RACEv2: Red Avanzada de Correo Electrónico

Criterios de calidad para la creación de un red avanzada de confianza

Apéndice A. Movilidad en el Correo Electrónico

Comité RACEv2 V2.2

11/03/2008

RACEv2: Red de Calidad de Correo Electrónico
Criterios de calidad para la creación de una red de confianza

Estado de este memorando

Este documento especifica unas "Mejores Prácticas Actuales", Best Current Practices (BCP), para la comunidad RedIRIS, y solicita su discusión y sugerencias para mejorarlas que puede hacer enviándolas a la dirección race@rediris.es

La distribución de este memorando es ilimitada.

Terminología

Las palabras clave "DEBE", "NO DEBE", "OBLIGATORIO", "DEBERÁ", "NO DEBERÁ", "DEBERÍA", "NO DEBERÍA", "RECOMENDADO", en este documento serán interpretadas como se describe en el RFC 2119 (Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels,” March1997.) [RFC2119].

Resumen

Este documento tiene como objetivo exponer las mejores recomendaciones para diseñar, configurar y gestionar un Servicio de Correo Electrónico desde el punto de vista de la excelencia en la calidad del servicio ofrecido tanto a los usuarios locales de una organización, como al resto de entidades con las que se intercambia tráfico SMTP.

Estas recomendaciones se estructuran en criterios de calidad, clasificados según su ámbito de aplicación y asignados a diferentes niveles, que permitirán medir la calidad del Servicio de Correo Electrónico de una organización, y promover la mejora del mismo

Apéndice A. Movilidad en el Correo Electrónico

El correo electrónico es el nexo fundamental entre los usuarios que se desplazan y su institución de origen. Por tanto el servicio que se les ofrezca es de gran importancia. Los usuarios móviles pertenecen a dos grandes grupos: el viajero ocasional y los viajeros frecuentes o 'guerreros de la carretera', por seguir el nombre que reciben en muchas publicaciones. Los servicios demandados por cada tipo de usuario son muy distintos. La premisa que debería marcar la política de acceso a nuestro Servicio es:

"Ningún servicio no seguro de nuestra institución debería pasar por redes que no son gestionadas por nosotros"

Es decir todos los servicios de nuestra institución deberían ser seguros usando cifrado TLS, sobre todo cuando se utilizan a través de redes no gestionadas por nosotros como es el caso del acceso móvil al servicio de correo electrónico.

Servicios para el viajero occasional:

Este tipo de usuarios requiere un servicio muy básico que les permita revisar con rapidez el correo por si han recibido un mensaje urgente y contestar o escribir una cantidad mínima de mensajes.

El servicio básico de correo electrónico en movilidad se presta de forma más que adecuada con un buen servicio de WebMail. Es RECOMENDABLE que el acceso al servidor de WebMail se realice con protocolo **cifrado HTTPS** (criterio 21 (Criterio 21: Acceso remoto por WebMail y otros)) y, MUY RECOMENDABLE, con certificados firmados por una autoridad certificadora reconocida por todos los navegadores, para evitar problemas con el navegador que el usuario desplazado se vea obligado a utilizar.

También es RECOMENDABLE disponer de un servicio WebMail adaptado a dispositivos móviles, que discrimine los navegadores de estos dispositivos y les presente un interfaz simplificado, en lenguajes de marcado adaptados (cHTML, WML, etc).

Servicios para el viajero frecuente:

Aunque algunos de estos usuarios pueden también manejar su correo desde ordenadores ajenos con el servicio de WebMail, normalmente suelen viajar con un ordenador portátil y un cliente de correo pesado con la misma configuración de su ordenador de sobremesa o incluso con todo su correo en el portátil.
Este tipo de usuario necesita habitualmente los mismos servicios que un usuario que se encuentra en la institución, es decir, acceso al buzón y la posibilidad de enviar mensajes a través del MTA de su institución para evitar problemas con la dirección de origen.

