (y en ocasiones con cierta destreza acceder a sus archivos). Todo esto pone en evidencia que el correo electrónico condensa una serie de datos del individuo, cuya manipulación (muchas veces invisible para el usuario) podría poner en vulnerabilidad su derecho a la autodeterminación informativa.

2.1.3.3 Como transmisor de material protegido por el derecho de autor

Finalmente, la naturaleza del correo electrónico puede ser analizada desde la perspectiva del derecho de autor, en tanto sea un medio de comunicación por el que se transmitan obras literarias, científicas o artísticas.

Al permitir el intercambio de documentos en formato de texto, imagen o sonido, e incluso archivos multimedia, el correo electrónico se ha constituido en una herramienta de difusión de material protegido por el derecho de autor. De allí que pudiera ser un medio que ponga en flaqueza los derechos de propiedad intelectual en la medida que el uso y distribución de material protegido a través de esta mensajería sea indiscriminado, ilegítimo y lesione el normal comercio de las obras.

El email efectivamente transporta material que ha sido digitalizado y por ende es de fácil transmisión, e imperceptible salvo para el emisor y los destinatarios, lo cual es uno de los problemas derivados de las nuevas tecnologías. El contenido mismo del mensaje de correo (aún si no se transmite una obra literaria, artística o científica) sería susceptible de protección en calidad de derechos de autor del titular de la cuenta, por que ademas el email posee una naturaleza similar a la del correo ordinario o cartas, la obra estaría protegida por ser precisamente una carta personal pero en formato digital. Para ello, deberá ser siempre original, que no implique solamente un mensaje informativo y que contenga las características de identificación de la personalidad.

2.1.4 Tratamiento del correo electrónico según su tipología

La tipología define características distintas para cada tipo de cuenta de correo, por lo cual, deben regir normas jurídicas distintas pero flexibles, justas y proporcionadas.

2.1.4.1 Correo electrónico personal

En principio el correo electrónico es un medio de comunicación privado protegido como una correspondencia inviolable. El correo electrónico típico, es aquel que el usuario posee de forma gratuita como un servicio proporcionado por algún host de la Red o un proveedor de servicios, e incluso existen direcciones de correo que se ofrecen previo pago de una cuota, lo cual es menos común, en virtud de la facilidad de acceder gratuitamente a una cuenta personal.

En estos casos, los usuarios del servicio quedan subordinados a las normas de seguridad y de uso de la cuenta que aceptan en el momento de realizar la suscripción al servidor que les proporciona el servicio. Este correo es de uso estrictamente personal y por ende no puede ser manipulado, interceptado, intervenido o alterado de alguna forma si no se posee una autorización judicial, pues corresponde legítimamente a una naturaleza idéntica a la del correo tradicional y por ende se encuentra protegido por el secreto de las comunicaciones y por el derecho a la intimidad.

El nuevo derecho de acceso a Internet, que es el derecho que tiene todo individuo a recibir los servicios disponibles en Internet como servicios universales, obliga a hacer accesible los servicios de Internet (y por ende de correo electrónico) a todos los ciudadanos del mundo sin distinción de situación política, social, económica, sexual, laboral o geográfica.

En este sentido, no se puede imponer al usuario obstáculos o limitaciones para poseer una cuenta de correo electrónico que le permita utilizar este servicio de mensajería de forma gratuita sin poner en peligro su derecho a la intimidad y a la privacidad de las comunicaciones.

La propiedad de los mensajes que se transmiten por este medio es del titular de la cuenta de correo (del usuario que recibe el servicio) y no del servidor que ofrece el servicio

(pues es un simple administrador técnico, una vez que proporciona la facilidad de acceso) y que por consiguiente se encuentra obligado a adoptar las medidas necesarias para proteger al usuario tanto en la manipulación de sus datos, como en lo que respecta a medidas para evitar que su correspondencia sea violentada por un tercero no autorizado. El usuario por su parte, queda obligado a adoptar sus propias precauciones como el resguardo de la clave, password o Pin que se le concede para el acceso exclusivo a su cuenta y a utilizar el servicio según las condiciones que acepte en el contrato de suscripción. La intimidad personal debe de estar siempre protegida.

Por tanto la persona que intente descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de papeles, cartas, mensajes de correo electrónico o cualesquiera otro documento o efectos personales o intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen o de cualquier otra señal de comunicación, debe ser castigado de forma penal. Si los hechos anteriormente mencionados son realizados por el encargado o responsable de fichero, soporte informático, electrónico o telemático; entonces estas actuaciones del administrador del correo deben estar estrictamente amparadas a medidas de resguardo de los datos del usuario, y todo acuerdo en contrario evidentemente sería inconstitucional y leonino. Por tanto, la protección evidencia la voluntad del legislador de proteger la intimidad de las comunicaciones por email privado contra el descubrimiento y revelación de secretos. El correo, así entendido, debe verse tanto como una correspondencia inviolable como también un domicilio personal (digital) pues por sus características es posible mediante las medidas técnicas pertinentes que cualquier sujeto mal intencionado pueda conocer la dirección IP del usuario o los datos para su ubicación geográfica.

2.1.4.2 Correo electrónico laboral

La naturaleza del correo electrónico laboral propone una nueva interpretación en la medida que se considera que su titular (trabajador o funcionario publico) no es el dueño de la cuenta; sino que lo es el Propietario, que proporciona la misma para fines exclusivamente laborales y por ende las normas deben tender en este caso, a proteger los intereses de una persona jurídica como nuevo titular de la cuenta de correo, que la asigna a un funcionario o trabajador para su uso y administración en nombre del cargo que desempeña y para fines estrictamente laborales.

En consideración que el propietario de las cuentas laborales de correo electrónico es una persona jurídica, este tiene todo el derecho legal de interceptar cualquier mensaje que por este medio se emita, ya que es parte del cuidado de su patrimonio, la única excepción permitida para que este correo pueda ser intervenido seria una orden judicial, pues no podríamos imponer limitaciones donde la ley no las indica expresamente es el caso de las instituciones privadas.

Muchos autores priman la protección del derecho del trabajador a la intimidad dentro del correo electrónico sobre el derecho de los empresarios. Sin embargo debe evaluarse en este caso que hoy en día todo ciudadano tiene amplias posibilidades de poseer una cuenta personal y gratuita de correo electrónico en uno de los múltiples sitios de la Red que proporcionan tal servicio, tales como Yahoo, Hotmail, Terra, Gmail, etc. Si el trabajador puede acceder por su cuenta a ese servicio, no existe razón alguna por la cual deba utilizar las cuentas de correo asignadas en su trabajo para fines personales, pues están en juego intereses de la empresa tales como el tiempo invertido por el trabajador para atender asuntos personales, el uso del equipo de la empresa, la imagen de la empresa, la vulnerabilidad de la seguridad de las comunicaciones de la empresa, eventuales daños al patrimonial empresarial o institucional, etc. Por tanto, quienes defienden este argumento consideran que si el ciudadano tiene acceso gratuito a cuentas de correo en Internet, la cuenta de correo que proporciona la empresa no tiene porqué

ser utilizada para fines personales o privados. Incluso se autoriza dentro de esta perspectiva, el control patronal sobre el contenido del correo, pues se interpreta que la cuenta no pertenece al usuario sino al patrono.

El almacenamiento informático es cada vez más una realidad, tanto en el sector público como en el sector privado. Igualmente, el envío de documentos laborales por medio del correo electrónico ha contribuido a que las funciones profesionales y administrativas ordinarias se agilicen y ha logrado conservar un contacto más expedito entre los trabajadores y entre éstos y los usuarios de sus servicios independientemente de la naturaleza de empresa de la que se trata.

El correo electrónico laboral lo constituye aquella cuenta proporcionada por el patrono privado o bien por la Administración Pública a sus trabajadores o servidores públicos (según corresponda), generándose así dos sub categorías de correo que son:

2.1.4.3 El correo proporcionado por propietario privado

En la empresa privada existe un porcentaje importante de trabajadores que laboran con cuentas de correo electrónico proporcionadas por sus patronos o empresas para el ejercicio de sus funciones.

En este sentido, el trabajador posee una cuenta que si bien, puede contener su nombre para identificación de usuario y la identificación de su persona con los actos que gestiona a través de su cuenta, también contiene un elemento que distingue a la empresa y por medio del cual quedan fusionadas todas sus actuaciones con esa empresa que le otorga la cuenta. Por ello, cada actuación que realice el usuario, indefectiblemente será una actuación que un tercero que reciba un mensaje por esa vía, identificará con la empresa que aparece en la dirección digital.

Si el trabajador utiliza el correo para asuntos personales, como por ejemplo para enviar chistes, mensajes religiosos, noticias, enlaces de Internet o cualquier otra actuación ajena a su trabajo, está utilizando para asuntos personales una mensajería laboral que no le pertenece y sobre todo está sobre utilizando los bienes de la entidad para la que labora y ejerciendo acciones sobre las que no ha sido autorizado por el servidor que le facilita la herramienta de comunicación.

Precisamente por ello resulta imprescindible que de previo a conceder una cuenta de correo electrónico, la empresa advierta al trabajador las condiciones de uso de ese servicio, y que proporcione las medidas pertinentes para que las restricciones del uso del email laboral estén siempre al alcance de los trabajadores, ya sea a través del portal de acceso o exhibido en sitios públicos en el lugar de trabajo. En todo caso siempre será necesaria una comunicación personal al trabajador en el momento de asignarle la clave de ingreso al buzón asignado. Este es sin duda un corolario del derecho a estar informado de los extremos del contrato laboral que afectan al trabajador, información que además debe contener la advertencia de las posibles consecuencias en caso de incumplimiento de las condiciones del servicio.

Igualmente, si el trabajador utiliza el email laboral para fines personales durante el ejercicio de sus funciones (en horas laborales) o bien con los medios empresariales (conexión empresarial a la red, ordenador de la empresa, electricidad a cargo de la empresa, etc.) la situación es aún más compleja pues deja en evidencia que no está destinando su tiempo al trabajo según lo exige su contrato laboral, que está abusando de los bienes patrimoniales de la empresa utilizándolos para uso privado no autorizado.

En este sentido, el propietario puede vigilar el uso que se le dé al correo electrónico sin previo aviso y sin intervención judicial, pues se trata de sus cuentas de correo, de sus

activos empresariales, de sus documentos laborales; siempre bajo el respeto de la autoridad jerárquica que rige en cada institución, y bajo el entendido de que el trabajador fue debidamente advertido que no estaba autorizado a ejercer ningún uso personal o privado de la cuenta de correo asignada. Sobre este punto, es importante resaltar que en el caso de asignación de una cuenta de correo laboral (privado o de la Administración Pública) se debe informar al trabajador de las limitaciones sobre el uso de tal herramienta

2.1.4.4 El correo proporcionado por la administración pública

En el caso de la Administración Pública, también se conceden cuentas de correo a los funcionarios o servidores públicos, con la particularidad que las cuentas identifican al usuario con el Gobierno Central o Institución descentralizado de un Estado. Son cuentas asignadas a los funcionarios públicos, para que ejerzan sus funciones ordinarias y para permitir la comunicación entre los servidores públicos, las instituciones estatales y los ciudadanos.

Aquí no solo existe en la dirección un elemento identificatorio de la institución pública sino que existe además una imagen pública de Estado que debe resguardarse tras las actuaciones que se realicen por medio de esa cuenta de correo, lo que hace más sensible el envío de datos (de interés público en su mayoría y exceptuando aquellos relativos al expediente personal del usuario) y la manipulación de este servicio.

Además, los documentos que emiten no son simple mensajería, sino que en la medida que cumplan los requisitos de un documento público, el contenido de los mensajes adquiere una importancia aún mayor, y por ende la publicidad de los mismos también. Si el archivo fue emitido por un empleado público competente, en el ejercicio de sus funciones, contiene los requisitos de un documento público y fue emitido con los medios

que facilita la Administración, el archivo es por tanto un documento público aún si es electrónico o digital

Hay aquí dos asuntos que interesan: el acceso de la Administración para el ejercicio del control de la acción administrativa a través del correo electrónico, y la publicidad que deben tener los documentos que emita la Administración de cara al administrado, aunque dichos documentos consten en los archivos de una cuenta de correo.

El derecho de acceso está relacionado al derecho que ostentan los ciudadanos de participar en su gobierno, controlando, criticando y velando por el buen funcionamiento de sus instituciones. Por tanto, no existiría motivo alguno que limite ese derecho de acceso a los documentos públicos que constan archivados o que se envíen por correo electrónico, sobre todo si éste es en sí mismo una base de datos, como vimos en su naturaleza jurídica.

Sin embargo, si bien ese acceso es libre, debe ser controlado. Al efecto, deben establecerse responsabilidades de administración y manipulación del correo administrativo pues el acceso solo debe ser autorizado con ciertas medidas de seguridad básicamente para evitar la alteración del contenido de los documentos o intromisiones en los sistemas informáticos del Estado o sus archivos. Por ende, a tales instrumentos solo accedería personal legítimo que los administren en virtud de una investidura de servidores públicos.

El principio de transparencia exige efectivamente que la Administración ponga a disposición de los ciudadanos todos los documentos que emite, incluso si son digitales y salvo que afecte la seguridad y defensa del Estado; pues el derecho de la información administrativa, el derecho de acceso a los archivos y los registros no declarados Secreto de Estado no pueden ser limitados en las nuevas comunicaciones generadas por Internet.

Por lo tanto, las comunicaciones electrónicas de la Administración son públicas y no privadas, por lo que no rige en esta tipología el principio de intimidad de las comunicaciones al no haber sujeto pasivo sobre el cual resguardar tal intimidad, pues el Estado es un ente público.

No obstante lo anterior, existe un principio que se ha evadido en la nueva sociedad de la información. Se trata del principio de la seguridad digital, en virtud del cual es legítimo establecer restricciones de acceso a esos documentos (en principio públicos) para evitar un daño posterior a los bienes e intereses del Estado. *Por ello, podríamos decir que el acceso a estos documentos puede ser indirecto a la luz de este principio, pero jamás ese acceso puede prohibirse, ni siquiera a la luz de la intimidad de un servidor público, quien está obligado a no tramitar asuntos personales a través de su cuenta de correo laboral/administrativo.*

2.1.4.5 Privilegios de acceso técnico

En cuanto al acceso a las cuentas de correo electrónico, existen ciertos sujetos que por su condición profesional o técnica tienen acceso privilegiado al contenido de los email's de los usuarios, y son los que administran el servicio en cada host o servidor de correo. En el caso de los correos electrónicos proporcionados en el ámbito laboral o de la Administración Pública, en principio dichos accesos no tendrían mayores controversias si se delimitan responsabilidades por abusos e indemnizaciones cuando se afecte a la institución, a la empresa o a terceros. Sin embargo, el privilegio de acceso debe estar centralizado y debidamente autorizado para evitar alteraciones de documentos o daños en los bienes informáticos de la Administración.

Por otro lado, en el caso de los Host privados, el que un sujeto desconocido y ajeno a nuestro entorno e incluso desarrollando su actividad en otra jurisdicción o geografía, pueda tener acceso tanto a los datos personales (y manipularlos de forma no autorizada) e incluso acceder al contenido de los correos, resulta evidentemente ilegal, no solo por la dificultad del usuario de acceder al administrador sino porque en este caso sí se trata de asuntos relativos a la inviolabilidad de la correspondencia privada.

Pero en tanto no se creen mecanismos técnicos que puedan impedir totalmente esta situación, los servidores deben contar con medidas de control de su personal y adoptar un código de conducta que los distinga como "sitios seguros en la Red"; mientras que el usuario debe acudir a los proveedores de servicios que ofrezcan las mayores garantías de seguridad y resguardo de los derechos fundamentales de los usuarios.

En resumen podemos decir que el email privado es de uso estrictamente personal y por ende no puede ser manipulado, interceptado, intervenido o alterado de alguna forma si no se posee una autorización judicial, pues corresponde legítimamente a una naturaleza idéntica a la del correo tradicional y por ende se encuentra protegido por el secreto de las comunicaciones y por el derecho a la intimidad. *El correo, así entendido, debe verse tanto como una correspondencia inviolable como también un domicilio personal (digital) pues por sus características es posible mediante las medidas técnicas pertinentes que cualquier sujeto mal intencionado pueda conocer la dirección IP del usuario o los datos para su ubicación geográfica*

.

El correo proporcionado por el patrono o por la administración pública, pertenece a ésta y lo delega como una herramienta de trabajo a sus servidores pero no como una dirección privada.

Permitir que el trabajador utilice el email empresarial para asuntos personales podría incidir en un daño directo a la imagen de la empresa o bien provocar una afectación patrimonial pues aumenta el riesgo ante un uso no diligente, de introducir virus o software ilegal en la empresa, de poner en entredicho la imagen empresarial o simplemente desviar los recursos de la empresa a otros fines.

2.2 Correo electrónico

2.2.1 Introducción

El correo electrónico sin duda fue uno de los grandes invenciones de la tecnología del Internet, tanto que revoluciono la forma de comunicación y se fue posesionando rápidamente entre las actividades mas frecuentes en el Internet.

Los beneficios de esta tecnología pasan más allá del orden tecnológico y se reflejan en el aspecto ambientalista ya que por su uso se vio un reemplazo gradual al correo postal; fue una gran invención para el cuidado del medio ambiente, el ahorro de papel, combustible, tinta, etc. Materiales que se utilizaban para el envío y recepción de correo postal y que constituían un gran costo para el medio ambiente fueron reduciéndose de tal forma que el correo postal que se utilizaba antes de la aparición del correo electrónico disminuyo a solo el 10% de su uso anterior

El correo electrónico o también conocido con su denominativo en ingles e-mail es un servicio de red que permite a sus usuarios enviar y recibir mensajes privados, estos mensajes se denominan mensajes electrónicos o correos electrónico y es posible enviarlos y recibirlos mientras estemos conectados a una red sea esta el Internet o una red privada Intranet, esta forma de comunicación abrió una nueva etapa en la tecnología de las comunicaciones pues mediante este medio uno puede enviar todo tipo de

información como documentos, archivos, música, etc. Con nuevas características como son la rapidez, economía y de forma muy simple, sin contar los lugares tan remotos a los que se tiene acceso. El único requisito que el usuario debe de cumplir, es que tenga una cuenta de acceso es decir un espacio reservado en un servidor de correo electrónico donde él tendrá la posibilidad de almacenar sus mensajes, esta cuenta tiene el nombre de Dirección Electrónica.

La dirección electrónica sirve como referencia de una dirección especifica, es decir nosotros la tenemos que utilizar para poder lograr que nuestro mensaje llegué al destino deseado, este tipo de direcciones electrónicas tiene un formato definido y están compuestas por un nombre de usuario seguido del símbolo ARROBA @ y al final los datos del proveedor del servicio y en algunos casos el país de donde proviene el servicio

Figura 2.2.1 Formato dirección electrónica

2.2.2 Tipos de cuentas de correo

Existen dos tipos de cuentas de correo electrónico una es la Web y el correo llamado POP y las desarrollaremos a continuación.

2.2.2.1 Correo web

El correo Web o también denominado Webmail es una forma de usar el correo electrónico basado en la Web, esta opción nos permite utilizar el explorador Web y las

interfaces desarrolladas por nuestros proveedores de correo electrónico para poder acceder a nuestra cuenta de correo electrónico, cuando recibimos un mensaje de correo electrónico generalmente se almacene en el servidor de correo Web y no en nuestro computador, es así que se ve la necesidad de conectarnos a Internet para poder visualizar estos mensajes. Al usar el correo electrónico de esta forma tenemos muchas ventajas y desventajas:

Ventajas

Entre las ventajas que se tiene, usando el correo mediante WEB están:

- No configuración del correo electrónico
- Uso irrestringido en cualquier computador con conexión a Internet
- Accesibilidad en cualquier sistema operativo
- Es mas difícil infectarse por algún virus por que los mensajes no se almacenan en nuestro ordenador

Desventajas

- Poca capacidad de almacenamiento
- Lentitud acorde a la velocidad de la conexión
- Almacenamiento temporal del contenido de nuestros correos en el computador que estemos utilizando

2.2.2.2 Correo POP

El correo POP es rápido, no se necesita estar conectado a Internet para redactar los mensajes, solo es necesario la conexión a la hora del envió y cuando recibimos algún mensaje, estos se descargan directamente a nuestro ordenador, la forma en que se envía un mensaje con este tipo de correo es la siguiente. Cuando recibimos un correo electrónico estos se almacenaran en una computadora llamada servidor POP, este

servidor tiene un archivo que esta asociado a nuestra cuenta de correo electrónico y aquí están contenidos todo lo que se nos ha sido enviado.

Por otra parte los correos salientes son enviados a una computadora llamada SMTP, este servidor básicamente busca el nombre de dominio en la direccion de correo electrónico a la que se envía, luego hace una búsqueda en el DNS a fin de verificar a qué servidor POP3 deberá enviar el correo.

Al iniciar el cliente de este tipo de correo electrónico estas son las operaciones que se hacen:

- El cliente abre una conexión de red hacia el servidor
- El cliente envía la contraseña secreta al servidor POP
- El servidor POP envía el correo entrante a tu computadora
- El cliente envía el correo saliente al servidor SMTP

Ventajas

- Rapidez
- Espacio de almacenamiento depende del espacio del ordenador
- Conexión directa con el servidor, disponibilidad de todos los correos
- Uso en Intranets

Desventajas

- Información transmitida en texto plano fácil de intervenir
- Login y password no se verifican ni en SMTP ni en POP
- Fácil infección por Virus
- Fácil de Monitorear

En general estas dos formas de uso de correo electrónico no nos brindan ninguna seguridad pero si las ventajas que ya de sobremanera conocemos, a continuación detallaremos estos aspectos de manera mas general.

2.2.2.3 Ventajas del correo electrónico

Costo

El e-mail es mucho más barato que el correo postal y llamadas telefónicas, no importa la distancia que el mensaje electrónico deba recorrer para llegar a destino ya sea de algun lugar remoto del planeta a otro lugar muy remoto, el costo es el mismo ya que en todos los casos representa el costo del tiempo de uso del servicio de Internet por el tiempo de redacción y envío. Generalmente se calcula el costo del e-mail en base al tiempo consumido para transferir el mensaje a través del proveedor de acceso a Internet. Este tiempo de transferencia de la correspondencia electrónica depende del tamaño del archivo: generalmente consume unos pocos segundos, no se paga por cada mensaje enviado sino que por una tarifa de tiempo de Internet consumido, se pueden enviar los e-mails que se deseen.

Versatilidad

Además del cuerpo del texto, es posible adjuntar al mensaje cualquier tipo de archivo que es procesable por una computadora como revistas, planillas de cálculo, sonidos, fotos, videos, documentos, etc. Para ello simplemente se debe anexar estos archivos de una forma especial (el programa de correo lo hace de manera automática). Los archivos enviados son despachados y recibidos en formato digital, lo cual permite que quien los reciba pueda modificarlos.

Velocidad

No importa la distancia que el mensaje deba recorrer el e-mail es muy veloz y no tardará más de unos pocos minutos en llegar a destino. Pueden existir demoras en la lectura del mensaje, ya sea porque la forma en que algunas empresas distribuyen internamente los mensajes electrónicos a cada destinatario final, o bien porque el destinatario mismo demora en leerlo.

Comodidad

Quien recibe un mensaje puede responderlo en el momento que desee, sin la presión de tiempo que implica una llamada telefónica. Según estadísticas de países con hábitos de este servicio refieren que las personas responden más a sus e-mails que sus llamados telefónicos. Y además, los que responden a un e-mail sólo tienen que apretar el botón "Responder", del programa de correo electrónico.

Alcance

Al momento de enviar mensajes de forma masiva como para reuniones, fechas de exámenes, etc, no es necesario enviarlos de forma individual, el e-mail permite enviar el mismo correo a varias personas a la vez sin incurrir en costos adicionales

Se debe destacar que en una mayoría de los casos los servidores de correo electrónico ofrecen este servicio de manera gratuita, y la forma en la que podemos acceder a toda la funcionalidad del correo electrónico es mediante el WebMail que nos ofrece el servidor de correo electrónico o usando programas de usuario de correo electrónico como Outlook.

2.3 SPAM

2.3.1 Introducción

El SPAM, correo electrónico basura o correo electrónico no solicitado, este fenómeno se originó hace algunos años, con el uso del fax y de llamadas Telefónicas, que para efectos de mercadeo tomó fuerza alrededor de los ochenta, y se crearon compañías especializadas en Telemercadeo que, utilizando máquinas efectuaban llamadas de manera automática, enviando faxes a distintas personas, promocionando de esta manera toda clase de productos o servicios; así sin saber cómo ni desearlo, llegaban a las máquinas de fax, publicidad con información como por ejemplo: lugares para vacacionar, información sobre el último modelo de auto, opciones para adquirir una casa en la playa, etc. Quien recibía dichos faxes, comúnmente le sucedía que cuando en realidad esperaba uno urgente, la máquina carecía de papel o de tinta provocando la perdida de mensajes realmente útiles y necesarios.

2.3.2 Evolución del término SPAM

El termino SPAM aparece con la Empresa Hormel Foods que en 1937 lanza un tipo de carne en lata llamada Hormel´s Spiced Ham. El éxito llevo a convertirla en una marca genérica "SPAM". Durante la Segunda Guerra Mundial fue usada para alimentar las tropas militares (soviéticas y británicas), El uso del término SPAM, para identificar el correo masivo no solicitado, fue porque éste embutido saturó el mercado estadounidense de tal forma que no había lugar donde este producto no se encuentre, es decir este producto aunque era no deseado, pero sin embargo estaba presente en todas las mesas haciendo de esta manera una relación con el correo electrónico no deseado o SPAM que esta presente en nuestras cuentas.

