RACEv2: Red Avanzada de Correo Electrónico

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

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

Índice

1. Introducción....4
2. Consideraciones previas....4
3. Niveles de Calidad....5
   3.1 Criterios de encaminamiento SMTP....5
      3.1.1 Criterio 1: Reglas anti-relay....5
      3.1.2 Criterio 2: Política de logs (trazas)....6
      3.1.3 Criterio 3: Resolución inversa de MTAs....6
      3.1.4 Criterio 4: Número máximo de destinatarios....6
      3.1.5 Criterio 5: Control de acceso al puerto 25 en entrada / salida....7
      3.1.6 Criterio 6: Tamaño máximo de mensaje....7
      3.1.7 Criterio 7: Definición de registros SPF (Sender Policy Framework)....7
      3.1.8 Criterio 8. Uso de Lista Blanca de RedIRIS....7
      3.1.9 Criterio 9: Chequeo de SPF en correo entrante....8
      3.1.10 Criterio 10: Control de destinatarios....8
      3.1.11 Criterio 11: Control de flujo SMTP....8
   3.2 Criterios de infraestructuras....8
      3.2.1 Criterio 12: Sincronización NTP....8
      3.2.2 Criterio 13: Alta disponibilidad....9
   3.3 Criterios de autenticación y cifrado....9
      3.3.1 Criterio 14: Autenticación centralizada....9
      3.3.2 Criterio 15: Acceso externo cifrado....9
      3.3.3 Criterio 16: Servicio SUBMISSION....9
      3.3.4 Criterio 17: Cifrado MTAi-MTAi....10
      3.3.5 Criterio 18: Cifrado MTA-MTA....10
   3.4 Criterios de servicios....10
      3.4.1 Criterio 19: abuse@ y postmaster@....10
      3.4.2 Criterio 20: Documento descriptivo del Servicio (DOCE)....10
      3.4.3 Criterio 21: Servicio de antivirus....11
      3.4.4 Criterio 22: Acceso remoto por WebMail y otros....11
      3.4.5 Criterio 23: Política de backup (buzones)....11
      3.4.6 Criterio 24: Servicio de cambio de contraseña....11
      3.4.7 Criterio 25: Servicio antispam....12
      3.4.8 Criterio 26: Servicio antispam personalizado....12
      3.4.9 Criterio 27: Servicio de respuesta automática por ausencia prolongada....12
      3.4.10 Criterio 28: Redirección de cuentas....13
      3.4.11 Criterio 29: Servicio de listas de distribución....13
   3.5 Otros Criterios....13
      3.5.1 Criterio 30: Datos del administrador del Servicio de Correo en la base de datos de RedIRIS....13
      3.5.2 Criterio 31: Estadísticas del tráfico SMTP....13
4. Evaluación de instituciones....13
5. Agradecimientos....14
6. Referencias....14
Apéndice A. Movilidad en el Correo Electrónico....15
Apéndice B. Definición de términos utilizados....16
Apéndice C. Declaración Completa de Copyright....21

1. Introducción

Los criterios de calidad expuestos en este documento, y las recomendaciones asociadas a los mismos, han sido extraídas de la experiencia adquirida a lo largo del tiempo por el conjunto de responsables de los Servicios de Correo Electrónico en la Comunidad Académica Española, a través del Grupo de Trabajo de RedIRIS: IRIS-MAIL

La iniciativa RACEv2 surge como evolución del proyecto RACE (Red Académica de Correo Electrónico) de RedIRIS, cuyos objetivos principales comparte plenamente y permanecen invariables:

- Estructurar de forma organizada la evolución del correo electrónico en la comunidad RedIRIS.
- Definir indicadores de calidad para Servicio de correo electrónico.
- Definir una línea de trabajo común en la evolución del servicio de correo-e en RedIRIS.
- Evaluar nuevas tecnologías en el servicio de correo.
- Mejorar el conocimiento del estado del correo-e en la Comunidad RedIRIS.
- Generar documentación y compartir desarrollos de forma organizada.
- Promover la mejora y evolución del servicio en las instituciones implicadas.
- Emisión de certificados de calidad para el público reconocimiento de las instituciones que sean auditadas.
- Desplegar una red privada de estafetas de correo-e conectadas entre sí con una estructura de certificados.