El acceso al buzón DEBERÍA hacerse con protocolos cifrados POP3s o IMAPs (criterio 21 (Criterio 21: Acceso remoto por WebMail y otros)). El uso de IMAP es más útil para este tipo de usuarios ya que permite mantener los mensajes centralizados en el buzón del servidor de su institución, incluida la carpeta de mensajes enviados. Además, este planteamiento permite utilizar diversos clientes, incluido WebMail o dispositivos móviles.

El envío de mensajes a través de la MTA de la institución de origen se debería realizar por medio de SMTP autenticado y, preferiblemente, cifrado. Para este uso se recomienda el servicio *submission* (587) en lugar del servicio SMTP estándar (25), que debería quedar para comunicaciones entre MTAs (criterio 15 (Criterio 15: Servicio SUBMISSION)).

Otro enfoque es utilizar el servicio VPN (Virtual Private Network) (mencionado en el criterio 21 (Criterio 21: Acceso remoto por WebMail y otros)) de nuestra institución para acceder al correo electrónico a través de los mismos puertos seguros. El usuario podrá acceder a su correo a través de los mismos puertos locales habituales y securizados.

La siguiente RECOMENDACIÓN puede aplicarse al acceso universal al correo electrónico en las instituciones miembros de RedIRIS:

"Se debería ofrecer el acceso al correo a través de los canales seguros de los puertos POP3s, IMAPs, SMTPs y HTTPs"

Para que todos los usuarios de la Comunidad RedIRIS puedan acceder a su servicio de correo independientemente de su ubicación, todas las instituciones deberán respetar estar recomendación:

‘‘*Habilitar en el router la entrada/salida hacia/desde los puertos seguros: POP3s (995), IMAPs (993) y SMTPs (587)”*

POP3S: 995 Acceso seguro POP3

IMAPs: 993 Acceso al buzón

Submission: 587 Envío de mensajes autenticados.

HTTPS: 443 Acceso seguro al servicio de WebMail

Es RECOMENDABLE deshabilitar en el router el acceso desde el exterior a los puertos no seguros de POP/IMAP (110/143) y SMTP.

El objetivo de estos modelos es que el usuario viajero no tenga que modificar absolutamente nada en su cliente de correo electrónico, es decir que funcione como si estuviera en su puesto de trabajo.

Apéndice B. Definición de términos utilizados

Cifrado:

Transformación de un mensaje en otro, utilizando una clave para impedir que el mensaje transformado pueda ser interpretado por aquellos que no conocen la clave.

Confidencialidad:

Característica o atributo de la información por el que la misma sólo puede ser revelada a los usuarios autorizados en tiempo y forma determinados.

Correo Web:

Casi todos los proveedores de correo dan el servicio de correo web (*webmail*) que permite enviar y/o recibir correos mediante una página web diseñada para ello, y por tanto usando sólo un programa navegador web. La alternativa es usar un *programa de correo* especializado.

El *correo web* es cómodo para mucha gente, porque permite ver y almacenar los mensajes desde cualquier sitio (en un servidor remoto, accesible por la página web) en vez de en un ordenador personal concreto.

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

Dirección de correo electrónico:

Es un conjunto de palabras que identifican a una persona que puede enviar y recibir correo. Cada dirección es única y pertenece siempre a la misma persona. La dirección de correo electrónico está

considerada como dato personal, ya que puede permitir la identificación del usuario de la misma.

Por ejemplo: **persona@servicio.es**, que se lee *persona arroba servicio punto es*. El signo **@** (llamado arroba) siempre está en cada dirección de correo, y la divide en dos partes: el nombre de usuario (a la izquierda de la arroba; en este caso, **persona**), y el dominio en el que está (lo de la derecha de la arroba; en este caso, **servicio.es).**

Es aconsejable elegir en lo posible una dirección fácil de memorizar para así facilitar la transmisión correcta de ésta a quien desee escribir un correo al propietario, puesto que es necesario transmitirla de forma exacta, letra por letra. Un solo error hará que no lleguen los mensajes al destino.