Se cree que el primer correo electrónico SPAM, pudo haber sido aquel que en 1978 envió un vendedor de la Digital Equipment Corporation de forma masiva para anunciar la inauguración de unas sucursales de la compañía.

Sin embargo, el 5 de marzo de 1994, es el primer día que se uso el SPAM del que se tiene registro, esto ocurrió en Estados Unidos; este día una firma de abogados de Canter and Siegel, publicó en Usenet un mensaje de anuncio de su firma legal, el cual en el primer día después de la publicación, facturó cerca de 10.000 dólares por casos de sus amigos y lectores de la Red. Desde ese entonces, el marketing mediante correo electrónico ha crecido a niveles impensados desde su creación.

2.3.3 ¿Qué es SPAM?

El SPAM o correo electrónico no solicitado o no deseado, se lo puede definir como el mal uso de la tecnología, ya que se la utiliza como un medio para poder hacer publicidad masiva, robo de información, Phishing, hacking, etc., a traves del correo electrónico; es decir prácticas muy ofensivas al usuario final, ya que las consecuencias de caer en este tipo de trampas, que vienen en nuestros correos electrónicos, involucran desde la perdida de grandes sumas de dinero "robo de información de tarjetas de crédito, fraudes" hasta el daño de nuestra computadora "computadora zombie"

A este tipo de ataque se le denomina SPAM, el SPAM son mensajes no solicitados, habitualmente de tipo publicitario enviados en cantidades masivas; aunque se puede publicitar a través de distintos medios, el más utilizado actualmente es el correo electrónico.

Se debe establecer que hay una diferencia, entre correo legítimamente publicitario y el SPAM, y está en que el correo legítimo publicitario, es aquel que el usuario autoriza recibir mientras que el SPAM es correo enviado sin permiso del receptor.

El contenido del SPAM puede variar

a. Información actual del tema en boga
b. Información para conseguir dinero de forma supuestamente fácil y rápida.
c. Información de que fuimos acreedores a un premio millonario
d. Cadenas de cartas y mensajes
e. Enlaces a páginas Web pornográficas o líneas eróticas.
f. Personas, generalmente niños (que son los que mas fácil nos conmueven el corazón) muy enfermos, los cuales podemos salvar enviando el correo que nos llega con la información a todos nuestros contactos y conocidos.
g. Información sobre Falsos virus, en ocasiones contienen virus reales

Con estos SPAM's los objetivos que persiguen los Spammers son distintos y los podemos detallar

- Robo de identidad, Negocios fraudulentos (Phishing)
- Robo de información con software (MalWare, Spammer bots o Spyware)
- Infección de la computadora "programas que hacen de nuestras computadoras emisoras de SPAM" (Computadoras zombis)
- Venta de servicios o productos

2.3.4 ¿Que son los Spammers?

Un Spammer es una persona, compañía o bot que se dedica a la distribución o envío de SPAM (correo o mensajes considerados basura), que para cuyo objetivo, estas personas roban o compran direcciones de correo electrónico sustraídas y verificadas con un grado de probabilidad de tener éxito a las que remiten e-mails no solicitados o SPAM. También se los conoce como cazadores de direcciones de correo electrónico por que además de emitir correo electrónico no deseado, también usan métodos ilegales para conseguir direcciones de correo electrónico a través de la creación de paginas Web fraudulentas, programas que utilizaran (bots, virus, gusanos, troyanos), Ingeniería social, Ingeniería social inversa, ataques de monitorización, búsqueda de puntos débiles de los sistemas, etc.

Esta actividad ilícita practicada por los Spammers en el mundo se puede controlar con algunos filtros anti SPAM y mecanismos legales; esta actividad es penada y sancionada por leyes en diferentes países en los cuales se tiene una normativa legal respecto a esta problemática, este tema lo desarrollaremos mas en el capitulo III del presente estudio.

2.3.5 Técnicas SPAM

Podemos definir la palabra técnica como el procedimiento o recurso del que se sirve una ciencia, arte o una actividad, para el presente estudio se define **TECNICA,** como los procedimientos lógicos y legales; en el caso de los Spammer técnica significa el procedimiento lógico que utiliza para el alcance de sus objetivos.

El uso de estas técnicas esta basada en la búsqueda de satisfacer algunas necesidades i/o conseguir algunos objetivos, y a continuación detallamos:

1. La existencia de personas mal intencionadas que persiguen objetivos hostiles como el robo, fraude, etc.

2. La necesidad de las empresas de reducir costos en la publicidad de sus productos o servicios mediante el correo electrónico

Debemos tomar en cuenta que en ambos casos, las entidades o personas particulares hacen contacto con el Spammer que es el encargado de conseguir las direcciones electrónicas, este a su vez debe de comprobar la información además de ser capaz de conseguir más información de las mismas cuentas como: los datos personales de cada dirección electrónica, preferencias del usuario, amistades del usuario, etc. Para esto hace uso de diferentes técnicas como:

2.3.5.1 MalWare:

Del inglés **mal**icious soft**ware**, también llamado **badware** o **software malicioso**, son aquellos programas o partes de ellos que tienen un efecto malicioso en la seguridad de la computadora. Este término engloba muchas definiciones las cuales son mas conocidas como "Virus", "Worm (gusano)" y "Trojan (troyano)" y otras de las que posiblemente no se conozcan tanto como "Rootkit", "Logicbomb (bomba lógica)" y "Spyware"; es un software que tiene como objetivo infiltrarse o dañar un ordenador sin el conocimiento de su dueño. Esta expresión es un término general muy utilizado por profesionales de la computación para definir una variedad de software o programas de códigos hostiles e intrusos.

Muchos usuarios de computadores no están aún familiarizados con este término y otros incluso nunca lo han utilizado. Sin embargo la expresión "virus informático" es más utilizada en el lenguaje cotidiano y a menudo en los medios de comunicación para describir todos los tipos de Malware. Generalmente el Malware relaciono al SPAM se presenta en dos formas: Spyware y Spammer bots

i. Spyware

Nació como un conjunto de aplicaciones incluidas junto al software gratuito, con el objetivo de obtener información sobre la actividad del usuario en su computadora, a fin de poder determinar su perfil de navegación e intereses. Esto tiene mucho valor para las compañías dedicadas al marketing en Internet, ya que gracias a esta información pueden confeccionar bases de datos que les permiten conocer fehacientemente qué es lo que puede interesarle a cada usuario o perfil en particular.
Posteriormente esta forma de uso de el spyware se fue desvirtuando en cuanto ya fue utilizado para espiar a las computadoras donde este residía, ya no solo se buscaba ver el tipo de actividad que tenia el usuario en su PC sino también el tipo de información que el almacenaba.

El Spyware tiene distintas formas de difusión, pueden llegar ocultos en programas (Troyanos), o enmascarados en algún correo electrónico ocultando su verdadera identidad mediante la manipulación de extensiones de archivos ejecutables (*.exe, *.bat, *.msi) a archivos generalmente manipulados por cualquier usuario estándar (*.doc, *.xls, *.ppt, *.pdf, etc).

La forma que uno puede caer en este tipo de trampa es la siguiente; consiste en que. el usuario recibe un archivo adjunto en un correo, este mail puede provenir de una persona conocida o desconocida, el contenido que dice brindar el archivo adjunto puede variar desde prometer un juego adjunto, un archivo de algún tema de interés del receptor, algún video o foto de nuestro artista favorito, etc. Si el usuario cree en lo que promete el dicho correo electrónico y descarga y abre ("Ejecuta") el archivo, luego que se ejecuta el archivo, se ejecuta el Spyware y es una de los Malwares mas dificiles de reparar por que se trata de un programa o virus que modifica el Firewall de la computadora y además modifica las firmas de virus del antivirus de la PC haciéndose imposible de detectar,

tiene como objetivo infiltrarse en el computador y comenzar a hacer conexiones con equipos remotos de la lista de direcciones de la PC local reenviándose asimismo, se comienza a crear un registro por pagina documento y datos que el usuario empieza a utilizar en su computador, robo de cookies, Keyloggers, etc. Por otro lado mientras se cree que la PC tiene un posible mínimo daño en su funcionamiento, la misma esta enviando de forma no intencionada una copia de toda la información que tiene el propietario hacia algún sitio del Internet haciendo así a esta computadora una computadora Zombie, que luego de cumplir con el total del objetivo del programa Spyware, la computadora puede ser manipulada por el agresor y nuevamente comenzar la cadena de difusión de Spyware pero ya con una nueva cuenta de correo electrónico y una nueva IP valida y con nuevos contactos validos, la computadora que este totalmente contaminada por Spyware podrá ser manipulada desde sus periféricos hasta una manipulación visual.

Si bien esta forma puede instalarse a través de algún correo electrónico como SPAM, también lo puede hacer a través de una página falsa que se enlaza desde el buscador.

ii. Spammers bots

Son otra forma de Malware, esta técnica se basa en el uso de pequeñas aplicaciones que llegan a nuestra computadora ocultos en programas que los Spammers publicitan; se los conoce como Troyanos, pero a diferencia de los Spyware estos programas trabajan siempre que se tenga conexión a Internet por que son manipulados por su creador mediante ordenes que se envían por Internet, residen en nuestras computadoras, hasta que nosotros los identifiquemos ellos revisan todos los documentos y buscan información contenida en el formato tradicional del Correo electrónico(Fig. 1), cualquier información que ellos obtengan la envían a su creador, el objetivo que estos programas persiguen es el de conseguir cuentas de correo electrónico y toda la información asociada, estos programas en muchos casos llegan a nuestras computadoras cuando

nosotros instalamos programas de dudosa procedencia y al desinstalarlo no eliminamos el Bot.

From	Nombre y dirección del usuario que envía el mensaje
to	Nombre y dirección del destinatario
Cc	Nombre y dirección del destinatario de la copia del mensaje
Date	Fecha y hora en la que se mando el mensaje
Subject	Tema o asunto del mensaje
Attachment	Contenido del mensaje

Figura 2.3.5.1.2 Campos estándar de la cabecera de un mensaje

2.3.5.2 Phishing, o envió de e-mails de forma aleatoria

El "Phishing" es una modalidad de estafa diseñada con la finalidad de robarle la identidad, el delito consiste en obtener información tal como números de tarjetas de crédito, contraseñas, información de cuentas u otros datos personales por medio de engaños. Este tipo de fraude se recibe habitualmente a través de mensajes de correo electrónico o SPAM.

En esta modalidad de fraude, el Spammer malintencionado envía millones de mensajes falsos (SPAM) que parecen provenir de sitios Web reconocidos o de su confianza, como su Banco de confianza o alguna empresa conocida. Dado que los mensajes y los sitios Web que envían estos usuarios parecen oficiales, logran engañar a muchas personas haciéndoles creer que son legítimos. La gente confiada normalmente responde a estas solicitudes de correo electrónico con sus números de tarjeta de crédito, contraseñas, información de cuentas u otros datos personales.

Para que estos mensajes parezcan aun más reales, el estafador suele incluir un vínculo falso que parece dirigir al sitio Web legítimo de la empresa o institución, pero en realidad lleva a un sitio falso o incluso a una ventana emergente que tiene exactamente el mismo aspecto que el sitio Web oficial. Estas copias se denominan "sitios Web piratas". Una vez que el usuario está en uno de estos sitios Web, introduce información personal sin saber que se transmitirá directamente al delincuente, que la utilizará para realizar compras, solicitar una nueva tarjeta de crédito o robar su identidad.

La idea central detrás del Phishing es pescar usuarios desprevenidos, robarles los datos de sus cuentas bancarias, y luego su dinero, todo por Internet... así de simple pero así de complejo, porque se requiere de profundos conocimientos en programación, y de una total falta de moral.

También el Phishing puede describirse como una extensión de los hoaxes (cadenas), de modo que llevan las técnicas de engaño a su peor nivel: las estafas bancarias. No obstante, existen otro tipo de fines, como recaudar información de los usuarios. Cuando uno piensa en el SPAM como una molesta técnica publicitaria, bajo la cual se envían millones de ofertas a diario de todo tipo de productos..

El envío de e-mails de forma aleatoria y masiva con títulos muy atractivos como información de Premios millonarios, Viajes a muy bajo costo o Terapias para mejorar la imagen que a veces son de nuestro interés, nosotros al abrir la URL relacionada estamos confirmando la validez de nuestra dirección de correo electrónico, en muchos casos estos correos vienen sustentados con paginas Web.

2.3.5.3 Hoaxes, e-mails en cadena

Los hoaxes (broma, engaño) son mensajes de correo electrónico engañosos que se distribuyen en cadena.

Esta técnica es una de las mas utilizadas, ya que en la actualidad los foros y salas de chats son una parte muy utilizada del Internet, los Spammers hacen correr programas que en cada pagina Web identifican el separador de nombre y dominio como es @ "Juan_perez@yahoo.com" y copian toda palabra que tenga esas características para poder tener una lista de correos electrónicos válidos y posibles a atacar por que están accesibles en los foros, los chats son otra forma de conseguir información verídica y susceptible, los Spammer hacen contactos en muchos grupos de Chat, y en esta interfaz también ellos consiguen información verificada.

Posteriormente ellos comienzan con los Hoaxes o cadenas enviando a las nuevas cuentas de correo electrónico nuevos mensajes que por su contenido y por lo que promete, los receptores de el email continúan muchas veces con la cadena, de alguna forma en este tipo de comunicación con Hoaxes, se ve el efecto boomerang y consiste en que el Spammer luego de lanzar la cadena o boomerang esta vuelve a el, pero con muchas mas direcciones de correo electrónico validas.

Actualmente los Hoaxes perdieron credibilidad y los Spammers ahora optan por otro tipo de Hoaxes en los cuales envían correo electrónico a un email valido informando de algún problema (guerra, enfermedad de alguna persona, animales en peligro, etc) que se podría solucionar con el solo reenvió del email a una x cantidad de personas, pero con una copia a el remitente para que así este pueda verificar la validez del supuesto apoyo y así coadyuvar a la solución del supuesto problema.

Posteriormente ellos clasifican las direcciones de correo electrónico obtenidas según la informaron adicional que ellos tengan sobre cada cuenta de correo electrónico, y nuevamente continúan con su practica pero en las restantes direcciones de correo electrónico.

2.3.5.4 Recolección de información a través de web bugs

Una forma mas actual de SPAM son los Web Bugs, una de las preocupaciones en material de seguridad con los correos basados en HTML. Los Web bugs son imágenes escondidas en los correos electrónicos y evaden muchas barreras anti SPAM, estos enlazan hacia el servidor de quien lo envía, generalmente estas imágenes vienen adjuntas en correos publicitarios y al no tener texto los filtros no pueden estudiar el contenido, al acceder al vinculo que viene tras la imagen, se hace notificación de que han abierto el correo, otro problema relacionado son los scripts en el correo y es que ejecutan una aplicación dando paso a algún bot.

Todas estas técnicas mencionadas son muy útiles para la obtención de direcciones de correo electrónico, y en sociedades como las nuestras donde aun no se han implementado políticas de prevención, información y de sanción contra problemáticas como el SPAM, en donde por el poco conocimiento que se tiene sobre la tecnología de Internet, la ingenuidad, inexperiencia y por las preferencias que tiene mucha gente a las cosas que se nos dan de forma gratuita somos muy vulnerables al SPAM

SEGURIDAD

2.4.1 Introducción

La "Seguridad es una necesidad básica, está interesada en la prevención de la vida y las posesiones, es tan antigua como ella". Los descubrimientos arqueológicos marcan, sin duda, las más importantes pruebas de seguridad de los antiguos pueblos y reinados, las

pirámides egipcias, el palacio de Sargon, el templo Karnak en el valle del Nilo; el dios egipcio Anubi representado con una llave en su mano.

Se sabe que los primitivos, para evitar amenazas, reaccionaban con los mismos métodos defensivos de los animales luchando o huyendo, para eliminar o evitar la amenaza. Así la pugna por la vida se convertía en una parte esencial y los conceptos de alertar, evitar, detectar, alarmar y reaccionar ya eran manejados por ellos.

Como todo concepto, la Seguridad se ha desarrollado y ha seguido una evolución dentro de las organizaciones sociales. La sociedad se conformó en familias, y esto se convirtió en un elemento limitante para huir. Se tuvieron que concebir nuevas estrategias de intimidación y disuasión para convencer al atacante que las pérdidas eran inaceptables contra las posibles ganancias.

La seguridad moderna se originó con al Revolución Industrial para combatir los delitos y movimientos laborales, tan comunes en aquella época. Finalmente, un teórico Henry Fayol en 1919 identifica la Seguridad como una de las funciones empresariales, luego de la técnica, comercial, financiera, contable y directiva. Al definir el objetivo de la Seguridad, Fayol dice: "…salvaguardar propiedades y personas contra el robo, fuego, inundación contrarrestar huelgas y felonías, y de forma amplia todos los disturbios sociales que puedan poner en peligro el progreso e incluso la vida del negocio. Es generalmente hablando, todas las medidas para conferir la requerida paz y tranquilidad al personal" *(**Henri Fayol** – 1949, General and Industrial Management.)*

Las medidas de seguridad a las que se refiere Fayol, sólo se restringían a los exclusivamente físicos de la instalación, ya que el mayor activo era justamente ese: los equipos, ni siquiera el empleado. Con la aparición de los "cerebros electrónicos", esta

mentalidad se mantuvo, porque ¿quien sería capaz de entender estos complicados aparatos como para poner en peligro la integridad de los datos por ellos utilizados?

Hoy la seguridad desde el punto de vista legislativo, está en manos de los políticos a quienes les toca decidir sobre su importancia, los delitos en que se pueden incurrir, y el respectivo castigo, si correspondiera. Este proceso ha conseguido importantes logros en las áreas de prevención del crimen, terrorismo y riesgo más que en el pensamiento general sobre Seguridad.

En cambio desde el punto de vista técnico, la seguridad está en manos de la dirección de las organizaciones y en última instancia en cada uno de nosotros y en nuestro grado de concientización respecto a la importancia de la información

2.4.2 ¿Que es la seguridad?

La Seguridad, es hoy día una profesión compleja con funciones especializadas, para dar una respuesta satisfactoria es necesario eliminar la incertidumbre y distinguir entre la seguridad filosófica y la operacional o práctica.

Analicemos; en un problema de seguridad pueden apreciarse tres actores:

1. El poseedor del valor: **Protector**.
2. Un aspirante a poseedor: **Competidor–Agresor**
3. Un elemento a proteger: **Valor**

Luego, la **Seguridad** se definirá como:

"La interrelación dinámica (competencia) entre el agresor y el protector para obtener (o conservar) el valor tratado, enmarcada por la situación global." (*Dr. Giovanni Manunta, SEGURIDAD UNA INTRODUCCION)*

Algunas aclaraciones:

1. El protector no siempre es el poseedor de valor.
2. El agresor no siempre es el aspirante a poseedor.
3. Ambas figuras pueden ser delegadas a terceros por el cambio de otro valor, generalmente dinero.
4. El valor puede no ser algo concreto. Por ejemplo se podría querer cuidar el honor, la intimidad, el conocimiento, etc.
5. La situación global indica que no será lo mismo el robo de un comercio en Argentina que en Andorra en donde sus habitantes se ven obligados a robar para subsistir.

Los competidores se pueden subdividir en:

• **Competidor Interno:** es aquel que piensa que el interés de la organización está por encima de sus intereses y por lo tanto, actúa para sobreponer su interés personal, provocando daños a la organización.
• **Competidor Externo:** es aquel que actúa para arrebatar al poseedor lo que para él significa un valor empresarial o personal (clientes, mercado, información, etc.).

"La seguridad en un problema de antagonismo y competencia. Si no existe un competidor y amenaza el problema no es de seguridad".

"El objetivo de la seguridad informática respecto al correo electrónico será mantener la privacidad, disponibilidad, integridad, autenticidad, y control de la información procesada por esta vía y sus aspectos fundamentales.

2.4.3 Análisis del objetivo de la seguridad informática

Para un buen análisis del concepto de Seguridad Informática se deberá conocer los conceptos de la información

Se define **Dato** como "la unidad mínima con la que compone cierta información. Datum es una palabra latina, que significa "lo que se da".

La **Información** es un conjunto de datos que tiene un significado específico más allá de cada uno de éstos y tendrá un sentido particular según como y quien la procese. Ejemplo: 1, 9, 8 y 7 son datos; su agregación 1987 es Información.

Establecer el valor de la información es algo totalmente relativo pues constituye un recurso que en muchos casos no se valora adecuadamente debido a su intangibilidad, cosa que no ocurre con los equipos las aplicaciones y la documentación.

Existe Información que **debe o puede ser pública** puede ser visualizada por cualquier persona (por ejemplo índice de analfabetismo en un país) y aquella que **debe ser privada** sólo puede ser visualizada por un grupo selecto de personas que trabaja con ella (por ejemplo antecedentes médicos). En esta última debemos maximizar nuestros esfuerzos para preservarla de ese modo reconociendo las siguientes características en la Información:

- Es Crítica: es indispensable para garantizar la continuidad operativa.

- Es Valiosa: es un activo con valor en sí misma.
- Es Sensitiva: debe ser conocida por las personas que la procesan y sólo por ellas.

2.4.4 Características de la información

2.4.4.1 Integridad

Es la característica que hace que su contenido permanezca inalterado a menos que sea modificado por personal autorizado, y esta modificación sea registrada para posteriores controles o auditorias. Una falla de integridad puede estar dada por anomalías en el hardware, software, virus informáticos y/o modificación por personas que se infiltran en el sistema (Spammers).

2.4.4.2 Disponibilidad u operatividad

La Información debe estar siempre disponible para ser procesada por las personas autorizadas. Esto requiere que la misma se mantenga correctamente almacenada con el hardware y el software funcionando perfectamente y que se respeten los formatos para su recuperación en forma satisfactoria.

2.4.4.3 Privacidad o confidencialidad

Es necesario que la Información sólo sea conocida por personas autorizadas. En casos de falta de confidencialidad, la Información puede provocar severos daños a su dueño (por ejemplo conocer antecedentes médicos de una persona) o volverse obsoleta (por ejemplo: los planes de desarrollo de un producto que se "filtran" a una empresa

competidora, facilitarán a esta última desarrollar un producto de características semejantes).

2.4.4.4 Control

El control sobre la información permite asegurar que sólo los usuarios autorizados pueden decidir cuando y como permitir el acceso a la misma.

2.4.4.5 Autenticidad

Define que la información requerida es válida y utilizable en tiempo, forma y distribución. Esta propiedad también permite asegurar el origen de la información, validando el emisor de la misma, para evitar suplantación de identidades. Adicionalmente pueden considerarse algunos aspectos adicionales, relacionados con los anteriores, pero que incorporan algunos aspectos particulares:

- **No Repudio:** mediante la cual se evita que cualquier entidad que envió o recibió información alegue, ante terceros, que no la envió o recibió.
- **Consistencia:** se debe poder asegurar que el sistema se comporte como se supone que debe hacerlo ante los usuarios que corresponda.
- **Aislamiento:** este aspecto, íntimamente relacionado con la **Confidencialidad**, permite regular el acceso al sistema, impidiendo que personas no autorizadas hagan uso del mismo.
- **Auditoria:** es la capacidad de determinar qué acciones o procesos se están llevando a cabo en el sistema, así como quién y cuando las realiza.

2.4.5 Amenazas

Cabe definir **Amenaza**, en el entorno informático, como cualquier elemento que comprometa la seguridad del sistema.

Amenazas para la Seguridad

Figura 2.4.5 Amenazas

Las amenazas pueden ser analizadas en tres momentos: antes del ataque durante y después del mismo. Estos mecanismos conformarán políticas que garantizarán la seguridad de nuestro sistema informático.

Se llama intruso al atacante o persona que accede o intenta acceder sin autorización a un sistema ajeno ya sea en forma intencional o no intencional, para el caso del presente estudio el atacante es el Spammer

2.4.5.1 Tipos de Intrusos

- Clase A.- Son el tipo de intrusos que bajan programas de Internet, prueba y juegan, son intrusos que hacen sus pruebas en el Internet

- Clase B.- Son un poco mas peligrosos saben compilar programas pero no conocen de programación, tienen conocimiento de sistemas operativos y sus vulnerabilidades
- Clase C.- Son intrusos que sabe conoce y define sus objetivos, conocen como usar accesos remotos y saben como ingresar
- Clase D.- Conocen lo sistemas a los cuales atacar y saben la información que buscan

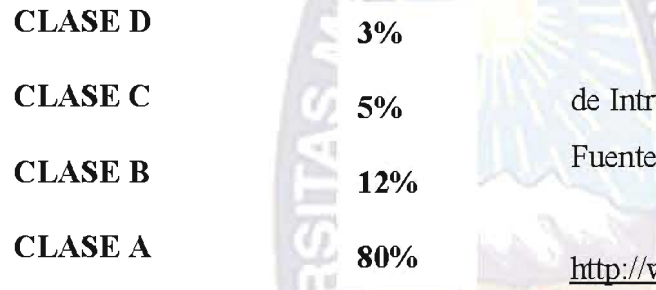

Figura 2.4.5.1 Tipos de Intrusos
Fuente: Cybsec estudio de tipos de intrusos: http://www.cybsec.com/

2.4.6 Relación seguridad y operatividad

El termino seguridad tiene mucho que ver con la operatividad o amigabilidad del sistema para el usuario. En este ejemplo veamos el caso de una computadora extremadamente segura, esta debe estar instalada a 20 metros bajo tierra en un recinto de hormigón, aislada informáticamente de otras computadoras, aislada electrónicamente y alimentada por un sistema autónomo, esta computadora brinda una seguridad excelente pero una utilidad casi nula.