Este documento es uno de los elementos de trabajo de la iniciativa RACEv2, que contiene los criterios de calidad, su clasificación, valoración y recomendaciones para poder alcanzar cada uno de ellos. Además, se prevé la disponibilidad de una aplicación web (*Evaluador*) que automatice, en lo posible, las tareas de validación de cada criterio para aquellas organizaciones que deseen ser auditadas y certificadas.

Igualmente, y con el compromiso de cubrir los objetivos de promover la mejora de los Servicios de Correo, y de crear una Red Privada de Confianza, se define en el anexo del presente documento extensiones de la iniciativa:

> Apéndice A: Movilidad en el correo electrónico: Cuyo Objetivo es definir con mayor nivel de detalle las recomendaciones asociadas a criterios de calidad que valoran los servicios ofrecidos a los usuarios de Correo desplazados fuera de sus instituciones.

El contenido del presente documento no es normativo, ni tampoco constituye un tutorial de los temas tratados. Su objetivo es abarcar el núcleo de la iniciativa: motivación de la misma, presentación de criterios y su valoración, recomendaciones y anexos de interés. Se prevé la publicación de otros documentos por parte de la iniciativa RACEv2 que cubran estos aspectos, instrucciones de configuración y uso en distintos entornos operativos, etc.

Todas las recomendaciones indicadas en el presente documento cumplen escrupulosamente el contenido de los diferentes estándares de Internet (RFCs) relacionados con SMTP y otros protocolos y tecnologías complementarias. [RFC2821] (Klensin, J., “Simple Mail Transfer Protocol,” April2001.) y otros.

2. Consideraciones previas

Tal y como se indica en la cabecera del presente documento, se ha utilizado en la descripción de los criterios las palabras clave recomendadas en el RFC 2119 (Bradner, S., “Key words for use in RFCs to Indicate Requirement Levels,” March 1997.) [RFC2119] para indicar niveles de requerimiento, y en concreto las traducciones para cada palabra clave disponible en el RFC 2119-es (Caínzos, J., “Palabras clave a utilizar en RFC para Indicar Niveles de Requerimiento,” Marzo1997.) [RFC2119 es].

En concreto, se han etiquetado los criterios como obligaciones (DEBE, NO DEBE), y como

recomendaciones (DEBERÍA, NO DEBERÍA).

Adicionalmente a este etiquetado, se han clasificado los criterios (y por ende sus recomendaciones asociadas) según su ámbito de aplicación:

1. Criterios de encaminamiento SMTP: Afectan al encaminador de correo -*Relay* o MTA -.

2. Criterios de infraestructuras: Definen los recursos necesarios para dar soporte a un Servicio de Correo Electrónico de calidad.

3. Criterios de autenticación y cifrado: Engloban los mecanismos de seguridad necesarios para garantizar la integridad y privacidad de los datos en el entorno del Correo Electrónico.

4. Criterios de Servicios: Servicios básicos y de valor añadido.

5. Criterios generales: Otro tipo de criterios que no encajan en las clases anteriores.

3. Niveles de Calidad

En las siguientes secciones se detalla cada criterio, su nivel, su valoración en puntos, sus recomendaciones asociadas y posibles enlaces a documentación de apoyo.

Cada criterio muestra la valoración establecida por el Grupo de Trabajo RACEv2, con un máximo de 100 puntos para cada uno. La suma total del valor de los criterios que cumple una institución permite asignarle un nivel cuantitativo que mide la calidad de su Servicio de Correo Electrónico. En paralelo, se establece un nivel cualitativo que requiere por parte de la organización auditada el cumplimiento de todos los criterios obligatorios (DEBE, OBLIGATORIO,...) y, adicionalmente, el cumplimiento de algun criterio recomendado (DEBERÍA, RECOMENDABLE,...).

3.1 Criterios de encaminamiento SMTP

Los criterios de encaminamiento SMTP engloban el conjunto de normas básicas que los administradores del Servicio de Correo Electrónico deben tener presentes a la hora de implementar y configurar el primer nivel de su infraestructura. Afectan, por tanto, en su totalidad a las estafetas de primer nivel, nodos de entrada/salida o *relays* de la organización, según las diferentes referencias disponibles para su identificación dentro de su institución.

El origen de cada criterio es variado: En ocasiones fruto del consenso de la comunidad académica al considerarlo la 'mejor práctica actual', proveniente de exigencias propias de los RFCs asociados al servicio o fruto de la necesidad del cumplimiento de las normas legales vigentes.