Directorios de correo:

Conjunto de direcciones de correo electrónico, estructurado para la realización de búsquedas. Es un concepto similar al de "guía telefónica", aplicado a las direcciones de correo electrónico.

Filtros:

Permiten ordenar el correo entrante basándose en una serie de reglas definidas previamente.

Firma electrónica:

Conjunto de datos electrónicos añadidos a un mensaje que permite al receptor de los mismos comprobar su fuente e integridad y protegerse así de la suplantación o falsificación. Para su generación se suelen utilizar técnicas criptográficas.

HOAX *(Del inglés, engaño o bulo)*:

Son mensajes de correo electrónico engañosos que se distribuyen en cadena. Algunos tienen textos alarmantes sobre catástrofes (virus informáticos, perder el trabajo o incluso la muerte) que pueden sucederte si no reenvías el mensaje a todos los contactos de tu libreta de direcciones.

También hay hoaxes que tientan con la posibilidad de hacerte millonario con sólo reenviar el mensaje o que apelan a la sensibilidad invocando supuestos niños enfermos.

IMAP *(Internet Message Access Protocol):*

Es un protocolo de acceso a mensajes electrónicos almacenados en un servidor.

Mediante IMAP se puede tener acceso al correo electrónico desde cualquier equipo que tenga una conexión a Internet.

IMAP tiene varias ventajas sobre POP. Por ejemplo, es posible especificar en IMAP carpetas del lado servidor. Por otro lado, es más complejo que POP ya que permite visualizar los mensajes de manera remota y no descargando los mensajes como lo hace POP.

ISP:

Proveedor de Servicios a Internet.

Lista Blanca de RedIRIS.

Base de datos de direcciones IP de *relays* de operadores nacionales, incluidos instituciones RedIRIS, de confianza según criterios previamente definidos. http://www.rediris.es/abuses/eswl

Lista de distribución:

Una lista que contiene las direcciones de un grupo de usuarios que intercambian mensajes a propósito de un tema de interés común. La lista es accesible a través de una dirección de correo electrónico, de tal forma que cualquier mensaje enviado a esa dirección se redistribuye a todas las direcciones de correo electrónico contenidas en la lista (p.ej. nombrelista@us.es).

Muchas organizaciones utilizan cada vez más esta herramienta para mantener informadas a las personas principalmente con noticias, publicidad e información de interés. Para no caer en prácticas de *spam*, los correos se envían previa inscripción del destinatario, dándole la oportunidad de cancelar la misma cuando guste.

Lista negra:

Mecanismo de control de identificación que permite diferenciar entre personas que pueden acceder a un determinado servicio de otros que, constando en dicha lista, no pueden acceder.

MUA *(Mail User Agent) ó Cliente de correo*:

Es un programa de ordenador usado para leer y enviar correos.

Originalmente, los clientes de correo electrónico fueron pensados para ser programas simples para leer los mensajes del correo de usuario, enviados por el agente de reparto de correo (MDA) conjuntamente con el agente de transferencia de correo (MTA) a un buzón local.

Los formatos de buzón de correo más importantes son MBOX y MAILDIR. Estos simplísimos protocolos para el almacenamiento local de e-mails realizan de una forma muy sencilla la importación, exportación y copia de seguridad de las carpetas de correo.

Los e-mails pendientes de envío serán entregados al MTA, tal vez a través de un agente de correo saliente de forma que el cliente de correo electrónico no necesita proporcionar ninguna clase de función de transporte.

Suelen incorporar muchas más funcionalidades que el *correo web*, ya que todo el control del correo pasa a estar en el ordenador del usuario. Por ejemplo, algunos incorporan potentes filtros antispam.

Por el contrario, necesitan que el proveedor de correo ofrezca este servicio, ya que no todos permiten usar un programa especializado (algunos sólo dan *correo web*). En caso de que sí lo permita, el proveedor tiene que explicar detalladamente cómo hay que configurar el programa de correo. Esta información siempre está en su página web, ya que es imprescindible para poder hacer funcionar el programa, y es distinta en cada proveedor.