Con esto demostramos que la utilidad y la seguridad de una computadora son inversamente proporcionales, es decir mientras mas seguro sea un sistema informático su utilidad desciende

OPERATIVIDA 1

UTILIDAD

Mecanismos de seguridad

A. **La Prevención (antes):** mecanismos que aumentan la seguridad (o fiabilidad) de un sistema durante su funcionamiento normal. Por ejemplo el cifrado de información para su posterior transmisión.
B. **La Detección (durante):** mecanismos orientados a revelar violaciones a la seguridad.
C. **La Recuperación (después):** mecanismos que se aplican, cuando la violación del sistema ya se ha detectado, para retornar éste a su funcionamiento normal. Por ejemplo recuperación desde las copias de seguridad (backup) realizadas.

2.4.7 La seguridad digital y el correo electrónico:

La seguridad digital surge como un principio de la nueva sociedad de la información que permite el resguardo preventivo de los bienes propiedad de los agentes que intervienen en los medios de comunicación, y que puedan verse vulnerados con los avances tecnológicos. La seguridad digital puede proteger la información que se resguarda en formato digital [ya sea en línea (en la Web) o en ordenadores públicos o privados] mediante mecanismos técnicos y normas de seguridad empresariales o institucionales que protejan los bienes y la información sensible o en trámite.

En el caso de los empleados estatales, éstos son depositarios de bienes públicos, llamados a ejercer todas las acciones de control y supervisión de aquellos bienes adquiridos con recursos del Estado. Es parte del deber de diligencia y sana

administración, proteger la información sensible, proteger los recursos y tomar toda previsión posible que evite eventuales responsabilidades administrativas, civiles o penales, o bien pérdidas que representen un perjuicio económico para el Estado. Igualmente, en el caso de los trabajadores de empresa privada, dentro de su contrato laboral están llamados a proteger los bienes de la empresa en la que trabajan, por lo que adoptar medidas para proteger la información que en ambos casos se manipula por el correo electrónico o evitar accesos no autorizados en virtud de un uso no diligente de sus claves o revelación de las mismas a terceros; resulta una obligación inherente a su condición de empleados.

Los derechos que se protegen con la seguridad digital se conocen con el carácter de sui generis, pues la doctrina constitucionalista no ha logrado consolidar la naturaleza de los mismos, aunque coinciden en la necesidad de su protección en virtud de los bienes jurídicos que resguardan. Por tanto, el acceso de los ciudadanos a los archivos y registros administrativos si bien es lícito y está protegido como parte del derecho a la información, ese derecho encuentra su límite si el acceso a la información afecta la seguridad y defensa del Estado, la averiguación de los delitos y la intimidad de las personas; o bien si se utiliza el derecho de forma abusiva para la manipulación, destrucción o uso ilegítimo de los bienes protegidos.

Las medidas de seguridad digital suelen variar dependiendo del servidor del que se trate. Por lo general, son normas de índole técnica y algunas que deben adoptar los usuarios según se obligan en las condiciones generales de acceso a los portales que proporcionan sus servicios.

.

3. MARCO PRÁCTICO

Resumen

El objetivo del presente capitulo es comprobar la validez global de la hipótesis, haciendo centro de estudio, la presencia del SPAM en Bolivia y las diferentes técnicas que existen para combatirlo.

En este contexto y, a partir de este enunciado, se retoman los problemas que fueron expuestos en el CAPITULO I, en el que se manifestaba sobre:

LA PRESENCIA DE SPAM EN EL CORREO ELECTRÓNICO DE USUARIOS BOLIVIANOS DE INTERNET

Para demostrar la validez de este problema, se recurrieron a técnicas de investigación que a continuación detallaremos, esto con el objetivo de corroborar o desvirtuar la siguiente hipótesis planteada:

UN ESTUDIO TECNICO SOBRE EL SPAM EN EL CORREO ELECTRONICO EN BOLIVIA NOS PERMITIRA OBTENER LOS LINEAMIENTOS TECNICO INFORMATICOS BASE PARA LA LUCHA CONTRA EL SPAM EN BOLIVIA

Considerando que, para la comprobación de la hipótesis se debe cumplir estrictamente las normas establecidas dentro de una investigación científica, inicialmente se realizo lo siguiente:

3.1 Operacionalización de variables

Identificación de variables: se identificaron 2 variables que son:

Variable Independiente (x): Estudio técnico sobre la presencia SPAM en Bolivia

Variable Dependiente (y): Lineamientos técnico informáticos base de la lucha Anti Spam en Bolivia

Para una mejor comprensión se realizara el estudio en 2 fases, la primera (FASE 1) hace el estudio respecto a la variable independiente con la finalidad de demostrar su validez, en esta primera fase se hará una investigación del tipo descriptivo para poder determinar la existencia o no de SPAM en Bolivia, su impacto y las medidas que se toman para evitarlo; la segunda fase (FASE 2) hará hincapié en la variable dependiente, también con la finalidad de demostrarla, en esta segunda fase la investigación será del tipo descriptivo o analítico, tratando de evaluar las medidas que se deben tomar para la lucha Anti SPAM

FASE 1

3.2 Variable Independiente

Tabla 3.2 Variable de independiente

Estudio técnico sobre la presencia de SPAM en Bolivia	Dimensión	Indicador	Instrumento

Definición Conceptual Presencia de correo no solicitado, dañino, fraudulento, en las cuentas de correo electrónico de personas e instituciones en Bolivia	Población	Población de usuarios de Internet que tiene una cuenta de correo electrónico	Análisis de Documentos Pruebas de laboratorio Entrevistas Encuestas
	Spammers bots o MalWare	Spyware Trojan horses, o caballos de troya	
	Phishing o envió de e-mails de forma aleatoria	Phishing	
	Hoaxes o distribución de e-mails en cadena	Alertas sobre virus incurables Mensajes de temática religiosa Cadenas de solidaridad Cadenas de la suerte Leyendas urbanas Métodos para hacerse millonario Regalos de grandes compañías	
	Recolección de Información a través de Web bugs	Imágenes	

A partir de la Operacionalización de las variables de la hipótesis planteada, la investigación demostró lo siguientes resultados.

3.3 Muestra y población

Para corroborar o desvirtuar la **"Presencia de correo no solicitado, dañino y fraudulento, en las cuentas de correo electrónico de personas en instituciones en Bolivia"** se hizo un estudio explorativo a través de encuestas aplicadas a usuarios de Internet en Bolivia, vía encuestas online, Encuestas físicas a personas, encuestas físicas a Altas autoridades informáticas en diferentes instituciones gubernamentales y no gubernamentales. Considerando la magnitud del propósito del presente estudio, se utilizaron técnicas estadísticas para poder hacer el cálculo apropiado y confiable del tamaño de la muestra n= 300 encuestados con un error apropiado para una tesis de grado equivalente a 0.06 o 6%.

3.3.1 Calculo del tamaño de la muestra

$$n = \frac{Z^2 * (p*q) * N}{Se^2 * (N-1) + Z^2 * (p*q)}$$

En la formula anterior y remplazando los siguientes datos:

N= Tamaño total de la población 480000 personas usuarios de Internet

Se= error aceptado= 6%=0.06

Z= Nivel de Confianza al 95%= 1.96

P= proporción en %

q=1-p 0

q y p se obtienen de estudios anteriores, si este no es el caso q y p= 0.5

Reemplazando los datos en la ecuación obtenemos:

n= 267, es decir que para tener una encuesta que represente con una confianza del 95% y un error aproximado de 6% debemos encuestar a por lo menos 267 personas, en el caso de estudio la encuesta se hará a un total de 300 personas haciendo asi el error mas pequeño aun, esto equivale al:

$$S^2 = Z^2 * (p*q)$$

Donde el nuevo error $n*(N-1)$ disminuye a un 5,65%, con una muestra de 300 personas bolivianas usuarias de Internet

Por sus características el SPAM en Bolivia esta identificado como:

Spammers bots o MalWare que hace daño lógico a una gran cantidad de computadoras con acceso a Internet o computadoras personales afectadas indirectamente

Existencia de Phishing o envió de e-mails de forma aleatoria, que atacan a muchos usuarios bolivianos de Internet que ingenuamente caen en esta trampa

Propagación de Hoaxes o distribución de e-mails en cadena, que esta presente en un 90% de las cuentas de correo y no existe información en los usuarios acerca de que esto es una problemática

A partir de la definición conceptual se avanza en los conocimientos interiorizándonos en las técnicas SPAM presentes en Bolivia, consecuencias y cantidades económicas perdidas a consecuencia de este problema, a continuación se hará la demostración de la afirmación de la variable independiente

3.4 Población Nacional

Para conocer el porcentaje de la población boliviana que utilizan Internet, tomaremos en cuenta la proyección de población hasta el año 2006, datos Proyección INE.

Tabla 3.4 Población Nacional

EDAD	2006			2007		
	Total	Hombres	Mujeres	Total	Hombres	Mujeres
TOTAL	9.627.269	4.799.178	4.828.091	9.827.522	4.900.162	4.927.360
0-4	1.287.479	656.475	631.003	1.293.134	659.355	633.779
5-9	1.198.737	611.181	587.556	1.215.036	619.415	595.621
10-14	1.135.680	578.457	557.223	1.145.858	583.750	562.108
15-19	1.006.825	510.944	495.882	1.035.164	525.644	509.520
20-24	876.469	442.185	434.285	898.751	453.775	444.976
25-29	767.145	384.014	383.130	785.260	393.514	391.746
30-34	683.878	339.150	344.728	697.867	346.506	351.361
70-74	124.009	55.640	68.368	127.389	57.146	70.242

Fuente Instituto Nacional de Estadística

3.5 Usuarios de internet en Bolivia

Tabla 3.5 Usuarios de Internet en Bolivia

Año	Número de usuarios de Internet	Posición	Cambio Porcentual	Fecha de la Información
2003	78.000	98		2000
2004	270.000	83	246,15 %	2002
2005	270.000	83	0,00 %	2002
2006	480.000	88	77,78 %	2005

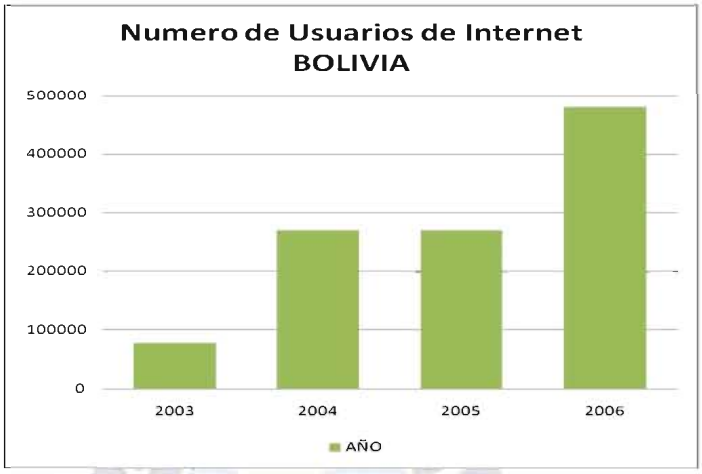

Figura 3.5 Usuarios de Internet en Bolivia
Super Intendencia de Telecomunicaciones (SITTEL), informe ITU
Año de información 2005

Según los datos que se observan en el cuadro anterior podemos notar que existe una cantidad aproximada de 480000 usuarios de Internet en Bolivia que constituye en relación a la proyección de población del INE de 2006 un equivalente a un 4.98% de la población hasta la fecha indicada. Así mismo se puede observar, que existe un substancial incremento de usuarios bolivianos de Internet entre los últimos años como se observa en la tabla

Se conoce de manera a priori que en Bolivia existe presencia de correo no solicitado (SPAM), y este afecta a un buen porcentaje de los usuarios bolivianos de Internet con cuentas de correo electrónico.

3.6 Estimación de presencia de SPAM en cuentas de usuarios de correo electrónico en Bolivia

Para poder tener una mayor precisión acerca de la presencia de SPAM en Bolivia, tanto a nivel institucional como a nivel personal se recolectaron datos en dos formas, la primera; cuestionarios cerrados aplicados a usuarios estándar de internet de diferentes edades en la cuidad de La Paz y el Alto, y el segundo cuestionario abierto aplicado a operadores informáticos de instituciones estatales y privadas.

3.6.1 Cuestionarios aplicados a Usuarios Bolivianos de Internet

Se considero para el presente estudio una muestra de 300 personas bolivianas, que tienen acceso al Internet, la encuesta fue realizada a personas de la ciudad de La Paz y El Alto, con el objetivo de obtener información valiosa en relación a el correo electrónico y el SPAM; la presente encuesta se aplico a determinados grupos sociales y de distintas edades, se visitaron colegios, instituciones privadas, Universidades y también se hizo una cantidad de encuestas en linea, con el siguiente cuestionario

CUESTIONARIO I

Problemas de seguridad en el Correo Electrónico en Bolivia

1.- Seguridad en el Uso del Correo Electrónico

Por favor, dedique unos momentos a completar esta pequeña encuesta, la información que nos proporcione será utilizada para un mejor estudio de la presencia de SPAM en B O L I V I A

Sus respuestas serán tratadas de forma confidencial y no serán utilizadas para ningún otro propósito distinto a el objetivo de la Investigación

Esta encuesta durara aproximadamente 5 minutos, gracias.

*1. ¿Tiene usted una cuenta de correo electrónico?

○ Si ○ No ○ Si tengo mas de una cuenta de correo

*2. Sabe usted ¿Qué es el SPAM? por favor responda con honestidad

2.- Satisfacción General en su Correo Electrónico

En esta sección le haremos preguntas que nos podrán guiar para poder saber si usted fue atacad@ por SPAM

*3. En general ¿Cuál es su grado de satisfacción con su proveedor de correo electrónico Hotmail, Gmail, Yahoo, Latinmail, etc?

○ Completamente satisfecho ○ Satisfecho ○ Insatisfecho ○ Completamente insatisfecho

*4. ¿Que aspectos de su proveedor de correo electrónico le molestan?

☐ El espacio que le brindan

☐ El correo no solicitado que le llega

☐ No control de los virus que llegan por e-mail

☐ El poco tiempo de caducidad de su cuenta

☐ Otro (Por favor especifique)

*5. ¿Tuvo usted alguna vez algún problema por el correo electrónico? Cómo:

☐ Phishing o Robo de cuentas o sus datos personales

☐ Pago de llamadas de larga distancia no deseadas

- ☐ Virus o Spyware (Software que copia información de su PC y la publica)
- ☐ Deposito de dinero en alguna cuenta como base para un premio que usted recibiría
- ☐ Cambio de su contraseña y robo de su cuenta de Correo Electrónico
- ☐ Ninguno
- ☐ Otro (Por favor especifique)

*6. ¿Cuantos e-mails a la semana usted recibe de personas que no conoce o empresas a las que no se suscribió?

- ☐ Ninguno
- ☐ De 1 a 3
- ☐ De 3 a 5
- ☐ De 5 a 10
- ☐ De 10 a 20
- ☐ Muchos mas que 20

*7. ¿Alguna vez respondió o reenvió un correo que le pedían hacerlo?

- ○ SI ○ NO

*8. ¿Si a usted le llega e-mails de personas o Instituciones que no conoce que hace usted?

- ☐ Reviso los e-mails
- ☐ Reviso los e-mails que en su titulo contiene aspectos que me interesan (Premios, Juegos, Regalos)
- ☐ Reviso los e-mails que vienen de personas con Nombres en Español
- ☐ Reviso los e-mails que tienen archivos adjuntos
- ☐ Elimino todos los e-mails
- ☐ No los reviso, ni los elimino
- ☐ Otro (Por favor especifique)

*9. ¿Cuánto tiempo usted tarda en revisar o eliminar e-mails que vienen de Personas que no conoce o Empresas a las que no se suscribió?

- ☐ No pierdo nada de tiempo no me llegan e-mails no solicitados
- ☐ De 1 a 5 minutos
- ☐ De 5 a 15 minutos
- ☐ De 15 a 30 minutos
- ☐ Mas de 30 minutos

*10. ¿Si le llega correo electrónico no solicitado por favor seleccione el tipo de contenido?

- ☐ Contenido de religión, amistad, amor que prometen cumplir un deseo si enviamos el correo a otros amigos.

- ☐ Información sobre el maltrato de los animales, el hambre en el mundo, escases de agua, etc. Y nos piden que enviemos el e-mail a más amigos para poder apoyar a la lucha contra estas problemáticas Correos como los de Hotmail, que nos piden que enviemos
- ☐ Empresas como Coca Cola, Sony Ericsson, Nokia que nos prometen viajes, Laptops o celulares si nosotros enviamos el correo a la mayor cantidad de personas posibles
- ☐ Correos que nos informan que ganamos un Premio millonario
- ☐ Personas que nos quieren apoyar económicamente como una buena causa antes de su muerte
- ☐ Programas gratuitos, para hacer llamadas mediante Internet, programas para descifrar contraseñas, etc.
- ☐ Personas que están agonizando y necesitan que enviemos el e-mail a mas personas para poderlas ayudar
- ☐ Otro (Por favor especifique)

*11. Si alguna vez le llegó algún e-mail, que le impacto o conmovió y le pedía que lo envíe a más personas ¿lo hizo? ¿A cuánt@s?

- ☐ A la cantidad de personas que me pedía que reenvíe el email
- ☐ A todos mis amigos
- ☐ A toda mi libreta de direcciones
- ☐ No lo envíe
- ☐ Otro (Por favor especifique)

*12. Si alguna vez reenvió un email, que le pedía que lo hiciera, ¿Volvió a

recibir el mismo email pero de otras Personas?

○ Si ○ No ○ Si lo recibí, pero de personas que no conocía

*13. ¿Generalmente que tipo de contenido cree, que es el más común en los emails que no pide que le lleguen?

☐ Publicitarios

☐ Archivos Adjuntos

☐ Cadenas para el cumplimiento de un deseo

☐ Contenido Sexual

☐ Otro (Por favor especifique)

14. Cuando le llega un e-mail que le pide que lo reenvíe, ¿Cómo lo reenvía?

☐ Uso el Botón Reenviar

☐ Uso el Botón Reenviar, pero borro el texto que enviare porque en el mismo hay texto sin sentido

☐ Creo un mensaje nuevo

☐ Nunca reenvío un email, cuando me pide que lo haga

☐ Otro (Por favor especifique)

*15. ¿Cuan Molesto es para usted recibir correo electrónico no solicitado ¿

○ Molesto perdida de tiempo ○ Muy Molesto perdida de Mucho tiempo ○ Tolerable

3. Sección Datos Personales

16. Sexo:

○ Hombre ○ Mujer

17. Edad:

18. Por favor, seleccione su grado de Educación*

○ Estudiante de Colegio ○ Estudiante Universitario ○ Profesional

19 Institución a la que pertenece o trabaja, Escriba:

20. En relación a su familia, cuántas personas más hacen uso del Internet y del Correo Electrónico

Nombre:

CI o Documento equivalente:

Firma:

3.6.1.1 Análisis de resultados

El objetivo de la encuesta realizada fue el de obtener información lo mas valiosa posible, a continuación se analizaran las preguntas que mayor información nos brindan sobre el SPAM en Bolivia.

PREGUNTA 1

Tabla 3.6.1.1.1 Análisis de resultados pregunta 1

Opciones	Cantidad	Porcentaje
Si	139	46%
No	6	2%
Si tengo mas de una cuenta de correo	155	52%
Total	300	100%

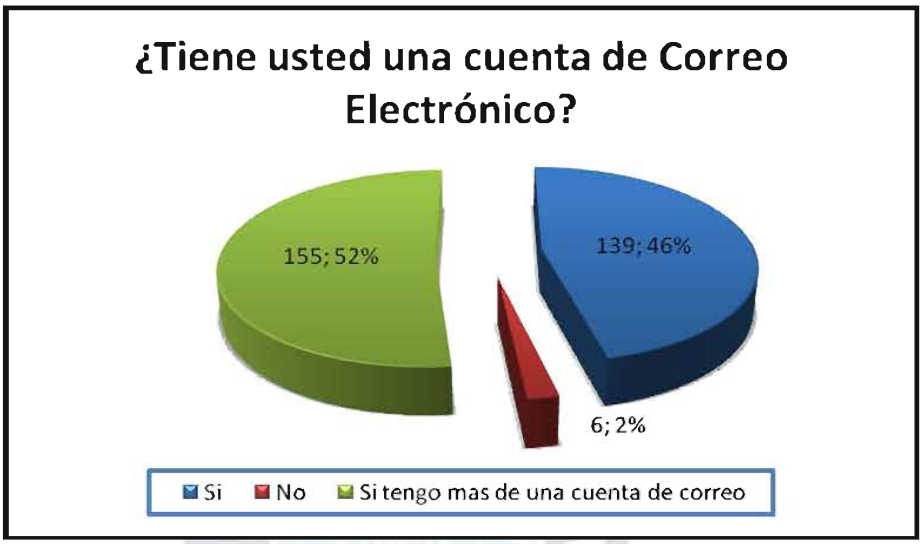

Figura 3.6.1.1.1 Análisis de resultados pregunta 1

Como se puede observar del total de 300 personas encuestadas, 139 tienen una cuenta de correo electrónico correspondiendo esto al 46%, 155 encuestados tienen más de 1 cuenta de correo electrónico, mismo que representa a un 52 % de la muestra y finalmente solo 6 personas no tienen cuenta de correo electrónico equivalen al 2% de la muestra total.

Por otro lado debemos tomar en cuenta que del total encuestado el **98 %** si tiene una o mas cuenta de correo electrónico, confirmando de esta manera que una gran parte de los usuarios de Internet en Bolivia hace uso de este servicio.

Para las siguientes preguntas debemos de tomar en cuenta que la muestra inicial cambio a un tamaño 294 personas, esto porque en cuanto concierne al resto de las preguntas de la encuesta el análisis estará basado en una población que sí tiene correo electrónico.

Población de la muestra por intervalo de edades

PREGUNTA 17

Tabla 3.6.1.1.2 Población de la muestra por intervalo de edades

Opciones	Cantidad	Porcentaje
De 14 a 20 años	51	17,3%
De 21 a 27 años	113	38,4%
De 28 a 34 años	91	31,0%
De 35 a 41 años	25	8,5%
De 42 a 48 años	14	4,8%
Total	294	100%

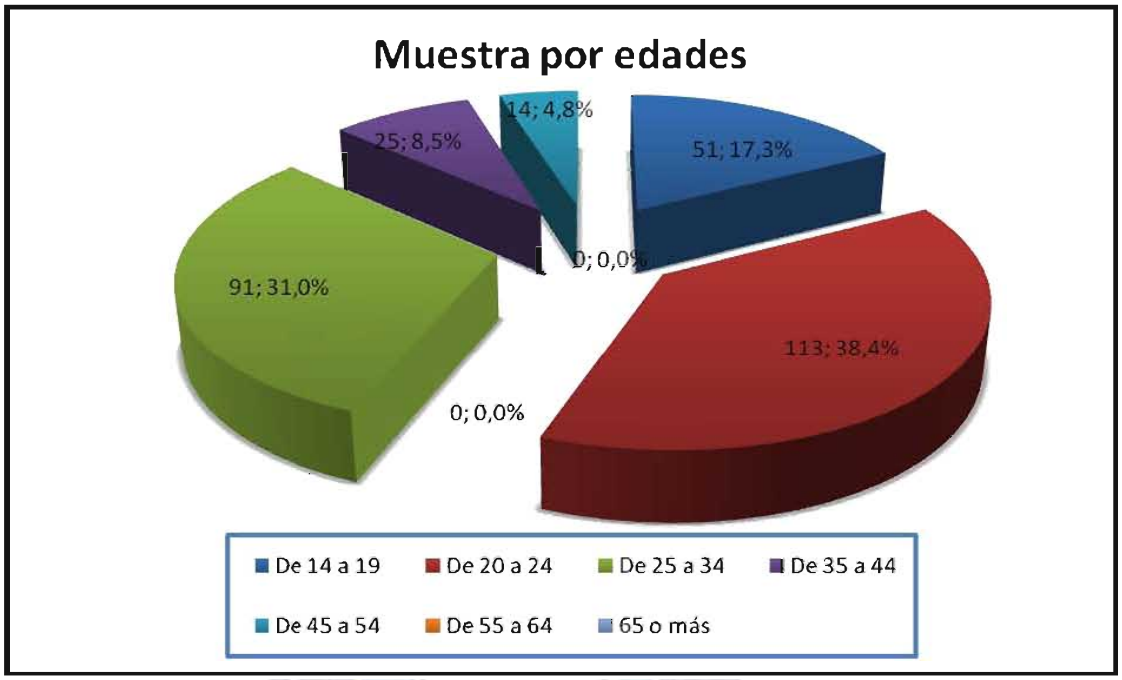

Figura 3.6.1.1.2 Población de la muestra por intervalo de edades Pregunta 17

Podemos notar en la grafica una distribución de usuarios de Internet bolivianos que tiene una cuenta de correo electrónico muy dispersa, tomando en cuenta el tamaño de población con el que se hizo el estudio.

El mayor porcentaje de personas que utilizan el correo electrónico en Internet es del 38% y representa a las personas entre las edades de 21 a 27 años, en segundo lugar están las personas entre los 28 a 34 años con un porcentaje del 31%, en tercer lugar están las personas entre los 14 a 20 años de edad con un 25%.

