AVISO IMPORTANTE: INTENTOS DE FRAUDE MEDIANTE SUPLANTACION DE IDENTIDAD

Al igual que muchas otras empresas, estamos observando un aumento de los intentos de fraude que utilizan indebidamente el nombre, la identidad visual o los datos de contacto de nuestra empresa, en particular mediante la creación de nombres de dominio falsos con el fin de engañar a la persona con la que se contacta y, en algunos casos, a antiguos empleados a través de aplicaciones de mensajería instantánea.

El objetivo de estas prácticas es engañar a los inversores ofreciéndoles productos financieros falsos, oportunidades de inversión falsas o intentando obtener información personal o bancaria.

Le recomendamos que esté atento para protegerse y le recordamos que:

- Nuestra página web oficial es https://www.comgest.com.
- Comgest no utiliza las redes sociales ni las aplicaciones de mensajería instantánea (como WhatsApp) como medio de contacto.

➢ Fraude y suplantación de identidad

El fraude es un acto intencionado de engaño u ocultación con el fin de obtener una ventaja indebida en detrimento de otra persona. Abarca una amplia gama de comportamientos desleales, como la suplantación de identidad cuando se utiliza con fines maliciosos.

La suplantación de identidad consiste en apropiarse deliberadamente de la identidad de una persona física o jurídica, o en utilizar sus datos de identificación (nombre, logotipo, dirección de correo electrónico, documentos oficiales) con el fin de engañar a un tercero. Cuando tiene por objeto obtener una ventaja indebida o causar un perjuicio, la usurpación de identidad constituye una forma de fraude y también puede considerarse estafa.

➢ ¿Qué medidas hay que tomar para protegerse del fraude?

- Tenga mucho cuidado con cualquier contacto no solicitado por teléfono, correo electrónico, SMS, redes sociales o aplicaciones de mensajería instantánea. Sea cual sea la forma (teléfono, correo, correo electrónico o mensaje), las usurpaciones son frecuentes, numerosas y fáciles de realizar.

- No facilite ninguna información personal (teléfono, correo electrónico, documentos de identidad, datos bancarios, IBAN, justificantes de domicilio...) a través de un sitio web o por teléfono a una persona que afirme representarnos, sin haber comprobado su autenticidad a través de nuestros canales oficiales.

- Infórmese sobre la empresa a la que dice pertenecer su interlocutor buscando sus datos de contacto oficiales (teléfono, correo electrónico y dirección postal) a través de otras fuentes para verificar la veracidad de la información proporcionada y no dude en verificar la

identidad de sus interlocutores enviando un correo electrónico o llamando a los números de teléfono que figuran en los sitios web oficiales.

- Si un mensaje le parece proceder de una fuente desconocida o dudosa, no haga clic en los enlaces ni abra los archivos adjuntos, y no responda.

Para obtener más recomendaciones, le invitamos a consultar la información educativa publicada en línea por la Autoridad de Mercados Financieros de Francia o por su regulador local.

➢ ¿Qué hacer si cree que ha sido víctima de un fraude?

1. Si el fraude está relacionado con Comgest, infórmenos directamente a la direcciónino@comgest.com .

2. En caso de suplantación de identidad a través de WhatsApp, denuncie el mensaje, el grupo y/o el perfil sospechoso de la siguiente manera y, a continuación, elimine el mensaje de su dispositivo después de denunciarlo:
    - Denuncia de un perfil: haga clic en el contacto que desea denunciar y, en la parte inferior de la página, haga clic en «Denunciar + número de teléfono».
    - Denuncia de un grupo: haga clic en el nombre del grupo en la parte superior de las conversaciones y, a continuación, en la parte inferior de la página, haga clic en «Denunciar el grupo».

3. Si es usted ciudadano francés, realice una denuncia a través de Pharos (portal oficial del Ministerio del Interior para la denuncia de contenidos ilícitos en Internet): https://internet-signalement.gouv.fr/.