

ABC sobre las nuevas medidas de la CRC contra el fraude mediante llamadas y mensajes de texto

La Comisión de Regulación de Comunicaciones (CRC) expidió la Resolución CRC 8308 de 2026, que establece nuevas herramientas para identificar comunicaciones sospechosas, dificultar la suplantación y ayudar a las personas a tomar decisiones más informadas antes de contestar una llamada o responder un mensaje.

En Colombia se reclaman más de **\$252 millones diarios** por fraudes asociados a llamadas y mensajes de texto. Entre 2022 y 2024, el valor de estas reclamaciones se triplicó, al pasar de \$30.622 millones a \$92.235 millones.

1. ¿Cuál es el objetivo de la resolución?

Reducir las oportunidades para la suplantación, facilitar la identificación de llamadas y mensajes y mejorar la capacidad del sector para detectar comportamientos atípicos.

En términos sencillos, la CRC busca que las personas tengan más información para verificar quién las contacta antes de contestar, responder o compartir datos.

2. ¿Estas medidas acabarán con el fraude?

No existe una medida que elimine por completo el fraude. Las nuevas reglas incorporan más alertas, controles y mecanismos de verificación para dificultar la suplantación y detectar más rápido posibles irregularidades.

Para contrarrestar estos delitos se requiere además que las personas actúen con cautela y no compartan datos personales, claves o códigos de seguridad sin verificar primero quién las contacta.

Medidas para las llamadas

3. ¿Cómo se identificarán las llamadas sospechosas?

Los operadores deberán analizar las llamadas en tiempo real. Cuando detecten comportamientos atípicos, en la pantalla del usuario aparecerá la advertencia: **"Alerta de llamada sospechosa"**.

4. ¿En qué casos podría aparecer esta alerta?

Por ejemplo, cuando una línea realice muchas llamadas cortas y repetitivas en poco tiempo.

5. ¿La alerta significa que la llamada es un fraude?

No. La alerta no confirma que exista un fraude. Es una advertencia preventiva para que la persona actúe con mayor cautela y verifique quién la está llamando.

6. ¿Qué debe hacer una persona si recibe una llamada con esta alerta?

Se recomienda:

- No entregar datos personales o financieros.
- No compartir claves ni códigos de seguridad.
- Evitar tomar decisiones bajo presión.
- Finalizar la llamada y comunicarse directamente con la empresa o entidad mediante sus canales oficiales.

7. ¿Cómo se identificarán las llamadas comerciales?

Las empresas deberán registrar ante su operador los números utilizados para realizar llamadas comerciales. Cuando una llamada provenga de una de estas líneas, aparecerá la etiqueta: **"Llamada con fines publicitarios"**.

Por ejemplo, si una empresa llama para ofrecer un plan de telefonía, un seguro o una tarjeta de crédito, el usuario podrá conocer el propósito de la comunicación antes de decidir si contesta.

8. ¿Una llamada identificada como publicitaria es sospechosa?

No necesariamente. La etiqueta solo informa que la llamada tiene una finalidad comercial. No significa que se trate de un fraude.

9. ¿Qué llamadas deberán ser bloqueadas?

Los operadores deberán impedir las llamadas realizadas desde:

- Números que no han sido asignados oficialmente.
- Números habilitados únicamente para recibir llamadas.
- Números que no están autorizados para originar comunicaciones.

Por ejemplo, si un número fue destinado exclusivamente para recibir llamadas de atención al cliente, no podrá utilizarse para llamar a los usuarios.

10. ¿Qué ocurrirá con las llamadas internacionales que aparecen como colombianas?

Serán bloqueadas cuando se detecte que una llamada realizada desde otro país intenta mostrarse en pantalla como si proviniera de un número colombiano.

Esta medida busca evitar que una persona confíe en una llamada solo porque ve un número nacional. Comenzará a aplicarse una vez la CRC defina las condiciones técnicas necesarias.

11. ¿Se bloquearán las llamadas de colombianos que están en el exterior?

No, cuando se trate de casos legítimos de roaming internacional, es decir, cuando una persona utilice su línea colombiana mientras se encuentra fuera del país.

Medidas para los mensajes de texto

12. ¿Qué cambiará en los mensajes enviados por empresas y entidades?

Los mensajes automáticos enviados por bancos, comercios, entidades públicas, plataformas y otras organizaciones deberán permitir identificar con claridad:

- **Quién los envía:** el remitente deberá estar registrado.
- **Cómo se envían:** deberán utilizar un código corto autorizado.
- **Qué tipo de mensaje es:** el contenido deberá corresponder a un formato registrado previamente.