A continuación analizaremos algunas variables estadísticas que nos brindaran datos acerca de la dispersión de la encuesta realizada; debemos aclarar que para el estudio se hizo uso de la estadística descriptiva en relación a las probabilidades

3.6.1.1.1 Análisis de la representatividad de la muestra

La siguiente tabla muestra los cálculos previos que se deben hacer para poder calcular la desviación estándar y la varianza

Tabla 3.6.1.1.1.3 Análisis de la representatividad de la muestra

	fi	xi		Fi			fi*
De 14 a 20 años	51	17	31	51	14	196	9996
De 21 a 27 años	113	24	31	164	7	49	5537
De 28 a 34 años	91	31	31	306	0	0	0
De 35 a 41 años	25	38	31	546	7	49	1225
De 42 a 48 años	14	45	31	1112	14	196	2744
	294	155					19502

Tamaño de Muestra

n= 294 personas

Media

años

Desviación Estándar

Reemplazando los datos en la formula anterior tenemos la desviación estándar siguiente:

$$\delta = 8{,}14 \text{ años}$$

Con este resultado, se observa que respecto a la media de 31 años se tiene una desviación estándar de 8,14 años es decir la dispersión de la muestra esta en un rango normal ya que el máximo valor con respecto a la media tomando en cuenta su desviación seria de 39,14 años; y esta frecuencia se encuentra en los limites del estudio, así podemos afirmar la representatividad de la muestra.

PREGUNTA 5

Se obtuvieron las siguientes respuestas

Tabla 3.6.1.1.1.4 Problemas con el correo electrónico Pregunta 5

Opciones	Cantidad	Porcentaje
Phishing o Robo de cuentas o sus datos personales	47	16,0%
Pago de llamadas de larga distancia no deseadas	27	9,2%
Virus o Spyware (Software que copia información de su PC y la publica)	112	38,1%
Deposito de dinero en alguna cuenta como base para un premio que usted recibiría	20	6,8%

Cambio de su contraseña y robo de su cuenta de Correo Electrónico	56	19,0%
Ninguno	139	47,3%
Otro (Por favor especifique)	24	8,2%

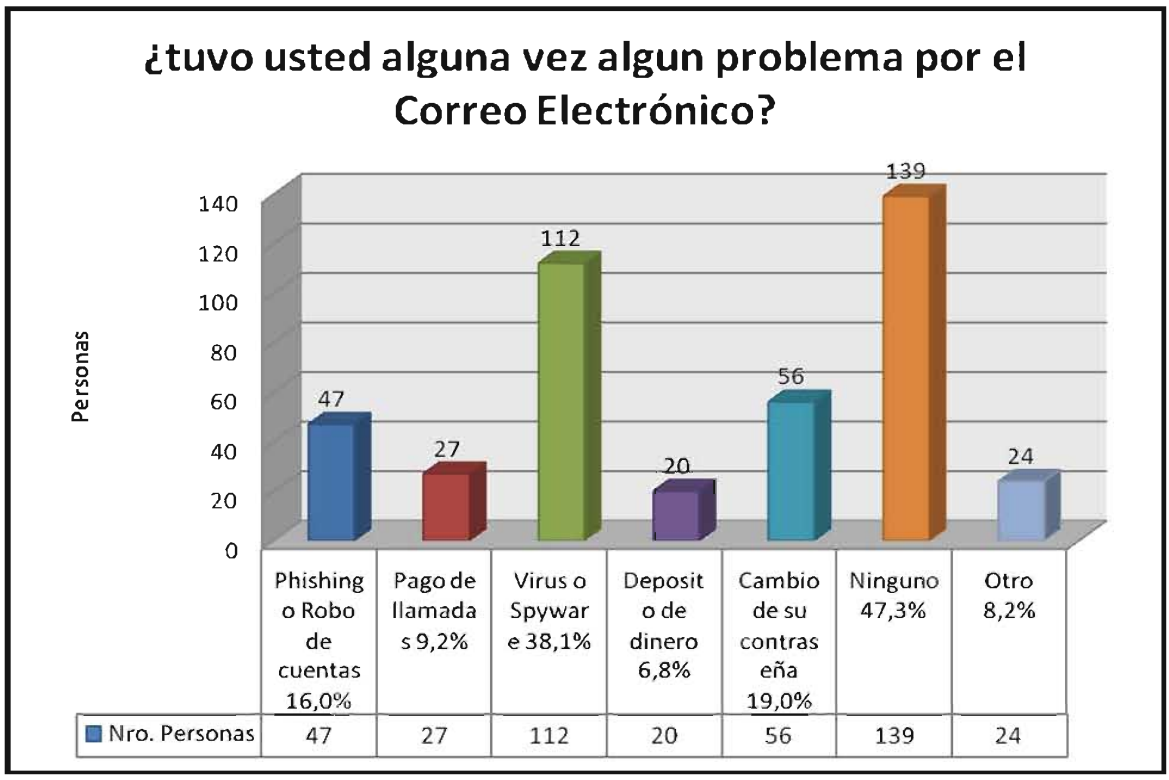

Figura 3.6.1.1 Problemas correo Electronico Pregunta 5

Podemos observar que en relación a la dimensión que tiene el SPAM en las cuentas de los usuarios bolivianos, existe un gran porcentaje que no tuvo ningún problema a consecuencia del correo electrónico no deseado y es de 47,3% de toda la muestra es decir son 139 personas encuestadas que no tuvieron problemas, en segundo lugar esta el spyware o virus informático con un 38,1% equivalente a 112 personas que tuvieron problemas con esta forma de SPAM, un 19 % sufrió de cambio de sus contraseñas o robo de sus cuentas de correo electrónico, un 16% equivalente a 47 personas tuvo problemas de Phishing o robo de datos personales.

A través de estos resultados podemos afirmar que en el caso boliviano, de toda la población que tiene correo electrónico, un 47,3% no tiene problemas a causa del SPAM, pero las cifras que nos hablan del daño que causa el SPAM a los bolivianos es de un 52,3% esto en todas las formas en las que el SPAM puede actuar.

PREGUNTA 11

Los resultados obtenidos los podemos observar en la siguiente grafica:

Tabla 3.6.1.1.1.5 Envío de SPAM por usuarios bolivianos, pregunta 11

Opciones	Cantidad	Porcentaje
A la cantidad de personas que me pedia que reenvie el email	41	13,9%
A todos mis amigos	98	33,3%
A toda mi libreta de direcciones	48	16,3%
No lo envie	135	45,9%
Otro	20	6,8%

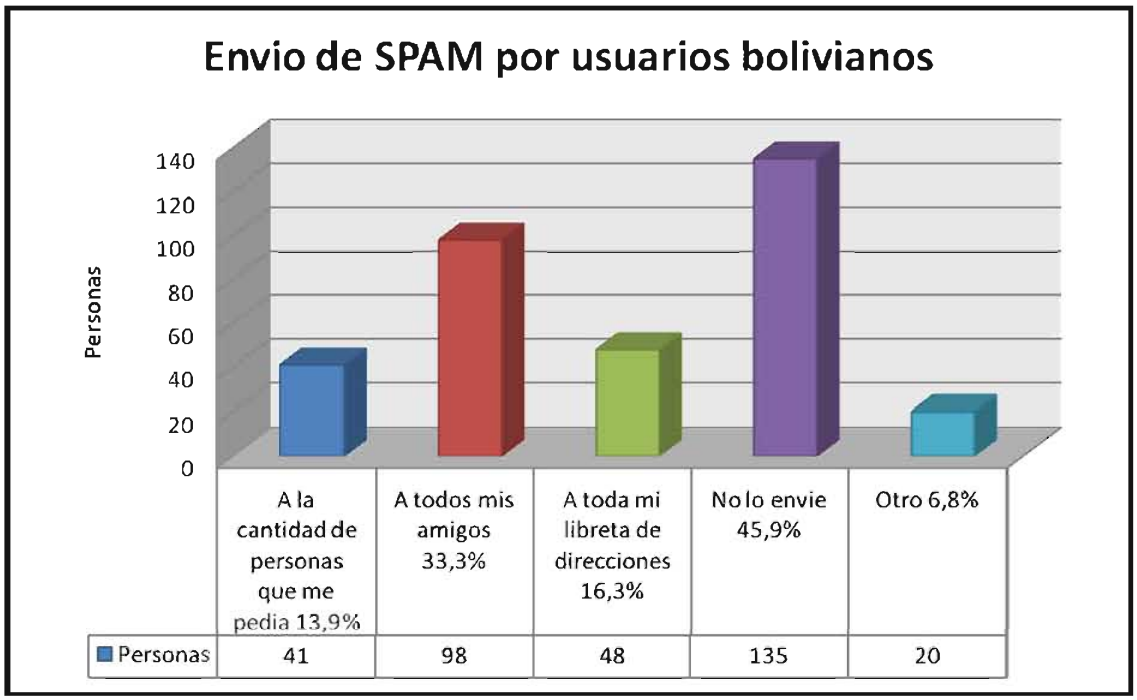

Figura 3.6.1.1.1.5 Envio de SPAM por usuarios bolivianos, pregunta 11

Podemos concluir de esta pregunta que un alto porcentaje tiene conocimiento de los fraudulento que son algunos mensajes de correo electrónico SPAM y este se ve reflejado en un 45,9% de toda la muestra encuestada, un 33,3% de la muestra respondió que son participes del reenvío de SPAM a sus amigos, un 16,3% reenvía el SPAM a toda su libreta de direcciones, un 13,9 % reenvía el SPAM a la cantidad indicada en el e-mail y un 6,8% indica tomar otras opciones como reenviar el mail a sus familiares o reenviar el mail a la lista de correos que vienen adjunta con el e-mail.

En este punto se puede observar que un gran porcentaje de los usuarios de correo electrónico bolivianos son de alguna manera emisores de SPAM i/o cómplices de alguna manera con el Spammer, esto por falta de conocimiento del tipo de información que están enviando, son

De la siguiente interrogante, se obtuvieron datos alarmantes:

Si usted si tuvo un problema con el correo electrónico no deseado (SPAM), este le causo algún perjuicio económico?, detalle por favor un monto económico.

Esta pregunta quedo abierta a los encuestados via internet y pudimos recoger los siguientes datos de 5 personas que contestaron esta pregunta y se detalla a continuación

Tabla 3.6.1.1.1.6 Problemas con el correo electrónico, perjuicio económico

Respuesta	Fecha de entrada
Perdida de espacio	07/11/2007 23:38:04
50	08/11/2007 1:42:11
no	08/11/2007 2:04:20
75	08/11/2007 15:58:21
50	08/11/2007 16:05:35

Se puede notar que existen cantidades económicas en el cuadro de respuesta de la pregunta ya mencionada y el total del costo perdido seria de 175 sin especificación de unidad monetaria, pero por el conocimiento que se tiene de este problema podríamos casi afirmar que no se trata de moneda nacional y se haría más grande el daño.

En otras encuestas y entrevistas realizadas a instituciones la respuesta fue mas precisa respecto a esta pregunta y puntualmente el Jefe de Sistemas de la Cámara Nacional de Comercio Ing. Enrique Chávez respondió que anualmente ellos tienen una perdida a causa del SPAM que asciende a 15000 $ dólares americanos, mismos que representan al tiempo de trabajo remunerado que se utiliza en el control y eliminación del SPAM, de igual manera podemos mencionar que muchas instituciones tienen costos extras para

poder tener bajo control el correo electrónico no deseado, es el caso de el Ministerio de Planificación, la Chancillería, Gobierno municipal de La Paz, que entre otras actividades laborales que su personal realiza están el de el control del SPAM.

PREGUNTA 6

Tabla 3.6.1.1.1.7 Cantidad de SPAM recibido por semana, pregunta 6

Opciones	Cantidad	Porcentaje
Ninguno	8	2,7%
1 a 3	68	23,1%
3 a 5	73	24,8%
5 a 10	68	23,1%
10 a 20	40	13,6%
mas que 20	37	12,6%
Total	294	100,0%

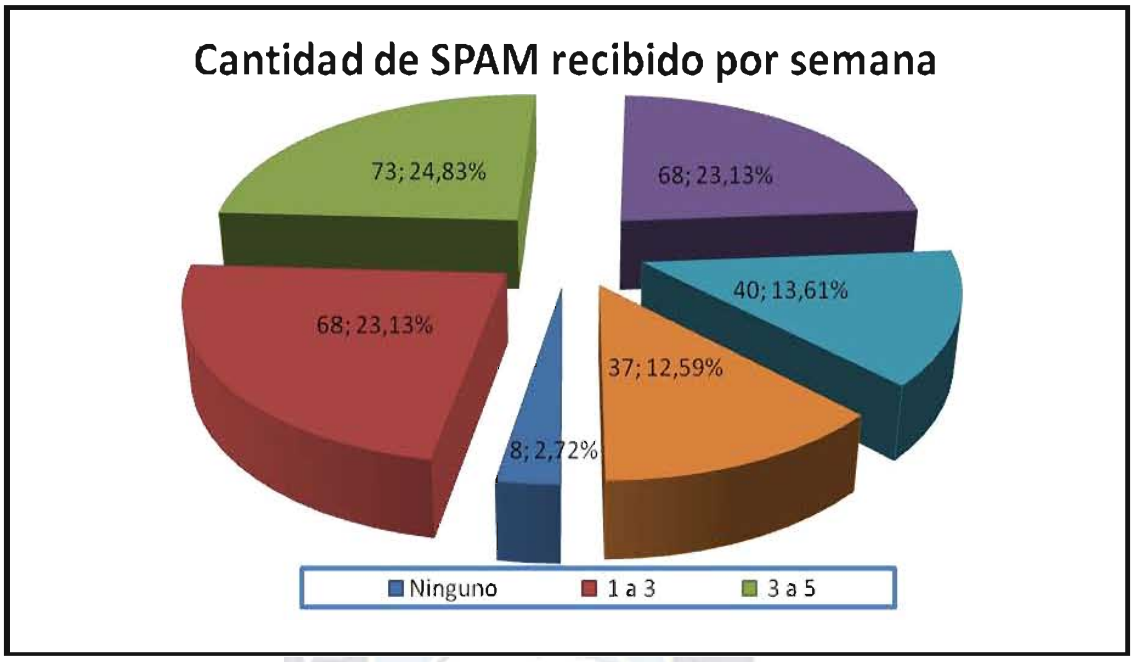

Figura 3.6.1.1.1.7 Cantidad de SPAM recibido por semana, pregunta 6

Podemos notar que sólo una pequeña cantidad de los encuestados no recibe correo no deseado a la semana y es de 8 personas de 294 equivalentes a un 2.7% de toda la muestra, la presunción que se tenia cuando se planteo la hipótesis y se presuponía que existía SPAM en el correo electrónico de usuarios bolivianos de Internet; ahora *podemos corroborar basándonos en ésta encuesta, que evidentemente el 97.3% de los usuarios bolivianos reciben SPAM en su cuenta de correo electrónico.*

PREGUNTA 9

Tabla 3.6.1.1.1.8 Tiempo de eliminación de SPAM, pregunta 9

Opciones	Cantidad	Porcentaje
No pierdo nada de tiempo	19	6,5%
De 1 a 5 minutos	143	48,6%
De 5 a 15 minutos	106	36,1%
De 15 a 30 minutos	20	6,8%
Mas de 30 minutos	6	2,0%
Total	294	100,0%

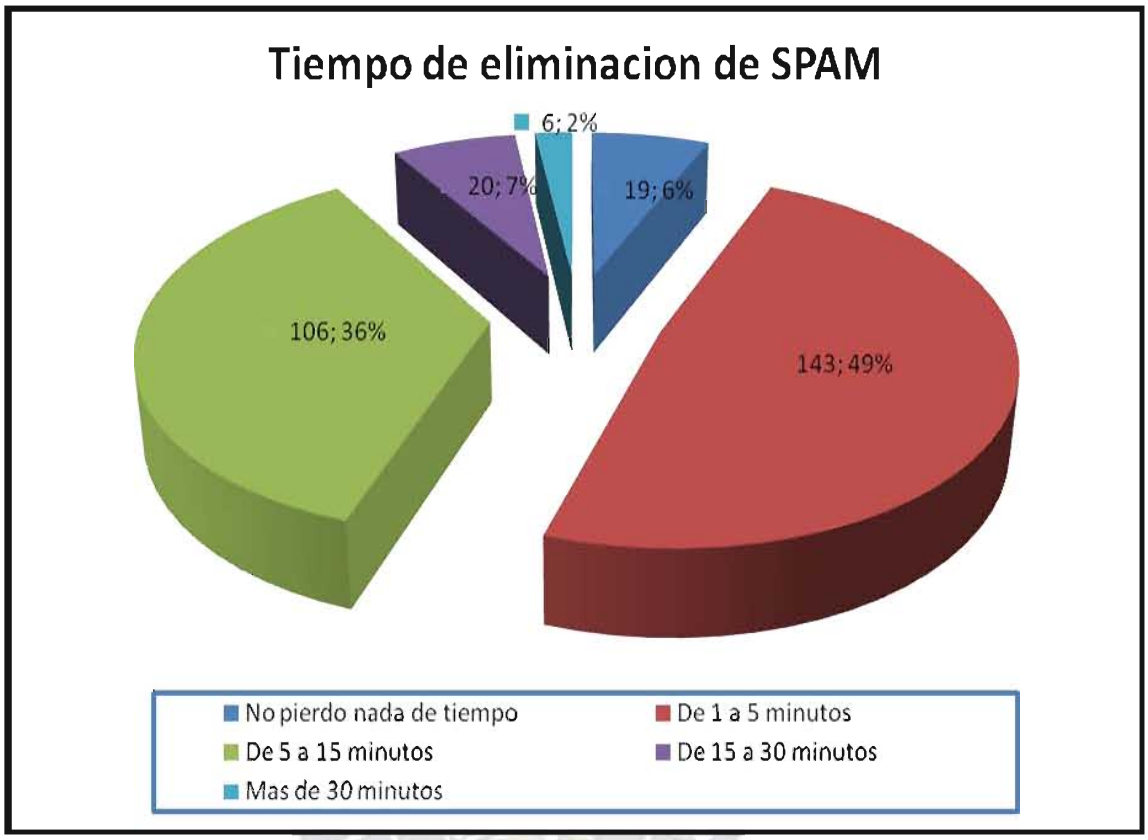

Figura 3.6.1.1.1.8 Tiempo de eliminación de SPAM, pregunta 9

Del total de los 294 encuestados solo 19 no tiene problemas en relación a la eliminación del SPAM o su presencia en las cuentas de correo mencionadas.

La siguiente tabla muestra los cálculos previos que se deben hacer para poder calcular la desviación estándar y la varianza

Tabla 3.6.1.1.1.9 Calculo de la desviación estándar pregunta 9

	fi	xi				fi*
No pierdo nada de tiempo	19	0	13	13	169	3211
De 1 a 5 minutos	143	3	13	10	100	14300
De 5 a 15 minutos	106	10	13	3	9	954
De 15 a 30 minutos	20	22	13	9	81	1620
Mas de 30 minutos	6	30	13	17	289	1734
	294	65				21819

Media Aritmética

Desviación Estándar

Desviación Estándar :

Con este número podemos demostrar que la muestra es representativa en relación a los datos obtenidos acerca de el tiempo que se utiliza en la eliminación del correo basura SPAM, si sumamos a la media la desviación estándar que seria 13+8,61 = 21,61min, podemos decir que este tiempo esta en las frecuencias que se tomaron en cuenta para

este estudio; así como también si le restamos a la media la desviación estándar 13-8,61=4,39min, también este tiempo esta en las frecuencias de la pregunta, por tanto la validez de la muestra en relación al tiempo de eliminación del SPAM se demuestran

Calculo económico a partir de los datos obtenidos

Costos muestra

A continuación se hará el calculo aproximado del costo económico que implica la eliminación del correo basura SPAM para los usuarios estándar, aplicado en un año de uso de correo electrónico por internet

El tiempo medio de eliminación de correo electrónico por persona es de 13 minutos a la semana:

60 min= 2 Bolivianos, es decir :

13 min internet = 45 ctvs de boliviano por persona

Costo Persona= 0,45 Bol/persona

Costo Muestra = n * costo persona

Costo Muestra = 294 personas * 0.45 bol/persona

Costo muestra =132.3 bol/semana

Costo muestra= 529,2 bol/mes; Costo muestra= 6350,4 bol/año

Es decir aproximadamente el costo anual general de las personas de la muestra es de 6350,4 bolivianos por año

Ahora haciendo el análisis en la población general, tomando en cuenta que del 100 % o 300 personas, aproximadamente 294 personas equivalen al 98% de la población total que incurren en este gasto.

Costos población

Según la Super Intendencia de Telecomunicaciones (SITTEL), informe ITU hasta el 2006 se tenia una población aproximada de usuarios de Internet N= 480000

Tomando en cuenta este dato calculemos el costo aproximado del total de la población de usuarios de Internet tomando en cuenta un intervalo de confianza del 95% y un error aproximado del 5, 65%; podemos calcular ahora una nueva población de usuarios de Internet con acceso al correo electrónico N'.

Población Aproximada N' = N * 0,98 = 480000*0.98

N'= 470400 personas

Como la media de costo de gasto de Internet es X= 0,45 bolivianos. por semana en un año que tiene 52 semanas tendremos 23, 4 bolivianos de gasto por persona en la eliminación del correo basura.

Haciendo la multiplicación de esta cantidad por el aproximado de usuarios que incurren en este gasto tenemos:

Costo Anual por eliminación SPAM= 470400 *23,4 Bolivianos

Costo anual por eliminación de SPAM = 11'007,360 Bolivianos

COSTO PERJUICIO SPAM A BOLIVIA APROXIMADAMENTE

11'007,360 Bolivianos por año

Once millones siete mil trescientos sesenta bolivianos

3.6.2 Cuestionarios elaborados en instituciones gubernamentales y no gubernamentales

Otro mecanismo que se contemplo para el estudio del SPAM en Bolivia fue la elaboración de cuestionarios orientados a Jefes de Sistemas, Responsables de Servidores de correo electrónico o algún otro cargo que tenga relación directa con el SPAM. Se

hizo un trabajo de campo en muchas instituciones, obteniendo respuesta de una gran mayoría de ellas, a continuación detallamos la lista de instituciones.

- Caja Nacional de Salud
- Cámara Nacional de Comercio
- Banco Central
- Banco de Crédito
- Banco Económico
- Universidad Real
- Ministerio de Obras Públicas
- Ministerio de Planificación
- Cancillería de la República de Bolivia
- Gobierno Municipal de La Paz
- Empresa Minera San Cristóbal
- Empresa Sinteplast
- Virtual Sistemas Informáticos

A continuación presentamos el cuestionario elaborado, y una generalización de las respuestas obtenidas, ya que este cuestionario era de carácter abierto.

ENCUESTA II

Técnicas Anti SPAM en el correo electrónico en Bolivia

Nombre……

(Opcional):……

CI ……

(Opcional):……..

Empresa o Institución:…… ……

Cargo:…… ……..…

1. **¿Cómo definiría usted el problema del correo electrónico no deseado (SPAM)?**

   De manera general la respuesta a esta pregunta fue que era correo no deseado y dañino

2. **¿En la Empresa o Institución en la que trabaja, ustedes tienen problemas con el Correo Electrónico no deseado (SPAM)?, detalle**

   En esta pregunta podemos señalar que de manera unánime todas las instituciones presentan problemas con el SPAM, se menciona que son atacadas por este tipo de correo no solicitado y también todas tienen filtros y mecanismos anti SPAM

3. **Podría usted detallar el problema mas grande que tuvo su Empresa o Institución en relación al Correo Electrónico no deseado (SPAM)**

   La respuesta a esta pregunta mayoritariamente fue que no se reporta ningún problema pero en algunos casos se respondió que saturan el servidor y en otros que los costos y tiempo de eliminación son elevados

4. **En relación a las perdidas económicas si es que las hubiese, indique la cantidad aproximada de dinero perdido, a consecuencia del SPAM**

   Solo se registro una respuesta con un monto económico y esta era de la Cámara Nacional de Comercio que indicaban que aproximadamente ellos gastaban unos 15000$ anuales por costos de eliminación de SPAM, en otros casos se tendría

que hacer la evaluación de costos por que casi la totalidad de las instituciones entrevistadas tenían filtros anti SPAM pero también tenían personal a cargo de estos filtros

5. **¿Cree usted que es necesario tomar medidas legales ante este problema, o cree que existen otras posibles soluciones?**

   De todas las encuestas realizadas solo 1 respondió que no era necesario porque existían filtros el resto decían que era necesario una ley anti SPAM en Bolivia y algunos mas respondieron que la solución esta en la aplicación de una legislación y el uso filtros anti SPAM

6. **¿Conoce usted de la existencia de alguna norma jurídica que regule este problema?**

   De todas las respuestas solo 2 conocen de algún proyecto de Ley Anti SPAM en Bolivia

7. **¿En lo personal, tuvo usted alguna vez algún problema con el Correo electrónico no deseado (SPAM), que le afecto de alguna forma substancial?, Ejem perdida de dinero, perdida de cuenta, etc. Detalle**

   Ninguno reporto algún problema personal

En el caso de las instituciones se puede concluir que el SPAM es un problema que les afecta diariamente, ellos para su prevención utilizan Software anti SPAM, pero de alguna manera todas estos mecanismos de protección que se utilizan implican un costo, que aun no ha sido concienzudamente asumido.

Para este caso y en relación al costo total obtenido y aproximado de eliminación de SPAM debemos de sumarle el costo obtenido en la Cámara Nacional de Comercio y este es un aproximado de 15000 $ dólares anuales equivalentes a 117000 Bolivianos.

