COSTA RICA
GOBIERNO DEL BICENTENARIO
2018 - 2022

ebadilla@jps.go.cr
Calle 20, San José. CR.
2522-2012
www.jps.go.cr

JUNTA DE PROTECCIÓN SOCIAL
JPS
Institución Benemérita ¡...para hacer el bien!

JPS ALERTA DE POSIBLES ESTAFAS

El día de hoy la Junta de Protección Social –JPS- tuvo conocimiento de que una persona que se identifica como funcionario de la Proveeduría institucional contactó a varios oferentes de pauta publicitaria con intención de obtener datos personales que podrían conducir a estafas. En tal sentido **la JPS aclara que NO está solicitando ninguna información** relacionada con contrataciones vía la red de compras SICOP, ni de la firma digital de las personas.

El sujeto llama con claras intenciones de generar un ambiente de confianza y cordialidad para lograr obtener la información de su interés, la que podría vulnerar la seguridad de datos privados y sensibles de las personas, relacionadas con operaciones financieras y trámites de contratación por vías digitales.

El individuo llega incluso a citar el número de la central telefónica de la JPS. En al menos un caso documentado, la persona que recibe la llamada le cuestionó por qué, si es funcionario de esta institución realiza la llamada desde un número privado que impide su identificación, corta la comunicación.

La JPS reitera que no está solicitando actualización de datos por ninguna vía. Todas las compras se realizan por la plataforma de compras SICOP del sector público costarricense.

SICOP ya emitió alertas y recomendaciones en ese sentido, las que le reenviamos por si le pueden ser útiles.

Estimados Usuarios:

Ante la constante amenaza de estafas por medio de diferentes estrategias, en el cual utilizan el nombre del Sistema Integrado de Compras Públicas (SICOP) o información extraída de los proceso de contratación de las diferentes Instituciones Públicas, queremos a continuación recordarles algunas pautas importantes que nos pueden ayudar a protegernos de estas conductas inescrupulosas:

1. **Detecte a los impostores.** Los estafadores suelen hacerse pasar por alguien que le inspira confianza, por ejemplo, **un funcionario del gobierno**, **un agente del Call Center**, o una compañía con la cual usted tiene una relación comercial. No envíe dinero ni dé su información personal en respuesta a un pedido inesperado — ya sea que lo reciba por mensaje de texto, llamada de teléfono o email.

2. **No confíe en lo que indica su aparato de identificación de llamadas.** Con la tecnología actual, a los estafadores les es más fácil falsear la información del aparato de identificación de llamadas, así que el nombre y número que ve en el aparato no siempre son reales. Si alguien lo llama para pedirle dinero o información personal, cuelgue el teléfono. Si cree que la persona que lo llama podría estar diciendo la verdad, vuelva a llamar a un número que le conste que es genuino.
3. **Hable con alguien.** Antes de dar su información personal, hable con alguien de confianza. Los estafadores oportunistas quieren que usted tome decisiones apresuradamente. Incluso podrían amenazarlo. Desacelere, verifique la historia, haga **una búsqueda en internet**, consulte a un experto, recuerde que pueden llamarnos al 4060-2525 o escribirnos a instituciones@sicop.go.cr, para cualquier consulta.
4. **Reclamo de datos personales**. El estafador pide datos claves como excusa para evitarle multas con el Estado, tales como documento de identidad, número de cuenta y número de tarjeta de crédito.
5. **Protocolo de claves y contraseñas:** Una buena manera de evitar ser víctima de fraude es cambiar periódicamente las claves y contraseñas. Estas no deben ser obvias. Se deben evitar las claves con combinaciones de fechas de cumpleaños, número de identificación, número telefónico, entre otras, ya que pueden ser fácilmente deducidas por los estafadores.
6. **Soporte remoto:** En **SICOP**, hemos deshabilitado totalmente el uso de la herramienta de Soporte Remoto, para la atención de nuestros usuarios en el Centro de llamadas, por lo que si alguien se contacta con ustedes y les pide descargar esta herramienta, es con la finalidad de intentar sustraerle información y poder concretar una estafa financiera**.**
7. **Notificaciones de correo:** También es importante que tengan mucho cuidado si reciben correos de los supuestos administradores de sus contratos, verifiquen con detalle el remitente del correo, del cual recibieron la información y siempre ante la duda, favor comunicarse con nosotros o con la institución directamente, la seguridad de nuestros datos está en el cuidado que tengamos al dar acceso y nuestra información.
8. **Recepción de Mercadería:** En su contrato siempre encontrará indicado fecha y lugar de entrega de los bienes contratados, siempre diríjase al Administrador del Contrato, quien le podrá corroborar cualquier información de su contratación.
9. **Llamadas telefónicas:** Ni el Ministerio de Hacienda, ni Tributación, están realizando llamadas, para hacer actualizaciones en SICOP, con el tema de Factura Digital y pretender evitarles multas.

10. Después de recibir éste correo, nosotros **NO LOS ESTAREMOS LLAMANDO,** ésta no es una práctica común de nuestro servicio.

Evitar el fraude, está en nuestras manos, no seamos confiados y ante cualquier duda,

mejor cortar la llamada y llamar o escribir a los siguientes contactos: instituciones@sicop.go.cr

Centro de llamadas: 4060-2525