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

LAC-2018-5 v5

Jordi Palet - jordi.palet@theipv6company.com

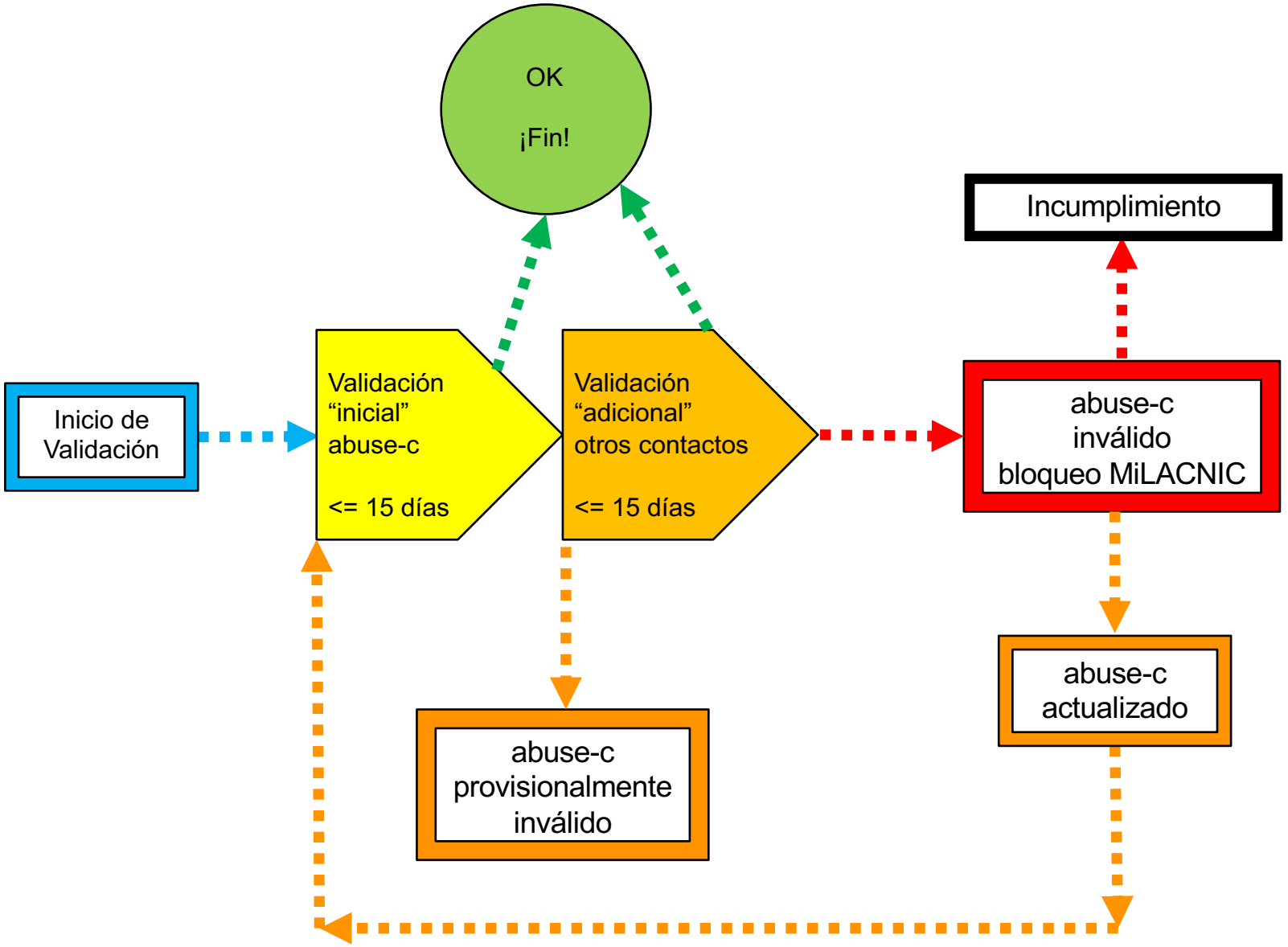
Resumen

- La propuesta permite garantizar y validar los contactos de abuso del WHOIS (abuse-c y abuse-mailbox) de las organizaciones y poder así reportar los casos de abuso.

Justificación

- 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.
- Puede haber receptores de recursos de LACNIC que no tienen dicho contacto registrado para sus recursos
  - Incluso hay casos que utilizan un buzón de correo inexistente o que no monitorizado.
- La falta de validación ha vuelto ineficaz el reporte de casos de abusos, generando problemas de seguridad y costes para las víctimas.
- Se plantea una sencilla verificación periódica del contacto de abuso.
- Para ello, el atributo abuse-c, que hasta ahora sólo estaba referenciado para el objeto “aut-num”, se hace obligatorio en los objetos “inetnum” (tanto para IPv4 como para IPv6), y cualesquiera puedan surgir en el futuro. Este atributo es un contacto de abuso, que contendrá como mínimo el atributo “abuse-mailbox”.