Costo anual por eliminación de SPAM =11'007,360 Bolivianos

Costo Anual reportado por una Institución = 117000 Bolivianos

Costo total de eliminación y control del SPAM en Bolivia aproximadamente

Costo Anual Bolivia = 11'124,360

COSTO PERJUICIO SPAM A BOLIVIA APROXIMADAMENTE

11'124,360 Bolivianos por año

Once millones ciento veinticuatro mil trescientos sesenta bolivianos

Ahora podemos tener una clara visión sobre el problema del SPAM en el Mundo y en Bolivia, según datos obtenidos de la pagina oficial de Microsoft [www.microsoft.com], se informa que del total del correo electrónico que circula a diario solo un 20% es correo electrónico legitimo, demostrando que el restante 80% es correo SPAM. Esta presencia tan alta de SPAM implica también el uso de mecanismos de seguridad y control que a su vez repercuten en un costo elevado, es así que el año 2002 Estados unidos invirtió en la lucha Anti SPAM 8.900 millones de dólares y la Unión Europea 2.500 millones de dólares, esto por que ese año diariamente se distribuían en estas regiones un total de 10 billones de correo basura SPAM.

Para concluir, se demuestra efectivamente que lo presumido en relación al SPAM, y expresado en la variable independiente es totalmente cierto y ha sido comprobado científicamente y superado las expectativas del estudio. Además a más de ser un daño social también representa un gran daño económico a la sociedad boliviana y a los usuarios de Internet.

Habiendo concluido con el análisis de la variable independiente y habiendo verificado su validez, mismo que dio conclusión a la FASE 1, ahora continuaremos con la segunda parte del Marco Practico FASE II de la presente Investigación.

LINEAMIENTOS TÉCNICO/INFORMÁTICOS BASE PARA LA LUCHA ANTI SPAM EN BOLIVIA

3.7 Variable dependiente

Tabla 3.7 Análisis variable dependiente

Lineamientos técnico/informáticos base para la lucha Anti Spam en Bolivia	Dimensión	Indicador	Instrumento

Definición conceptual Lineamientos técnicos base para el desarrollo de legislaciones y comportamientos anti SPAM en Bolivia; basado en estudios técnicos e informáticos, relacionados al tema	Legislación Nacional	Ley Decretos Reglamentos Proyectos de ley	Relevamiento de Información a través de entrevistas y cuestionarios Revisión y análisis de legislación Boliviana y proyectos de ley Análisis comparativo de legislaciones Internacionales Análisis de Documentos Estudio de filtros Anti SPAM existentes
	legislación Internacional	Ley Tratados	
	Código Penal	Artículos	
	Código Civil	Artículos	
	Software Anti SPAM	Filtros	

En esta Fase II se hará un estudio minucioso de las técnicas anti SPAM existentes, así mismo se analizaran cada una de ellas y su presencia en Bolivia, para posteriormente concluir con los lineamientos técnico/informáticos.

Como se vio anteriormente en el marco teórico del presente estudio, el SPAM es un problema social como muchos otros (robo, corrupción, fraude, etc.), pero el SPAM a diferencia de los problemas mencionados tiene características adicionales como:

1. Problema Digital
2. No esta vinculado a le legislación de solo una región del mundo por que es un problema de la Globalización
3. En muchos casos el Agresor es un SOFBOT y no un ser Humano
4. Consecuencias de ataques SPAM son exponenciales a los delitos comunes
5. La no presencia física del atacante hace a este problema mas difícil de sancionar

3.7.1 Problema digital.- Desde el nacimiento del correo electrónico como un nuevo medio de comunicación, junto a el se vinieron presentando algunas desventajas como fueron la validez a los mensajes que uno recibía, el costo por la revisión de correo no deseado siempre implica algún perjuicio económico y además la información que los usuarios brindan a las empresas de correo electrónico en muchos casos puede ser que sea violada y publicada.

3.7.2 Legislación mundial.- En relación a la legislación para el uso regular y licito de el correo electrónico, esta se puede ver presenten en muchos piases del mundo, pero no en su totalidad, mostrando así vacíos legales en regiones en las cuales el SPAM se puede decir que es supuestamente legal, ya que en términos jurídicos lo que no esta sancionado esta permitido. A esto también se tiene que agregar, que en los países donde no se tiene normado el uso del correo electrónico, es ahí donde se presentan pérdidas económico sociales muy importantes.

3.7.3 Agresor sofbot.- En cuanto se refiere al éxito de ésta práctica SPAM, en muchas ocasiones ocurre que el agresor no es un ente físico sino mas bien actúa en todo el entorno lógico ocultándose en la legitimidad de algunos programas, en este tipo de inconvenientes que se presentan es muy difícil descubrir al verdadero agresor, ya que el programa, bot, spyware que fue utilizado para la agresión generalmente no esta en manos de el verdadero creador, sino mas bien este fue obtenido por terceras personas.

3.7.4 Consecuencias exponenciales a delitos comunes.- El uso constante de las nuevas tecnologías como lo es el correo electrónico, ha venido haciendo nuevas innovaciones en las instituciones y empresas, brindando a sus consumidores nuevas y cómodas formas de acceder a los servicios, estas van desde la compra de algún producto vía Internet hasta el pago y cobro de servicios. Es en este punto donde los Spammers haciendo uso de algunas técnicas SPAM buscan puntos débiles entre los consumidores para así obtener algún beneficio propio.

Cuando se utiliza una técnica SPAM, esta presenta una taza de efectividad del 10% de personas afectadas es decir mientras mas masivo sea el SPAM, mas ganancias obtiene el Spammer, asemejando esta realidad a el mundo físico, para que un delito físico tenga el mismo alcance en relación a magnitud de los afectados se necesitarían recursos económicos y humanos muy altos.

3.7.5 No presencia física del atacante.- Existen regiones del mundo donde existe un alto uso de tecnología pero a la par no existe un control acerca de el mal uso que se hace de la misma, son lugares como estos ejemplo Rusia de donde provienen una gran cantidad de SPAM y las técnicas fraudulentas que estos utilizan, es así que en virtud de que alguno de estos delincuentes informáticos sean juzgados culpables no existe el mecanismo para poder dar sanción a estas personas.

Es por las anteriores razones y por que el SPAM es un problema que se prevé estará presente durante toda la era de la Computación y el Internet puesto que trae muchos beneficios a los atacantes y además por que usa el Correo Electrónico como su eje de acción, podemos decir que se deben de tomar múltiples mecanismos de lucha para poder combatir contra esta problemática.

A continuación se propone 4 técnicas anti SPAM, que contribuirán de la lucha contra este delito:

1. ***Educación del usuario boliviano de correo electrónico***
2. ***Software anti SPAM o filtros anti SPAM***
3. ***Legislación anti SPAM***
4. ***Tratados multilaterales con países que también tienen normado este problema.***

3.8 Educación al usuario boliviano de correo electrónico

El SPAM en la actualidad es un problema global, en diferentes ámbitos socio culturales ya se tiene una conciencia acerca de este problema pero en muchos otros aun no, es necesario notar que una medida de control a esta problemática es la concientización de los usuarios de internet, para que estos puedan tomar decisiones acertadas en relación a el uso de su información en Internet y el Correo Electrónico.

En una sociedad como la boliviana donde la presencia del SPAM es real y dañina, pero no se tiene la conciencia e información necesarias para poder luchar contra esta problemática, se deben tomar medidas del tipo educativo e informativo, esto con el objetivo de mejorar la relación de la sociedad y la tecnología, en este caso el Correo electrónico.

Se deben tener definidos perfiles de buenas conductas y comportamientos en el uso del Correo Electrónico y del Internet, que tomen en cuenta características como:

- No publicar la dirección de correo electrónico en páginas Web, o en caso de ser necesario, mostrarla en una imagen.
- No reenviar mensajes que hagan parte de una cadena de correo electrónico.
- De ninguna manera indique información relacionada a su cuenta de banco o tarjeta de crédito sin primero estar completamente seguro de que la pagina Web o el correo electrónico es legítimo.
- Si necesita reenviar un correo que ya contiene alguna dirección en el mensaje, importante asegurarse de borrarlas antes de enviarlo.
- Tener siempre al día las actualizaciones de seguridad del sistema operativo.
- Instalar software de seguridad tal como cortafuegos (firewall), antivirus, anti Spyware, anti SPAM, y mantenerlos siempre activados y actualizados.
- Es conveniente disponer de más de una cuenta de correo. Una para recibir correo serio o aquel que se da a conocer a los conocidos o empresas para que nos envíen correo que resulta "importante". El otro se recomienda utilizar para participar en foros o demás medios. Esta segunda cuenta seguramente será un blanco perfecto para recibir *SPAM*.
- No dejar la dirección de correo electrónico en cualquier foro o formulario si no es absolutamente necesario; si requiere hacerlo, se recomienda escribir la palabra "arroba" en lugar del símbolo @, de este modo se evita que sea capturada la dirección por algún programa generador de *SPAM*. Hay que recordar que ésta es información que puede ser captada y robada por los programas diseñados por los Spammer comúnmente llamados bots.
- No realizar ninguna compra desde un correo no solicitado.

Esto con el fin de hacer que la tecnología sea una herramienta de desarrollo, aprendizaje y difusión de nuevos conocimientos, tecnologías, actividades, comunicaciones, etc., para lograr estos objetivos y tener un impacto positivo es necesario que en sociedades como la boliviana se implanten este tipo de políticas educativas y poder garantizar una efectiva inserción de los bolivianos a las nuevas tecnologías.

3.9 Software anti SPAM o filtros anti SPAM

El software anti SPAM o filtros son mecanismos que sirven de mucho para la lucha contra la problemática del SPAM y el correo electrónico, estos mecanismos, o técnicas Anti SPAM son del tipo preventivo y lógico o software, al igual que cualquier otro tipo de software existen 2 tipos de filtros los de acceso libre y los que tienen un costo, las plataformas en las cuales se pueden aplicar estos filtros son diversas ya que el SPAM al ser un problema del Internet y el correo electrónico afecta a distintos tipos de plataformas que admitan el código HTML como gestor de paginas web, entre estos sistemas tenemos a Windows y Linux;

Los programas que filtran el SPAM utilizan distintas técnicas, entre estas tenemos los del tipo probabilístico o Bayesianos, filtros de listas negras, filtros de contenido.

3.9.1 Filtros bayesianos

El filtrado Bayesiano se basa en el principio de que la mayoría de los sucesos están condicionados y que la probabilidad de que ocurra un suceso en el futuro puede ser deducido de las apariciones previas de ese suceso, esta misma técnica se puede utilizar para clasificar SPAM si algún patrón de texto se encuentra a menudo en el SPAM pero no en el correo legítimo, entonces sería razonable asumir que este correo es probablemente SPAM, los filtros anti SPAM que utilizan esta técnica para depurar el

correo electrónico no deseado utilizan bases de datos donde almacenan las direcciones que probabilísticamente son SPAM

3.9.2 Filtros listas negras

Existen en Internet listas que registran los ordenadores que han sido utilizados muy recientemente para generar SPAM, otras registran ordenadores que tienen el servicio de correo mal configurados y son muy susceptibles de ser emisoras de SPAM, el filtro por lista negra averigua, mirando en las cabeceras de los mensajes, quién es el ordenador que ha emitido el mensaje. Si este ordenador está registrado en alguna de las listas negras, lo marca como "posible SPAM"

3.9.3 Filtros por contenido

Los filtros anti SPAM por contenido es un filtro que estudia el contenido de los mensajes, consiste en que se tiene una lista de las cabeceras de mensaje que ya fueron identificadas como SPAM entre las mas comunes “Viagra”, “Millones”, etc., y si algún mensaje se recepciona con alguna de las palabras ya definidas como posibles SPAM el mensaje se bloquea

3.9.4 Software anti Spam a nivel del servidor

Todos los mensajes de correo electrónico llegan a un servidor de correo electrónico, es en este punto el mejor lugar para poder interceptar el SPAM existen muchos programas anti SPAM para servidores (tanto Linux como Windows), que se pueden encontrar en diversos sitios en la red, algunos de ellos son:

DNS Blocklists

Este tipo de filtros utilizan bases de datos que contienen direcciones IP o nombres de Dominio de sitios de los cuales no se desea recibir correos, en estas se encuentran enumeradas Opens Relays, fuentes conocidas de SPAM, IP's que son identificadas y relacionadas con Spammers.
Este tipo de filtros se actualiza en relación a las nuevas IP's identificadas como emisoras de SPAM, generalmente estas IP's son de países donde el SPAM es legal.

SpamAssassin

Es un filtro inteligente que usa diferentes pruebas para identificar el SPAM, estas pruebas son aplicadas a la cabecera de los correos y al contenido para clasificarlo usando métodos estadísticos avanzados. Adicionalmente, tiene una arquitectura modular que permite unirse a otras arquitecturas rápidamente.
Entre la información que este filtro utiliza, se basa en la actualización vía Internet de los mensajes SPAM y sus cabeceras, este filtro al identificar una nueva cabecera de mensaje lo filtra y no lo remite, en relación a el contenido filtra haciendo una comparación de los contenidos mas actuales de los SPAM y si este es parecido al nuevo mensajes lo filtra.
Debemos tomar en cuenta que si nosotros enviamos un email con alguna cabecera parecida a un SPAM, este será filtrado; además, crea automáticamente listas blancas y listas negras. Usa DNS Blocklists y también bases de datos de identificación de SPAM tales como DCC, Pyzor y Razor2.

3.9.5 Software anti Spam a nivel usuario

Debemos aclarar que estos filtros Anti SPAM funcionan solamente para el correo electrónico tipo POP y no así para el correo electrónico tipo WEB, es por esto que muchas compañías que proveen este servicio utilizan sus propios filtros anti SPAM, de manera general los sistemas antivirus actuales en sus versiones profesionales incluyen software anti SPAM para computadoras personales pero con costo

Aquí detallamos algunos de los filtros anti SPAM más conocidos y utilizados

- AntiSPAM 1.0 (*http://www.xde.net/antiSPAM*)

Programa anti-SPAM que cuenta con el aliciente de que su base de datos sobre Spammers se va actualizando periódicamente a través de Internet.

- CYBERSitter Anti-SPAM 1.0 (*http://www.solidoak.com/antiSPAMpg.htm*)

Permite seleccionar el E-mail que queremos recibir por palabras clave, dominio, dominios inexistentes y otros filtros.

- Deadletter 1.12 (*http://www.deadletter.com*)

Se trata de un módulo anti-Spammer específico para Eudora Pro y Light 3.05 o superior. Lleva la consabida lista de Spammers y otras opciones de filtrado.

- E-Mail Remover 2.4 (*http://home.pacific.net.sg/~thantom/eremove.htm*)

Permite ver las cabeceras de los mensajes en el servidor antes de descargarlos, permitiendo su eliminación. Puede que no sea el mejor, pero tiene el aliciente de que es Freeware (gratuito).

- MailShield 1.0 (*http://www.mailshield.com*)

Una auténtica barrera que filtra el SPAM y el mail-bombing en el servidor antes de que lo recibamos.

- MailTalkX 2.3 (*http://www.softbytelabs.com/MailTalkX*)

Además de ser una herramienta anti-SPAM efectiva permite monitorizar nuestro E-mail con todo tipo de filtros y avisos. Permite el control total sobre todas las cuentas de correo que queramos. Está considerado como uno de los mejores programas anti-SPAM.

- SPAM Exterminator 3.2f (*http://www.unisyn.com/SPAMex/SPAMEx.htm*)

Permite ver las cabeceras de los mensajes en el servidor y eliminar el SPAM. Incluye una lista de Spammers, filtros diversos. Incluso permite responder de forma automática a los Spammers diciendo que no nos gusta su conducta (una mala idea, como ya sabemos).

- SPAM Hater 2.08 (*http://www.cix.co.uk/~net-services/SPAM/SPAM_hater.htm*)

Programa Freeware que se integra en nuestro cliente de correo o lector de news para responder al SPAM. Responde a postmasters de los dominios con Spammers que no nos gustan sus mensajes. La idea es que algunos dominios no permiten la realización de SPAM y los darán de baja. Sinceramente no creo que esto sirva de mucho, pero es una forma de ejercer nuestro derecho al pataleo de forma automática.

- SPAMBuster 1.61 (*http://www.contactplus.com*)

Se trata de una de los programas más conocidos de este género. Funciona con el tradicional sistema de filtros y actualizaciones de firmas, se debe mencionar además que en la actualidad la mayoría de los programas antivirus traen con ellos la funcionalidad anti SPAM para que la podamos instalar.

3.9.6 Firewalls anti SPAM

También existen otro tipo de filtros del orden fisico o también conocidos como dispositivos Firewall, que entre sus cualidades están las de no permitir la llegada de SPAM a las computadoras protegías bajo un determinado perfil entre este tipo de Firewall Físicos podemos nombrar los siguientes:

- Symantec 8220
- Mail-SeCure 5000
- Panda GateDefender Performa
- SeCure SoHo
- Cisco ASA 5500

3.10 Legislación anti SPAM

En relación a la parte que rige y sanciona el uso inadecuado del correo electrónico como es el SPAM, muchos países del mundo, ya cuentan con medidas legales que combaten estos actos ilícitos, ya que no es suficiente una medida de prevención y protección lógica Anti SPAM (filtros anti SPAM). En este sentido, se hizo un relevamiento sobre algunos marcos legales existentes a nivel mundial; como los existentes en los países signatarios de la Unión Europea, Estados Unidos, México; respecto a nuestro continente se tomo en cuenta a algunos países limítrofes de Bolivia que tienen una ley anti SPAM u otro mecanismo parecido; estos países son Perú, Argentina, Chile. A continuación se presenta un cuadro comparativo tomando en cuenta el marco jurídico, los artículos clave y la sanción que se tienen sobre este problema.

UNIVERSITAS MAJOR PACENSIS DIVI ANDREÆ

Tabla 3.10 Legislación anti SPAM Mundo

Pais	Marco Jurídico Ley	Artículos Objeto	Per
España	Ley 13758 de servicios de la sociedad de la información y de comercio electrónico	**Artículo 21** Queda prohibido el envío de comunicaciones publicitarias o promocionales por correo electrónico u otro medio de comunicación electrónica	a) Por la comis muy graves, mul 600.000 euros. b) Por la comis graves, multa de euros. c) Por la comis leves, multa de ha
Estados Unidos	S. 1293 CAN SPAM (Se muestra toda la ley Can SPAM americana en el Anexo I)	**SEC. 2.** Prohibition against predatory and abusive commercial e-mail. (a) offense- (1) in general	PENALTIES- Th offense under sub (c) FORFEITUR convicted of an section shall fo States such perso REMEDIES
Mexico	Ley federal de protección al consumidor	**ARTÍCULO 17.-** En la publicidad que se envíe a los consumidores se deberá indicar el nombre, domicilio, teléfono y, en su defecto, la dirección electrónica del proveedor; de la empresa que, en su caso, envíe la publicidad a nombre del proveedor, y de la Procuraduría.	Art.127 Toda infi los articulos, 7, 42, 43, 44, 75, Quater, 90, 91, 9 sancionados con 993,207.03$
Chile	Ley 19.496, Protección de los derechos de los consumidores	**Artículo 28 B.-** Toda comunicación promocional o LEY 19955 publicitaria enviada por correo electrónico deberá	Los proveedores proporcionar al S Consumidor l

		indicar la materia o asunto sobre el que versa, la identidad del remitente y contener una dirección válida a la que el destinatario.	antecedentes que por escrito la injustificada en antecedentes sancionada con unidades tributari
Argentina	Ley 25.326, Protección de datos personales (Se muestra esta ley de protección de datos personales y SPAM en el Anexo II)	**ARTICULO 27.-** Podrán recopilarse, tratarse y cederse datos con fines de publicidad sin consentimiento de su titular, cuando estén destinados a la formación de perfiles determinados	ARTICULO 31. 1. Las sancio establecidas en Ley N° 25.326 s responsables o u registros, bases públicos, y privad Destinados a d hubieren inscript correspondiente.
Peru	Ley 28493, Regula el uso del correo electrónico comercial no solicitado SPAM (La ley peruana anti SPAM se encuentra de manera completa en el anexo III)	**Artículo 1°.Objeto de la Ley** La presente Ley regula el envío de comunicaciones comerciales publicitarias o promocionales no solicitadas, realizadas por correo electrónico, Artículo 6°.Correo electrónico comercial no solicitado considerado ilegal	Artículo 8°.Dere pecuniaria el electrónico ilegal la vía del proces la persona que compensación, uno por ciento Impositiva Tribut los mensajes de transmitidos
Bolivia	NO existe	NO existe	NO

Como se puede observar en la legislación española, se acata los mandatos de la directiva creada para el efecto, es así que todos los países asociados en la Unión Europea apoyan a la lucha contra el SPAM, seguidamente se detalla las organizaciones existentes, el país donde tienen funcionamiento y sus páginas Web

Tabla 3.10.1 Organizaciones del Mundo que luchan contra el SPAM

País	**Organización**	**Pagina Web**
Austria	Austrian Data Protection Authority	http://www.dsk.gv.at/
Bélgica	Privacy Protection Commission	http://www.privacycommission.be/
Chipre	Office of the Commissioner for Personal Data Protection.	http://www.dataprotection.gov.cy/
Dinamarca	Danish Consumer Ombudsman	http://www.forbrug.dk/english/dco/
Eslovaquia	Slovak Personal Data Protection	http://www.dataprotection.gov.sk/
Estonia	Estonian Data Protection Inspectorate	http://www.dp.gov.ee/
Finlandia	Data Protection Ombudsman	http://www.tietosuoja.fi/
Francia	Commission Nationale de l'informatique et des Libertés (CNIL)	http://www.cnil.fr/
Grecia	Hellenic Data Protection Authoritie	http://www.dpa.gr/
Hungría	Data Protection and Freedom of Information Commissioner	http://abiweb.obh.hu/abi/

	of Hungary	
Irlanda	Data Protection Commissioner	http://www.dataprivacy.ie/
Italia	Garante per la protezione dei dati personali	http://www.garanteprivacy.it/
Letonia	Datu valsts inspekcijas	http://www.dvi.gov.lv/
Lituania	Valstybinė duomenu apsaugos inspekcija	http://www.ada.lt/
Luxemburgo	Commission nationale pour la protection des données	http://www.cnpd.lu/fr/
Malta	Data Protection Commissioner	http://www.dataprotection.gov.mt/
Paises Bajos	College bescherming persoonsgegevens	http://www.cbpweb.nl/
Polonia	Inspector General for the Protection of Personal Data	http://www.giodo.gov.pl/168/j/en/
Portugal	Comissão Nacional de Protecção de Dados	http://www.cnpd.pt/
República Checa	Office for Personal Data Protection	http://www.cnpd.pt/
Suecia	Swedish Data Inspection Board	http://www.datainspektionen.se/

3.11 Legislación boliviana

Leyes y decretos, el marco jurídico nacional que norma el uso correcto de la tecnología y sus posibles sanciones, esta constituido por leyes, decretos y reglamentos, para el

presente estudio se hizo un relevamiento de todos estos datos, a continuación se detallara toda la información legal recolectada en relación al área tecnológica en general y el uso correo electrónico en particular, a lo largo de la historia de Bolivia

Tabla 3.11 Leyes y decretos Bolivia

Año	Marco Legal	Objeto Jurídico
2004	**Decreto Supremo 27329**	Procurar la transparencia y acceso a La información gubernamental
2000	**Decreto Supremo 25950**.	Modificaciones al Marco Jurídico Regulatorio del Sector de Telecomunicaciones
2000	**Decreto Supremo 26005**	Plan para la apertura del mercado en el sector de telecomunicaciones
2000	**Decreto Supremo 26011**	Reglamento De Interconexión
1998	**Reglamento para los Servicios Móviles Satelitales** No. 57/98.	
1997	**Decreto supremo No. 24778**	Reglamento a la Ley de Telecomunicaciones
1997	**Decreto Supremo No.24505**.	Que la ley 1600 de 28 de octubre de 1,994 ha creado el Sistema de Regulación Sectorial, SIRESE, cuyo articulo 27 determina su reglamentación por el Poder Ejecutivo, en concordancia con el articulo 96 numeral 1 de la Constitución Política del Estado que reconoce al Presidente de la República la atribución de ejecutar y hacer cumplir las

		leyes, expidiendo los decretos y órdenes convenientes, sin definir privativamente derechos, alterar los definidos por ley ni contrariar sus disposiciones
1995	**Decreto Supremo No. 24132**	Reglamento a la ley de telecomunicaciones
1995	**Ley No. 1632**	Ley de telecomunicaciones
1994	**Decreto Supremo No. 24504**	Reglamento a la ley SIRESE
1994	**Ley No. 1600**	Del sistema de regulación sectorial – SIRESE

Como se podrá observar en el cuadro superior, Bolivia carece de un Marco Jurídico que regule la presencia de los correos electrónicos no solicitados abusivos y depredadores (SPAM), en las cuentas de correo electrónico de los ciudadanos bolivian@s.

Sin embargo ya existen algunos esfuerzos institucionales realizados que significan un gran avance como iniciativas de lucha contra este problema. A continuación se detalla toda la información que se pudo recolectar de estas iniciativas.

3.11.1 Legislation and SPAM control in Bolivia (este proyecto de ley esta disponible en la siguiente dirección electrónica [www.itu.int/osg/csd/spam/presentations/URQUIDI_Session%205.pdf])

8 de julio de 2004, Ponencia en la International Telecomunication Union (ITU), en esta organización de la cual Bolivia es miembro se presento a nombre de la Superintendencia de Telecomunicaciones (SITTEL), la ponencia sobre la situación legislativa que se tenia en ese tiempo en relación al Correo electrónico, además de otros datos. El titulo de la ponencia fue LEGISLATION AND SPAM CONTROL IN BOLIVIA y fue presentada a

por la **Dra. Gabriela Urquidi Morales Directora Legal de SITTEL BOLIVIA.** Podemos destacar de esta ponencia los siguientes aspectos: "Traducción del Ingles" Situación Actual (2004)

3.11.2 Autorregulación y protección de datos personales

Los días 3 al 5 de mayo de 2006, se tuvo la reunión de un grupo de trabajo en la ciudad de Santa Cruz, con el objetivo de hacer un análisis de la legislación que rige el control de la privacidad de los datos personales presente en los países Iberoamericanos, entre estos Bolivia; para dicho estudio se tomo en cuenta las normas jurídicas existentes en el país y las de otros países de la región, puesto que este estudio era a nivel regional y se tomaron en cuenta los siguientes puntos.