3.1.1 Criterio 1: Reglas anti-relay

Valoración - 100 puntos

El proveedor DEBE configurar adecuadamente el puerto 25 de sus estafetas de primer nivel, disponiendo de reglas *anti-relay* que garanticen un uso legítimo, aceptando mensajes cuyo destino sea la propia organización o bien dominios delegados.

La adopción de medidas *anti-relay* se considera uno de los pasos básicos para la puesta en marcha de una estafeta de correo, y si no se cumple este criterio seremos listados en múltiples repositorios utilizados para bloquear estafetas mal configuradas, utilizadas habitualmente como salto de envío de *spam*. La práctica totalidad de las aplicaciones utilizadas para poner en marcha una MTA incluyen estas medidas, por lo que

su uso es simple y sencillo.

Se dispone de variadas recomendaciones generales sobre la lucha contra el *spam*, donde se refleja la importancia para los responsables del Servicio de Correo de no ser considerados*relays* incontrolados: RFC 2505 (Lindberg, G., “Anti-Spam Recommendations for SMTP MTAs,” February 1999.) [RFC2505] y RFC 2635 (Hambridge, S. and A. Lunde, “DON'T SPEW A Set of Guidelines for Mass Unsolicited Mailings and Postings (spam*),” June 1999.) [RFC2635].

3.1.2 Criterio 2: Política de logs (trazas)

Valoración - 100 puntos

El proveedor DEBE almacenar y conservar convenientemente los ficheros de trazas (logs) de acuerdo a la legislación vigente en cada momento.

Las trazas permitirán la identificación de posibles problemas o incidentes, y servirán como fuente de datos para estudios estadísticos. A estos efectos, DEBEN contener los siguientes datos: fecha y hora de la transacción, nombres de las MTAs que reciben y envían, identificador (ID) del mensaje, dirección de origen y destino, la MTA que actúa de relay, el estado de la transacción y el tamaño del mensaje.

Sería RECOMENDABLE que en dichas trazas además apareciesen datos propios de los filtros de la institución (puntuaciones de spam, virus detectados y tipo de contenido en cada parte de los mensajes multiparte). Con estos datos se facilitaría el estudio de nuevas técnicas usadas por spammers, extensión y peligrosidad de virus, filtros que ya no son efectivos y estadísticas

En concreto, la legislación española obliga a conservar, por un periodo mínimo de 6 meses, todos los ficheros de traza generados (Boletín Oficial de las Cortes Generales, 121/000128 “Conservación de datos relativos a las Comunicaciones Electrónicas y a las Redes Públicas de Comunicaciones”)

3.1.3 Criterio 3: Resolución inversa de MTAs

Valoración - 100 puntos

El proveedor DEBE definir la resolución inversa de las direcciones IP asignadas a las estafetas de primer nivel, encargadas del encaminamiento de entrada y salida de la organización.

De hecho, es muy común que las MTAs receptores apliquen como restricción al tráfico SMTP el que la MTA emisora no disponga de resolución inversa, por lo que incumplir este criterio nos situaría en un escenario de posibles rechazos y problemas de entrega de los mensajes emitidos por nuestros usuarios.

El RFC 3172 (Huston, G., “Management Guidelines & Operational Requirements for the Address and Routing Parameter Area Domain ("arpa"),” September 2001.) [RFC3172] detalla éste y otros requisitos asociados al direccionamiento y encaminamiento en la Red.

3.1.4 Criterio 4: Número máximo de destinatarios

Valoración - 100 puntos

El numero máximo de destinatarios de un correo DEBE estar comprendido entre 100 (RFC 2821 Klensin, J., "Simple Mail Transfer Protocol," April 2001) y 150 (recomendación de RedIRIS).

3.1.5 Criterio 5: Control de acceso al puerto 25 en entrada / salida

Valoración - 100 puntos

El proveedor DEBERÍA diseñar y aplicar una topología del Servicio de Correo que concentre en varias estafetas todo el tráfico de entrada y salida de su organización (estafetas de primer nivel), estando éstas bajo su directa administración.