Proceso de Validación



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 (y por tanto ocultar URLs que correspondan a ataques como “phishing”, etc.).
3) A criterio de LACNIC, de forma generalizada o en casos puntuales (por ejemplo para la confirmación en casos de escalado según el 12.6), LACNIC podrá utilizar dominios diferentes a lacnic.*, e incluso modificar el asunto y cuerpo del mensaje, para realizar dichas validaciones de forma mas eficaz.
4) 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.
5) El segundo de los emails contendrá un código alfanumérico único de validación.
6) El receptor que atiende el “abuse-mailbox”, deberá acceder a la URL y pegar en el formulario el código recibido en el segundo email.
7) 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.
8) El código alfanumérico sólo será válido durante un máximo de 15 días.
9) 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 receptor del recurso.
10) En caso de no obtener una respuesta, con la confirmación de la corrección de la situación, en un plazo adicional de 15 días, el “abuse-c” será marcado de forma permanente como “inválido”.
11) 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.
12) LACNIC contará con mecanismos (formulario, correo electrónico y otros en el futuro) para facilitar el escalado en los casos en los que se quiera reportar un incumplimiento de esta política. Ello permitirá la re-validación (12.4) y la intervención de LACNIC en aplicación de las políticas, procedimientos y requisitos contractuales vigentes.

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 receptores de recursos de LACNIC actualizar sus contactos abuse-c.
- LACNIC podrá enviar un recordatorio con la ratificación de la propuesta por parte del Directorio.

Referencias

- En APNIC ha alcanzado consenso una versión equivalente a esta propuesta.
- En RIPE se adoptó una propuesta similar pero solo de verificación automática, y el debate reciente de la lista, precisamente ha indicado la necesidad de hacerlo de forma “no exclusivamente automática”, pues el procedimiento actual permite numerosos engaños.
- En RIPE, AfriNIC y ARIN se ha presentado una propuesta equivalente.

Análisis de Impacto (LACNIC)

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 que utilicen los sistemas de registro de LACNIC deben incluir obligatoriamente, en las entradas de WHOIS correspondientes, el atributo de contacto abuse-c (contacto de abuso), como mínimo con un 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 tecnologías.

Teniendo en cuenta la naturaleza jerárquica de los objetos, los heredados de aquellos distribuidos directamente por LACNIC (por ejemplo, sub-asignaciones), estan cubiertos por los objetos de nivel superior y su propio atributo “abuse-c” es opcional.

Siguiendo prácticas habituales, otros atributos “email” 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, en algunos casos, la recepción de un reporte de abuso. Por ejemplo, un reporte de spam, al incluir el propio mensaje de spam o URLs o contenidos habitualmente clasificados como spam.

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 entidad que necesite reportar abusos, generalmente de forma automatizada, se vea obligada a desarrollar una interfaz específica para cada receptor de recursos al que tiene que reportar un abuso. Ello sería inviable, ya que haría recaer el coste del procesado de los abusos en el que envía la reclamación, víctima del abuso, en lugar de sobre aquel que (directa o indirectamente) causa el abuso.

Lo razonable, es que quien informa del abuso, lo haga en el primer reporte, enviando información suficiente (log, copia del spam o cabeceras completas, lo equivalente en cada tipo de abuso). Igualmente, es razonable que el email inicial de auto-respuesta indique que, si no se ha enviado dicha información, 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. Habitualmente, cabe esperar que, si se ha asignado un número de ticket, el mismo sea mantenido en todas las comunicaciones (típicamente como parte del asunto).

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:

1) Garantizar su funcionalidad y permitir a los “helpdesk” que atienden los reportes de abuso, la verificación de que la validación efectivamente proviene de LACNIC y no de terceras fuentes (implicando riesgos de seguridad, evitando, por ejemplo, una única URL “directa” para la validación).
2) Impedir un proceso exclusivamente automatizado.
3) Confirmar que quien valida:
   - asegura conocer el procedimiento y las políticas de LACNIC
   - monitoriza regularmente el “abuse-mailbox”
   - toma medidas al respecto
   - responde al reporte de abuso.
4) Plazo de validación “inicial” de 15 días.
5) Si no se valida correctamente, “escalado” con el resto de los contactos disponibles, en un plazo “adicional” de 15 días.

Los plazos de validación podrán ser modificados a criterio de LACNIC, informando a la comunidad de los motivos.

(a título de recomendación, 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 la política de forma periódica, al menos dos veces al año, y cuando se creen o modifiquen los atributos del “abuse-c”.

La frecuencia de validación podrá ser modificada a criterio de LACNIC, informando a la comunidad de los motivos.

Texto Propuesto (5)

12.5. De los incumplimientos

El incumplimiento por parte de cualquier organización se produce si no se ha validado en el plazo “inicial” ni “adicional”. Ello implicará el bloqueo de MiLACNIC y medidas equivalentes en los sistemas de los NIRs, para todos los recursos asociados con dicha organización. Quedan exceptuadas las cuestiones exclusivamente contractuales y relacionadas con pagos, así como la actualización de los contactos abuse-c/abuse-mailbox, de tal forma que puedan ser automáticamente re-validados para permitir el desbloqueo de MiLACNIC.

Cualquier acceso a MiLACNIC (o sistemas equivalentes de los NIRs), durante dicho bloqueo, mostrará un mensaje de advertencia, incluyendo el texto de esta política, y para permitir continuar será necesario que dicho mensaje sea “leído” hasta el final, y se confirme mediante un check-box o similar. Se podrán utilizar mecanismos equivalentes adaptados al avance de la tecnología.

De mantenerse el incumplimiento, LACNIC actuará de conformidad con sus políticas y procedimientos pertinentes.

Texto Propuesto (6)

12.6. Mecanismo de escalado a LACNIC

Comportamientos fraudulentos (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), podrán ser reportados a LACNIC, para su re-validación según 12.4.