Síguenos en

JORNADA “FRAUDE DIGITAL EN LA EMPRESA: PREVENCIÓN, RESPUESTA Y DEFENSA JURÍDICA”

El fraude digital tiene ya tiene un coste de 300 millones de euros al año en España

Nueve de cada diez ciberdelitos producidos en nuestro país están relacionados con ciberestafas

Las primeras horas tras detectar el fraude resultan decisivas para paralizar las transferencias y recuperar el dinero

Grant Thornton propone reforzar los controles internos y la protección jurídica para recuperar los fondos sustraídos



Ignacio Ripol y Eloi Font, socios de Legal de Grant Thornton, durante la presentación de la jornada

USO RESTRINGIDO -INFORMACIÓN DE DIFUSIÓN LIMITADA-

Barcelona, 5 de noviembre de 2026

El fraude digital se ha convertido en una amenaza creciente para las empresas, no solo por sus consecuencias económicas, sino también por las **responsabilidades legales y de cumplimiento** que puede generar. **Grant Thornton** ha celebrado hoy en **Barcelona** el encuentro **«Fraude digital en la empresa: prevención, respuesta y defensa jurídica»**, un desayuno práctico dirigido a analizar cómo pueden las organizaciones anticiparse a estos riesgos, actuar ante un incidente y proteger sus intereses por la vía legal.

Durante la jornada, **Ignacio Ripol y Eloi Font, socios de Legal de Grant Thornton**, han expuesto la dimensión que está alcanzando este fenómeno y sus implicaciones para el tejido empresarial. Según los datos presentados durante el encuentro, **las ciberestafas representan el 87,3% de los ciberdelitos**. En Cataluña, constituyen **el segundo delito más denunciado**, solo por detrás de los hurtos, con **más de 80.000 denuncias anuales —unas 220 al día—** y **más de 200.000 víctimas** entre 2024 y agosto de 2026.

El impacto económico también refleja la magnitud del problema. Las últimas cifras disponibles, procedentes del BCE y la EBA, apuntan a un coste de **4.200 millones de euros en el Espacio Económico Europeo** y de **300 millones de euros en España**. A esta situación se suma la evolución de las técnicas de ataque, **impulsadas por la inteligencia artificial**, que permiten desarrollar fraudes más sofisticados y dirigidos. Aunque pueden reducir el número de víctimas, estos ataques perfilan cada vez más sus objetivos, con **especial atención a directivos y empresas**.

Según ha señalado Font, “con la llegada de la Inteligencia Artificial igual hay menos víctimas, **pero están más seleccionadas e identificadas y se les puede atacar más fácilmente**”. “Es evidente que todos los ciudadanos y empresas **vamos a ser víctimas de un ciber incidente** y por ello tenemos que estar preparados para reaccionar con agilidad y poner las medidas oportunas”, ha añadido.

Un riesgo para los administradores

Uno de los aspectos centrales del encuentro ha sido la **responsabilidad de los órganos de administración** en la prevención y gestión de los riesgos digitales.

USO RESTRINGIDO -INFORMACIÓN DE DIFUSIÓN LIMITADA-

La creciente exposición de las organizaciones a este tipo de amenazas exige **reforzar los mecanismos de control interno** y acreditar que se han adoptado las medidas de seguridad y diligencia necesarias.

En este sentido, los expertos han recordado que **la obligación de los administradores es de medios y no de resultado**: no se trata de garantizar que nunca se produzca un incidente, sino de implantar las medidas adecuadas y asegurar que se utilizan correctamente. Marcos regulatorios como **NIS2 y DORA** refuerzan, además, la responsabilidad de los órganos de dirección en materia de ciberseguridad y resiliencia operativa.

"La responsabilidad de los órganos de administración en materia de prevención de la ciberdelincuencia es cada vez más clara. **La CNMV está incorporando nuevas recomendaciones** para que los consejos de administración establezcan medidas de prevención frente a estos riesgos", ha señalado Ripol.

Entre las principales medidas preventivas recomendadas figuran **la formación periódica de los empleados** y los ejercicios de concienciación, **la doble o triple verificación** ante cambios en las cuentas de cobro de clientes o de pago a proveedores, y el establecimiento de **sistemas de apoderamiento** que impidan que una única persona pueda ordenar y ejecutar determinados pagos. También se ha destacado la importancia de contar con **pólizas de ciberseguridad** adecuadas, realizar **auditorías periódicas y pruebas de intrusión**, disponer de **protocolos internos frente a suplantaciones** y mantener formalizados los contratos con proveedores críticos.