Este criterio pretende enfatizar la necesidad de implantar una topología de encaminamiento del correo con el fin de homogeneizar de una forma centralizada el tratamiento del correo electrónico, de entrada/salida, de cada unidad organizativa del proveedor, facilitando el uso adecuado de las infraestructuras, previniendo posibles ataques y haciendo posible la implantación de los demás criterios de RACEv2

3.1.6 Criterio 6: Tamaño máximo de mensaje

Valoración - 100 puntos

El tamaño máximo de mensaje DEBERÍA ser controlado, formando parte de la configuración de las estafetas de primer nivel corporativas. El tamaño máximo de mensaje lo definirá cada institución atendiendo a las cuestiones que considere oportunas.

Dado que los sistemas de correo electrónico no están pensados para transferir ficheros de gran tamaño, el proveedor DEBERÍA ofrecer a los usuarios algún sistema de transferencia de ficheros para paliar esta situación. Existen varios desarrollos para ofrecer este servicio a los usuarios.

3.1.7 Criterio 7: Definición de registros SPF (Sender Policy Framework)

Valoración - 100 puntos

El proveedor DEBERÍA definir en su zona DNS los registros SPF (Sender Policy Framework) de todos los dominios de su responsabilidad, asociándolos a los nodos de correo que efectúen el encaminamiento de salida SMTP (estafeta de primer nivel)

Con esta medida el proveedor pone a disposición de toda aquella MTA que implemente chequeos SPF la relación de MTAs que están autorizadas para enviar el correo que se encuentra bajo su responsabilidad, lo que disminuiría la probabilidad ante posibles ataques y/o aumentos de carga en sus estafetas por mensajes devueltos.

La especificación SPF actual está contenida en el RFC 4408 (Wong, M. and W. Schlitt, “Sender Policy Framework (SPF) for Authorizing Use of Domains in E-Mail, Version 1,” April 2006.) [RFC4408].

3.1.8 Criterio 8. Uso de Lista Blanca de RedIRIS

Valoración – 100 puntos

El proveedor DEBERÍA declarar y mantener actualizadas en la Lista Blanca de RedIRIS las direcciones IP de sus relays de correo así como incluirlas en los chequeos de conexión SMTP para evitar el bloqueo de tráfico generado en dicha Lista Blanca

La Lista Blanca de RedIRIS incluye direcciones IP de Estafetas de salida de universidades españolas y de operadores españoles de confianza para RedIRIS. El chequeo de dicha lista garantizará que no se bloquee el tráfico procedente de las estafetas incluidas reduciendo la posibilidad de falsos positivos.

La Lista Blanca es un Servicio de RedIRIS cuyas especificaciones pueden ser encontradas en http://www.rediris.es/abuses/

3.1.9 Criterio 9: Chequeo de SPF en correo entrante

Valoración - 55 puntos

El proveedor DEBERÍA configurar sus estafetas de primer nivel para que se lleven a cabo los correspondientes chequeos SPF del correo entrante.

Es posible que nuestra aplicación habitual de MTA ya incorpore esta posibilidad, y por tanto simplifique las tareas de integración de los chequeos de SPF. Este criterio establece en todo caso la posibilidad de analizar los mensajes entrantes a nuestra organización para determinar si cumplen los registros SPF publicados por el dueño del dominio, pero no indica las acciones a realizar con los mensajes que no pasen el test aplicado.

3.1.10 Criterio 10: Control de destinatarios

Valoración - 95 puntos

La organización DEBERÍA disponer de algún tipo de mecanismo que permita rechazar en sus estafetas de primer nivel aquellos mensajes dirigidos a destinatarios no existentes.

3.1.11 Criterio 11: Control de flujo SMTP

Valoración - 80 puntos

Se DEBERÍA disponer de algún tipo de mecanismo de control de flujo en transacciones SMTP internas y externas. Este mecanismo permite controlar el numero de correos enviados por una IP en un intervalo de tiempo.

3.2 Criterios de infraestructuras

Los criterios de infraestructuras comprenden aquellas recomendaciones básicas y genéricas, aplicables a todo tipo equipamiento informático y cualquier sistema operativo utilizado, que se consideran útiles para el objetivo de garantizar una adecuada calidad de servicio.

3.2.1 Criterio 12: Sincronización NTP

Valoración - 100 puntos

El proveedor DEBERÍA tener correctamente configurada la zona horaria, y sincronizadas mediante NTP todas las estafetas de correo electrónico de la organización, tanto las de primer nivel, como nodos intermedios, estafetas de almacenamiento de mensajes, etc (Mills, D., “Network Time Protocol (Version 3) Specification, Implementation,” March 1992.) [RFC1305][RFC4330] (Mills, D., “Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI,” January 2006.) con un servidor de la propia organización o de otro proveedor que ofrezca este servicio.

