Registro y Validación del “abuse-c” y “abuse-mailbox”

Propuesta de Política LAC-2018-5 V2

Jordi Palet
(jordi.palet@theipv6company.com)

Resumen

- La política actual (ASN) no es clara en cuanto a la obligación de registrar un contacto de abuse (abuse-c) ni al formato específico y si aplica a otros casos de registros en el whois.

- Como consecuencia, puede haber LIRs que no tienen dicho contacto registrado para sus recursos, o incluso hay casos de LIRs que utilizan un buzón de correo inexistente o que no es procesado.

- Ello origina en la práctica, que dicho contacto sea ineficaz para poder reportar abusos y en general problemas de seguridad y costes para las víctimas.

- Esta propuesta pretende resolver el problema y garantizar la existencia de un contacto abuse-c correcto y el proceso para su uso .

Justificación

- La comunidad de Internet se basa en la colaboración, pero en muchas ocasiones esto no es suficiente y hace falta que todos podamos ser capaces de contactar con aquellos LIRs que pueden tener un problema en la red y no conocerlo.

- Esta propuesta crea una nueva sección en el manual de políticas, para permitir resolver este problema, por medio de una sencilla verificación periódica y establece las reglas básicas para la misma y evitar así costes innecesarios a terceras partes en su función de contactar con los responsables de resolver los abusos de una determinada red.

- La propuesta garantiza que el coste de procesar los abusos recaiga sobre el LIR cuyo cliente está provocando el abuso (y del cual recibe compensación económica por el servicio), en lugar de recaer sobre la víctima, tal y como ocurriría si hubiera que acudir a la vía judicial, evitando por lo tanto el agravamiento económico (abogados, procuradores, etc.) y en tiempo, para ambas partes.

- Para ello, el atribute abuse-c, que hasta ahora sólo estaba referenciado para el objeto “aut-num”, se hace obligatorio en los objetos “inetnum” e “inetnum6”, y cualesquiera puedan surgir en el futuro. Este atributo es un contacto de abuso, que contendrá como mínimo el atributo “abuse-mailbox”

Texto Propuesto (1)

12. Registro y Validación de “abuse-c” y “abuse-mailbox”

12.1. Descripción del “abuse-c” y “abuse-mailbox”

Todos los recursos distribuidos por LACNIC deben incluir, obligatoriamente, en la entrada de WHOIS correspondiente, el atributo de contacto “abuse-c” (contacto de abuso) como mínimo con un único email (abuse-mailbox) válido, monitorizado y adecuadamente atendido, que permita enviar reportes manuales o automáticos de comportamientos abusivos, seguridad, y similares.

El atributo “abuse-mailbox” debe estar disponible sin restricciones vía whois, APIs y futuras técnicas.

Teniendo en cuenta la naturaleza jerárquica de los objetos de direcciones IP, los objetos heredados de aquellos distribuidos directamente por LACNIC, pueden estar cubiertos por los objetos de nivel superior o tener su propio atributo “abuse-c”.

Siguiendo prácticas habituales, otros atributos “e-mail” pueden ser incluidos para otros propósitos.

Texto Propuesto (2)

12.2. Características del “abuse-mailbox”

Los emails enviados a ”abuse-mailbox” deben requerir intervención manual en algún momento, por parte del destinatario, y no pueden estar filtrados, ya que ello podría impedir, que en algunos casos, el envío de un reporte de abuso, por ejemplo por spam, al incluir el propio mensaje de spam o URLs o contenidos habitualmente clasificados como spam, evite su recepción.

El buzón “abuse-mailbox” podrá devolver inicialmente, una respuesta automática, por ejemplo, asignando un número de ticket, aplicando procedimientos de clasificación, pidiendo más información, etc. Sin embargo, no podrá requerir el uso de un formulario, ya que ello implicaría que cada empresa que necesite reportar abusos, generalmente de forma automatizada, se vea obligada a desarrollar una interfaz específica para cada caso de abuso, lo cual es inviable e ilógico, ya que haría recaer el coste del procesado de los abusos en el que envía la reclamación y por tanto es víctima del abuso, en lugar de ser costeada por aquel cuyo cliente (y de quién recibe ingresos), causa el abuso.

A título informativo, cabe mencionar que, lo razonable, es que quien reporta el abuso, lo haga desde el primer momento y en ese primer reporte, enviando los logs, o copia del spam (adjuntando ejemplo del email de spam o sus cabeceras completas) o similares, que demuestren el abuso. Igualmente, es razonable esperar que el email inicial de auto-respuesta indique que, si no se han enviado dichos registros, no será atendido, dando así la oportunidad a repetir el envío con las pruebas procedentes. Esto permite reportes automatizados, por ejemplo, mediante fail2ban, SpamCop u otros, con mínimo coste para ambas partes.

Texto Propuesto (3)

12.3. Objetivos de la validación del “abuse-c”/“abuse-mailbox”

El procedimiento, que habrá de ser desarrollado por LACNIC, deberá cumplir con estos objetivos:

Proceso simple que garantice su funcionalidad y permita a los “helpdesk” que atienden los reportes de abuso, verificar que las peticiones de validación efectivamente provienen de LACNIC y no de terceras fuentes (que pudieran implicar riesgos de seguridad), evitando, por ejemplo, una única URL “directa” para la validación.

