RACEv2: Red Avanzada de Correo Electrónico

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

Criterios de servicios

Comité RACEv2 V2.2

11/03/2008

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.