En el ámbito académico de RedIRIS - Red Española de I+D , es posible obtener información de interés en las páginas en la página de RedIRIS de zonas horarias de España.

3.2.2 Criterio 13: Alta disponibilidad

Valoración - 100 puntos

La infraestructura hardware que soporta la plataforma del Servicio de Correo Electrónico DEBERÍA diseñarse para ofrecer alta disponibilidad en, al menos, los siguientes puntos:

- Alta disponibilidad en estafetas de entrada/salida (MTAs) [round robin, balanceadores hw, ...]
- Alta disponibilidad en estafetas de segundo nivel (buzones - MDAs)
- Alta disponibilidad en Servidor WebMail
- Alta disponibilidad en los servidores de autenticación centralizada.

Es RECOMENDABLE que dicha infraestructura disponga de mecanismos de balanceo de carga que permita un reparto de la carga equitativo entre los nodos. Esto sería aplicable a configuraciones de alta disponibilidad en modo activo/activo.

3.3 Criterios de autenticación y cifrado

Esta sección engloba la valoración de criterios y recomendaciones de uso de autenticación en el contexto de la autenticación (mecanismos, protocolos y arquitecturas) que garanticen la privacidad de las credenciales y la integridad de la información transferida.

3.3.1 Criterio 14: Autenticación centralizada

Valoración - 100 puntos

El proveedor DEBERÍA disponer de un sistema de autenticación centralizada, aplicado a su infraestructura de servicio.

3.3.2 Criterio 15: Acceso externo cifrado

Valoración - 100 puntos

La organización DEBERÍA ofrecer únicamente servicios basados en protocolos de recogida de mensajes con cifrado SSL/TLS (POPs, IMAPs) y un servicio de correo saliente SMTP con TLS, así como acceso al correo por Web vía HTTPs para los usuarios externos.

El RFC 2595 (Newman, C., “Using TLS with IMAP, POP3 and ACAP,” June 1999.) [RFC2595] detalla el uso de TLS en los protocolos más comunes de recogida de mensajes.

3.3.3 Criterio 16: Servicio SUBMISSION

Valoración - 100 puntos

El proveedor DEBERÍA ofrecer acceso autenticado (SASL) y cifrado (TLS) a través del puerto 587 (SUBMISSION) para todos sus usuarios, dejando el puerto 25 (SMTP) para tráfico entre MTAs, tal y como se define en el RFC4409 (Gellens, R. and J. Klensin, “Message Submission for Mail,” April 2006.) [RFC4409].

La separación de ambos tráficos SMTP, desde el punto de vista del administrador aporta la posibilidad de aplicar reglas y controles más específicos en cada caso. Adicionalmente, desde el punto de vista de un usuario desplazado fuera de su organización, no se verá afectado por posibles cortes del puerto 25 en las instalaciones que visita, pudiendo seguir utilizando el servicio, cifrado y autenticado, de correo saliente de

su institución origen en el TCP/587.

Se recomienda leer el RFC5068 (BCP 134,RFC5068 on Email Submission Operations: Access and Accountability Requirements) que complementa al RFC4409 y que define unas buenas prácticas para administradores de correo para gestionar el servicio de correo por el puerto 587 tanto para usuarios locales como viajeros (*roaming*).

3.3.4 Criterio 17: Cifrado MTAi-MTAi

Valoración - 60 puntos

El proveedor DEBERÍA configurar sus sistemas para permitir la comunicación cifrada (SMTP con TLS) entre las distintas MTAs de su organización, tal y como se establece en el RCF 3207 (Hoffman, P., "SMTP Service Extension for Secure SMTP over Transport Layer Security," February 2002.) [RFC3207], que define la extensión del protocolo SMTP para su cifrado sobre TLS.

El cumplimiento de este criterio aporta privacidad adicional al mensaje, y evita que entornos de la red de la organización expuestos a captura de tráfico sirvan a los fines de usuarios maliciosos.

