**Ibagué, 4 de enero de 2025**

**Comunicado de prensa 013**

# ¡No se deje estafar! Inescrupulosos están pidiendo plata en perfiles falsos de redes a nombre de la Alcaldesa

*¡No caiga! La Mandataria no solicita dinero por ningún motivo, razón o circunstancia.*

Con el objetivo de prevenir a la ciudadanía y evitar que personas caigan en una estafa, la alcaldesa Johana Aranda informa que por ninguna causa está solicitando dinero a través de sus redes sociales u otro medio.

En efecto, en las últimas horas las autoridades detectaron que perfiles falsos de la mandataria son utilizados por inescrupulosos para pedir plata a personas a cambio de la realización de favores, como conseguir un empleo o cupos en colegios.

Es importante resaltar que no se trata de los perfiles oficiales de la Alcaldesa, sino montajes falsos, burdos, recién creados, sin seguidores, donde los delincuentes utilizan las fotos de la primera autoridad del Municipio, incluso de su campaña, como se puede apreciar en el siguiente link o enlace de la red social Facebook: **https://www.facebook.com/jhoana.aranda.2024?mibextid=ZbWKwL**

Estos intentos de estafa ya están en las manos de las autoridades competentes y expertos en delitos informáticos, que iniciaron las investigaciones pada dar con el paradero de los responsables y evitar que inocentes caigan en la trampa.

La oferta de empleos, cupos escolares y otros bienes y servicios es una de las estafas más comunes que utilizan en Colombia para exigir sumas de dinero por trámites inexistentes, como cursos de actualización, exámenes médicos, seguros o agilización de desembolsos de créditos.

También están las redes sociales 'hackeadas' para hacerse pasar por familiares o amigos con lo que los delincuentes envían mensajes a los contactos de los usuarios, ofreciendo encomiendas desde el exterior, dólares a buen precio, e incluso solicitando dinero en situaciones de supuestos apuros o extorsión.

Finalmente, **tenga en cuenta las siguientes recomendaciones de expertos en ciberdelitos para evitar estafas en redes sociales:**

- Desconfiar de mensajes que ofrezcan ventajas exageradas, grandes descuentos u ofertas "gratis". Estas son las promesas más comunes en estafas en línea.

- Verificar la dirección de los mensajes y sitios web. Prestar atención a los errores gramaticales o el uso de términos genéricos. Los sitios oficiales siempre comenzarán con el nombre de la institución. La ausencia del nombre es una alerta importante de estafa.

- Tener cuidado con las publicaciones en redes sociales, especialmente las promovidas. Muchas de las 'deepfakes' se comparten de esta manera para que la víctima haga clic y descargue una aplicación o proporcione sus datos personales. Solo abra mensajes y haga clic en enlaces si está seguro de que puede confiar en el remitente.

- Si un remitente es legítimo, pero el contenido del mensaje parece extraño, vale la pena verificarlo a través de un canal de comunicación alternativo, como una llamada.