Autoridad de Acueductos y Alcantarillados

ESTADO LIBRE ASOCIADO DE PUERTO RICO

OFICINA DEL PRESIDENTE EJECUTIVO

ORDEN ADMINISTRATIVA

NÚMERO: OA-2011-02

DISTRIBUCIÓN: "D"

FECHA: 13 de julio de 2011

ASUNTO: POLÍTICA DE MANEJO DE CORREO ELECTRÓNICO

PROPÓSITO:

El propósito de esta política es ofrecer las guías necesarias para el buen uso y manejo del correo electrónico en la Autoridad de Acueductos y Alcantarilladlos (AAA).

EXPOSICIÓN DE MOTIVOS:

Esta política es aplicable a todos los empleados y contratistas de la AAA con acceso a una cuenta de correo electrónico en los sistemas de información de la AAA.

DEFINICIONES DE TERMINOS:

1. Correo electrónico – es un servicio de red que permite a los usuarios enviar y recibir mensajes mediante sistemas de comunicación electrónicos.

2. Contraseña – es una forma de autenticación que utiliza información secreta para controlar el acceso hacia algún recurso. La contraseña tiene que mantenerse en secreto.

3. File Transfer Protocol (FTP) – herramienta electrónica para transferir archivos electrónicos.

4. Mensaje en cadena – consiste en un mensaje que intenta inducir al receptor a realizar algún número de copias del mismo para luego pasarlos a uno o más receptores nuevos.

5. SPAM – mensajes no solicitados, no deseados o de remitente desconocido, habitualmente de tipo publicitario, enviados en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptor.

6. Usuario- persona que utiliza un sistema de información.

7. Virus – es un programa que tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o el conocimiento del usuario. Los virus, habitualmente, reemplazan archivos ejecutables por otros infectados con el código de éste.

DETERMINACIÓN:

1. El servicio de correo electrónico de la AAA es parte integral de sus sistemas de información, por lo que la AAA se reserva el derecho absoluto de intervenir, monitorear e investigar para constatar el uso adecuado del mismo.

2. La AAA se reserva el derecho de acceder y divulgar el contenido de los mensajes creados, recibidos y/o enviados a recipientes internos o externos.

3. Toda información catalogada como confidencial, privada o sensitiva no podrá ser divulgada sin la previa autorización de la AAA.

4. El servicio de correo electrónico será administrado en una herramienta debidamente autorizada por la AAA.

5. El acceso al correo electrónico estará controlado mediante la utilización de contraseñas.

6. La herramienta para administrar el correo electrónico contará con un mecanismo automatizado que permitirá la retención de los correos, configurado para ejecutarse cada quince (15) días. Cuando el mecanismo automatizado no pueda ser utilizado, existirán alternativas de configuración manual para establecer la retención de los correos.

7. Las comunicaciones en los correos electrónicos deben ser breves, para evitar el congestionamiento de la red y el mal uso del tiempo del personal. Si es imprescindible enviar bastante información porque el tema lo justifica, se debe insertar como documento.

8. La capacidad máxima de los correos electrónicos estará limitada a 10 *megabytes* (10mb). Toda información mayor de esta capacidad deberá ser enviada mediante métodos alternos de transmisión de información como lo es el servicio de *File Transfer Protocol* (*FTP*).

9. Sólo se deben ***marcar como urgente*** los correos electrónicos que realmente lo son.

10. Los correos electrónicos deben ser dirigidos solamente a las personas que requieran la información.

11. Se debe hacer buen uso de las agrupaciones que contiene la libreta de direcciones. A tales efectos, las libretas de direcciones y las agrupaciones oficiales deberán estar restringidas y controladas por los mecanismos de seguridad que provee la herramienta de correo electrónico.

12. El usuario podrá crear libretas de direcciones individuales y agrupaciones dentro de su cuenta de correo, y deberá cumplir con el buen uso de las mismas. El usuario es responsable de mantener actualizada su propia libreta de direcciones.

13. La información que se recibe de manera personal y confidencial por correo electrónico no puede ser enviada a otra persona, sin la autorización del remitente.