3.3.5 Criterio 18: Cifrado MTA-MTA

Valoración - 60 puntos

Tal y como se indicó en el criterio anterior, y aplicado al tráfico externo, el proveedor DEBERÍA configurar sus sistemas para permitir la comunicación cifrada (SMTP con TLS) con *relays* externos (RFC 3027 (Hoffman, P., "SMTP Service Extension for Secure SMTP over Transport Layer Security," February 2002.) [RFC3207]).

3.4 Criterios de servicios

3.4.1 Criterio 19: abuse@ y postmaster@

Valoración - 100 puntos

Se DEBE disponer de un servicio de soporte y gestión de incidentes, cuyas direcciones de contacto sean abuse@ (buzón orientado a la recepción de incidentes como falsificaciones, correo no deseado, etc) y postmaster@ RFC 2821 (4.5.1) (Klensin, J., "Simple Mail Transfer Protocol," April 2001.) [RFC2821] y RFC 1123 (5.2.7) (Braden, R., "Requirements for Internet Hosts - Application and Support," October 1989.) [RFC1123].

3.4.2 Criterio 20: Documento descriptivo del Servicio (DOCE)

Valoración - 100 puntos

El proveedor DEBERÍA disponer de un documento público accesible via web que describa el Servicio de Correo Electrónico, incluyendo la política de uso y los servicios ofrecidos.

Este documento DEBERÍA ser conocido por los usuarios, e incluir, al menos información sobre los siguientes puntos de interés:

- Responsabilidades del Servicio.

- Topología básica del Servicio de Correo Electrónico y encaminamiento de los mensajes en entrada/salida.
- Modelo de acceso: POPS, IMAPS, HTTPS.
- Política antivirus aplicada.
- Política antispam aplicada.
- Política de logs (trazas).
- Límites: Cuotas, Tamaño máximo de mensaje, etc.
- Políticas de limpieza o eliminación de buzones, si existe.
- Otros servicios de valor añadido: Cambio de clave, etc.
- Puntos de contacto: postmaster, abuse.

Es RECOMENDABLE consultar la documentación disponible para la creación de un Documento de Correo Electrónico, DOCE (Recomendaciones para generar un documento descriptivo del Servicio), publicado por IRIS-MAIL

3.4.3 Criterio 21: Servicio de antivirus

Valoración - 100 puntos

La organización DEBERÍA disponer de un servicio de antivirus que analice tanto los mensajes entrantes como los salientes en las estafetas de primer nivel.

Es RECOMENDABLE disponer de diferentes motores de antivirus a fin que no se encuentre en un único fabricante la detección de este tipo de amenaza que puede causar graves daños, tanto a infraestructuras como a usuarios finales. Se pueden encontrar diferentes soluciones antivirus gratuitas, que podrían complementar la solución principal.

La política de cada organización determinará las acciones a tomar en cada caso detectado (eliminación del adjunto infectado sustituyéndolo por un aviso, puesta en cuarentena del mensaje completo, eliminación, aviso al remitente, etc).

3.4.4 Criterio 22: Acceso remoto por WebMail y otros

Valoración - 100 puntos

La organización DEBERÍA ofrecer uno o más mecanismos de acceso remoto al correo institucional individual. DEBERÍA ofrecerse, al menos, un servicio de acceso al correo vía Web (*WebMail*) con cifrado SSL, y DEBERÍA ofrecerse otro tipo de servicios adicionales, por ejemplo:

- Protocolos de recogida de mensajes, con cifrado SSL/TLS: IMAPs, POPs.
- Servicio de VPN (Red privada virtual).

3.4.5 Criterio 23: Política de backup (buzones)

Valoración - 100 puntos

El proveedor DEBERÍA disponer y aplicar una política de copias de seguridad de los buzones de los usuarios. Esta política podrá ser de uso interno, únicamente diseñada para garantizar la restauración de los buzones en caso de problemas en los servidores, o bien podrá ser extendida para ofrecer un servicio de recuperación de buzones a la carta para los usuarios.

3.4.6 Criterio 24: Servicio de cambio de contraseña

Valoración - 100 puntos

Se DEBERÍA ofrecer al usuario la posibilidad de cambiar su contraseña, de forma autónoma e inmediata, sin intervención de un tercero, y con el objetivo de garantizar la privacidad de la misma.

Es RECOMENDABLE que este servicio sea ofrecido mediante un interfaz Web, de acceso seguro, y de uso simple, donde figuren además las instrucciones de ámbito local de nuestra institución (instrucciones para la elección de una buena contraseña, caracteres válidos, longitud aceptada, restricciones, etc.).