Entre los datos necesarios están: tipo de conexión (POP/POPS o IMAP/IMAPS), *dirección del servidor de correo*, *nombre de usuario* y *contraseña*. Con estos datos, el programa ya es capaz de obtener y descargar nuestro correo.

El funcionamiento de un *programa de correo* es muy diferente al de un *correo web*, ya que un programa de correo descarga de golpe *todos* los mensajes que tenemos disponibles, y luego pueden ser leídos sin estar conectados a Internet (además, se quedan grabados en el ordenador). En cambio, en una página web se leen de uno en uno, y hay que estar conectado a la red todo el tiempo.

Algunos ejemplos de programas de correo son Mozilla Thunderbird, Evolution, Outlook Express, Eudora, ..., etc.

MDA *(Agente de Reparto de Correo)*:

El **Mail Delivery Agent** es un software que acepta correo entrante y los distribuye a los buzones de los destinatarios (si la cuenta de destino está en la máquina local), o lo reenvía a un servidor SMTP (si los destinatarios están en máquinas remotas).

MIME *(Multipurpose Internet Mail Extensions), (Extensiones de Correo Internet Multipropósito)*:

Del inglés Multimedia Internet Message Extensions, estándar que soportan prácticamente todos los

lectores de correo y que permite el uso de caracteres nacionales en el cuerpo del mensaje y el intercambio de documentos formateados.

En sentido general las extensiones de MIME van encaminadas a soportar:

- texto en conjuntos de caracteres distintos de US-ASCII,
- adjuntos que no son de tipo texto,
- cuerpos de mensajes con múltiples partes (multi-part),
- información de encabezados con conjuntos de caracteres distintos de ASCII.

MTA *(Agente de Transferencia de Correo)***:**

Es el servidor de correo (SMTP) en sí.

El MTA, recibe los mensajes desde otro MTA (*relaying*), un MSA (*Mail submission Agent*) que toma por sí mismo el mensaje electrónico desde un MUA (*Mail user agent*), o recibe directamente el correo desde un MUA, actuando como un MSA. El MTA trabaja en segundo plano, mientras el usuario usualmente interactúa con el MUA.

Algunos de los más conocidos son Sendmail, Postfix, Qmail, ..., etc.

MX:

Un Registro MX o Mail eXchange Record (registro de intercambio de correo) es un tipo de registro, un recurso DNS que especifica cómo debe ser encaminado un correo electrónico en Internet. Los registros MX apuntan a los servidores a los cuales enviar un correo electrónico, y a cual de ellos debería ser enviado en primer lugar, por prioridad.

NTP *(Network Time Protocol)***:**

Es un protocolo para sincronizar los relojes de los servidores conectados a Internet, en este caso especialmente los que forman parte de la infraestructura del servicio de correo.

POP *(Post Office Protocol)***:**

En clientes locales de correo para obtener los mensajes de correo electrónico almacenados en un servidor remoto. La mayoría de los suscriptores de los proveedores de internet acceden a sus correos a través de POP3.

Las versiones del protocolo POP (informalmente conocido como POP1) y POP2 se han hecho obsoletas debido a las últimas versiones de POP3. En general cuando uno se refiere al término *POP*, nos referimos a *POP3* dentro del contexto de protocolos de correo electrónico.

El diseño de POP3 es para recibir correo y no para enviar y sus predecesores permite que los usuarios con conexiones intermitentes, descarguen su correo electrónico cuando se encuentren conectados de tal manera que puedan ver y manipular sus mensajes sin necesidad de permanecer conectados. La mayoría de los clientes de correo incluyen la opción de *dejar los mensajes en el servidor*, de manera tal que, un cliente que utilice POP3 se conecta, obtiene todos los mensajes, los almacena en la computadora del usuario como mensajes nuevos, los elimina del servidor y finalmente se desconecta.

Proveedor:

Organismo responsable del Servicio de Correo Electrónico

Open Relay:

El ataque de **Open Relay** consta en usar el MTA (*Mail Transport Agent*, Agente de Transporte de Correo)

como puente para correos (usualmente spam, aunque pueden ser muchas otras cosas, como los Hoax) que de otra manera no podrían llegar a destino, gracias a que los servidores bloquearon la dirección IP de origen.