14. La persona que envía el correo electrónico es responsable del contenido del mismo, considerando que la información enviada es irreversible.

15. El usuario es responsable de todas las actividades realizadas con sus cuentas de acceso y su buzón asociado a nuestra Corporación.

16. Todo usuario que utiliza el servicio de correo electrónico será notificado sobre las mejores prácticas en el uso del mismo. (ver Apéndice)

17. El servicio de correo electrónico de la AAA será utilizado solamente para propósitos profesionales relacionados con sus responsabilidades en la Autoridad y ningún usuario debe tener expectativa de privacidad sobre la información contenida en los correos recibidos y enviados. El Departamento de Sistemas de Información se reserva el derecho de monitorear y asegurar el cumplimiento de toda política de seguridad establecida para el servicio de correo electrónico.

18. Cada correo electrónico que sea enviado a recipientes fuera de la AAA incluirá un mensaje de descargo de responsabilidad o "disclaimer".

19. El usuario se compromete a dar aviso al Oficial Principal de Seguridad Informática o su representante autorizado de cualquier fallo de seguridad que afecte el funcionamiento del correo electrónico y/o del cumplimiento con esta política.

20. La delegación de una cuenta de correo electrónico a otra persona está totalmente prohibido. Sin embargo, y de ser necesario, esta delegación puede ocurrir en apoyo al personal ejecutivo, en el cual se puede delegar la cuenta a su asistente administrativo.

21. El Departamento de Sistemas de Información es la entidad responsable de vigilar el cumplimiento, mantenimiento y actualización de esta política.

Actividades Prohibidas:

La AAA se reserva el derecho de establecer, modificar o eliminar las actividades prohibidas concernientes a la utilización y manejo del correo electrónico. Las actividades contempladas en esta política son:

1. Se prohíbe utilizar el correo electrónico para propósitos personales o comerciales ajenos a la AAA. Esto incluye, pero no se limita a fines políticos, religiosos, personales, sentimentales, comerciales, juegos, ventas y demás actividades no autorizadas.

2. Se prohíbe participar en la propagación de *mensajes en cadenas* y en esquemas piramidales dentro y fuera de la AAA.

3. Se prohíbe distribuir de forma masiva grandes cantidades de mensajes con contenidos inapropiados para la AAA que atenten contra el buen funcionamiento del servicio de correo electrónico.

4. Se prohíbe enviar o reenviar mensajes con contenido difamatorio, ofensivo, racista u obsceno.

5. Se prohíbe utilizar seudónimos y enviar mensajes anónimos, así como aquellos que consignen títulos, cargos o funciones no oficiales.

6. Se prohíbe utilizar mecanismos y sistemas que intenten ocultar o suplantar la identidad del emisor de correo.

7. Se prohíbe enviar correos SPAM de cualquier índole.

8. Se prohíbe intentar modificar los sistemas y parámetros de seguridad con la intención de acceder de manera no autorizada una cuenta de correo ajena.

Se prohíbe en todo momento enviar información oficial de la AAA a través de cuentas de correo electrónico no autorizadas por la AAA, tales como: gmail, hotmail, AOL, entre otras.

VIGENCIA:

Esta Orden Administrativa tiene vigencia inmediata y deja sin efecto todas las comunicaciones que se hayan cursado sobre este asunto.

APROBADO POR:

Ing. José F. Ortiz Vázquez
Presidente Ejecutivo

12/23/2011
Fecha de Aprobación

MEJORES PRÁCTICAS EN EL USO DEL CORREO ELECTRÓNICO

APÉNDICE OA-2011-02

Tomado y adaptado de: arsys.es
julio 2011

TABLA DE MATERIAS

Página

Propósito 3
Alcance 3
Mejores prácticas generales 3
Mejores prácticas en la recepción de correo electrónico 4
Mejores prácticas en el envío de correo electrónico 4
Mejores prácticas en la realización de envíos masivos 6

Propósito

El propósito de este documento es dual, por un lado, pretende informar a los usuarios de las medidas que pueden tomar para evitar ser víctimas del spam. Por otro lado, pretende dar una serie de sencillas pautas para no incurrir en dicha práctica.

