

Recomendaciones para operadores de Servicio de Correo Electrónico

Revisado: 12 Marzo 2007

Introducción

Son conocidos los problemas que afectan a una aplicación tan ampliamente utilizado y crítica como el correo electrónico. Los problemas en el correo se han englobado en el término **spam** y han ido evolucionando con el tiempo y continuarán haciéndolo. Para mitigar sus efectos y conseguir progresos reales y medibles son necesario acciones coordinadas entre los diferentes actores y para ello es recomendable crear un marco común de actuación basado en lo estándares de Internet.

Este documento presenta una propuesta preliminar puede servir de marco para la elaboración de un código de buenas prácticas entre operadores del Servicio (ESPs). A través de estas buenas prácticas España dispondría de un modelo que podría compartir internacionalmente en la lucha contra el spam. También podrá servir como incentivo a la industria y empresas para armonizar sus tecnologías anti-spam.

El objetivo del Decálogo es conseguir el primer consenso nacional en medidas técnicas para combatir el spam. Pretende definir un marco de confianza para el intercambio de correo electrónico entre operadores españoles, garantizando la seguridad y calidad del servicio de correo electrónico y estableciendo las bases para la autorregulación del sector.

Principios básicos para operadores de Correo Electrónico (ESPs)

Estas recomendaciones se aplican al intercambio de correo electrónico entre operadores de correo electrónico (ESPs). Un ESP es cualquier entidad que disponga de servidor de correo electrónico conectado a Internet

Estas recomendaciones serán revisadas periódicamente para ajustarlas a la evolución de los cambios tecnológicos.

Control de Red

- 1. Regular los sistemas de encaminamiento de mensajes que pueden ser utilizados por terceras partes no autorizadas para la transmisión de correo electrónico (open-relays).**

Se deberán hacer los esfuerzos comercialmente razonables para prevenir el open-proxies, open-relays y la diseminación de virus, gusanos o troyanos

2. **Evitar, con carácter general, transacciones que utilicen el protocolo SMTP entre Internet y máquinas que no estén ni reconocidas ni preparadas para aceptar este tipo de tráfico. El usuario final deberá solicitar este servicio en caso de necesitarlo.**

Es recomendable que el puerto 25/smtp no sea utilizado por los usuarios. Para enviar correo los usuarios deben utilizar accesos autenticados como:

- o Puerto 587 (RFC2476)
- o Webmail
- o Túneles ssh
- o VPN (Red Privada Virtual)

Los ESPs deben utilizar dentro de sus posibilidades los mecanismos apropiados para garantizar esta autenticación

3. **Respetar los protocolos y estándares de Internet en las transacciones SMTP así las recomendaciones de seguridad en lo relativo al mantenimiento y gestión de los servidores de correo así como de las cabeceras de los correos.**

- **Resolución inversa.** Todos los servidores de correo saliente conectado a la Red deben tener resolución inversa coherente de sus IPs. Si es posible la resolución inversa y directa deben ser coincidir o ser consistentes.

Fundamentos técnicos: RFC 1912, Operativa común de DNS y errores frecuentes en su sección 2.1 especifica claramente que “Cada maquina conectada a Internet debe tener un nombre .. Muchos servicios disponibles en Internet no se conectaran si no esta correctamente registrado en el sistema DNS”

RFC 1123, Requerimientos para maquinas en Internet en su sección 6.1.1 también especifica que “cada maquina tiene que implementar un sistema de resolución DNS y debe también implementar un mecanismo usando DNS para convertir nombres de maquina en direcciones IP y viceversa”

Valor del campo **HELO/EHLO** correcto. Asegurarse que el HELO/EHLO del relay de salida es un nombre de maquina cualificado con resolución directa que coincida con la dirección IP del cliente SMTP o bien el literal de su dirección ip. Este bloqueo no puede producirse en la orden HELO/EHLO ya que el estándar no permite rechazar esta orden y se deberá ejecutar en ordenes posteriores (MAIL FROM o RCPT TO)

Fundamentos técnicos: RFC 2821, Especificaciones del protocolo SMTP en su sección 4.1.1.1 dice referente al campo HELO/EHLO “Estas ordenes se usan para identificar el cliente SMTP al servidor SMTP. El argumento de esta orden contiene el nombre de dominio totalmente cualificado del cliente SMTP si esta disponible. En situaciones donde el cliente SMTP no tiene un nombre de dominio significativo... el cliente puede usar el literal de su dirección ip”

RFC 1123, Requerimientos para maquinas en Internet en su sección 5.2.5 también especifica que “El cliente SMTP debe asegurarse que el parámetro <dominio> de la orden HELO es el nombre de dominio principal del cliente SMTP ... El receptor de la orden HELO puede verificar que el parámetro HELO realmente corresponde a la direccion ip del cliente SMTP”