De esta manera, la gente que manda spam de forma indiscriminada se ve obligada a usar otros servidores para esta tarea. Estos servidores que permiten que se envíe correos a través de ellos, se los denomina Open Relay.

Para solucionar esto (o castigar a la gente que tiene el MTA aceptando este *"puenteo de correos"* para cualquier lugar) se crearon listas negras en tiempo real que bloquean dichos hosts en los cuales se detectó un MTA que hacía Open Relay. Y para que se saque una IP de estas listas negras, se deben pasar ciertas pruebas y esperar cierto tiempo.

Normas PEM *(Privacy Enhanced Mail)***:**

Correo con Privacidad Mejorada. Norma aplicable al protocolo de correo electrónico utilizado en Internet, que permite cifrar de manera automática los mensajes de correo electrónico antes de enviarlos. No es necesario invocar procedimientos separados para cifrar el mensaje de correo.

PGP *(Pretty Good Privacy)***:**

Programa de libre distribución, escrito por Phil Zimermann, que impide, mediante técnicas de criptografía, que ficheros y mensajes de correo electrónico puedan ser interpretados por personas no autorizadas. Puede también utilizarse para firmar electrónicamente un documento o un mensaje, realizando así la autenticación del autor.

Proveedor de correo:

Para poder enviar y/o recibir correo electrónico, generalmente hay que estar registrado en alguna empresa que ofrezca este servicio (gratuito o de pago). El registro permite tener una *dirección de correo* personal única y duradera, a la que se puede acceder mediante un nombre de usuario y una contraseña.

Relay:

Servidor que, utilizando el protocolo SMTP tiene como finalidad el interambio de mensajes de correo electrónico. También se identifica como MTA (Mail Transfer Agent) o Estafeta.

SASL *(Simple Authentication and Security Layer)***:**

Es un sistema autenticación y autorización en protocolos de internet. SASL sólo maneja la autenticación y requiere otros mecanismos --como por ejemplo TLS-- para cifrar el contenido que se transfiere.

SCS:

Servicio de Certificados de Servidor para la comunidad RedIRIS.http://www.rediris.es/pki/scs/

SPAM:

Se denomina Spam o “correo basura” a todo tipo de comunicación no solicitada, realizada por vía electrónica. De este modo se entiende por Spam cualquier mensaje no solicitado y que normalmente tiene el fin de ofertar, comercializar o tratar de despertar el interés respecto de un producto, servicio o empresa. Aunque se puede hacer por distintas vías, la más utilizada entre el público en general es mediante el correo electrónico. Quienes se dedican a esta actividad reciben el nombre de spammers.

Spammer:

La persona o compañía que realiza el envío de Spam.

Spamming lists:

Listas comerciales. Listas de direcciones de correo para envío de publicidad de forma masiva.

SPF *(Sender Policy Framework)***:**

Es una protección contra la falsificación de direcciones en el envío de correo electrónico.

Identifica, a través de los registros de nombres de dominio (DNS), a los servidores de correo SMTP autorizados para el transporte de los mensajes.

Este convenio puede significar el fin de abusos como el spam y otros males del correo electrónico.

SSL *(Secure Sockets Layer)***:**

El protocolo de seguridad más usado en Internet. Utiliza criptografía asimétrica para generar una clave de sesión con la que se cifran las comunicaciones entre el cliente y el servidor. Proporciona también servicios de autenticación del servidor y, opcionalmente, del cliente.

TLS *(Transport Layer Security)***:**

Protocolo para cifrar las transacciones en los protocolos de Internet.

Transacciones SMTP:

Intercambio de información entre servidores de correo, basada en el protocolo SMTP.

Usuario:

Cliente que hace uso del Servicio de Correo del proveedor en función de la Política de Uso previamente establecida.

Apéndice C. Declaración Completa de Copyright