Alcance

La práctica del *spam* constituye un verdadero problema que afecta de forma negativa a todos los usuarios de Internet. Dicha práctica consiste en la realización de envíos masivos no solicitados, generalmente de comunicaciones de carácter comercial. El medio a través del cual se realiza más frecuentemente es el correo electrónico, aunque también tiene lugar a través de otros, tales como: mensajes de texto a móviles, publicaciones en foros, etc.

Tanto la legislación vigente como nuestra orden administrativa prohíben de forma expresa la realización de spam.

Confiamos en que este documento *mejores prácticas* pueda ser de utilidad y contribuya a evitar, en todo lo posible, el envío y recepción masivos de correos electrónicos no solicitados.

Mejores prácticas generales

1. Mantenga al día de parches y actualizaciones el sistema operativo y aplicaciones instaladas en el ordenador (especialmente el antivirus). Muchos virus se aprovechan de esas vulnerabilidades para infectar los equipos.

2. El tamaño de su buzón de correo es limitado. Debe controlar asiduamente su buzón de correo a fin de evitar que este se quede sin espacio libre. Este cuidado no sólo lo agradecerán quienes remiten los e-mails sino también el propio servidor de correo y su propio equipo. En este sentido, conviene borrar periódicamente aquellos correos de poca importancia como acuses de recibo, o aquellos que proporcionaron la información, cumplieron su cometido y ya no son necesarios, así como e-mails no deseados (SPAM). Elimine mensajes (descargue los adjunto se imprima el contenido del mensaje si lo necesita) y vacíe la papelera y la carpeta de correos enviados siempre que sea posible.

3. Proteja las claves asociadas a los buzones de correo electrónico, evitando su divulgación a terceras personas. En caso de pérdida o robo de sus claves de correo, el usuario deberá cambiarla lo antes posible.

4. Debe proporcionar la dirección de correo con moderación. Utilice, siempre que sea posible, una cuenta gratuita para el registro en páginas web, ya que podrían enviar publicidad no deseada.

Mejores prácticas en la recepción de correo electrónico

1. No acepte documentos ni archivos adjuntos provenientes de desconocidos o que tengan un origen poco fiable. Debe prestar atención a correos electrónicos con datos adjuntos susceptibles de contener virus.

2. Algunos mensajes pueden aparecer como provenientes de otra persona distinta del autor. Aplique su sentido común antes de asumir que un mensaje es válido.

3. No abra o ejecute directamente los documentos o ficheros adjuntos. Es mucho más seguro extraerlos previamente a un directorio del ordenador y analizarlos con un buen antivirus.

4. No confíe en regalos y promociones de fácil obtención. En ocasiones la infección de su equipo se puede producir al visitar una página Web facilitada en un correo aparentemente inofensivo.

5. Desconfíe de los correos de supuestas entidades bancarias que le solicitan introducir o modificar sus claves de acceso. No es la forma de proceder de las entidades legítimas y probablemente se trate de un intento de fraude. Ante cualquier duda póngase en contacto con su entidad.

Mejores prácticas en el envío de correo electrónico

1. Incluya un "Asunto" en el mensaje. Indique en dicho campo una breve frase descriptiva del mismo. Esto facilita la lectura, clasificación y posterior recuperación al destinatario y constituye una norma de cortesía.

2. Utilice las mayúsculas y minúsculas correctamente. No se debe escribir todo el texto del mensaje en mayúsculas, ya que implica GRITAR. En la medida de lo posible, limite el uso de letras mayúsculas en el texto del correo. Si desea enfatizar un término, puede usar comillas, negrita, otros colores, etc. Si estima que la letra es muy pequeña, puede agrandar la letra hasta un tamaño que resulte más conveniente, pero no extravagante. El uso de mayúsculas en Internet sugiere emociones fuertes. Tenga esto en cuenta.

