Políticas para el Buen Uso de las Redes

EXPOSICION DE MOTIVOS

La Cámara Venezolana de Comercio Electrónico (Cavecom-e) y la Cámara de Empresas de Servicios de Telecomunicaciones (CASETEL) promovieron una iniciativa para investigar y desarrollar un conjunto de mejores prácticas para fomentar el buen uso de las redes.

Para esto, se conformó una Comisión integrada por un grupo de trabajo de carácter permanente, en el que participaron algunas de las empresas que tienen interés o se ven afectadas por los problemas generados por la mala utilización y actos hostiles en la operatividad de las redes.

En esta Comisión participaron activamente representantes tanto de los Proveedores de Servicios de Internet (ISP) y Proveedores de Envío de Mensajes Electrónicos (PEME), así como otras empresas de mercadeo electrónico. Dicho grupo de trabajo estuvo conformado por: CANTV, Dayco Telecom (Dayco Host), Etheron, Expomarketing, Génesis Telecom, Imolko, IP Net, Net Uno y Telcel.

Es así, que la motivación de este documento es identificar soluciones prácticas y seguras, a los fines de: i) informar a los usuarios de las redes sobre el buen uso de las mismas ii) proteger las redes iii) establecer las mejores prácticas para el uso de las redes, el envío de mensajes masivos en general y la comercialización de productos y servicios iv) investigar permanentemente las modalidades de uso de las redes con el objeto de identificar las prácticas que puedan considerarse como nocivas, en perjuicio de los operadores y usuarios, a fin de fomentar el desarrollo de mecanismos que las impidan.

Estas políticas procuran el desarrollo de los derechos que le acredita la Ley Orgánica de Telecomunicaciones en cuanto el uso y protección de sus redes e instalaciones empleadas en la prestación de sus servicios, así como, el deber, con arreglo a la misma disposición, de respetar los derechos de los usuarios establecidos en la Constitución y en las leyes; en contar con una información adecuada y no engañosa sobre el contenido y características de los productos y servicios que consumen, sobre la base de la libertad de elección y un trato equitativo y digno y proveer de un servicio de calidad.

Este documento, servirá de referencia o complemento para el establecimiento de las prácticas y políticas de uso particulares de cada empresa.

Este documento desarrollará solo al spam y enumerará las otras formas de práctica que afectan las redes. En una segunda fase del trabajo de la Comisión, se desarrollarán las políticas y recomendaciones para otro tipo de prácticas.

OBJETIVOS

Artículo 1:

Los objetivos generales de estas políticas son:

1. Fomentar las mejores prácticas para el buen uso de las redes en las empresas venezolanas.
2. Establecer mecanismos que permitan educar a los usuarios para el buen uso de las redes.
3. Incorporar mecanismos de intercambio de información para incrementar la efectividad de la implantación de estas mejores prácticas.

Los objetivos específicos de estas políticas son:

1. Definir las prácticas que deben ser consideradas como actos hostiles en la operatividad de las redes y proponer recomendaciones para su tratamiento.
2. Definir políticas de investigación y desarrollo entre los participantes de este grupo de trabajo, para ayudar a disminuir las prácticas hostiles en el uso de las redes.
3. Considerar la creación de un registro de empresas PEME para evaluar y certificar el cumplimiento de las mejores prácticas en el uso de las redes.
4. Designar subcomisiones de trabajo que velarán por el cumplimiento de las políticas aceptadas, así como la recepción, canalización y seguimiento de las quejas de los usuarios.
5. Establecer canales de comunicación con los usuarios en general, a fin de mantenerlos informados acerca de las acciones y efectos que tendrán las recomendaciones dadas por la Comisión sobre su servicio.

AMBITO DE ACCIÓN

Artículo 2:
Las políticas para el buen uso de las redes será aplicable a personas naturales y/o jurídicas en el ejercicio de cualquier tipo de actividad que se efectúe a través de las redes.

OBJETOS DE ESTUDIO Y ATENCIÓN

Artículo 3:
A los fines de estas políticas, se presume como malas prácticas:

1.- Spam

Se entiende por spam:
Toda comunicación electrónica enviada en forma masiva y no solicitada.

Entendiendo como:

- *envío masivo:* Cuando ésta se envía en lotes o puede inferirse razonablemente que existe más de un destinatario.
- *no solicitado:* Cuando el destinatario no ha otorgado de forma verificable, deliberada, explícita y revocable, el permiso para recibir la comunicación.