3.4.7 Criterio 25: Servicio antispam

Valoración - 100 puntos

La organización DEBERÍA disponer de un servicio de antispam en sus estafetas, que analice los mensajes entrantes y actúe sobre aquellos que considere spam según su política interna (Criterio 18: Documento DOCE)

Este servicio se considera común a todos los usuarios, o de aplicación general, y es RECOMENDABLE que se base en detección por contenidos, de modo que se garantice el 100% de fiabilidad y no se generen casos de falsos positivos, dado que, posteriormente, se propone un servicio de antispam personalizado (Criterio 26: Servicio antispam personalizado), configurable por el usuario.

Junto a esta medida, es RECOMENDABLE que exista un único backend compartido para todas las estafetas del proveedor donde se almacenen las listas blancas, bayesianos si los hubiese, listas grises y todo aquello que sea compartible y asegure un tratamiento uniforme del correo por cada estafeta.

3.4.8 Criterio 26: Servicio antispam personalizado

Valoración - 85 puntos

El correo no solicitado (*spam*) es en parte algo subjetivo. Por ello, de forma complementaria al servicio antispam instalado en el relay de la institución (Criterio 24: Servicio de antispam) sería RECOMENDABLE ofrecer a nuestros usuarios un servicio antispam personalizado, que les permita configurar mínimamente sus preferencias y que éstas se apliquen en el análisis de los mensajes que reciben en su carpeta de entrada.

Los mensajes detectados como spam pueden ser marcados, derivados automáticamente a una carpeta determinada, o cualquier otra acción que determine la organización en su política de servicio y que haga pública en su documento de Descripción Pública del Servicio de Correo Electrónico (Criterio 18: Documento DOCE)

3.4.9 Criterio 27: Servicio de respuesta automática por ausencia prolongada

Valoración - 40 puntos

Es RECOMENDABLE ofrecer a los usuarios un servicio de respuesta automática por ausencia prolongada (*vacation*), que les permita programar el texto a enviar en la respuesta y la fecha de caducidad del auto-respondedor. En caso de ofrecerlo este servicio DEBERÍA ser acorde a los estándares vigentes, para evitar múltiples respuestas, no responder a listas de distribución, etc.

En concreto, debería formatearse la respuesta auto-generada como una notificación de estado de entrega (*delivery status notification* - DSN) tal y como se define en el RFC 1894 (Moore, K. and G. Vaudreuil, “An Extensible Message Format for Delivery Status Notifications,” January1996.) [RFC1894].

3.4.10 Criterio 28: Redirección de cuentas

Valoración - 50 puntos

Debido a los problemas asociados a estos servicios, el proveedor, NO DEBERÍA ofrecer servicios de redirección de mensajes (*forwarding*).

La redirección (forwarding) de una dirección local hace que se reenvíe todo el correo que se reciba (el bueno, el marcado como spam etc) hacia otra externa, incluido el correo no deseado o malicioso. Esto puede provocar que de forma indirecta algún servidor remoto al recibir grandes cantidades de spam decida bloquear todo el tráfico.

El *forwarding* DEBERÍA de utilizarse en caso que las reglas anti-spam sean severas para hacer que spam no sea reenviado. Actualmente cualquier usuario externo podrá acceder a diferentes cuentas vía Webmail, POPs o IMAPs.

3.4.11 Criterio 29: Servicio de listas de distribución

Valoración - 60 puntos

Las listas de distribución facilitan el uso adecuado del correo electrónico como medio de comunicación dentro de la institución, y con otros usuarios de otras organizaciones. El proveedor DEBERÍA ofrecer a sus usuarios un servicio de gestión de listas de distribución privadas, que permita solicitar la creación de las mismas, y dar de alta o baja miembros de forma autónoma.

Es RECOMENDABLE que este servicio se preste mediante un interfaz WEB, de acceso seguro, y que incluya ayuda en línea.