1. Impedir un proceso automatizado.
2. Confirmar que quien valida asegura conocer el procedimiento, la política, que monitoriza regularmente el “abuse-mailbox”, se toman medidas y se responde al reporte de abuso.
3. Plazo de validación no superior a 2 días hábiles.
4. Si no se valida correctamente, escalado con el LIR y un nuevo plazo, no superior a 3 días hábiles.

(a título de ejemplo se propone un procedimiento detallado en “información adicional” de esta propuesta de política)

Texto Propuesto (4)

12.4. Validación del “abuse-c”/“abuse-mailbox”

LACNIC validará el cumplimiento de los puntos anteriores, tanto en el momento en que se crean o modifican los atributos “abuse-c” y/o “abuse-mailbox”, periódicamente, no menos de una vez cada tres meses y en cualquier momento que LACNIC considere oportuno.

A criterio de LACNIC, de forma generalizada o en casos puntuales (por ejemplo para la confirmación en casos de escalado según el 12.5), LACNIC podrá utilizar dominios diferentes a lacnic.*, e incluso modificar el asunto y cuerpo del mensaje, para realizar dichas validaciones.

El incumplimiento, implicará un seguimiento más exhaustivo, de conformidad con las políticas/procedimientos pertinentes de LACNIC y especialmente “7.1. Recuperación de recursos”.

Texto Propuesto (5)

12.5. Mecanismo de escalado a LACNIC

Con el objetivo de evitar engaño (por ejemplo, “abuse-mailbox” que solo responden a emails de LACNIC, a determinado asunto o determinado cuerpo del mensaje), o el incumplimiento del resto de los aspectos de esta política (la incorrecta o no atención de los casos de abuso) y, por lo tanto, para garantizar la calidad de los servicios en la región con los recursos distribuidos por LACNIC, se dispondrá de un buzón (por ejemplo, “escalado-abusos@lacnic.net”), que permita escalar dichas situaciones, permitiendo así la re-validación (según el punto 12.4 anterior) e incluso la intermediación de LACNIC y en su caso, la aplicación de las políticas/procedimientos pertinentes y especialmente “7.1. Recuperación de recursos”.

Información Adicional

Ejemplo de procedimiento de validación:

1. La validación se inicia de forma automatizada, por parte de LACNIC, con el envío de DOS emails consecutivos al “abuse-mailbox”.
2. Dichos emails tendrán exclusivamente formato texto.
3. El primero de los emails contendrá la URL donde debe realizarse la validación, que será “validacion.lacnic.net”, y podrá contener información respecto del procedimiento, extracto de esta política, etc.
4. El segundo de los emails contendrá un código alfanumérico único de validación.
5. El receptor que atiende el “abuse-mailbox”, deberá acceder a la URL y pegar en el formulario el código recibido en el segundo email.
6. Dicha URL, deberá estar diseñada de tal forma que impida un proceso automatizado (por ejemplo, “captcha”), y contendrá un texto que confirme que el receptor de la validación conoce el procedimiento, la política y que monitoriza de forma regular el “abuse-mailbox” y se toman medidas apropiadas para resolver los abusos reportados y responder a los mismos, con un “checkbox” que necesariamente deberá ser aceptado.
7. El código alfanumérico sólo será válido durante un máximo de 2 días laborables.
8. Si el código no es introducido en ese plazo, el sistema marcará el “abuse-c” como “provisionalmente inválido”, y alertará al staff de LACNIC para que se pueda iniciar el seguimiento personalizado con el LIR.
9. En caso de no obtener una respuesta, con la confirmación de la corrección de la situación, en un plazo adicional de 3 días laborables, el “abuse-c” será marcado de forma permanente como “inválido”.
10. Se repetirá de forma automática el proceso de validación (puntos 1 al 7 anteriores), y en este caso, el “abuse-c” será marcado como “válido” en caso satisfactorio, o en caso insatisfactorio, se trataría de un caso de incumplimiento de la política.

Tiempo de Implementación

- 90 días, de forma prudencial y a confirmar con LACNIC, para permitir tanto al staff el desarrollo de la herramienta, como a los LIRs actualizar sus contactos abuse-c.

Referencias

- En RIPE se está tramitando una propuesta similar, aunque aún está en debate y no ha alcanzado consenso (a fecha de envío de esta propuesta).

- En AfriNIC se ha presentado también.

- **En APNIC esta propuesta obtuvo consenso hace 2 semanas.**

Análisis de Impacto (LACNIC)

- Comentarios del staff:

- En la sección 12.4 y 12.5, cuando se indica “El incumplimiento, implicará un seguimiento más exhaustivo, de conformidad con las políticas/procedimientos pertinentes de LACNIC y especialmente "7.1. Recuperación de recursos", LACNIC entiende que en este caso aplicaría la política 7.1.
- Se observa que para la implementación de esta propuesta LACNIC necesitará invertir nuevos recursos para atender el seguimiento de todos los casos que lo necesiten.
- En la propuesta se hace referencia al objeto “inetnum6 “. En el whois de LACNIC, solamente se hace referencia al objeto inetnum, tanto para IPv4 e IPv6.
- Se recomienda poner la sección del apéndice sin numeración, sino como A. (apéndice). Esta recomendación es con el fin de no tener que actualizar la numeración del apéndice tantas veces como secciones que se agreguen al manual, lo cual podría generar errores debido a todas las referencias al apéndice (sección 12), que aparecen en todo el texto del manual de políticas.