3. No utilice estilos con fondos de mensaje, ya que aumentan el tamaño del mismo y pueden provocar problemas de recepción en el destinatario (filtrado por el sistema antivirus-anti spam).

4. Debe tener cuidado con el tamaño de los mensajes. Incluir documentos de gran tamaño, imágenes o programas puede hacer su mensaje tan pesado que tenga problemas de recepción, así como un consumo de recursos innecesarios al receptor del mensaje. Cuando envíe un adjunto se debe indicar en el mensaje cuáles su contenido y su propósito para evitar que el destinatario sospeche que se trata de un virus. Asimismo es recomendable comprimirlos siempre que sea posible.

5. Las aplicaciones Internet hay que conocerlas y usar cada una para la finalidad con la que fueron diseñadas. El correo electrónico debe ser usado con tamaños de mensajes moderados pues para tamaños grandes es más útil usar otros medios (cuentas FTP, por ejemplo). El correo electrónico no es el mecanismo adecuado ni eficiente para transferir ficheros.

6. Las firmas automáticas deben ser lo más esquemáticas posible, tratando de evitar imágenes o información innecesaria.

7. No facilite datos personales o financieros a personas desconocidas.

8. No se debe responder al correo no solicitado (spam). Responder al correo comercial no solicitado es una forma de aumentar la cantidad de correo basura ya que indica al remitente que la cuenta es leída.

9. No debe enviar publicidad, a no ser que el receptor esté de acuerdo en recibirla.

10. Debe evitarse el participar en el reenvío de correo no solicitado (cadenas de mensajes, rumores, publicidad, etc.). Las casas comerciales y centros de alerta legítimos tienen como norma redirigir a servidores Web donde dan información de forma fiable y detallan las acciones a tomar.

11. Se debe respetar la privacidad de los mensajes y el destinatario. No reenvíe mensajes destinados a usted sin el permiso del remitente, sobre todo aquellos con contenido conflictivo o confidencial.

12. No debe abusarse de funcionalidades como el "aviso de lectura", su eficacia es escasa cuando lo utilizamos de manera indiscriminada o continuada, llegando a molestar al remitente. Se debe activar sólo en los casos en los que realmente sea necesario.

Mejores prácticas en la realización de envíos masivos

1. Si necesita realizar envíos masivos haga uso de las herramientas diseñadas para ello (listas de distribución) o realice un diseño a medida de su aplicación de forma que se cumplan las recomendaciones que citamos en los apartados siguientes.

2. Divida los destinatarios en varios grupos o listas de distribución de forma que el volumen de correo quede repartido de forma equitativa. Mejor cuantos más grupos y menor número de destinatarios por grupo. Recuerde que hay proveedores de correo con sistemas de monitorización que chequean el número de correos que reciben desde una determinada IP o remitente.

3. Realice los envíos en horas valle y espaciando los envíos entre grupos.

4. Realice un mantenimiento periódico de los usuarios suscritos a sus listas, tratándose evitar suscripciones no deseadas, direcciones de correo sospechosas, y direcciones de correo que rebotan constantemente los correos que les envía.

5. Asegúrese que el proceso de suscripción a sus listas de distribución cuenta con el mecanismo de confirmación necesario para verificar el deseo expreso del destinatario por pertenecer a ellas.

6. Revise los posibles correos de abuso relacionados con envíos que haya realizado, así como los emails devueltos y estudie las posibles causas.

7. Incluya en cada uno de sus envíos masivos las instrucciones necesarias para que un destinatario pueda darse de baja de su lista de distribución.

8. Realice sus envíos con la periodicidad necesaria o permita a sus usuarios elegir cada cuanto tiempo desean recibirlos.

9. Asegúrese que para sus usuarios es fácil ponerse en contacto con usted.

10. Nunca ponga su lista completa de destinatarios en el campo "To" o "CC" por dos razones fundamentales:

    a. Todas las personas en el campo "To" o "CC" pueden ver las direcciones de email en esos campos y podrán usarlas en la forma que ellos deseen.
    b. Si alguien decide "Responder a todos", todas las direcciones en los campos "To" o "CC" recibirán la respuesta.