- Los ESPs emisores deberán definir algún tipo de reputación del tipo:
 - Definir registros SPF. Se recomienda que cualquier dominio que desee enviar correo por la Red defina registros SPF. **[Ver recomendaciones del Foro ABUSES**
 - Darse de alta en la Lista Blanca española: (<http://www.rediris.es/abuses/eswl/>). Se recomienda la configuración en su relay de correo de esta ListaBlanca para reducir falsos positivos.
- **Políticas de correo.** Los ESPs emisores deberán disponer de Políticas públicas de aceptación de tráfico SMTP
- **Datos Whois.** Los ESP emisores deberán disponer de datos actualizados en el WHOIS.
- **Datos postmaster/abuses.** Los ESPs emisores deberán disponer de contactos para recibir y atender incidencias del Servicio en direcciones del estilo abuse,postmaster@dominio.es . RFC2821. Estos contactos se deben crear en cualquier dominio que envíe correo.
- **Consistencia de dominios** Los ESPs emisores deberán intentar utilizar una consistencia de dominios en HELO/EHLO,inversa, MAIL FROM etc.
- **Listas Negras.** Los ESPs emisores deberán intentar no estar incluidos en ninguna de las listas negras existentes. Si utiliza ListasNegras como medida de protección AntiSpam. Se recomienda que la selección tengan muy en cuenta las políticas de gestión (altas,bajas) de dichas ListasNegras. **[Ver recomendaciones del Foro ABUSES]**

Monitorización de los sistemas

4. **Establecer sistemas de monitorización de la calidad y disponibilidad de sus servicios de correo electrónico en producción.**
5. **Establecer planes de contingencia.**

Los ESPs, dentro de sus posibilidades, deberán monitorizar los eventos de su red y sistemas de correo electrónico con el objeto de detectar tráfico que pueda perjudicar la seguridad y disponibilidad de sus sistemas y de otros actores de la red. . Los ESPs deben intentar asegurar que su infraestructura de distribución de correo electrónico es correctamente mantenida y operada de un una forma responsable. También se debería

intentar asegurar la fuente de los mensajes que distribuyen (dominio, cabeceras no falsificables etc.)

Protección de los datos de carácter personal

- 6. Respetar la Ley Orgánica de Protección de Datos de Carácter Personal en el tratamiento de las direcciones IP y las direcciones de correo electrónico que pueden permitir identificar a una persona física.**
 - o Se deben garantizar y especificar claramente la recolección, intercambio y uso de direcciones de correo electrónico como datos de carácter personal así como garantizar la salvaguarda de direcciones IP que permitan identificar a personas físicas.
 - o Se debe garantizar habilitar cuentas de correo asociadas a personas físicas o jurídicas.

Protección de los usuarios

- 7. Establecer unos acuerdos de prestación de servicio que permitan denegar el acceso a la red a aquellos usuarios finales que comprometan la seguridad y el funcionamiento eficiente de Internet.**
- 8. Informar a los usuarios de las políticas de filtrado aplicadas, así como de las medidas básicas de seguridad que deben adaptar en sus terminales.**

Los ESPs deberán proteger la calidad y seguridad del servicio que suministra informando a sus clientes a través de los mecanismos que disponga especialmente de los documentos de aceptación de condiciones generales del Servicio. Deben intentar asegurar, siempre que sea económica viable, medidas para proteger la seguridad y privacidad del correo recibido.

Colaboración nacional entre operadores

- 9. Colaborar en foros nacionales e internacionales adecuados para el intercambio de información sobre incidentes en el sistema de correo electrónico.**
- 10. Procurar que todos los nombres de dominios, registros del DNS, direcciones IP son mantenidas de forma correcta, completa y actualizada. Establecer direcciones electrónicas de contacto que estén operativas.**

Para la mejora del tráfico SMTP es imprescindible tener actualizados los datos de registros DNS así como la de los repositorios públicos de rangos IPs como WHOIS. De forma particular se considera de gran relevancia la colaboración entre operadores para el intercambio de incidentes que beneficiará la resolución de problemas. Para ello es

necesario participar en Foros de gestores de incidentes de seguridad (Foro ABUSES) para disponer de una lista de datos actualizados.

Recomendaciones similares en otros países

Electronic Commerce in Canada

<http://e-com.ic.gc.ca/epic/site/ecic-ceac.nsf/en/gv00329e.html>

Finlandia: Regulation ON INFORMATION SECURITY AND FUNCTIONALITY OF E-MAILSERVICES

<http://www.ficora.fi/englanti/document/FICORA112004M.pdf>

Grandes proveedores internacionales que ya rechazan correo proveniente de maquinas sin resolución inversa

AOL <http://postmaster.aol.com/info/rdns.html>

Netlink <http://www.netlink.com.au/mailblocked.html>

CERN: <http://mmmservices.web.cern.ch/mmmservices/Antispam/ActionServer.aspx>