3.5 Otros Criterios

3.5.1 Criterio 30: Datos del administrador del Servicio de Correo en la base de datos de RedIRIS

Valoración - 100 puntos

Los responsables de la gestión del Servicio de Correo Electrónico DEBERÍAN estar dados de alta en la base de datos que, a tal efecto, mantiene RedIRIS con el objetivo de coordinar a las instituciones miembros de RedIRIS, y facilitar la comunicación entre las mismas. Esta lista esta disponible en http://www.rediris.es/list/info/iris-mail.html

3.5.2 Criterio 31: Estadísticas del tráfico SMTP

Valoración - 55 puntos

Es RECOMENDABLE disponer de estadísticas del tráfico SMTP de la institución, que permitan detectar problemas de funcionamiento, dimensionar adecuadamente las infraestructuras y controlar la evolución del Servicio de Correo.

4. Evaluación de instituciones

Cualquier institución miembro de RedIRIS podrá solicitar su evaluación RACEv2 y obtener un certificado que le indicará el nivel cuantitativo y cualitativo de calidad de sus Servicios. Para solicitar la evaluación será

necesario cumplir 5 criterios que se han considerado de obligado cumplimiento (DEBE) según lo establecido en los RFCs y legislación española que son:

- Criterio 1: Reglas anti-relay
- Criterio 2: Política de trazas (logs)
- Criterio 3: Resolución inversa de MTAs
- Criterio 4: Control de destinatarios.
- Criterio 19: Disponibilidad de direcciones abuse@ y postmaster@

Si estos sencillos criterios son cumplidos, el proveedor podrá seleccionar los criterios que considera cumple para ser evaluados por RACEv2. Dado que cada criterio dispone de una puntuación, la suma de los puntos de todos los criterios superados corresponderá a uno de los 3 niveles existentes según los siguientes baremos:

- Nivel imprescindible: 500 puntos
- Nivel 1. 501- 800 puntos
- Nivel 2. 801-1600 puntos
- Nivel 3. 1601-2240 puntos

En el caso de ser satisfactoria la evaluación el certificado obtenido tendrá una validez de 2 años.

5. Agradecimientos

Este documento ha sido elaborado y redactado apoyándose en opiniones, colaboraciones y aportaciones realizadas en las distintas reuniones desarrolladas por los miembros del Grupo de Apoyo RACEv2 (IRIS-MAIL, RedIRIS), y de los Grupos de Apoyo del proyecto RACEv2 original.

Se hace extensible el agradecimiento a todos los asistentes a las reuniones del Grupo de Trabajo IRIS-MAIL, y a otros grupos de trabajo dentro del ámbito de RedIRIS (Red española de I+D).

6. Referencias

[Ley34-2002]	B.O.E., "Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico," julio 2002.
[RFC1123]	Braden, R., "Requirements for Internet Hosts - Application and Support," STD 3, RFC 1123, October 1989.
[RFC1305]	Mills, D., "Network Time Protocol (Version 3) Specification, Implementation," RFC 1305, March 1992 (TXT, PDF).
[RFC1894]	Moore, K. and G. Vaudreuil, "An Extensible Message Format for Delivery Status Notifications," RFC 1894, January 1996.
[RFC2119]	Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels," BCP 14, RFC 2119, March 1997 (TXT, HTML, XML).
[RFC2119-es]	Caínzos, J., "Palabras clave a utilizar en RFC para Indicar Niveles de Requerimiento," Marzo 1997.
[RFC2505]	Lindberg, G., "Anti-Spam Recommendations for SMTP MTAs," BCP 30, RFC 2505, February 1999.
[RFC2595]	Newman, C., "Using TLS with IMAP, POP3 and ACAP," RFC 2595, June 1999.

[RFC2635]	Hambridge, S. and A. Lunde, "DON'T SPEW A Set of Guidelines for Mass Unsolicited Mailings and Postings (spam*)," RFC 2635, June 1999.
[RFC2821]	Klensin, J., "Simple Mail Transfer Protocol," RFC 2821, April 2001.
[RFC3172]	Huston, G., "Management Guidelines & Operational Requirements for the Address and Routing Parameter Area Domain ("arpa")," BCP 52, RFC 3172, September 2001.
[RFC3207]	Hoffman, P., "SMTP Service Extension for Secure SMTP over Transport Layer Security," RFC 3207, February 2002.
[RFC4330]	Mills, D., "Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI," RFC 4330, January 2006.
[RFC4408]	Wong, M. and W. Schlitt, "Sender Policy Framework (SPF) for Authorizing Use of Domains in E-Mail, Version 1," RFC 4408, April 2006.
[RFC4409]	Gellens, R. and J. Klensin, "Message Submission for Mail," RFC 4409, April 2006.

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