Outlook

Comentarios y aportes proyecto regulación mensajes masivos

Desde Ing. German Cruz <ceoyear@gmail.com>
Fecha Sáb 06/06/2026 12:53
Para [2025] [DR] Medidas para mitigar el fraude cibernético <medidasantifraude@crcom.gov.co>

Buen día

Los interesados en que se protejan los usuarios son los mismos usuarios de número celular en Colombia. Para un operador de mensajes masivos su núcleo de negocio es vender mensajes y entre más mensajes mejor, y si no hay barreras para enviar mensajes muchísimo mejor, si la multa impuesta puede ser asumida vendiendo aún más mensajes, una multa no afecta.

1. Se debe implementar una página de la crcom donde se pueda digitar el código corto y como resultado muestre las empresas que hagan uso de ese uso de ese número masivo junto con las posibles tipos de mensaje, con el fin que el usuario de celular antiguo, pueda consultar el número en la página web desde otro dispositivo que no sea un celular smartphone, ejemplos:
Código corto 87787: Red Mas (Noticias)
Código corto 890059: Registraduria Civil Nación (Designaciones Jurado, Cambio de cédula digital, Notificaciones), Azteca Comunicaciones (Cobros, Ventas, Premiaciones), BRE-B (Notificaciones), Cooperativas (Notificaciones)
Código corto 87881: Rendinstantic (cobro jurídico)
Código corto 892000: Rendinstantic (cobro jurídico con descuentos)
Código corto 899097: Rendinstantic (amenazas de cobro jurídico incremental)
Código corto 893182: Estafa phishing enlace malicioso.
Código corto 87377: Nueva-EPS (Recordatorios).
Código corto 898944: Nueva-EPS (Amenazas de no continuidad de servicio), MinTransporte (Recordatorios)
Código corto 890708: Microsoft (2FA)
Código corto 85980: SPAM link hacia whatsapp ganar plata en una hora.
Código 894466: Movistar (Ofertas), Cooperativas (Notificaciones)
Código corto 89902: Estafa link hacia whatsapp reclamar premio.
Código corto 898912: Cooperativas (Premiaciones, Notificaciones, Cobros cartera, Avisos asamblea general)
Código corto 3333: Claro (Notificaciones, Premiaciones)
Código corto 890103: Claro (Recordatorios).
Código corto 1002: Claro (Notificaciones)
Código corto 892717: Claro (Recordatorios).
Código corto 87638: Claro (Ofertas).
Código corto 85437: Asopagos (Notificaciones)
Código corto 891150: BRE-B (Notificaciones)
Código corto 890023: TV-Colombia (Facturación)
Código corto 890162: TV-Colombia (Facturación)
Código corto 893252: TV-Colombia (Notificaciones, Facturación)
Código corto 890037: BanAgrario (Notificaciones)
Código corto 85049: Whatsapp (2FA), Claude (2FA).
Código corto 363: Movistar (Notificaciones)

Código corto 85301: Mercado libre (Notificaciones), Telegram (2FA)
Código corto 87770: Mercado libre (2FA).

2. Se debe obligar a las empresas operadoras de códigos cortos masivos a asignar un rango de números fijo a empresas fijas y reportar cada asignación a la crcom.

3. Obligar a las empresas operadoras de códigos cortos masivos a analizar cada plantilla de mensaje de texto del sender con inteligencia artificial en busca de Spam, Phishing, Amenazas, y otras violaciones a la norma, antes de ser enviado masivamente; en caso positivos se debe notificar al sender que tiene una alarma y el mensaje masivo no se ha podido enviar por favor revise el mensaje masivo para remediar, si es recurrente en alarmas su cuenta será bloqueada e informada a la crCom por generar plantillas masivas que violan la norma, para desbloquear debe contactarse con el administrador. Esto el lo más importante de toda la regulación que es el control activo que permite filtrar lo que está fuera de la norma de lo que está dentro de la norma, sin este paso, un cracker podría NO leer la norma y enviar spam y ya, pues no se tomó la tarea de leer la norma ni de analizar si el mensaje es spam, pero si hay un control activo de por medio no se podrá enviar el mensaje masivo, así soborne generosamente y exitósamente a la empresa operadora de códigos cortos masivos ya que el soborno cubre la multa que se imponga cubre abogados que demanden especulativamente a quien diga la palabra soborno + nombre de empresa así pierdan la demanda, la inteligencia artificial la debería operar un tercero, ya que un actor estatal extranjero malicioso podría comprar toda la empresa operadora de mensajes masivos de phishing, comprar un empresa al borde de quiebra y mandar los mensajes pichos en nombre del quebrado, sin necesidad de aplicar generosos sobornos que cubran la multa y luego revender, liquidar o abandonar las dos empresas una vez logrado el cometido.

3. Las operadoras de celular (*claro, movistar, tigo, otros*) deben guardar en bases de datos comprimido por un plazo de un mes la totalidad de mensajes masivos excepto aquellos que sean 2FA (s*egundo factor de autenticación, esto es fácil de saber si se implanta el punto 2 descrito anteriormente*) diariamente que pasen por sus torres que sean generados por medio del listado de códigos cortos de empresas registradas, después de ese periodo solo guardar una muestra representativa con el fin de consultar Phising, SPAM y amenazas, con el objetivo de cruzar con las operadoras de códigos cortos masivos en caso de corrupción (sobornos, actores estatales extranjeros maliciosos) para borrar plantillas o alterarlas antes de envío o adulterarlas después de cometida la infracción para que parezca que eso es un error de otro y que nunca hubo violación de la norma.

4. La crcom debería tener una página donde se reciban quejas de manera fácil, donde no toque llenar un formulario gigante, si no simplemente escribir el código corto (*se muestre las empresas relacionadas y los tipos de mensaje que estas emiten*), un chulito para agregar una muestra -con fecha hora- del mensaje recibido y otro chulito de agregar correo si quiere ser notificado sobre la queja, luego hacer un cruce con la base de datos para revisar si es verdad la queja (*comparar la muestra de la fecha y hora versus mensajes enviados en esa hora aproximada*) o es otra empresa implantando falso testimonio a través del pitufeo de quejas o alguien simplemente no contento o inconforme.

En este caso un control activo (*inteligencia artificial revisa mensajes en búsqueda de spam, amenazas y phising antes de ser enviado masivamente*) es mucho mejor que un control pasivo (*el sender se ponga la mano en el corazón y lea la norma, recuerde las capacitaciones y charlas de la moral y la etica, y genere una plantilla de mensaje masivo sin violar la norma, a pesar de saber que la ganancia final puede cubrir la multa*).

Att,

--

Germán Alberto Cruz Vargas
Usuario de número celular
CEOyear@gmail.com