Claves para recuperar los fondos

La respuesta durante las primeras horas tras detectar un fraude resulta determinante para limitar sus consecuencias y aumentar las posibilidades de recuperar el dinero. Los expertos han insistido en la necesidad de **activar de inmediato un protocolo** que incluya el análisis técnico del incidente, la preservación de las evidencias digitales y la valoración de su alcance, especialmente cuando pueda existir una afectación de datos personales.

En palabras de Ripol, "la vía penal tiene un recorrido muy limitado en este tipo de fraudes. **Aunque se consiga identificar al titular de la cuenta, el dinero suele haber desaparecido o estar repartido entre otras cuentas.** Por eso, la

USO RESTRINGIDO -INFORMACIÓN DE DIFUSIÓN LIMITADA-

reclamación frente a la entidad financiera puede convertirse en la principal vía para recuperar los fondos."

Entre las primeras actuaciones se encuentra **contactar urgentemente con la entidad financiera para intentar paralizar la transferencia**, documentar el incidente y, cuando corresponda, **notificar la brecha de seguridad a la Agencia Española de Protección de Datos en el plazo máximo de 72 horas**. También puede ser necesario informar a los afectados, denunciar los hechos ante las autoridades policiales y comunicar el incidente a organismos especializados como **INCIBE o Catalonia-CERT**.

La jornada ha dedicado asimismo una parte específica a las **reclamaciones frente a las entidades financieras y a la recuperación de los fondos sustraídos**. En este ámbito, se han analizado las obligaciones de las entidades en las operaciones de pago no autorizadas y la evolución reciente de la jurisprudencia. En particular, se ha abordado **la sentencia del Tribunal Supremo 571/2025, de 9 de abril**, y **la sentencia del Tribunal de Justicia de la Unión Europea de 15 de octubre de 2026, en el asunto C-70/25 (Tukowiecka)**, relativa a la interpretación de las obligaciones de reembolso en operaciones de pago no autorizadas.

Con este encuentro, Grant Thornton ha puesto el foco en la necesidad de abordar el fraude digital desde una perspectiva integral, que combine **prevención tecnológica, cultura de control interno y preparación jurídica**. La capacidad de **anticiparse a los riesgos, reaccionar con rapidez y contar con una estrategia legal adecuada** resulta esencial para proteger los activos, la actividad y la reputación de las organizaciones.

Sobre Grant Thornton

En Grant Thornton España ayudamos a que tu empresa vaya más allá. Servicios profesionales de Auditoría & Assurance, Advisory, Tax, Asesoramiento Financiero, Legal, Laboral y Outsourcing. 11 oficinas y 900 profesionales en nuestro país. Pertenecemos a Grant Thornton Advisors, una plataforma multinacional y multidisciplinar que proporciona una experiencia de cliente única y transfronteriza, con soluciones y capacidades potenciadas por la última tecnología y los mejores equipos. A su vez, formamos parte de Grant Thornton International, una de las redes globales de servicios profesionales líderes, con 80.000 profesionales presente en más de 150 mercados en todo el mundo.

USO RESTRINGIDO -INFORMACIÓN DE DIFUSIÓN LIMITADA-

Síguenos en

Para ampliar información o hablar con profesionales de Grant Thornton, no dudes en llamarnos:

DEPARTAMENTO COMUNICACIÓN GRANT THORNTON

POLICARPO AROCA
Director de Comunicación, Marketing y Desarrollo de Negocio
T 91 576 39 99
M 650 71 31 21
Policarpo.aroca@es.gt.com

JOSÉ MARÍA GÓMEZ VALLEJO
Supervisor de Comunicación Corporativa
T 91 576 39 99
M 681 15 65 13
josemaria.gomez@es.gt.com

MARTA CARDENAL
Técnica de Comunicación Corporativa
T 932 06 39 00
M 608 99 02 14
marta.cardenal@es.gt.com

LEAD BY THOUGHT

MARÍA CUESTA
+34 646 494 090
maria.cuesta@leadbythought.com

GUILLERMO GINÉS
+34 637 916 561
guillermo.gines@leadbythought.com

USO RESTRINGIDO -INFORMACIÓN DE DIFUSIÓN LIMITADA-