2.- MALWARE:
Son programas informáticos que ejecutan tareas fuera del control del usuario, con propósitos hostiles, malignos, peligrosos o dañinos. De acuerdo a su naturaleza y a las acciones que estos programas ejecutan, se pueden clasificar en:

i. **Adware**: programas que ejecutan secuencias de ciertas páginas Web, a fin de desplegar información no solicitada (publicidad).
ii. **Spyware:** programas que capturan información sobre las actividades del usuario y la reportan a su centro de operación.
iii. **Virus, Gusanos, Troyanos y similares:** programas que al ejecutarse tienen la capacidad de dañar parcial o totalmente la data, hardware y software o incluso facilitar el acceso a terceros de forma remota.

3.- ATAQUE A LA RED Y/O CUALQUIERA DE SUS ELEMENTOS
Acción ejecutada para explotar una vulnerabilidad en la red y/o cualquier de sus elementos.

4.- BARRIDO DE PUERTOS NO SOLICITADO:
Acción de buscar vulnerabilidades explotables remotamente para poder acceder a un sistema sin el debido consentimiento del usuario.

5.- RELAYS ABIERTOS Y PROXIES ABIERTOS:
Son servicios que al estar mal configurados pueden ser utilizados como puente para alcanzar otros destinos a fin de cometer actos hostiles.

6.- SPOOFING:
Es la usurpación o falsificación de la identidad de un elemento de red, a fin de cometer actos hostiles.

7.- Cualquier otra práctica existente o por existir considerada perjudicial o que conforme un acto hostil en el uso de las redes.

RECOMENDACIONES EN EL MANEJO DE LISTAS DE CORREO PARA COMBATIR EL Spam

Artículo 4: Se recomienda como buen manejo de las listas de correo, aquellos envíos que cumplan con las siguientes condiciones:

1. *Envíos Segmentados*: que el PEME u originador de la información demuestre un esfuerzo razonable para asegurar que el mensaje sea de interés para el destinatario.

2. *Envíos Personalizados*: que el PEME u originador de la información demuestre un esfuerzo razonable para asegurar que la comunicación contenga elementos que identifiquen individual y personalmente al destinatario.

3. *Envíos Autorizados*: la comunicación se envía de acuerdo a una autorización cuya evidencia consta en los registros del PEME u originador. Cada mensaje debe hacer referencia al mecanismo a través del cual, el destinatario pasó a formar parte de esa base de datos de suscripciones. El proceso de autorización incluye una confirmación para garantizar el consentimiento del destinatario final, previo al inicio del envío del mensaje.

4. *Envíos Identificados*: que el PEME u originador de la información demuestre un esfuerzo razonable para asegurar que los datos de contacto del remitente, incluyan: el nombre de la empresa y de la persona responsable en caso que sea persona jurídica, así como, la dirección física y el teléfono de contacto, lo cual deber ser parte de cada uno de los mensajes enviados al destinatario.

5. *Envíos Removibles*: el destinatario puede, en cualquier momento y sin intervención de la discrecionalidad de ningún tercero, removerse de las bases de datos del remitente, y ser eliminado en un período no mayor a dos días hábiles.

RECOMENDACIONES TÉCNICAS PARA LA CONFIGURACIÓN DE SERVIDORES DE CORREO.

Artículo 5: A los fines de reducir el envío de spam a través de las redes, los ISPs podrán poner en práctica las siguientes recomendaciones:

1. Configurar los *"relays"* y los *"proxies"* para evitar su mal uso.

2. Activar la opción de validación por zona reversa en el servidor de correo entrante. Esta opción permite confirmar la existencia del dominio desde donde se origina el correo, ya que gran parte del spam proviene de nombres de dominios forjados o no válidos.

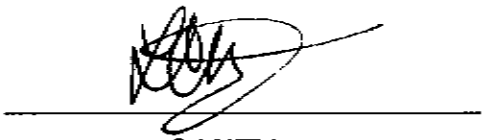
3. Implementar mecanismos que eviten actos hostiles que afecten la operatividad de los servicios de mensajería, como por ejemplo:
   - Uso de SMTP con autenticación, para prevenir el acceso a usuarios no autorizados al envío de correo.
   - Bloqueo de los envios directos a otros servidores SMTP, desde espacios dinámicos de la red.
   - Implantación de software anti-viral que revise tanto los mensajes de correo salientes como los entrantes, descartando en línea los mensajes contaminados, sin generar NDRs.