13. ¿Qué mensajes están incluidos?

Entre otros:

- Alertas bancarias o de transacciones.
- Códigos de autenticación o seguridad.
- Confirmaciones de pedidos.
- Recordatorios de citas.
- Avisos relacionados con trámites o servicios.

Cuando una persona reciba uno de estos mensajes, será posible verificar que realmente proviene de la empresa o entidad que aparece como remitente.

14. ¿Cómo se verificará esa información?

Se implementará un sistema central que reunirá la información de las empresas, las marcas, los remitentes, los códigos y los tipos de mensajes registrados.

Los operadores consultarán este sistema antes de entregar los mensajes a los usuarios.

15. ¿Las medidas restringirán las alertas bancarias, los códigos de seguridad o las confirmaciones de pedidos?

No. El objetivo no es limitar estos mensajes, sino permitir que su origen pueda verificarse y reducir el riesgo de que alguien se haga pasar por un banco, un comercio, una entidad pública o una plataforma.

Una vez finalice el periodo de transición, los mensajes empresariales cuyo origen o contenido no pueda verificarse no serán entregados a los usuarios.

16. ¿Qué es un código corto?

Es un número de pocos dígitos utilizado por empresas y entidades para enviar mensajes automáticos, como alertas, códigos de seguridad o confirmaciones.

Con las nuevas medidas, estos códigos deberán estar autorizados y asociados con un remitente identificado.

17. ¿Qué pasará con los mensajes masivos enviados desde líneas móviles comunes?

Los operadores deberán detectar cuando una línea móvil común sea utilizada de manera inusual para enviar mensajes masivos o automatizados.

Por ejemplo, si una línea personal comienza a enviar cientos o miles de mensajes iguales en poco tiempo, el operador deberá analizar si se trata de una actividad legítima o de un posible uso irregular.

18. ¿La línea será bloqueada inmediatamente?

No. La respuesta será gradual. El operador deberá:

1. Analizar el comportamiento detectado.
2. Informar al titular de la línea.
3. Permitirle explicar si existe una razón legítima.
4. Aplicar controles adicionales si el comportamiento continúa.
5. Restringir temporalmente el envío de mensajes cuando sea necesario.

El usuario podrá solicitar la revisión de la medida.

Coordinación y pedagogía

19. ¿Qué papel tendrá la CRC?

La CRC liderará el Comité Técnico de Lucha contra el Fraude en Redes de Servicios Móviles, un espacio para compartir alertas, analizar nuevas modalidades de fraude y coordinar acciones entre operadores, empresas de mensajería y autoridades.

También realizará seguimiento a la implementación de las medidas y promoverá acciones permanentes de información, prevención y actualización de las medidas ya adoptadas.

20. ¿Cómo se explicarán estas medidas a los ciudadanos?

La CRC pondrá en funcionamiento un micrositio con información, guías y recomendaciones para reconocer señales de alerta y saber cómo actuar frente a una llamada o un mensaje sospechoso.

Los operadores y demás actores involucrados deberán realizar, como mínimo, cuatro campañas pedagógicas al año, con contenidos claros, accesibles y dirigidos especialmente a las poblaciones con mayores riesgos o menores niveles de alfabetización digital.

Implementación

21. ¿Cuándo comenzarán a aplicarse las medidas?

La implementación será gradual:

- **En tres meses:** identificación de llamadas sospechosas y publicitarias, y bloqueo de números que no deben originar llamadas.
- **En seis meses:** monitoreo de mensajes masivos enviados desde líneas comunes y puesta en funcionamiento del micrositio pedagógico.

- **En doce meses:** entrada en operación del sistema de identificación y validación de mensajes empresariales. Este plazo comenzará a contarse desde la expedición del acto que defina la remuneración de este ecosistema.
- **Posteriormente:** bloqueo de llamadas internacionales que aparenten provenir de Colombia, una vez se adopten las condiciones técnicas.

22. ¿Dónde puede consultarse la resolución?

La Resolución CRC 8308 de 2026 y el documento de respuesta a comentarios pueden consultarse en: <https://www.crcm.gov.co/es/proyectos-regulatorios/2000-41-7-1>

Recuerde

Una alerta ayuda a tomar precauciones, pero no reemplaza la verificación. Antes de entregar información, ingresar a un enlace o realizar un pago, comuníquese directamente con la empresa o entidad mediante sus canales oficiales.