SUMARIO: I. ANTECEDENTES; II. AUTORREGULACIÓN Y PROTECCIÓN DE DATOS PERSONALES: 1. Referencias normativas; 2. Alcance, efectividad y contenido de los instrumentos de autorregulación; III. RECOMENDACIONES

3.11.3 Proyecto de Ley, enero de 2004

Ley de documentos, firmas y comercio electrónica (Este proyecto de ley se encuentra en el Anexo IV de manera completa)

Se ha remitido a la Comisión de Industria, Comercio, Turismo, Ciencia y Tecnología, el Proyecto de Ley 037/05-06: "**COMUNICACIÓN ELECTRONICA DE DATOS Y COMERCIO ELECTRONICO"**, cuya iniciativa parlamentaria corresponde al Senador Oscar Ortiz Antelo.

En fecha Enero 2004, recogiendo una serie de trabajos previos, a indicativa de la Agencia para el Desarrollo de la Sociedad de la Información en Bolivia (ADSIB), bajo el financiamiento del programa BID ATN SF 7692 BO, se presentó un Anteproyecto de

Ley de Comunicación Electrónica de Datos, Firmas Electrónicas y Comercio Electrónico, Proyecto de Ley que al socializarlo y al contar con la valiosa participación de diversos sectores, sufrió una serie de modificaciones inclusiones y adecuaciones, finalmente en Noviembre del 2005 el grupo encargado de dicho proyecto compuesto por la ADSIB, el Viceministro de Justicia, el Viceministro de Electricidad Energías Alternativas y Telecomunicaciones y el Banco Central de Bolivia, hicieron llegar el Proyecto a la Cámara Alta para ser introducido al debate parlamentario.

Este Proyecto de Ley al haber sufrido una serie de modificaciones (56 versiones), fue estudiado por esta Comisión en la Legislatura precedente, en ese entonces a la cabeza del ex Senador Huascar Aguilar, quien luego de convocar a los sectores involucrados en el Proyecto de Ley, (Enero 6 del 2006), sugirió una nueva revisión global al documento y se hizo la recomendación colectiva de que le den consistencia pues a causa de las múltiples modificaciones habían incongruencias contenidas en el propio documento final.

ADSIB al contar con un convenio con la CAINCO, a objeto de impulsar esta Ley, solicito a esta entidad que al ser la encargada de la ejecución de un crédito FOMIN BID, se haga cargo de dicho trabajo, en el marco de dicho financiamiento, situación que se hizo posible mediante la contratación de un consultor internacional, quien estuvo encargado justamente de cumplir con las recomendaciones antes mencionadas.

El Título V "Delitos Informáticos", con su Capítulo Único que en su momento se consideró excluirlo por la complejidad de reformar el Código Penal, pero excluirlo podía dar lugar a vacíos legales en relación a este tema y la oportunidad de regularlos en esta Ley es única, razón por la cual el Título V introduce modificaciones al Código Penal en sus once numerales. Asimismo, señalar que se contó con la participación de un experto en peritaje informático y delitos informáticos, quien hizo conocer sus observaciones y sugerencias que fueron consideradas en la redacción de este Título.

Este proyecto de ley a diferencia de los anteriores documentos estudiados, se aproxima mucho al espíritu que tiene la presente investigación, pero por otro lado debemos resaltar que por el poco conocimiento que se tiene acerca de esta área de la informática (Delitos Informáticos), no se tiene un desarrollo total de las especificaciones técnicas relacionadas a la sanción de actividades ilícitas como es el SPAM. También debemos de observar que este proyecto de ley tiene artículos parecidos a algunos de la ley Norteamericana anti SPAM (CAN SPAM) que en esencia esta dirigida a una sociedad mas tecnológica que la nuestra, con muchos mas años de vida digital y su propósito es castigar actividades totalmente fraudulentas, es en este aspecto que aun se tiene que hacer mas énfasis por que en un país donde se llevan campañas para cerrar la Brecha Digital y el uso de las TIC's, la sociedad Boliviana aun esta en periodo de aprendizaje e información y por tanto se deben tomar en cuenta la realidad socio cultural Boliviana para poder sancionar una ley anti SPAM.

Otra punto importante que se debe observar, es que el SPAM, no es un problema netamente nacional, sino mas bien un delito global, en la mayoría de los casos los Spammers no se encuentran el la región donde cometen el delito, mas al contrario operan de forma remota y a través de terceros, para solucionar este tipo de inconvenientes se deben recurrir a tratados internacionales que coadyuven en la lucha contra este delito. Estos aspectos se deben tomaran en cuenta para los lineamentos técnicos de un futuro proyecto de ley Anti SPAM en Bolivia

Para la parte legal se hizo contacto con el Doctor Ariel Agramont Loza, Director de la **DERECHOTECA BOLIVIANA**, y a partir de este contacto, se puede expresar que la información que el brindo para este estudio fue valiosa; en cuanto a la corroboración de la Investigación, ya que lo investigado referente a la legislación o proyectos de

legislación existentes en el país, son todos los datos que este profesional nos brindo, Hasta el día viernes 09 de Noviembre de 2007 no se tiene ningún proyecto de ley Anti SPAM en ninguna de las instancias ejecutivas correspondientes, vale mencionar que se hizo una investigación vía Internet y revisión de documentos, y una Investigación de campo en las siguientes instancias de gobierno y son:

- Cámara de Diputados
- Senado Nacional
- Vicepresidencia
- Biblioteca del congreso

*Debemos exponer además que si hay un anteproyecto de ley en el Senado de la República pero este ya tiene mas de 66 modificaciones, el nombre del proyecto es el de "**LEY DE DOCUMENTOS, FIRMAS Y COMERCIO ELECTRÓNICO**", no se pudo tener acceso a mas información referente al mismo, pero según reportes de la pagina Web de la Agencia para el desarrollo de la sociedad de la Información en Bolivia, se tubo acceso a la ultima versión de este proyecto, versión 5 de enero de 2007, pudiendo asegurar en relación a la versión a la que se tuvo acceso que de ninguna manera este proyecto de ley tiene como su contenido alguna legislación sobre el SPAM, tómese en cuenta que desde enero de 2004 hasta la fecha aun no se promulgo nada.*

3.12 Mecanismos de control legal existentes en Bolivia

Se hizo una recopilación y análisis de la información contenida en la Constitución Política del Estado, códigos y normas existentes

PRIMERO.- En la constitución Política del Estado Boliviano no existe norma alguna que regule este delito de forma clara o especifica, sin embargo se puede tomar como un

articulo valido para el presente estudio el articulo 23 Habeas Data (garantías constitucionales)

SEGUNDO.- En el código civil boliviano, no existe ninguna norma jurídica respecto a esta problemática

TERCERO.- en el Código Penal Boliviano ya se hace referencia a algún tipo de control sobre alguna forma derivada del SPAM.

Delitos informáticos

Art. 363bis. El que con la intención de obtener un beneficio indebido para sí o un tercero, manipule un procesamiento o transferencia de datos informáticos que conduzca a un resultado incorrecto o evite un proceso tal cuyo resultado habría sido correcto, ocasionando de esta manera una transferencia patrimonial en perjuicio de tercero, será sancionado con reclusión de uno a cinco años y con multa de sesenta a doscientos días. Alteración, Acceso y Uso Indebido de Datos Informáticos

Art. 363. El que sin estar autorizado se apodere, acceda, utilice, modifique, suprima o inutilice, datos almacenados en una computadora o en cualquier soporte informático, ocasionando perjuicio al titular de la información, será sancionado con prestación de trabajo hasta un año o multa hasta doscientos días.

SITTEL.- En la Superintendencia de Telecomunicaciones no se tiene legislación alguna o algún reglamento que pueda ayudar en la lucha contra esta problemática.

Se identifico que si existe una lista de malos comportamientos informáticos como el SPAM y se toman algunas medidas que para el caso, que no solucionan en nada el problema

Toda la legislación aplicable en relación a las acciones abusivas se pueden interpretar en el articulo 306 del Reglamento de la Ley de Telecomunicaciones, que en caso de peligro para la red, inminente Actualmente, el operador de una red pública podrá

solicitar, en virtud de un procedimiento acelerado, la autorización de la Superintendencia de Telecomunicaciones para cortar el servicio de los usuarios en lo causa... "

3.13 Tratados internacionales con países que también tienen normado este problema

Para que una política nacional reguladora del SPAM tenga buenos resultados, es necesario establecer tratados y acuerdos multilaterales con Países y organizaciones que también luchan contra esta problemática, ya que el SPAM al ser un problema global; una política nacional no seria suficiente.

En este marco que también se tiene que demostrar la presencia de un país ante un problema de la globalización y el Internet.
Entre las organizaciones países que luchan contra el SPAM en el mundo podemos destacar:

- Organización de las Naciones Unidas N.N. U.U.
- Organización de los Estados Americanos O.E.A
- Canada
- Estados Unidos
- Mexico
- Unión Europea U.E.
- Austria
- Bélgica
- Chipre

- Dinamarca
- Eslovaquia
- Estonia
- Finlândia
- Inglaterra
- Francia
- Grecia
- Hungría
- Irlanda
- Italia
- Letonia
- Lituania
- Luxemburgo
- Malta
- Paises Bajos
- Polonia
- Portugal
- República Checa
- Suecia
- Sud America
- Argentina
- Chile
- Uruguay
- Peru

- Coalition Against Unsolicited Commercial Email (*http://www.cauce.org*)
- Fight SPAM on the Internet! (*http://SPAM.abuse.net/*)
- ChooseYourMail (*http://www.chooseyourmail.com*)
- Mail-abuse (*http://www.mail-abuse.com/an_sec3rdparty.html*)
- International Telecommunication Union (http://www.itu.int/)

Luego de haber estudiado las técnicas que se presentaron en este estudio, podemos concluir que en relación a la lucha contra el SPAM en Bolivia, no se esta haciendo casi nada. Debemos enfatizar que algunas técnicas no son muy difíciles de aplicar pero algunas otras que tienen mayor impacto en esta lucha como son la legislación y los tratados Anti SPAM no se tiene nada aun avanzado.

Al concluir el estudio de la segunda variable y haber evaluado la posible solución que se propuso a esta problemática a través de lineamientos técnico informáticos para la lucha anti SPAM en Bolivia, se concluye que lo expresado en la variable dependiente también se demuestra por todo el estudio realizado que así lo respalda y reflejan la necesidad de basarse en normas jurídicas, Software Anti SPAM, tratados internacionales y una buena política de información y educación de lucha contra el SPAM.

Para finalizar debemos concluir que al haberse demostrado las variables independiente Estudio técnico sobre la presencia SPAM en Bolivia (x) y la variable dependiente Lineamientos técnico informáticos base de la lucha Anti Spam en Bolivia (y); podemos concluir que

$X \rightarrow Y$ *donde:* X *= Verdad y* Y *= Verdad*

$X \rightarrow Y$ *= Verdad*

Con lo que demostramos satisfactoriamente la corroboración de la hipótesis planteada en este estudio

4. CONCLUSIONES Y RECOMENDACIONES

Resumen

En este capitulo se establecen las conclusiones generales de acuerdo a la investigación realizada y según los resultados obtenidos, también se mencionan los trabajos futuros posibles a realizarse y se dan los lineamientos técnico informáticos además de otros que de gran manera solucionaran el problema del SPAM en Bolivia.

4.1 Conclusiones generales

No existe un conocimiento de la verdadera dimensión del problema del SPAM en Bolivia, es por esto que aun en el Estado y en otras instituciones descentralizadas y privadas no se manifiestan algunas posibles soluciones generales a esta problemática,

esto se puede reflejar en la ausencia de políticas públicas y la existencia de problemas con el SPAM.

El daño que ocasiona la presencia del SPAM en Bolivia, en las cuentas de correo electrónico, personales e institucionales, pasa de ser un daño social a ser un daño económico, es así que en este estudio se aproximo un costo muy elevado a un problema que no se lo percibe como tal.

En la consideración de que para una lucha contra el SPAM en Bolivia se debe presentar una solución integral que agrupe a políticas de educación y concientización de la sociedad sobre este problema, directrices que orienten hacia el uso de algún filtro anti SPAM, legislación nacional e internacional; solo tomando en cuenta a estas técnicas Anti SPAM podremos acercarnos hacia un uso legitimo del correo electrónico que no involucre la presencia de ningún ente fisico o lógico dañino.

Un medio que puede resultar efectivo para el control del SPAM es la adopción de legislación anti SPAM en la mayor cantidad de países posibles, lo cual no será eficaz si no se cuenta con un marco legislativo elemental que le dé fuerza a través de leyes de protección al usuario, leyes para delitos informáticos, de privacidad y de seguridad en las redes.

Hay que ser conscientes que en el corto plazo el volumen de SPAM continuará aumentando debido a la falta de acciones correctivas y preventivas, se puede llegar a la conclusión que todos los aspectos económicos favorecen al Spammer y perjudican notablemente al usuario Boliviano de correo electrónico.

Es importante penalizar a la persona o personas que se dedican a esta tarea, pues es real que el SPAM es una amenaza a la viabilidad del Internet como un medio efectivo de comunicación, comercio electrónico, y productividad, y mientras no se penalice es dificil pensar en una mejora.

Es indispensable y de prioridad que de la mano de la adopción de las nuevas tecnologías de la información y comunicación también se cree una cultura de uso adecuado de los medios electrónicos, la misma debe ir dirigida tanto a usuarios, como a los proveedores de servicio de internet. La concientización acerca de la información, educación y capacitación a los usuarios es un elemento primordial dentro del desarrollo de mecanismos de combate contra el SPAM para esto se deben crear campañas de difusión informativa y educativa en los distintos ámbitos sociales

4.2 Aportes

Luego de haber comprobado la veracidad de las dos variables de la hipótesis planteada en el presente estudio, a continuación se darán los lineamientos técnicos informáticos, además de otras técnicas que se pudieron observar como muy necesarias en la lucha contra el SPAM

4.2.1 Lineamentos técnicos informáticos

1. **Software anti SPAM o filtros Anti SPAM**

   Es necesario aplicar de manera obligatoria en todas las instituciones estatales descentralizadas y privadas mecanismos lógicos Anti SPAM.

   Los proveedores Bolivianos de servicio de correo electrónico, deben de aplicar filtros lógicos en sus servidores de correo electrónico, para así poder minimizar el impacto del SPAM en las cuentas de sus usuarios.

2. **Legislación anti SPAM**

En relación a la legislación ANTI SPAM en BOLIVIA debemos tomar en cuenta los siguientes puntos.

A. En cuanto refiere al servidor de correo electrónico

El servidor que provea del servicio de correo electrónico deberá de de proteger siempre los datos de sus usuarios, brindando la menor cantidad posible de información de estos

Se deben plantear políticas que normen el acceso técnico a los encargados de los servidores de correo electrónico, en cuanto a estos refiere, si estos utilizaran de manera mal intencionada, fraudulenta o procedieran con alevosía en cuanto al manejo de la información que tienen en sus manos, estos deberán ser sancionados en cuestión de la protección de la intimidad de las personas y el derecho privado.

Se debe establecer legalmente que el servicio de correo electrónico es para cualquier persona, sin importar su tendencia religiosa, preferencia sexual, lugar de residencia, preferencia política, si esto no ocurriese, se debe sancionar este comportamiento

B. En cuanto al correo publicitario

Se debe establecer que la publicidad es necesaria para el desarrollo de la economía de un país pues hace que se puedan hacer visibles algunos productos o servicios no son conocidos. Sin embargo se deben establecer algunas políticas de control de este tipo de publicidad, y entre ellos considerar los siguientes:

a) Rechazar o no la recepción de correos electrónicos comerciales.

b) Revocar la autorización de recepción, salvo cuando dicha autorización sea una condición esencial para la provisión del servicio de correo electrónico.
c) Que su proveedor de servicio de correo electrónico cuente con sistemas o programas que filtren los correos electrónicos no solicitados.

D. Correo electrónico comercial no solicitado

Todo correo electrónico comercial, promocional o publicitario no solicitado, originado en el país, debe contener:

a) La palabra "PUBLICIDAD", en el campo del "asunto o subject" del mensaje.
b) Nombre o denominación social, domicilio completo y dirección de correo electrónico de la persona natural o jurídica que emite el mensaje.
c) La inclusión de una dirección de correo electrónico válido y activo de respuesta para que el receptor pueda enviar un mensaje para notificar su voluntad de no recibir más correos no solicitados o la inclusión de otros mecanismos basados en Internet que permita al receptor manifestar su voluntad de no recibir mensajes adicionales.

El correo electrónico comercial no solicitado será considerado ilegal en los siguientes casos:

a) Contenga nombre falso o información falsa que se oriente a no identificar a la persona natural o jurídica que transmite el mensaje.
b) Contenga información falsa o engañosa en el campo del "asunto" (o subject), que no coincida con el contenido del mensaje.
c) Se envíe o transmita a un receptor que haya formulado el pedido para que no se envíe dicha publicidad, luego del plazo de dos días.

Educación del usuario boliviano de correo electrónico

Se debe establecer una política de educación y concientización a toda la población que tienen acceso al Internet, ya que en la actualidad, se vienen empleando políticas publicas con relación al acceso a la tecnología TIC's , es por esta razón, que cuando se inserta a un ciudadano boliviano al mundo digital, paralelamente también se le debe de informar sobre algunos de los problemas que encontrara es este ámbito como es el SPAM.

En casos en que el SPAM ya alcanzo su objetivo también se deben establecer políticas de información acerca de la legislación vigente en relación a sanciones de malas prácticas digitales

Tratados multilaterales con países que también tienen normado este problema

Al ser el SPAM un problema Global no es suficiente la normativa de esta mala practica a nivel nacional, es asi que se tienen que establecer mecanismos multilaterales como son los tratados y acuerdos para poder hacer que el impacto dañino sea menor

4.2.2 Proyecto de ley anti SPAM

Luego de haber logrado diseñar los lineamientos técnico informáticos base para la lucha anti SPAM en Bolivia, en base a los mismos se logro construir un proyecto de ley Anti SPAM para Bolivia, esto como un aporte fundamental ya que como se vio en el marco practico es de suma prioridad la creación de este tipo de mecanismos que coadyuven a la lucha contra el SPAM (Este proyecto de ley en su versión inicial se encuentra adjunto en el Anexo V)

4.3 Recomendaciones

Se debe lograr que en base a los lineamientos técnicos informáticos del presente trabajo se desarrolle un proyecto de ley anti SPAM orientado a la sociedad Boliviana

Se recomienda hacer un estudio minucioso acerca del comportamiento que tiene el usuario de correo electrónico en Bolivia para así poder delimitar y percibir las deficiencias y vulnerabilidades que se tiene para poder adaptarse bien a las nuevas tecnologías

Ver la posibilidad de hacer convenios de carácter internacional para que la lucha contra el SPAM en Bolivia también tenga validez en el exterior ya que al ser un problema global la mayoría de las veces el Spammer no esta en el país

Profundizar este estudio con otros complementarios en otros departamentos del Pais con el objetivo de estimar y corroborar el gran daño económico que el SPAM hace en Bolivia y además poder identificar el lugar de procedencia de SPAM

4.4 Trabajos futuros

El presente trabajo debe complementarse con la investigación de SPAM en otro tipo de tecnologías y se las describen en orden prioritario

- Telefonía Celular
- Chats
- Foros
- Ventanas Emergentes

Para poder tener una mayor precisión en relación a el impacto que tiene el SPAM a nivel Nacional es necesario que los estudios recomendados tengan base estadística y sean complementarios unos con otros, de esta forma se podrá lograr tener un verdadero sistema de lucha anti SPAM en Bolivia

BIBLIOGRAFIA

Castells, M.2001, LA GALAXIA INTERNET, 1ra Edicion, Barcelona, Plaza & James Editores S.A.

Plant, R., 2000, E-COMMERSE, 1ra Edicion, San Pablo Brasil, Pearson Education S.A.

Ragoni, R., 2001, E-MONEY, 1ra Edicion, San Pablo Brasil, Pearson Education S.A.

Northcutt, S., Novak, J., 2001, DETECCION DE INTRUSOS, 2da Edicion, Madrid Espana, Prentice Hall

Padilla, A., 1999, TELETRABAJO DIRECCION Y ORGANIZACIÓN, 1ra Edicion, Madrid España, AlfaOmega

Whelan, J., 2000, E-MAIL EN EL TRABAJO, 1ra Edicion, Madrid España, Prentice May

Vassos, T., 1996, ESTRATEGIAS DE MERCADOTECNIA EN INTERNET, 1ra Edicion, Mexico D.F, Prentice Hall

Janal, D., 2000, MARKETING EN INTERNET, 1ra Edicion, Mexico, Prentice Hall

Fellenstein, C.. & Ron, W., 2000, E- COMMERSE, 1ra Edicion, Buenos Aires Argenina, Pearson Education & Prentice Hall

Dvorak, J.& Anir, N., 1992, TELECOMUNICACIONES PARA PC, MODEMN, SOFTWARE BBS, CORREO ELECTRÓNICO E INTERCONEXIÓN, 1ra Edicion, Madrid España, Mc Graw Hill.

Azpilcueta, H. T., 1987, DERECHO INFORMATICO, 1ra Edicion, Mexico DF., Abeledo – Perrot

Farol, H. 1949, GENERAL AND INDUSTRIAL MANAGEMENT, 1ra Edicion, Pitman London.

DIRECCIONES WEB

Soluciones humanas a Problemas Técnicos – Anti SPAM
http://microasist.com.mx/

Computadoras Zombies en el mundo del SPAM
http://www.ciphertrust.com/resources/statistics/zombie.php

Sophos es un líder mundial en soluciones de control y seguridad informática para empresas, educación y gobiernos Informe de Sophos de los principales Pises emisores de SPAM

http://esp.sophos.com/pressoffice/news/articles/2006/04/dirtydozapr06.html

Unión internacional de Telecomunicaciones
Cooperación internacional contra el SPAM, Actividades y legislaciones contra el SPAM

http://www.itu.int/osg/spu/SPAM/intcoop.html

Tecnologías Microsoft Anti SPAM
http://www.microsoft.com/SPAM

Ataques por SPAM en Países del mundo Diferentes soluciones
http://www.ciphertrust.com/resources/statistics/SPAM_sources.php

Informes sobre SPAM legislaciones y Artículos presentados
http://www.itu.int/osg/spu/SPAM/background.html

II Congreso Mundial Uso legitimo del correo electrónico
www.ieid.org/congreso/ponencias/Castro%20Bonilla,%20Alejandra.pdf

Microsoft Seguridad Informe SPAM
http://www.microsoft.com/spain/enterprise/perspectivas/numero_9/seguridad.mspx

Correo Electrónico SPAM
www.monografias.com

Superintendencia de Telecomunicaciones SITTEL
Informe Usuarios Internet Bolivia
www.sittel.gov.bo/

Honorable congreso de la República de Bolivia
Proyectos de ley
www.congreso.gov.bo/

Instituto Nacional de Estadística INE
Informe Estimación población por edades 2007
www.ine.gov.bo/

Google Noticias SPAM
Se duplica volumen de SPAM a nivel mundial
www.google.com

Google Noticias SPAM
MILLONES DE USUARIOS PAGAN EL SALARIO DE LOS SPAMMERS
www.google.com

BANCO Nacional de Bolivia BNB
Recomendaciones Usuarios de Internet
www.bnb.com.bo/

ANEXO I

1st Session
S. 1293

To criminalize the sending of predatory and abusive e-mail.

IN THE SENATE OF THE UNITED STATES

June 19, 2003

Mr. HATCH (for himself, Mr. LEAHY, Mr. SCHUMER, Mr. GRASSLEY, Mrs. FEINSTEIN, Mr. DEWINE, and Mr. EDWARDS) introduced the following bill; which was read twice and referred to the Committee on the Judiciary

---

A BILL

To criminalize the sending of predatory and abusive e-mail.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the Criminal Spam Act of 2003'.

SEC. 2. PROHIBITION AGAINST PREDATORY AND ABUSIVE COMMERCIAL E-MAIL.

(a) OFFENSE-

(1) IN GENERAL- Chapter 47 of title 18, United States Code, is amended by adding at the end the following new section:

Sec. 1037. Fraud and related activity in connection with electronic mail

(a) IN GENERAL- Whoever, in or affecting interstate or foreign commerce, knowingly--

(1) accesses a protected computer without authorization, and intentionally initiates the transmission of multiple commercial electronic mail messages from or through such computer;

(2) uses a protected computer to relay or retransmit multiple commercial electronic mail messages, with the intent to deceive or mislead recipients, or any Internet access service, as to the origin of such messages;

(3) falsifies header information in multiple commercial electronic mail messages and intentionally initiates the transmission of such messages; or

(4) registers, using information that falsifies the identity of the actual registrant, for 5 or more electronic mail accounts or online user accounts or 2 or more domain names, and intentionally initiates the transmission of multiple commercial electronic mail messages from such accounts or domain names;

or conspires to do so, shall be punished as provided in subsection (b).

