Recomendaciones al Auditor para la Evaluación

Criterio 1: Reglas anti-relay.

- Forma de Evaluación: Testeo utilizando la utilidad Mail Relay Tester (www.monkeys.com/mrt) . Alternativamente, usar otros programas como rlytest (www.unicom.com/sw/rlytest/) o RelayTest (www.digiarch.org/relaytest.html). Existe un listado de herramientas similares, y de páginas web que realizan testeos de open relay en http://spamlinks.net/prevent-secure-relay-test.htm

Criterio 2: Política de trazas (logs) .

- Forma de Evaluación: Descripción del servicio en DOCE y envío de datos de logs de alguna fecha/hora determinada

Criterio 3: Resolución inversa de MTAs .

- Forma de Evaluación: Chequeo DNS con nslookup / dig

Criterio 4: Nº máximo de destinatarios.

- Forma de Evaluación: Documentación aportada por la solicitante, especificando como implementa este control.
- Envió de mensaje con un número de destinatarios superior al especificado por el solicitante.

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

- Forma de Evaluación: Testeo usando la utilidad nmap

Criterio 6: Tamaño máximo de mensaje

- Forma de Evaluación: Envío de mensaje con adjuntos de tamaño ligeramente superior e inferior al límite establecido, comprobando en el mensaje rechazado el tamaño máximo especificado

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

- Forma de Evaluación: Uso de una herramienta web de chequeo SPF (http://www.politemail.com/check-spf.aspx), o haciendo un dig TXT dominio.es

Criterio 8. Uso de Lista Blanca de RedIRIS

- Forma de Evaluación: Documentación aportada por la solicitante certificando el uso de la lista blanca.
- Haciendo chequeos DNS de las IP de los relays de salida aportados por el solicitante. Para ello basta con con hacer un dig de la IP en la zona eswl.dnsbl.rediris.es

Criterio 9: Chequeo de SPF en correo entrante

- Forma de Evaluación: Documentación aportada por la solicitante

certificando como realiza el chequeo del SPF

Criterio 10: Control de destinatarios

- Forma de Evaluación: Conexión al puerto smtp de destino con RCPT TO falsos del dominio del solicitante, comprobando que son rechazados inmediatamente.

Criterio 11: Control de flujo SMTP

- Forma de Evaluación: Documentación aportada por la solicitante. Envío masivo a la cuenta de prueba, en caso de que sea posible.

Criterio 12: Sincronización NTP

- Forma de Evaluación: Aportación de documentación por la solicitante y comprobación de cabeceras en correos enviados.

Criterio 13: Alta disponibilidad

- Forma de Evaluación: Documentación aportada por la solicitante en la que se especifique la arquitectura del sistema de correo

Criterio 14: Autenticación centralizada

- Forma de Evaluación: Documentación aportada por la solicitante en la que se explique como se realiza la autenticación centralizada

Criterio 15: Acceso externo cifrado

- Forma de Evaluación: Acceso al webmail por https, y recepción y envío mediante SSL con comprobación del certificado

Criterio 16: Servicio SUBMISSION

- Forma de Evaluación: Envío SMTP en el puerto 587 (submission)
- Forma de Evaluación: Envío SMTP en el puerto 587 (submission) desde la cuenta suministrada por el solicitante

Criterio 17: Cifrado MTAi-MTAi

- Forma de Evaluación: Documentación aportada por la solicitante en la que certifique el cifrado entre MTAi

Criterio 18: Cifrado MTA-MTA

- Forma de Evaluación: Acceso por telnet al puerto SMTP y comprobación en el EHLO de que está habilitada la opción STARTTLS

Criterio 19: Disponibilidad de direcciones abuse@ y postmaster@

- Forma de Evaluación: Envío a ambas direcciones solicitando una respuesta al mismo

Criterio 20: Documento descriptivo del Servicio (DOCE)

- Forma de Evaluación: Acceso al DOCE en la URL facilitada por la solicitante

Criterio 21: Servicio de antivirus

- Forma de Evaluación: Test EICAR (www.eicar.org)

Criterio 22: Acceso remoto por WebMail

- Forma de Evaluación: Acceso por webmail, y envío y recepción de mensajes

Criterio 23: Política de backup (buzones)

- Forma de Evaluación: Documentación aportada por la solicitante en la que especifique cual es su política de copias de seguridad

Criterio 24: Servicio de cambio de contraseña

- Forma de Evaluación: Comprobación mediante acceso a la url de cambio de contraseña y cambio de clave de la cuenta de prueba.

Criterio 25: Servicio antispam

- Forma de Evaluación: Realización del test GTUBE (http://spamassassin.apache.org/gtube/). Envío de mensajes ya identificados como SPAM a la cuenta de prueba. Comprobación de cabeceras de correo

Criterio 26: Servicio antispam personalizado

- Forma de Evaluación: Acceso a la personalización del servicio antispam usando la cuenta de prueba.

Criterio 27: Servicio de respuesta automática por ausencia prolongada

- Forma de Evaluación: Activación de este servicio para la cuenta de prueba y comprobación del correcto funcionamiento del mismo enviando un mensaje.

Criterio 28: Redirección de cuentas

- Forma de Evaluación: Documentación aportada por la solicitante en la que indique que no se realizan redirecciones de cuentas.

Criterio 29: Servicio de listas de distribución

- Forma de Evaluación: Acceso a los interfaces web de las listas.

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

- Forma de Evaluación: Comprobación de los datos en la web de RedIRIS. O confirmación por parte de RedIRIS de la inclusión de los administradores en la base de datos

Criterio 31: Estadísticas del tráfico SMTP

- Forma de Evaluación: Informe proporcionado po la institución con ejemplos de las estadísticas del correo.

MINISTERIO
DE INDUSTRIA, TURISMO
Y COMERCIO

red.es impulsamos la sociedad en red

Red IRIS