

Logs Servidor Correo

Detección temprana de reenvíos no autorizados y spam

1. ¿Qué es un reenvío no autorizado?

Un **reenvío no autorizado** (open relay) ocurre cuando un atacante usa nuestro servidor SMTP para mandar correos (normalmente spam o phishing) sin autenticación válida.

Riesgo	Consecuencia
Spam enviado desde nuestra IP	Listas negras (RBL), correos legítimos bloqueados
Phishing o malware	Pérdida de confianza de usuarios y clientes
Sobrecarga de recursos	CPU, ancho de banda y almacenamiento saturados
Problemas legales	Posibles sanciones por incumplir normativas anti-spam

3. Qué revelan los logs

1. **Volumen inusual de mensajes:** picos que indican un robot o script.
2. **Fallos de autenticación repetidos:** intentos de forzar contraseñas.
3. **IPs desconocidas enviando correo:** posible exploiter de credenciales.
4. **Bloqueos externos (RBL):** rebotes con errores 550/451 apuntando a spam.

4. Beneficios de un monitoreo constante

- **Reacción temprana:** se bloquea la actividad antes de que sea masiva.
- **Reputación protegida:** menos riesgo de terminar en listas negras.
- **Visibilidad:** se identifican usuarios o scripts mal configurados.

- **Cumplimiento:** ayuda a demostrar buenas prácticas anti-spam.
-

5. Flujo de detección (conceptual)

1. **Rotación diaria** de logs.
2. **Revisión automática** para buscar patrones sospechosos.
3. **Alerta** al administrador si se supera un umbral.
4. **Acción:** bloqueo temporal de IP/cuenta y análisis manual.

“ Resultado: el servidor permanece limpio y los correos legítimos llegan a destino.

6. Conclusión

Supervisar los registros de Exim no es un lujo, sino una **medida esencial de higiene y reputación**.

Permite detectar uso indebido, evitar bloqueos globales y garantizar que el correo de la organización siga siendo confiable.

Aviso

Esta documentación y su contenido, no implica que funcione en tu caso o determinados casos. También implica que tienes conocimientos sobre lo que trata, y que en cualquier caso tienes copias de seguridad. El contenido el contenido se entrega, tal y como está, sin que ello implique ningún obligación ni responsabilidad por parte de [Castris](#)

Si necesitas soporte profesional puedes contratar con Castris [soporte profesional](#).

Revision #3

Created 2025-06-19 08:28:53 UTC by Abkrim

Updated 2025-06-19 08:52:43 UTC by Abkrim