(b) PENALTIES- The punishment for an offense under subsection (a) is--

(1) a fine under this title, imprisonment for not more than 5 years, or both, if--

(A) the offense is committed in furtherance of any felony under the laws of the United States or of any State; or

(B) the defendant has previously been convicted under this section or section 1030, or under the law of any State for conduct involving the transmission of multiple commercial electronic mail messages or unauthorized access to a computer system;

(c) FORFEITURE- A person who is convicted of an offense under this section shall forfeit to the United States such person's interest in--

(1) any property, real or personal, constituting or traceable to gross profits or other proceeds obtained from such offense; and

(2) any equipment, software, or other technology used or intended to be used to commit or to promote the commission of such offense.

(d) CIVIL REMEDIES-

(1) IN GENERAL- The Attorney General, or any person engaged in the business of providing an Internet access service to the public aggrieved by reason of a violation of subsection (a), may commence a civil action against the violator in any appropriate United States District Court for the relief set forth in paragraphs (2) and (3). No action may be brought under this subsection unless such action is begun within 2 years of the date of the act which is the basis for the action.

(e) DEFINITIONS- In this section:

(1) COMMERCIAL ELECTRONIC MAIL MESSAGE- The term commercial electronic mail message' means any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service (including content on an Internet website or online site operated for a commercial purpose).

(2) COMPUTER AND PROTECTED COMPUTER- The terms computer' and protected computer' have the meaning given those terms in section 1030(e) of this title.

(3) DOMAIN NAME- The term domain name' means any alphanumeric designation which is registered with or assigned by any domain name registrar, domain name registry, or other domain name registration authority, and that is included in an electronic mail message.

(4) HEADER INFORMATION- The term header information' means the source, destination, routing information, or information authenticating the sender, associated with an electronic mail message, including but not limited to the originating domain name, originating electronic mail address, information regarding any part of the route that an electronic mail message travels or appears to travel on the Internet or on an online service, or other authenticating information.

(5) INITIATE- The term initiate' means to originate an electronic mail message or to procure the origination of such message, regardless of whether the message reaches its intended recipients, and does not include the actions of an Internet access service used by another person for the transmission of an electronic mail message for which another person has provided and selected the recipient electronic mail addresses.

(6) INTERNET ACCESS SERVICE- The term Internet access service' has the meaning given that term in section 231(e)(4) of the Communications Act of 1934 (47 U.S.C. 231(e)(4)).

(7) LOSS- The term loss' has the meaning given that term in section 1030(e) of this title.

(8) MESSAGE- The term message' means each electronic mail message addressed to a discrete addressee.

(9) MULTIPLE- The term multiple' means more than 100 electronic mail messages during a 24-hour period, more than 1,000 electronic mail messages during a 30-day period, or more than 10,000 electronic mail messages during a 1-year period.'.

(2) CONFORMING AMENDMENT- The chapter analysis for chapter 47 of title 18, United States Code, is amended by adding at the end the following:

Sec.

1037. Fraud and related activity in connection with electronic mail.'.

(b) UNITED STATES SENTENCING COMMISSION-

(1) DIRECTIVE- Pursuant to its authority under section 994(p) of title 28, United States Code, and in accordance with this section, the United States Sentencing Commission shall review and, as appropriate, amend the sentencing guidelines and policy statements to provide appropriate

penalties for violations of section 1037 of title 18, United States Code, as added by this section.

(2) REQUIREMENTS- In carrying out this subsection, the Sentencing Commission shall consider providing sentencing enhancements for those convicted under section 1037 of title 18, United States Code, who--

(A) obtained electronic mail addresses through improper means, including--

(i) harvesting electronic mail addresses of the users of a website, proprietary service, or other online public forum operated by another person, without the authorization of such person; and

(ii) randomly generating electronic mail addresses by computer; or

(B) knew that the commercial electronic mail messages involved in the offense contained or advertised an Internet domain for which the registrant of the domain had provided false registration information.

SEC. 3. REPORT AND SENSE OF CONGRESS REGARDING INTERNATIONAL SPAM.

(a) FINDINGS- Congress finds the following:

(1) The Internet is a global communications medium.

(2) Commercial e-mail sent in violation of this Act can be sent from virtually anywhere in the world.

(3) As domestic deterrence and enforcement against predatory and abusive commercial e-mail improves, there is a risk that predatory and abusive spammers will move their activities abroad and spam into the United States.

(4) As with other forms of cyber-crime, international cooperation of law enforcement officials is essential to combat predatory and abusive spam.

(b) REPORT- The Department of Justice and the Department of State shall report to Congress within 18 months of the date of enactment of this Act regarding the status of their efforts to achieve international cooperation in the investigation and prosecution of spammers who engage in conduct that violates this Act, including the jurisdictions involved and the outcomes of any prosecutions, and any recommendations for addressing predatory and abusive spam sent to the United States from other countries.

(c) SENSE OF CONGRESS- It is the sense of Congress that the Department of Justice and the Department of State, as part of their efforts to improve investigation and prosecution of international cyber-crime, should work through international fora for the cooperation of other countries in investigating and

prosecuting predatory and abusive spammers who engage in conduct that violates this Act.

END

ANEXO II

Ley 25.326
Protección de datos personales
(Actualización: Diciembre 2001)

Texto elaborado a base de las siguientes disposiciones:

- **Ley 25.326, sancionada el 04.10.00, B.O. 02.11.00**
- **Decreto 995/2000, sancionada 04.10.00, B.O. 02.11.00**

• Decreto 1558/2001, sancionado el 29.11.01, B.O. 03.12.01

Disposiciones Generales. Principios generales relativos a la protección de datos. Derechos de los titulares de datos. Usuarios y responsables de archivos, registros y bancos de datos. Control. Sanciones. Acción de protección de los datos personales.
El Senado y Cámara de Diputados de la Nación Argentina reunidos en Congreso, etc. sancionan con fuerza de Ley:
Capítulo I
Disposiciones Generales
Articulo 1°: (Objeto).
La presente ley tiene por objeto la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre, de conformidad a lo establecido en el artículo 43, párrafo tercero de la Constitución Nacional.
Las disposiciones de la presente ley también serán aplicables, en cuanto resulte pertinente, a los datos relativos a personas de existencia ideal.
En ningún caso se podrán afectar la base de datos ni las fuentes de información periodísticas.
Capítulo II
Principios generales relativos a la protección de datos
Articulo 3° :(Archivos de datos – Licitud). La formación de archivos de datos será lícita cuando se encuentren debidamente inscriptos, observando en su operación los principios que establece la presente ley y las reglamentaciones que se dicten en su consecuencia.
Los archivos de datos no pueden tener finalidades contrarias a las leyes o a la moral pública.
Articulo 4° :(Calidad de los datos).
1. Los datos personales que se recojan a los efectos de su tratamiento deben ser ciertos, adecuados, pertinentes y no excesivos en relación al ámbito y finalidad para los que se hubieren obtenido.
2. La recolección de datos no puede hacerse por medios desleales, fraudulentos o en forma contraria a las disposiciones de la presente ley.
3. Los datos objeto de tratamiento no pueden ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención.
4. Los datos deben ser exactos y actualizarse en el caso de que ello fuere necesario.
5. Los datos total o parcialmente inexactos, o que sean incompletos, deben ser suprimidos y sustituidos, o en su caso completados, por el responsable del archivo o base de datos cuando se tenga conocimiento de la inexactitud o carácter incompleto de la información de que se trate, sin perjuicio de los derechos del titular establecidos en el artículo 16 de la presente ley.

6. Los datos deben ser almacenados de modo que permitan el ejercicio del derecho de acceso de su titular.
7. Los datos deben ser destruidos cuando hayan dejado de ser necesarios o pertinentes a los fines para los cuales hubiesen sido recolectados.
Articulo 10. :(Deber de confidencialidad).
1. El responsable y las personas que intervengan en cualquier fase del tratamiento de datos personales están obligados al secreto profesional respecto de los mismos. Tal obligación subsistirá aun después de finalizada su relación con el titular del archivo de datos.
2. El obligado podrá ser relevado del deber de secreto por resolución judicial y cuando medien razones fundadas relativas a la seguridad pública, la defensa nacional o la salud pública.
Articulo 18. :(Comisiones legislativas).
Las Comisiones de Defensa Nacional y la Comisión Bicameral de Fiscalización de los Organos y
Actividades de Seguridad Interior e Inteligencia del Congreso de la Nación y la Comisión de Seguridad Interior de la Cámara de Diputados de la Nación, o las que las sustituyan, tendrán acceso a los archivos o bancos de datos referidos en el artículo 23 inciso 2 por razones fundadas y en aquellos aspectos que constituyan materia de competencia de tales Comisiones.
Articulo 19. :(Gratuidad).
La rectificación, actualización o supresión de datos personales inexactos o incompletos que obren en registros públicos o privados se efectuará sin cargo alguno para el interesado.
Articulo 20. :(Impugnación de valoraciones personales).
1. Las decisiones judiciales o los actos administrativos que impliquen apreciación o valoración de conductas humanas, no podrán tener como único fundamento el resultado del tratamiento informatizado de datos personales que suministren una definición del perfil o personalidad del interesado.
2. Los actos que resulten contrarios a la disposición precedente serán insanablemente nulos.
Capítulo IV
Usuarios y responsables de archivos, registros y bancos de datos
Articulo 22. :(Archivos, registros o bancos de datos públicos).
1. Las normas sobre creación, modificación o supresión de archivos, registros o bancos de datos pertenecientes a organismos públicos deben hacerse por medio de disposición general publicada en el
Boletín Oficial de la Nación o diario oficial.
2. Las disposiciones respectivas, deben indicar:
a) Características y finalidad del archivo;
b) Personas respecto de las cuales se pretenda obtener datos y el carácter facultativo u obligatorio de su suministro por parte de aquéllas;

c) Procedimiento de obtención y actualización de los datos;
d) Estructura básica del archivo, informatizado o no, y la descripción de la naturaleza de los datos personales que contendrán;
e) Las cesiones, transferencias o interconexiones previstas;
f) Organos responsables del archivo, precisando dependencia jerárquica en su caso;
g) Las oficinas ante las que se pudiesen efectuar las reclamaciones en ejercicio de los derechos de acceso, rectificación o supresión.
3. En las disposiciones que se dicten para la supresión de los registros informatizados se establecerá el destino de los mismos o las medidas que se adopten para su destrucción.
Articulo 23. :(Supuestos especiales).
1. Quedarán sujetos al régimen de la presente ley, los datos personales que por haberse almacenado para fines administrativos, deban ser objeto de registro permanente en los bancos de datos de las fuerzas armadas, fuerzas de seguridad, organismos policiales o de inteligencia; y aquellos sobre antecedentes personales que proporcionen dichos bancos de datos a las autoridades administrativas
o judiciales que los requieran en virtud de disposiciones legales.
2. El tratamiento de datos personales con fines de defensa nacional o seguridad pública por parte de las fuerzas armadas, fuerzas de seguridad, organismos policiales o inteligencia, sin consentimiento de los afectados, queda limitado a aquellos supuestos y categoría de datos que resulten necesarios para el estricto cumplimiento de las misiones legalmente asignadas a aquéllos para la defensa nacional, la seguridad pública o para la represión de los delitos. Los archivos, en tales casos,
Articulo 27. :(Archivos, registros o bancos de datos con fines de publicidad).
1. En la recopilación de domicilios, reparto de documentos, publicidad o venta directa y otras actividades análogas, se podrán tratar datos que sean aptos para establecer perfiles determinados con fines promocionales, comerciales o publicitarios; o permitan establecer hábitos de consumo, cuando éstos figuren en documentos accesibles al público o hayan sido facilitados por los propios titulares u obtenidos con su consentimiento.
2. En los supuestos contemplados en el presente artículo, el titular de los datos podrá ejercer el derecho de acceso sin cargo alguno.
3. El titular podrá en cualquier momento solicitar el retiro o bloqueo de su nombre de los bancos de datos a los que se refiere el presente artículo.
ARTICULO 27.- Podrán recopilarse, tratarse y cederse datos con fines de publicidad sin consentimiento de su titular, cuando estén destinados a la formación de perfiles determinados, que categoricen preferencias y comportamientos similares de las personas, siempre que los titulares de los datos sólo se identifiquen por su pertenencia a tales grupos genéricos, con más los datos individuales estrictamente necesarios para formular la oferta a los destinatarios.
En toda comunicación con fines de publicidad que se realice por correo, teléfono, correo electrónico, Internet u otro medio a distancia a conocer, se deberá indicar, en forma expresa y destacada, la posibilidad del titular del dato de solicitar el retiro o bloqueo,

total o parcial, de su nombre de la base de datos. A pedido del interesado, se deberá informar el nombre del responsable o usuario del banco de datos que proveyó la información.
A los fines de garantizar el derecho de información del artículo 13 de la Ley N° 25.326, se inscribirán únicamente las cámaras, asociaciones y colegios profesionales del sector que dispongan de un Código de Conducta homologado por la DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES, al que por estatuto adhieran obligatoriamente todos sus miembros. Al inscribirse, las cámaras, asociaciones y colegios profesionales deberán acompañar una nómina de sus asociados indicando nombre, apellido y domicilio.
Los responsables o usuarios de archivos, registros, bancos o bases de datos con fines de publicidad que no se encuentren adheridos a ningún Código de Conducta, cumplirán el deber de información inscribiéndose en el Registro a que se refiere el artículo 21 de la Ley N° 25.326.
Los datos vinculados a la salud sólo podrán ser tratados, a fin de realizar ofertas de bienes y servicios, cuando hubieran sido obtenidos de acuerdo con la Ley N° 25.326 y siempre que no causen discriminación, en el contexto de una relación entre el consumidor o usuario y los proveedores de servicios o tratamientos médicos y entidades sin fines de lucro. Estos datos no podrán transferirse a terceros sin el consentimiento previo, expreso e informado del titular de los datos. A dicho fin, este último debe recibir una noticia clara del carácter sensible de los datos que proporciona y de que no está obligado a suministrarlos, junto con la información de los artículos 6° y 11, inciso 1, de la Ley N° 25.326 y la mención de su derecho a solicitar el retiro de la base de datos.
CAPITULO VI
SANCIONES
ARTICULO 31.
1. Las sanciones administrativas establecidas en el artículo 31 de la Ley N° 25.326 serán aplicadas a los responsables o usuarios de archivos, registros, bases o bancos de datos públicos, y privados destinados a dar información, se hubieren inscripto o no en el registro correspondiente.
La cuantía de las sanciones se graduará atendiendo a la naturaleza de los derechos personales afectados, al volumen de los tratamientos efectuados, a los beneficios obtenidos, al grado de intencionalidad, a la reincidencia, a los daños y perjuicios causados a las personas interesadas y a terceros, y a cualquier otra circunstancia que sea relevante para determinar el grado de antijuricidad y de culpabilidad presentes en la concreta actuación infractora. Se considerará reincidente a quien habiendo sido sancionado por una infracción a la Ley N° 25.326 o sus reglamentaciones incurriera en otra de similar naturaleza dentro del término de TRES (3) años, a contar desde la aplicación de la sanción.
2. El producido de las multas a que se refiere el artículo 31 de la Ley N° 25.326 se aplicará al financiamiento de la DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES.

3. El procedimiento se ajustará a las siguientes disposiciones: a) La DIRECCION NACIONAL DE
PROTECCION DE DATOS PERSONALES iniciará actuaciones administrativas en caso de presuntas infracciones a las disposiciones de la Ley N° 25.326 y sus normas reglamentarias, de oficio o por denuncia de quien invocare un interés particular, del Defensor del Pueblo de la Nación o de asociaciones de consumidores o usuarios.
a) Se procederá a labrar acta en la que se dejará constancia del hecho denunciado o verificado y de la disposición presuntamente infringida.
En la misma acta se dispondrá agregar la documentación acompañada y citar al presunto infractor para que, dentro del plazo de CINCO (5) días hábiles, presente por escrito su descargo y ofrezca las pruebas que hacen a su derecho.
Si se tratare de un acta de inspección, en que fuere necesaria una comprobación técnica posterior a los efectos de la determinación de la presunta infracción y que resultare positiva, se procederá a notificar al presunto responsable la infracción verificada, intimándolo para que en el plazo de CINCO (5) días hábiles presente por escrito su descargo. En su primera presentación, el presunto infractor deberá constituir domicilio y acreditar personería.

ANEXO III

LEY N° 28493
EL PRESIDENTE DE LA REPÚBLICA

POR CUANTO:

EL Congreso de la República;
Ha dado la Ley siguiente:

LEY QUE REGULA EL USO DEL CORREO ELECTRONICO COMERCIAL NO SOLICITADO (SPAM)

Artículo 1°.Objeto de la Ley
La presente Ley regula el envío de comunicaciones comerciales publicitarias o promocionales no solicitadas, realizadas por correo electrónico, sin perjuicio de la aplicación de las disposiciones vigentes en materia comercial sobre publicidad y protección al consumidor.
Artículo 2°.Definiciones
Para efectos de la presente Ley se entiende por:
a) Correo electrónico: Todo mensaje, archivo, dato u otra información electrónica que se transmite a una o más personas por medio de una red de interconexión entre computadoras o cualquier otro equipo de tecnología similar. También se considera correo electrónico la información contenida en forma de remisión o anexo accesible mediante enlace electrónico directo contenido dentro del correo electrónico.
b) Correo electrónico comercial: Todo correo electrónico que contenga información comercial publicitaria o promocional de bienes y servicios de una empresa, organización, persona o cualquier otra con fines lucrativos.
c) Proveedor del servicio de correo electrónico: Toda persona natural o jurídica que provea el servicio de correo electrónico y que actúa como intermediario en el envío o recepción del mismo.
d) Dirección de correo electrónico: Serie de caracteres utilizado para identificar el origen o el destino de un correo electrónico.
Artículo 3°.Derechos de los usuarios
Son derechos de los usuarios de correo electrónico:
a) Rechazar o no la recepción de correos electrónicos comerciales.
b) Revocar la autorización de recepción, salvo cuando dicha autorización sea una condición esencial para la provisión del servicio de correo electrónico.
c) Que su proveedor de servicio de correo electrónico cuente con sistemas o programas que filtren los correos electrónicos no solicitados.
Artículo 4°.Obligaciones del proveedor
Los proveedores de servicio de correo electrónico domiciliados en el país están obligados a contar con sistemas o programas de bloqueo y/o filtro para la recepción o la transmisión que se efectúe a través de su servidor, de los correos electrónicos no solicitados por el usuario.
Artículo 5°.Correo electrónico comercial no solicitado
Todo correo electrónico comercial, promocional o publicitario no solicitado, originado en el país, debe contener:
a) La palabra "PUBLICIDAD", en el campo del "asunto" (o subject) del mensaje.
b) Nombre o denominación social, domicilio completo y dirección de correo electrónico de la persona natural o jurídica que emite el mensaje.

c) La inclusión de una dirección de correo electrónico válido y activo de respuesta para que el receptor pueda enviar un mensaje para notificar su voluntad de no recibir más correos no solicitados o la inclusión de otros mecanismos basados en Internet que permita al receptor manifestar su voluntad de no recibir mensajes adicionales.

Artículo 6°.Correo electrónico comercial no solicitado considerado ilegal

El correo electrónico comercial no solicitado será considerado ilegal en los siguientes casos:

a) Cuando no cumpla con alguno de los requisitos establecidos en el artículo 5° de la presente Ley.

b) Contenga nombre falso o información falsa que se oriente a no identificar a la persona natural o jurídica que transmite el mensaje.

c) Contenga información falsa o engañosa en el campo del "asunto" (o subject), que no coincida con el contenido del mensaje.

d) Se envíe o transmita a un receptor que haya formulado el pedido para que no se envíe dicha publicidad, luego del plazo de dos (2) días.

Artículo 7°.Responsabilidad

Se considerarán responsables de las infracciones establecidas en el artículo 6° de la presente Ley y deberán compensar al receptor de la comunicación:

1. Toda persona que envíe correos electrónicos no solicitados conteniendo publicidad comercial.

2. Las empresas o personas beneficiarias de manera directa con la publicidad difundida.

3. Los intermediarios de correos electrónicos no solicitados, tales como los proveedores de servicios de correos electrónicos.

Artículo 8°.Derecho

a compensación pecuniaria

El receptor de correo electrónico ilegal podrá accionar por la vía del proceso sumarísimo contra la persona que lo haya enviado, a fin de obtener una compensación pecuniaria, la cual será equivalente al uno por ciento (1%) de la

Unidad Impositiva Tributaria por cada uno de los mensajes de correo electrónico transmitidos en contravención de la presente Ley, con un máximo de dos (2) Unidades Impositivas Tributarias.

Artículo 9°.Autoridad competente

El Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual INDECOPI, a través de la Comisión de Protección al Consumidor y de la Comisión de Represión de la Competencia Desleal, será la autoridad competente para conocer las infracciones contempladas en el artículo 6° de la presente Ley; cuyas multas se fijarán de acuerdo a lo establecido en el Decreto Legislativo N° 716, Ley de Protección al Consumidor, o en el Decreto Legislativo N° 691, Normas de la Publicidad en Defensa del Consumidor, según corresponda.

Artículo 10°.Reglamento

El Poder Ejecutivo mediante decreto supremo, refrendado por el Ministro de Transportes y Comunicaciones, reglamentará la presente Ley en un plazo máximo de noventa (90) días desde su vigencia.

Artículo 11°.Vigencia

La presente Ley entrará en vigencia a los noventa (90) días de su publicación en el Diario Oficial "El Peruano".

Comuníquese al señor Presidente de la República para su promulgación.

En Lima, a los dieciocho días del mes de marzo de dos mil cinco.

ÁNTERO FLORESARAOZ E.

Presidente del Congreso de la República

JUDITH DE LA MATA FERNÁNDEZ

Segunda Vicepresidenta del Congreso de la República

AL SEÑOR PRESIDENTE CONSTITUCIONAL DE LA REPÚBLICA

Mando se publique y se cumpla

Dado en la Casa de Gobierno, en Lima, a los once días del mes de abril del año dos mil cinco.

ALEJANDRO TOLEDO

Presidente Constitucional de la República

CARLOS FERRERO

Presidente del Consejo de Ministros

ANEXO IV

PROYECTO DE LEY 037/06-07

EL HONORABLE CONGRESO NACIONAL:
DECRETA:

"LEY DE DOCUMENTOS, FIRMAS Y COMERCIO ELECTRÓNICO"

TITULO I

DISPOSICIONES GENERALES

CAPITULO UNICO

OBJETO Y PRINCIPIOS GENERALES

Artículo 1 (Objeto). La presente Ley tiene por objeto reconocer el valor jurídico y probatorio de:

a) Los actos jurídicos celebrados mediante medios electrónicos u otros de mayor avance tecnológico realizados por personas naturales, jurídicas, empresas colectivas o unipersonales, comunidades de bienes y otras entidades que constituyan una unidad económica sujeta a derechos y obligaciones.

b) El uso de firmas electrónicas debidamente certificadas por una Entidad de Certificación acreditada bajo lo estipulado en la presente ley.

c) Los actos civiles y comerciales que utilicen directa o indirectamente medios electrónicos u otros de mayor avance tecnológico para realizar actividades del comercio electrónico.

Artículo 2 (Ámbito de aplicación). I. Los principios y normas establecidas en esta Ley se aplicarán a los actos jurídicos otorgados o celebrados a través de mensajes de datos y documentos electrónicos que den origen a contratos, operaciones o servicios. Igualmente, será aplicable a todo tipo de información que tenga relación con la naturaleza de los servicios de la sociedad de la información utilizada en el contexto de actividades del comercio electrónico.

Artículo 3 (Interpretación, aplicación y definiciones).

I. Por Reglamento se establecerán las definiciones técnicas para mejor interpretación de la presente Ley, dicho instrumento se sujetará a las siguientes directrices:

a) Las definiciones tomarán en cuenta los principios y alcances técnicos de esta Ley.

b) Toda complementación, modificación o actualización a las definiciones, se efectuará en función del avance tecnológico.

c) Tomará en cuenta los derechos adquiridos para otorgar seguridad jurídica a los usuarios del sistema.

Artículo 4 (Principios). Las actividades reguladas por esta Ley se sujetarán a los siguientes principios:

a) Neutralidad tecnológica, en virtud de la cual no favorece ni restringe el uso de ciertas tecnologías, en tanto y en cuanto cumplan los requisitos y presupuestos establecidos en las normas aplicables;

b) Asimilación jurídica, en el entendido de que los actos jurídicos celebrados por medios electrónicos, gozarán de la validez y eficacia jurídica reconocida para los medios convencionales vigentes;

c) Equivalente funcional, reconoce la misma validez jurídica y fuerza probatoria a los mensajes de datos, documentos electrónicos, firmas electrónicas y demás procedimientos tecnológicos respecto de los medios convencionales para manifestar la voluntad, hacer constar información por escrito e instrumentar un acto jurídico;

Artículo 5 (Protección de datos personales). I. La utilización de los datos personales respetará los derechos a la intimidad personal y familiar, imagen, honra, reputación, y demás derechos garantizados por la Constitución Política del Estado.

II. El tratamiento de datos personales en el sector publico y privado en todas sus modalidades, incluyendo entre éstas las actividades de recolección, grabación, conservación, elaboración, modificación, bloqueo, cancelación, transferencias, consultas e interconexiones, requerirá del consentimiento previo, expreso e informado del titular, el que será brindado por escrito o por otro medio equiparable de acuerdo a las circunstancias. Este consentimiento podrá ser revocado cuando exista causa justificada para ello, pero tal revocatoria no tendrá efecto retroactivo.