COMPROMISOS DE LOS ISPs EN LA PRESTACIÓN DEL SERVICIO

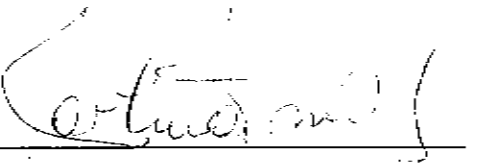
Artículo 6: A los fines de garantizar la difusión por parte de los ISPs de las Políticas de Investigación y Desarrollo para el Buen Uso de las Redes, así como las condiciones particulares que son aplicables por cada ISP a sus usuarios, estos deberán:

1. Difundir y poner al alcance de todas las personas naturales o jurídicas que contraten sus servicios, las Condiciones de Uso de sus redes.
2. Monitorear el tráfico de la red a fin de detectar posibles generadores de spam.
3. Recibir, procesar y responder las denuncias sobre la recepción spam y/o cualquier otro acto hostil, notificando en la medida de la posible a las partes involucradas.
4. Garantizar la confidencialidad de la información provista por los usuarios a sus proveedores de servicios contratados.
5. Hacer de conocimiento público, a través de los URL específicos de cada uno de los miembros de la Comisión para el Buen Uso de las Redes, las presentes políticas; así como las actualizaciones y modificaciones realizadas a este en cualquier momento.
6. Incorporar mecanismos de intercambio de información con los usuarios en los cuales estos puedan ofrecer sus opiniones en referencia a los asuntos relacionados con las Condiciones de Uso.
7. Utilización y actualización regular de software antiviral, para los servidores instalados en la plataforma del proveedor y en especial para los servidores de correos; así como la configuración de los *firewalls* para que filtren puertos y protocolos adecuadamente.
8. Informar a los usuarios de la necesidad de software de antivirus, *firewall* personal y disponer de las últimas actualizaciones de seguridad en sus estaciones conectadas directamente a Internet.

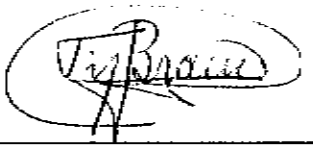
Estas políticas se presentaron en Caracas a los veintiséis (26) días del mes de Octubre de 2004.



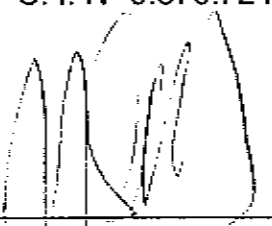
CANTV
Luis Muñoz
Gerente Corporativo de Seguridad de la Información
C. I. N° 11.308.811



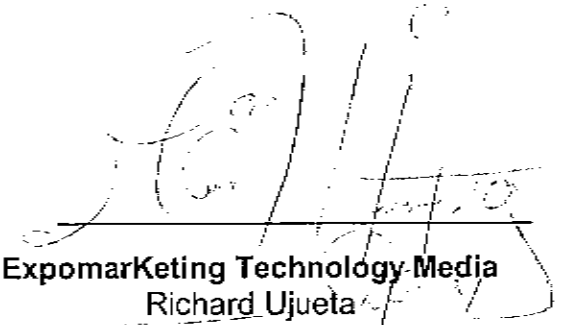
CANTV.NET
Carolina Tomic
Coordinadora de Asuntos Regulatorios
C. I. N° 9.878.724



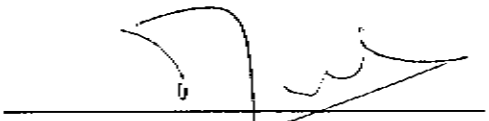
Dayco Telecom
Tijelino Bravo
Vicepresidente de Operaciones
C. I. N° 4.744.312



Etheron Servicios C. A.
José Joaquín Soarez
Gerente General
C. I. N° 9.969.226

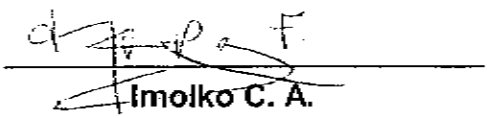


ExpomarKeting Technology Media
Richard Ujueta
Presidente
C. I. N° 5.520.230



Genesis Telecom C. A.
Victoria Zerolo
Vicepresidente de Ventas, Servicios y Mercadeo
C. I. N° 5.610.616

Imolko C. A.
Francisco Andrés A.
Presidente
C. I. N° 4.765.074



Imolko C. A.
Moisés Ramírez
Director Ejecutivo
C. I. N° 4.387.085

IPNet
Carlos Salas
Director Técnico
C. I. N° 6.562.421

Telcel, C. A.
Haydée Cisneros de Salas
Vicepresidente de Comunicaciones Corporativas
C. I. N° 3.150.388

NetUno
Alberto Scharffenorth
Vicepresidente Corporativo y Asuntos Regulatorios
C. I. N° 5.310.685

NetUno
Gregorio Manzano
Supervisor de Operaciones IP
C. I. N° 6.692.732

Cámara de Empresas de Servicios de Telecomunicaciones (Casetel)
Ricardo Baquero Aristeguieta
Presidente
C. I. N° 1.740.206

Cámara Venezolana de Comercio Electrónico (Cavecom-e)
Francisco J. Briceño C.
Presidente
C. I. N° 5.967.440