TÍTULO V
DELITOS INFORMATICOS
CAPÍTULO ÚNICO
DELITOS INFORMÁTICOS

Artículo 72 (Modificaciones al Código Penal)

Se modifica el Código Penal, en los siguientes términos:

1. Inclúyase al artículo 179 bis del Código Penal lo siguiente:

Artículo 179° bis.- "(DESOBEDIENCIA A RESOLUCIONES EN PROCESOS DE HABEAS CORPUS, HABEAS DATA Y AMPARO CONTITUCIONAL)

El funcionario o particular que no diere exacto cumplimiento a las resoluciones judiciales, emitidas en procesos de hábeas corpus, hábeas data o amparo constitucional, será sancionado con reclusión de dos a seis años y con multa de cien a trescientos días."

2. Sustitúyase el artículo 188 del Código Penal, por el siguiente:

Artículo 188°.- "(EQUIPARACIÓN DE VALORES A LA MONEDA)

A los efectos de la ley penal, quedan equiparados a la moneda:

1. Los billetes de Banco legalmente autorizados
2. Los bonos de la deuda nacional
3. Los valores, cédulas y acciones al portador, emitidos legalmente por los Bancos, entidades, compañías o sociedades autorizados para ello
4. Los cheques.

El presente artículo se aplicará también a los instrumentos señalados en los numerales 2, 3 y 4 que se encuentran desmaterializados y representados en documentos electrónicos.

3. Añádase como segundo o tercer párrafo de los artículos 198 (FALSEDAD MATERIAL), 199 (FALSEDAD IDEOLÓGICA) y 200 (FALSIFICACIÓN DE DOCUMENTO PRIVADO) del Código Penal, lo siguiente:

"El presente artículo se aplicará también a los documentos electrónicos".

4. Sustitúyase el artículo 300 del Código Penal, por el siguiente:

Artículo 300°.- "(VIOLACIÓN DE LA CORRESPONDENCIA Y PAPELES PRIVADOS)

El que indebidamente abriere una carta, un pliego cerrado, correo electrónico o una comunicación telegráfica, radiotelegráfica, telefónica u otros medios electrónicos, dirigidos a otra persona, o el que, sin abrir la correspondencia, por medios técnicos se impusiere de su contenido, será sancionado con reclusión de tres meses a un año o multa de sesenta a doscientos cuarenta días.

Con la misma pena será sancionado el que de igual modo se apoderare, ocultare o destruyere una carta, un pliego, un despacho, correo electrónico u otro papel privado, aunque estén abiertos, o el que arbitrariamente desviare de su destino la correspondencia que no le pertenece.

Se elevará el máximo de la sanción a dos años, cuando el autor de tales hechos divulgare el contenido de la correspondencia y despachos indicados".

7. Sustitúyase el artículo 363 bis del Código Penal, por el siguiente:

"Artículo 363° bis.- (MANIPULACIÓN INFORMÁTICA)

El que con la intención de obtener un beneficio indebido para sí o un tercero, incurra en la realización de una manipulación informática, ocasionando de esta manera una transferencia patrimonial en perjuicio de un tercero, será sancionado con reclusión de uno a cinco años y con multa de sesenta a doscientos días. Se entiende por manipulación informática, toda acción conducente a alterar en su contenido o forma los datos de entrada o de salida, los que se encuentran en proceso, o el proceso mismo de un sistema de información, o los que se encuentran almacenados en una base de datos de cualquier estructura, con el objetivo de obtener un resultado diferente al que se hubiera producido sin la intervención del autor, existiendo intencionalidad por parte del autor y sin la autorización expresa del titular de los datos de referencia."

8. Sustitúyase el artículo 363 ter del Código Penal, por el siguiente:

"Artículo 363° ter.- "(ALTERACION, ACCESO Y USO INDEBIDO DE DATOS INFORMATICOS)

El que sin estar autorizado o haciendo abuso de la autorización, se apodere, acceda, utilice, modifique, suprima, oculte o inutilice, datos almacenados en una computadora o en cualquier soporte informático, o que se encuentren en proceso

de transmisión mediante cualquier sistema electrónico y/o informático de datos, ocasionando perjuicio al titular de la información o a un tercero u obtenga beneficio indebido, será sancionado con reclusión de seis meses a dos años".

10. Inclúyase como artículo 363 quinquies del Código Penal, el siguiente:

"Artículo 363° quinquies.- (SABOTAJE INFORMÁTICO)

Quien obstaculice, modifique o atente contra el normal funcionamiento de un sistema de información, impidiendo la ejecución de sus funciones, o haciendo más lentos los mismos, mediante recursos fisicos o lógicos; incurrirá en privación de libertad de uno a tres años".

11. Inclúyase como artículo 363 septies del Código Penal, el siguiente:

"Artículo 363 septies.- (DISPOSICIÓN COMUN)

En los casos previstos por este Título, cuando fueren autores servidores públicos o las personas encargadas por su oficio o profesión de la administración de un sistema de información, se impondrá la sanción con privación de libertad de tres a seis años".

TITULO VI
DISPOSICIONES TRANSITORIAS Y FINALES
CAPITULO I
DISPOSICION TRANSITORIAS

Primera (Sellado de tiempo).- Con excepción de la Administración Tributaria, hasta que se aprueben los correspondiente Reglamentos de la presente Ley, la prestación del servicio de sellado de tiempo, deberá cumplir con los requisitos de seguridad e inalterabilidad exigidos para la firma electrónica y los certificados electrónicos.

Segunda (Administración del comercio sin papeles).- El Estado procurará poner a disposición del público en general en forma electrónica todos los documentos que tengan relación con el comercio. Se esforzará por aceptar los documentos de administración del comercio presentados electrónicamente como el equivalente legal de la versión en papeles de dichos documentos

Tercera (Medios técnicos en las entidades públicas).- La incorporación de medios técnicos en las entidades públicas, se sujetará a las siguientes regulaciones:

a) Las entidades públicas impulsarán el empleo y aplicación de las técnicas y medios electrónicos, informáticos, para el desarrollo de su actividad y el ejercicio de sus funciones y atribuciones.

b) Cuando sea compatible con los medios técnicos de que dispongan las entidades públicas, los ciudadanos podrán relacionarse con ellas para ejercer sus derechos a través de los medios electrónicos, con respecto de las garantías y requisitos previstos en cada procedimiento.

c) La Agencia para el Desarrollo de la Sociedad de Información en Bolivia, coordinará las tareas y acciones para la creación del Equipo de Respuesta para Emergencias Informáticas en Bolivia, el cual estará encargado del monitoreo, vigilancia y respuesta

frente a posibles ataques cibernéticos generados hacia y desde las redes electrónicas del Estado.

d) Los procedimientos que se tramiten y terminen en soporte electrónico garantizarán la identificación y el ejercicio de la competencia por el órgano que la ejerce.

CAPITULO II
DISPOSICIONES FINALES

Primera (Reglamentos).- La Entidad Acreditadora, será responsable de la elaboración de los reglamentos a los que hace referencia esta Ley, que serán presentados en el plazo de noventa (90) días para su aprobación. Con ese fin coordinará con el Consejo Interinstitucional, conformando las comisiones de trabajo que considere necesarias.

Segunda (Vigencia).- La presente Ley entrará en vigencia desde su publicación en la Gaceta Oficial de Bolivia. En cuanto a la acreditación de las Entidades de Certificación esta ley entrará en vigencia desde la promulgación de los respectivos reglamentos.

Tercera (Derogaciones).- A partir de la fecha de entrada en vigencia de esta Ley, quedan derogadas todas las disposiciones contrarias a la presente disposición.

ANEXO V

PROYECTO DE LEY

LEY ANTI SPAM Y DE SERVICIOS DE LA SOCIEDAD DE LA INFORMACIÓN

TITULO I

DISPOSICIONES GENERALES

CAPITULO I
OBJETO Y PRINCIPIOS GENERALES

Articulo 1 (OBJETO). La presente ley tiene por objeto reconocer, probar y regir el valor jurídico de las comunicaciones publicitarias realizadas por correo electrónico, la protección al consumidor que mediante internet desea realizar operaciones transaccionales, proteger la identidad de todo usuario boliviano de correo electrónico

Articulo 2 (AMBITO DE APLICACIÓN). **La presente Ley se aplica a efectos de proteger a los usuarios de los servicios de Correo Electrónico y de INTERNET de las consecuencias derivadas de la recepción de Correos Electrónicos no deseados a fin de garantizar mejores servicios y mayor eficiencia en el funcionamiento de las redes de telecomunicaciones. De esta forma se tipifican los delitos informáticos relativos al envío de correos electrónicos no deseados.**

Artículo 3 (INTERPRETACIÓN, APLICACIÓN Y DEFINICIONES).

Para una mejor interpretación se establecen las definiciones técnicas de la presente Ley, definidas por:

CORREO ELECTRÓNICO.- Es todo mensaje que contiene o no, archivos, datos u otra información electrónica, que se transmite a una o más personas por medios electrónicos utilizando en su origen y destino una dirección de correo electrónico.

CORREO ELECTRÓNICO PERSONAL.- Es todo mensaje, sea que incluya o no, archivos, datos u otra información electrónica, que se transmite a una persona determinada por medios electrónicos hábiles al efecto, utilizando en su origen y destino una dirección de correo electrónico privada.

CORREO ELECTRÓNICO LABORAL.- Es todo mensaje, sea que incluya o no, archivos, datos u otra información electrónica, que se transmite a una persona determinada por medios electrónicos hábiles al efecto, utilizando en su origen y destino una dirección de correo electrónico laboral.

DIRECCIÓN DE CORREO ELECTRÓNICO: **significa el destino expresado comúnmente por una fila de caracteres consistente en un nombre de usuario o casilla de correo (llamada *local part*) y una referencia de dominios de Internet (llamada *domain part*), en el cual los mensajes de correo electrónico pueden ser enviados o recibidos.**

DIRECCIÓN DE CORREO ELECTRÓNICO.- Una serie de caracteres utilizados para identificar el origen o el destino de un mensaje de correo electrónico, compuesto por una exclusiva combinación de dos elementos, un nombre o identificador de usuario y el nombre de servidor (de correo electrónico) o de dominio, siendo otorgada y administrada por un proveedor de correo electrónico.
CORREO ELECTRÓNICO COMERCIAL: este término se refiere a todo mensaje, archivo, dato u otra información electrónica enviado con el fin de hacer publicidad, comercializar o tratar de despertar el interés respecto a un producto o servicio

ACUSE DE RECIBO.- Es el procedimiento por el cual se verifica, al momento de recepción por parte del destinatario, la integridad, autenticidad y origen de un mensaje de datos o documento electrónico, y un aviso de recepción del mensaje de datos o documento es enviado por el destinatario del documento.

AUTENTICACIÓN.- Es el medio o procedimiento a través del cual es posible verificar la identidad de un emisor o un destinatario de documentos electrónicos mediante su firma electrónica.

EMISOR.- Persona natural o jurídica a la cual se le atribuye la generación, comunicación o archivo de un mensaje de datos o documento electrónico.

RECEPTOR: toda persona que recibe un correo electrónico comercial no solicitado. A los fines de la presente, este término significa, además, un usuario autorizado de una dirección electrónica al cual el mensaje ha sido enviado

INICIADOR U ORIGINADOR.- Toda persona que, a tenor del mensaje, haya actuado por su cuenta o en cuyo nombre se haya actuado para enviar o generar ese mensaje de ser archivado, si éste es el caso, pero que no haya actuado a título de intermediario con respecto a él.

INFORMACIÓN DE CABECERA: Significa la fuente, destino y ruta de la información adjunta en un correo electrónico, incluyendo el nombre de dominio de origen y la dirección electrónica de origen y toda otra información que aparezca en la línea identificadora, que permite conocer de manera fehaciente el origen real y el camino seguido por el correspondiente correo electrónico

CAMPO DEL ASUNTO: es el área que contiene una breve descripción del contenido del mensaje

PERSONA: Comprende a toda persona física o jurídica

CAPITULO II

PROHIBICION CONTRA SPAM O CORREO

ELECTRONICO NO DESEADO

Artículo 4: Todo SPAM debe de contener la siguiente información y cumplir las condiciones detalladas a continuación

a) La palabra "Publicidad" debe de incluirse al inicio del texto que figure en el Campo del Asunto o "Subject" del mensaje de Correo electrónico no Deseado
b) Los datos de identificación (nombre o denominación social, domicilio completo, teléfono y dirección de correo electrónico de la persona natural o jurídica que emite el mensaje) deben consignarse en la parte inferior del mensaje, incluyendo el nombre de una persona de contacto.
c) Rechazar la recepción de SPAM, con la inclusión de una dirección de correo electrónica de respuesta válida a la que se pueda enviar un mensaje de correo electrónico para notificar su voluntad de no recibir más correos no solicitados,

Articulo 5 (CORREO ELECTRÓNICO COMERCIAL ILEGAL).
El Correo Electrónico Comercial no solicitado será considerado ilegal, dando lugar a las acciones y sanciones que esta ley establece, cuando

a) No cumpla con alguno de los requisitos establecidos en el artículo 4º de la presente ley

b) Contenga el nombre, nombre falso o nombre de dominio de un tercero en el campo de la dirección de respuesta sin autorización de ese tercero;

c) Contenga información falsa que imposibilite identificar el punto de origen del recorrido de la transmisión del correo electrónico;

d) Se envíe o transmita a un receptor que haya formulado el pedido para que no se envíe dicha publicidad, pasados los cinco días hábiles de que el receptor haya remitido el mensaje a que se refiere el artículo 4° inciso c).

e) Contenga información falsa o engañosa en el campo del asunto, que no coincida con el contenido del mensaje.

Articulo 6 (OBLIGACIONES DE LOS PROVEEDORES DE SERVICIO DE CORREO ELECTRÓNICO).

a) Deben de contar con mecanismos anti SPAM para el bloqueo de mensajes que afecten a los usuarios finales del servicio
b) Informar a los usuarios los alcances de los sistemas de filtros y programas de bloqueo así como sus condiciones de uso.
c) Publicar la información referida a las vulnerabilidades que tiene su servicio

Artículo 7 (EQUIPARACIÓN)

a) A los efectos de esta Ley el correo electrónico personal se equipara a la correspondencia postal, estando comprendido dentro del alcance su inviolabilidad establecida en el ordenamiento jurídico vigente. La protección de los mensajes de datos abarca su creación, transmisión y almacenamiento.

b) Se exceptúan de la regulación del inciso a), al correo electrónico laboral que tiene la calidad de herramienta de trabajo, por lo que la información contenida en el mismo y su titularidad le corresponden al empleador, sin tener en cuenta que el nombre y la clave de acceso le pertenecen al trabajador.

c) A efectos del inciso b), el empleador podrá revisar el correo electrónico laboral siempre que medie justa causa para su revisión, y siempre y cuando las características sobre el acceso, condiciones de uso, prohibiciones, entre otros sean establecidas por el empleador y dadas a conocer al inicio de la relación

laboral, o al poner a disposición del trabajador el correo electrónico, mediante documento escrito, debidamente firmado por el trabajador, anterior a la revisión del correo electrónico. En el caso que esto no ocurriera, se entenderá que el correo electrónico es personal

Articulo 8 (DELITOS INFORMÁTICOS).

Se considerará delito informático a las siguientes conductas:

a) Acceder a computadoras protegidas sin autorización, e intencionalmente iniciar la transmisión de mensajes múltiples de correo electrónico comerciales desde o a través de dichas computadoras.

b) Utilizar una computadora protegida para reenviar o retransmitir múltiples mensajes de correos electrónicos con la intención de engañar a los receptores o cualquier acceso al servicio de Internet como procedencia de tal mensaje.

c) Falsificar el asunto del mensaje de un correo electrónico comercial e intencionalmente iniciar la transmisión del mismo.

d) Registrar, usando información que falseara la identidad del registrante por cinco (5) o más cuentas de correo electrónico o dos (2) o más nombres de dominio, e iniciar intencionalmente la transmisión de múltiples correos de mensajes electrónicos comerciales desde cualquier combinación de tales cuentas o dominios.

e) Representar falsamente al registrante o legítimo sucesor del registrante en cinco (5) o más direcciones de protocolo de Internet, e intencionalmente iniciar la transmisión de mensajes múltiples de correos electrónicos comerciales desde tales direcciones.

f) Ofrecer la venta de bases de datos con direcciones de correos electrónicos sin el consentimiento expreso de los propietarios de los mismos

Articulo 9 (PROHIBICIONES).

Quedan expresamente prohibidas las siguientes actividades

a) Uso de medios que permitan facilitar la recolección de direcciones electrónicas sin autorización previa y comercialización de bases de datos.
b) La implementación y uso ilegal de software, sistemas, programas o cualesquiera herramientas que permitan crear, generar, compilar, recolectar, registrar o validar automáticamente direcciones de correos electrónicos sin el consentimiento previo y expreso de los titulares.
c) Generar automáticamente lista de contactos de correo electrónico mediante el empleo de algoritmos u otras herramientas tecnológicas que combinen nombres, caracteres o códigos.
d) Falsear u ocultar cualquier información que permita identificar el punto de origen del recorrido o del trayecto de transmisión del mensaje de correo electrónico comercial no solicitado.
e) Cualquier violación a algún inciso del presente articulo será tipificado como un delito informático del articulo 8 tomando en cuenta la sanción respectiva

Artículo 10 (MODIFICACIONES AL CÓDIGO PENAL)

Se modifica el Código Penal, en los siguientes parágrafos:

a) Sustitúyase el artículo 188 del Código Penal, por el siguiente:
Artículo 188°.- "(EQUIPARACIÓN DE VALORES A LA MONEDA)
A los efectos de la ley penal, quedan equiparados a la moneda:
   1. Los billetes de Banco legalmente autorizados
   2. Los bonos de la deuda nacional
   3. Los valores, cédulas y acciones al portador, emitidos legalmente por los Bancos, entidades, compañías o sociedades autorizados para ello
   4. Los cheques.

   El presente artículo se aplicará también a los instrumentos señalados en los numerales 2, 3 y 4 que se encuentran desmaterializados y representados en documentos electrónicos.

b) Añádase como segundo o tercer párrafo de los artículos 198 (FALSEDAD MATERIAL), 199 (FALSEDAD IDEOLÓGICA) y 200 (FALSIFICACIÓN DE DOCUMENTO PRIVADO) del Código Penal, lo siguiente:

   "El presente artículo se aplicará también a los documentos electrónicos".

c) Sustitúyase el artículo 300 del Código Penal, por el siguiente:

Artículo 300°.- "(VIOLACIÓN DE LA CORRESPONDENCIA Y PAPELES PRIVADOS)

El que indebidamente abriere una carta, un pliego cerrado, correo electrónico o una comunicación telegráfica, radiotelegráfica, telefónica u otros medios electrónicos, dirigidos a otra persona, o el que, sin abrir la correspondencia, por medios técnicos se impusiere de su contenido, será sancionado con reclusión de tres meses a un año o multa de sesenta a doscientos cuarenta días.
Con la misma pena será sancionado el que de igual modo se apoderare, ocultare o destruyere una carta, un pliego, un despacho, correo electrónico u otro papel privado, aunque estén abiertos, o el que arbitrariamente desviare de su destino la correspondencia que no le pertenece.
Se elevará el máximo de la sanción a dos años, cuando el autor de tales hechos divulgare el contenido de la correspondencia y despachos indicados".

d) Sustitúyase el artículo 301 del Código Penal, por el siguiente:
Artículo 301°.- "(VIOLACIÓN DE SECRETOS EN CORRESPONDENCIA NO DESTINADA A LA PUBLICIDAD)
El que grabare, utilizando cualquier método analógico o digital, las palabras de otro no destinadas al público, sin su consentimiento o el que mediante procedimientos técnicos escuchare manifestaciones privadas que no le estén dirigidas, o el que hiciere lo mismo con papeles privados o con una correspondencia epistolar, telegráfica o correo electrónico aunque le hubieren sido dirigidos, siempre que el hecho pueda ocasionar algún perjuicio, será sancionado con privación de libertad de tres meses a un año".

e) Añádase como segundo párrafo del artículo 362 del Código Penal, lo siguiente:
Artículo 362°.- "(DELITOS CONTRA LA PROPIEDAD INTELECTUAL)
"Incurrirá en la misma sanción quién por medios electrónicos obtenga un beneficio indebido y en perjuicio ajeno:

1) El que incorpore por cualquier soporte electrónico una obra protegida sin la correspondiente autorización de los titulares de los derechos de propiedad intelectual o de sus concesionarios.
2) El que almacene definitivamente en un dispositivo interno o externo, o imprima en soporte papel una obra protegida sin la correspondiente autorización de los titulares de los derechos de propiedad intelectual o de sus concesionarios".

f) Sustitúyase el artículo 363 bis del Código Penal, por el siguiente:
"Artículo 363° bis.- (MANIPULACIÓN INFORMÁTICA)

El que con la intención de obtener un beneficio indebido para sí o un tercero, incurra en la realización de una manipulación informática, ocasionando de esta manera una transferencia patrimonial en perjuicio de un tercero, será sancionado con reclusión de uno a cinco años y con multa de sesenta a doscientos días. Se entiende por manipulación informática, toda acción conducente a alterar en su contenido o forma los datos de entrada o de salida, los que se encuentran en proceso, o el proceso mismo de un sistema de información, o los que se encuentran almacenados en una base de datos de cualquier estructura, con el objetivo de obtener un resultado diferente al que se hubiera producido sin la intervención del autor, existiendo intencionalidad por parte del autor y sin la autorización expresa del titular de los datos de referencia."

g) Sustitúyase el artículo 363 ter del Código Penal, por el siguiente:
"Artículo 363° ter.- "(ALTERACION, ACCESO Y USO INDEBIDO DE DATOS INFORMATICOS)
El que sin estar autorizado o haciendo abuso de la autorización, se apodere, acceda, utilice, modifique, suprima, oculte o inutilice, datos almacenados en una computadora o en cualquier soporte informático, o que se encuentren en proceso de transmisión mediante cualquier sistema electrónico y/o informático de datos, ocasionando perjuicio al titular de la información o a un tercero u obtenga beneficio indebido, será sancionado con reclusión de seis meses a dos años".

h) Inclúyase como artículo 363 quater del Código Penal, el siguiente:
"Artículo 363° quater.- (FALSIFICACIÓN Y SUPLANTACION DE IDENTIDAD ELECTRÓNICA)
Será sancionado con reclusión de uno a seis años, el que causando perjuicio ajeno u obteniendo beneficio para sí o un tercero:
a) Simule o altere un mensaje de datos en todo o en parte, utilizando una identidad fisica o electrónica que no le pertenece.

b) Altere el contenido de un mensaje de datos en algunos de sus elementos o etapas de transmisión.

c) Intercepte, interfiera y/o altere el proceso mismo de transmisión del mensaje de datos entre los titulares de origen y destino del mismo.

i) Inclúyase como artículo 363 quinquies del Código Penal, el siguiente:
"Artículo 363° quinquies.- (SABOTAJE INFORMÁTICO)
Quien obstaculice, modifique o atente contra el normal funcionamiento de un sistema de información, impidiendo la ejecución de sus funciones, o haciendo más lentos los mismos, mediante recursos fisicos o lógicos; incurrirá en privación de libertad de uno a tres años".

j) Inclúyase como artículo 363 septies del Código Penal, el siguiente:
"Artículo 363 septies.- (DISPOSICIÓN COMUN)
En los casos previstos por este Título, cuando fueren autores servidores públicos o las personas encargadas por su oficio o profesión de la administración de un sistema de información, se impondrá la sanción con privación de libertad de tres a seis años".

Articulo 11(MODIFICACIONES CÓDIGO CIVIL)

b) Sustitúyase el articulo 19 del código civil por el siguiente:

Art. 19.- (INVIOLABILIDAD DE LAS COMUNICACIONES Y PAPELES PRIVADOS).
i. Las comunicaciones, la correspondencia epistolar el correo electrónico y otros papeles privados son inviolables y no pueden ser ocupados sino en los casos previstos por las leyes y con orden escrita de la autoridad competente. (Art. 301 Código Penal).
ii. No surten ningún efecto legal las cartas y otros papeles privados que han sido violados o sustraídos, ni las grabaciones clandestinas de conversaciones o comunicaciones privadas.- (Art. 20 Const. Pol. del Estado, Art. 30o Código Penal)

Articulo 12 (SANCIONES).

La comisión de los hechos previstos en el artículo 8, dará lugar a la aplicación de las siguientes sanciones:

a. Cuando el hecho haya sido cometido por personas físicas:

i. Se sancionara de acuerdo a la modificación de los incisos del articulo 10 de la presente ley, las sanciones serán producto de las modificaciones del código penal

b. Cuando el hecho haya sido cometido por los directores, administradores, gerentes, mandatarios, gestores o miembros de una o varias personas de existencia ideal, con los medios o recursos facilitados por la misma u obtenidos de ella con tal fin, de manera que el hecho resulte cumplido en nombre, con la ayuda o en beneficio de la persona ideal, se impondrá:

Serán sancionados con los artículos 363° bis.- (MANIPULACIÓN INFORMÁTICA), 363° ter ALTERACION, ACCESO Y USO INDEBIDO DE DATOS INFORMATICOS), 363° quinquies.- (SABOTAJE INFORMÁTICO)

c. Las personas físicas o de sentencia ideal condenadas a penas de multa, Artículo 301°.- "(VIOLACIÓN DE SECRETOS EN CORRESPONDENCIA NO DESTINADA A LA PUBLICIDAD).

d. Cuando la comisión de los hechos tipificados como guardar las direcciones de correo electrónico de clientes, adherentes o cualquier otra vinculación comercial y/o social, el mínimo y el máximo de la pena pertinente se evaluara de acuerdo al "Artículo 363° ter.- "(ALTERACION, ACCESO Y USO INDEBIDO DE DATOS INFORMATICOS) y Artículo 300°.- "(VIOLACIÓN DE LA CORRESPONDENCIA Y PAPELES PRIVADOS)